ZYXEL

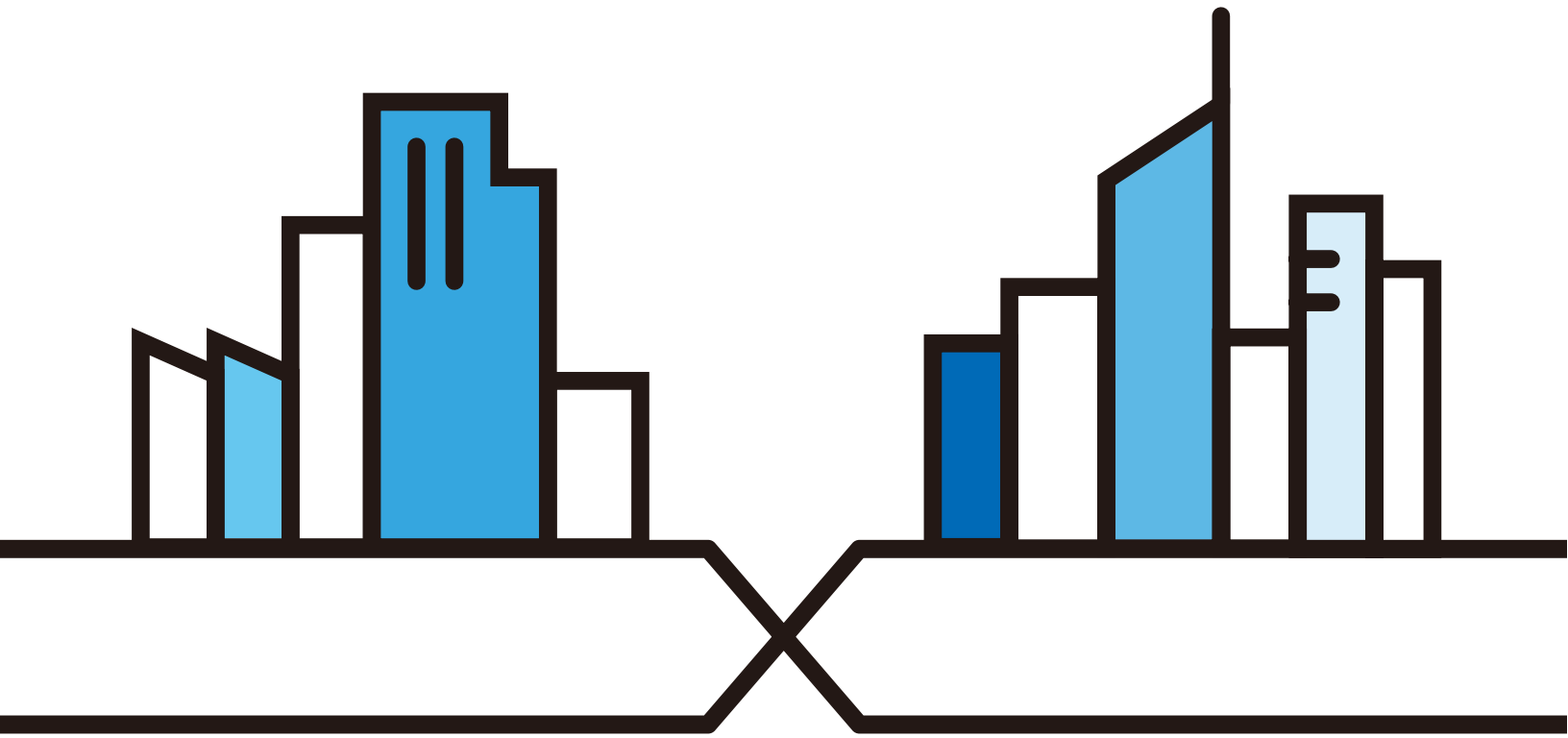
User's Guide

NR2301

5G NR Portable Router

Default Login Details	
LAN IP Address	http://192.168.1.1
Login	admin
Password	See the NR2301's LCD About screen

Version 1.00 Ed 1, 11/2023



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 NR2301.

Contents Overview

Get to Know Your NR2301 9

User's Guide 21

Web Configurator 22
Tutorials 27

Technical Reference 37

Network Status 38
User List 40
WI-FI SETTINGS 47
Device Status 55
Network Settings 60
Device Management 66
Troubleshooting 109

Table of Contents

Contents Overview **3**

Table of Contents **4**

Document Conventions **8**

Chapter 1
Get to Know Your NR2301 ..... **9**

1.1 Overview 9
1.2 Applications 9
1.3 Ways to Manage the NR2301 10
1.4 Hardware Description 10
1.4.1 Power Button 11
1.4.2 Hardware Connections 11
1.4.3 Reset the NR2301 11
1.5 LCD Screens 12
1.5.1 LCD Menu Screen 13
1.5.2 SSID & Password Setting 14
1.5.3 Network Connection 15
1.5.4 Data Plan Limitation 16
1.5.5 Wi-Fi Settings 17
1.5.6 WPS 17
1.5.7 Viewing SMS 18
1.5.8 Fota Screen 19
1.5.9 About Screen 19

Part I: User's Guide **21**

Chapter 2
Web Configurator **22**

2.1 Introduction 22
2.2 Accessing the Web Configurator 22
2.3 Navigating the Web Configurator 23
2.3.1 Title Bar 24
2.3.2 The Main Window 25
2.3.3 Menu List 25

Chapter 3
Tutorials **27**

3.1 Overview 27
3.2 WiFi Network Setup 27
3.2.1 Changing Security on a WiFi Network 27
3.2.2 Connecting to the NR2301's WiFi Network Using WPS 28
3.3 MAC Filter 32
3.3.1 Configuring a Blacklist 32
3.4 Device Maintenance 34
3.4.1 Manually Upgrading the Firmware 34
3.4.2 Backing up the Device Configuration 35
3.4.3 Restoring the Device Configuration 35

Part II: Technical Reference 37

Chapter 4
Network Status 38

4.1 Overview 38
4.2 NETWORK STATUS 38

Chapter 5
User List 40

5.1 Overview 40
5.2 Online Users 40
5.3 Offline Users 41
5.4 Forbidden Users 43
5.5 Allow Users 44
5.6 MAC Filter Mode 45

Chapter 6
WI-FI SETTINGS 47

6.1 Overview 47
6.1.1 What You Need to Know 47
6.2 The Wi-Fi Settings Screen 48
6.3 Guest Wi-Fi 52
6.4 Advanced Settings 53

Chapter 7
Device Status 55

7.1 Overview 55
7.2 Status 55
7.3 Statistics 57
7.4 Network Information 58

Chapter 8
Network Settings 60

8.1 Overview 60
8.2 Network Settings 60
8.3 Network Operators 62
8.4 DHCP 63

Chapter 9
Device Management 66

9.1 Overview 66
9.2 Package Settings 66
9.3 Firewall 71
9.3.1 IP Filter 72
9.3.2 URL Filter 73
9.3.3 Port Forward 74
9.3.4 Port Trigger 76
9.3.5 Port Filter 78
9.3.6 UPnP 79
9.3.7 Remote 80
9.3.8 DMZ Settings 81
9.4 VPN 82
9.5 Messages 83
9.5.1 Inbox 83
9.5.2 Outbox 84
9.5.3 Drafts 85
9.5.4 New Messages 85
9.6 PIN Settings 86
9.7 Admin Settings 87
9.8 Update 88
9.8.1 Online Update 89
9.8.2 Firmware Management 89
9.9 Configuration Backup 90
9.10 Device Reboot 91
9.11 Diagnosis 92
9.12 WPS 94
9.13 DDNS 95
9.14 VPN Passthrough 96
9.15 Power Save 97
9.16 Technical Reference 98
9.16.1 NAT Port Forwarding: Services and Port Numbers 98
9.16.2 NAT Port Forwarding Example 98
9.16.3 Trigger Port Forwarding 99
9.16.4 Trigger Port Forwarding Example 99

9.16.5 Two Points To Remember About Trigger Ports 100
9.16.6 NAT Traversal 100
9.16.7 Cautions With UPnP 100
9.16.8 VPN 100
9.16.9 PPTP 101
9.16.10 L2TP 102
9.16.11 WiFi Protected Setup (WPS) 102

Chapter 10
Troubleshooting 109

10.1 Overview 109
10.2 Power 109
10.3 NR2301 Access and Login 109
10.4 Internet Access 111
10.5 IP Address Setup 112
10.6 WiFi Connections 115
10.7 Getting More Troubleshooting Help 115

Appendix A Legal Information 116

Index 121

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 NR2301 icon is not an exact representation of your device.

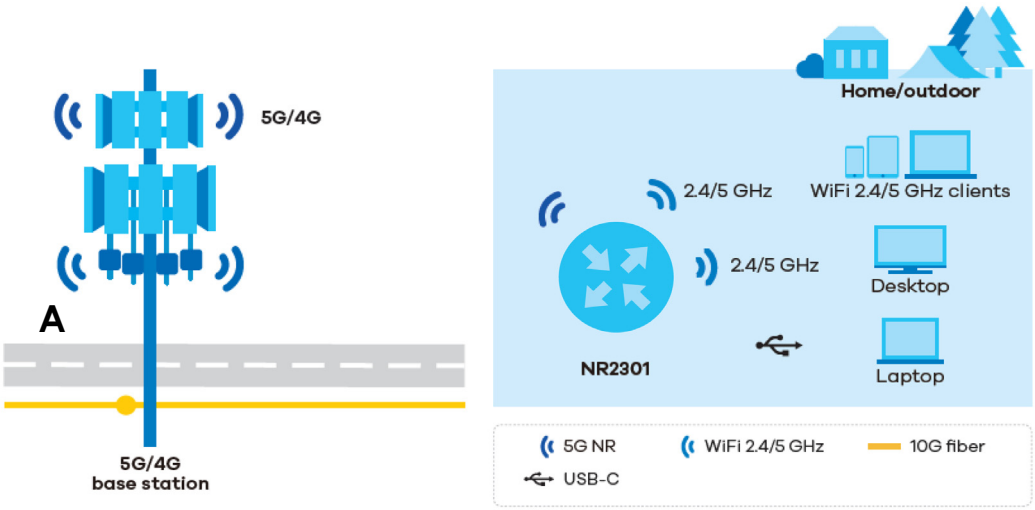
NR2301 	Switch 	5G/4G Base Station 
Server 	Firewall 	Smartphone 
Tablet 	Antenna Tower 	Home 
Desktop 	Printer 	Outdoors 
Notebook 		

CHAPTER 1
Get to Know Your NR2301

1.1 Overview

The NR2301 is a 5G NR portable router that complies with the 3GPP release 16 standard, ensuring seamless compatibility with 4G networks. Offering high-speed broadband service through WiFi 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 NR2301 has 5G NR download speeds of up to 3.4 Gbps and 4G LTE download speeds of up to 1.6 Gbps, increasing internet speed and reducing network latency. It also supports the WiFi 6 (11ax) standard, offering speeds of up to 1.8 Gbps with 2x2 UL/DL MU-MIMO. The NR2301 delivers premium speed for multi-streaming data access and optimal WiFi experience without dead zones.



1.2 Applications

Wireless WAN

The NR2301 can connect to the Internet through a SIM card to access a 4G or 5G wireless WAN connection. Just insert a SIM card into the SIM card slot on the NR2301.

Note: You must insert the SIM card into the card slot before turning on the NR2301.

USB Tethering

A computer with Windows or Mac OS can connect to the NR2301's USB 3.0 port with a USB 3.0 cable to access the Web Configurator without installing any drivers.

Wireless LAN (WiFi)

The NR2301's WiFi allows access to high-speed broadband service and local management. Connect a computer/smartphone/tablet to the NR2301's WiFi and use the Web Configurator to configure your NR2301.

1.3 Ways to Manage the NR2301

- **LCD Screen Interface**

You can use the LCD screen interface along with the buttons on the right side of the NR2301 to manage it.

- **Web Configurator**

The Web Configurator is recommended for everyday management by using a supported web browser.

1.4 Hardware Description

The following images show the front and side panels of the NR2301.

