ZYXEL

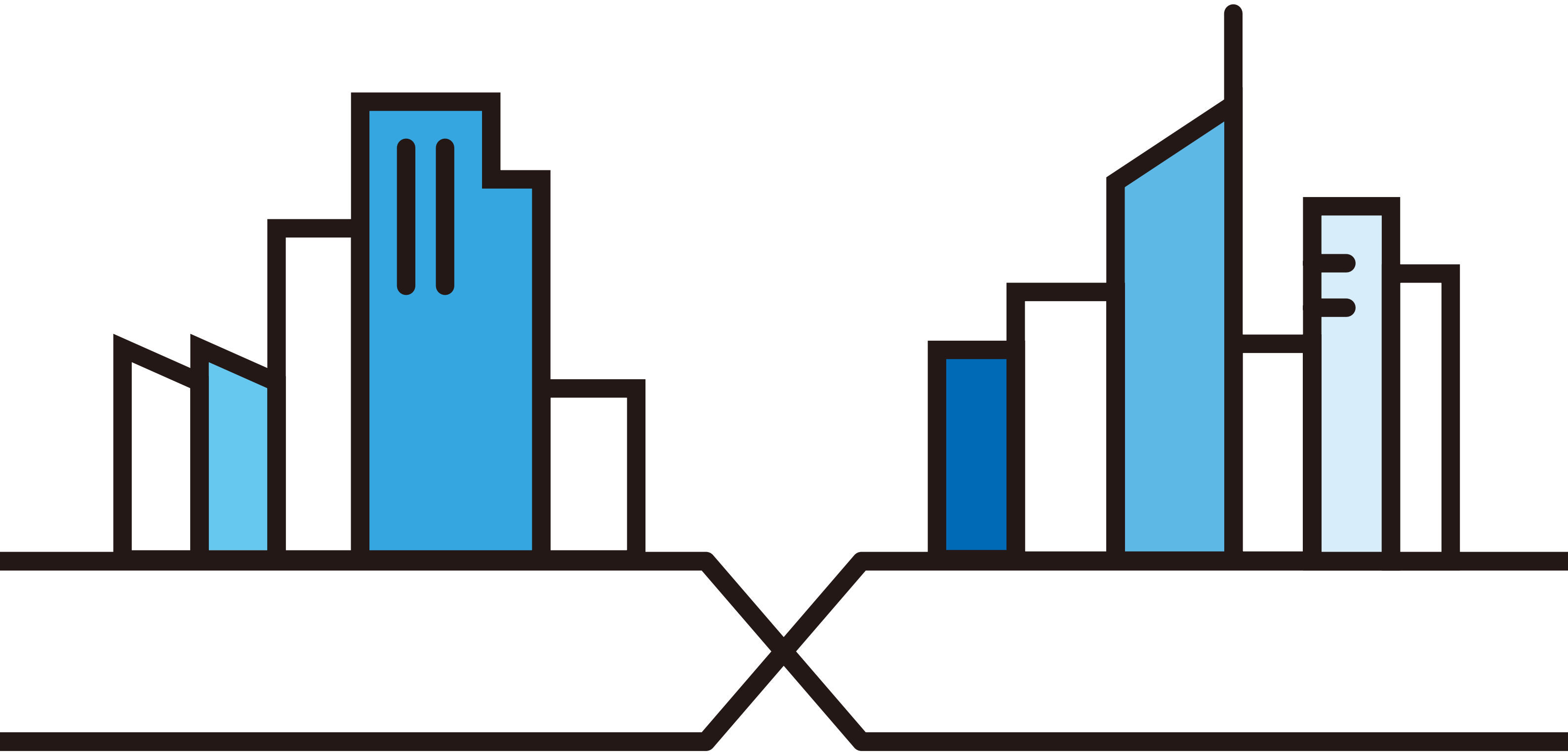
# User's Guide

# NR2111

5G NR Portable Router

Version 1.00 Edition 1, 08/2025

| Default Login Details | |
|---|---|
| LAN IP Address | http://192.168.1.1 |
| Login | admin |
| Password | See the NR2111's LCD About screen |



**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

Screenshots and graphics in this book may differ slightly from what you see due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

## Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NR2111.

- Go to *https://service-provider.zyxel.com/global/en/tech-support* to find other information on the NR2111.

# Contents Overview

# Table of Contents

**Chapter 8**

**Chapter 9**

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this guide.

**Warnings tell you about things that could harm you or your device.**

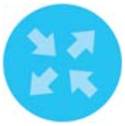
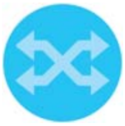
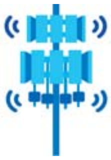
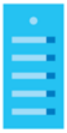
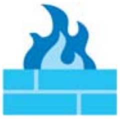
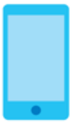
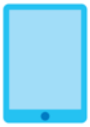
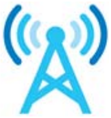
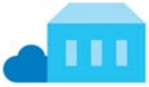
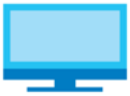
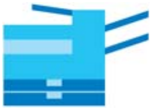
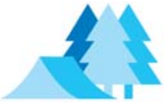
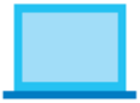
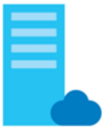
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **APP MODULE** > **Firewall** > **Port Trigger** means you first click **APP MODULE** in the menus, then **Firewall** and finally the **Port Trigger** tab to get to that screen.

## Icons Used in Figures

Figures in this user guide may use the following generic icons. The NR2111 icon is not an exact representation of your device.

| | | |
|---|---|---|
| NR2111<br> | Switch<br> | 5G/4G Base Station<br> |
| Server<br> | Firewall<br> | Smartphone<br> |
| Tablet<br> | Antenna Tower<br> | Home<br> |
| Desktop<br> | Printer<br> | Outdoors<br> |
| Notebook<br> | Office<br> | |

# Accessibility and Compatibility

## Introduction

This User's Guide complies with the accessibility requirements set out in EAA (European Accessibility Act) (EU) 2019/882.

Accessibility makes this User's Guide usable for people with disabilities, including those with visual, auditory, motor, and cognitive impairments. Compatibility ensures this User's Guide works well with a wide range of devices, software, and assistive technologies.

## Accessibility Feature – Screen Reader Support

The visually impaired may use screen readers, such as NVDA to read contents.

To use the screen reader, do the following:

**1** Open your screen reader software.

**2** Navigate to this User's Guide; the screen reader should automatically start reading the contents.

**3** Use the keyboard shortcuts to navigate through this User's Guide (refer to the screen reader documentation).

## Accessibility Feature – Keyboard Navigation

Keyboard navigation allows you to read the contents in this User's Guide without a mouse. Use the following keys.

- **Tab** key: navigate between interactive elements (for example, buttons, links, fields).
- **Enter** key: select or activate the highlighted item.
- Arrow keys: move between options in menus or lists.
- **Esc** (Escape) key: close pop-up windows or cancel actions.

## How to Get Support

If you are an Internet Service Provider (ISP), please contact your Zyxel sales or service representative for direct support.

If you obtained your NR2111 from an ISP, please contact your ISP's support team directly, as the NR2111s may have custom configurations.

# PART I

# User's Guide

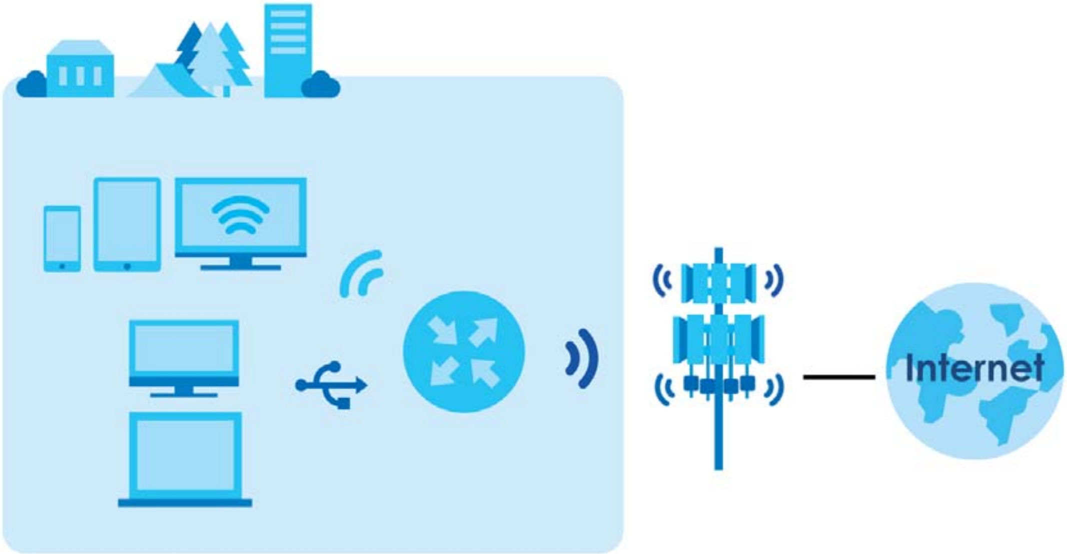
# CHAPTER 1
# Get to Know Your NR2111

## 1.1 Overview

The NR2111 is a 5G NR portable router that complies with the 3GPP release 15 standard, ensuring seamless compatibility with 4G networks. Offering high-speed broadband service through Wi-Fi 6, it provides enhanced network security and supports up to 32 connected devices. With its compact design, subscribers can stay connected on the go, enjoying unparalleled connectivity and convenience.

The NR2111 supports the Wi-Fi 6 (802.11ax) standard. The NR2111 delivers premium speed for multi-streaming data access and optimal Wi-Fi experience without dead zones.

**Figure 1** NR2111 Application



## 1.2 Applications

### Wireless WAN

The NR2111 can connect to the Internet through a Nano SIM card to access a 4G or 5G wireless WAN connection. Just insert a Nano SIM card into the SIM card slot on the NR2111.

### Wired LAN (USB Tethering)

A computer with Windows or Mac OS can connect to the NR2111's USB Type-C port with a Type-A to Type-C USB cable to access the Web Configurator.

### Wireless LAN (Wi-Fi)

The NR2111's Wi-Fi allows access to high-speed broadband service and local management. Connect a computer/smartphone/tablet to the NR2111's Wi-Fi and use the Web Configurator to configure your NR2111.

## 1.3 Ways to Manage the NR2111

Use any of the following methods to manage the NR2111.

- LCD Screen Interface: You can use the LCD screen interface along with the buttons to manage it.
- Web Configurator. This is recommended for management of the NR2111 using a (supported) web browser.

## 1.4 Good Habits for Managing the NR2111

Do the following things regularly to make the NR2111 more secure and to manage the NR2111 more effectively.

- Change the Wi-Fi and Web Configurator passwords. Use a password that is not easy to guess and that consists of different types of characters, such as numbers, letters, and special characters.
- Write down the passwords and put it in a safe place.
- Back up the configuration. Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NR2111 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NR2111. You could simply restore your last configuration.

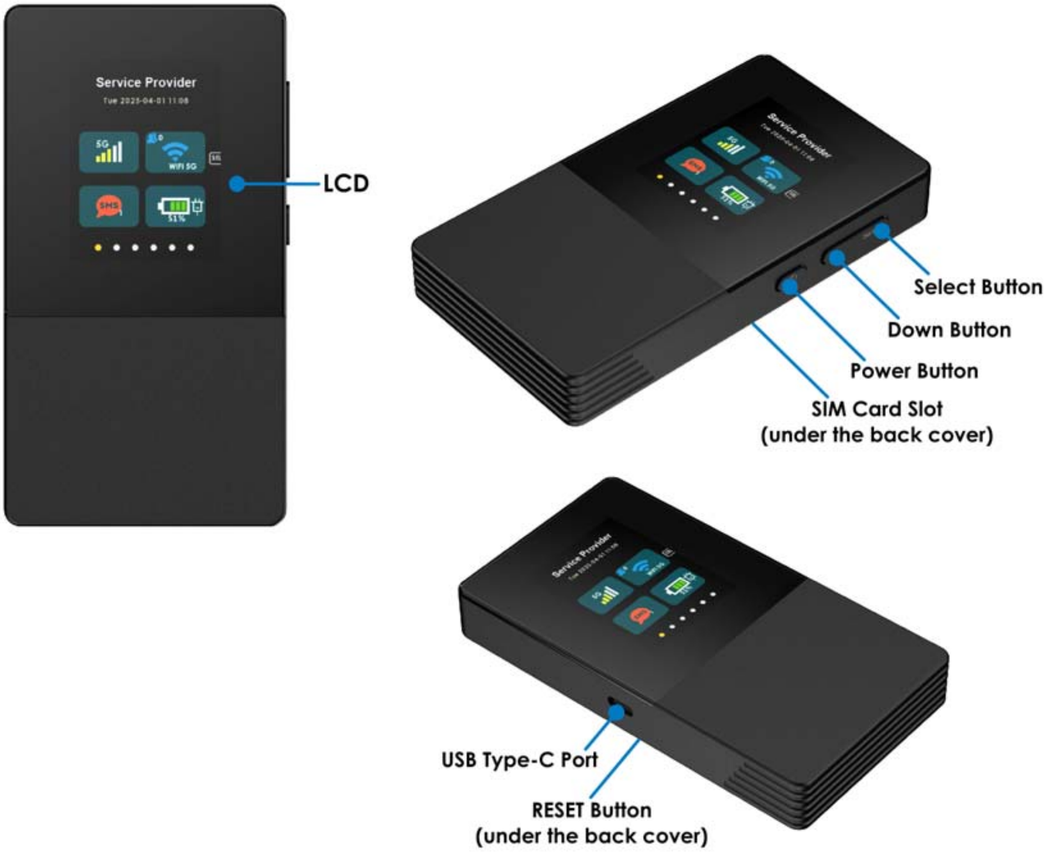
## 1.5 Hardware Description

This section describes the front, rear, and side panels of the NR2111. Refer to the NR2111's Quick Start Guide for product illustrations and hardware connection instructions.

Place the NR2111 with the LCD screen facing you with the USB Type-C port is on the left.

The following figures show the port, buttons and SIM card slot of the NR2111.

**Figure 2** NR2111's Ports, Buttons and SIM Card Slot



### 1.5.1 Power Button

Use the power button on the right side panel to do the following.

- Power on: Press and hold the power button for about 6 seconds until the LCD screen turns on.
- Power off: When the LCD is on, press and hold the power button for about 6 seconds until the LCD screen displays **Shut down**.
- Waking up the screen: The LCD turns off automatically after 30 seconds when idle. Press the power button once to turn it back on.

### 1.5.2 Hardware Connections

See your Quick Start Guide for more information about hardware installation.

### 1.5.3 Reset the NR2111

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously, such as Wi-Fi SSID and password. The default LAN IP address and login password will be reset to the factory default (see the LCD screens).

1 Remove the back cover.

2 Use a pin or a paper clip to press the **RESET** button to reset the NR2111 to the factory default settings.

# 1.6 LCD Screens

This section describes the screens, labels, icons, buttons displayed on the LCD screen of your NR2111. The LCD screen turns off after 30 seconds when idle. Press the power button once to turn the LCD screen back on. Press the **Down** button to switch between the screens.

### LCD Screens Summary

- Main Screen: View the NR2111's overall information.
- Bandwidth Usage: View the upload/download speed and the total amount of consumed data. Set up the network connection.
- Wi-Fi LCD Screen: View the Wi-Fi information and set up the Wi-Fi network.
- WPS LCD Screen: Activate the WPS on the NR2111.
- SMS LCD Screen: View and manage messages.
- About LCD Screen: View the device and network information, check the firmware, and change the display language.

### LCD Button Labels

The following table describes the LCD button labels.

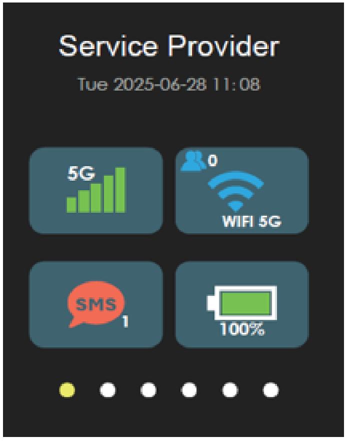
Table 1 LCD Button Labels

| LABEL | DESCRIPTION |
|---|---|
| SEL | Use it to switch between options. |
| ☰ | Use it to open the setup window. |
| OK | Use it to confirm your selection. |
| WPS | Use it to activate your NR2111's WPS. |

## 1.6.1 Main Screen

The main screen displays when the NR2111 is turned on.

**Figure 3** Main LCD Screen



The following table describes the labels in this screen.

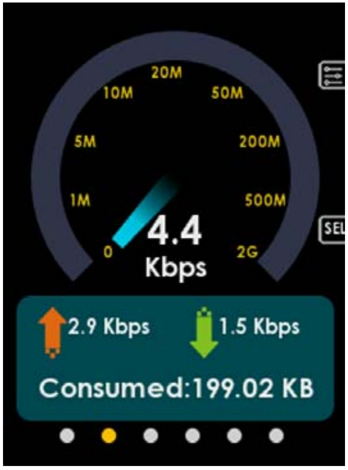
Table 2 Main LCD Screen

| **LABEL** | **DESCRIPTION** |
|---|---|
| (Service Provider) | This displays your NR2111's Internet Service Provider. |
| Date and time | This displays the current date and time. |
| 4G 5G | This displays the type of network the NR2111 is connected to and its signal strength. |
| ✕ | This displays if the NR2111 could not detect a SIM card. |
| 🔒 | This displays when the NR2111 cannot access the SIM card because it is locked. |
| 2 WIFI 5G | This displays the Wi-Fi band currently in use. The number next to the user icon indicates how many client devices are currently connected to the NR2111. |
| SMS 1 | This displays the number of new messages. |
| 100% | This displays the percentage of battery power left on the NR2111. |

## 1.6.2 Bandwidth Usage

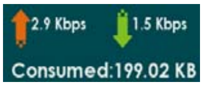
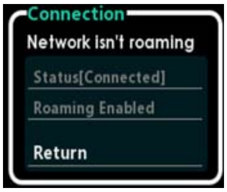
This screen shows the real-time bandwidth usage, including the current upload and download speeds as well as the total data used.

**Figure 4** Bandwidth Usage LCD Screen



The table below describe the labels on this screen.

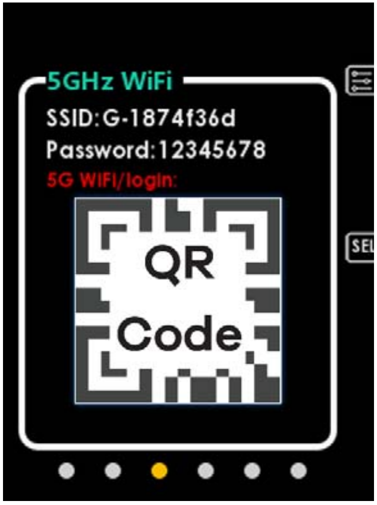
Table 3 Bandwidth Usage LCD Screen

| LABEL | DESCRIPTION |
|---|---|
|  | This displays the real-time NR2111's upload/download speed when receiving/ transmitting data to/from the Internet. **Consumed** shows the total data usage, with the gauge chart above providing a visual representation. |
| Connection<br>  Connection Network isn't roaming Status[Connected] Roaming Enabled Return | Press the **Select** button to open the **Connection** setting screen. |
| Status [Connected/ Disconnected] | Select this to enable or disable the network of the NR2111. See Network Chapter for more information. |
| Roaming Enabled/ Disabled | Select this to enable or disable roaming on the NR2111. See Network Chapter for more information. |
| Return | Select this to return to the bandwidth usage screen. |

## 1.6.3 Wi-Fi LCD Screen

This screen displays Wi-Fi information. You can use it to select a Wi-Fi band for client devices to connect to your NR2111.

**Figure 5** Wi-Fi LCD Screen



5GHz WiFi

SSID:G-1874f36d

Password:12345678

The table below describe the labels on this screen.

Table 4 Wi-Fi LCD Screen

| LABEL | DESCRIPTION |
|---|---|
| 2.4GHz/5GHz Wi-Fi | This displays the currently enabled Wi-Fi band on the NR2111. |
| SSID | This displays the descriptive name used to identify the NR2111. Client devices use this name to connect to the NR2111. |
| Password | This displays the password of the Wi-Fi. Client devices use this password to connect to the NR2111. |
| 2.4/5G Wi-Fi/login | A client device can simply scan this QR code to connect to the Wi-Fi network without manually selecting the SSID and entering the password. |
| Wi-Fi Band | You can change the Wi-Fi band by pressing the **Select** button to open the Wi-Fi Band setting window. |
| 2.4G Wi-Fi | Select this to enable the **2.4G** band. **(Current)** indicated the currently enabled band. |
| 5G Wi-Fi | Select this to enable the **5G** band. **(Current)** indicated the currently enabled band. |
| Return | Select this to return to the Wi-Fi screen. |

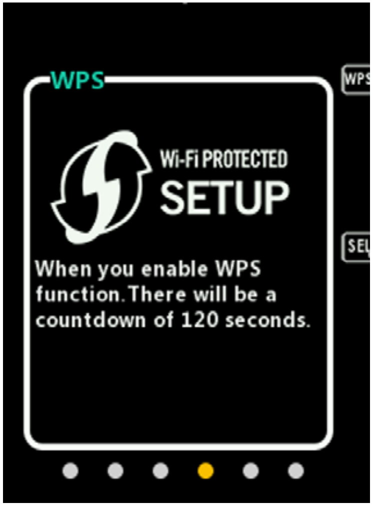
## 1.6.4 WPS LCD Screen

Your NR2111 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure Wi-Fi network. WPS is an industry standard specification, defined by the Wi-Fi Alliance. You can use this LCD screen to activate WPS to set up a Wi-Fi network with security.

WPS allows you to quickly set up a Wi-Fi network with security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

Note: You can activate WPS from this LCD screen only after enabling the **WPS** in the Web Configurator at **APP MODULE > WPS**. Refer to Section 9.11 on page 95 to allow your NR2111 activate WPS from this LCD screen.

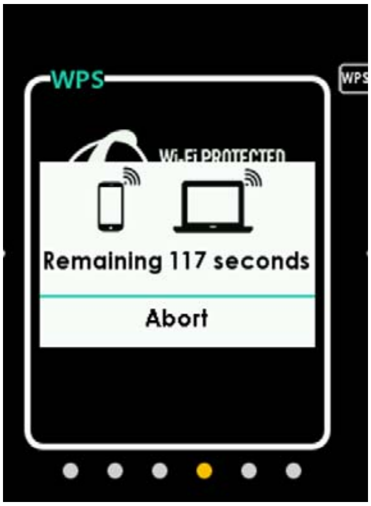
**Figure 6** WPS LCS Screen



When you enable WPS function.There will be a countdown of 120 seconds.

Press the **Select** button on the device to start WPS pairing with another WPS-enabled device within range of the NR2111. You have to activate WPS on the NR2111 and on another device within 2 minutes of each other.

To abort the pairing, press the **Select** or **Down** button to select **Abort**. The NR2111 will stop the WPS pairing process.

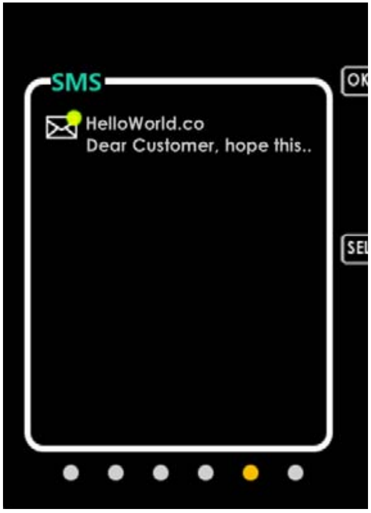


Remaining 117 seconds

## 1.6.5 SMS LCD Screen

SMS (Short Message Service) allows you to view the text messages that the NR2111 received from the service provider. When the SMS box is full the NR2111 automatically deletes the oldest SMS message.

**Figure 7** SMS LCD Screen



SMS

HelloWorld.co
Dear Customer, hope this..

The table below describe the labels on this screen.

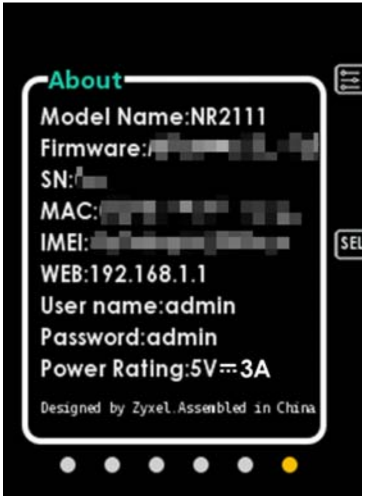
Table 5 SMS LCD Screen

| LABEL | DESCRIPTION |
|---|---|
| SMS (overview) | This is the list of messages you receive. A green dot indicates the message is unread. |
| SMS (detail) | Press the **Select** button to view/manage the messages.<br>Press the **Down** button to switch between the messages. Press the **Select** button to select the message you want to view or manage. A select menu display. |
| View | Select this to view the full message. When you're done reading, press the **Select** button to choose **OK**. |
| Cursor up | Select this to get back to the previous message. |
| Cancel | Select this to delete the message. |
| Return | Select this to return to the SMS overview screen. |

Note: It is highly recommended to delete unwanted SMS messages to prevent the SMS box from getting full.

## 1.6.6 About LCD Screen

Use the **About** screen to view the NR2111's hardware and network information, check the firmware, and change the device language.



About<br>
Model Name:NR2111<br>
Firmware:[redacted]<br>
SN:[redacted]<br>
MAC:[redacted]<br>
IMEI:[redacted]<br>
WEB:192.168.1.1<br>
User name:admin<br>
Password:admin<br>
Power Rating:5V⎓3A<br>
Designed by Zyxel.Assembled in China

**Figure 8** About LCD Screen

The following table describes the labels on this screen.

Table 6 About LCD Screen

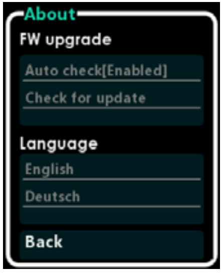
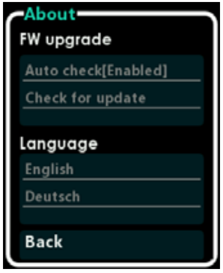
| LABEL | DESCRIPTION |
|---|---|
| Model Name | This displays the model name of your NR2111 |
| Firmware | This displays the present firmware version of your NR2111. |
| SN | This displays the serial number issued by the manufacturer for your NR2111. |
| MAC | This displays the MAC address of the NR2111. |
| IMEI | This displays the International Mobile Equipment Number (IMEI) which is the serial number of the built-in 4G/5G module. IMEI is a unique 15-digit number used to identify a mobile device. |
| WEB | This displays the IP address of the NR2111. Launch your web browser and use this IP address to access the Web Configurator. |
| User name | This displays the default user name of your NR2111. |
| Password | This displays the default password of your NR2111. |
| Power Rating | This displays the NR2111's power rating in volts and amperes. |
| FW upgrade<br><br>About<br>FW upgrade<br>Auto check[Enabled]<br>Check for update<br>Language<br>English<br>Deutsch<br>Back | Press the **Select** button to get in to the setup screen. |
| Auto check [Enable/ Disable] | Select this to enable or disable automatic check for new firmware. If there is new firmware version available, a reminder will display on the LED when you power on the NR2111. Select **OK** to update the firmware or select **Cancel** to dismiss the reminder. |
| Check for update | Select this to see if any new firmware is available. If there is a new firmware version available, a reminder will display. Select **OK** to update the firmware or select **Cancel** to dismiss the reminder. |

Table 6   About LCD Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| Language<br><br> About<br>FW upgrade<br>Auto check[Enabled]<br>Check for update<br>Language<br>English<br>Deutsch<br>Back | Press the **Select** button to get in to the setup screen.<br>Press the **Down** button to select the desired language then press the **Select** button to confirm. **(Current)** indicated the currently used language. |
| Back | Select this to return to the previous screen. |

# CHAPTER 2 Web Configurator

## 2.1 Introduction

The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

## 2.2 Accessing the Web Configurator

This section shows how to access the Web Configurator through Wi-Fi and wired connections. Follow the steps below to connect your device to the NR2111. For the first login, you can only access the Web Configurator through a Wi-Fi connection.

**1** Ensure your NR2111 hardware is properly assembled. See the Quick Start Guide.

**2** Connect your device to the NR2111 using the Wi-Fi or the included USB cable.

**2a** Wi-Fi Connection

From a Wi-Fi-enabled device, use the default SSID and Wi-Fi password to connect to your NR2111. You can find the default SSID and the Wi-Fi password from the **Wi-Fi** screen of the NR2111's LCD. If your device has a camera, simply scan this QR code shown on the LCD to connect to the Wi-Fi without manually selecting the SSID and entering the password.

**2b** Wired Connection

Use the included USB cable to connect your device to the NR2111.

Note: You can only connect to the NR2111 through the USB cable when the **USB Network** is enabled. To do this, first access the Web Configurator through a Wi-Fi connection (see Section 2 on page 22). Then, enable the **USB Network** from the wizard (see Section 2.2.1 on page 23) or **APP MODULE** > **USB Network** (see Section 9.18 on page 102).

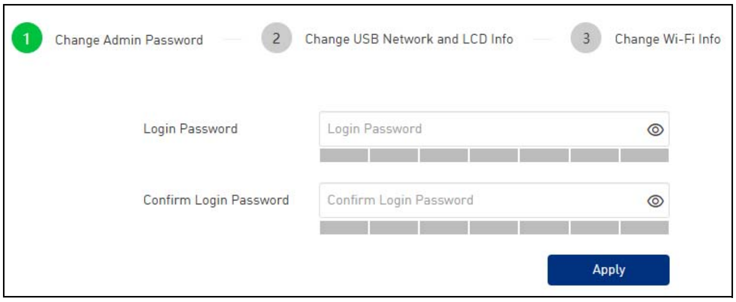
**3** Launch your web browser. Enter http://192.168.1.1 in your browser address bar. Make sure your device has an IP address in the same subnet as the NR2111. Your device should have an IP address from 192.168.1.2 to 192.168.1.254. See your device help or refer to Section 10.6 on page 118.

4 The login screen displays. Enter the default username **admin** and password. You can find the default password from the **About** screen of the NR2111's LCD.

## 2.2.1 Wizard

For the first login, the wizard displays after the login. Set up these configurations to secure your network.

1 **Change Admin Password**: Enter a new login password with a minimum length of 5 and up to 32 characters. Special characters and spaces are allowed. Reenter the new password to confirm. Click **Apply**.

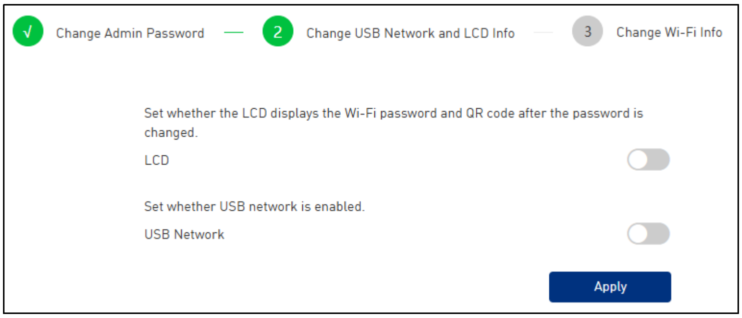


Login Password: Login Password

Confirm Login Password: Confirm Login Password

2 **Change USB Network and LCD Info**: Enable or disable the following features by sliding the switch to the right or left. Click **Apply** after you finish the setup.

- **LCD**: Turn this on to display the Wi-Fi password and the QR code for Wi-Fi connection on the NR2111's LCD **Wi-Fi** screen. See Section 1.6.3 on page 16 for more information.
- **USB Network**: Turn this on to allow a device to connect to the NR2111's LAN through a wired connection. See Section 9.18 on page 102 for more information.



Set whether the LCD displays the Wi-Fi password and QR code after the password is changed.

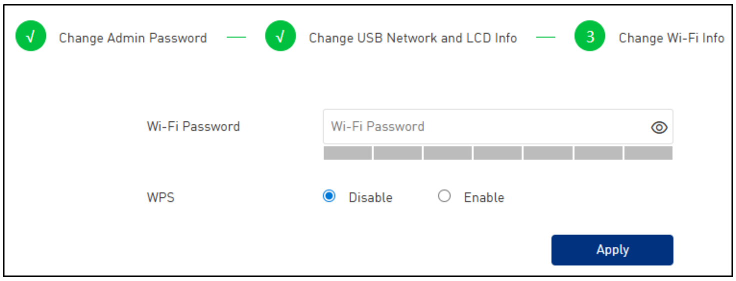
LCD

Set whether USB network is enabled.

USB Network

3 **Change Wi-Fi Info**: Set up a new Wi-Fi password and enable or disable the WPS function on the NR2111. Click **Apply** to finish the wizard setup.

- **Wi-Fi Password**: Enter a new Wi-Fi password with a minimum length of 8 and up to 64 characters. Special characters and spaces are allowed.
- **WPS**: Select **Enable** to allow the NR2111 to activate WPS. Or select **Disable** to prevent the NR2111 from activating WPS.



√ Change Admin Password — √ Change USB Network and LCD Info — 3 Change Wi-Fi Info

Wi-Fi Password: Wi-Fi Password

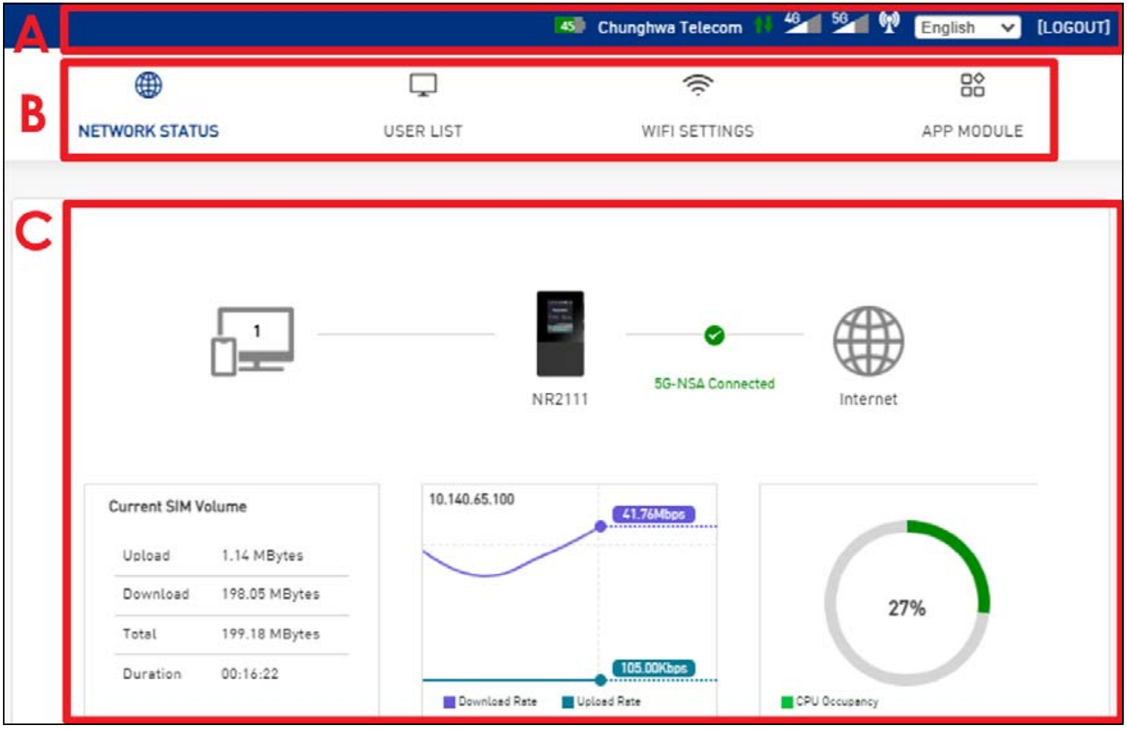
WPS: ● Disable ○ Enable

Apply

## 2.3 Web Configurator Layout

This section summarizes the layout of the Web Configurator.

**Figure 9** Web Configurator Layout



Current SIM Volume

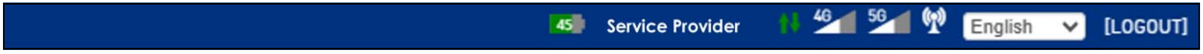
| | |
|---|---|
| Upload | 1.14 MBytes |
| Download | 198.05 MBytes |
| Total | 199.18 MBytes |
| Duration | 00:16:22 |

- **A** - Title Bar
- **B** - Menus
- **C** - Main Window

### 2.3.1 Title Bar

The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

**Figure 10** Title Bar



The icons provide the following functions.

Table 7   Title Bar: Web Configurator Icons

| LABEL | DESCRIPTION |
|---|---|
| Unread messages | This shows the number of unread SMS messages in the NR2111. Click this to go to the **APP MODULE** > **Messages** screen to read the messages. |
| Battery 45 | The shows the battery status. |
| (Service Provider) | This shows the name of the ISP (Internet Service Provider) of the SIM card that the NR2111 is using. |
| No SIM No SIM | This shows when no SIM card is detected by the NR2111. |
| Transmission ⇅ | This shows when the NR2111 is receiving/transmitting data to/from the Internet. |
| Signal Strength<br>4G 5G | This shows the current signal strength to the mobile network.<br>The icon is grayed out if the mobile data connection is not up. |
| Wi-Fi | This shows whether the NR2111's Wi-Fi network is active. |
| Language | This shows the language that your Web Configurator is currently using. Select your preferred option from the drop-down list to change the language. |
| LOGOUT | Click this to log out from the NR2111's Web Configurator. |

## 2.3.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

After you log in, the **Status** screen is displayed. See Chapter 4 on page 45 for more information about the **Status** screen.

## 2.3.3 Menu List

Use the **Menu** list to open screens to configure NR2111 features.

**Figure 11**   Menu List

NETWORK STATUS    USER LIST    WI-FI SETTINGS    APP MODULE

The following table introduces the menus.