Figure 1 Front Panel

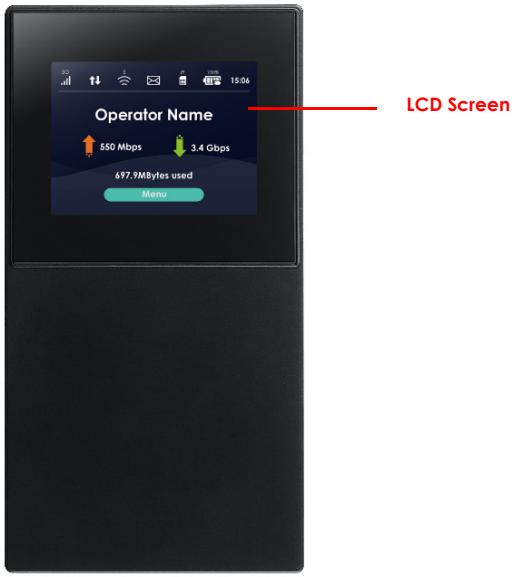
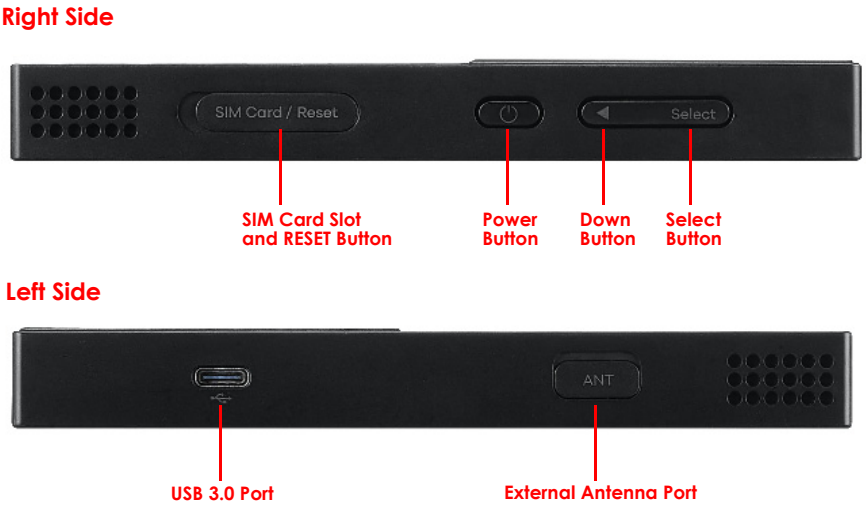


Figure 2 Side Panels



1.4.1 Power Button

Use the power button on the right side panel to turn the NR2301 on or off. To turn on, press the power button for 4 to 5 seconds until the LCD screen turns on.

Power Off

To turn the NR2301 off, press the power button once to wake up the LCD, then press for 6 to 7 seconds and release it when the LCD screen displays **MiFi is shutting down....**

1.4.2 Hardware Connections

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

1.4.3 Reset the NR2301

Remove the SIM card cover. Use a SIM ejector pin or a paper clip to press the **RESET** button for 3 seconds to restore to the NR2301's factory default settings.

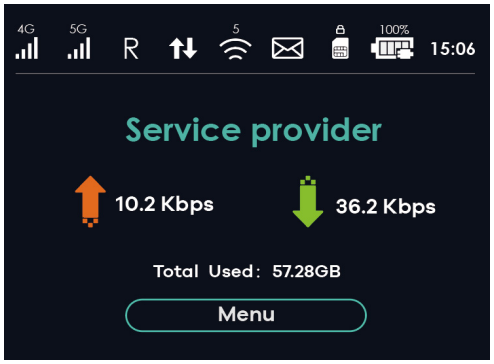
This resets the NR2301 to the factory default configuration. This means that you will lose all configurations that you had previously, such as WiFi SSID and password.

1.5 LCD Screens

This section describes the labels or icons displayed on the LCD screen of your NR2301. The following **Home** screen displays when the NR2301 is powered on and finishes initializing.

Note: The LCD screen turns off after 30 seconds if it is idling. Press the power button once to turn the LCD screen on again.

Figure 3 LCD Home Screen

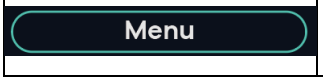


The following table describes the labels in this screen.

Table 1 LCD Home Screen

LABEL	DESCRIPTION
	This displays the type of network the NR2301 is connected to and its signal strength. Both icons display if both 4G and 5G are connected.
	This displays when roaming is enabled on the NR2301. See Chapter 8 on page 60 for more information.
	This displays when the NR2301 is receiving/transmitting data to/from the Internet.
	This displays the WiFi network status. The number indicates how many clients are currently connected to the NR2301.
	This displays when the NR2301 receives an SMS (Short Message Service) message.
	This displays if the NR2301 could not detect a SIM card.
	This displays if the SIM card's data plan is not compatible with any of the detected available networks.
	This displays when the NR2301 cannot access the SIM card because it is locked.

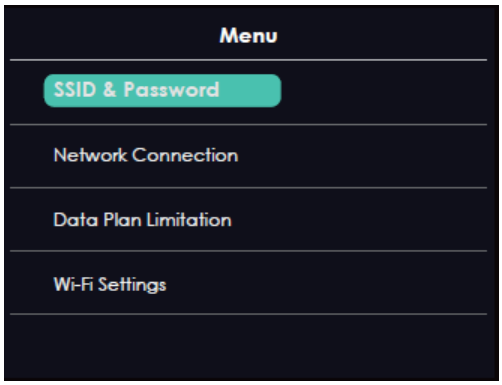
Table 1 LCD Home Screen (continued)

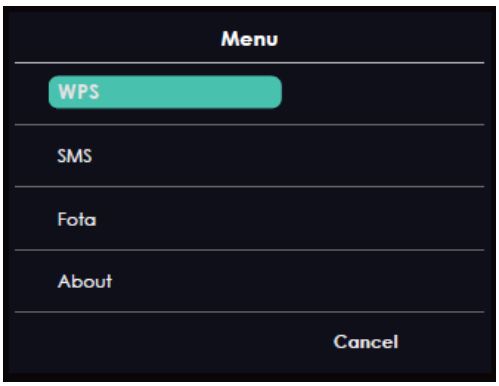
LABEL	DESCRIPTION
	This icon shows the NR2301 battery life.
	This displays the current time.
	This displays your NR2301's Internet Service Provider.
	This displays the NR2301's speed when receiving/transmitting data to/from the Internet.
	This displays the mobile data used in total by the NR2301.
	Select this to enter and navigate the NR2301's menu.

1.5.1 LCD Menu Screen

Press the **Select** button to select the **Menu** button on the LCD **Home** screen. The LCD **Menu** screen appears. Press the down button to navigate the menu. Press the **Select** button to select an option.

Figure 4 Menu Screen





The following table describes the labels in the **Menu** screen.

Table 2 LCD Menu Screen

LABEL	DESCRIPTION
SSID & Password	Use **SSID & Password** to allow a client device to find this SSID and enter the Password to connect wirelessly to the NR2301.
Network Connection	Use **Network Connection** to see your network status and connection information.
Data Plan Limitation	Use **Data Plan Limitation** to display your data usage and limit.
Wi-Fi Settings	Use **Wi-Fi Settings** to select the NR2301's WiFi mode.
WPS	If your client supports WPS, use **WPS** to connect wirelessly to the NR2301.
SMS	Use **SMS** to check SMS messages.
Fota	Use **Fota** to display the current firmware version and check for firmware updates.
About	Use **About** to display the NR2301's hardware and software information.
Cancel	Select **Cancel** to return to the LCD **Home** screen.

1.5.2 SSID & Password Setting

WiFi clients can use the **SSID & Password** screen to find the SSID and password for wireless connection to the NR2301.

1 From the LCD **Home** screen, press the **Select** button to go to the **Menu** screen.

2 The **SSID & Password** option is on top of the **Menu** screen. Press the **Select** button to enter the screen.

3 The **2.4GHz SSID & Password** is displayed.

4 Select **Next** to show **5GHz SSID & Password**. Select **Back** to return to the **Menu** screen.

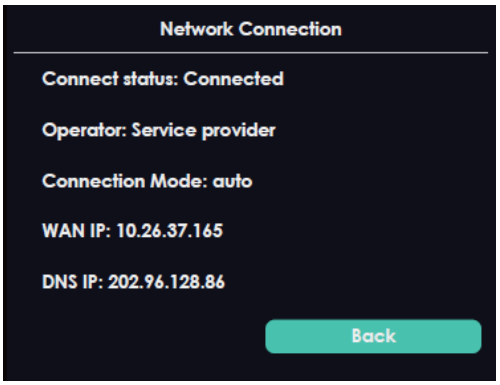
From a WiFi client enter and the displayed **SSID** and **Password** to connect wirelessly to the NR2301. Alternatively, use the QR code to scan the SSID and password.

Figure 5 2.4GHz/5GHz SSID & Password Screens

1.5.3 Network Connection

To show the 5G or 4G (WAN) network status, press the down button to navigate to **Network Connection** and the **Select** button to select it.

Figure 6 Network Connection Screen



The following table describes the labels in this screen.

Table 3 Network Connection Screen

LABEL	DESCRIPTION
Connect Status	This displays the WAN network status of the NR2301.
Operator	This displays the service provider's name of your 4G/5G network (WAN).

Table 3 Network Connection Screen (continued)

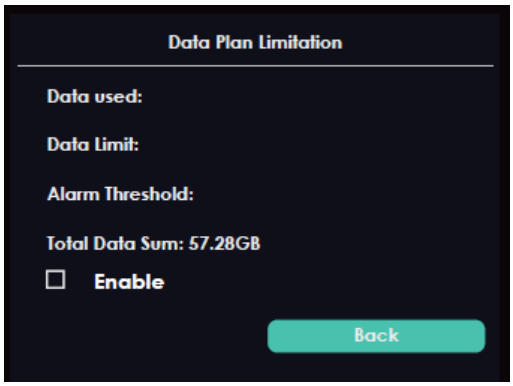
LABEL	DESCRIPTION
Connection Mode	This displays the current mode of your NR2301 (**4G**, **5G**, or **auto**).
WAP IP	This displays the current IP address of the NR2301 in the WAN.
DNS IP	This displays the DNS server address assigned to the NR2301.
Back	Select this button to return to the **Menu** list.

1.5.4 Data Plan Limitation

The **Data Plan Limitation** screen displays the amount of mobile data usage and limit for the NR2301 if it is enabled. In the LCD **Menu** screen, press the down button to go to **Data Plan Limitation** and the **Select** button to select it.

Note: You can go to the Web Configurator's **APP MODULE** > **Package Settings** screen to set up a data limit. See Chapter 9 on page 66 for more information.

Figure 7 Data Plan Limitation Screen



The following table describes the labels in this screen.

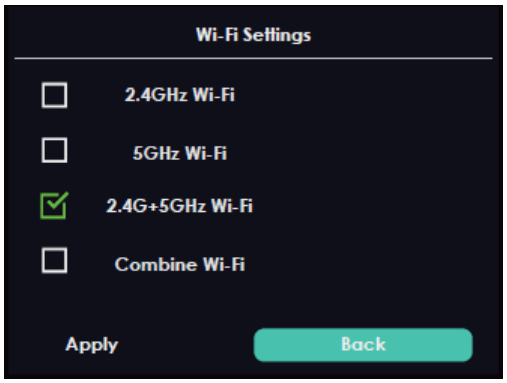
Table 4 Data Plan Limitation Screen

LABEL	DESCRIPTION
Data used	This displays the mobile data used by your NR2301 in total for the current period. This field is empty if no data plan limitation was configured in the Web Configurator.
Data Limit	This displays the NR2301's configured mobile data limit. This field is empty if no data plan limitation was configured in the Web Configurator.
Alarm Threshold	This displays the remaining percentage of available data usage before the NR2301 displays a warning on the LCD **Home** screen. This field is empty if no data plan limitation was configured in the Web Configurator.
Total Data Sum	This displays the mobile data used in total by your NR2301.
Enable	Select the **Enable** check box to enable the data plan limit configured in the Web Configurator. Once you reach that limit, your cellular data will be disabled. Clear the **Enable** check box to disable the data plan limit.
Back	Select this button to return to the **Menu** list.

1.5.5 Wi-Fi Settings

To enable the WiFi clients (up to 32) to connect to the 2.4GHz / 5GHz WiFi band, press the down button to go to **Wi-Fi Settings** and press the **Select** button to select it. The following screen displays.

Figure 8 Wi-Fi Settings Screen



The following table describes the labels in this screen.

Table 5 Wi-Fi Settings Screen

LABEL	DESCRIPTION
2.4GHz Wi-Fi	Select **2.4GHz Wi-Fi** to enable the 2.4GHz WiFi band.
5GHz Wi-Fi	Select **5GHz Wi-Fi** to enable the 5GHz WiFi band.
2.4G+5GHz Wi-Fi	Select **2.4G+5GHz Wi-Fi** to enable both the 2.4GHz and 5GHz WiFi bands.
Combine Wi-Fi	Select **Combine Wi-Fi** to have the 2.4GHz and 5GHz use the same SSID.
Apply	Click **Apply** to save your changes back to the NR2301.
Back	Select this button to return to the **Menu** list.

1.5.6 WPS

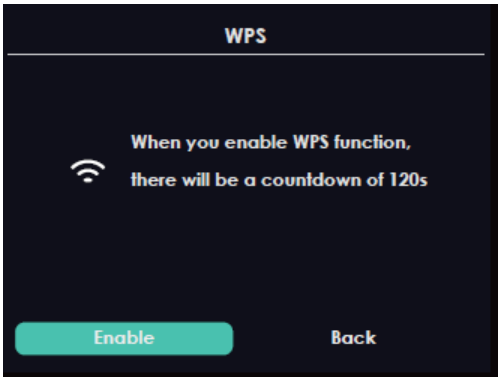
Your NR2301 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a WiFi network with 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). 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.

You can use the LCD of the NR2301 to activate WPS in order to quickly set up a WiFi network with security.

In the LCD **Menu** screen, press the down button to go to **WPS** and press the **Select** button to select it. The following screen displays.

Figure 9 WPS Screen



Select the **Enable** button to start WPS pairing. Press the WPS button on another WPS-enabled device within range of the NR2301 within 120 seconds.

Note: You must activate WPS on the NR2301 and on another device within 2 minutes of each other.

1.5.7 Viewing SMS

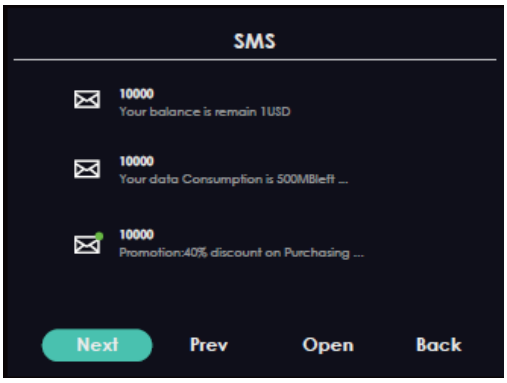
SMS (Short Message Service) allows you to view the text messages that the NR2301 received from mobile devices or the service provider.

When the SMS box is full the NR2301 automatically deletes the oldest SMS message.

In the LCD **Menu** screen, press the down button to go to **SMS** and press the **Select** button to select it. The following screen displays.

Use the **Next** and **Prev** buttons to navigate through the SMS list and use the **Open** button to open the highlighted option. A green dot indicates the message is unread.

Figure 10 SMS Screen



After reading an SMS message, press the **Back** button to return to the SMS list.

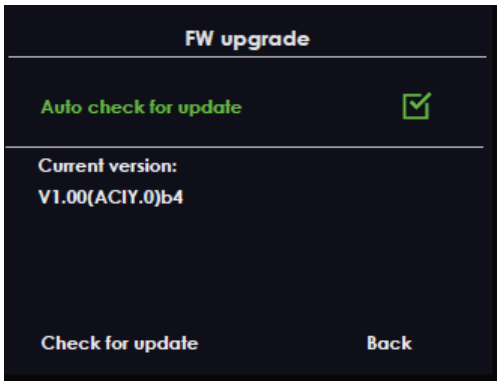
Note: It is highly recommended to delete unwanted SMS messages to prevent the SMS box from getting full. You can only delete SMS messages using the Web Configurator.

1.5.8 Fota Screen

Firmware Over the Air (FOTA) allows for timely and automatic firmware upgrades. Use the **Fota** screen to display the current firmware version and check for firmware updates automatically or manually. By default, the NR2301 checks for firmware update automatically. It will do so each time it is turned on and connected to the Internet.

In the LCD **Menu** screen, press the down button to go to **Fota** and press the **Select** button to select it. The following screen displays.

Figure 11 Fota Screen



The following table describes the labels in this screen.

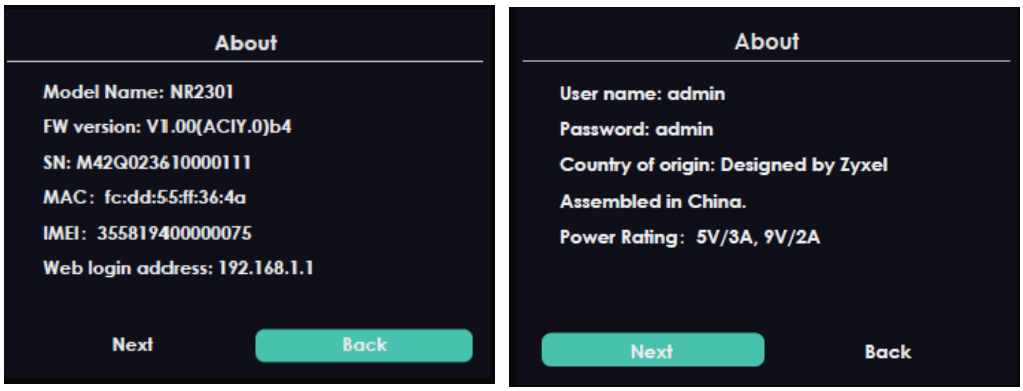
Table 6 Fota Screen

LABEL	DESCRIPTION
Auto check for update	Select this to enable automatic firmware upgrades on your NR2301.
Current version	This displays the present firmware version of your NR2301.
Check for update	Select this to manually check for firmware upgrades for your NR2301.
Back	Select this button to return to the **Menu** list.

1.5.9 About Screen

Use the **About** screens to display the NR2301's hardware and firmware information. In the LCD **Menu** screen, press the down button to go to **About** and press the **Select** button to select it. The following screen displays.

Figure 12 About Screens



The following table describes the labels in these screens.

Table 7 About Screens

LABEL	DESCRIPTION
Model Name	This displays the model name of your NR2301
FW version	This displays the present firmware version of your NR2301.
SN	This displays the serial number issued by the manufacturer for your NR2301.
MAC	This displays the MAC address of the NR2301.
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 login address	This displays **http://192.168.1.1**. Launch your web browser and go to **http://192.168.1.1** to access the Web Configurator.
User name	This displays the user name of your NR2301.
Password	This displays the password of your NR2301.
Country of origin	This displays where your NR2301 is designed and assembled.
Power Rating	This displays the NR2301's power rating in volts and amperes.
Next	Click this button to display the next screen page.
Back	Click this button to return to the **Menu** list.

PART I
User's Guide

CHAPTER 2
Web Configurator

2.1 Introduction

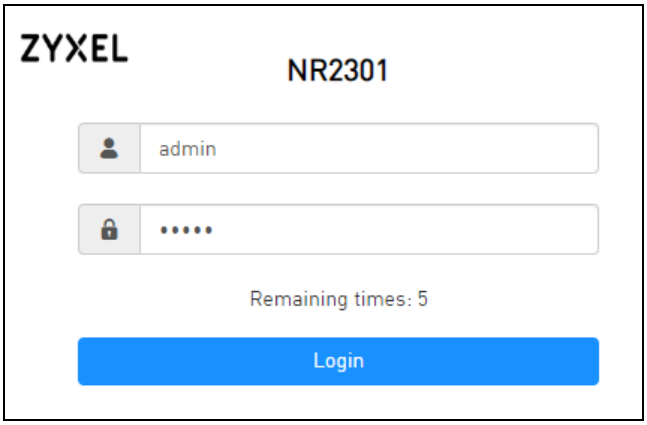
The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

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

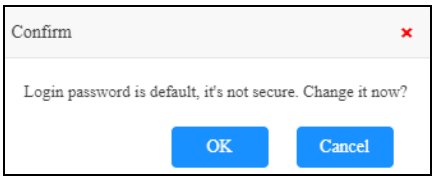
- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.2 Accessing the Web Configurator

1. Use the included USB cable to connect your NR2301 to a computer (refer to the Quick Start Guide).
2. Make sure your computer has an IP address in the same subnet as the NR2301. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See your computer help or refer to Section 10.5 on page 112.
3. Launch your web browser. Go to http://192.168.1.1.
4. A login screen displays. To access the administrative Web Configurator and manage the NR2301, type the default username **admin** and password (check the NR2301's **About** screen for the default password (See Chapter 1 on page 14 for more information)) in the login screen and click **Login**. If you have changed the password, enter your password and click **Login**.

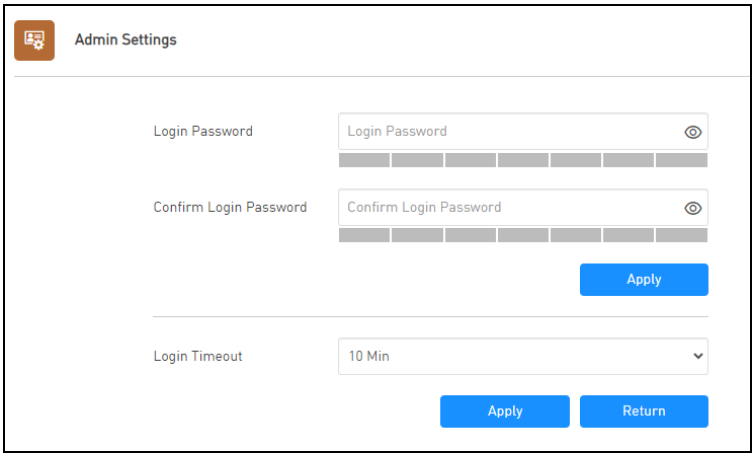


5 The following screen displays if you have not changed your password yet. Click **OK** to set a new password.



6 Enter a new password (at least 5 printable ASCII characters), retype it to confirm, and click **Apply**. The strength of your password is displayed. Use long and complex passwords that are harder to crack to increase the password strength.

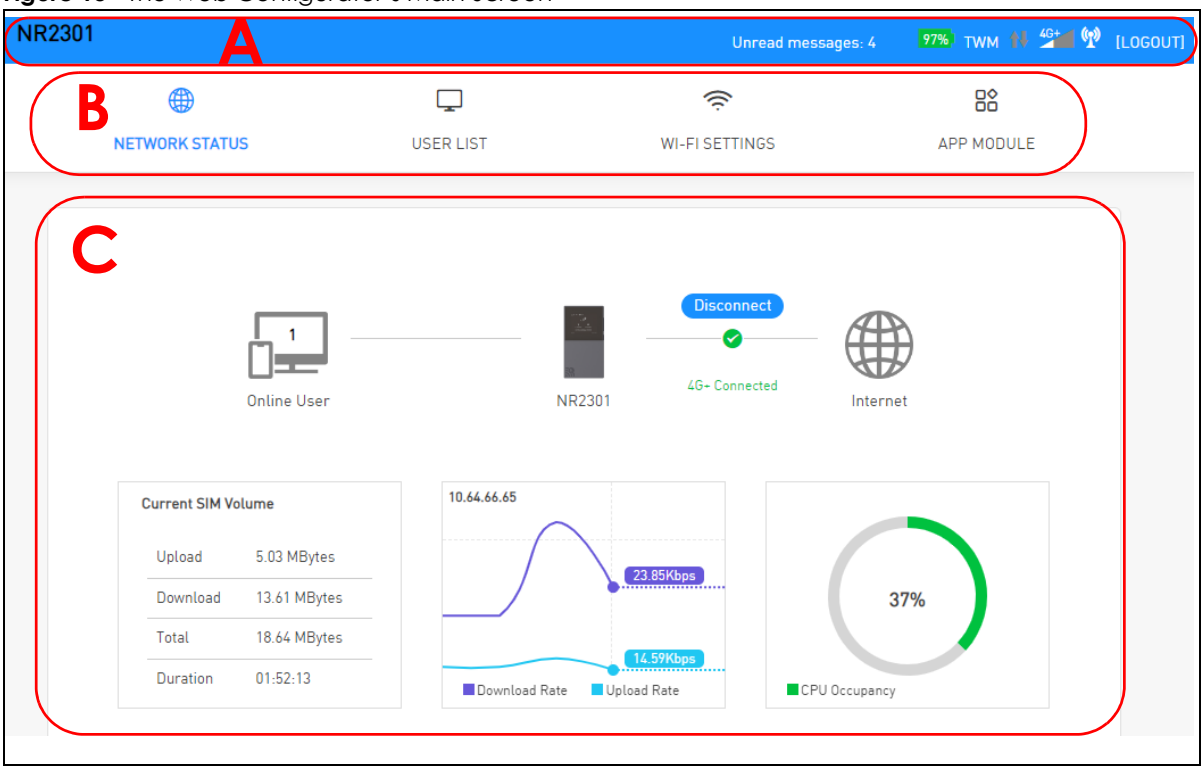
7 You can also set the length of inactive time before the NR2301 automatically logs the user out of the Web Configurator. Click **Apply** to save the change. Click **Return** to exit the screen without saving the changes.