Table 8   Menus Summary

| LINK | TAB | DESCRIPTION |
|---|---|---|
| NETWORK STATUS | | Use this screen to view the network status of the NR2111 and devices connected to it. |
| USER LIST | Online Users | Use this screen to view and configure clients that are currently connected to the NR2111. |
| | Offline Users | Use this screen to view and configure clients that were connected to the NR2111 previously. |
| | Allow/Forbidden Users | Use this screen to view and add clients that are allowed/denied access to the NR2111. |
| | MAC Filter Mode | Use this screen to configure the NR2111's MAC filter mode. |
| WI-FI SETTINGS | Wi-Fi Settings | Use this screen to enable and configure the 2.4G/5G Wi-Fi settings and security. |

Table 8 Menus Summary (continued)

| LINK | TAB | DESCRIPTION |
|---|---|---|
| APP MODULE | Status | Use this screen to view the NR2111's device status and information. |
| | Statistics | Use this screen to view the SIM card's usage details. |
| | Network Information | Use this screen to view the NR2111's network information. |
| | Network Settings | Use this screen to configure the NR2111's network, APN, and roaming settings. |
| | Network Operators | Use this screen to view available PLMNs (Public Land Mobile Networks) and select your preferred network. |
| | DHCP & DNS | Use this screen to configure DHCP and DNS settings on the NR2111. |
| | Package Settings | Use this screen to set up a limited allowance of data on the NR2111. |
| | Firewall | Use these screens to configure IP filters, port forward, port trigger, remote management, and DMZ. |
| | IP Filter | Use this screen to configure IP filter settings to block clients from accessing specific Internet services. |
| | Port Forward | Use this screen to forward incoming service requests to specific servers on your local network. |
| | Port Trigger | Use this screen to change your NR2111's trigger port settings. |
| | Port Filter | Use this screen to enable and create firewall rules to block unwanted traffic. |
| | Remote | Use this screen to allow or forbid WAN users from pinging or configuring the NR2111. |
| | DMZ Settings | Use this screen to enable DMZ (Demilitarized Zone) on the NR2111. The client devices in the DMZ can run any Internet applications without restrictions. |
| | Messages | Use this screen to view and manage SMS messages on the NR2111. |
| | PIN Settings | Use this screen to enable PIN code authentication on the NR2111. |
| | Admin Settings | Use this screen to configure the NR2111's password and timeout settings. |
| | Update | Use these screens to display the current firmware version and update new firmware to the NR2111. |
| | Online Update | Use this screen to display the current firmware version and check for firmware updates. |
| | Firmware Management | Use this screen to upload new firmware to the NR2111. |
| | Configuration Backup | Use this screen to backup and restore the configuration or reset the factory defaults to your NR2111. |
| | Device Reboot | This screen allows you to reboot the NR2111 without turning the power off. You can also set a schedule to reboot the NR21111 |
| | Diagnosis | Use this screen to check the Wi-Fi and status of the NR2111. |
| | WPS | Use this screen to configure and activate WPS. |
| | Wi-Fi Signal Strength | Use this screen to adjust Wi-Fi signal strength. |
| | DDNS | Use this screen to set up dynamic DNS. |
| | Ping | Use this screen to test connectivity from the NR2111 to the destination host. |
| | NTP Settings | Use this screen to configure the time server. |
| | VPN Passthrough | Use this screen to enable or disable L2TP, IPSec, and PPTP on the NR2111. |
| | Power Save | Use this screen to configure the NR2111's sleep mode. |

Table 8 Menus Summary (continued)

| LINK | TAB | DESCRIPTION |
|---|---|---|
| | USB Network | Use this screen to allow client devices connect to the NR2111 through the USB cable. |
| | LCD | Use this screen to show or hide the Wi-Fi information on the LCD. |

# CHAPTER 3
# Tutorials

## 3.1 Overview

This chapter shows you how to use the NR2111's various features.

- SIM Card Setup- Unlock the SIM card, disable the PIN code protection.
- Wi-Fi Network Setup - Change the Wi-Fi security mode, connect to the Wi-Fi using the WPS.
- Network Security - Configure a MAC Filter rule, configure an IP Filter.
- NR2111 Maintenance - Upgrade the firmware, back up and restore the device configuration.

## 3.2 SIM Card Setup

This section shows you how to:

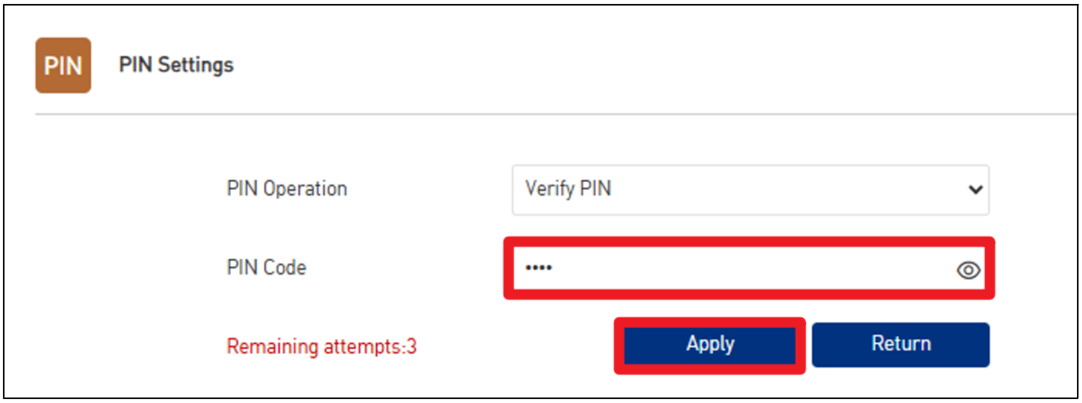
- Unlock the SIM Card
- Disable the PIN code protection

### 3.2.1 Unlock the SIM Card

This section shows you how to unlock the SIM card if the SIM card you insert into the NR2111 has PIN code protection. If **PIN Locked** display on the NR2111's LCD main screen, follow the steps below to unlock your SIN card.

1 Go to **APP MODULE** > **PIN Settings**.

2 Enter the 4-digit PIN code (0000 for example) provided by your ISP in the **PIN Code** field. Click **Apply**.



PIN Settings

PIN Operation: Verify PIN

PIN Code: ••••

Remaining attempts:3

Note: If you enter the PIN code incorrectly too many times, the SIM card will be blocked. You will have to contact your ISP to unblock your SIM card.

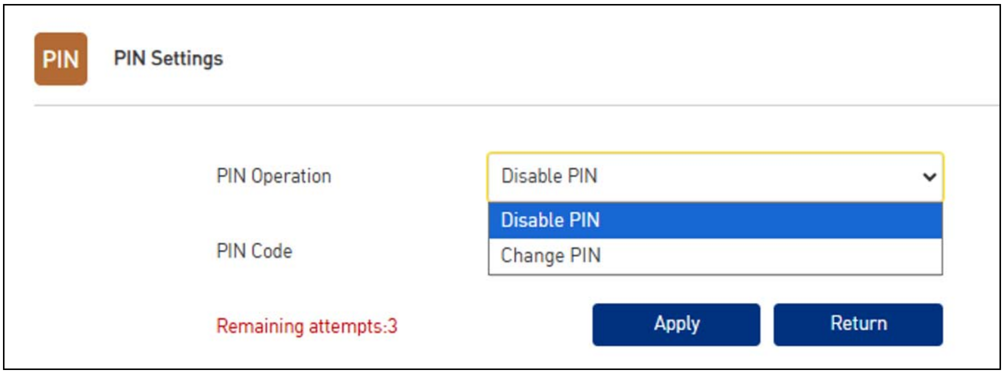
Note: To avoid unlocking the SIM card after each restart, refer to Section 3.2.2 on page 29 to disable the PIN code protection of your SIM card.

### 3.2.2 Disable the PIN code protection

You can avoid manually enter the PIN code every time you restart the NR2111 or reinsert the SIM card by disabling your SIM card's PIN protection.

1 After you unlock the SIM card (see Section 3.2.1 on page 28), go to **APP MODULE** > **PIN Settings**.

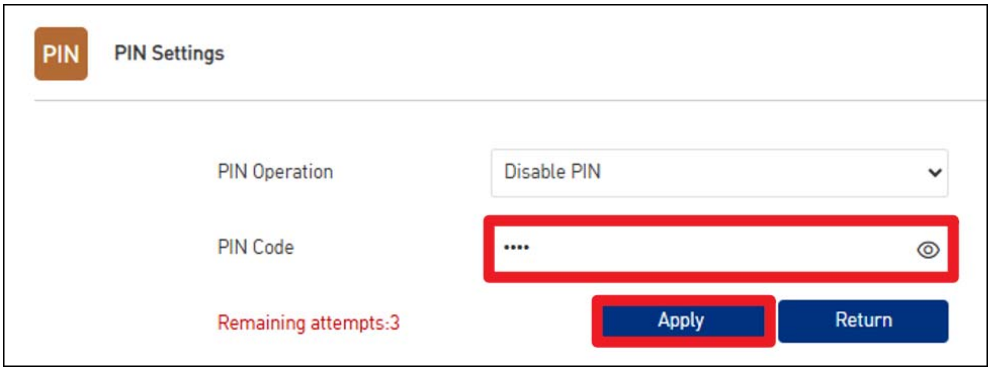
2 Select **Disable PIN** from the drop-down list of **PIN Operation.**



PIN Settings

PIN Operation: Disable PIN

3 Enter the current 4-digit PIN code of the SIM card. Click **Apply**.



PIN Settings

PIN Operation: Disable PIN

PIN Code: ••••

## 3.3 Wi-Fi Network Setup

This section shows you how to:

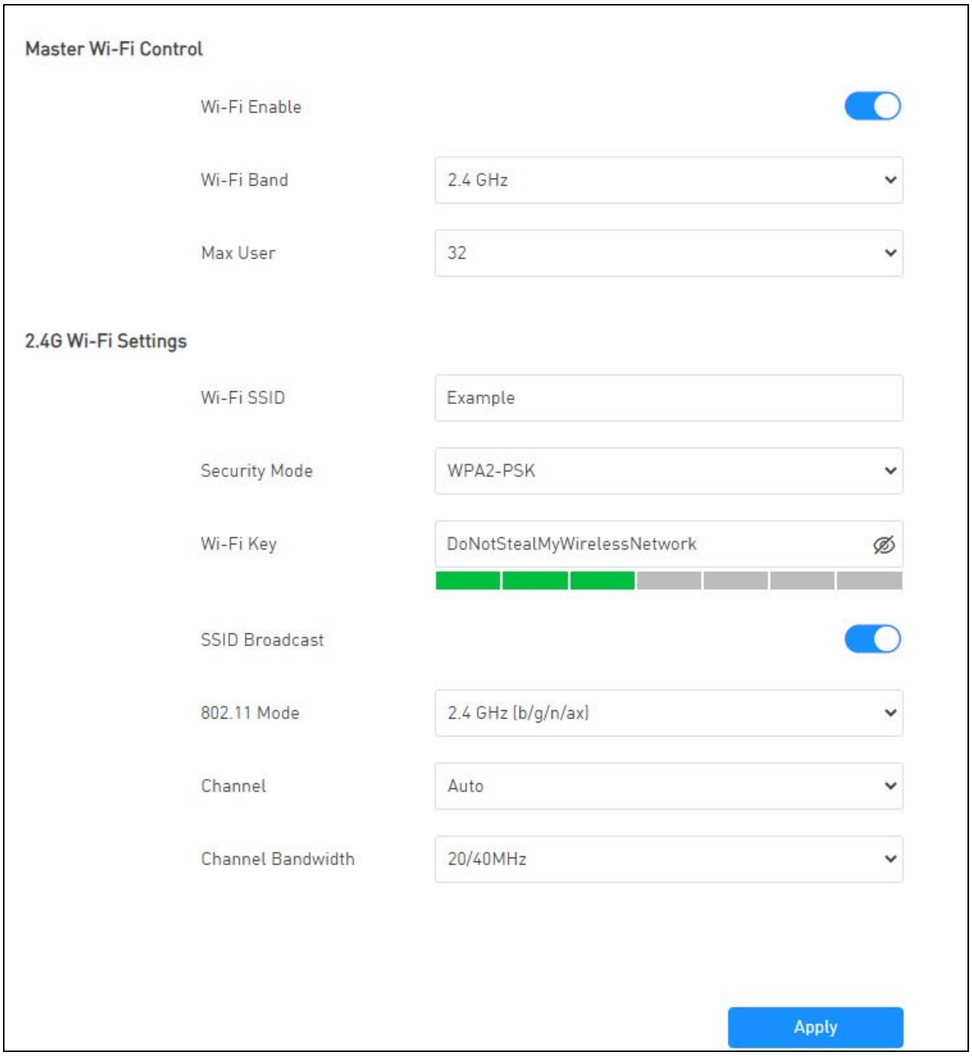
- Change Security on a Wi-Fi Network
- Connect to the NR2111's Wi-Fi Network Using WPS

### 3.3.1 Change Security on a Wi-Fi Network

This example changes the settings of a Wi-Fi network to the following:

| | |
|---|---|
| **SSID** | Example |
| **Wi-Fi Band** | 2.4 GHz |
| **Security Mode** | WPA2-PSK |
| **Pre-Shared Key** | DoNotStealMyWirelessNetwork |
| **802.11 Mode** | 2.4 GHz (b/g/n/ax) |

Go to the **WI-FI SETTINGS** > **Wi-Fi Settings** screen. Select **2.4 GHz** as the Wi-Fi band. Select **WPA2-PSK** as the security mode. Configure the screen using the provided parameters. Click **Apply**.



Master Wi-Fi Control

Wi-Fi Enable: on

Wi-Fi Band: 2.4 GHz

Max User: 32

2.4G Wi-Fi Settings

Wi-Fi SSID: Example

Security Mode: WPA2-PSK

Wi-Fi Key: DoNotStealMyWirelessNetwork

SSID Broadcast: on

802.11 Mode: 2.4 GHz (b/g/n/ax)

Channel: Auto

Channel Bandwidth: 20/40MHz

You can now establish a Wi-Fi connection between your notebook or other devices and the NR2111 (see Section 1.6.3 on page 16).

## 3.3.2 Connect to the NR2111's Wi-Fi Network Using WPS

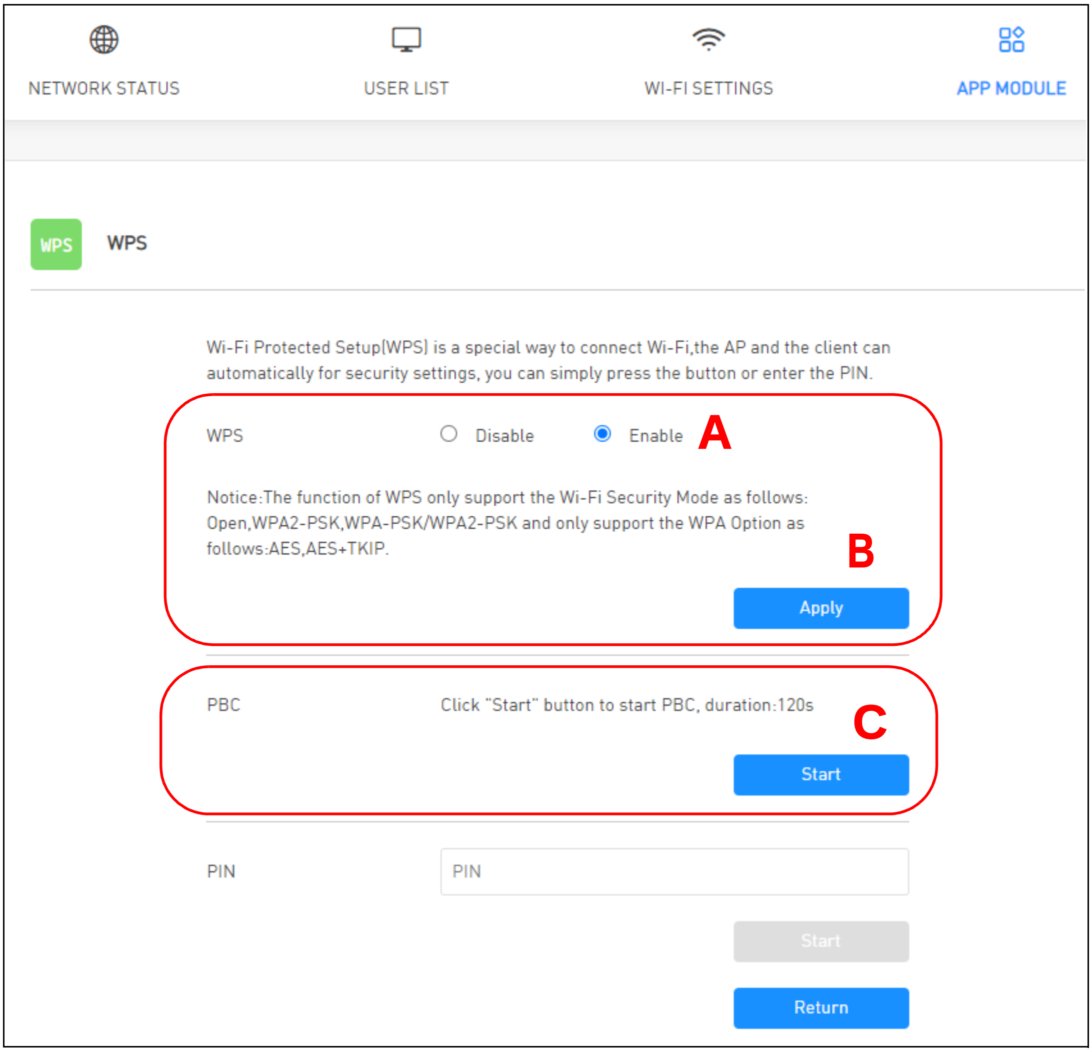
This section shows you how to connect a Wi-Fi device to the NR2111's Wi-Fi network using WPS. WPS (Wi-Fi Protected Setup) is a security standard that allows devices to connect to a router securely without you having to enter a password. There are two methods:

- **PBC (Push Button Configuration)** – Connect to the Wi-Fi network by pressing a button. See Section 3.3.2.1 on page 31. This is the simplest method.
- **PIN** – Connect to the Wi-Fi network by entering a PIN (Personal Identification Number) from a Wi-Fi-enabled device in the NR2111's Web Configurator. See Section 3.3.2.2 on page 34. This is the more secure method, because one device can authenticate the other.

### 3.3.2.1 WPS Push Button Configuration (PBC)

This example shows how to connect to the NR2111's Wi-Fi network from a notebook computer running Windows 10.

1. Make sure that your NR2111 is turned on, and your notebook is within range of the NR2111's Wi-Fi signal.
2. Log into the NR2111's Web Configurator, and then go to the **APP MODULE** > **WPS** screen. Enable **WPS** (**A**) and click **Apply** (**B**). Then click **Start** in the **PBC** section (**C**).



WPS

Wi-Fi Protected Setup(WPS) is a special way to connect Wi-Fi,the AP and the client can automatically for security settings, you can simply press the button or enter the PIN.

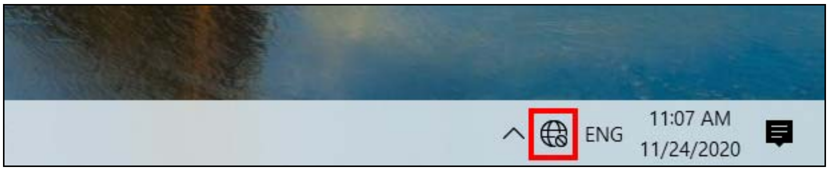
WPS ○ Disable ● Enable

Notice:The function of WPS only support the Wi-Fi Security Mode as follows: Open,WPA2-PSK,WPA-PSK/WPA2-PSK and only support the WPA Option as follows:AES,AES+TKIP.

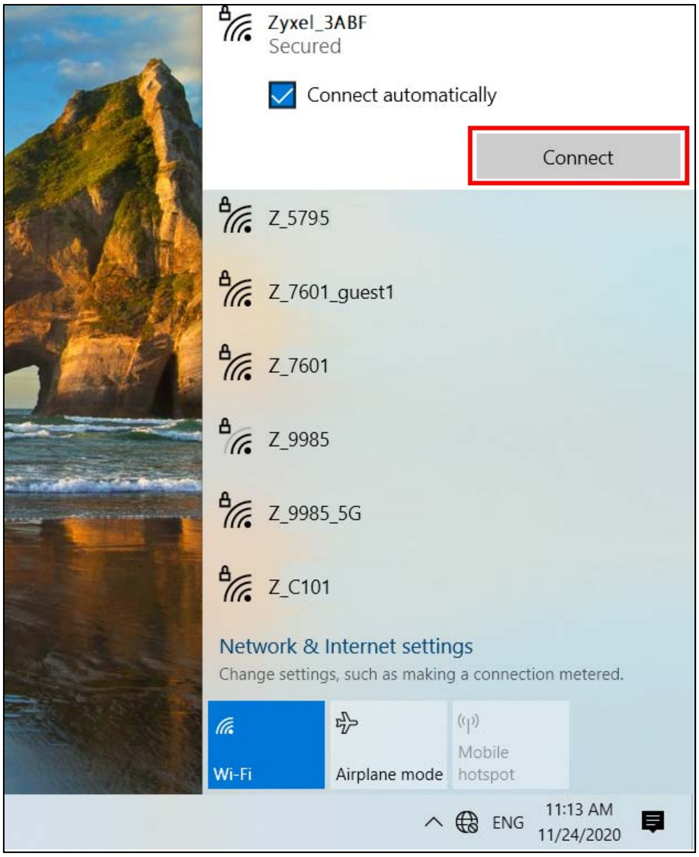
PBC Click "Start" button to start PBC, duration:120s

PIN PIN

**3** In Windows 10, click on the Network icon in the system tray to open the list of available Wi-Fi networks.



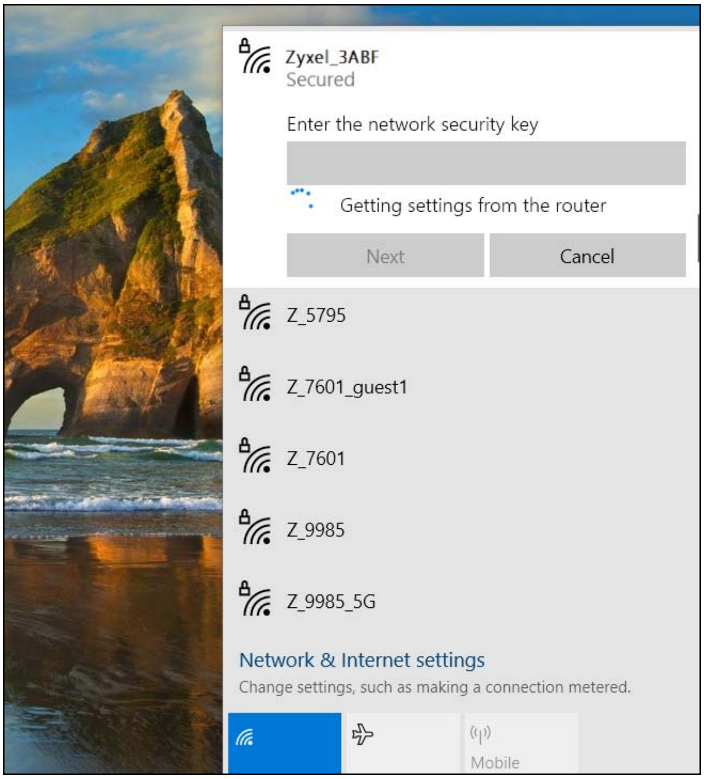
**4** Locate the Wi-Fi network of the NR2111. Then click **Connect**.



☑ Connect automatically

Change settings, such as making a connection metered.

The NR2111 sends the Wi-Fi network settings to Windows using WPS. Windows displays “Getting settings from the router”.



Zyxel_3ABF
Secured

Enter the network security key

Getting settings from the router

Next
Cancel
Z_5795
Z_7601_guest1
Z_7601
Z_9985
Z_9985_5G
Network & Internet settings
Change settings, such as making a connection metered.
Mobile

The Wi-Fi device is then able to connect to the Wi-Fi network securely.

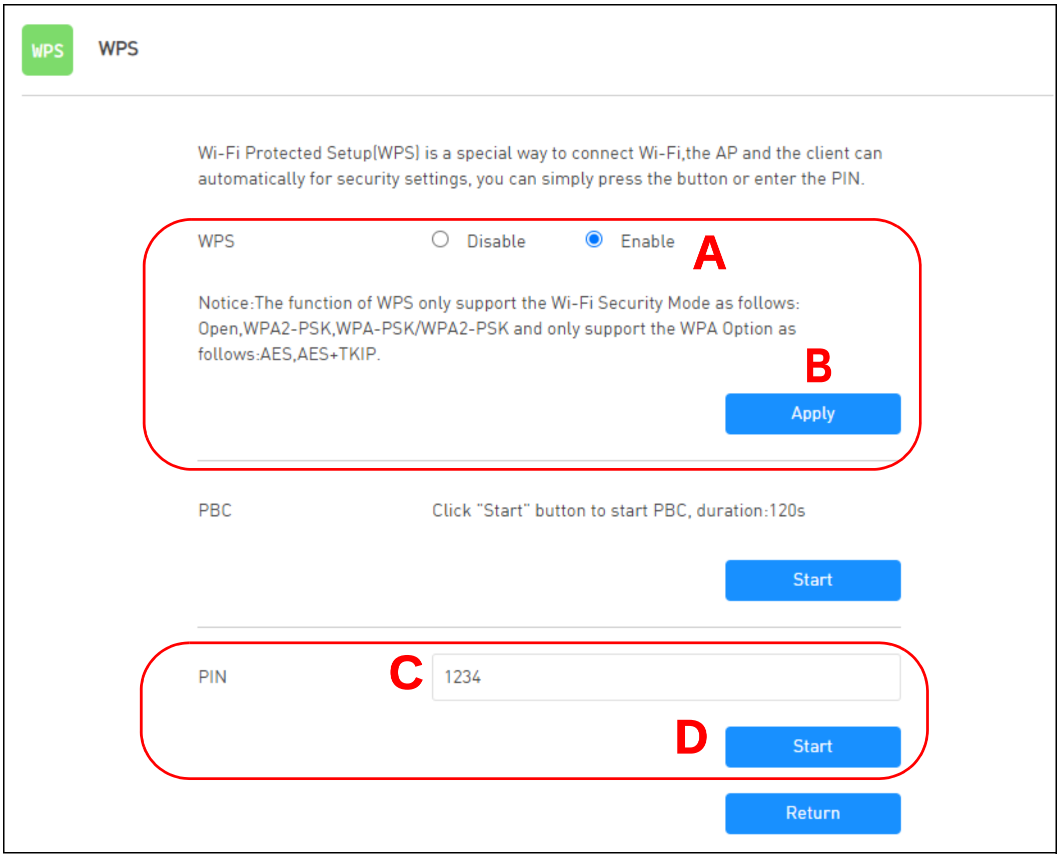
### 3.3.2.2 WPS PIN Configuration

The WPS PIN (Personal Identification Number) method is a more secure version of WPS, used by Wi-Fi-enabled devices such as printers. To use this connection method, you need to log into the NR2111's Web Configurator.

1 Enable Wi-Fi on the device you want to connect to the Wi-Fi network. Then, note down the WPS PIN in the device's Wi-Fi settings.

2 Log into NR2111's Web Configurator, and then go to the **APP MODULE** > **WPS** screen. Enable **WPS** (**A**), and then click **Apply** (**B**).

3 Enter the PIN of the Wi-Fi device in the **PIN** field (**C**) and then click **Start** (**D**).



WPS

Wi-Fi Protected Setup(WPS) is a special way to connect Wi-Fi,the AP and the client can automatically for security settings, you can simply press the button or enter the PIN.

WPS ○ Disable ● Enable

Notice:The function of WPS only support the Wi-Fi Security Mode as follows: Open,WPA2-PSK,WPA-PSK/WPA2-PSK and only support the WPA Option as follows:AES,AES+TKIP.

PBC Click "Start" button to start PBC, duration:120s

PIN 1234

4 Within 2 minutes, enable WPS on the Wi-Fi device.

The NR2111 authenticates the Wi-Fi device using the PIN, and then sends the Wi-Fi network settings to the device using WPS. This process may take up to 2 minutes. The Wi-Fi device is then able to connect to the Wi-Fi network securely.

## 3.4 Network Security

This section shows you how to:

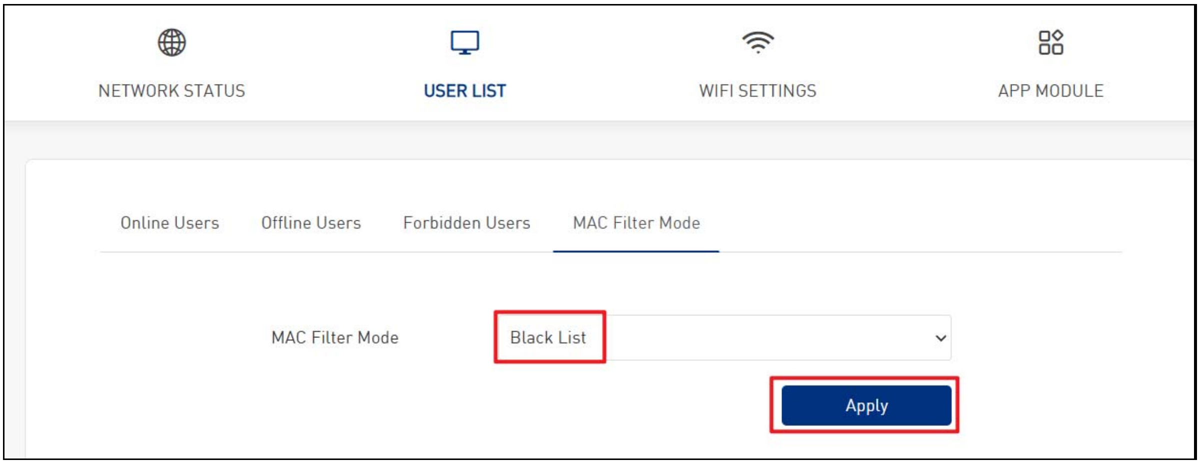
- Configure a MAC Filter Blacklist
- Configure an IP Filter Rule

### 3.4.1 Configure a MAC Filter Blacklist

A MAC (Media Access Control) address is a unique identifier assigned to each device. You can configure a MAC address blacklist on NR2111 to block access from specified devices. Configure a whitelist instead if you want to only allow access to specified devices. When using a whitelist, make sure that your own device's MAC address is included.

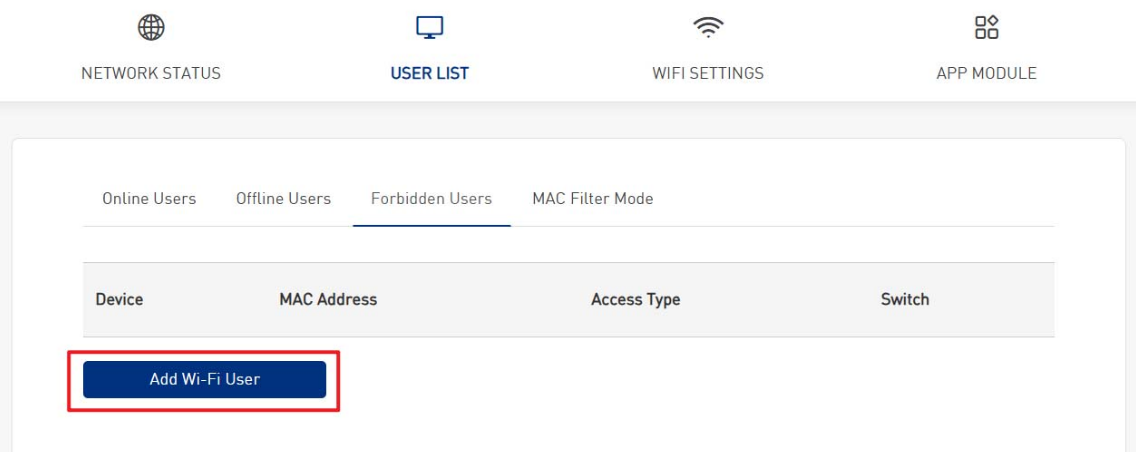
1 Log into NR2111's configurator, and go to **USER LIST > MAC Filter Mode**.

2 Select **Black List** from the drop-down menu, and click **Apply**.



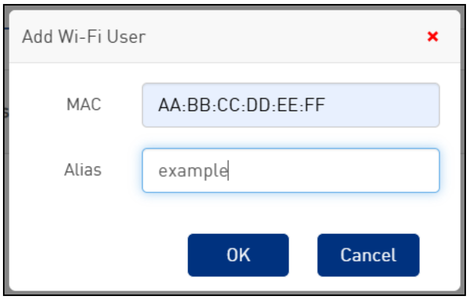
MAC Filter Mode: Black List

3 Go to the **Forbidden Users** tab, and click the **Add Wi-Fi User** button.



| Device | MAC Address | Access Type | Switch |
|---|---|---|---|

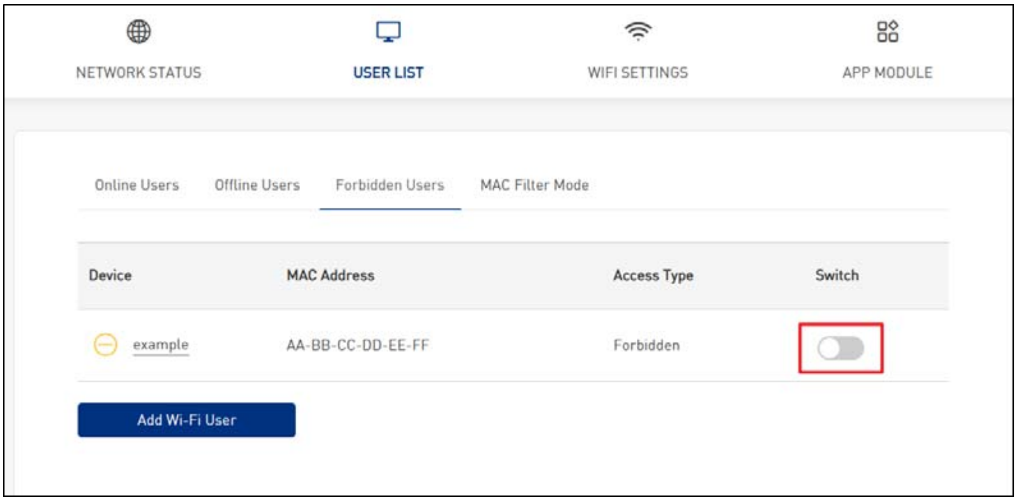
4 Enter the **MAC** address and the **Alias** of the device you want to block, and click **OK**. The Alias is a user-defined name that helps identify the device more easily.



MAC: AA:BB:CC:DD:EE:FF

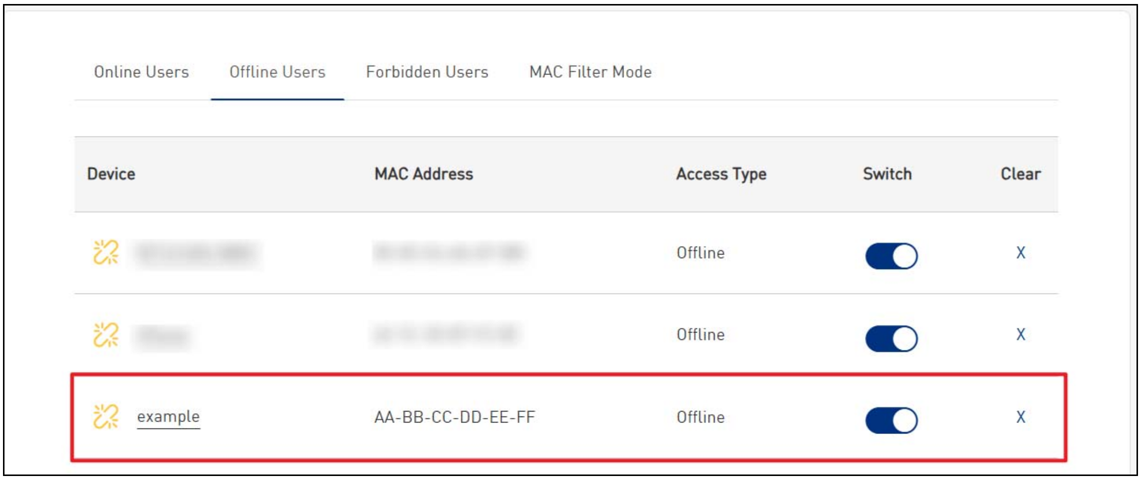
Alias: example

5 The device is now added to the blacklist. If you want to block it from accessing the NR2111, click the switch button to the right.



| Device | MAC Address | Access Type | Switch |
|---|---|---|---|
| example | AA-BB-CC-DD-EE-FF | Forbidden | ○ |

6 You can find the device under the **Offline Users** tab.



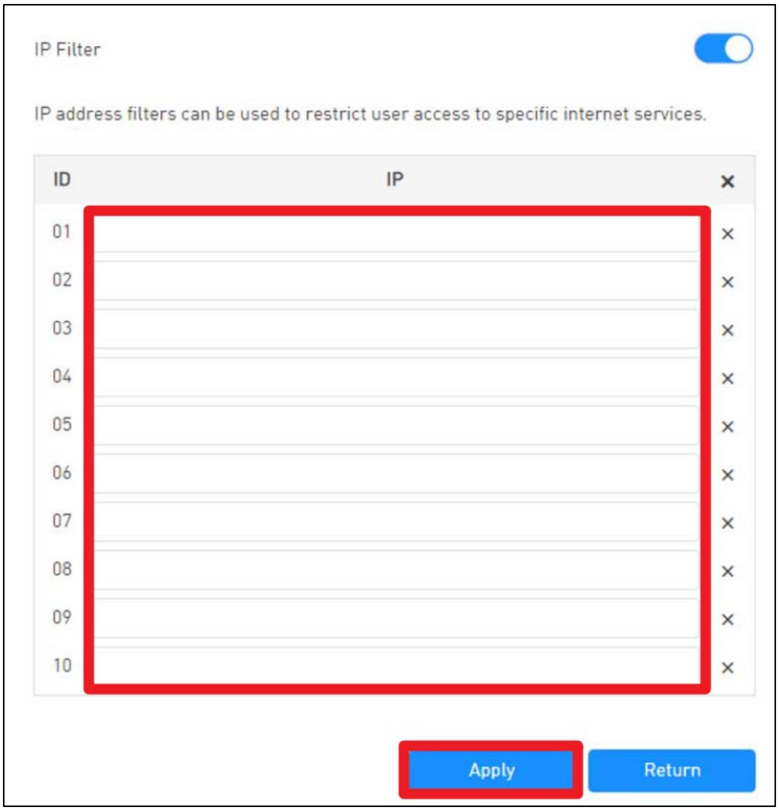
| Device | MAC Address | Access Type | Switch | Clear |
|---|---|---|---|---|
| [redacted] | [redacted] | Offline | ● | X |
| [redacted] | [redacted] | Offline | ● | X |
| example | AA-BB-CC-DD-EE-FF | Offline | ● | X |

## 3.4.2 Configure an IP Filter Rule

You can configure a list on the NR2111 to block clients from accessing specified Internet services. For example, you can block a gaming server from your kids.

1 Go to **APP MODULE** > **Firewall** > **IP Filter**.

2 Enter the IP addresses you want to block in the IP fields. After entering them, click **Apply** to save the entries.



IP Filter

IP address filters can be used to restrict user access to specific internet services.

| ID | IP | × |
|---|---|---|
| 01 | | × |
| 02 | | × |
| 03 | | × |
| 04 | | × |
| 05 | | × |
| 06 | | × |
| 07 | | × |
| 08 | | × |
| 09 | | × |
| 10 | | × |

3 The clients are now unable to access the Internet services with the IP address you specified here.

# 3.5 NR2111 Maintenance

This section shows you how to upgrade the NR2111 firmware, backup the NR2111's configuration, restore the NR2111 to its previous settings, and reset the NR2111 to its default factory settings.

- Upgrade the NR2111
- Back up the NR2111's Configuration
- Restore the NR2111's Configuration
- Reset the NR2111's Configuration to Default

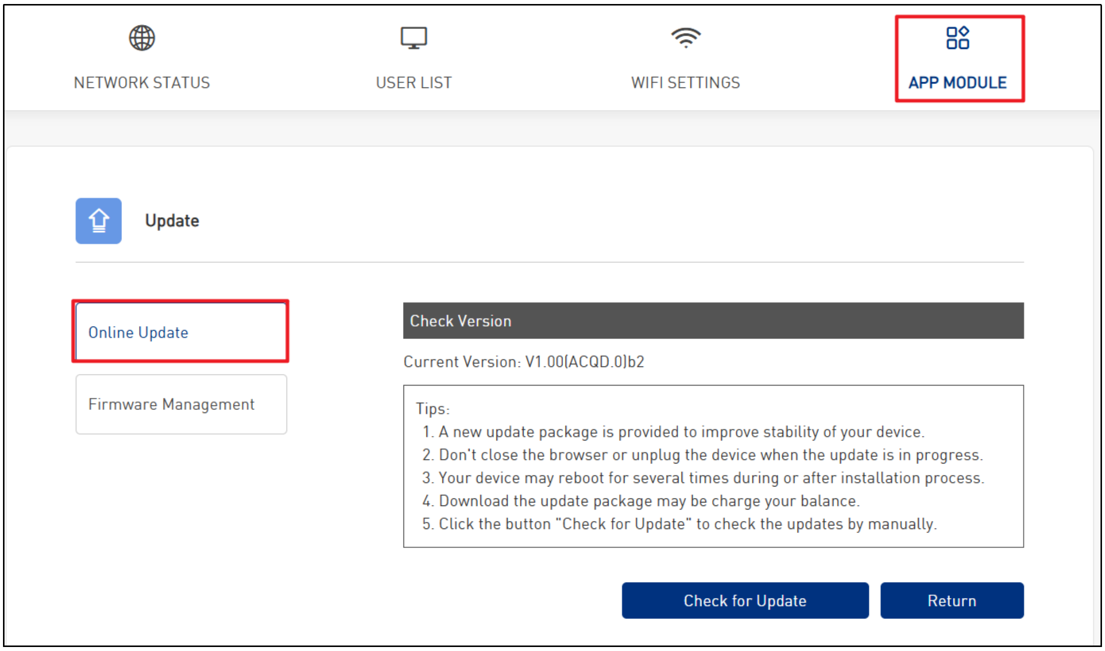
## 3.5.1 Upgrade the NR2111

This section shows you how to update your NR2111 both online and locally.