2.3 Navigating the Web Configurator

The following section summarizes how to navigate the Web Configurator.

Figure 13 The Web Configurator's Main Screen



- **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 14 Title Bar

The icons provide the following functions.

Table 8 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Unread messages	This shows the number of unread SMS messages in the NR2301. Click this to go to the **APP MODULE** > **Message**s screen to read the messages.
Battery 100%	The shows the battery status.
ISP TWM	This shows the name of the ISP (Internet Service Provider) of the SIM card that the NR2301 is using.
No SIM No SIM	This shows when no SIM card is detected by the NR2301.
Transmission	This shows when the NR2301 is receiving/transmitting data to/from the Internet.
Signal Strength 4G+	This shows the current signal strength to the mobile network. The icon is grayed out if the mobile data connection is not up.

Table 8 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
WiFi	This shows whether the NR2301's WiFi network is active.
LOGOUT	Click this to log out from the NR2301's Web Configurator.

2.3.2 The Main Window

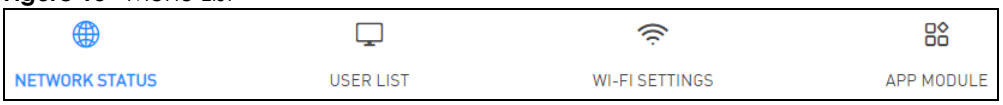
The main window displays information and configuration fields. It is discussed in the rest of this document.

After you log in the **Status** screen is displayed. See Chapter 4 on page 38 for more information about the **Status** screen.

2.3.3 Menu List

Use the **Menu** list to open screens to configure NR2301 features.

Figure 15 Menu List



The following table introduces the menus.

Table 9 Menus Summary

LINK	TAB	DESCRIPTION
NETWORK STATUS		Use this screen to view the network status of the NR2301 and devices connected to it.
USER LIST	Online Users	Use this screen to view and configure clients that are currently connected to the NR2301.
	Offline Users	Use this screen to view and configure clients that were connected to the NR2301 previously.
	Allow/Forbidden Users	Use this screen to view and add clients that are allowed/denied access to the NR2301.
	MAC Filter Mode	Use this screen to configure the NR2301's MAC filter mode.
WI-FI SETTINGS	Wi-Fi Settings	Use this screen to enable and configure the 2.4G/5G WiFi settings and security.
	Guest Wi-Fi	Use this screen to enable and configure the guest WiFi settings and security.
	Advanced Settings	Use this screen to configure a period of time after which the NR2301 automatically turns off its WiFi network.

Table 9 Menus Summary (continued)

LINK	TAB	DESCRIPTION
APP MODULE	Status	Use this screen to view the NR2301'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 NR2301's network information.
	Network Settings	Use this screen to configure the NR2301's network, APN, and roaming settings.
	Network Operators	Use this screen to view available PLMNs and select your preferred network.
	DHCP	Use this screen to configure DHCP settings on the NR2301.
	Package Settings	Use this screen to set up a limited allowance of data on the NR2301.
	Firewall	Use these screens to configure IP and URL filters, port forward, port trigger, UPnP, remote management, and DMZ.
	IP Filter	Use this screen to configure IP filter settings to block clients from accessing specific Internet services.
	URL Filter	Use this screen to configure URL filtering settings to block the users on your network from accessing certain web sites.
	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 NR2301's trigger port settings.
	Port Filter	Use this screen to enable and create firewall rules to block unwanted traffic.
	UPnP	Use this screen to enable or disable UPnP on the NR2301.
	Remote	Use this screen to allow or forbid WAN users from pinging or configuring the NR2301.
	DMZ Settings	Use this screen to enable DMZ on the NR2301.
	VPN	Use this screen to configure VPN client settings on the NR2301.
	Messages	Use this screen to view and manage SMS messages on the NR2301.
	PIN Settings	Use this screen to enable PIN code authentication on the NR2301.
	Admin Settings	Use this screen to configure the NR2301's password and timeout settings.
	Update	Use these screens to display the current firmware version and update new firmware to the NR2301.
	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 NR2301.
	Configuration Backup	Use this screen to backup and restore the configuration or reset the factory defaults to your NR2301.
	Device Reboot	This screen allows you to reboot the NR2301 without turning the power off. You can also set a schedule to reboot the NR2301
	Diagnosis	Use this screen to check the WiFi and status of the NR2301.
	WPS	Use this screen to configure and use WPS.
	DDNS	Use this screen to set up dynamic DNS.
	VPN Passthrough	Use this screen to enable or disable L2TP, IPSec, and PPTP on the NR2301.
	Power Save	Use this screen to configure the NR2301's sleep mode.

CHAPTER 3
Tutorials

3.1 Overview

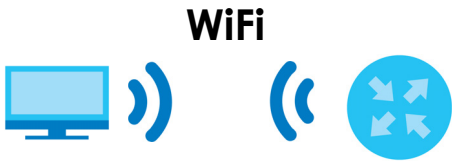
This chapter shows you how to use the NR2301's various features.

- WiFi Network Setup
- MAC Filter
- Device Maintenance

3.2 WiFi Network Setup

In this example, you want to set up a WiFi network so that you can use your notebook or other devices like a smart phone to connect to the NR2301 (for configuration).

Figure 16 NR2301's Configuration Through WiFi Connection



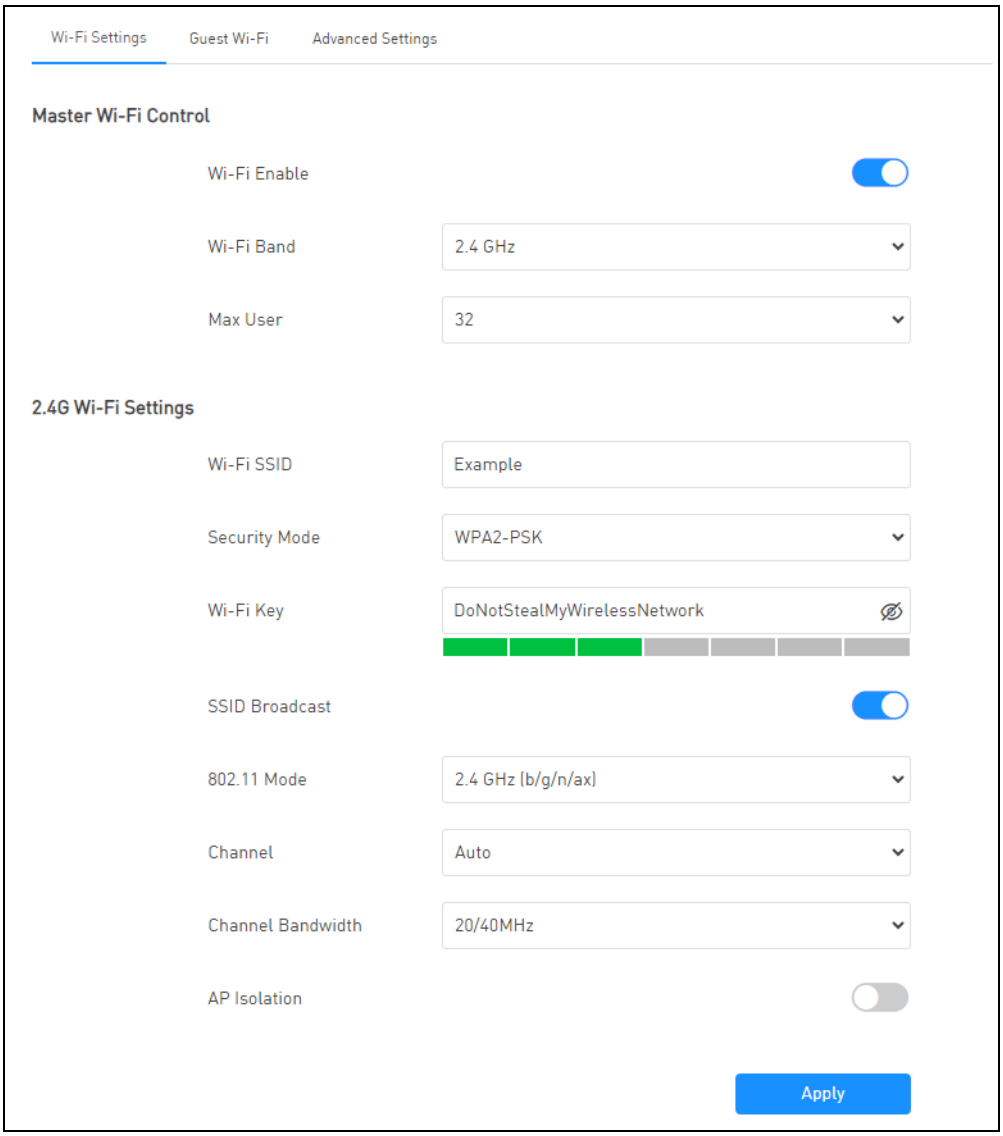
Log into the NR2301's Web Configurator as described in Chapter 2 on page 22.

3.2.1 Changing Security on a WiFi Network

This example changes the settings of a WiFi network to the following:

SSID	Example
WiFi 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 WiFi band. Select **WPA2-PSK** as the security mode. Configure the screen using the provided parameters. Click **Apply**.



You can now use the WPS feature to establish a WiFi connection between your notebook or other devices and the NR2301 (see Section 3.2.2 on page 28).

3.2.2 Connecting to the NR2301's WiFi Network Using WPS

This section shows you how to connect a WiFi device to the NR2301's WiFi network using WPS. WPS (WiFi 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:

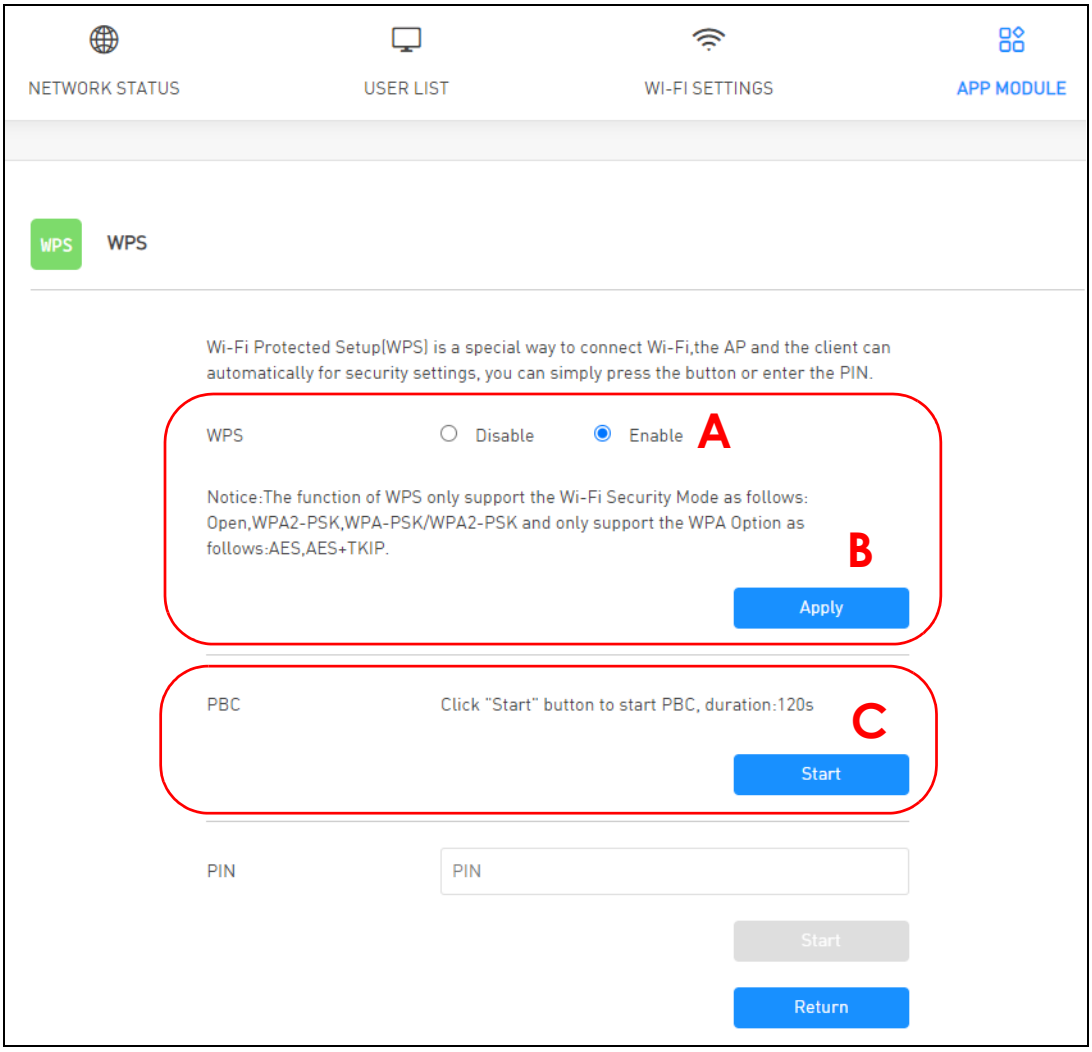
- **PBC (Push Button Configuration)** – Connect to the WiFi network by pressing a button. See Section 3.2.2.1 on page 29. This is the simplest method.
- **PIN** – Connect to the WiFi network by entering a PIN (Personal Identification Number) from a WiFi-enabled device in the NR2301's Web Configurator. See Section 3.2.2.2 on page 31. This is the more secure method, because one device can authenticate the other.

3.2.2.1 WPS Push Button Configuration (PBC)

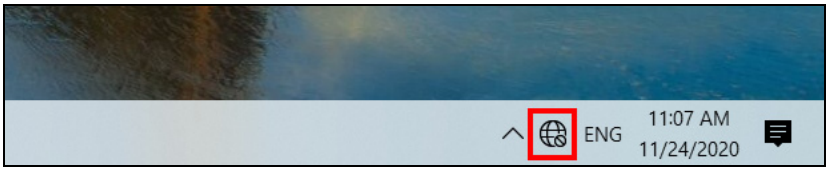
This example shows how to connect to the NR2301's WiFi network from a notebook computer running Windows 10.

1 Make sure that your NR2301 is turned on, and your notebook is within range of the NR2301's WiFi signal.

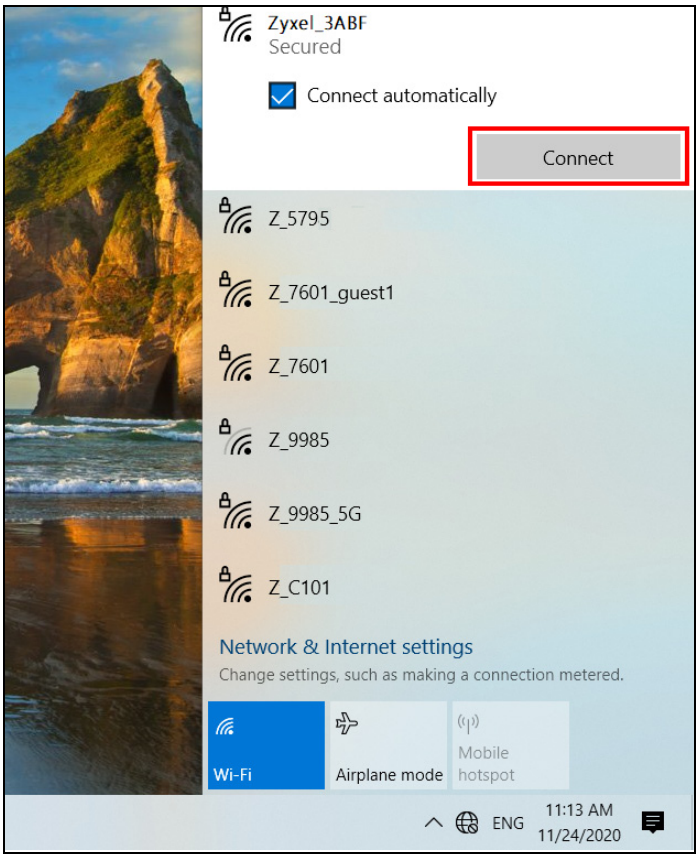
2 Log into the NR2301's Web Configurator, and then go to the **APP MODULE** > **WPS** screen. Enable **WPS** (A) and click **Apply** (B). Then click **Start** in the **PBC** section (C).



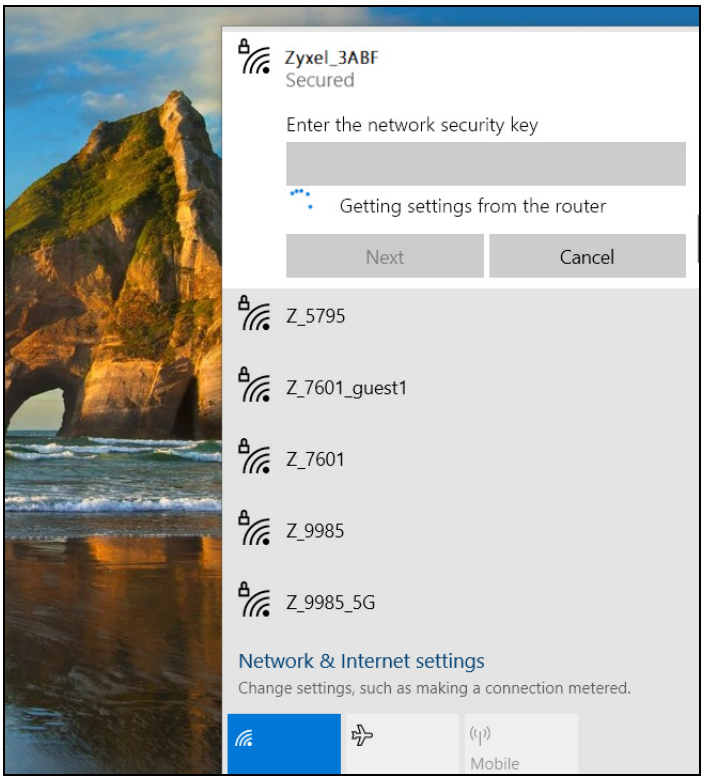
3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



4 Locate the WiFi network of the NR2301. Then click **Connect**.



The NR2301 sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".

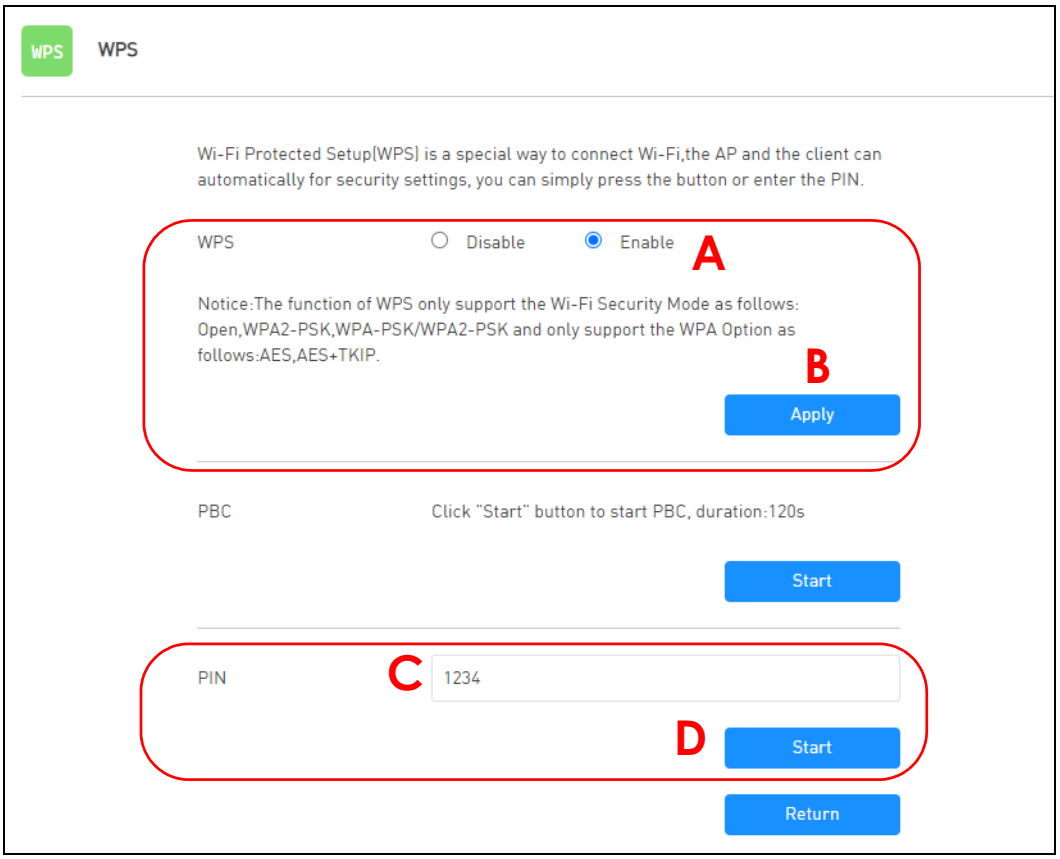


The WiFi device is then able to connect to the WiFi network securely.

3.2.2.2 WPS PIN Configuration

The WPS PIN (Personal Identification Number) method is a more secure version of WPS, used by WiFi-enabled devices such as printers. To use this connection method, you need to log into the NR2301's Web Configurator.

1. Enable WiFi on the device you want to connect to the WiFi network. Then, note down the WPS PIN in the device's WiFi settings.
2. Log into NR2301'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 WiFi device in the **PIN** field (C) and then click **Start** (D).



4 Within 2 minutes, enable WPS on the WiFi device.

The NR2301 authenticates the WiFi device using the PIN, and then sends the WiFi network settings to the device using WPS. This process may take up to 2 minutes. The WiFi device is then able to connect to the WiFi network securely.

3.3 MAC Filter

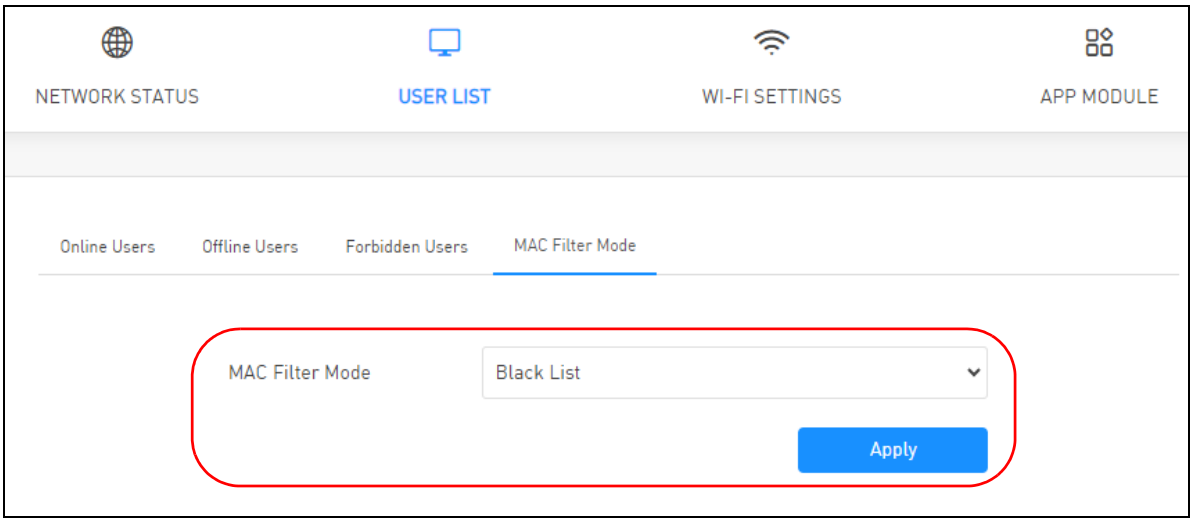
This section shows you how to configure a MAC filter blacklist rule.