- Online Update
- Local Update

### 3.5.1.1 Online Update

1 Go to **APP MODULE > Update** screen, select **Online Update** on the left sidebar.



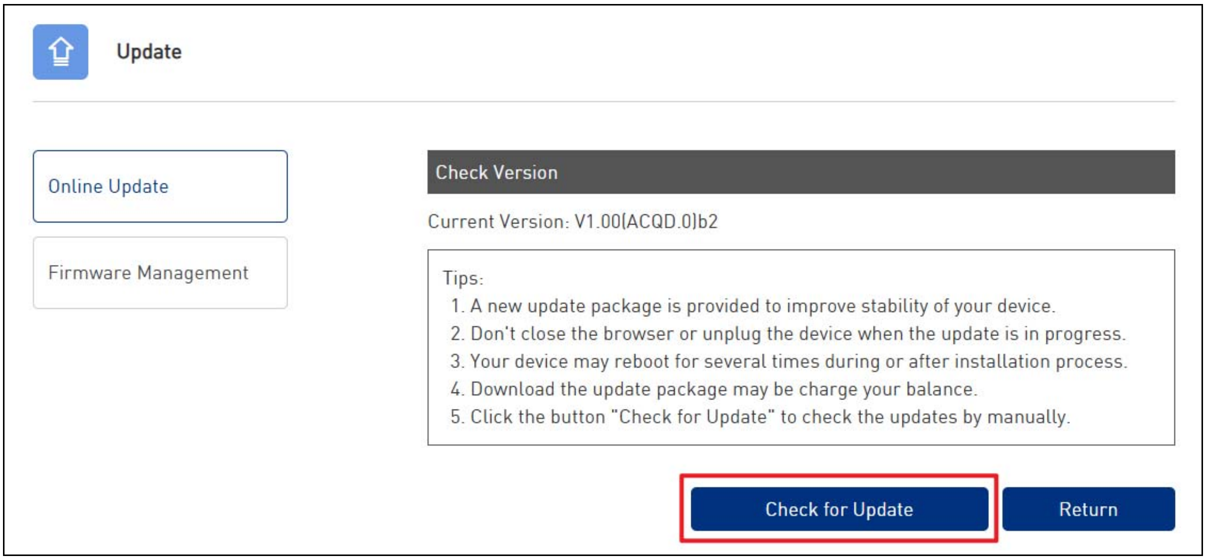
Check Version

Current Version: V1.00(ACQD.0)b2

Tips:

1. A new update package is provided to improve stability of your device.
2. Don't close the browser or unplug the device when the update is in progress.
3. Your device may reboot for several times during or after installation process.
4. Download the update package may be charge your balance.
5. Click the button "Check for Update" to check the updates by manually.

2 Click the **Check for Update** button. You can see the available updates in the pop-up window.



Check Version

Current Version: V1.00(ACQD.0)b2

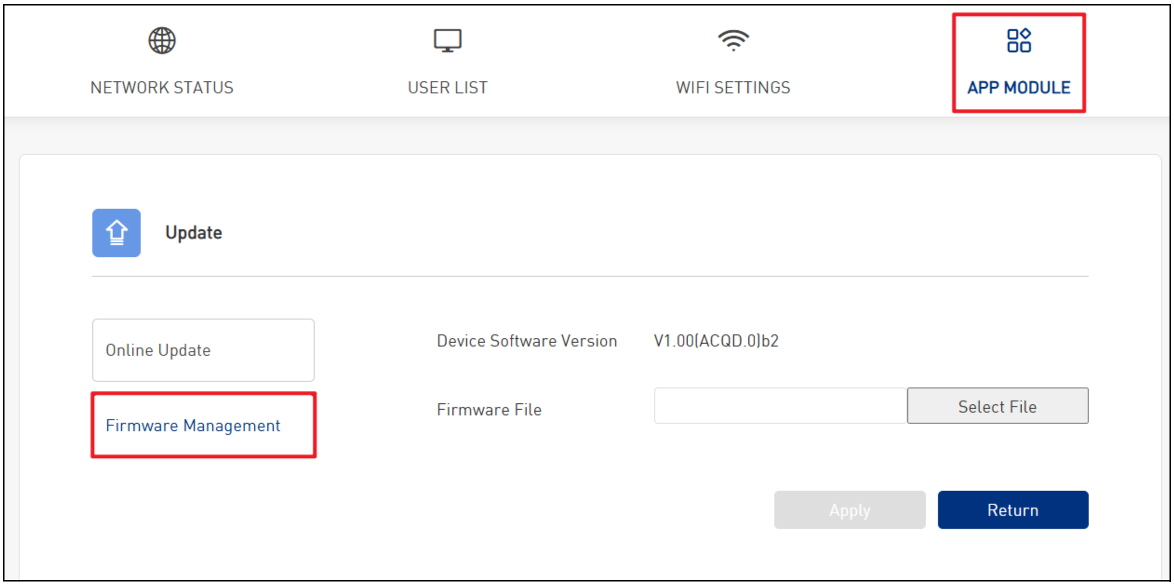
Tips:

1. A new update package is provided to improve stability of your device.
2. Don't close the browser or unplug the device when the update is in progress.
3. Your device may reboot for several times during or after installation process.
4. Download the update package may be charge your balance.
5. Click the button "Check for Update" to check the updates by manually.

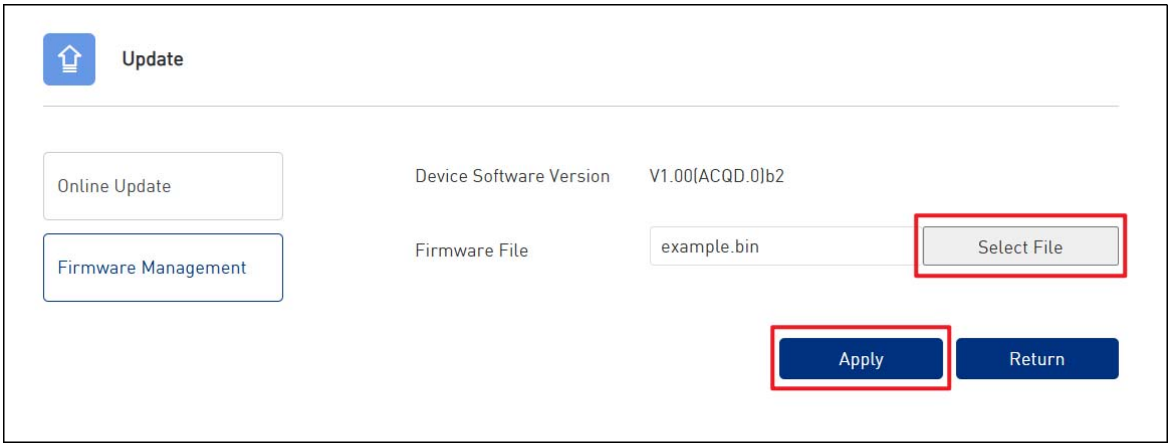
### 3.5.1.2 Local Update

If you want to upgrade the firmware manually, go to the Zyxel website (*www.zyxel.com*) to download the firmware file for your device.

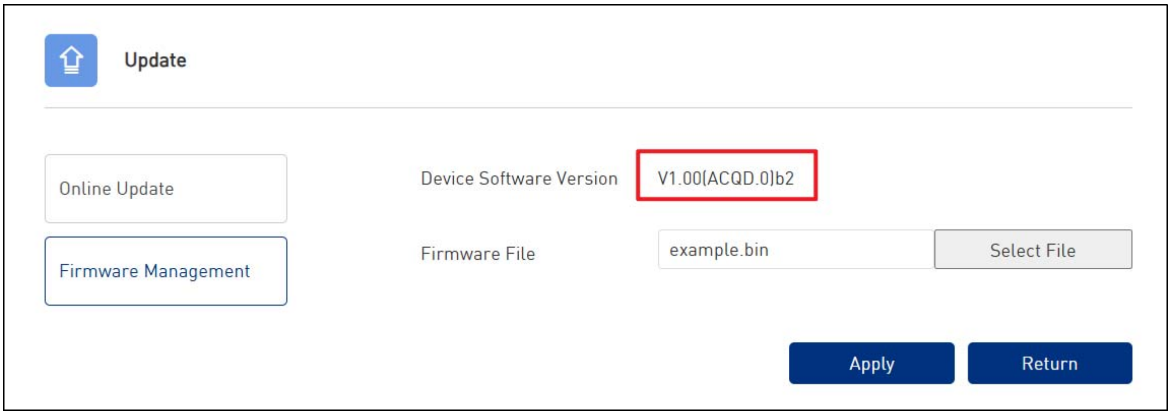
1 Go to **APP MODULE > Update**. Select **Firmware Management** on the left sidebar.



2 Click the **Select File** button to select the firmware file from your local computer, and click **Apply**.



3 This process may take a few minutes to finish. Log in again to check the updated version in the **Device Software Version** field.

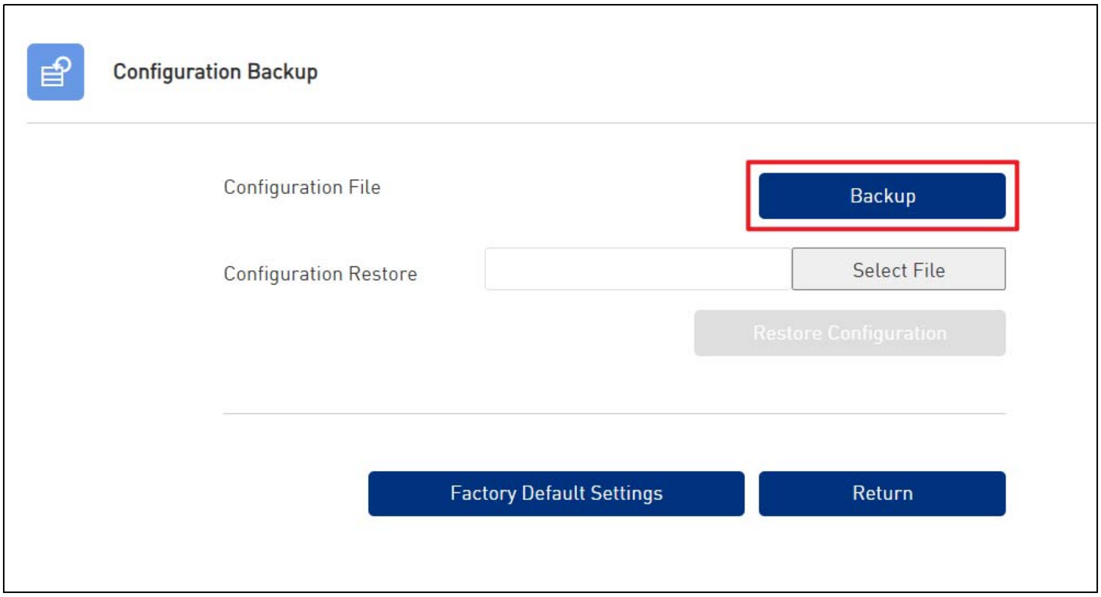


### 3.5.2 Back up the NR2111's Configuration

This section shows how to save your NR2111's configuration for future rollback.

1 Go to **APP MODULE > Configuration Backup**.

2 Click the **Backup** button to save the NR2111's configuration into a .bin file.



Configuration Backup

Configuration File

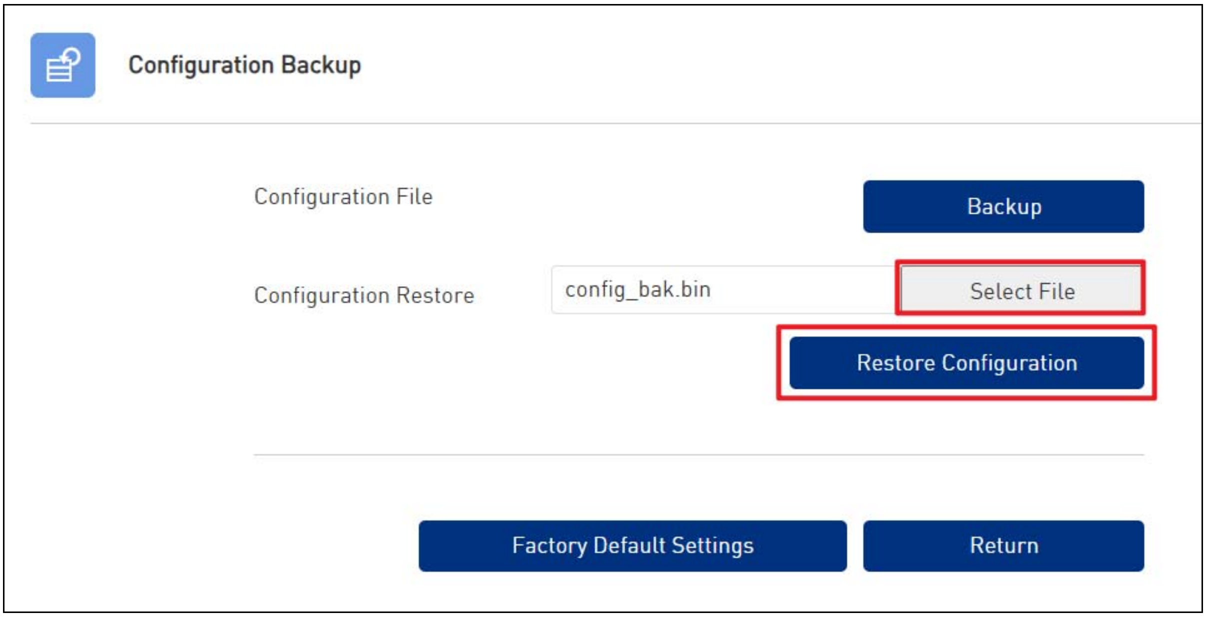
Configuration Restore

### 3.5.3 Restore the NR2111's Configuration

This section shows you how to restore the NR2111's configuration.

1 Go to **APP MODULE > Configuration Backup**.

2 Click **Select File** to select the .bin file that you want, and click the **Restore Configuration** button.

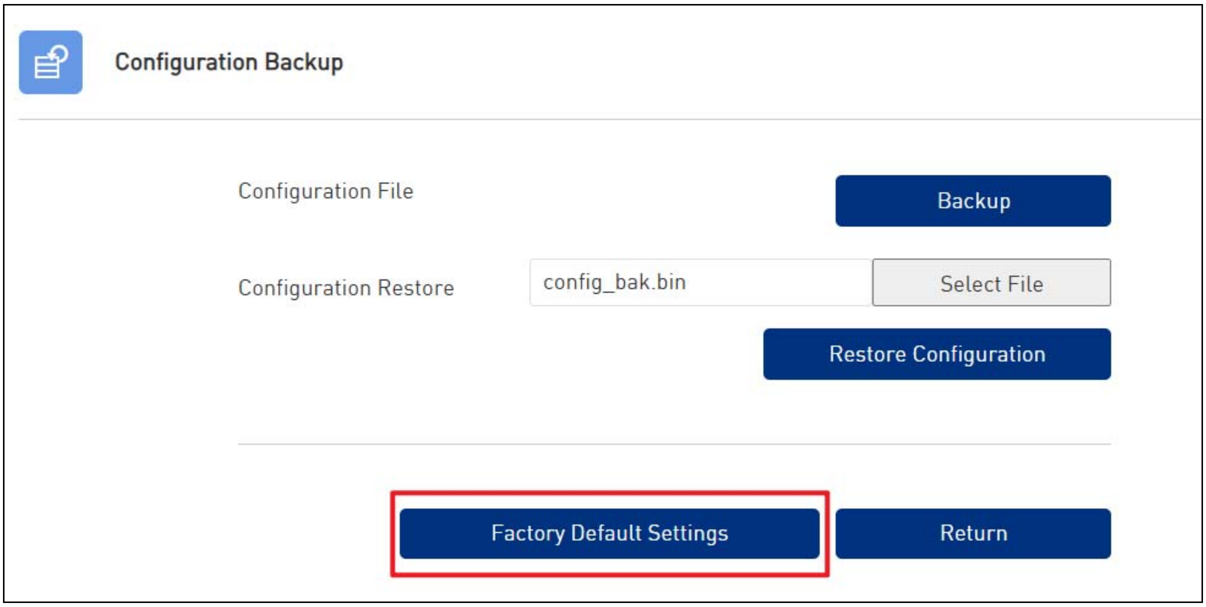


## 3.5.4 Reset the NR2111's Configuration to Default

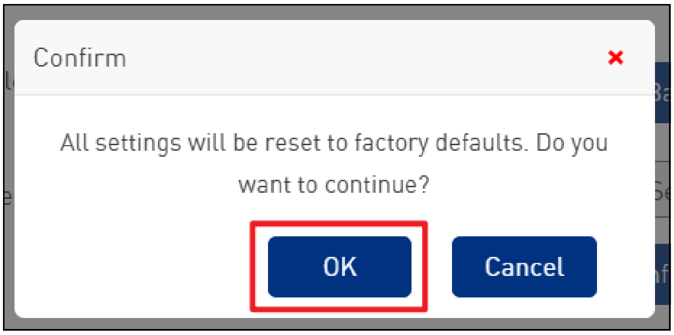
You can also reset your NR2111's configuration to the default settings. Before doing so, make sure to back up your current configuration to prevent data loss.

1 Go to **APP MODULE > Configuration Backup**.

2 Click the **Factory Default Settings** button.



3 Click **OK** in the pop-up window to confirm.



Confirm

All settings will be reset to factory defaults. Do you want to continue?

# PART II

# Technical Reference

# CHAPTER 4 Network Status

## 4.1 Overview

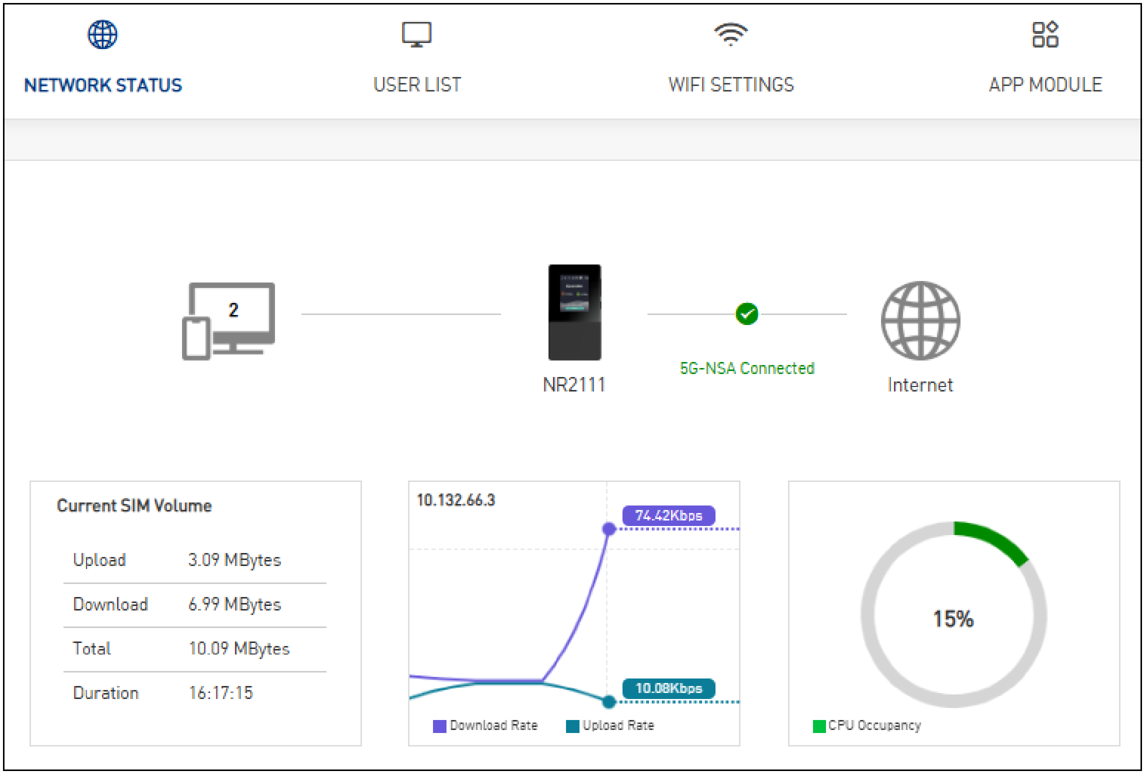
Use the **NETWORK STATUS** screen to check status information about the NR2111.

## 4.2 NETWORK STATUS

This screen is the first thing you see when you log into the NR2111. You can also click **NETWORK STATUS** from the **Menu** list to access this screen.

The **NETWORK STATUS** screen displays the NR2111's WAN network type, connection status, connection mode, SIM card information, traffic statistics, and WAN IP address.

**Figure 12** NETWORK STATUS



Current SIM Volume

| | |
|---|---|
| Upload | 3.09 MBytes |
| Download | 6.99 MBytes |
| Total | 10.09 MBytes |
| Duration | 16:17:15 |

The following table describes the labels in this screen.

Table 9 NETWORK STATUS

| LABEL | DESCRIPTION |
|---|---|
| Online User | This field displays the number of clients that are currently connected to the NR2111. Click this to go to the **USER LIST** > **Online Users** screen to view information of the clients and configure them.<br>See Section 5.2 on page 47 for more information. |
| Current SIM Volume | This sections shows the current SIM card usage statistics. Click this to go the **APP MODULE** > **Statistics** screen. |
| Upload | This field displays the number of transmitted packets on the SIM card for the current connection session. |
| Download | This field displays the number of received packets on the SIM card for the current connection session. |
| Total | This field displays the total number of transmitted and received packets on the SIM card for the current connection session. |
| Duration | This field displays the duration of the current connection session |
| Download Rate | This field displays the NR2111's traffic download rate. |
| Upload Rate | This field displays the NR2111's traffic upload rate. |
| CPU Occupancy | This field displays what percentage of the NR2111's processing ability is currently used. When this percentage is close to 100%, the NR2111 is running at full load, and the throughput is not going to improve anymore. |

# CHAPTER 5
# User List

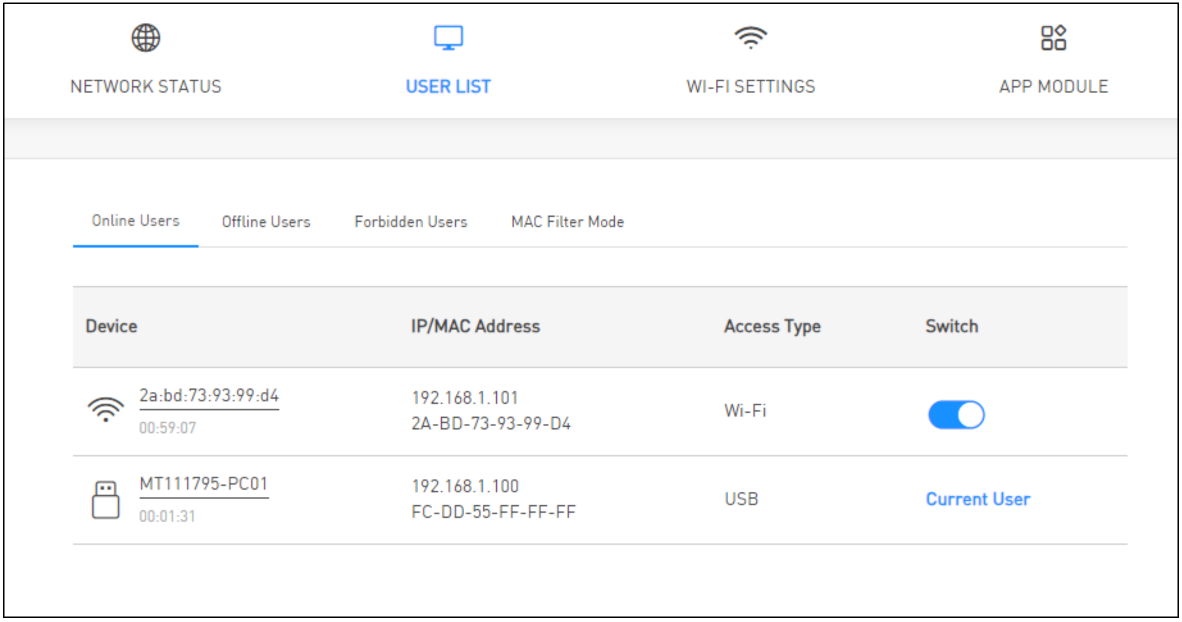
## 5.1 Overview

Use the **USER LIST** screens screen to view and manage the NR2111's clients. You can also allow or deny clients' access to the NR2111.

## 5.2 Online Users

Click **USER LIST** from the **Menu** list to display the **Online Users** screen. Use this screen to view and configure the clients currently connected to the NR2111.

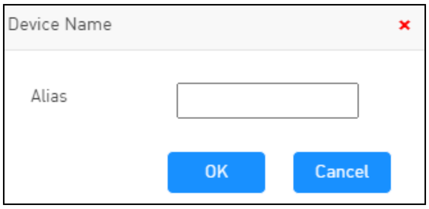
**Figure 13** USER LIST > Online Users



| Device | IP/MAC Address | Access Type | Switch |
|---|---|---|---|
| 2a:bd:73:93:99:d4<br>00:59:07 | 192.168.1.101<br>2A-BD-73-93-99-D4 | Wi-Fi | ● |
| MT111795-PC01<br>00:01:31 | 192.168.1.100<br>FC-DD-55-FF-FF-FF | USB | Current User |

The following table describes the labels in this screen.

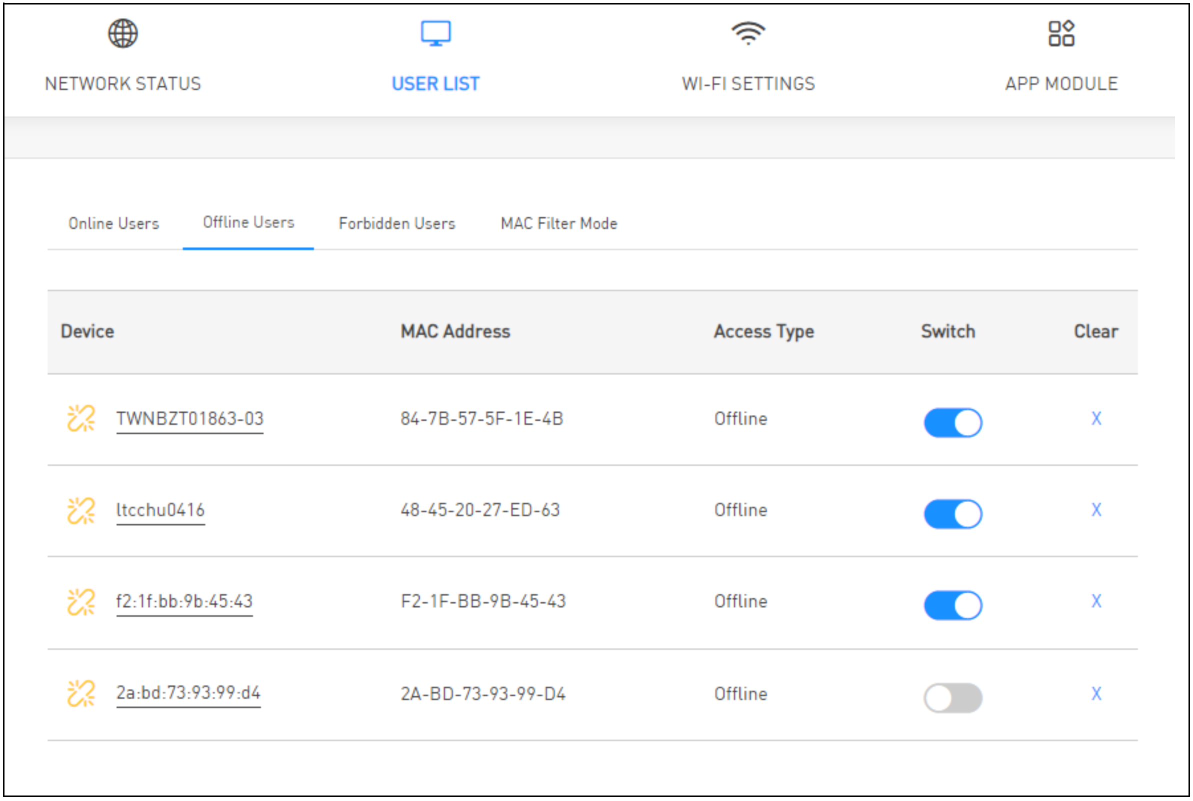
Table 10 USER LIST > Online Users

| LABEL | DESCRIPTION |
|---|---|
| Device | This field displays the name of the client that is currently connected to the NR2111. Its connected time duration is also displayed.<br>If you want to change the name of the device, click on its name and enter the new name in the **Alias** field of the following screen. Click **OK** to save the change.<br> |
| IP/MAC Address | This field displays the LAN IP address and MAC address of a client currently connected to the NR2111. |
| Access Type | This field displays whether the client is connected to the NR2111 by **Wi-Fi** or **USB**. |
| Switch | When the switch button is on , the client is connected to the NR2111.<br>Turn the switch button off to disable the connection of the client to the NR2111. This client will be added to the **Offline Users** list. If the MAC filer mode is set as **Black List**, this client will be automatically added to the **Forbidden Users** list. You can allow the connection again in the **Offline Users** screen or the **Forbidden Users** screen. If the MAC filer mode is set as **White List**, this client will be automatically added to the **Allow Users** list. The client may connect to the NR2111 again without entering the SSID and password.<br>Note: You cannot disable the connection of the device that you are currently using to access the NR2111. **Current User** is displayed for this device. |

## 5.3 Offline Users

Click **USER LIST** from the **Menu** and select **Offline Users** to display the following screen. Use this screen to view and configure the clients that were connected to the NR2111 previously.

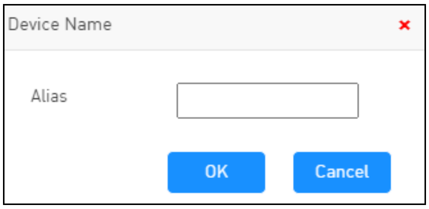
**Figure 14** USER LIST > Offline Users



| Device | MAC Address | Access Type | Switch | Clear |
|---|---|---|---|---|
| TWNBZT01863-03 | 84-7B-57-5F-1E-4B | Offline | ● | X |
| ltcchu0416 | 48-45-20-27-ED-63 | Offline | ● | X |
| f2:1f:bb:9b:45:43 | F2-1F-BB-9B-45-43 | Offline | ● | X |
| 2a:bd:73:93:99:d4 | 2A-BD-73-93-99-D4 | Offline | ○ | X |

The following table describes the labels in this screen.

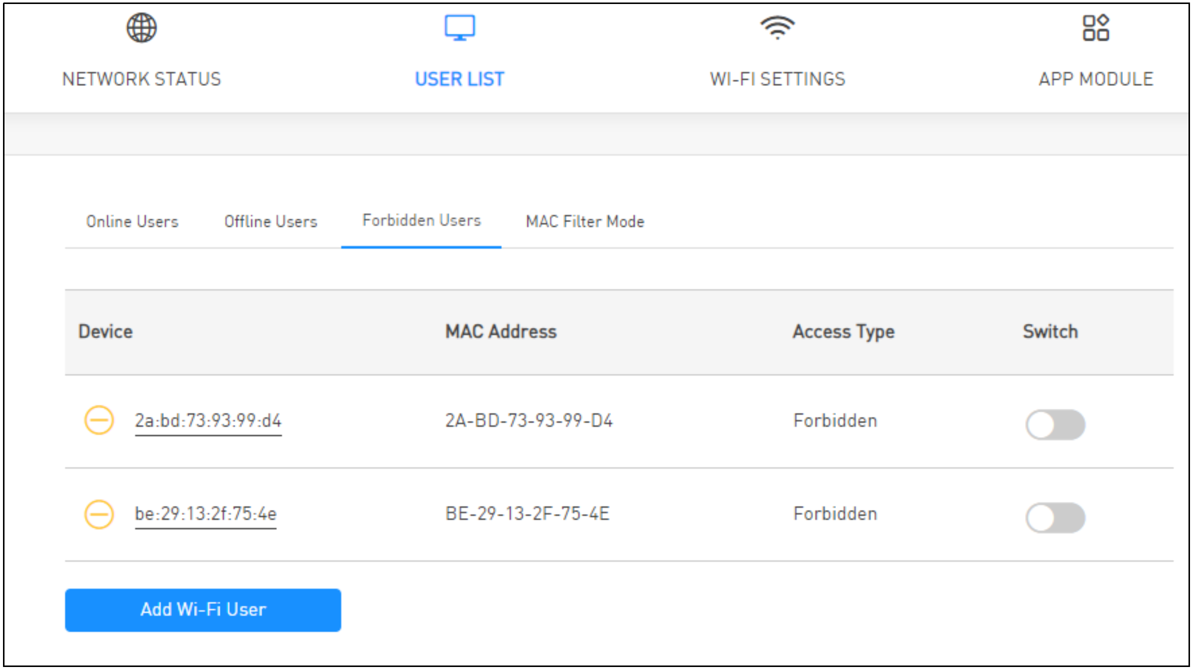
Table 11 USER LIST > Offline Users

| LABEL | DESCRIPTION |
|---|---|
| Device | This field displays the name of the client that was connected to the NR2111 previously.<br>If you want to change the name of the device, click on its name and enter the new name in the **Alias** field of the following screen. Click **OK** to save the change.<br><br>Device Name<br>Alias<br>OK<br>Cancel |
| MAC Address | This field displays the MAC address of the client that was connected to the NR2111 previously. |
| Access Type | This field displays **Offline** since the client is not connected to the NR2111 currently. |
| Switch | Turn the switch button on ● to allow the connection of the client to the NR2111. If the client connects to the NR2111, it will be added to the **Online Users** screen. If the MAC filer mode is set as **White List**, this client will be automatically added to the **Allow Users** list. The client may connect to the NR2111 again without entering the SSID and password.<br>If the switch button is off ○ , the client is not allowed to connect to the NR2111. If the MAC filer mode is set as **Black List**, this client will be automatically added to the **Forbidden Users** list. You can allow the connection again in either the **Offline Users** screen or the **Forbidden Users** screen. |
| Clear | Click the **X** next to a client to remove it from the list. |

## 5.4 Forbidden Users

If the **MAC Filter Mode** is set to **Black List** in the **MAC Filter Mode** screen, this screen is displayed by clicking **USER LIST** > **Forbidden Users**. Use this screen to view and add clients that are denied access to the NR2111.

**Figure 15** USER LIST > Forbidden Users



| Device | MAC Address | Access Type | Switch |
|---|---|---|---|
| 2a:bd:73:93:99:d4 | 2A-BD-73-93-99-D4 | Forbidden | |
| be:29:13:2f:75:4e | BE-29-13-2F-75-4E | Forbidden | |

The following table describes the labels in this screen.

Table 12 USER LIST > Forbidden Users

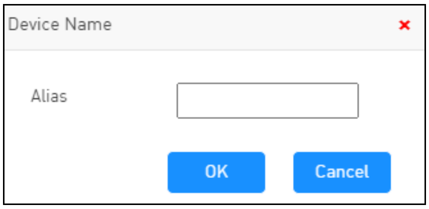
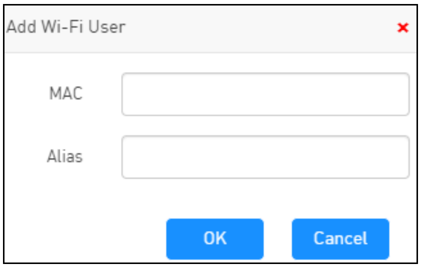
| LABEL | DESCRIPTION |
|---|---|
| Device | This field displays the name of the client that is not allowed to access the NR2111.<br>If you want to change the name of the device, click on its name and enter the new name in the **Alias** field of the following screen. Click **OK** to save the change.<br><br>Device Name<br>Alias |
| MAC Address | This field displays the MAC address of the client that is forbidden to access the NR2111. |
| Access Type | This field displays **Forbidden** since the client is forbidden access to the NR2111. |

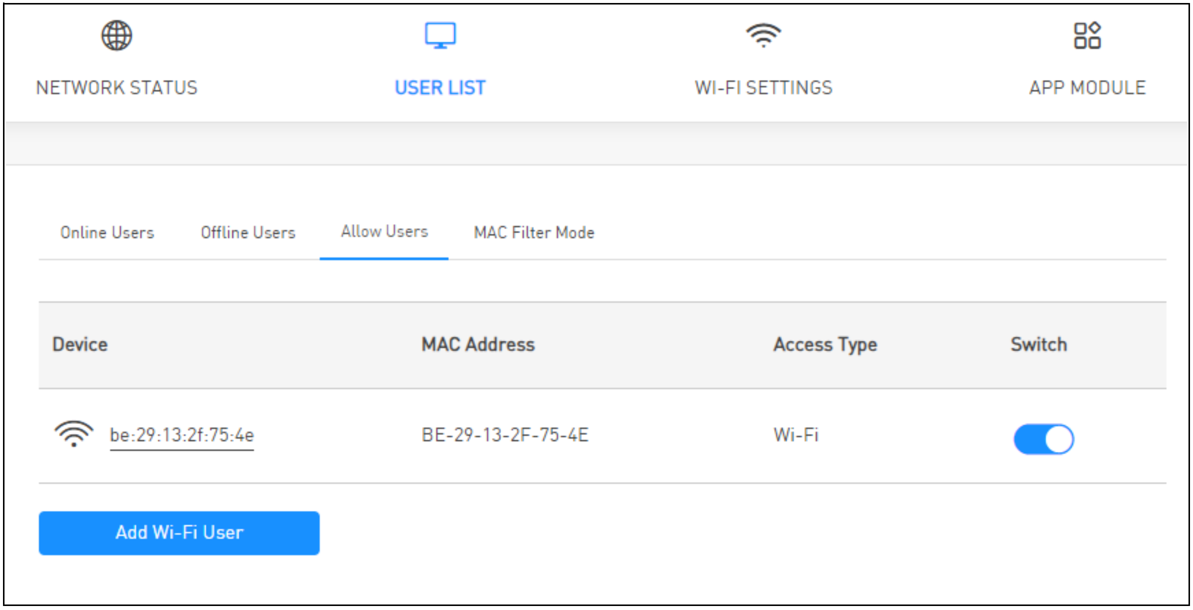
Table 12 USER LIST > Forbidden Users (continued)

| LABEL | DESCRIPTION |
|---|---|
| Switch | The switch button is off ○ so that the client is not allowed to connect to the NR2111.<br>Turn the switch button on ● to allow the connection of the client to the NR2111. If the client connects to the NR2111, it will be added to the **Online Users** screen. If the client is not connected to the NR2111, it will be added to the **Offline Users** list. |
| Add Wi-Fi User | Click this to manually add a client to the **Forbidden Users** list. The following screen is displayed. Enter the device's MAC address in the **MAC** field and name in the **Alias** field. Click **OK** to save the change.<br><br> |

## 5.5 Allow Users

If the **MAC Filter Mode** is set to **White List** in the **MAC Filter Mode** screen, this screen is displayed by clicking **USER LIST** > **Allow Users**. Use this screen to view and add clients that are allowed access to the NR2111.