3.3.1 Configuring a Blacklist

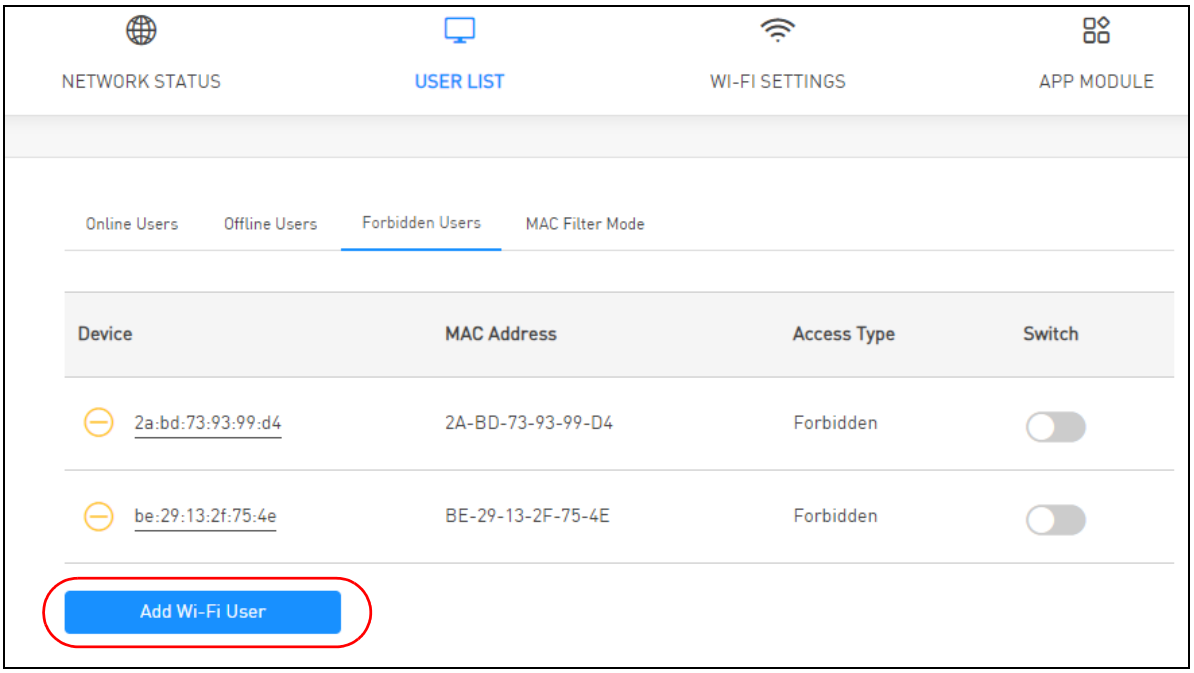
You can configure a blacklist on the NR2301 to block specified devices from accessing the NR2301.

1 Log into NR2301's Web Configurator, and then go to the **USER LIST** > **MAC Filter Mode** screen.

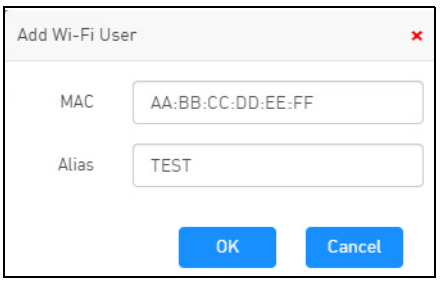
2 Select **Black List** from the **MAC Filter Mode** field and then click **Apply**.



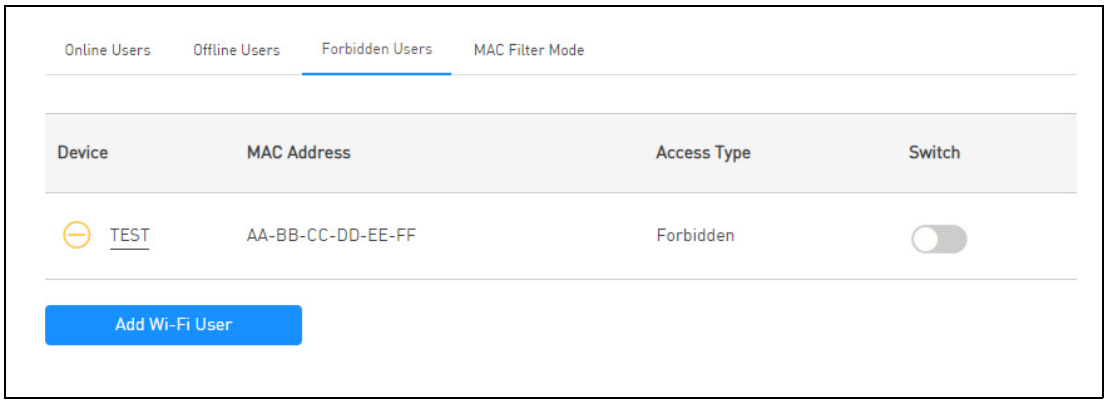
3 Open the **USER LIST** > **Forbidden Users** screen. Click the **Add Wi-Fi User** button.



4 Enter the MAC address and name of the device that you want to block access to the NR2301 in the pop-up screen. Click **Apply**.



5 This device is now added to the blacklist and cannot access the NR2301. If you want to allow it to access the NR2301, turn the switch button on .



3.4 Device Maintenance

This section shows you how to upgrade device firmware, back up the device configuration and restore the device to its previous or default settings.

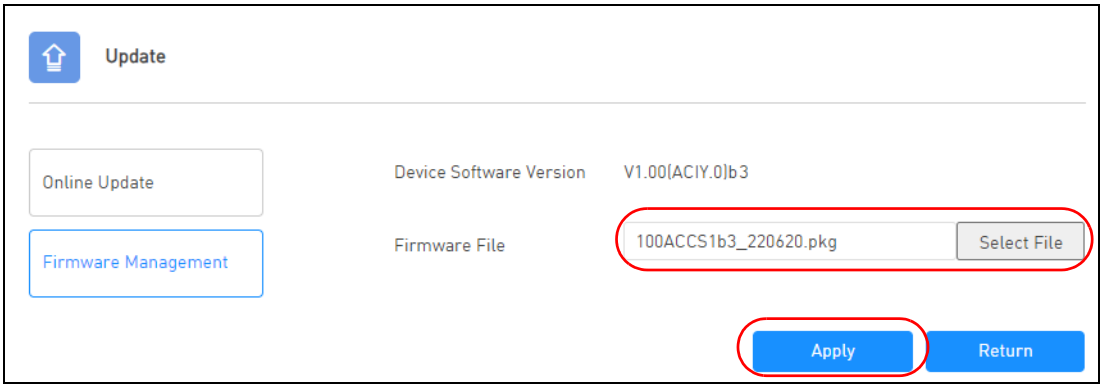
3.4.1 Manually Upgrading the Firmware

Upload the router firmware to the NR2301 for feature enhancements.

1 If you want to upgrade the firmware manually, you can download the correct firmware file from the download library at the Zyxel website. Note the model code for your device. Unzip the file.

2 Go to the **APP MODULE** > **Update** > **Firmware Management** screen.

3 Click **Select File** and select the file with a ".pkg" extension to upload. Click **Apply**.



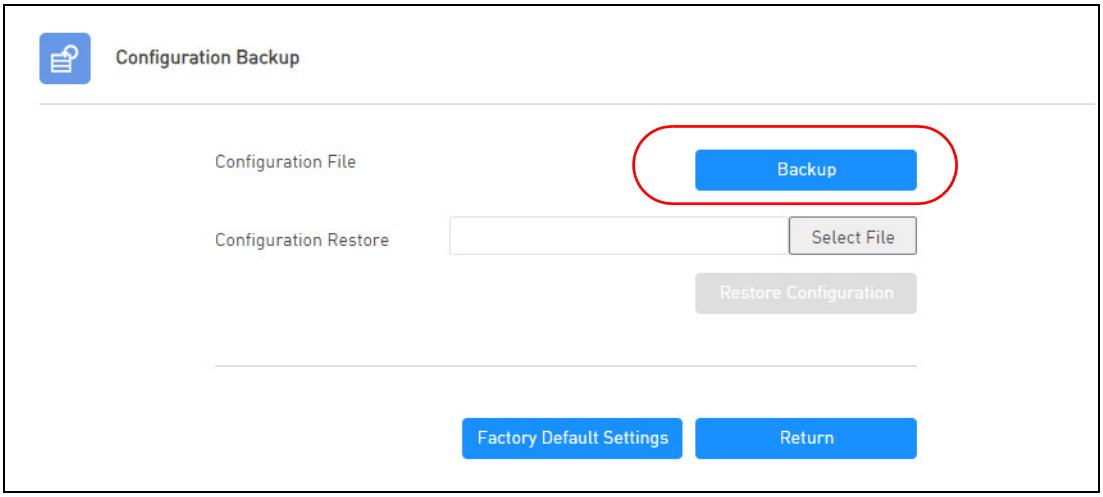
4 This process may take up to several minutes to finish. After several minutes, log in again and check your new firmware version in the **Device Software Version** field.

3.4.2 Backing up the Device Configuration

Back up a configuration file allows you to return to your previous settings.

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

2 Click **Backup** to save the NR2301's configuration file with a ".bin" extension to your computer.

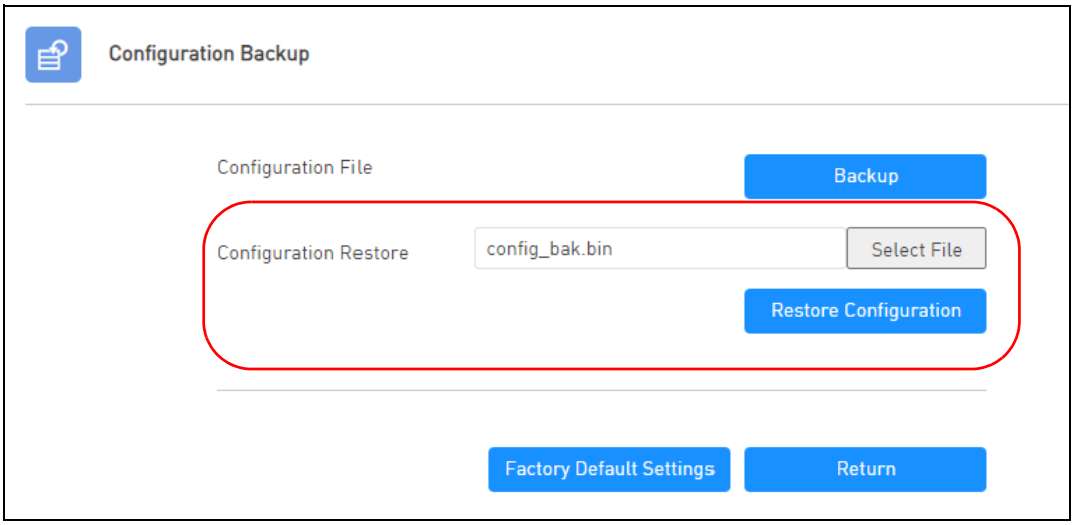


3.4.3 Restoring the Device Configuration

This section shows you how to restore a previously-saved configuration file from your computer to your NR2301.

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

2 In the **Configuration Restore** field, click **Select File**, and then select the configuration file with a ".bin" extension that you want to upload. Click **Restore Configuration**.



3 The NR2301 automatically restarts after the configuration file is successfully uploaded. Wait for one minute before logging into the NR2301 again.

PART II
Technical Reference

CHAPTER 4
Network Status

4.1 Overview

Use the **NETWORK STATUS** screen to check status information about the NR2301.

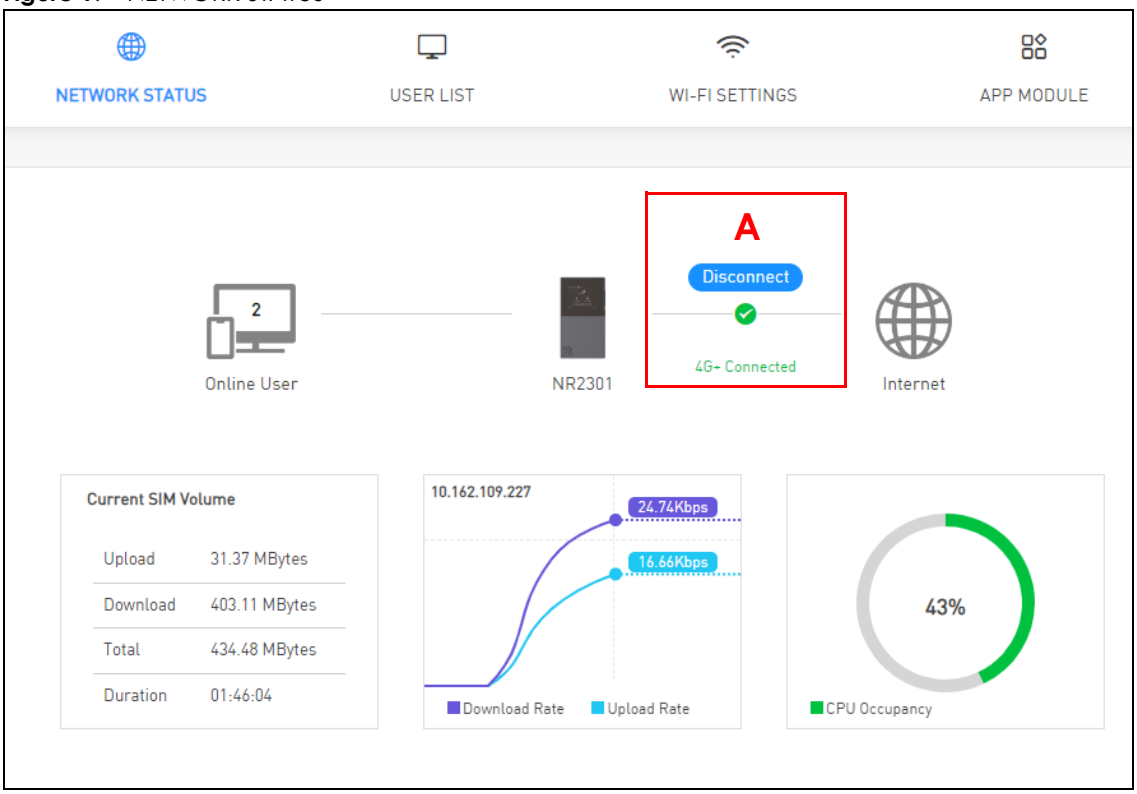
4.2 NETWORK STATUS

This screen is the first thing you see when you log into the NR2301. You can also click **NETWORK STATUS** from the **Menu** list to access this screen.

The **NETWORK STATUS** screen displays the NR2301's WAN network type, connection status, connection mode, status, SIM card information, traffic statistics, and WAN IP address.

If the **Connect Mode** in the **APP MODULE** > **Network Settings** screen is set to manual, you can manually connect or disconnect the NR2301's mobile network connection (see **A** in the screen below). See Chapter 8 on page 60 for more information.

Figure 17 NETWORK STATUS



The following table describes the labels in this screen.

Table 10 NETWORK STATUS

LABEL	DESCRIPTION
Online User	This field displays the number of clients that are currently connected to the NR2301. Click this to go to the **USER LIST** > **Online Users** screen to view information of the clients and configure them. See Section 5.2 on page 40 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 NR2301's traffic download rate.
Upload Rate	This field displays the NR2301's traffic upload rate.
CPU Occupancy	This field displays what percentage of the NR2301's processing ability is currently used. When this percentage is close to 100%, the NR2301 is running at full load, and the throughput is not going to improve anymore.

CHAPTER 5
User List

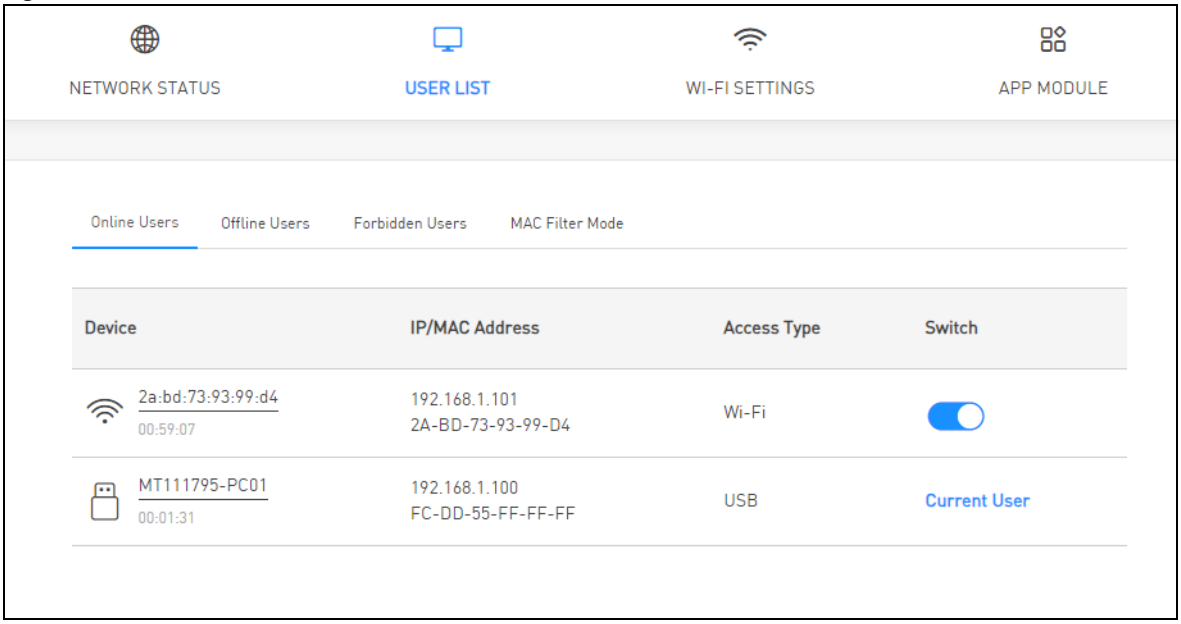
5.1 Overview

Use the **USER LIST** screens screen to view and manage the NR2301's clients. You can also allow or deny clients' access to the NR2301.

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 NR2301.

Figure 18 USER LIST > Online Users



The following table describes the labels in this screen.

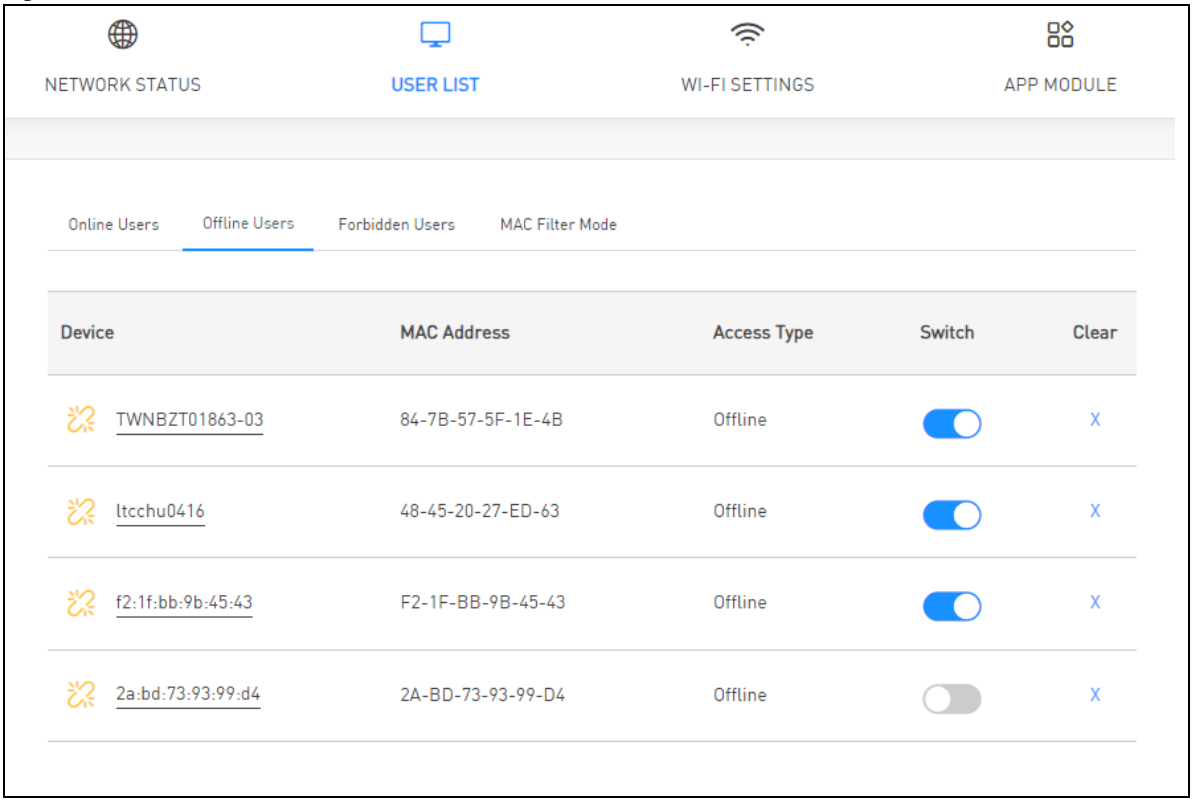
Table 11 USER LIST > Online Users

LABEL	DESCRIPTION
Device	This field displays the name of the client that is currently connected to the NR2301. Its connected time duration is also displayed. 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. 
IP/MAC Address	This field displays the LAN IP address and MAC address of a client currently connected to the NR2301.
Access Type	This field displays whether the client is connected to the NR2301 by **Wi-Fi** or **USB**.
Switch	When the switch button is on , the client is connected to the NR2301. Turn the switch button off to disable the connection of the client to the NR2301. 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 NR2301 again without entering the SSID and password. Note: You cannot disable the connection of the device that you are currently using to access the NR2301. **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 NR2301 previously.

Figure 19 USER LIST > Offline Users



The following table describes the labels in this screen.

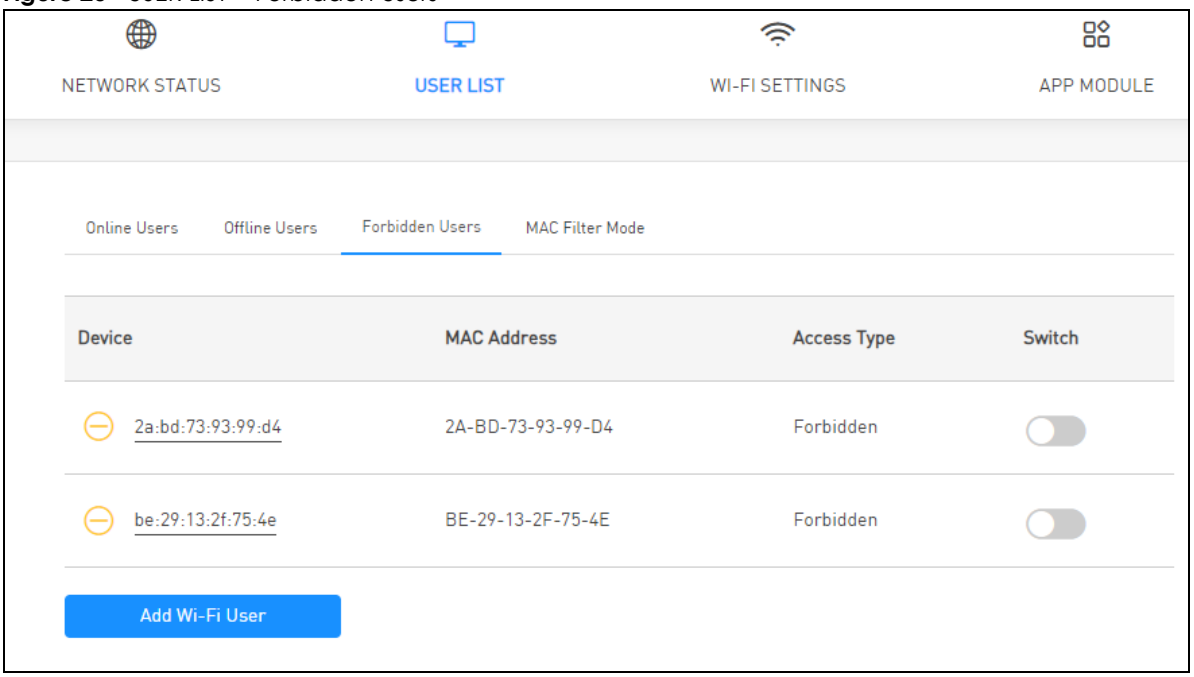
Table 12 USER LIST > Offline Users

LABEL	DESCRIPTION
Device	This field displays the name of the client that was connected to the NR2301 previously. 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. 
MAC Address	This field displays the MAC address of the client that was connected to the NR2301 previously.
Access Type	This field displays **Offline** since the client is not connected to the NR2301 currently.
Switch	Turn the switch button on to allow the connection of the client to the NR2301. If the client connects to the NR2301, 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 NR2301 again without entering the SSID and password. If the switch button is off , the client is not allowed to connect to the NR2301. 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 NR2301.