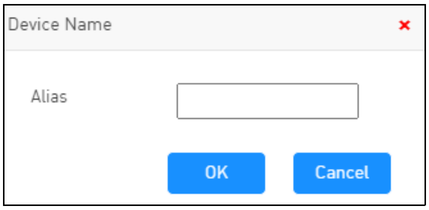
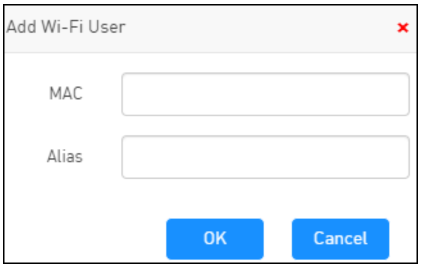
**Figure 16** USER LIST > Allow Users



| Device | MAC Address | Access Type | Switch |
|---|---|---|---|
| be:29:13:2f:75:4e | BE-29-13-2F-75-4E | Wi-Fi | ● |

The following table describes the labels in this screen.

Table 13 USER LIST > Allow Users

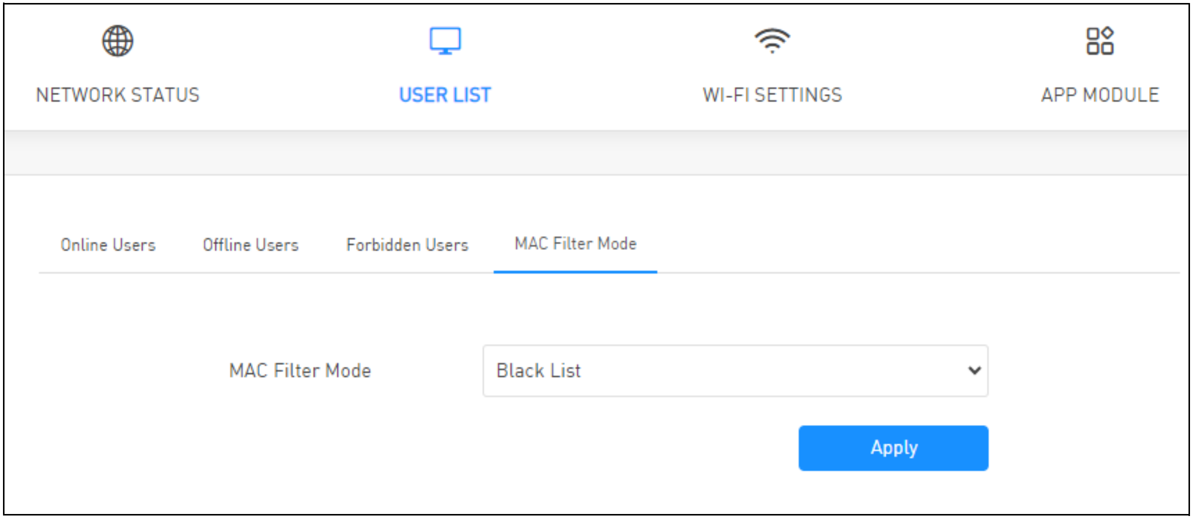
| LABEL | DESCRIPTION |
|---|---|
| Device | This field displays the name of the client that is allowed to access the NR2111.<br>If you want to change the name of the device, click on its name and enter the new name in the **Alias** field of the following screen. Click **OK** to save the change.<br><br> |
| MAC Address | This field displays the MAC address of the client that is allowed to access the NR2111. |
| Access Type | This field displays how the client connects to the NR2111 (**Wi-Fi**). |
| Switch | The switch button is on ● to allow the connection of the client to the NR2111. If the client is connecting to the NR2111, it will be added to the **Online Users** screen. If the client is not connecting to the NR2111, it will be added to the **Offline Users** list.<br>Turn the switch button off ○ to forbid the client to connect to the NR2111. |
| Add Wi-Fi User | Click this to manually add a client to the **Allow Users** list. The following screen is displayed. Enter the device's MAC address in the **MAC** field and name in the **Alias** field. Click **OK** to save the change.<br><br> |

## 5.6 MAC Filter Mode

This screen allows you to configure the NR2111 to allow or deny specific devices from accessing the NR2111. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use the **MAC Filter Mode** screen to configure your NR2111's MAC filter mode. Click **USER LIST** > **MAC Filter Mode**. The screen appears as shown.

**Figure 17** USER LIST > MAC Filter Mode



MAC Filter Mode: Black List

The following table describes the labels in this screen.

Table 14 USER LIST > MAC Filter Mode

| LABEL | DESCRIPTION |
|---|---|
| MAC Filter Mode | Define the MAC filter action for the NR2111.<br>Select **Black List** to block the devices listed in the **Forbidden Users** screen from accessing the NR2111. Devices not listed will be allowed to access the NR2111. See Section 5.4 on page 50 for more information.<br>Select **White List** to permit the devices listed in the **Allow Users** screen to access the NR2111. Devices not listed will be denied access to the NR2111. See Section 5.5 on page 51 for more information. |
| Apply | Click **Apply** to save your changes. |

# CHAPTER 6
# WI-FI SETTINGS

## 6.1 Overview

This chapter discusses how to configure the Wi-Fi network settings in your NR2111.

### 6.1.1 What You Need to Know

Every Wi-Fi network must follow these basic guidelines.

- Every Wi-Fi client in the same Wi-Fi network must use the same SSID.

  The SSID is the name of the Wi-Fi network. It stands for Service Set IDentity.
- If two Wi-Fi networks overlap, they should use different channels.

  Like radio stations or television channels, each Wi-Fi network uses a specific channel, or frequency, to send and receive information.
- Every Wi-Fi client in the same Wi-Fi network must use security compatible with the AP.

  Security stops unauthorized devices from using the Wi-Fi network. It can also protect the information that is sent in the Wi-Fi network.

#### Wi-Fi Security Overview

The following sections introduce different types of Wi-Fi security you can set up in the Wi-Fi network.

#### SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the Wi-Fi network.

#### MAC Address Filter

Every Wi-Fi client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each Wi-Fi client, see the appropriate User's Guide or other documentation.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

You can use the MAC address filter to tell the AP which Wi-Fi clients are allowed or not allowed to use the Wi-Fi network. If a Wi-Fi client is allowed to use the Wi-Fi network, it still has to have the correct settings (SSID, channel, and security). If a Wi-Fi client is not allowed to use the Wi-Fi network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the Wi-Fi network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized Wi-Fi client. Then, they can use that MAC address to use the Wi-Fi network.

### WPS

Wi-Fi Protected Setup (WPS) is an industry standard specification, defined by the Wi-Fi Alliance. WPS allows you to quickly set up a Wi-Fi network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure Wi-Fi network using WPS in the Chapter 9 on page 106.

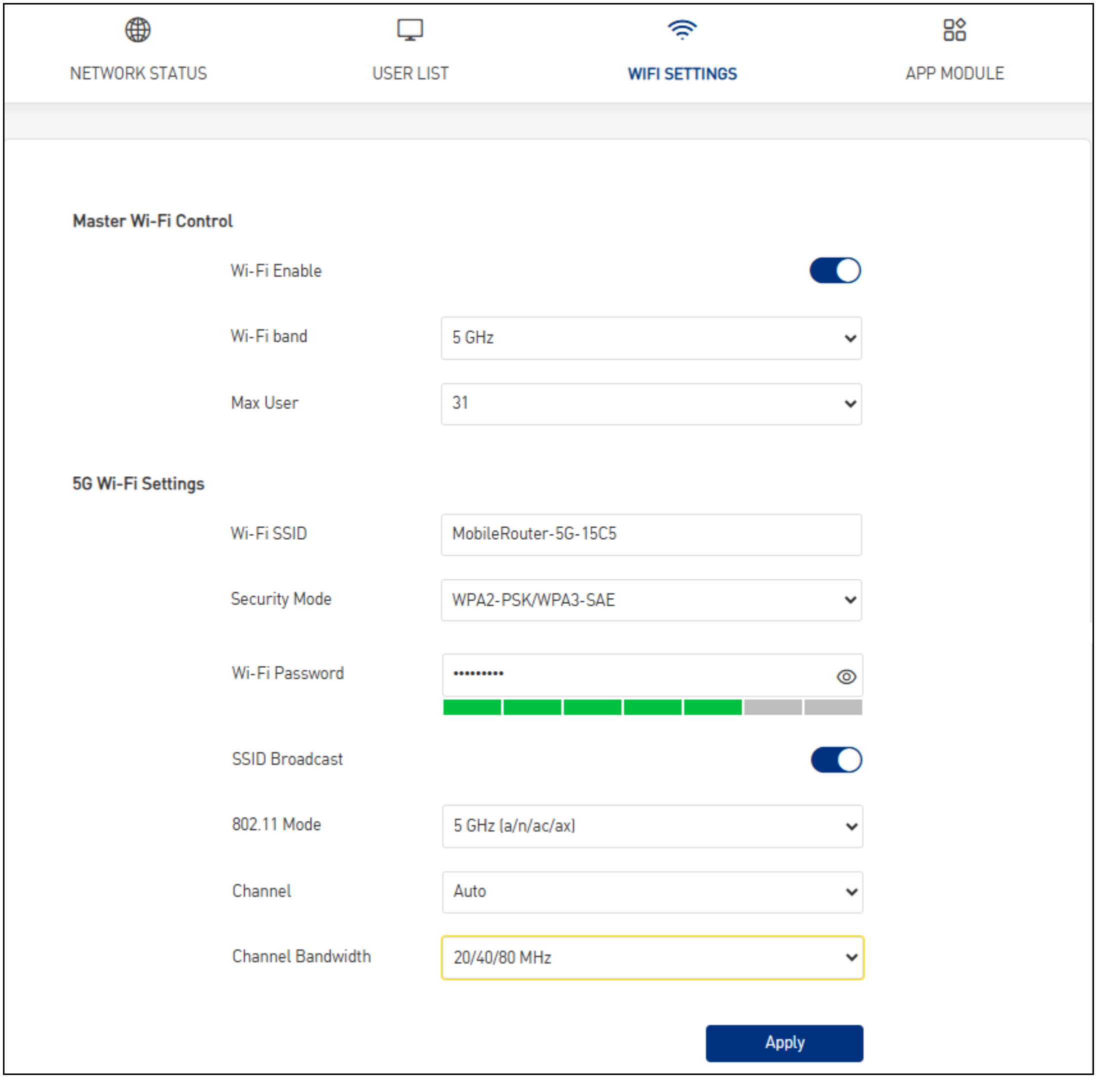
## 6.2 The WiFi Settings Screen

Use this screen to enable the wireless LAN, enter the SSID, and configure security and other Wi-Fi settings.

Note: If you are configuring the NR2111 from a device connected to the wireless LAN and you change the NR2111's SSID, channel or security settings, you will lose your Wi-Fi connection when you press **Apply** to confirm. You must then change the Wi-Fi settings of your device to match the NR2111's new settings.

To access this screen, click **WIFI SETTINGS**.

**Figure 18** WIFI SETTINGS



Master Wi-Fi Control

Wi-Fi Enable

Wi-Fi band: 5 GHz

Max User: 31

5G Wi-Fi Settings

Wi-Fi SSID: MobileRouter-5G-15C5

Security Mode: WPA2-PSK/WPA3-SAE

Wi-Fi Password: •••••••••

SSID Broadcast

802.11 Mode: 5 GHz (a/n/ac/ax)

Channel: Auto

Channel Bandwidth: 20/40/80 MHz

The following table describes the labels in this screen.

Table 15 WIFI SETTINGS

| LABEL | DESCRIPTION |
|---|---|
| Master Wi-Fi Control | |
| Wi-Fi Enable | Turn the switch button on to activate Wi-Fi on the NR2111. |
| Wi-Fi Band | Select whether the NR2111 uses the 2.4 GHz Wi-Fi band or the 5 GHz Wi-Fi band. |
| Max User | Specify the maximum number of clients (up to 31) that can connect to this network at the same time. |
| 2.4G Wi-Fi Settings/5G Wi-Fi Settings | |
| Wi-Fi SSID | The SSID (Service Set IDentity) identifies the Service Set with which a Wi-Fi client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. |

Table 15 WIFI SETTINGS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Select **WPA2-PSK, WPA-PSK/WPA2-PSK, WPA3-SAE**, or **WPA2-PSK/WPA3-SAE** to add security on this Wi-Fi network. Wi-Fi clients must support one of the selected security modes and use the same Wi-Fi key (password) to connect to the Wi-Fi network. Or you can select **Open** to use no security and allow any client to connect to this network without authentication.<br>The WPA-PSK (Wi-Fi Protected Access-Pre-Shared Key) security mode provides both data encryption and user authentication. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the NR2111 and a connecting client at the beginning of a Wi-Fi session.<br>Note: WPS can be used only when the security mode is set to **Open**, **WPA2-PSK,** or **WPA-PSK/WPA2-PSK**. |
| Wi-Fi Key/Password | Unless the **Security Mode** is set to **Open**, you need to configure a Wi-Fi key for this Wi-Fi network. Enter a Wi-Fi key from 8 to 63 case-sensitive keyboard characters. The strength of your password is displayed below. |
| SSID Broadcast | Turn the switch button on to show the SSID in the outgoing beacon frame. Turn it off to hide the SSID so a station cannot obtain the SSID through scanning using a site survey tool. |
| 802.11 Mode | Select one of the following for the 2.4G network:<br>• **2.4 GHz (b)**: allows either IEEE 802.11b compliant WLAN devices to associate with the NR2111. In this mode, all Wi-Fi devices can only transmit at the data rates supported by IEEE 802.11b.<br>• **2.4 GHz (b/g)**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NR2111. The NR2111 adjusts the transmission rate automatically according to the Wi-Fi standard supported by the Wi-Fi devices.<br>• **2.4 GHz (b/g/n)**: allows IEEE802.11b, IEEE802.11g, and IEEE802.11n compliant WLAN devices to associate with the NR2111. The transmission rate of your NR2111 might be reduced.<br>• **2.4 GHz (b/g/n/ax)**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the NR2111. The transmission rate of your NR2111 might be reduced.<br>Select one of the following for the 5G network:<br>• **5 GHz (a)**: allows only IEEE 802.11a compliant WLAN devices to associate with the NR2111.<br>• **5 GHz (a/n)**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NR2111. The transmission rate of your NR2111 might be reduced.<br>• **5 GHz (a/n/ac)**: allows both IEEE802.11a, IEEE802.11n, and IEEE802.11ac compliant WLAN devices to associate with the NR2111. The transmission rate of your NR2111 might be reduced.<br>• **5 GHz (a/n/ac/ax)**: allows both IEEE802.11a, IEEE802.11n, IEEE802.11ac, and IEEE802.11ax compliant WLAN devices to associate with the NR2111. The transmission rate of your NR2111 might be reduced. |
| Channel | Set the operating frequency/channel depending on your particular region.<br>Select **Auto** for the NR2111 to automatically choose the channel with the least interference.<br>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. |

Table 15 WIFI SETTINGS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Channel Bandwidth | Select the Wi-Fi channel width the NR2111 uses.<br>A standard 20 MHz channel (**20 MHz**) offers transfer speeds of up to 144 Mbps (2.4G) or 217 Mbps (5G) whereas a 40 MHz channel (**40 MHz**) uses two standard channels and offers speeds of up to 300 Mbps (2.4G) or 450 Mbps (5G). An IEEE 802.11ac-specific 80 MHz channel (**80 MHz**) offers speeds of up to 1.3 Gbps.<br>Because not all devices support 40 MHz and/or 80 MHz channels, select **20/40/80 MHz** to allow the NR2111 to adjust the channel bandwidth automatically.<br>**40 MHz** (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. An **80 MHz** channel consists of two adjacent 40 MHz channels. The Wi-Fi clients must also support **40 MHz** or **80 MHz**. It is often better to use the 20 MHz setting in a location where the environment hinders the Wi-Fi signal.<br>Select **20 MHz** if you want to lessen radio interference with other Wi-Fi devices in your neighborhood or the Wi-Fi clients do not support channel bonding. |
| AP Isolation | If the switch button is turned on , the clients in the NR2111's network are blocked from connecting to each other directly. |
| Apply | Click **Apply** to save your changes. |

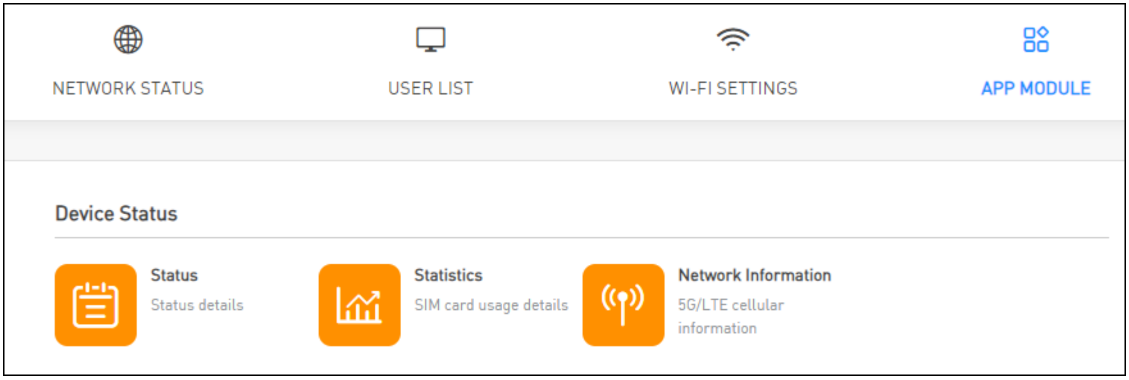
# CHAPTER 7
# Device Status

## 7.1 Overview

Use the **Device Status** screens to view the NR2111's device status information, network information, and the SIM card usage details.

- Status: Use this screen to view the NR2111's device status and information.
- Statistics: Use this screen to view the SIM card's usage details.
- Network Information: Use this screen to view the network information.

**Figure 19** APP MODULE: Device Status

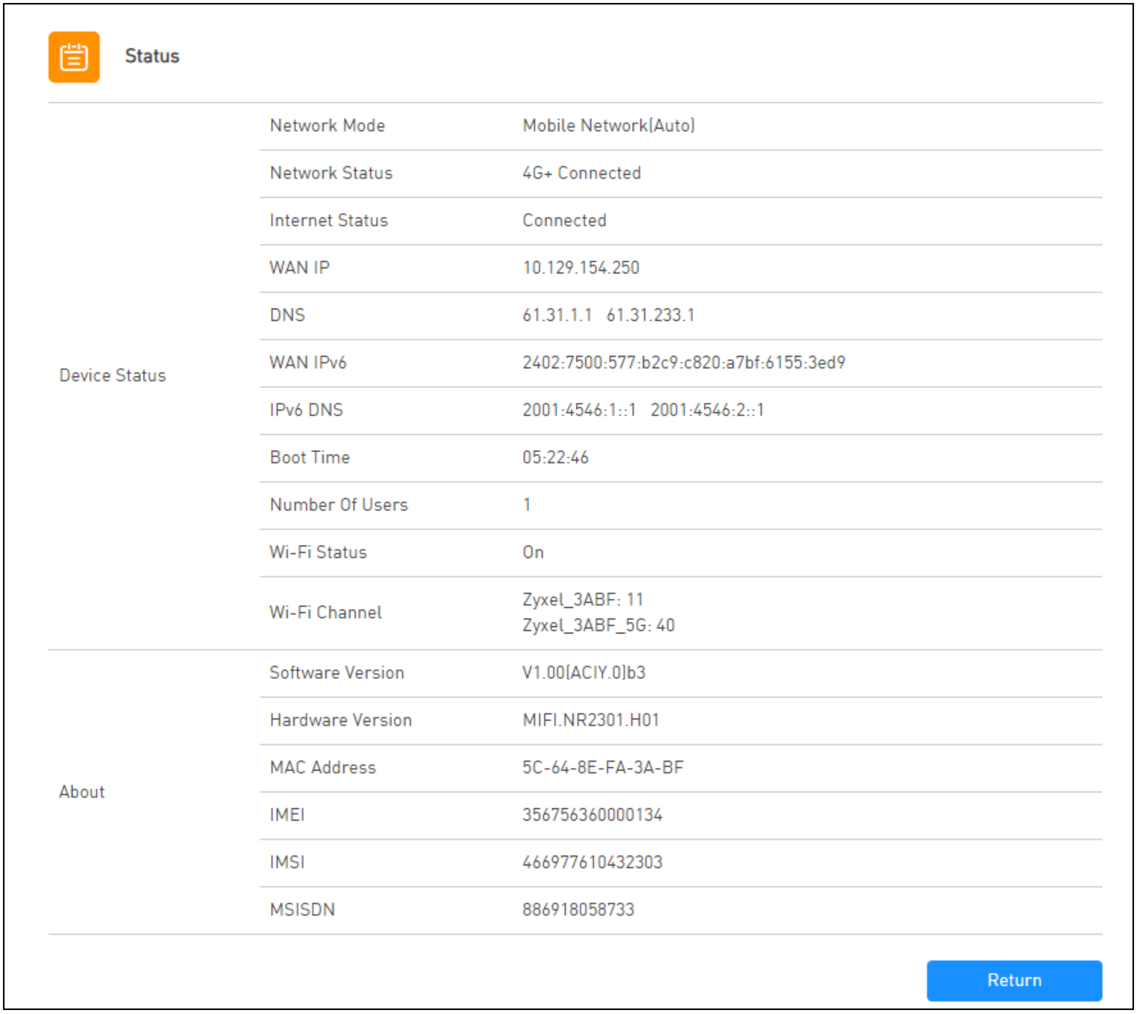


## 7.2 Status

Use the **Status** screen to check status information about the NR2111.

To access this screen, click **APP MODULE** > **Status**.

**Figure 20** APP MODULE > Status



Status

| | | |
|---|---|---|
| Device Status | Network Mode | Mobile Network(Auto) |
| | Network Status | 4G+ Connected |
| | Internet Status | Connected |
| | WAN IP | 10.129.154.250 |
| | DNS | 61.31.1.1 61.31.233.1 |
| | WAN IPv6 | 2402:7500:577:b2c9:c820:a7bf:6155:3ed9 |
| | IPv6 DNS | 2001:4546:1::1 2001:4546:2::1 |
| | Boot Time | 05:22:46 |
| | Number Of Users | 1 |
| | Wi-Fi Status | On |
| | Wi-Fi Channel | Zyxel_3ABF: 11<br>Zyxel_3ABF_5G: 40 |
| About | Software Version | V1.00(ACIY.0)b3 |
| | Hardware Version | MIFI.NR2301.H01 |
| | MAC Address | 5C-64-8E-FA-3A-BF |
| | IMEI | 356756360000134 |
| | IMSI | 466977610432303 |
| | MSISDN | 886918058733 |

The following table describes the labels in this screen.

Table 16 APP MODULE > Status

| LABEL | DESCRIPTION |
|---|---|
| Device Status | |
| Network Mode | This field displays the network mode of the NR2111. |
| Network Status | This field displays the type of network the NR2111 is using. |
| Internet Status | This field displays whether the NR2111 is connected to the Internet. |
| WAN IP | This field displays the current WAN IP address of the NR2111 in the WAN. |
| DNS | This field displays the DNS server address assigned by the ISP. |
| WAN IPv6 | This field displays the current WAN IPv6 address of the NR2111 in the WAN. |
| IPv6 DNS | This field displays the IPv6 DNS server address assigned by the ISP. |
| Boot Time | This field displays how long the current WAN connection has been up. |
| Number Of Users | This field displays the total number of devices connected to the NR2111. |
| Wi-Fi Status | This field displays whether Wi-Fi is enabled or disabled. |
| Wi-Fi Channel | This field displays the channel numbers currently used by the 2.4G and 5G wireless LAN. |
| About | |

Table 16 APP MODULE > Status (continued)

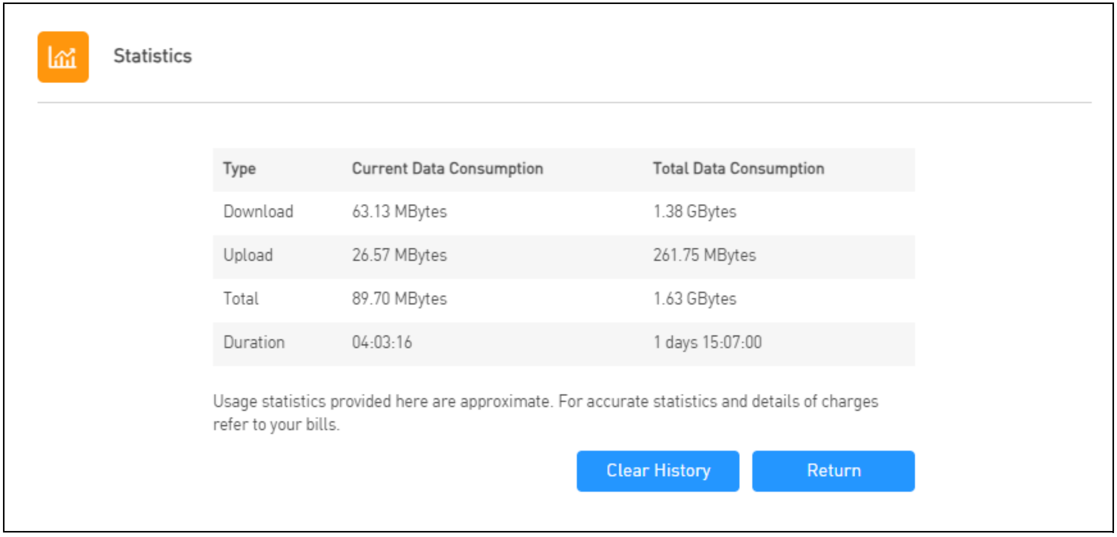
| LABEL | DESCRIPTION |
|---|---|
| Software Version | This field displays the current version of the firmware inside the NR2111. |
| Hardware Version | This field displays the hardware version of the NR2111. |
| MAC Address | This field displays the MAC address of the NR2111. |
| IMEI | This field displays the International Mobile Equipment Number (IMEI) which is the serial number of the built-in 4G/5G module. IMEI is a unique 15-digit number used to identify a mobile device. |
| IMSI | This field displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network. |
| MSISDN | This field displays the MSISDN (Mobile Subscriber ISDN) number, a phone number assigned to a mobile subscriber to call a mobile device. |
| Return | Click this button to return to the **APP MODULE** list. |

# 7.3 Statistics

Use the **Statistics** screen to view the SIM card's usage details.

To access this screen, click **APP MODULE** > **Statistics**.

**Figure 21** APP MODULE > Statistics



Statistics

| Type | Current Data Consumption | Total Data Consumption |
|---|---|---|
| Download | 63.13 MBytes | 1.38 GBytes |
| Upload | 26.57 MBytes | 261.75 MBytes |
| Total | 89.70 MBytes | 1.63 GBytes |
| Duration | 04:03:16 | 1 days 15:07:00 |

Usage statistics provided here are approximate. For accurate statistics and details of charges refer to your bills.

The following table describes the labels in this screen.

Table 17 APP MODULE > Statistics

| LABEL | DESCRIPTION |
|---|---|
| Type | This column displays the type of statistics you are viewing. |
| Current Data Consumption | This column displays the data consumption of the specified statistics on the SIM card for the current connection session. |
| Total Data Consumption | This column displays the total data consumption of the specified statistics on the SIM card since it has been activated. |

Table 17 APP MODULE > Statistics (continued)

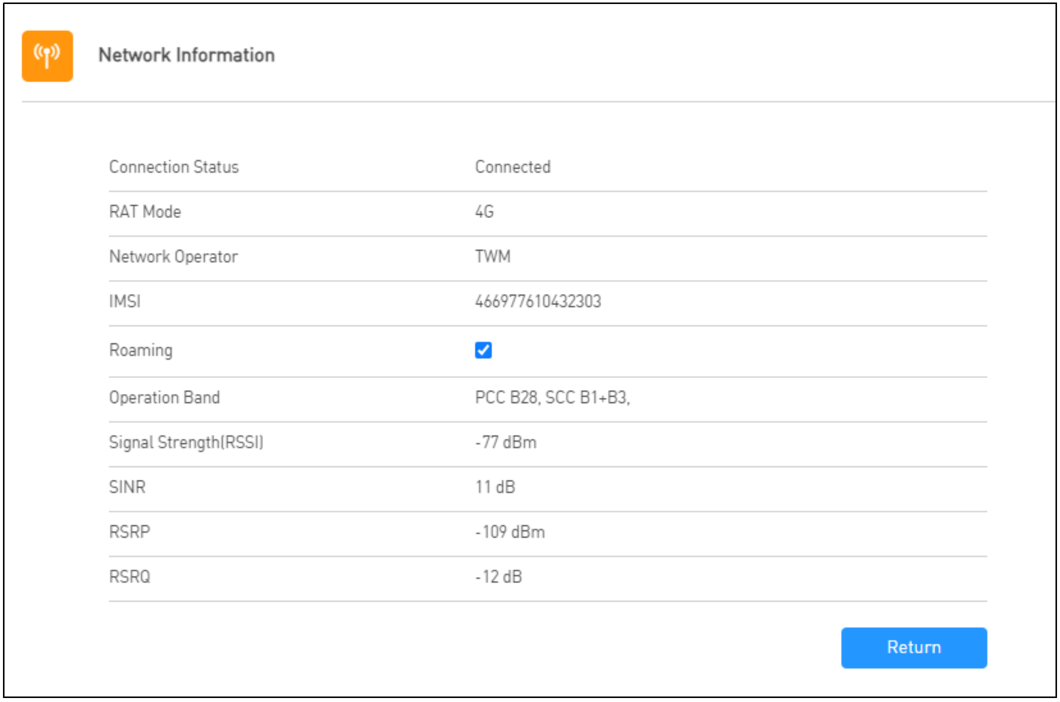
| LABEL | DESCRIPTION |
|---|---|
| Download | This field displays the number of received packets on the SIM card for the current connection session or in total. |
| Upload | This field displays the number of transmitted packets on the SIM card for the current connection session or in total. |
| Total | This field displays the total number of transmitted and received packets on the SIM card for the current connection session or in total. |
| Duration | This field displays the duration of the current connection session or in total. |
| Clear History | Click this button to clear all history statistics from the SIM card. |
| Return | Click this button to return to the **APP MODULE** list. |

## 7.4 Network Information

Use the **Network Information** screen to view the NR2111's network information.

To access this screen, click **APP MODULE** > **Network Information**.

**Figure 22** APP MODULE > Network Information



Network Information

| | |
|---|---|
| Connection Status | Connected |
| RAT Mode | 4G |
| Network Operator | TWM |
| IMSI | 466977610432303 |
| Roaming | ☑ |
| Operation Band | PCC B28, SCC B1+B3, |
| Signal Strength(RSSI) | -77 dBm |
| SINR | 11 dB |
| RSRP | -109 dBm |
| RSRQ | -12 dB |

The following table describes the labels in this screen.

Table 18 APP MODULE > Network Information

| LABEL | DESCRIPTION |
|---|---|
| Connection Status | This displays whether the NR2111 is connected to the Internet. |
| RAT Mode | This displays the network mode that the NR2111 used to register with the service provider's mobile network. |
| Network Operator | This displays the name of the service provider. |

Table 18   APP MODULE > Network Information (continued)

| LABEL | DESCRIPTION |
|---|---|
| IMSI | This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network. |
| Roaming | This displays whether the NR2111 is connected to another service provider's mobile network using roaming. |
| Operation Band | This displays the network type and the frequency band used by the mobile network to which the NR2111 is connecting. |
| Signal Strength(RSSI) | This displays the received signal strength indicator (RSSI), that is, the received signal strength in dBm. |
| SINR | This displays the Signal to Interference plus Noise Ratio (SINR). A negative value means more noise than signal. |
| RSRP | This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Elements (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. |
| RSRQ | This displays the Reference Signal Received Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. |
| Return | Click this button to return to the **APP MODULE** list. |

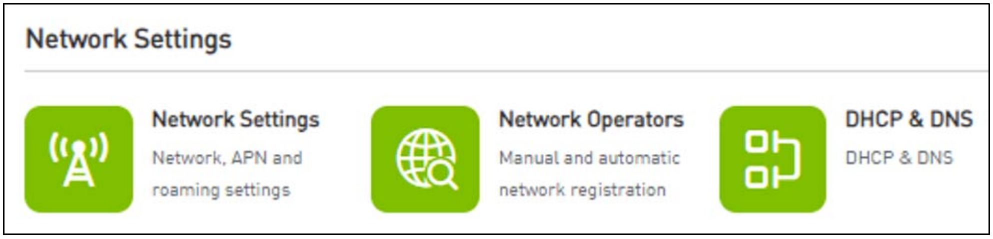
# CHAPTER 8 Network Settings

## 8.1 Overview

Use the **Network Settings** screens to configure the NR2111's network, APN, roaming, and DHCP/DNS settings. You can also view available Public Land Mobile Networks (PLMNs) and select your preferred network.

- Network Settings: Use this screen to configure the NR2111's network, APN, and roaming settings.
- Network Operators: Use this screen to view available PLMNs and select your preferred network.
- DHCP & DNS: Use this screen to configure DHCP and DNS settings.

**Figure 23** APP MODULE: Network Settings

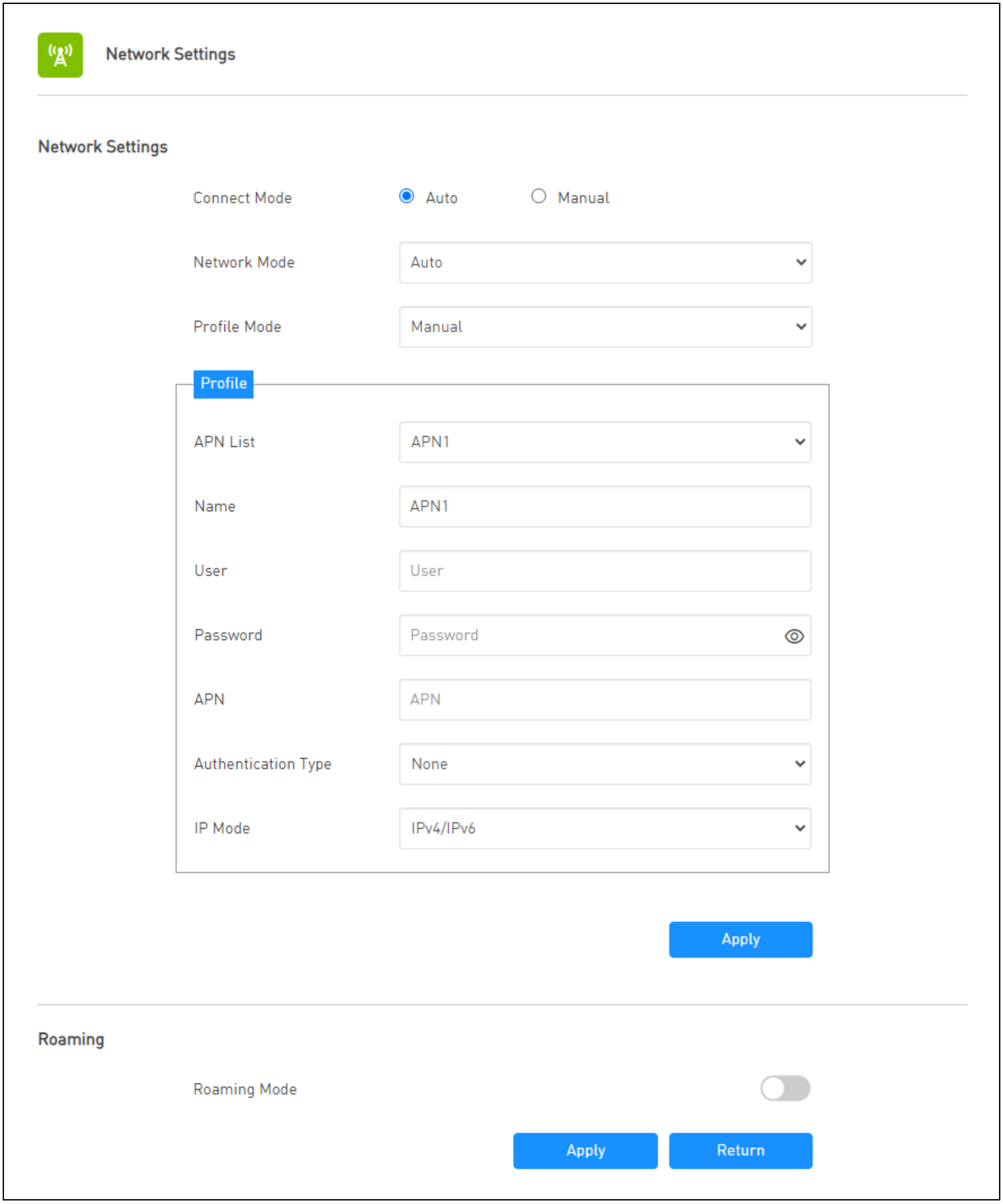

Network Settings
Network Settings
Network, APN and roaming settings
Network Operators
Manual and automatic network registration
DHCP & DNS
DHCP & DNS

## 8.2 Network Settings

Use the **Network Settings** screen to configure the NR2111's network, APN, and roaming settings.

To access this screen, click **APP MODULE** > **Network Settings**.

**Figure 24** APP MODULE > Network Settings



Network Settings

| | |
|---|---|
| Connect Mode | ● Auto ○ Manual |
| Network Mode | Auto |
| Profile Mode | Manual |

Profile

| | |
|---|---|
| APN List | APN1 |
| Name | APN1 |
| User | User |
| Password | Password |
| APN | APN |
| Authentication Type | None |
| IP Mode | IPv4/IPv6 |

Roaming

Roaming Mode ○

The following table describes the labels in this screen.

Table 19 APP MODULE > Network Settings

| LABEL | DESCRIPTION |
|---|---|
| Network Settings | |
| Connect Mode | Select **Auto** to have the NR2111 connect to the mobile network automatically after it has been restarted or registered.<br>If you select **Manual**, you can manually connect or disconnect the NR2111's mobile network connection in the **NETWORK STATUS** screen. See Chapter 4 on page 45 for more information. |

Table 19 APP MODULE > Network Settings (continued)

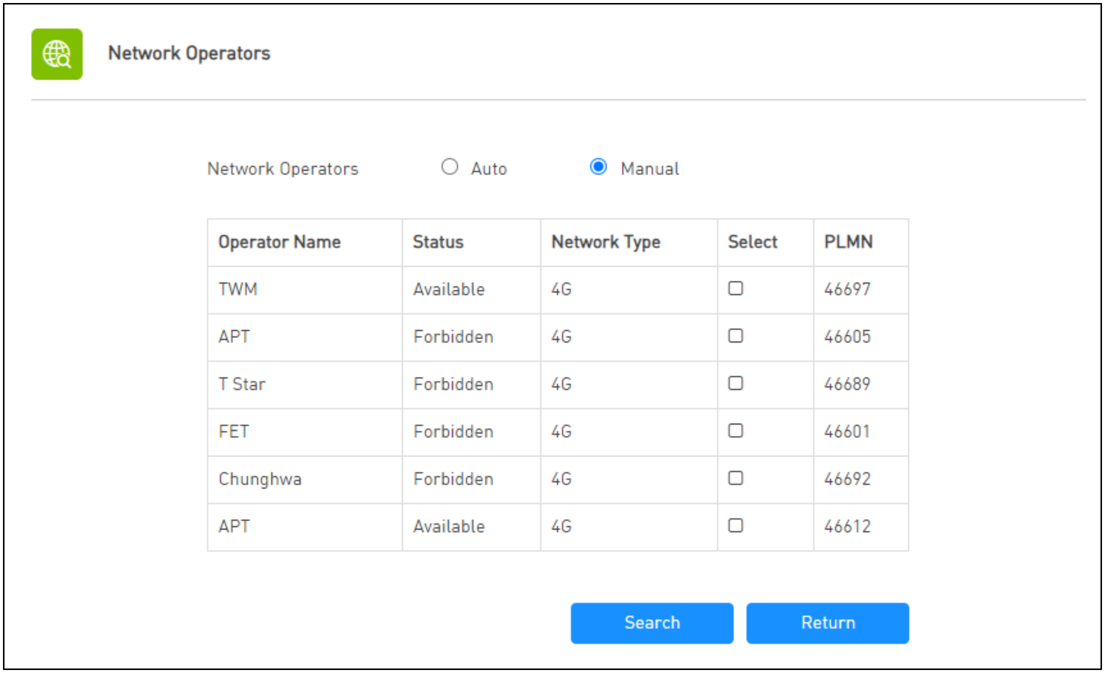
| LABEL | DESCRIPTION |
|---|---|
| Network Mode | Select the type of the network (**5G-SA**, **5G-NSA**, or **4G**) to which you want the NR2111 to connect. Otherwise, select **Auto** to have the NR2111 connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the NR2111 switches to another available mobile network. |
| Profile Mode | Connections with different APNs (Access Point Names) may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge methods.<br>Select **Auto** to have the APN information automatically configured.<br>If you select **Manual** in the **Connect Mode** field, manually enter the APN information provided by your service provider. |
| APN List | Select the APN profile from the list to configure. |
| Name | Enter the descriptive name for this APN (of up to 64 ASCII printable characters). |
| User | Enter the user name (of up to 64 ASCII printable characters) given to you by your service provider. |
| Password | Enter the password (of up to 64 ASCII printable characters) associated with the user name above. |
| APN | Enter the APN (of up to 64 ASCII printable characters) given to you by your service provider. |
| Authentication Type | The NR2111 supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms<br>Select an authentication protocol (**PAP**, or **CHAP**) used by the service provider. Otherwise, select **Auto** to have the NR2111 accept either CHAP or PAP. |
| IP Mode | Select **IPv4/IPv6** to allow the NR2111 to run IPv4 and IPv6 at the same time.<br>Select **IPv4** if you want the NR2111 to run IPv4 only.<br>Select **IPv6** if you want the NR2111 to run IPv6 only. |
| Apply | Click **Apply** to save your changes. |
| Roaming | |
| Roaming Mode | Turn the switch button on to enable roaming on the NR2111.<br>4G/5G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your NR2111 is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

## 8.3 Network Operators

Use the **Network Operators** screen to view available Public Land Mobile Networks (PLMNs) and select your preferred network when the NR2111 is outside the geographical coverage area of the network to which you are registered and roaming is enabled.

To access this screen, click **APP MODULE** > **Network Operators**.

**Figure 25** APP MODULE > Network Operators



Network Operators

Network Operators ○ Auto ● Manual

| Operator Name | Status | Network Type | Select | PLMN |
|---|---|---|---|---|
| TWM | Available | 4G | □ | 46697 |
| APT | Forbidden | 4G | □ | 46605 |
| T Star | Forbidden | 4G | □ | 46689 |
| FET | Forbidden | 4G | □ | 46601 |
| Chunghwa | Forbidden | 4G | □ | 46692 |
| APT | Available | 4G | □ | 46612 |

The following table describes the labels in this screen.

Table 20 APP MODULE > Network Operators

| LABEL | DESCRIPTION |
|---|---|
| Auto | Select **Auto** to have the NR2111 automatically connect to the first available mobile network. |
| Manual | Select **Manual** to manually select a preferred network. |
| Operator Name | This shows the ISP name. |
| Status | This displays **Current** to display the PLMN to which your NR2111 is currently connected.<br>This displays **Available** to display other PLMNs available from your ISP.<br>This displays **Forbidden** to display PLMNs available by other ISPs. To connect to one of these networks you need a working SIM card of the ISP shown. |
| Network Type | This shows the type of network the ISP provides. |
| Select | Click **Select** to have the NR2111 establish a connection to the selected mobile network. |
| PLMN | This shows the PLMN number. |
| Search | Click **Search** so the NR2111 can search for PLMNs in the area. You need a working SIM card to be able to scan for PLMNs. |
| Return | Click this button to return to the **APP MODULE** list. |

# 8.4 DHCP & DNS

### DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NR2111's WLAN as a DHCP server or disable it. When configured as a server, the NR2111 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

The NR2111 has built-in DHCP server capability that assigns IP addresses to systems that support DHCP client capability. Use the **DHCP** screen to enable the DHCP server.

## DNS

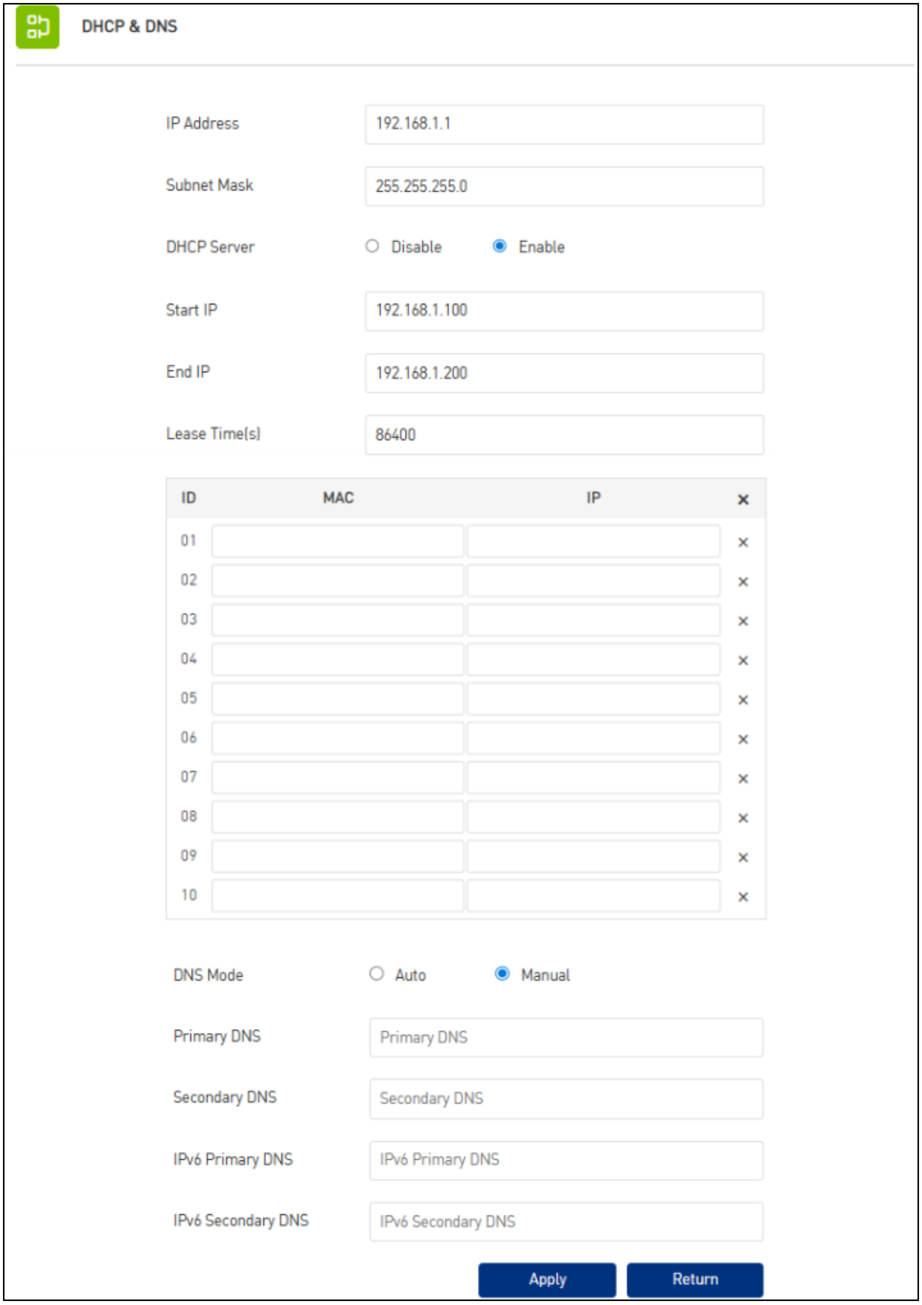
A Domain Name System (DNS) server records mappings of FQDN (Fully Qualified Domain Names) to IP addresses. A FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com” is the top level domain.

The NR2111 can get the DNS server addresses in the following ways.

- If your ISP dynamically assigns the DNS server IP addresses (along with the NR2111’s WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- You can manually enter the IP addresses of other DNS servers.

To access this screen, click **APP MODULE** > **DHCP & DNS**.

**Figure 26** APP MODULE > DHCP & DNS



DHCP & DNS

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server: ○ Disable ● Enable

Start IP: 192.168.1.100

End IP: 192.168.1.200

Lease Time(s): 86400

| ID | MAC | IP | × |
|---|---|---|---|
| 01 | | | × |
| 02 | | | × |
| 03 | | | × |
| 04 | | | × |
| 05 | | | × |
| 06 | | | × |
| 07 | | | × |
| 08 | | | × |
| 09 | | | × |
| 10 | | | × |

DNS Mode: ○ Auto ● Manual

Primary DNS: Primary DNS

Secondary DNS: Secondary DNS

IPv6 Primary DNS: IPv6 Primary DNS

IPv6 Secondary DNS: IPv6 Secondary DNS

The following table describes the labels in this screen.

Table 21 APP MODULE > DHCP & DNS

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the LAN IPv4 IP address you want to assign to the NR2111 in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| Subnet Mask | Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). The NR2111 automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so. |

Table 21 APP MODULE > DHCP & DNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| DHCP Server | Select **Disable** to stop the DHCP server on the NR2111.<br>Select **Enable** to have the NR2111 act as a DHCP server or DHCP relay agent.<br>When configured as a server, the NR2111 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, enter the following fields. |
| Start IP | This field specifies the first of the contiguous addresses in the IP address pool. |
| End IP | This field specifies the last of the contiguous addresses in the IP address pool. |
| Lease Time(s) | This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. |
| This following part allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can configure up to 10 entries. | |
| ID | This is the index number of the entry. |
| MAC | Enter the MAC address (with colons) of a computer on your LAN. |
| IP | Enter the LAN IP address of a computer on your LAN. |
| X | Click the **X** next to an entry to clear it. |
| DNS Mode | Select **Auto** to use the DNS server address assigned by the ISP.<br>Select **Manual** to manually enter the IP addresses of the DNS servers. |
| Primary DNS | Enter the DNS when the NR2111 is on an IPv4 Network. |
| Secondary DNS | Enter a DNS the NR2111 uses when the **Primary DNS** is not available. |
| IPv6 Primary DNS | Enter the DNS when the NR2111 is on an IPv6 Network. |
| IPv6 Secondary DNS | Enter a DNS the NR2111 uses when the **IPv6 Primary DNS** is not available. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

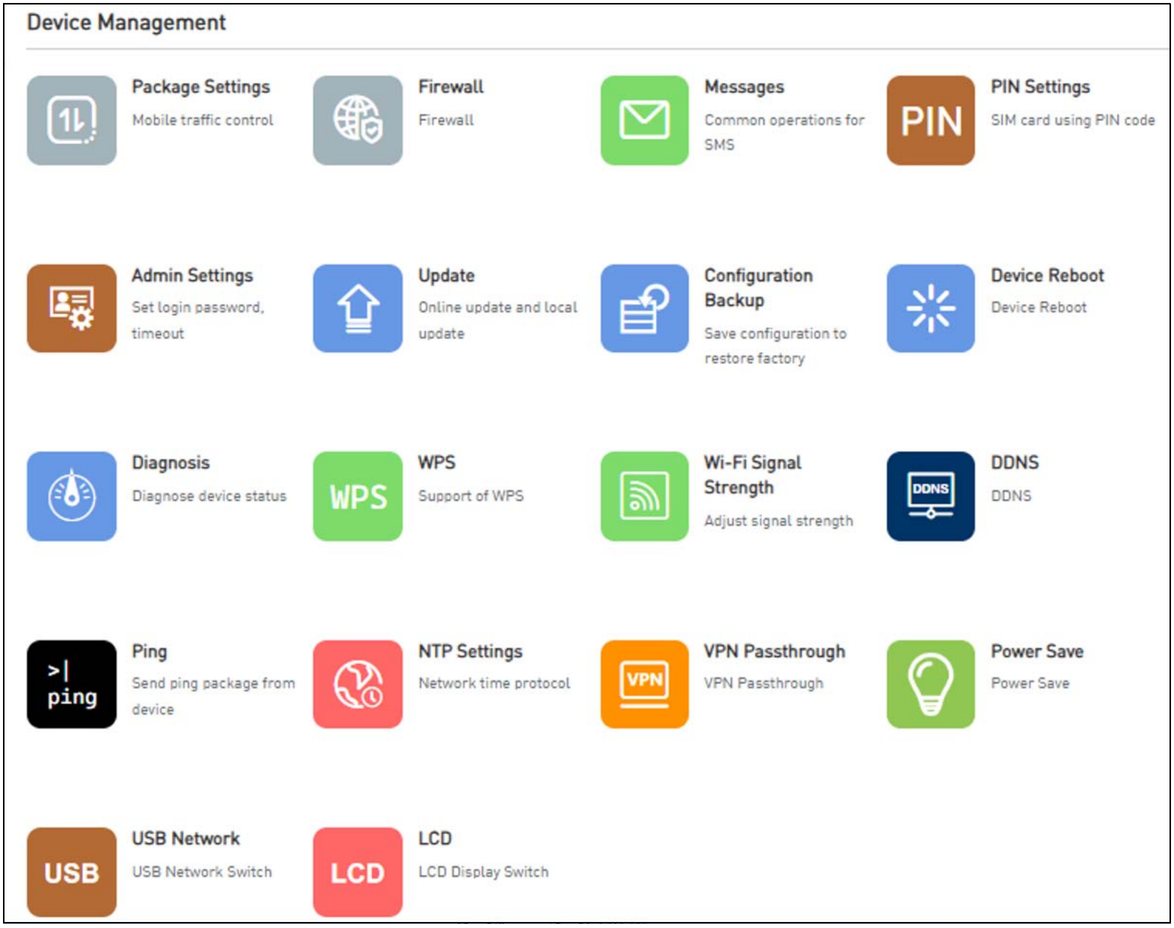
# CHAPTER 9
# Device Management

## 9.1 Overview

Use the **Device Management** screens to configure advanced settings on the NR2111.

- Package Settings: Use this screen to set up a limited allowance of data.
- Firewall: Use these screens to configure IP filters, port forward, port trigger, remote management, and DMZ.
- Messages: Use this screen to view and manage SMS messages.
- PIN Settings: Use this screen to set up PIN code authentication.
- Admin Settings: Use this screen to configure the login password and timeout settings.
- Update: Use these screens to display the current firmware version and update new firmware to the NR2111.
- Configuration Backup: Use this screen to backup and restore the configuration or reset the factory defaults to your NR2111.
- Device Reboot: This screen allows you to reboot the NR2111 without turning the power off. You can also set a schedule to reboot the NR2111
- Diagnosis: Use this screen to check the Wi-Fi and status of the NR2111.
- WPS: Use this screen to configure and activate WPS.
- Wi-Fi Signal Strength: Use this screen to adjust Wi-Fi signal strength.
- DDNS: Use this screen to set up dynamic DNS.
- Ping: Use this screen to test connectivity between two devices on the network.
- NTP Settings: Use this screen to configure the time server.
- VPN Passthrough: Use this screen to enable or disable L2TP, IPSec, and PPTP on the NR2111.
- Power Save: Use this screen to configure the NR2111's sleep mode.
- USB Network: Use this screen to allow client devices connect to the NR2111 through the USB cable.
- LCD: Use this screen to show or hide the Wi-Fi information on the LCD.

**Figure 27** APP MODULE: Device Management



Device Management

Package Settings
Mobile traffic control

Firewall
Firewall

Messages
Common operations for SMS

PIN Settings
SIM card using PIN code

Admin Settings
Set login password, timeout

Update
Online update and local update

Configuration Backup
Save configuration to restore factory

Device Reboot
Device Reboot

Diagnosis
Diagnose device status

WPS
Support of WPS

Wi-Fi Signal Strength
Adjust signal strength

DDNS
DDNS

Ping
Send ping package from device

NTP Settings
Network time protocol

VPN Passthrough
VPN Passthrough

Power Save
Power Save

USB Network
USB Network Switch

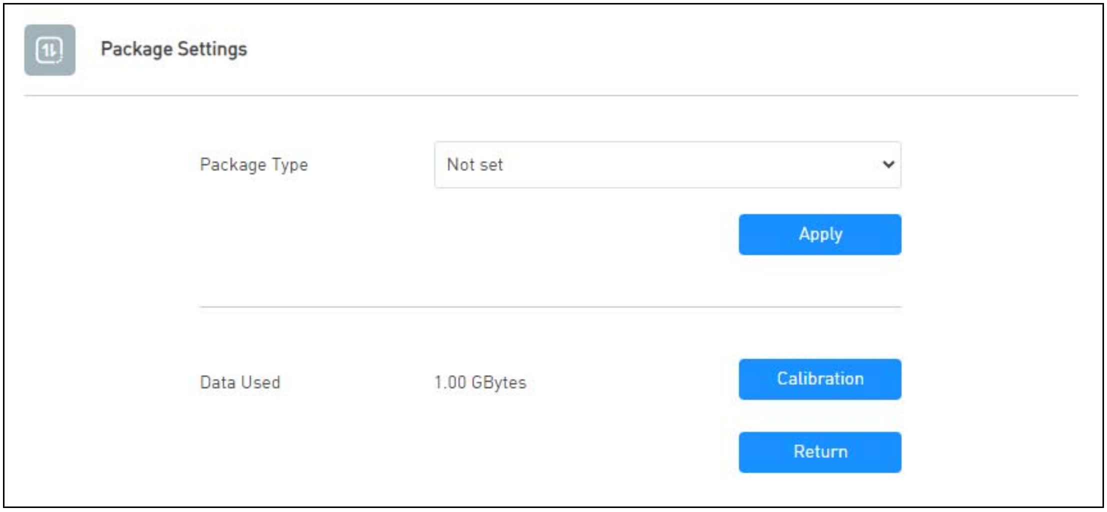
LCD
LCD Display Switch

## 9.2 Package Settings

Use the **Package Settings** screen to enable mobile data usage control and set a data limit for a certain period of time.

To access this screen, click **APP MODULE** > **Package Settings**. The screen may vary depending on the package type you select.

**Figure 28** APP MODULE > Package Settings: Not set



Package Settings

Package Type: Not set

The following table describes the labels in this screen.

Table 22 APP MODULE > Package Settings: Not set

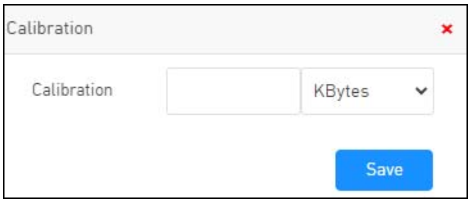
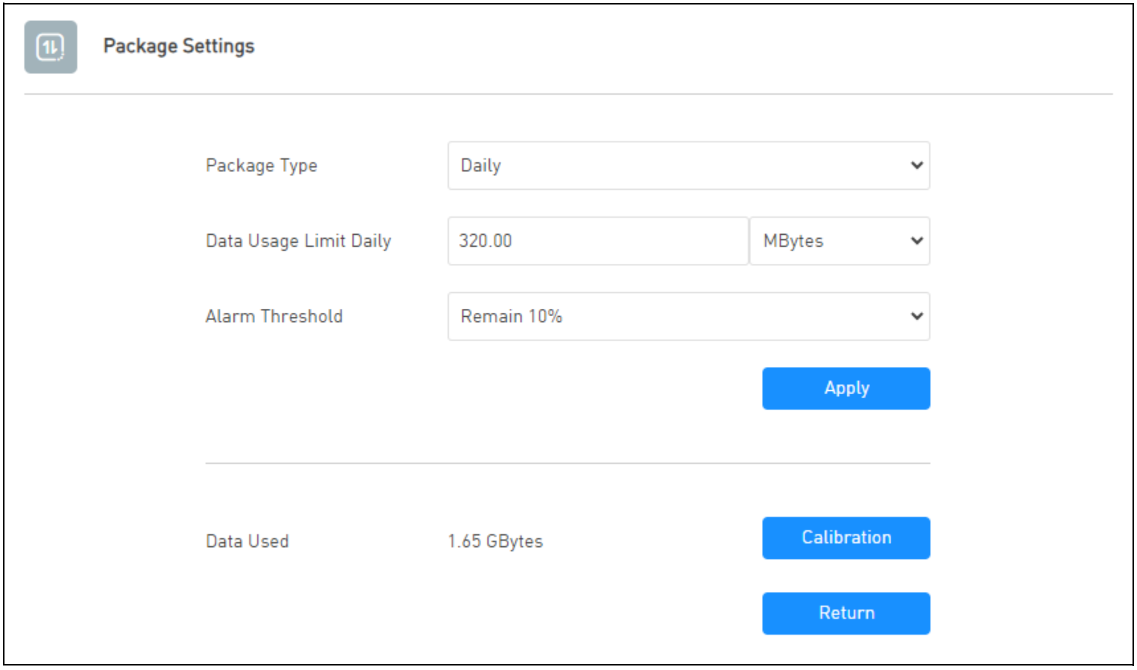
| LABEL | DESCRIPTION |
|---|---|
| Package Type | Select **Not set** to disable mobile data usage control. There is no data usage limit on the NR2111. |
| Apply | Click **Apply** to save your changes. |
| Data Used | This displays the mobile data used by the NR2111 so far. |
| Calibration | Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting.<br><br>Calibration<br>Calibration: KBytes<br>Save |
| Return | Click this button to return to the **APP MODULE** list. |

**Figure 29** APP MODULE > Package Settings: Daily



Package Settings

Package Type: Daily

Data Usage Limit Daily: 320.00 MBytes

Alarm Threshold: Remain 10%

Data Used: 1.65 GBytes

The following table describes the labels in this screen.

Table 23 APP MODULE > Package Settings: Daily

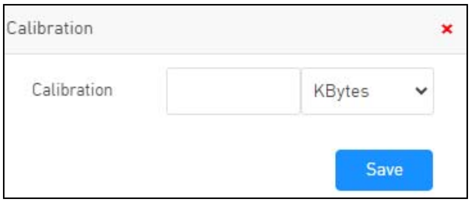
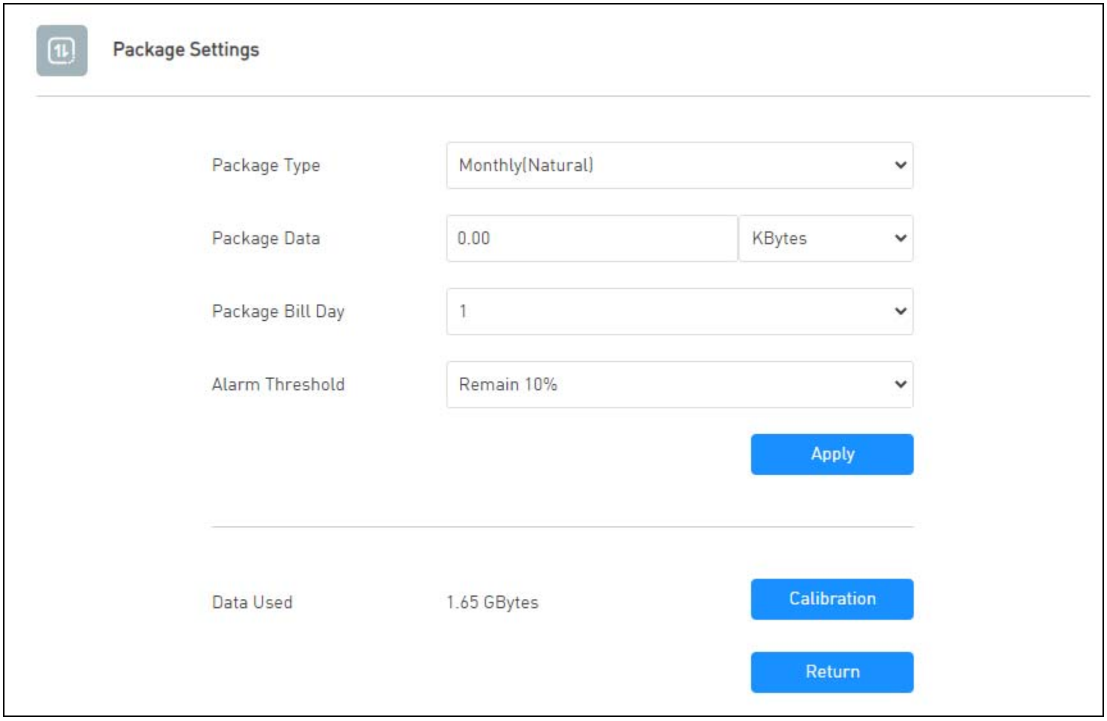
| LABEL | DESCRIPTION |
|---|---|
| Package Type | Select **Daily** to enable mobile data usage control and set a daily data limit. |
| Data Usage Limit Daily | Specify the amount of data that can be transmitted via the mobile connection daily. |
| Alarm Threshold | Specify the percentage of data usage the NR2111 has to reach to display a notification on the NR2111's LCD **Home** screen and Web Configurator's **Main** screen. |
| Apply | Click **Apply** to save your changes. |
| Data Used | This displays the mobile data used by the NR2111 so far. |
| Calibration | Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting.<br><br>Calibration<br>Calibration KBytes<br> |
| Return | Click this button to return to the **APP MODULE** list. |

**Figure 30** APP MODULE > Package Settings: Monthly



Package Settings

Package Type: Monthly(Natural)

Package Data: 0.00 KBytes

Package Bill Day: 1

Alarm Threshold: Remain 10%

Data Used: 1.65 GBytes

The following table describes the labels in this screen.

Table 24 APP MODULE > Package Settings: Monthly

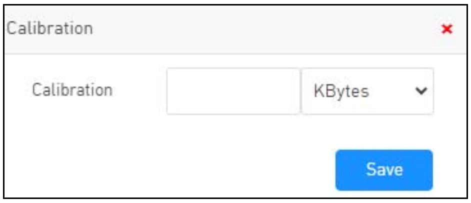
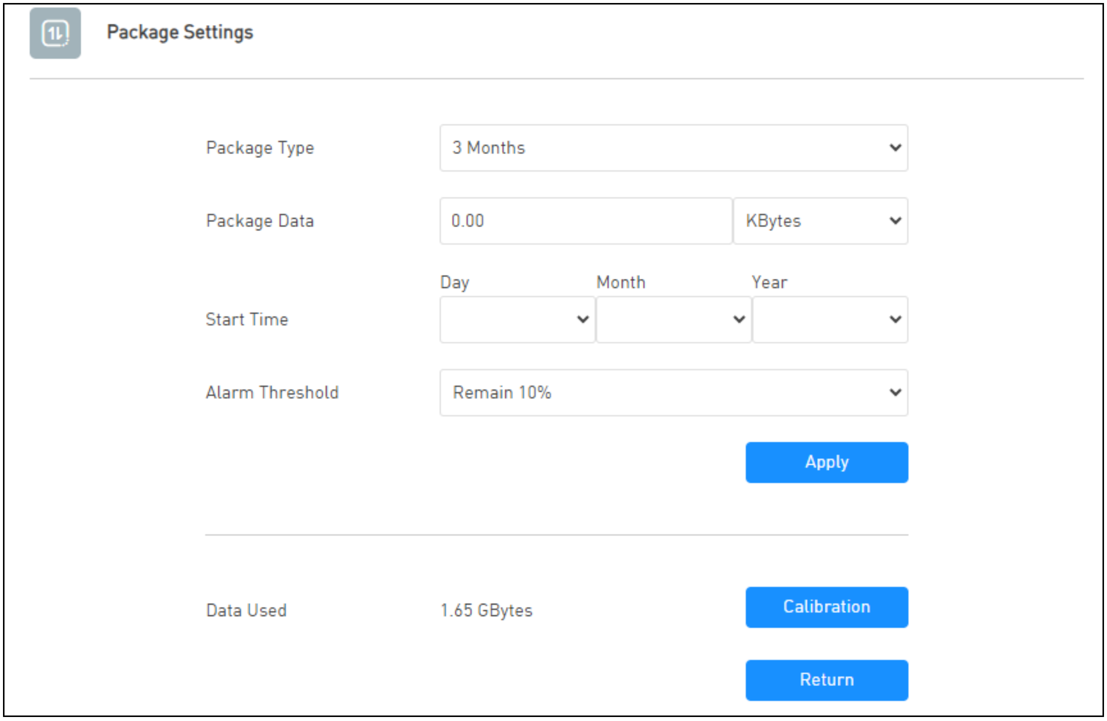
| LABEL | DESCRIPTION |
|---|---|
| Package Type | Select **Monthly** to enable mobile data usage control and set a monthly data limit. |
| Package Data | Specify the amount of data that can be transmitted via the mobile connection monthly. |
| Package Bill Day | Select the day of the month on which the NR2111 restarts calculating the amount of data per month. |
| Alarm Threshold | Select the percentage of data usage the NR2111 has to reach to display a notification on the NR2111's LCD **Home** screen and Web Configurator's **Main** screen. |
| Apply | Click **Apply** to save your changes. |
| Data Used | This displays the mobile data used by the NR2111 during the current period. |
| Calibration | Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting.<br><br>Calibration<br>Calibration: KBytes<br> |
| Return | Click this button to return to the **APP MODULE** list. |

**Figure 31** APP MODULE > Package Settings: 3 Months/Half year/Year



Package Settings

Package Type: 3 Months

Package Data: 0.00 KBytes

Start Time: Day, Month, Year

Alarm Threshold: Remain 10%

Data Used: 1.65 GBytes

The following table describes the labels in this screen.

Table 25 APP MODULE > Package Settings: 3 Months/Half year/Year

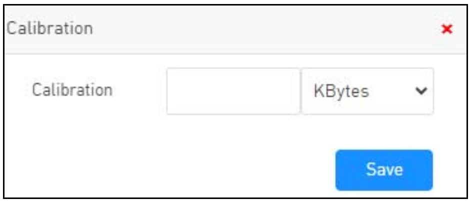
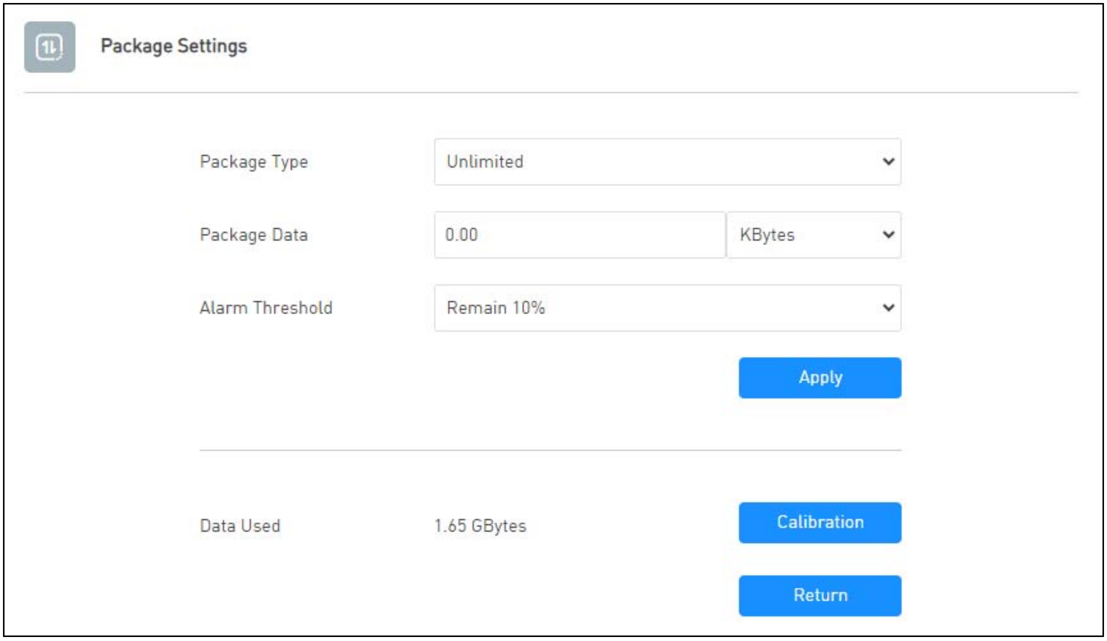
| LABEL | DESCRIPTION |
|---|---|
| Package Type | Select **3 Months/Half year/Year** to enable mobile data usage control and set a data limit every 3 months/half a year/year. |
| Package Data | Specify the amount of data that can be transmitted via the mobile connection every 3 months/half a year/year. |
| Start Time | Select the day, month, and year on which the NR2111 restarts calculating the amount of data. |
| Alarm Threshold | Select the percentage of data usage the NR2111 has to reach to display a notification on the NR2111's LCD **Home** screen and Web Configurator **Main** screen. |
| Apply | Click **Apply** to save your changes. |
| Data Used | This displays the mobile data used by the NR2111 during the current period. |
| Calibration | Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting.<br><br>Calibration<br>Calibration: KBytes<br> |
| Return | Click this button to return to the **APP MODULE** list. |

**Figure 32** APP MODULE > Package Settings: Unlimited



Package Settings

Package Type: Unlimited

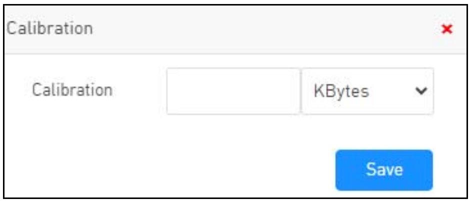
Package Data: 0.00 KBytes

Alarm Threshold: Remain 10%

Data Used: 1.65 GBytes

The following table describes the labels in this screen.

Table 26 APP MODULE > Package Settings: Unlimited

| LABEL | DESCRIPTION |
|---|---|
| Package Type | Select **Unlimited** to enable mobile data usage control and set a data limit. |
| Package Data | Specify the amount of data that can be transmitted via the mobile connection. |
| Alarm Threshold | Select the percentage of data usage the NR2111 has to reach to display a notification on the NR2111's LCD **Home** screen and Web Configurator's **Main** screen. |
| Apply | Click **Apply** to save your changes. |
| Data Used | This displays the mobile data used by the NR2111 during the current period. |
| Calibration | Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting.<br><br>Calibration<br>Calibration: KBytes<br>Save |
| Return | Click this button to return to the **APP MODULE** list. |

# 9.3 Firewall

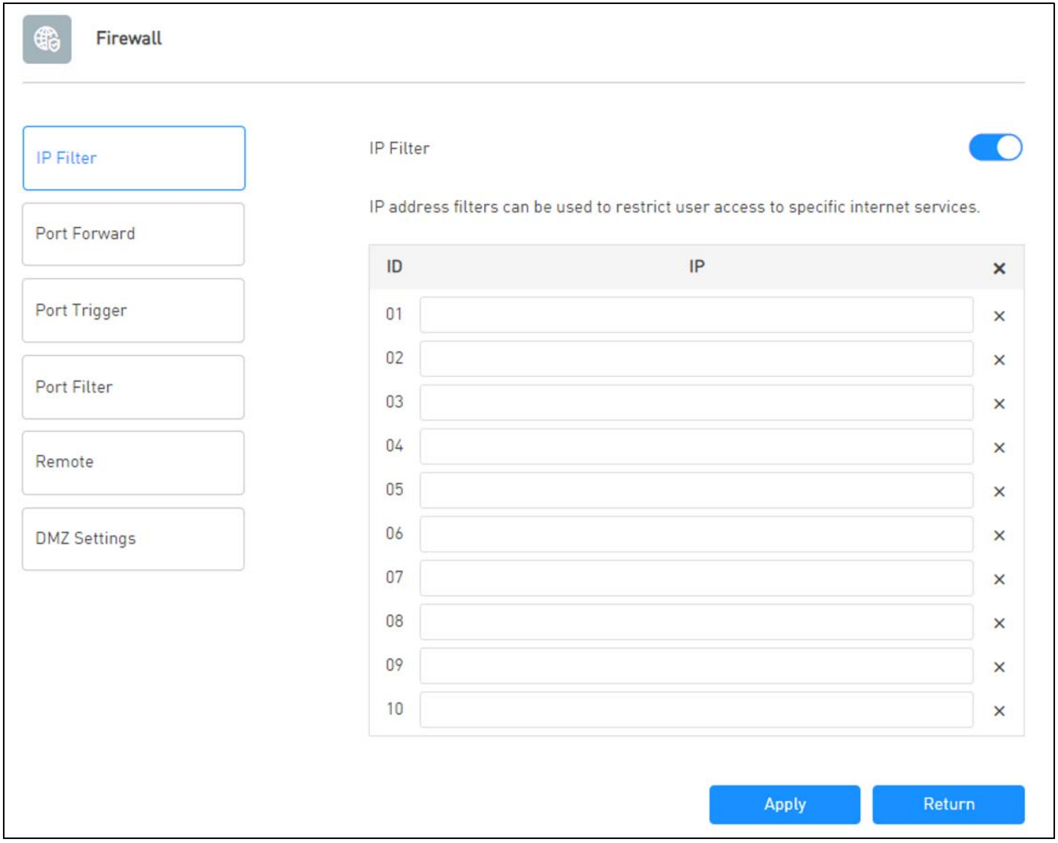
Use the **Firewall** screens to configure IP filters, port forward, port trigger, port filters, remote management, and DMZ.

### 9.3.1 IP Filter

Use the **IP Filter** screen to block clients from accessing specific Internet services.

To access this screen, click **APP MODULE** > **Firewall**.

**Figure 33** APP MODULE > Firewall > IP Filter



IP address filters can be used to restrict user access to specific internet services.

| ID | IP | × |
|---|---|---|
| 01 | | × |
| 02 | | × |
| 03 | | × |
| 04 | | × |
| 05 | | × |
| 06 | | × |
| 07 | | × |
| 08 | | × |
| 09 | | × |
| 10 | | × |

The following table describes the labels in this screen.

Table 27 APP MODULE > Firewall > IP Filter

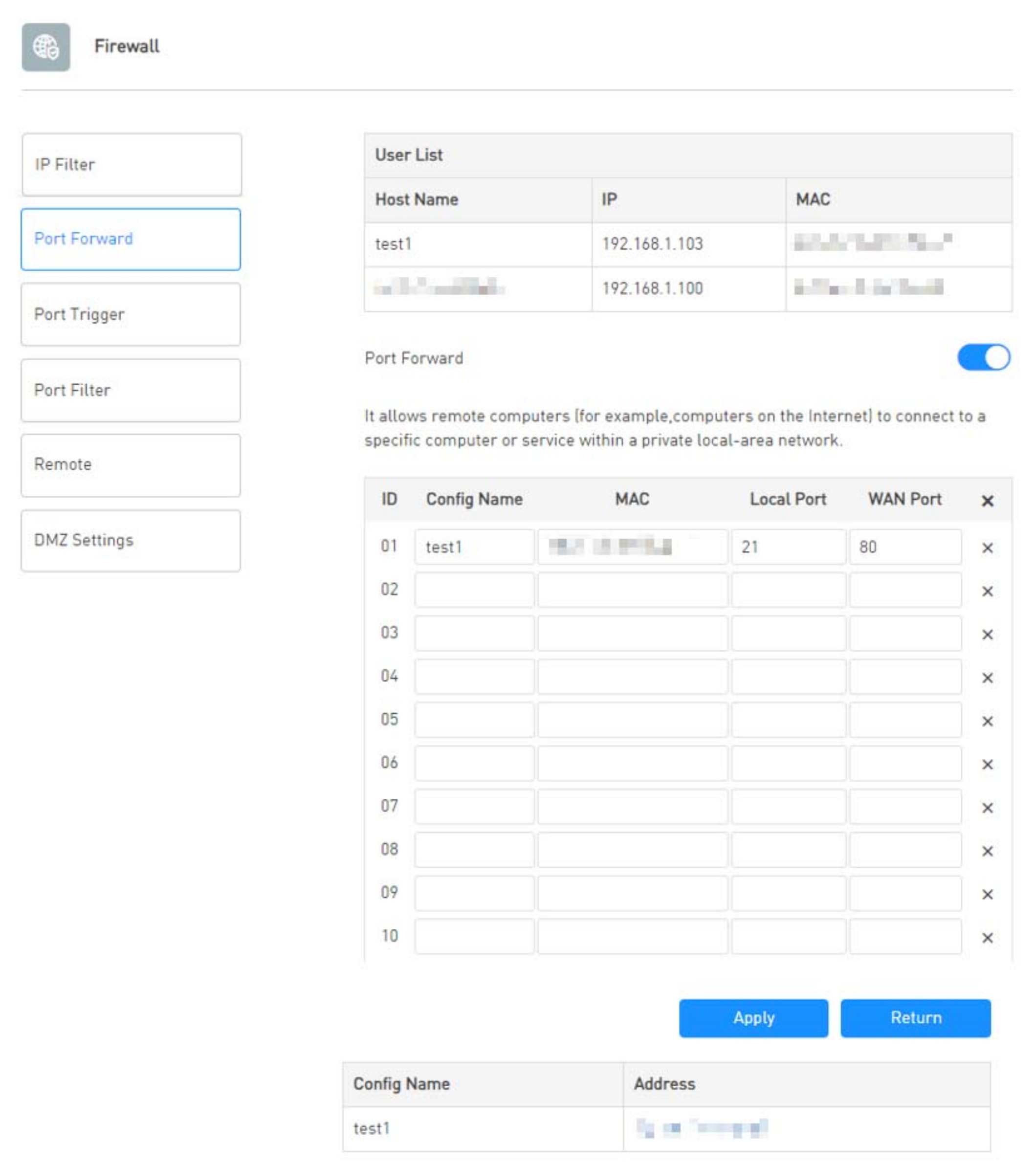
| LABEL | DESCRIPTION |
|---|---|
| Turn the switch button on ● to enable IP filter on the NR2111. This blocks clients from accessing specific Internet services listed below. | |
| ID | This is the index number of the entry. |
| IP | Enter the IP address of the Internet service which you do not want the NR2111's clients to access. You can configure up to 10 entries. |
| X | Click the **X** next to an entry to clear it. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

### 9.3.2 Port Forward

Use the **Port Forward** screen to forward incoming service requests to the specific servers on your local network. You may configure different servers for different service ports. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. See Section 9.20.1 on page 103 for more information.

To access this screen, click **APP MODULE** > **Firewall** > **Port Forward**.

**Figure 34** APP MODULE > Firewall > Port Forward



User List

| Host Name | IP | MAC |
|---|---|---|
| test1 | 192.168.1.103 | [redacted] |
| [redacted] | 192.168.1.100 | [redacted] |

Port Forward

It allows remote computers (for example,computers on the Internet) to connect to a specific computer or service within a private local-area network.

| ID | Config Name | MAC | Local Port | WAN Port | × |
|---|---|---|---|---|---|
| 01 | test1 | [redacted] | 21 | 80 | × |
| 02 | | | | | × |
| 03 | | | | | × |
| 04 | | | | | × |
| 05 | | | | | × |
| 06 | | | | | × |
| 07 | | | | | × |
| 08 | | | | | × |
| 09 | | | | | × |
| 10 | | | | | × |

| Config Name | Address |
|---|---|
| test1 | [redacted] |

The following table describes the labels in this screen.

Table 28 APP MODULE > Firewall > Port Forward

| LABEL | DESCRIPTION |
|---|---|
| User List | This section displays information of the NR2111's network clients. You may configure the client as the service servers. If port forwarding is enabled, incoming service requests are forwarded to the specified service server on your network. |
| Host Name | This displays the name of the service server. |
| IP | This displays the IP address of the service server. |

Table 28 APP MODULE > Firewall > Port Forward (continued)

| LABEL | DESCRIPTION |
|---|---|
| MAC | This displays the MAC address of the service server. |
| Turn the switch button on to enable port forwarding on the NR2111. This allows remote clients to connect to the service server within a private local-area network. | |
| ID | This is the index number of the entry. |
| Config Name | Enter a name for the service server. |
| MAC | Enter the MAC address of the service server. |
| Local Port | Enter the internal port number that identifies a service. |
| WAN Port | Enter the external port number that identifies a service. |
| X | Click the **X** next to an entry to clear it. |
| Apply | Click **Apply** to save your changes. A list of the configured servers displays below. |
| Return | Click this button to return to the **APP MODULE** list. |
| Config Name | This displays the name of the service server. |
| Address | This displays the IP address of the service server. |

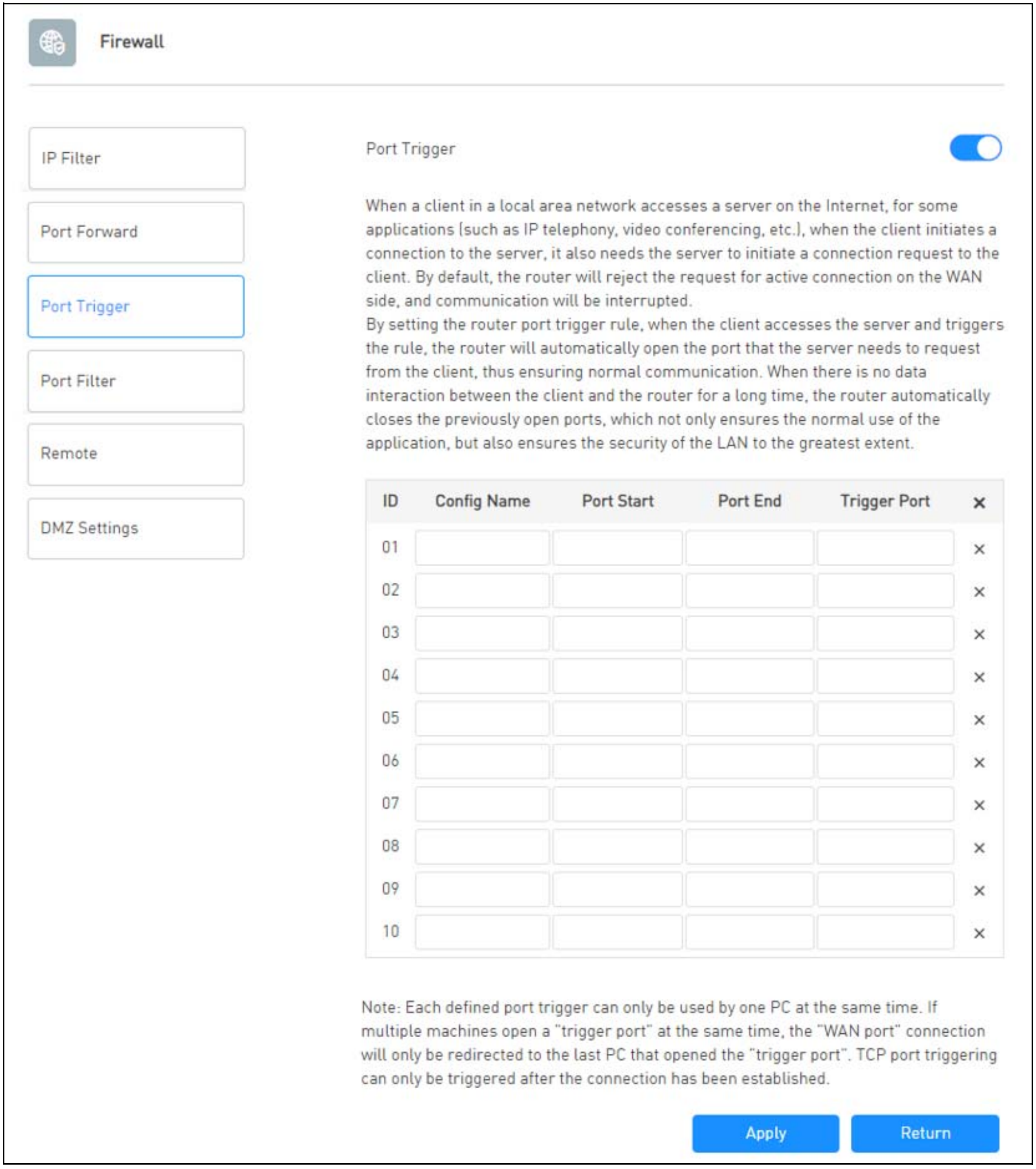
## 9.3.3 Port Trigger

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The NR2111 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number (a “trigger” port). When the NR2111's WAN port receives a response with a specific port number, the NR2111 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application. See Section 9.20.3 on page 103 for more information.

To change your NR2111’s trigger port settings, click **APP MODULE** > **Firewall** > **Port Trigger**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

**Figure 35** APP MODULE > Firewall > Port Trigger



When a client in a local area network accesses a server on the Internet, for some applications (such as IP telephony, video conferencing, etc.), when the client initiates a connection to the server, it also needs the server to initiate a connection request to the client. By default, the router will reject the request for active connection on the WAN side, and communication will be interrupted.
By setting the router port trigger rule, when the client accesses the server and triggers the rule, the router will automatically open the port that the server needs to request from the client, thus ensuring normal communication. When there is no data interaction between the client and the router for a long time, the router automatically closes the previously open ports, which not only ensures the normal use of the application, but also ensures the security of the LAN to the greatest extent.

| ID | Config Name | Port Start | Port End | Trigger Port | × |
|---|---|---|---|---|---|
| 01 | | | | | × |
| 02 | | | | | × |
| 03 | | | | | × |
| 04 | | | | | × |
| 05 | | | | | × |
| 06 | | | | | × |
| 07 | | | | | × |
| 08 | | | | | × |
| 09 | | | | | × |
| 10 | | | | | × |

Note: Each defined port trigger can only be used by one PC at the same time. If multiple machines open a "trigger port" at the same time, the "WAN port" connection will only be redirected to the last PC that opened the "trigger port". TCP port triggering can only be triggered after the connection has been established.

The following table describes the labels in this screen.

Table 29 APP MODULE > Firewall > Port Trigger

| LABEL | DESCRIPTION |
|---|---|
| Turn the switch button on ● to enable port trigger on the NR2111. | |
| ID | This is the index number of the entry. |
| Config Name | Enter a name for the port trigger rule. |
| Port Start | Enter a port number or the starting port number in a range of port numbers. |
| Port End | Enter a port number or the ending port number in a range of port numbers. |
| Trigger Port | The trigger port is a port that causes (or triggers) the NR2111 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| X | Click the **X** next to an entry to clear it. |

Table 29 APP MODULE > Firewall > Port Trigger (continued)

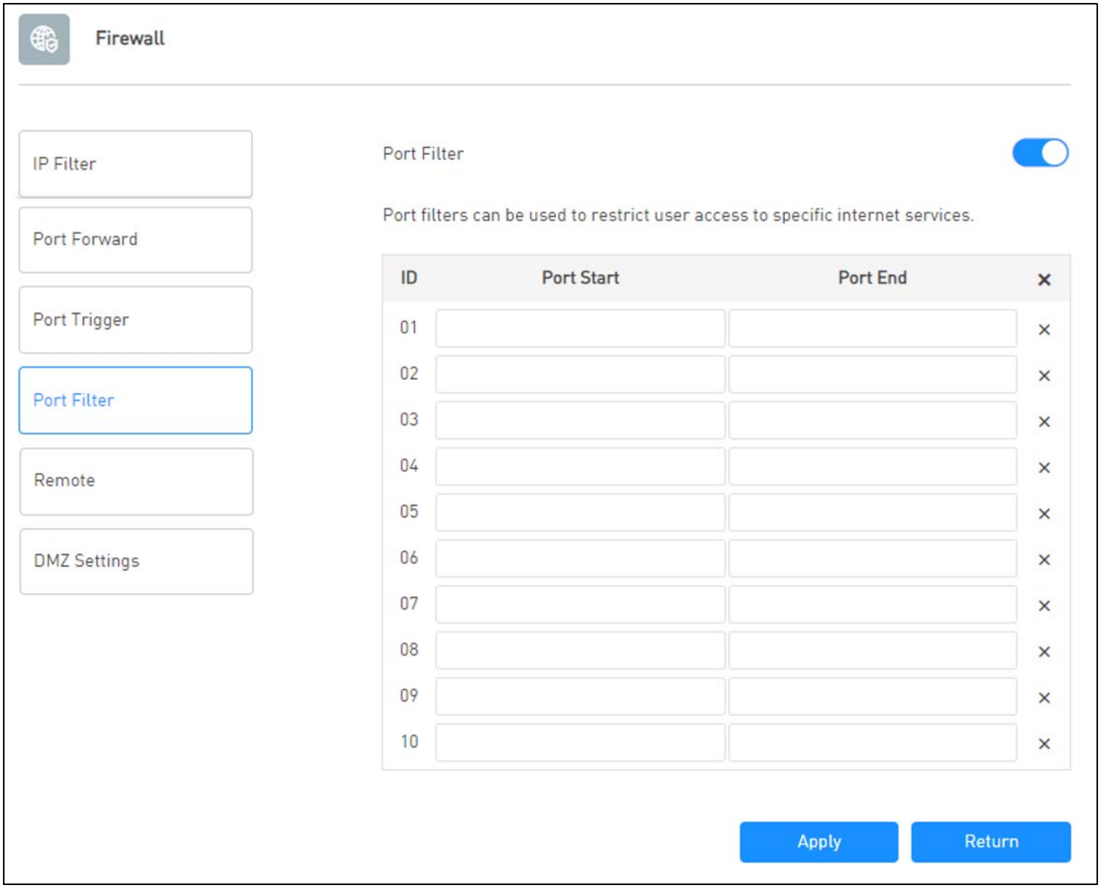
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.3.4 Port Filter

Use the **Port Filter** screen to enable and create firewall rules to block unwanted traffic.

To access this screen, click **APP MODULE** > **Firewall** > **Port Filter**.

**Figure 36** APP MODULE > Firewall > Port Filter



Port Filter

Port filters can be used to restrict user access to specific internet services.

| ID | Port Start | Port End | × |
|---|---|---|---|
| 01 | | | × |
| 02 | | | × |
| 03 | | | × |
| 04 | | | × |
| 05 | | | × |
| 06 | | | × |
| 07 | | | × |
| 08 | | | × |
| 09 | | | × |
| 10 | | | × |

The following table describes the labels in this screen.

Table 30 APP MODULE > Firewall > Port Filter

| LABEL | DESCRIPTION |
|---|---|
| Turn the switch button on ● to enable port filter on the NR2111. The port filter rules block clients from accessing specific Internet services. | |
| ID | This is the index number of the entry. |
| Port Start | Enter the beginning port number of the source that defines the traffic type. |
| Port End | Enter the ending port number of the source that defines the traffic type. |
| X | Click the **X** next to an entry to clear it. |

Table 30 APP MODULE > Firewall > Port Filter (continued)

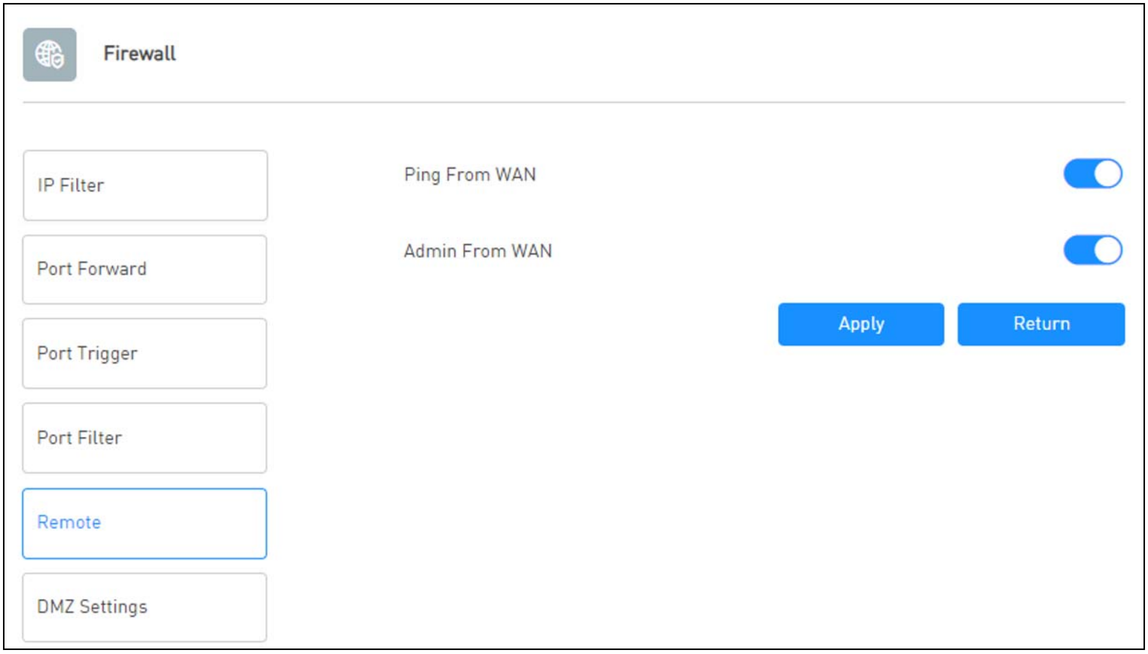
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.3.5 Remote

Use the **Remote** screen to allow or forbid WAN users from pinging or configuring the NR2111.

To access this screen, click **APP MODULE** > **Firewall** > **Remote**.

**Figure 37** APP MODULE > Firewall > Remote



The following table describes the labels in this screen.

Table 31 APP MODULE > Firewall > Remote

| LABEL | DESCRIPTION |
|---|---|
| Ping From WAN | Turn the switch button on ● to allow WAN users to ping the NR2111. |
| Admin From WAN | Turn the switch button on ● to allow WAN users to access the NR2111's Web Configurator. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

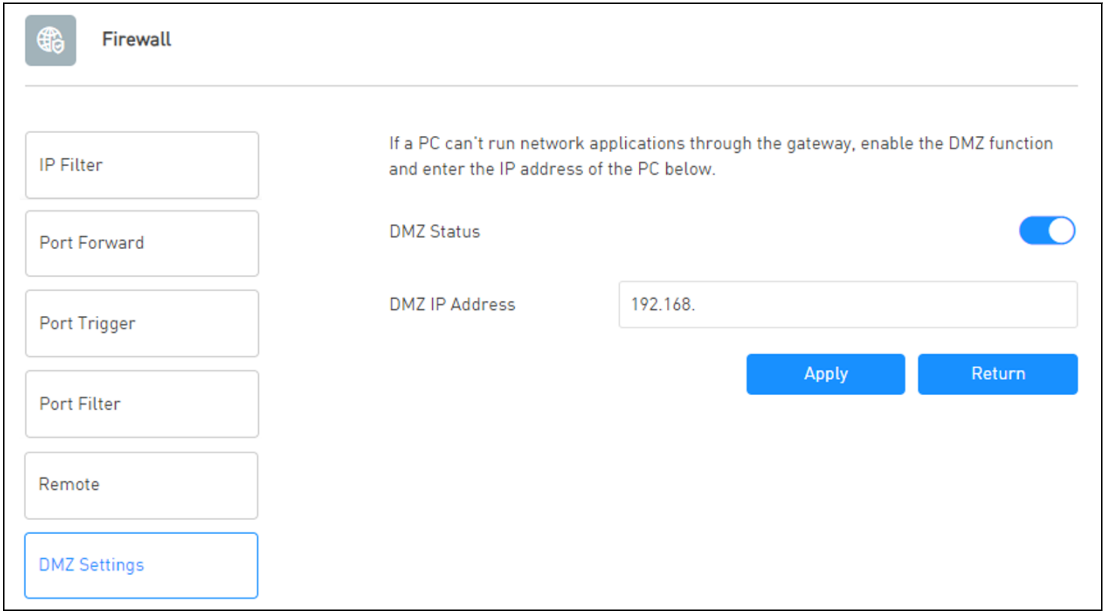
## 9.3.6 DMZ Settings

A client in the Demilitarized Zone (DMZ) is no longer behind the NR2111 and therefore can run any Internet applications such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the NR2111.

Use the **DMZ Settings** screen to enable DMZ on the NR2111.

To access this screen, click **APP MODULE** > **Firewall** > **DMZ Settings**.

**Figure 38** APP MODULE > Firewall > DMZ Settings



If a PC can't run network applications through the gateway, enable the DMZ function and enter the IP address of the PC below.

DMZ Status ●

DMZ IP Address: 192.168.

The following table describes the labels in this screen.

Table 32 APP MODULE > Firewall > DMZ Settings

| LABEL | DESCRIPTION |
|---|---|
| DMZ Status | Turn the switch button on ● to enable DMZ on the NR2111. |
| DMZ IP Address | Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen.<br>Note: If you do not assign the DMZ IP Address, the NR2111 discards all packets received for ports that are not specified in the **Port Forwarding** screen. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.4 Messages

SMS (Short Message Service) allows you to receive, view, and send text messages.

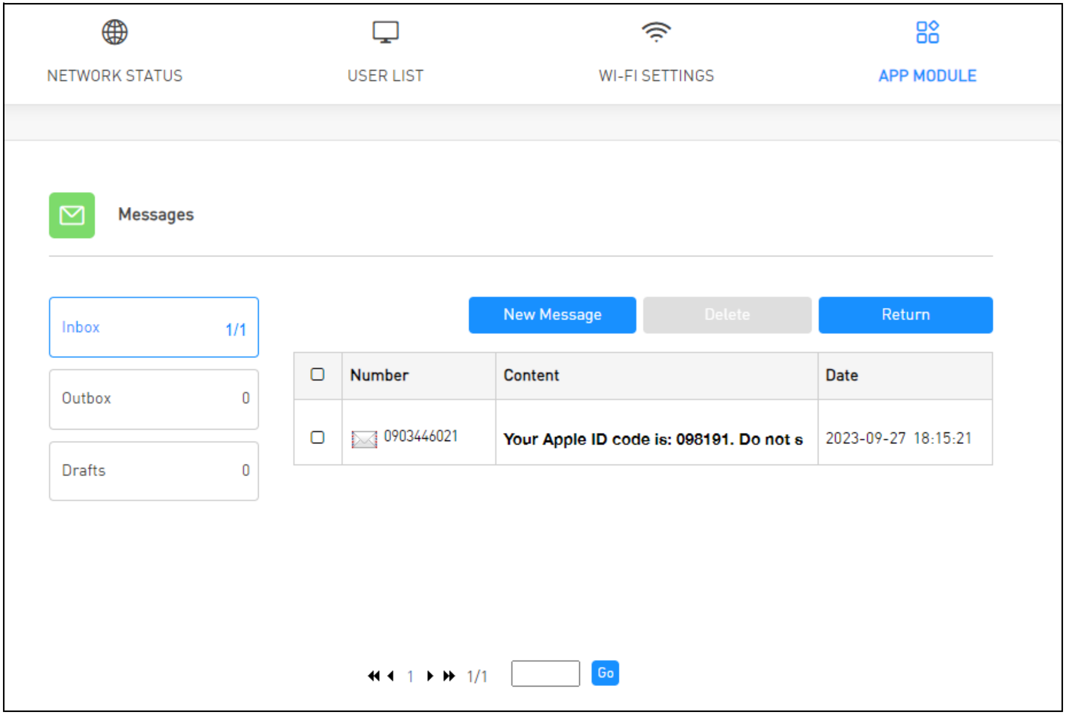
Use the **Messages** screens to view and manage SMS messages on the NR2111.

To access this screen, click **APP MODULE** > **Messages**.

Note: You can store an approximate total of 500 messages, which includes Inbox, Outbox, and Draft box altogether.

## 9.4.1 Inbox

Use this screen to view messages received by the NR2111. To access this screen, click **APP MODULE** > **Messages** > **Inbox**.



| □ | Number | Content | Date |
|---|---|---|---|
| □ | 0903446021 | Your Apple ID code is: 098191. Do not s | 2023-09-27 18:15:21 |

**Figure 39** APP MODULE > Messages > Inbox

The following table describes the labels in this screen.

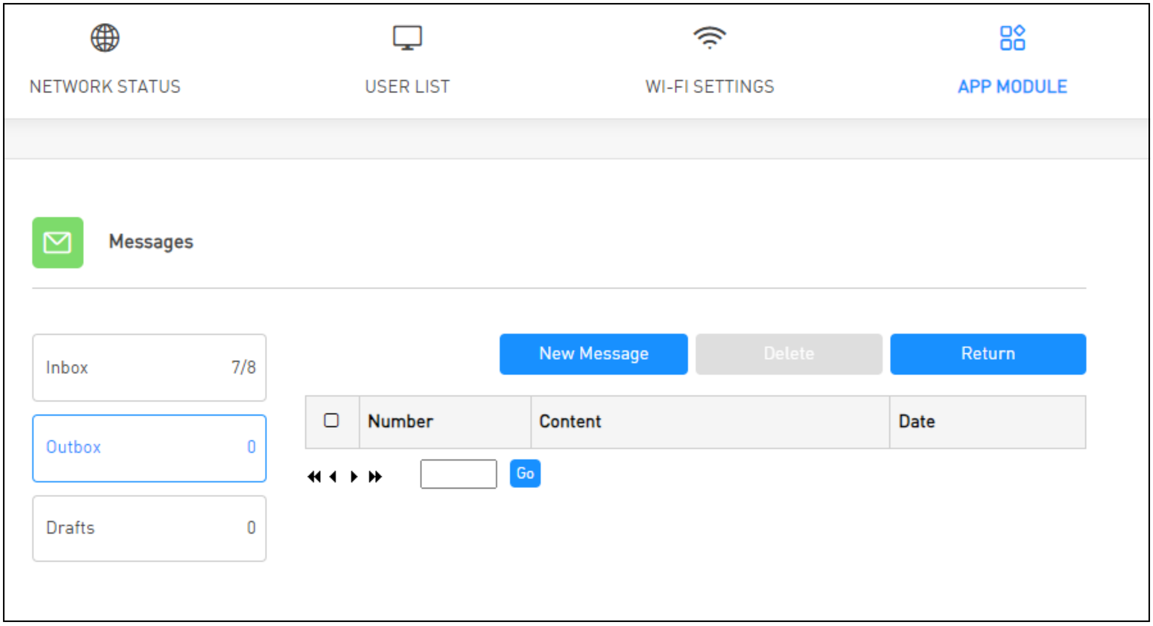
Table 33 APP MODULE > Messages > Inbox

| LABEL | DESCRIPTION |
|---|---|
| New Message | Click this button to send messages using the NR2111. See Section 9.4.4 on page 87 for more information. |
| Delete | Select a message you want to remove to click **Delete** to remove it. |
| Return | Click this button to return to the **APP MODULE** list. |
| Number | This field displays the phone number that sent the message. |
| Content | This field displays the content of the message. |
| Date | This field displays the date and time the message was received. |

## 9.4.2 Outbox

Use this screen to view messages sent from the NR2111. To access this screen, click **APP MODULE** > **Messages** > **Outbox**.

**Figure 40** APP MODULE > Messages > Outbox



The following table describes the labels in this screen.

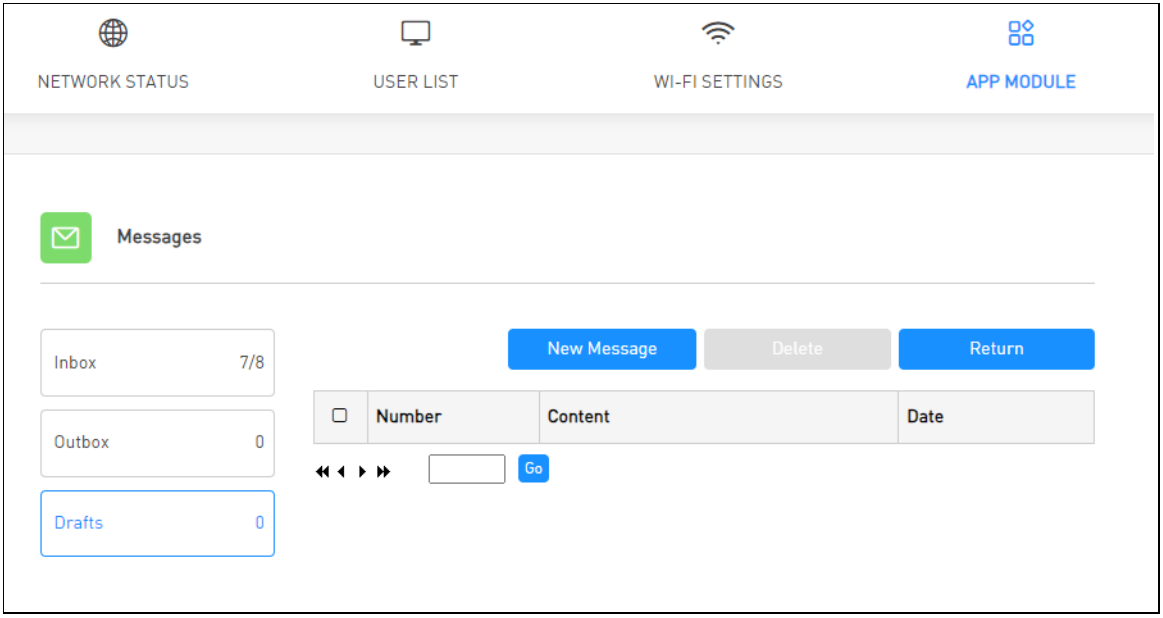
Table 34 APP MODULE > Messages > Outbox

| LABEL | DESCRIPTION |
|---|---|
| New Message | Click this button to send messages using the NR2111. See Section 9.4.4 on page 87 for more information. |
| Delete | Select a message you want to remove and click **Delete** to remove it. |
| Return | Click this button to return to the **APP MODULE** list. |
| Number | This field displays the phone number the message was sent to. |
| Content | This field displays the content of the message. |
| Date | This field displays the date and time the message was sent. |

## 9.4.3 Drafts

Use this screen to view messages not yet sent from the NR2111. To access this screen, click **APP MODULE** > **Messages** > **Drafts**.

**Figure 41** APP MODULE > Messages > Drafts



The following table describes the labels in this screen.

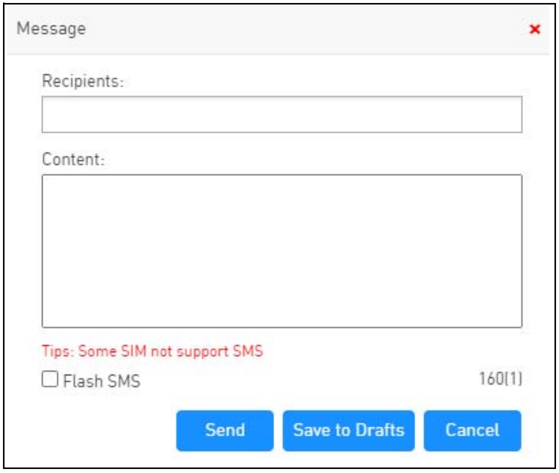
Table 35 APP MODULE > Messages > Drafts

| LABEL | DESCRIPTION |
|---|---|
| New Message | Click this button to send messages using the NR2111. See Section 9.4.4 on page 87 for more information. |
| Delete | Select a message you want to remove and click **Delete** to remove it. |
| Return | Click this button to return to the **APP MODULE** list. |
| Number | This field displays the phone number the message is to be sent to. |
| Content | This field displays the content of the message. |
| Date | This field displays the date and time the message was last modified. |

## 9.4.4 New Messages

Use this screen to send messages using the NR2111. To access this screen, click the **New Messages** button in the **Messages** screen.

**Figure 42** APP MODULE > Messages: New Messages



Message ×

Recipients:

Content:

Tips: Some SIM not support SMS

□ Flash SMS 160(1)

The following table describes the labels in this screen.

Table 36 APP MODULE > Messages: New Messages

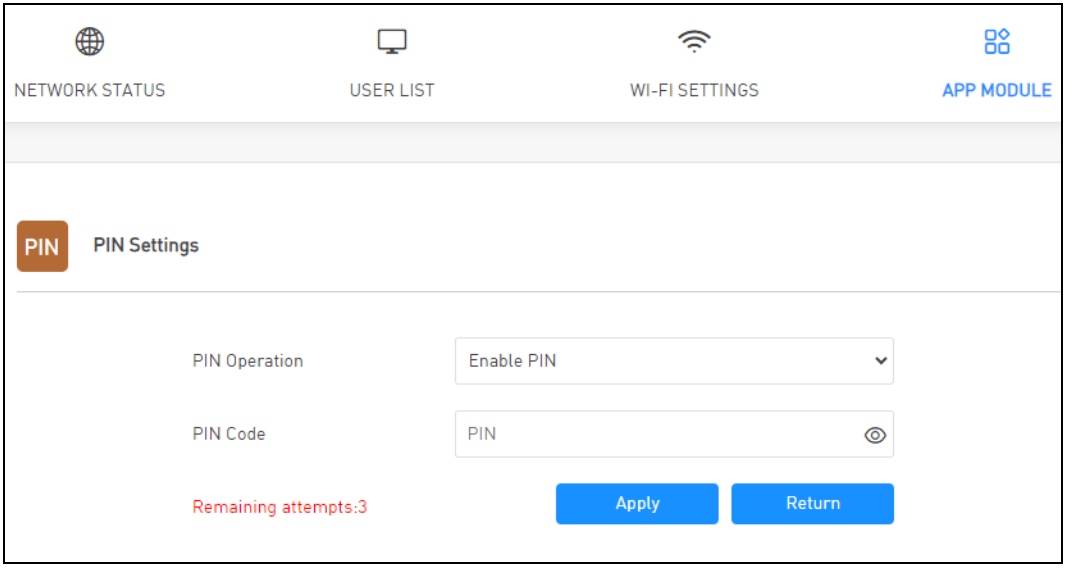
| LABEL | DESCRIPTION |
|---|---|
| Recipients | Enter the phone number to which to send the message. Press **Enter** on your keyboard if you want to add another phone number. You can add up to 5 phone numbers. |
| Content | Enter the message content. You can send up to 160 characters in one message. If the message exceeds 160 characters, more than one SMS will be sent. |
| Flash SMS | If you want to display the message as a flash message for the receiver, select the checkbox. Flash SMS is a special type of text message that displays immediately on the mobile phone screen without the user having to take any action to read it. |
| Send | Click this to send the message. |
| Save to Drafts | Click this to store the message as a draft. |
| Cancel | Click this to cancel the message and return to the **Messages** screen. |

## 9.5 PIN Settings

Use the **PIN Settings** screens to enable PIN code authentication on the NR2111.

To access this screen, click **APP MODULE** > **PIN Settings**.

**Figure 43** APP MODULE > PIN Settings



PIN Operation: Enable PIN

PIN Code: PIN

Remaining attempts:3

The following table describes the labels in this screen.

Table 37 APP MODULE > PIN Settings

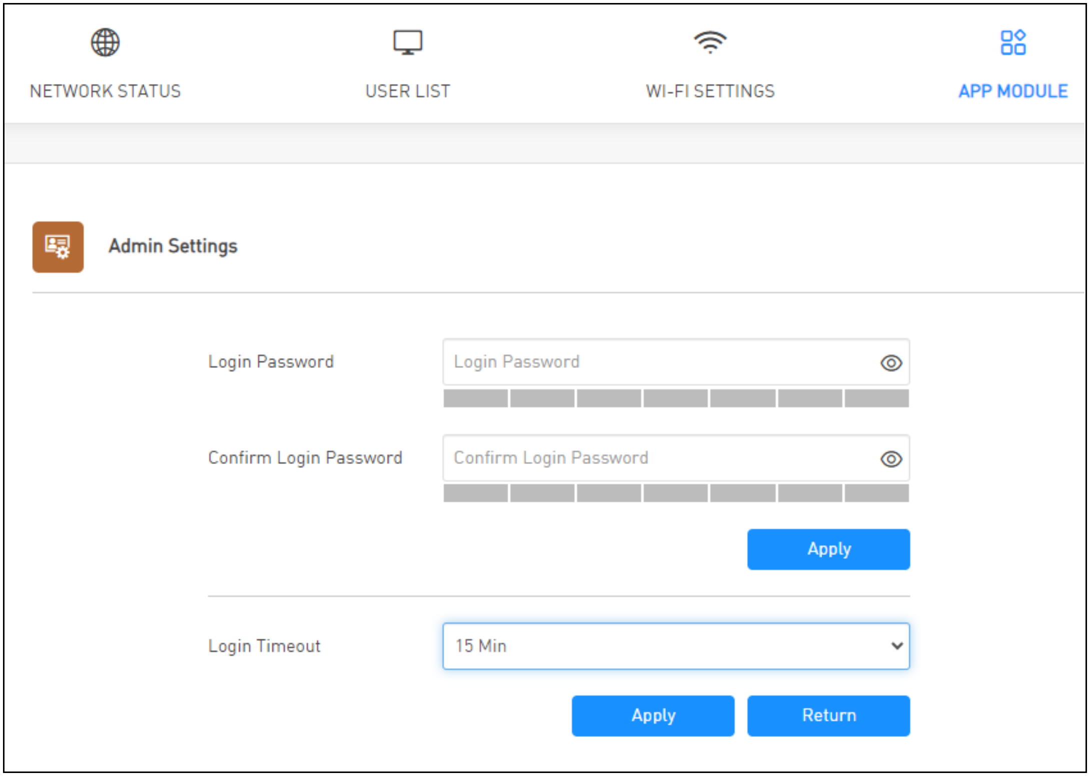
| LABEL | DESCRIPTION |
|---|---|
| PIN Operation | This displays **Enable PIN** so that PIN code authentication is enabled. You need to enter the PIN code every time the NR2111 reboots. |
| PIN Code | Enter a 4-digit PIN code (0000 for example) provided by your ISP for the inserted SIM card. If you have entered the wrong PIN code 3 times, the PIN card will be locked. You will need the PUK code that comes with the SIM card. If you cannot find the PUK code, contact your ISP. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

# 9.6 Admin Settings

Use the **Admin Settings** screens to change the NR2111's system password and time-out setting. It is strongly recommended that you change your NR2111's system password.

To access this screen, click **APP MODULE** > **Admin Settings**.

**Figure 44** APP MODULE > Admin Settings



Login Password: Login Password

Confirm Login Password: Confirm Login Password

Login Timeout: 15 Min

The following table describes the labels in this screen.

Table 38 APP MODULE > Admin Settings

| LABEL | DESCRIPTION |
|---|---|
| Login Password | Enter your new system password of between 4 and 24 characters. The strength of your password is displayed below. Use long and complex passwords that are harder to crack to increase the password strength. |
| Confirm Login Password | Enter the new password again in this field. |
| Login Timeout | Select how many minutes a management session can be left idle before the session times out. After it times out you have to log in with your password again. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

# 9.7 Update

Use the **Update** screens to upload new firmware to your NR2111. You can download new firmware releases or check for new firmware online to use to upgrade your NR2111's performance.

**Only use firmware for your device's specific model.**

## 9.7.1 Online Update

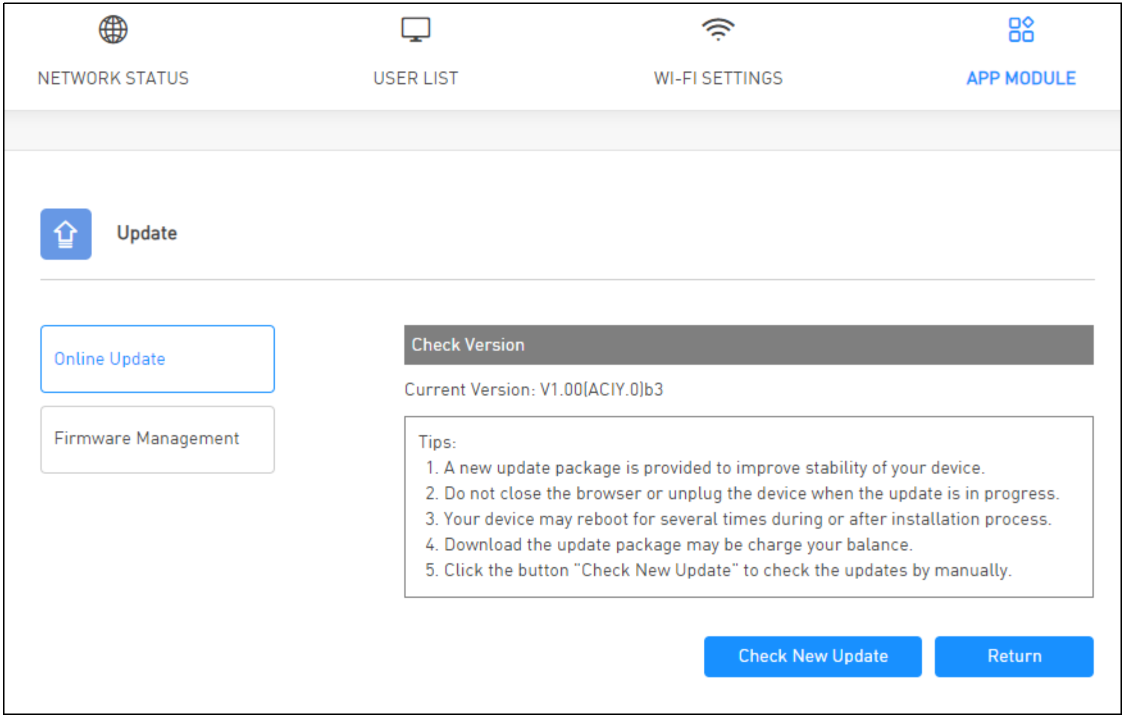
Firmware Over the Air (FOTA) allows for timely and automatic firmware upgrades. By default, FOTA is enabled on the NR2111 and it checks for firmware updates automatically. It will do so each time it is turned on and connected to the Internet. You can disable it in the NR2111's LCD screen. See Section 1.6 on page 14 for more information.

Use the **Online Update** screen to manually check for new firmware online. To access this screen, click **APP MODULE** > **Update** > **Online Update**. The current firmware version is displayed. Click the **Check New Update** button to see if any update is available. Make sure your NR2111 is connected to the Internet. Click **Return** to return to the **APP MODULE** list.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take several minutes. After a successful upload, the system will reboot.

**Do NOT turn off the NR2111 while firmware upload is in progress!**

**Figure 45** APP MODULE > Update > Online Update



Current Version: V1.00(ACIY.0)b3

Tips:
1. A new update package is provided to improve stability of your device.
2. Do not close the browser or unplug the device when the update is in progress.
3. Your device may reboot for several times during or after installation process.
4. Download the update package may be charge your balance.
5. Click the button "Check New Update" to check the updates by manually.

## 9.7.2 Firmware Management

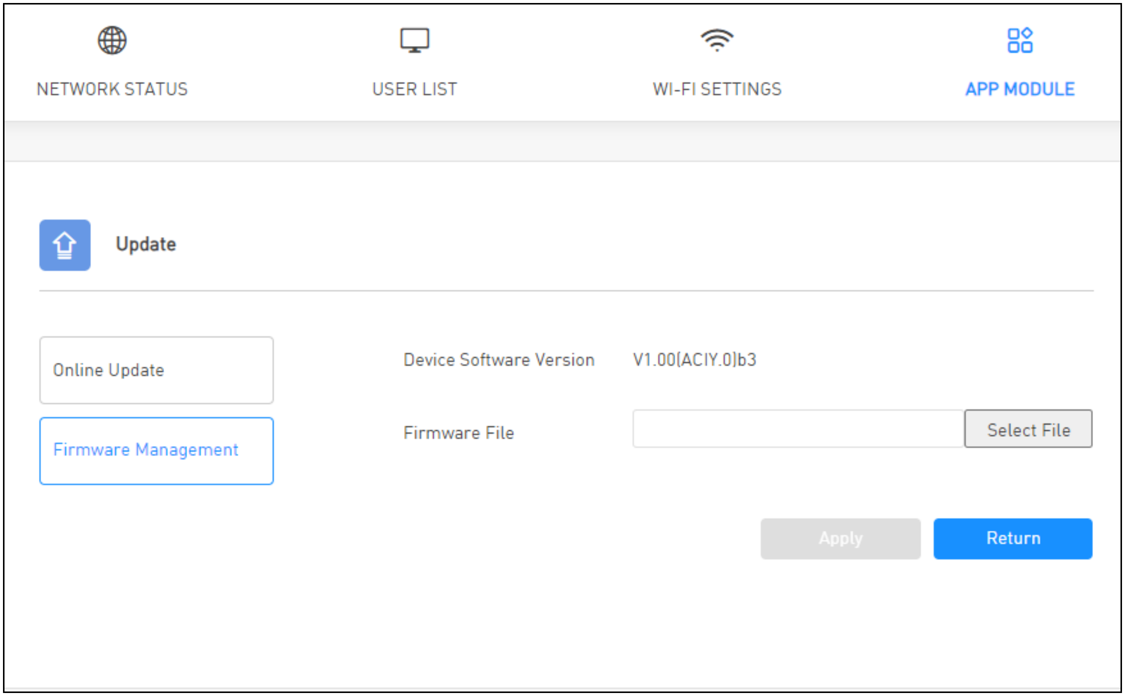
The **Firmware Management** screen allows you to upload new firmware to your NR2111. You can download new firmware releases from the download library at the Zyxel website (*www.zyxel.com*) to use to upgrade your NR2111's performance.

To access this screen, click **APP MODULE** > **Update** > **Firmware Management**. The current firmware version is displayed. Click **Select File** to find the location of the file. Remember that you must decompress compressed (.ZIP) files before you can upload them. Click **Apply** to begin the upload process.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. Click **Return** to return to the **APP MODULE** list.

**Do NOT turn off the NR2111 while firmware upload is in progress!**

**Figure 46** APP MODULE > Update > Firmware Management



Device Software Version V1.00(ACIY.0)b3

Firmware File

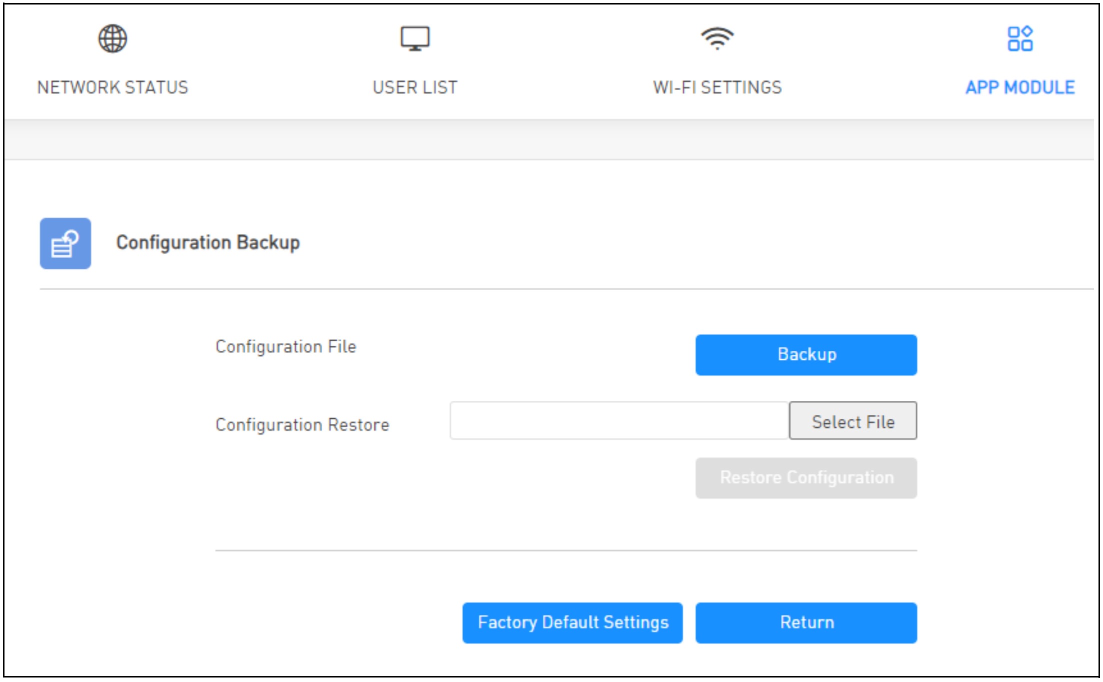
## 9.8 Configuration Backup

Backup configuration allows you to back up (save) the NR2111's current configuration to a file with a "bin" extension on your computer. Once your NR2111 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NR2111.

Click **APP MODULE** > **Configuration Backup** to display the following screen.

**Figure 47** APP MODULE > Configuration Backup



The following table describes the labels in this screen.

Table 39 APP MODULE > Configuration Backup

| LABEL | DESCRIPTION |
|---|---|
| Configuration File | Click **Backup** to save the NR2111's current configuration file with a ".bin" extension to your computer. |
| Configuration Restore | |
| Select File | Click **Select File** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.<br>Note: Do not turn off the NR2111 while configuration file upload is in progress.<br>The NR2111 automatically restarts in this time causing a temporary network disconnect. |
| Factory Default Settings | Press this button to clear all user-entered configuration information and returns the NR2111 to its factory defaults.<br>You can also press the **RESET** button to reset the factory defaults of your NR2111. See Section 1.5.3 on page 13 for more information on the **RESET** button. |
| Return | Click this button to return to the **APP MODULE** list. |

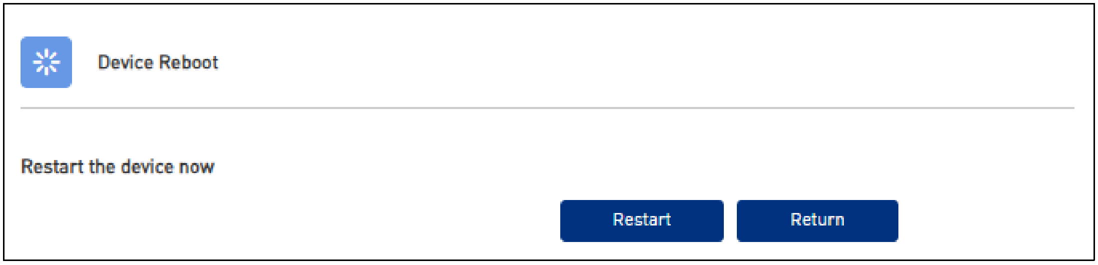
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NR2111 IP address (192.168.1.1).

## 9.9 Device Reboot

Use the **Device Reboot** screen to restart the NR2111. System restart allows you to reboot the NR2111 without turning the power off. Click **Reboot** to restart the NR2111. Wait a few minutes until the login screen appears. If the login screen does not appear, enter the IP address of the NR2111 in your Web browser.

To access this screen, click **APP MODULE** > **Device Reboot**.

**Figure 48** APP MODULE > Device Reboot



Restart the device now

The following table describes the labels in this screen.

Table 40 APP MODULE > Device Reboot

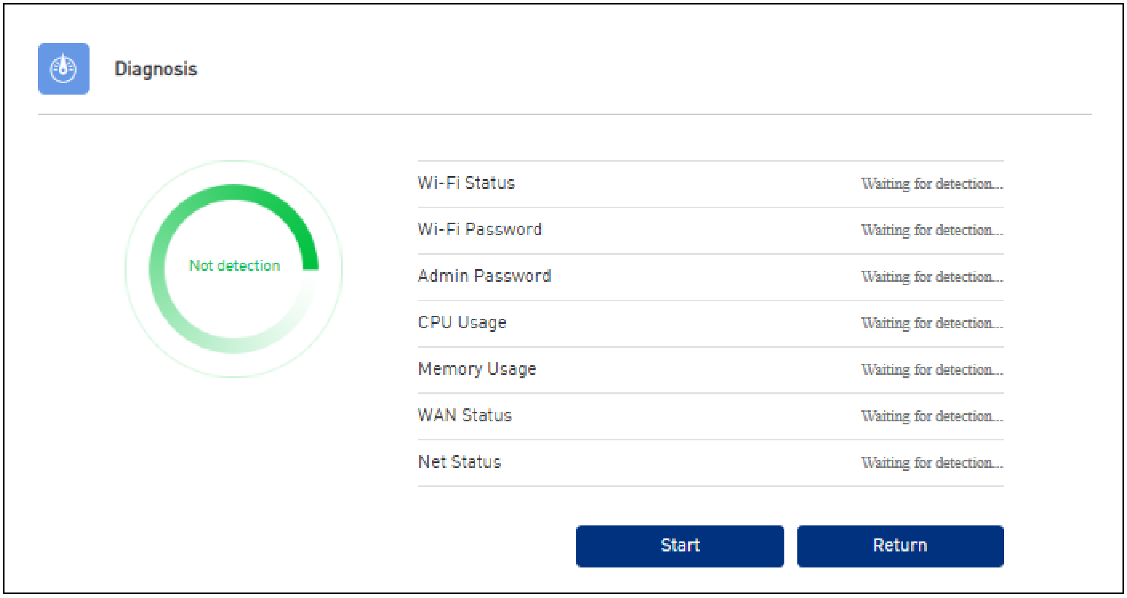
| LABEL | DESCRIPTION |
|---|---|
| Restart | Click this button to reboot the NR2111. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.10 Diagnosis

Use the **Diagnosis** screen to check the Wi-Fi and status of the NR2111. Click the **Start** button to begin diagnosing. You can check the results displayed in the screen and make changes in the NR2111's settings accordingly. Click **Rediagnosis** to diagnose the NR2111 again or **Return** to return to the **APP MODULE** list.

To access this screen, click **APP MODULE** > **Diagnosis**.

**Figure 49** APP MODULE > Diagnosis



Wi-Fi Status Waiting for detection...

Wi-Fi Password Waiting for detection...

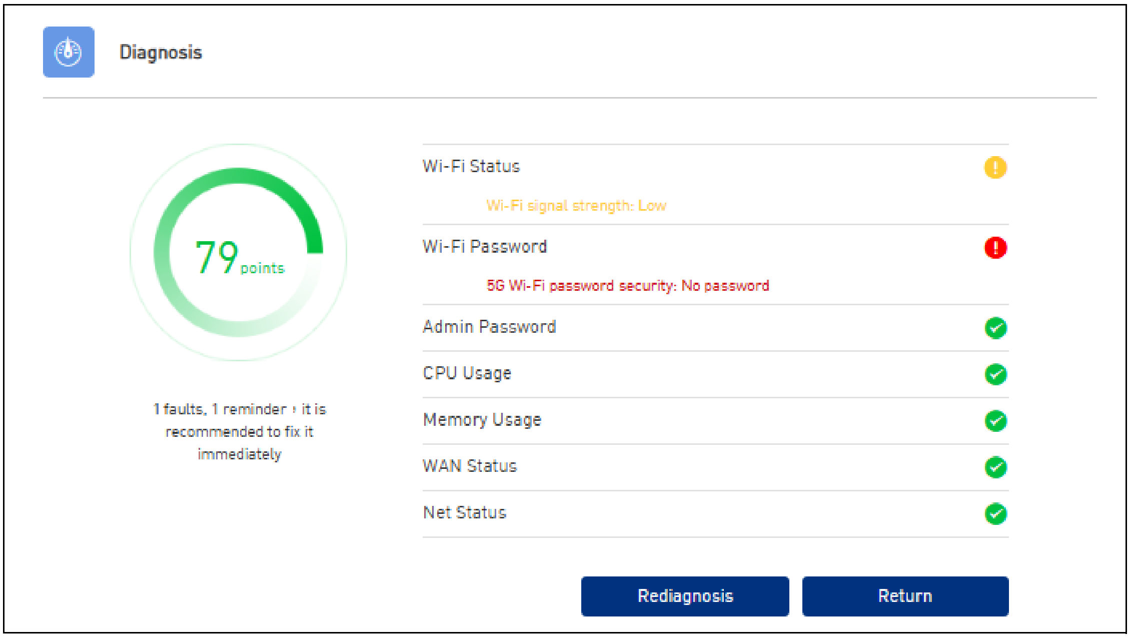
Admin Password Waiting for detection...

CPU Usage Waiting for detection...

Memory Usage Waiting for detection...

WAN Status Waiting for detection...

Net Status Waiting for detection...



Diagnosis

79 points

1 faults, 1 reminder，it is recommended to fix it immediately

Wi-Fi Status !
Wi-Fi signal strength: Low

Wi-Fi Password !
5G Wi-Fi password security: No password

Admin Password ✓

CPU Usage ✓

Memory Usage ✓

WAN Status ✓

Net Status ✓

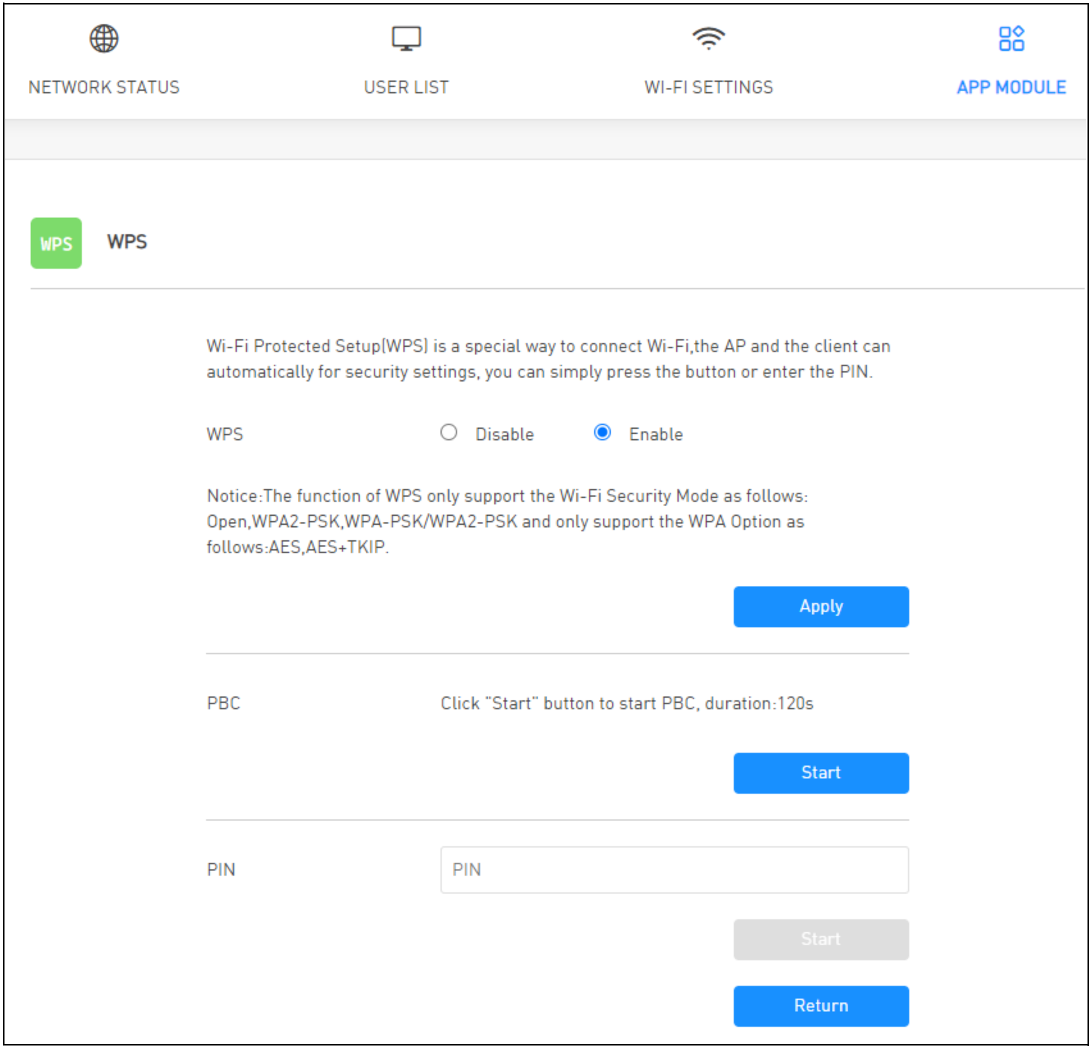
## 9.11 WPS

Wi-Fi Protected Setup (WPS) allows you to quickly set up a wireless network with security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it. See Section 9.20.9.3 on page 109 for more information about WPS.

Note: The NR2111 applies the security settings of the SSID profile (see Section 6.2 on page 55).

Click **APP MODULE** > **WPS** to display the following screen.

**Figure 50** APP MODULE > WPS



Wi-Fi Protected Setup(WPS) is a special way to connect Wi-Fi,the AP and the client can automatically for security settings, you can simply press the button or enter the PIN.

WPS ○ Disable ● Enable

Notice:The function of WPS only support the Wi-Fi Security Mode as follows: Open,WPA2-PSK,WPA-PSK/WPA2-PSK and only support the WPA Option as follows:AES,AES+TKIP.

PBC Click "Start" button to start PBC, duration:120s

PIN PIN

The following table describes the labels in this screen.

Table 41 APP MODULE > WPS

| LABEL | DESCRIPTION |
|---|---|
| WPS | Turn the switch button on ● to enable WPS on the NR2111. |
| Apply | Click **Apply** to save your changes. |
| PCB | Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Click **Start** and add another WPS-enabled wireless device (within wireless range of the NR2111) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen.<br>Note: You must press the other wireless device's WPS button within two minutes of pressing this button. |

Table 41 APP MODULE > WPS (continued)

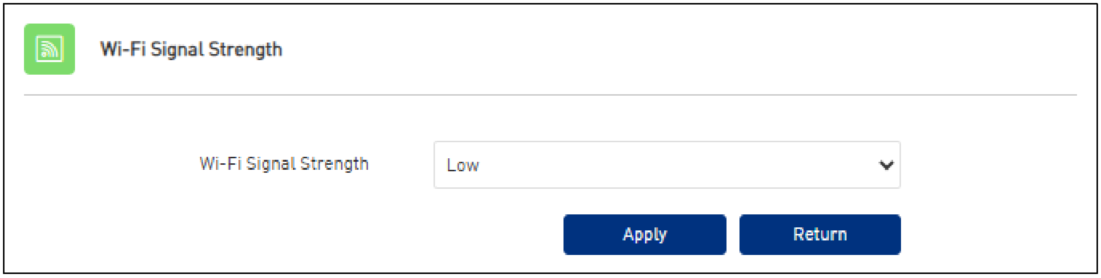
| LABEL | DESCRIPTION |
|---|---|
| PIN | Use this section to set up a WPS wireless network by using the PIN of the client. Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network.<br>You can find the PIN by checking the device's settings.<br>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the NR2111. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.12 Wi-Fi Signal Strength

Use this screen to adjust your NR2111's Wi-Fi signal. Wi-Fi Signal refers to the transmission power of the Wi-Fi. A lower Wi-Fi signal results in lower power and a shorter transmission range. You can adjust the Wi-Fi signal to save battery power.

To adjust your NR2111's Wi-Fi signal, click **APP MODULE** > **Wi-Fi Signal Strength**. The screen appears as shown.

**Figure 51** APP MODULE > Wi-Fi Signal Strength



Wi-Fi Signal Strength

Wi-Fi Signal Strength: Low

The following table describes the labels in this screen.

Table 42 APP MODULE > Wi-Fi Signal Strength

| LABEL | DESCRIPTION |
|---|---|
| Wi-Fi Signal Strength | Select **Low** to reduce the NR2111's Wi-Fi signal. You can reduce the Wi-Fi signal strength when client devices are in a small area, such as a hotel room. Otherwise, select **Normal**. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

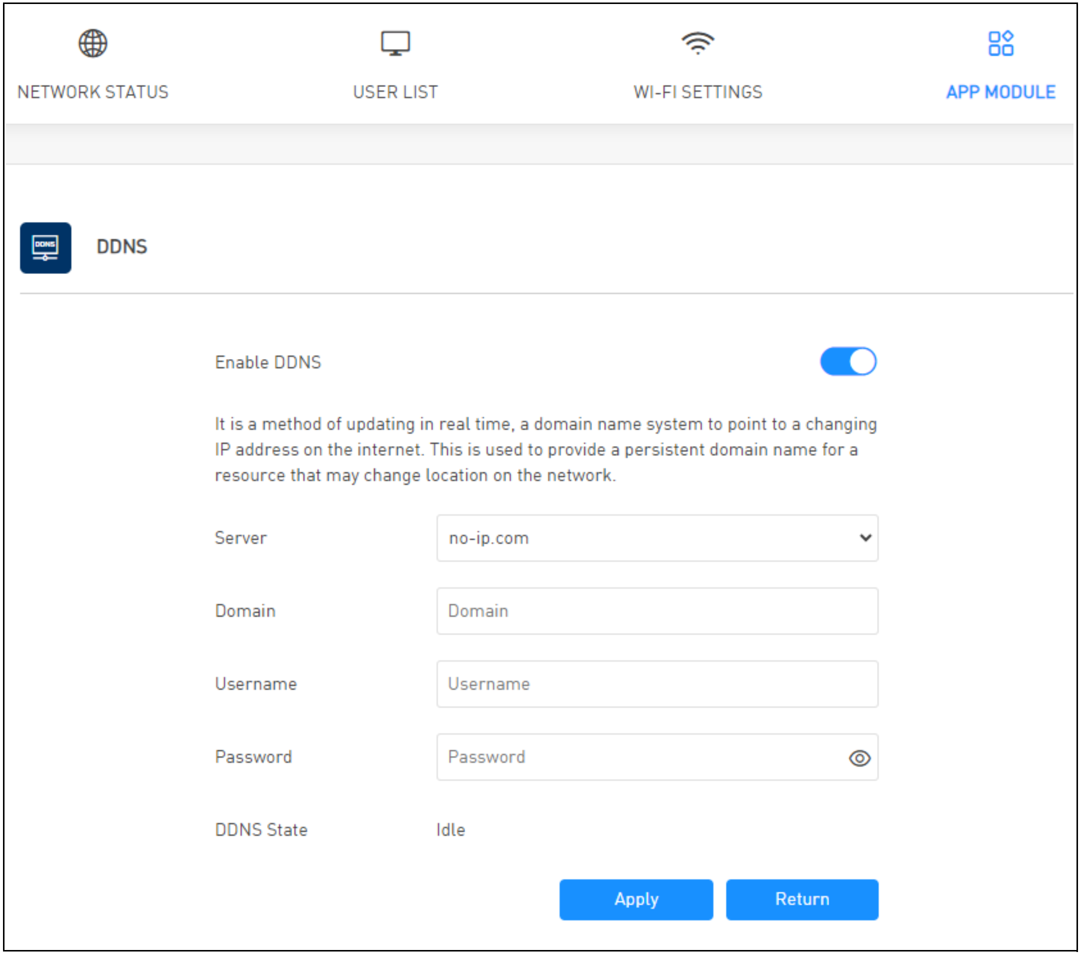
## 9.13 DDNS

Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NR2111 or a server in your network.

Note: The NR2111 must have a public global IP address and you should have your registered DDNS account information on hand.

To change your NR2111's DDNS, click **APP MODULE** > **DDNS**. The screen appears as shown.

**Figure 52** APP MODULE > DDNS



Enable DDNS

It is a method of updating in real time, a domain name system to point to a changing IP address on the internet. This is used to provide a persistent domain name for a resource that may change location on the network.

Server: no-ip.com

Domain: Domain

Username: Username

Password: Password

DDNS State: Idle

The following table describes the labels in this screen.

Table 43 APP MODULE > DDNS

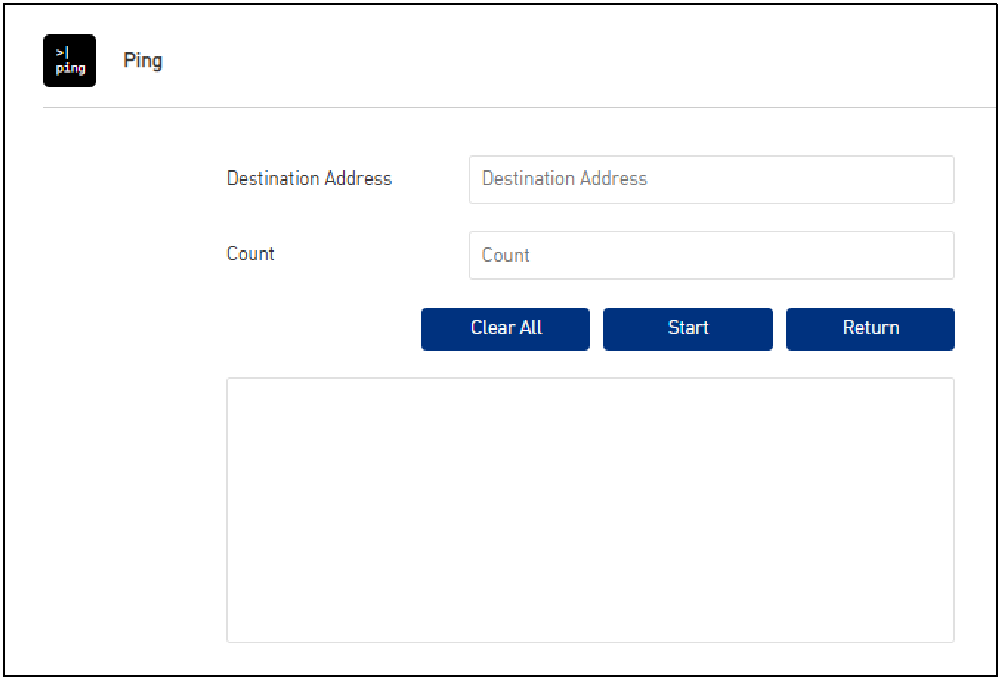
| LABEL | DESCRIPTION |
|---|---|
| DDNS | Turn the switch button on ● to enable Dynamic DNS on the NR2111. |
| Server | Select the name of your Dynamic DNS service provider. |
| Domain | Enter the domain of your Dynamic DNS service provider. |
| Username | Enter your user name. |
| Password | Enter the password assigned to you. |
| DDNS State | This displays the current DDNS status. |
| Apply | Click **Apply** to save your changes |
| Return | Click this button to return to the **APP MODULE** list. |

# 9.14 Ping

Ping is a simple network tool used to test if the NR2111 is reachable across a network or the Internet. It also measure the response time between the NR2111 and the target.

To check the connection between your NR2111's and another server, click **APP MODULE** > **Ping**. The screen appears as shown.

**Figure 53** APP MODULE > Ping



The following table describes the labels in this screen.

Table 44 APP MODULE > Ping

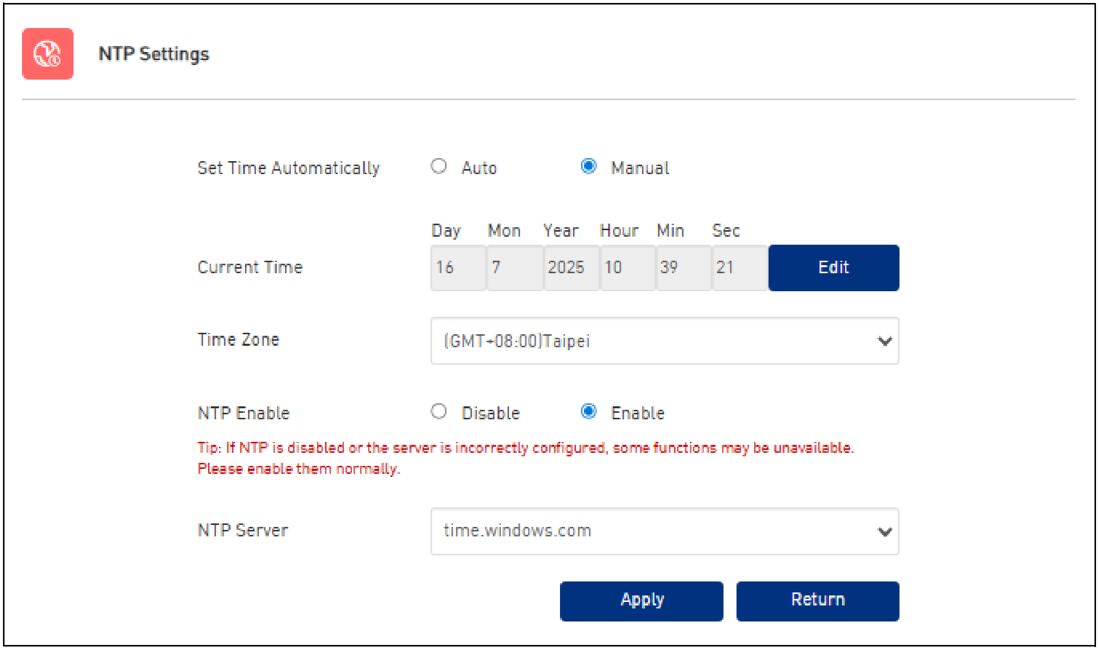
| LABEL | DESCRIPTION |
|---|---|
| Destination Address | Enter the IP address of the target device or server to check the connection. |
| Count | Enter the number of ping packets that are sent to a target device or server. Set a count can limit the number of packets sent, instead of sending continuous pings. |
| Clear All | Click **Clear All** to clear the ping result. |
| Start | Click **Start** to start the ping process. The result displays in the field below. |
| Return | Click this button to return to the **APP MODULE** list. |

# 9.15 NTP Settings

Use this screen to configure the NR2111 time settings. For effective scheduling and logging, the NR2111 system time must be accurate. You can set the time manually or get the current date and time from an NTP (Network Time Protocol) server. An NTP server is a time server that uses the NTP protocol to provide accurate time information to devices on a network.

To configure your NR2111's NTP, click **APP MODULE** > **NTP Settings**. The screen appears as shown.

**Figure 54** APP MODULE > NTP Settings



NTP Settings

Set Time Automatically ○ Auto ● Manual

Current Time: Day 16, Mon 7, Year 2025, Hour 10, Min 39, Sec 21 — Edit

Time Zone: (GMT+08:00)Taipei

NTP Enable ○ Disable ● Enable

Tip: If NTP is disabled or the server is incorrectly configured, some functions may be unavailable. Please enable them normally.

NTP Server: time.windows.com

The following table describes the labels in this screen.

Table 45 APP MODULE > NTP Settings

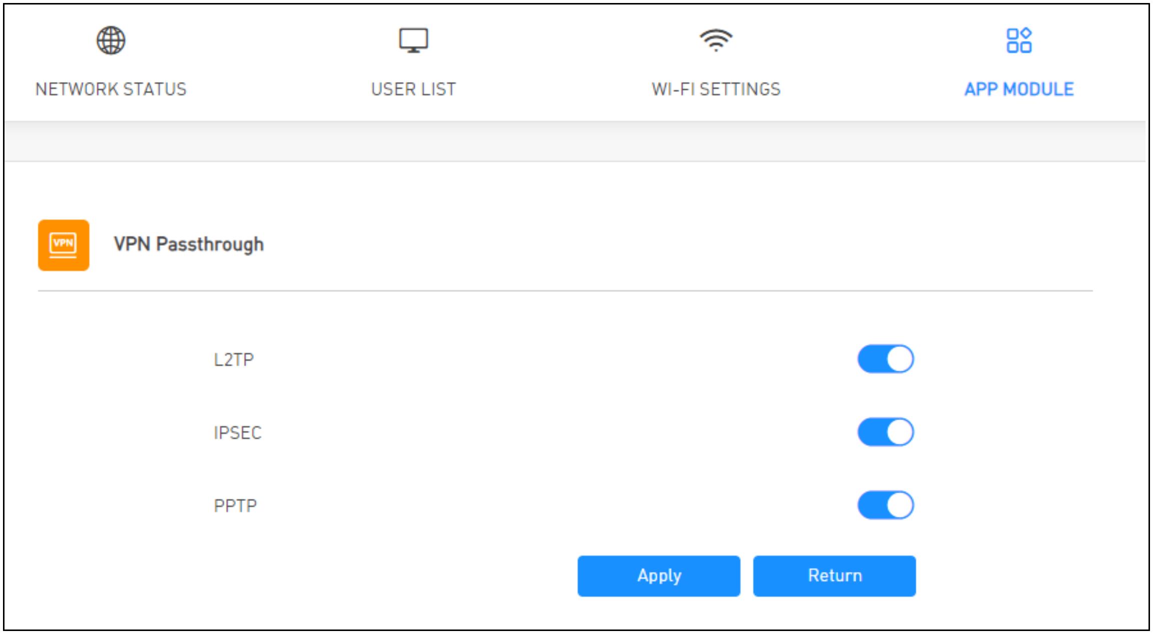
| LABEL | DESCRIPTION |
|---|---|
| Set Time Automatically | Select **Auto** to allow the NR2111 to obtain the date and time from the NTP server specified below. The NR2111 will synchronize automatically with the selected NTP server.<br>Select **Manual** to set the date and time manually using the **Current Time** field. The NR2111 will use the date and time you enter when there is no Internet access. |
| Current time | This displays the time when you open or refresh this screen. |
| Edit | If you select **Manual** under **Set Time Automatically**, click **Edit** to manually enter the date and time.<br>Note: NTP takes priority once it becomes available. If NTP is enabled, the manually entered date and time will not be saved after clicking **Apply**. |
| Time Zone | Select your time zone with the time difference in GMT (Greenwich Mean Time) from the drop-down list. This will set the time difference between your time zone and GMT. |
| NTP Enable | Select **Enable** or **Disable** to synchronize the NR2111's date and time with the configured NTP server. NTP ensures accurate and automatic timekeeping. It is recommended to enable NTP to avoid abnormal system behavior. |
| NTP Server | Select an NTP server from the drop-down list. To use a custom server, select **User Define** and the IPv4/IPv6 address or domain name of your time server. |
| Apply | Click **Apply** to save your changes. |
| Return | Click this button to return to the **APP MODULE** list. |

## 9.16 VPN Passthrough

Use the **VPN Passthrough** screen to allow VPN traffic including the L2TP, IPSec, and PPTP network protocols to operate through the NR2111. See Section 9.20.6 on page 105 for more information.

Click **APP MODULE** > **VPN Passthrough** to display the following screen. Turn the switch button on ● to enable **L2TP**, **IPSEC**, and **PPTP**. Then click **Apply** to save your changes. Click the **Return** button to return to the **APP MODULE** list.

**Figure 55** APP MODULE > VPN Passthrough



VPN Passthrough

L2TP ●

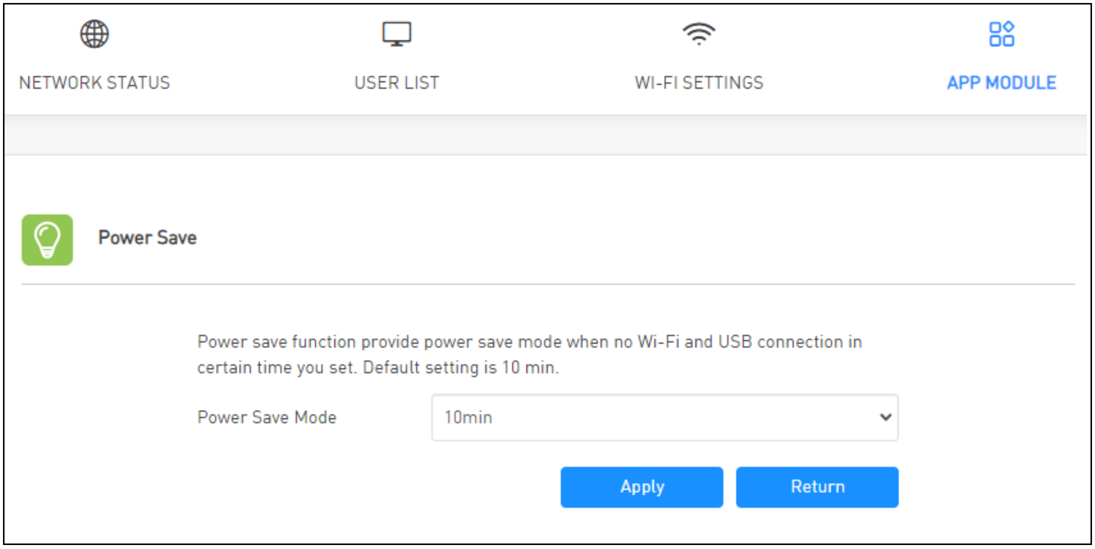
IPSEC ●

PPTP ●

## 9.17 Power Save

Use the **Power Save** screen to enable and configure the power saving settings in the NR2111.
Click **APP MODULE** > **Power Save** to display the following screen.
Select the number of minutes after which the NR2111 activates power saving and enters sleep mode. In **Power Saving** the NR2111 turns off its Wi-Fi connections to save battery power when the USB port is not connected, and there are no Wi-Fi clients associating with the NR2111. Then click **Apply** to save your changes. Click the **Return** button to return to the **APP MODULE** list.

**Figure 56** APP MODULE > Power Save



Power Save

Power save function provide power save mode when no Wi-Fi and USB connection in certain time you set. Default setting is 10 min.

Power Save Mode: 10min

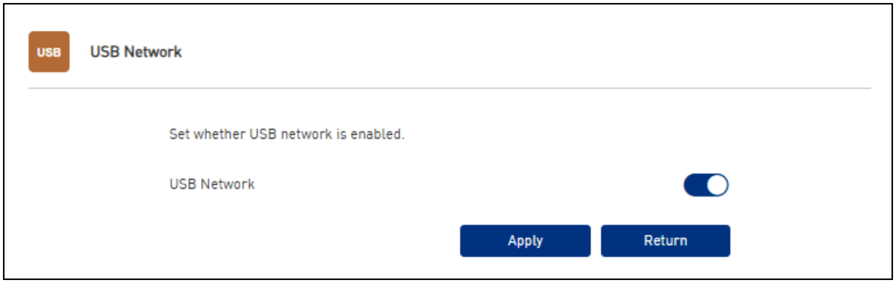
## 9.18 USB Network

The NR2111 can share the network with a client device or be configured through a wired connection (see Section 2.2 on page 22). To allow a device to connect to the NR2111 through the USB port, you have to first enable the USB Network feature. Use the switch on this screen to turn on or off the **USB Network**, then click **Apply**.

Note: The USB Network is disabled by default. You have to log into the Web Configurator using Wi-Fi first to turn on the **USB Network**. Refer to Section 2.2 on page 22 for the Wi-Fi connection steps.

Click **APP MODULE** > **USB Network** to display the following screen.

**Figure 57** APP MODULE > USB Network



Set whether USB network is enabled.

USB Network

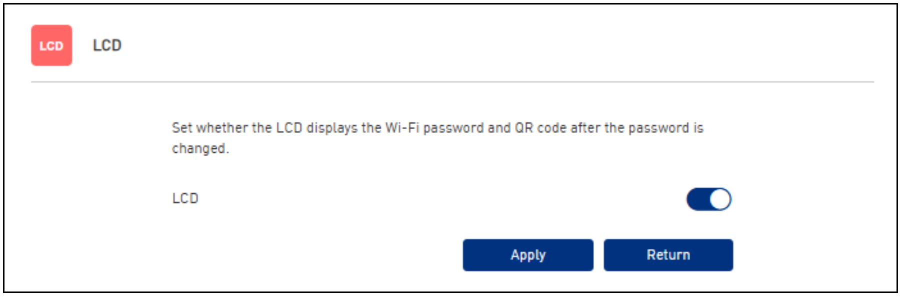
## 9.19 LCD

The NR2111's LCD Wi-Fi screen displays the Wi-Fi SSID, password, and QR code for pairing by default. A client device can use this information to connect to the NR2111's Wi-Fi. Refer to Section 1.6.3 on page 16 for the details on LCD Wi-Fi screen.

You can hide the password and QR code on the LCD to prevent unauthorized access. Use the switch on this screen to show or hide the information on the LCD, then click **Apply**.

Click **APP MODULE** > **Power Save** to display the following screen.

**Figure 58** APP MODULE > LCD



Set whether the LCD displays the Wi-Fi password and QR code after the password is changed.

LCD

## 9.20 Technical Reference

The following section contains additional technical information about the NR2111 features described in this chapter.

## 9.20.1 NAT Port Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Port Forwarding** screen to forward incoming service requests to the servers on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21.

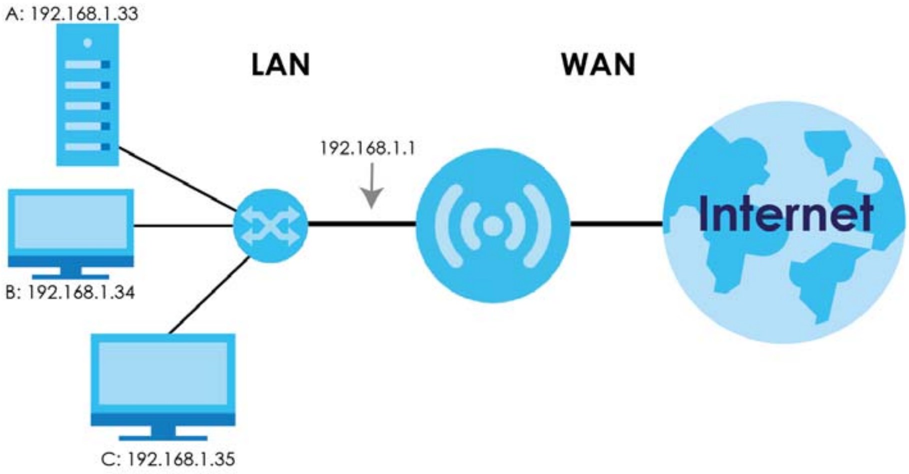
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

## 9.20.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 59** Multiple Servers Behind NAT Example



## 9.20.3 Trigger Port Forwarding

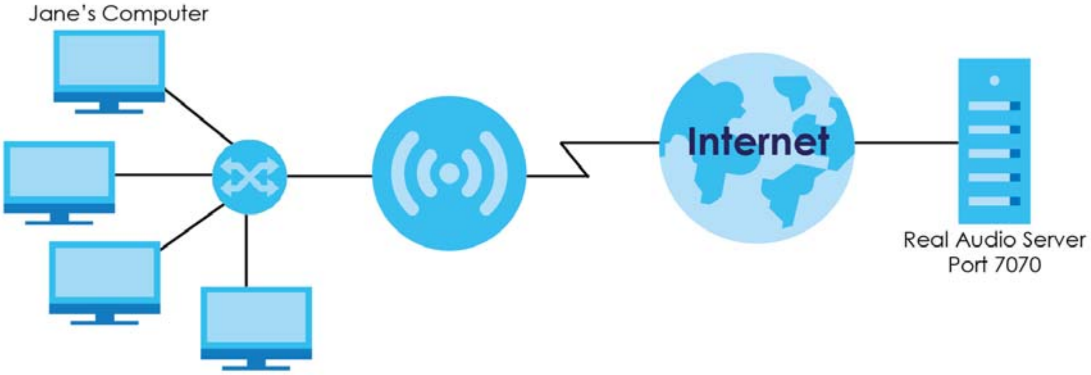
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NR2111 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NR2111's WAN port receives a response with a specific port number and protocol ("incoming" port), the NR2111 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

## 9.20.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

**Figure 60** Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the NR2111 to record Jane's computer IP address. The NR2111 associates Jane's computer IP address with the "incoming" port range of 6970-7170.

3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The NR2111 forwards the traffic to Jane's computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The NR2111 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

## 9.20.5 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is coming from inside the NR2111 and going to the outside.

2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN cannot trigger it.

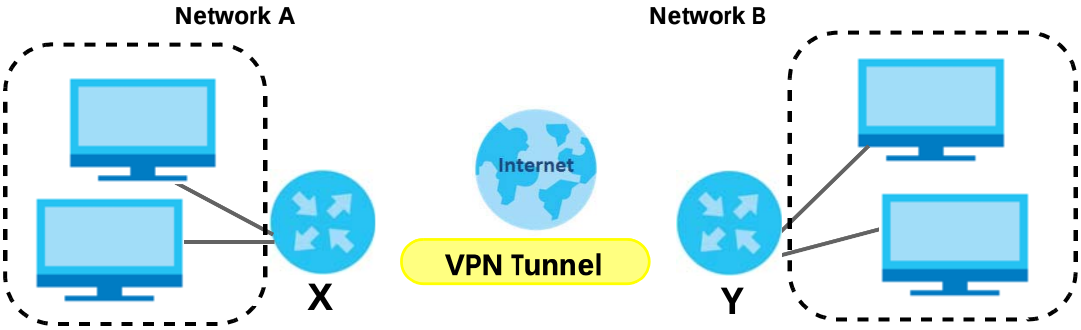
### 9.20.6 VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

**Figure 61** IPSec VPN: Overview



The VPN tunnel connects the Device (X) and the remote IPSec router (Y). These routers then connect the local network (A) and remote network (B).

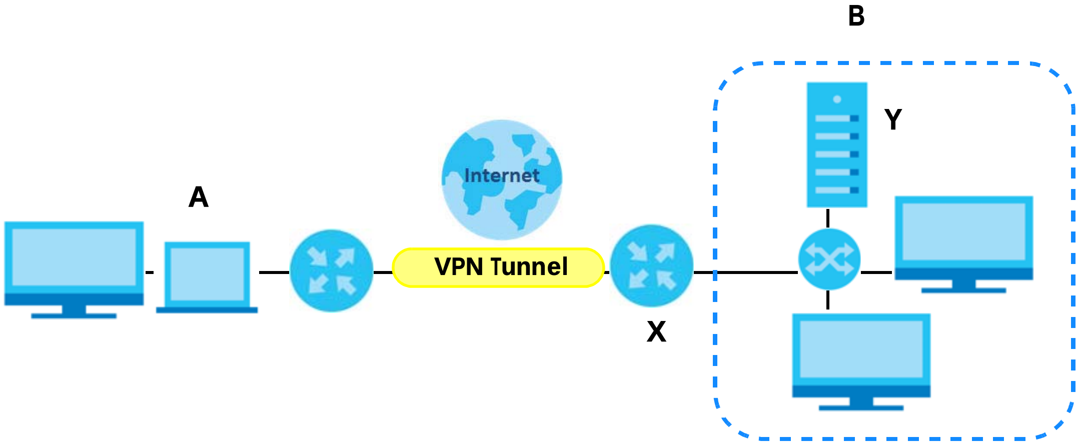
### 9.20.7 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a VPN using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

PPTP sets up two sessions and uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers. It is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

PPTP works on a client-server model and is suitable for remote access applications. For example, an employee (**A**) can connect to the PPTP VPN gateway (**X**) as a PPTP client to gain access to the company network resources from outside the office. When you connect to a remote network (**B**) through a PPTP VPN, all of your traffic goes through the PPTP VPN gateway (**X**).

**Figure 62** PPTP VPN Example

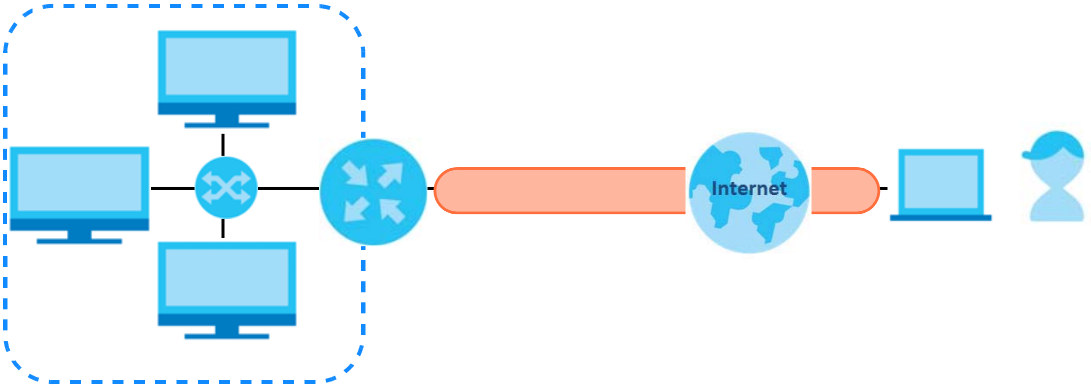


## 9.20.8 L2TP

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it.

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the NR2111. The remote users do not need their own IPSec gateways or VPN client software.

**Figure 63** L2TP VPN Overview



## 9.20.9 Wi-Fi Protected Setup (WPS)

Your NR2111 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### 9.20.9.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the NR2111, see Section 9.11 on page 95).
3. Press the button on one of the devices (it does not matter which). For the NR2111 you must press the WPS button for more than five seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### 9.20.9.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the NR2111, see Section 9.11 on page 95).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

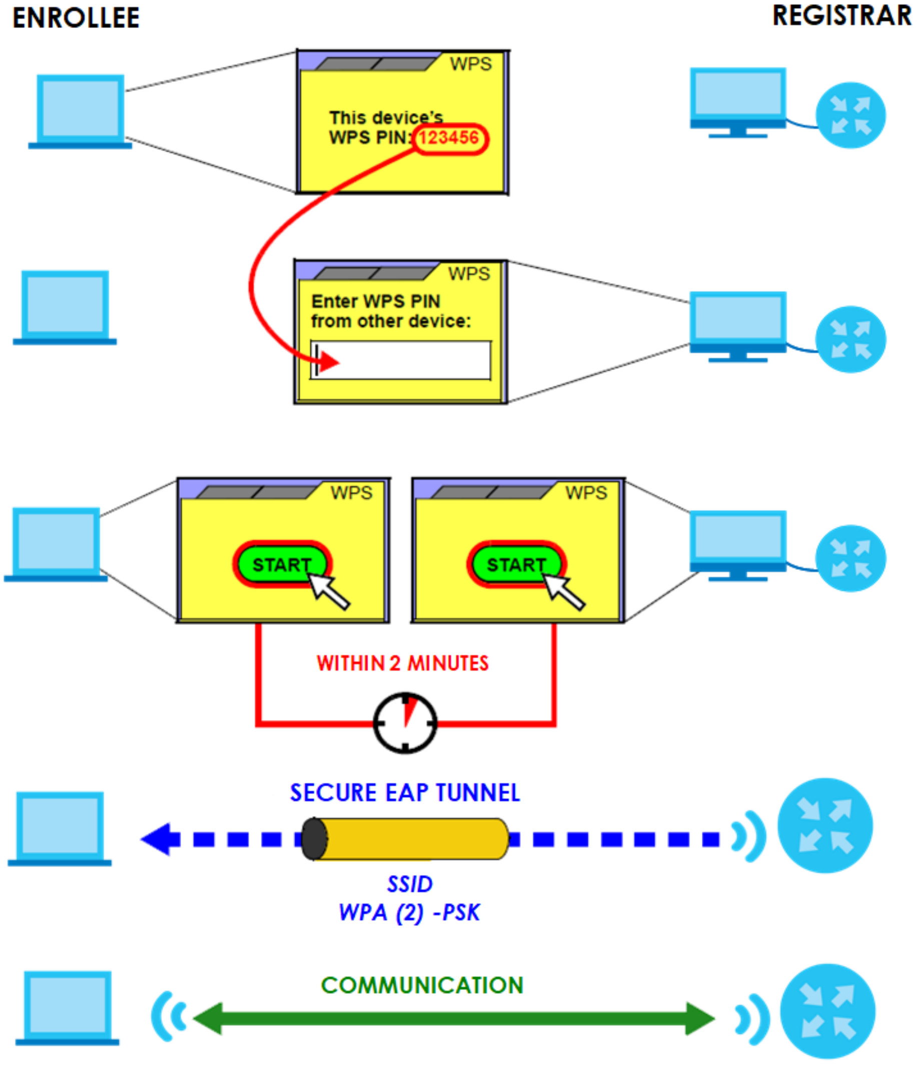
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

**Figure 64** Example WPS Process: PIN Method

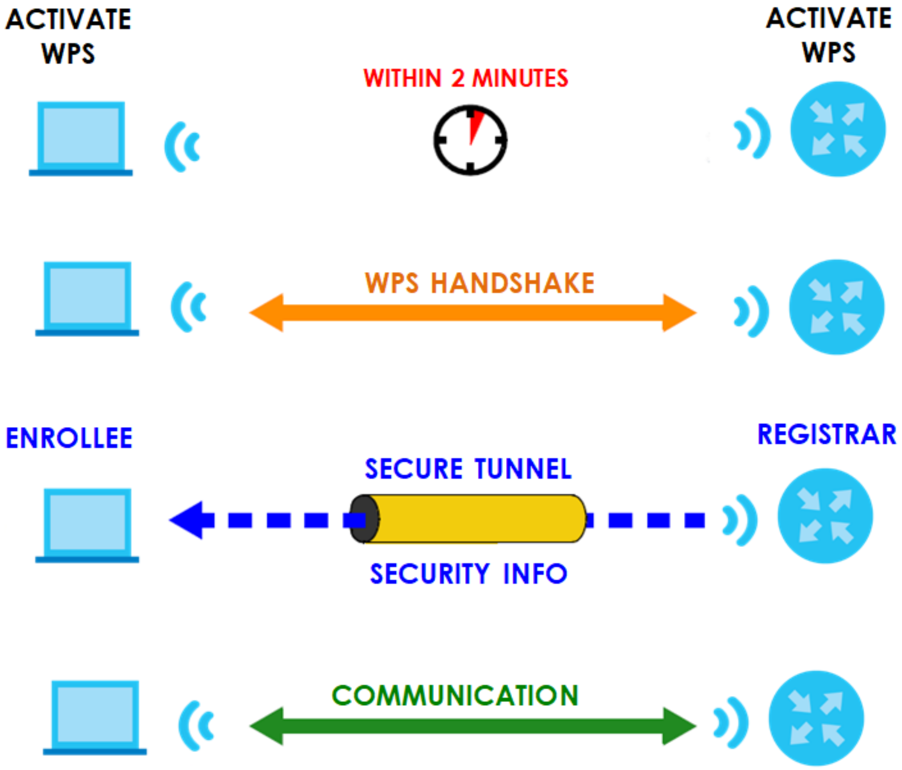


### 9.20.9.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

**Figure 65** How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

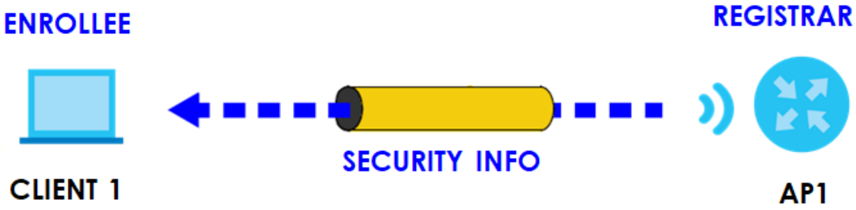
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

### 9.20.9.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

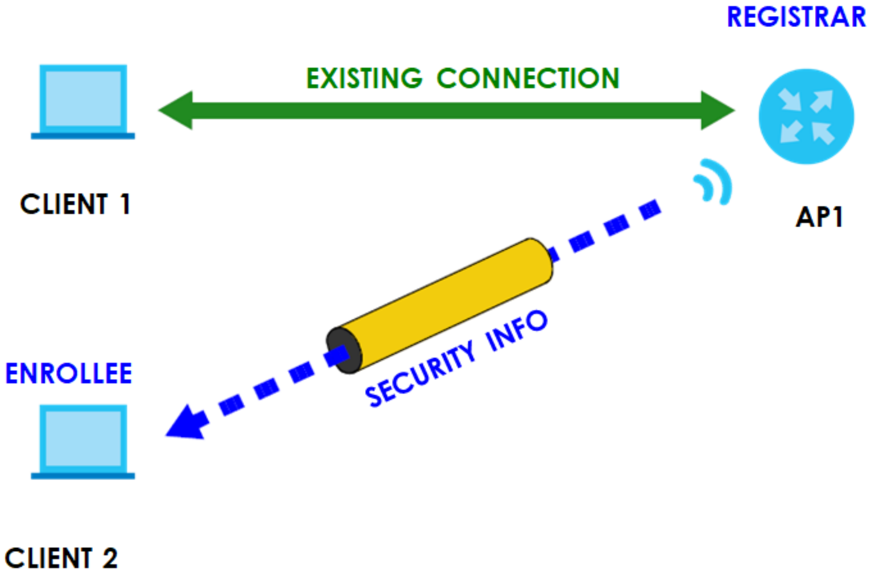
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 66** WPS: Example Network Step 1



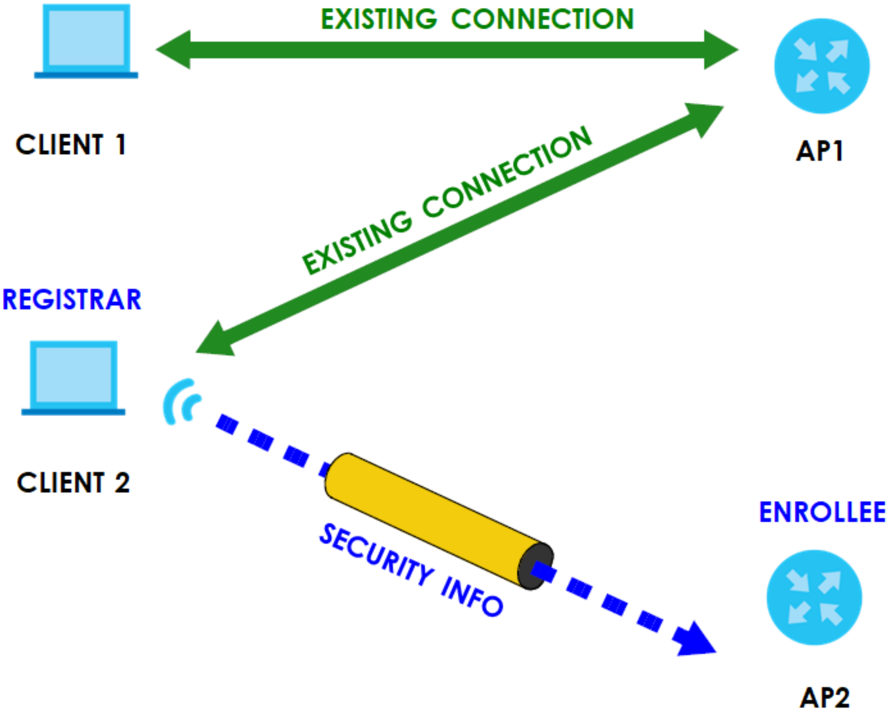
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

**Figure 67** WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 68** WPS: Example Network Step 3



### 9.20.9.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

# CHAPTER 10 Troubleshooting

## 10.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Accessibility and Compatibility Problems
- Power
- NR2111 Access and Login
- Internet Access
- IP Address Setup
- Wi-Fi Connections

## 10.2 Accessibility and Compatibility Problems

### Screen reader not reading content.

- Ensure the latest version of the screen reader is installed.
- Check if the screen reader's accessibility settings are enabled.

### Web browser not displaying correctly.

- Clear your web browser cache.
- Ensure that JavaScript is enabled.
- Try using a different supported web browser.

## 10.3 Power

### The NR2111 does not turn on. The LCD display is not on.

1 Make sure the built-in battery is charged. Press the power button to turn the NR2111 on. See (Chapter 1 on page 13.)

2 If the problem continues, contact the vendor.

## 10.4 NR2111 Access and Login

### I forgot the IP address for the NR2111.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. To reset your NR2111, press the **RESET** button.

### I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the NR2111.

2 Make sure the NR2111 is correctly installed and turned on. See the Quick Start Guide and Chapter 1 on page 13.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is connected to the NR2111 and is in the same subnet as the NR2111.

5 Make sure the NR2111's Wi-Fi is enabled. You can enable or disable the NR2111's Wi-Fi network using **Wi-Fi Settings** on the Web Configurator (see Chapter 6 on page 55).

6 Reset the device to its factory defaults, and try to access the NR2111 with the default IP address. To reset your NR2111, press the **RESET** button. See Chapter 1 on page 13.

7 Disconnect your computer from the NR2111 and then connect once again.

8 If the problem continues, contact the vendor.

### I forgot the password of the Web Configurator.

1 The default user name is **admin**. Check the NR2111's LCD **About** screen for the default password (see Chapter 1 on page 19 for more information).

2 If this does not work, you have to reset the device to its factory defaults. To reset your NR2111, press the **RESET** button.

### I can access the **Login** screen, but I cannot log in to the NR2111.

1 Make sure you have entered the user name and password correctly. The default user name is **admin** and check the NR2111's LCD **About** screen for the default password (see Chapter 1 on page 19 for more information). These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after five minutes.

3 Disconnect and connect to the NR2111 again.

4 If this does not work, you have to reset the device to its factory defaults. To reset your NR2111, press the **RESET** button.

## 10.5 Internet Access

### I cannot access the Internet through a 4G or 5G wireless WAN connection.

1 Make sure you insert a 4G or 5G SIM card into the card slot before turning on the NR2111.

2 If your SIM card has a PIN code, connect to the Web Configurator (http://192.168.1.1) using the user name (Default: **admin**) and password (check the NR2111's **About** screen for the default password (see Chapter 1 on page 19 for more information)) to unlock your SIM card.

3 Make sure your mobile access information (such as APN) is entered correctly. You can check this in the Web Configurator (http://192.168.1.1). The APN fields are case-sensitive, so make sure [Caps Lock] is not on. Check with your service provider for the correct APN if you do not have it.

4 Make sure your SIM card's account is valid and has an active data plan. Check your service contract or contact your service provider directly.

5 Make sure your data plan has not reached its limit.

6 If you are using a pre-paid SIM card, insert the SIM card on another mobile device to check if the SIM card still works. If the SIM card works without any problems on another mobile device, contact the vendor. Otherwise, contact your service provider.

7 Make sure you are in the ISP's coverage area.

8 If the problem continues, contact your ISP.

### I cannot access the Internet anymore. I had access to the Internet (with the NR2111), but my Internet connection is not available anymore.

1. Reboot the NR2111.
2. Make sure the NR2111's Wi-Fi network is enabled. You can enable NR2111's Wi-Fi network on the LCD.
3. Make sure your SIM card's mobile data is enabled. Check this in the Web Configurator. (Chapter 9 on page 72).
4. If you have set a data limit, make sure you have not reached it yet. Check your data left in the Web Configurator.
5. If the problem continues, contact your ISP.

### One of my clients cannot access the Internet anymore. They had access to the Internet (with the NR2111), but the Internet connection is not available anymore.

1. Make sure your client is not blocked. You can check this on the Web Configurator (see Chapter 5 on page 50).
2. Make sure your SIM card's mobile data is enabled. Check this on the Web Configurator (see Chapter 4 on page 45).
3. If you have set a data limit, make sure you have not reached it yet. You can check your data left in the Web Configurator.
4. Reboot the NR2111.

### The Internet connection is slow or intermittent.

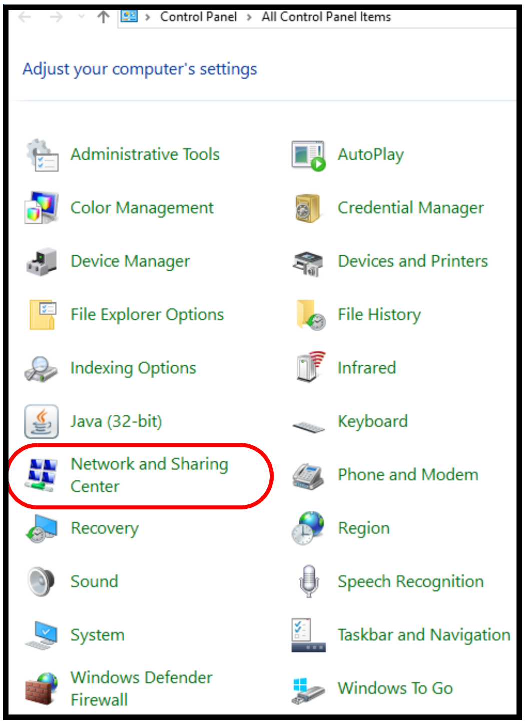
1. There might be a lot of traffic on the network. If the NR2111 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength on the Device LCD screen. If the signal strength is low, try moving the NR2111 closer to the ISP's base station if possible, or try pointing it directly to the ISP's base station. Look around to see if there are any devices that might be interfering with the Wi-Fi network (for example, microwaves, other Wi-Fi networks, and so on).
3. Reboot the NR2111.
4. If the problem continues, contact the network administrator or vendor.

## 10.6 IP Address Setup

I need to set the computer's IP address to be in the same subnet as the NR2111.

1 In Windows 10, open the **Control Panel**.

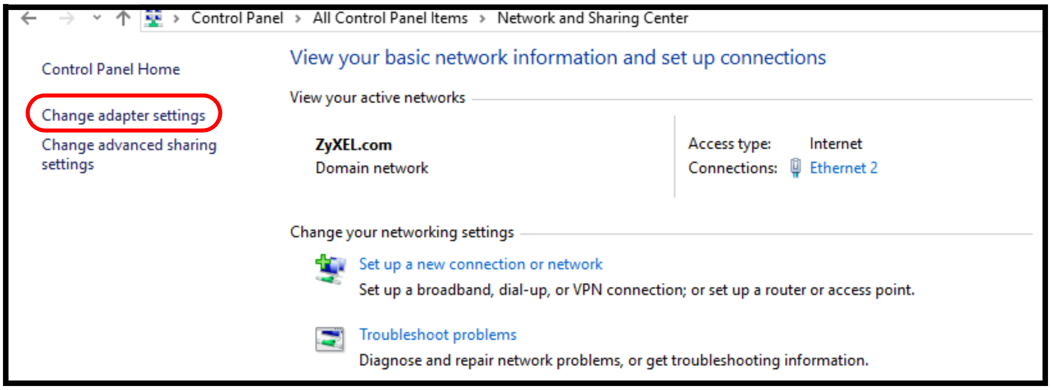
2 Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.



Control Panel > All Control Panel Items

Adjust your computer's settings

3 Click **Change adapter settings**.



Control Panel > All Control Panel Items > Network and Sharing Center

View your basic network information and set up connections

View your active networks

ZyXEL.com
Domain network

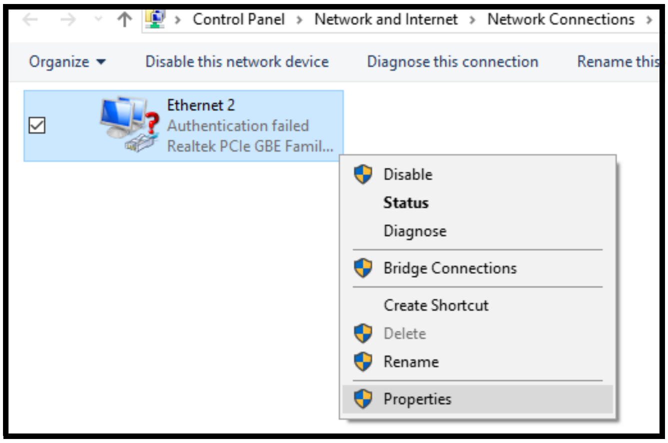
Access type: Internet
Connections: Ethernet 2

Change your networking settings

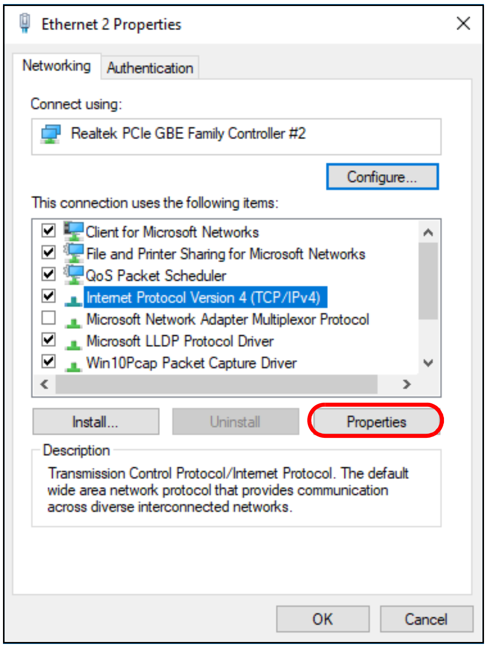
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

4 Right-click the **Ethernet** icon, and then select **Properties.**



5 Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.



Connect using:

Realtek PCIe GBE Family Controller #2

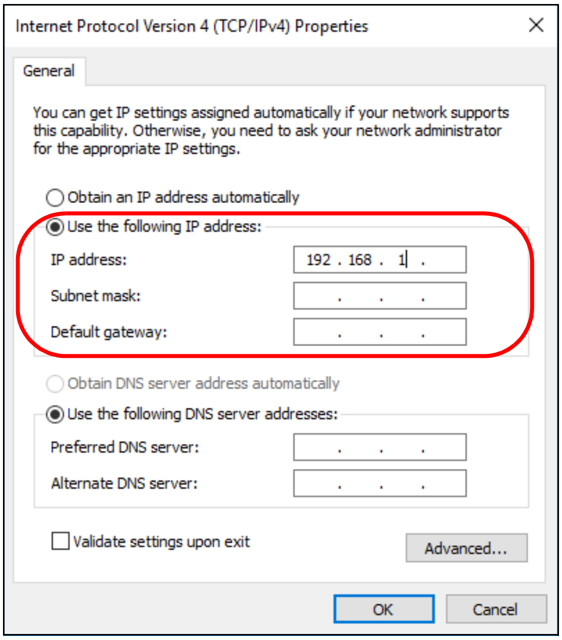
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Win10Pcap Packet Capture Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6 Select **Use the following IP address** and enter an **IP address** from **192.168.1.2** to **192.168.1.254**. The **Subnet mask** will be entered automatically.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

7 Click **OK** when you are done and close all windows.

## 10.7 Wi-Fi Connections

### I cannot access the NR2111.

1 Make sure Wi-Fi is enabled on the NR2111. You can enable or disable the NR2111's Wi-Fi network using the **Wi-Fi** screen on the NR2111's LCD screen. See Chapter 1 on page 16.

2 Make sure the Wi-Fi adapter (installed on your computer) is IEEE 802.11 compatible and supports the same Wi-Fi standard as the NR2111's active radio.

3 Make sure your device (with a Wi-Fi adapter installed) is within the transmission range of the NR2111.

4 Make sure you are using the correct Wi-Fi network name and password to connect to your NR2111. Check your Wi-Fi network settings by reexamining the network name **Wi-Fi SSID** and/or **Wi-Fi Key/ Password** in the Web Configurator (see Section 6.2 on page 55).

5 If you changed your network **Wi-Fi SSID** and/or **Wi-Fi Key** you will be automatically disconnected from the NR2111. Try reconnecting to the network wirelessly with the new **Wi-Fi SSID** and/or **Wi-Fi Key**.

### One of my clients cannot access the NR2111.

1 Make sure the Wi-Fi is enabled on the NR2111. You can enable or disable the NR2111's Wi-Fi network using the **Wi-Fi** screen on the NR2111's LCD screen. See Section 1.6.3 on page 16.

2 Make sure the Wi-Fi adapter (installed on your computer) is IEEE 802.11 compatible and supports the same Wi-Fi standard as the NR2111's active radio.

3 Make sure your client's device (with a Wi-Fi adapter installed) is within the transmission range of the NR2111.

4 Make sure your client is using the correct Wi-Fi network name **(Wi-Fi SSID)** and password **(Wi-Fi Key/ Password)** to connect to your NR2111 (see Section 6.2 on page 55).

# APPENDIX A Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

## Corporate Headquarters (Worldwide)

### Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

## Asia

### China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

### India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

### Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

### Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

### Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

### Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

### Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

### Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

### Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

### Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

## Europe

### Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

### Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

### Bulgaria

- Zyxel Bulgaria

- *https://www.zyxel.com/bg/bg*

## Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

## Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

## Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

## France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

## Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

## Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

## Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

## Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

## Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

## Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

### Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

### Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

### Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

### Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

### Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

### Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

### UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

### Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

## South America

### Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

### Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

### Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

### Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

### South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

## Middle East

### Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

## North America

### USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

# APPENDIX B
# Legal Information

## Copyright

## Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Regulatory Notice and Statement

## Europe

The following information applies if you use the product within the European Union.

### Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- The maximum RF power operating for each band as follows:

- WCDMA band I/VIII is 24 dBm
- LTE band 1/3/7/8/20/28/38/40/41is 23 dBm
- NR band n1/n3/n7/n8/n20/n28/n38/n40 is 23 dBm
- NR band n41/n77/n78 is 26 dBm
- Wi-Fi:

  The band 2400 – 2483.5 MHz is 20 dBm  
  The band 5150 – 5350 MHz is 23 dBm  
  The band 5470 – 5725 MHz is 30 dBm  
  The band 5745 – 5825 MHz is 14 dBm

| | |
|---|---|
| Belgium (English)<br>België (Flemish)<br>Belgique (French) | National Restrictions<br>• The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check *http://www.bipt.be* for more details.<br>• Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens.<br>• Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.ibpt.be* pour de plus amples détails. |
| Čeština (Czech) | Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. |
| Dansk (Danish) | Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. |
| Deutsch (German) | Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. |
| Eesti keel (Estonian) | Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| Ελληνικά (Greek) | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EE. |
| English | Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. |
| Español (Spanish) | Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE. |
| Français (French) | Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE. |
| Hrvatski (Croatian) | Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE. |
| Íslenska (Icelandic) | Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE. |
| Italiano (Italian) | Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.<br>National Restrictions<br>• This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check *https://www.mise.gov.it/it/* for more details.<br>• Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli. |

| | |
|---|---|
| Latviešu valoda (Latvian) | Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| Lietuvių kalba (Lithuanian) | Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas. |
| Magyar (Hungarian) | Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. |
| Malti (Maltese) | Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE. |
| Nederlands (Dutch) | Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. |
| Norsk (Norwegian) | Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU. |
| Polski (Polish) | Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE. |
| Português (Portuguese) | Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE. |
| Română (Romanian) | Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/UE. |
| Slovenčina (Slovak) | Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ. |
| Slovenščina (Slovene) | Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. |
| Suomi (Finnish) | Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska (Swedish) | Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. |
| Български (Bulgarian) | С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/EC. |

Notes:

1. Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

## List of national codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|---|---|---|---|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | CZ | Norway | NO |
| Denmark | DK | Poland | PL |
| Estonia | EE | Portugal | PT |
| Finland | FI | Romania | RO |
| France | FR | Serbia | RS |
| Germany | DE | Slovakia | SK |
| Greece | GR | Slovenia | SI |
| Hungary | HU | Spain | ES |
| Iceland | IS | Switzerland | CH |
| Ireland | IE | Sweden | SE |
| Italy | IT | Turkey | TR |
| Latvia | LV | United Kingdom | GB |

### Safety Warnings

- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- The Power Supply is not waterproof, avoid contact with liquid. Handle the Power Supply with care; do not pry open, nor pull or press the pins on it.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.

- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Environment Statement

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

## 台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

· 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

· 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

· 前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

· 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

· 無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

· 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

· 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示 :

· 請勿將此產品接近水、火焰或放置在高溫的環境。

· 避免設備接觸 :

- 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。

· 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。

· 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。

· 若接上不正確的電源變壓器會有爆炸的風險。

- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 ( 如：台灣供應電壓 110 伏特。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|---|
| ∿ | Alternating current (AC):<br>AC is an electric current in which the flow of electric charge periodically reverses direction. |
| ⎓ | Direct current (DC):<br>DC is the unidirectional flow or movement of electric charge carriers. |
| ⏚ | Earth; ground:<br>A wiring terminal intended for connection of a Protective Earthing Conductor. |
| ⧈ | Class II equipment:<br>The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

## Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor.

## Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: *https://service-provider.zyxel.com/global/en/gpl-oss-software-notice*

# Index