Figure 20 USER LIST > Forbidden Users

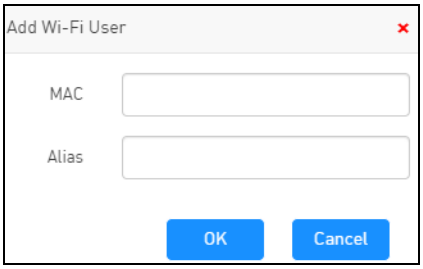


The following table describes the labels in this screen.

Table 13 USER LIST > Forbidden Users

LABEL	DESCRIPTION
Device	This field displays the name of the client that is not allowed to access the NR2301. 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. 
MAC Address	This field displays the MAC address of the client that is forbidden to access the NR2301.
Access Type	This field displays **Forbidden** since the client is forbidden access to the NR2301.

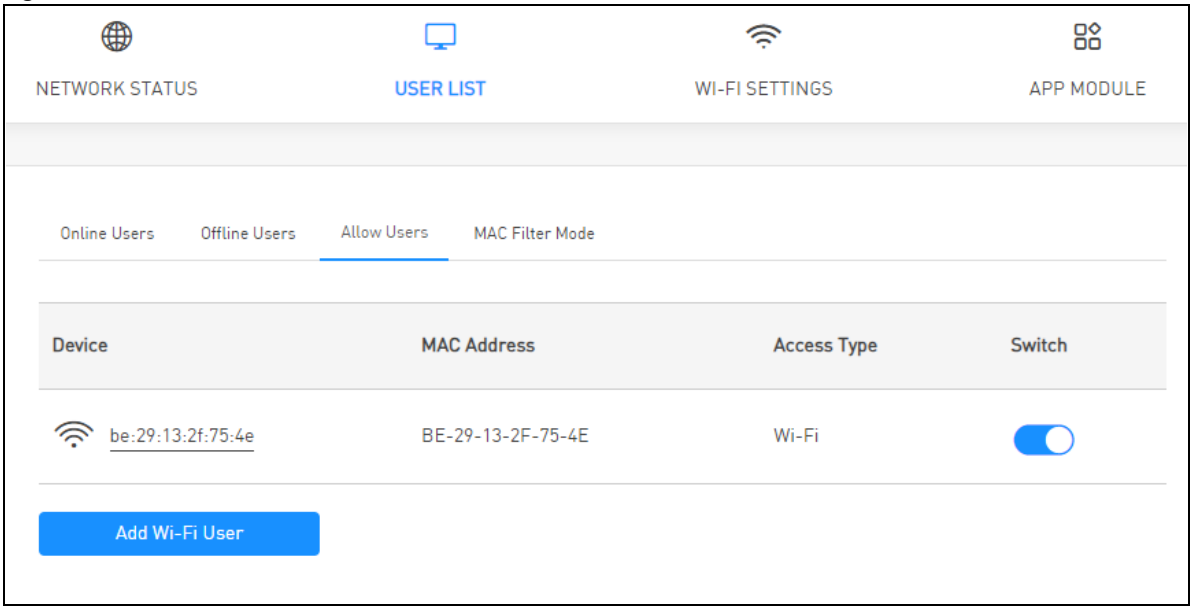
Table 13 USER LIST > Forbidden Users (continued)

LABEL	DESCRIPTION
Switch	The switch button is off so that the client is not allowed to connect to the NR2301. Turn the switch button on to allow the connection of the client to the NR2301. If the client connects to the NR2301, it will be added to the **Online Users** screen. If the client is not connected to the NR2301, 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. 

5.5 Allow Users

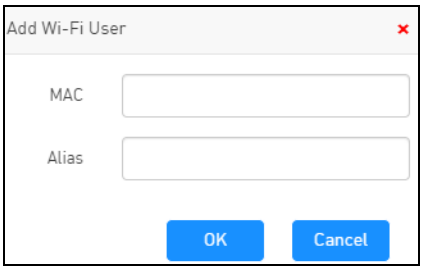
If the **MAC Filter Mode** is set to **White List** in the **MAC Filter Mode** screen, this screen is displayed by clicking **USER LIST** > **Allow Users**. Use this screen to view and add clients that are allowed access to the NR2301.

Figure 21 USER LIST > Allow Users



The following table describes the labels in this screen.

Table 14 USER LIST > Allow Users

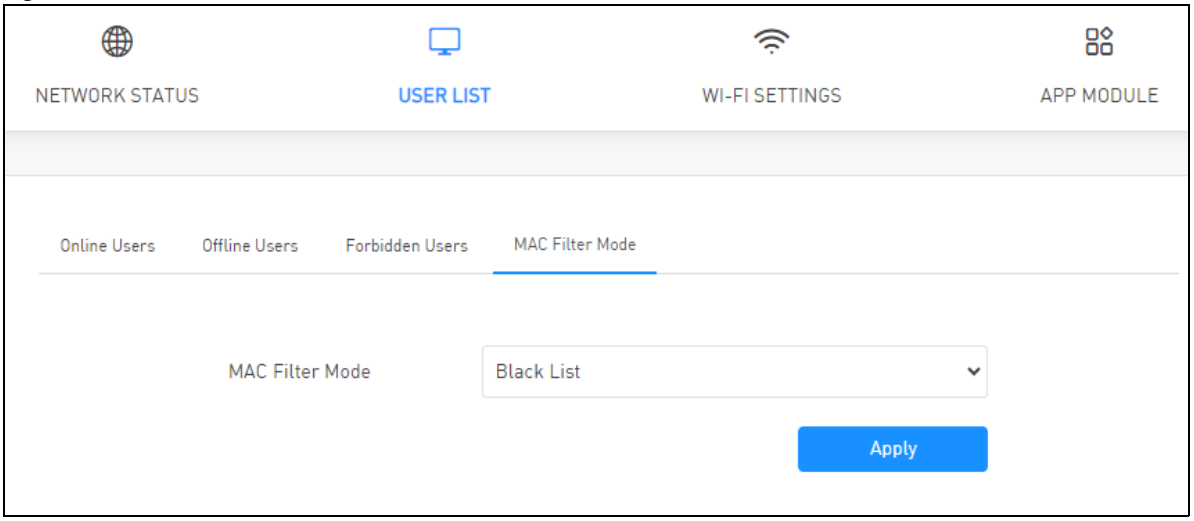
LABEL	DESCRIPTION
Device	This field displays the name of the client that is allowed to access the NR2301. If you want to change the name of the device, click on its name and enter the new name in the **Alias** field of the following screen. Click **OK** to save the change. 
MAC Address	This field displays the MAC address of the client that is allowed to access the NR2301.
Access Type	This field displays how the client connects to the NR2301 (**Wi-Fi**).
Switch	The switch button is on to allow the connection of the client to the NR2301. If the client is connecting to the NR2301, it will be added to the **Online Users** screen. If the client is not connecting to the NR2301, it will be added to the **Offline Users** list. Turn the switch button off to forbid the client to connect to the NR2301.
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. 

5.6 MAC Filter Mode

This screen allows you to configure the NR2301 to allow or deny specific devices from accessing the NR2301. 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 NR2301's MAC filter mode. Click **USER LIST** > **MAC Filter Mode**. The screen appears as shown.

Figure 22 USER LIST > MAC Filter Mode



The following table describes the labels in this screen.

Table 15 USER LIST > MAC Filter Mode

LABEL	DESCRIPTION
MAC Filter Mode	Define the MAC filter action for the NR2301. Select **Black List** to block the devices listed in the **Forbidden Users** screen from accessing the NR2301. Devices not listed will be allowed to access the NR2301. See Section 5.4 on page 43 for more information. Select **White List** to permit the devices listed in the **Allow Users** screen to access the NR2301. Devices not listed will be denied access to the NR2301. See Section 5.5 on page 44 for more information.
Apply	Click **Apply** to save your changes back to the NR2301.

CHAPTER 6
WI-FI SETTINGS

6.1 Overview

This chapter discusses how to configure the WiFi network settings in your NR2301.

6.1.1 What You Need to Know

Every WiFi network must follow these basic guidelines.

- Every WiFi client in the same WiFi network must use the same SSID.

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

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

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

WiFi Security Overview

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

MAC Address Filter

Every WiFi 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 WiFi 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 WiFi clients are allowed or not allowed to use the WiFi network. If a WiFi client is allowed to use the WiFi network, it still has to have the correct settings (SSID, channel, and security). If a WiFi client is not allowed to use the WiFi 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 WiFi network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized WiFi client. Then, they can use that MAC address to use the WiFi network.

WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a WiFi 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 WiFi network using WPS in the Chapter 9 on page 102.

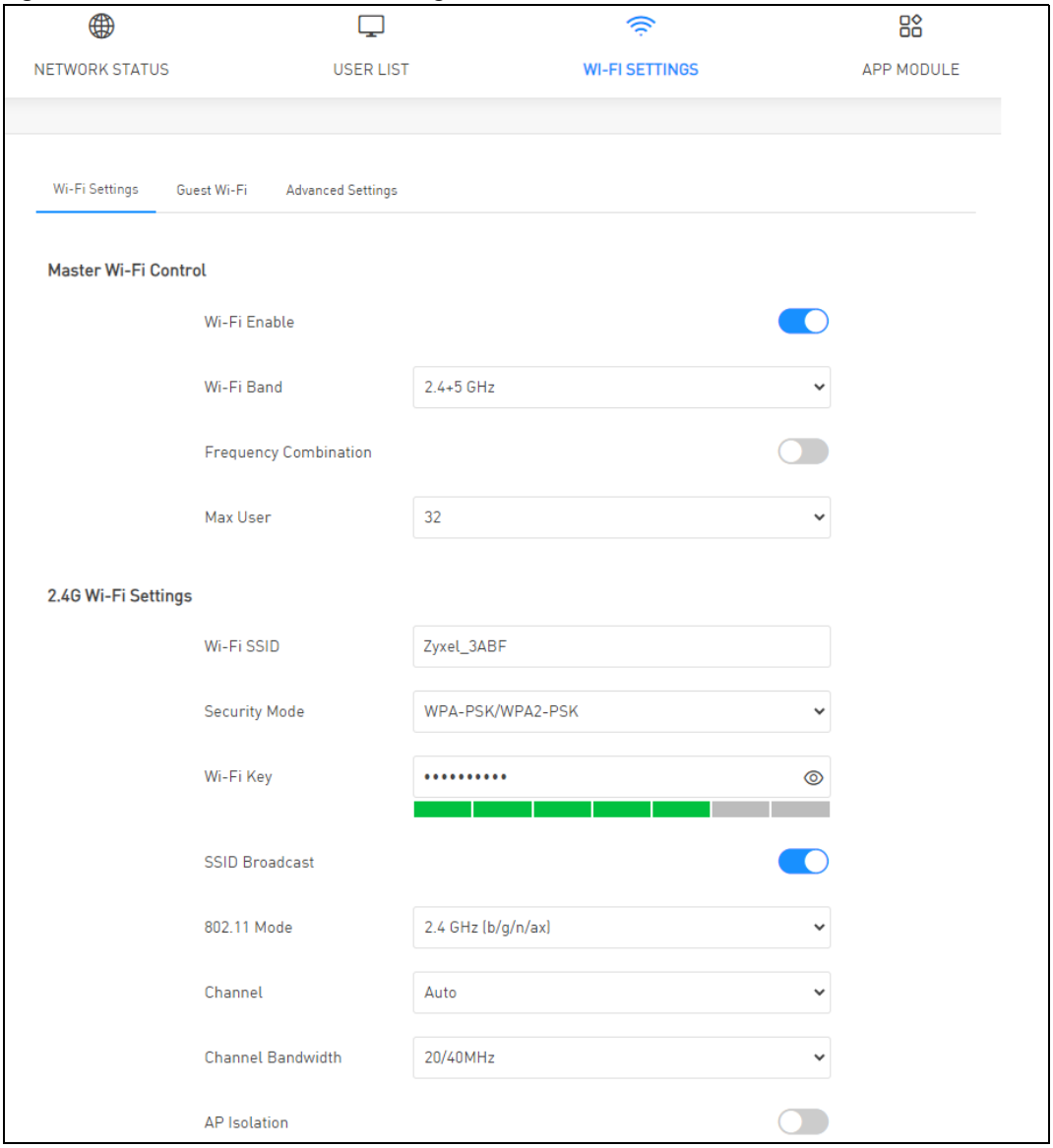
6.2 The Wi-Fi Settings Screen

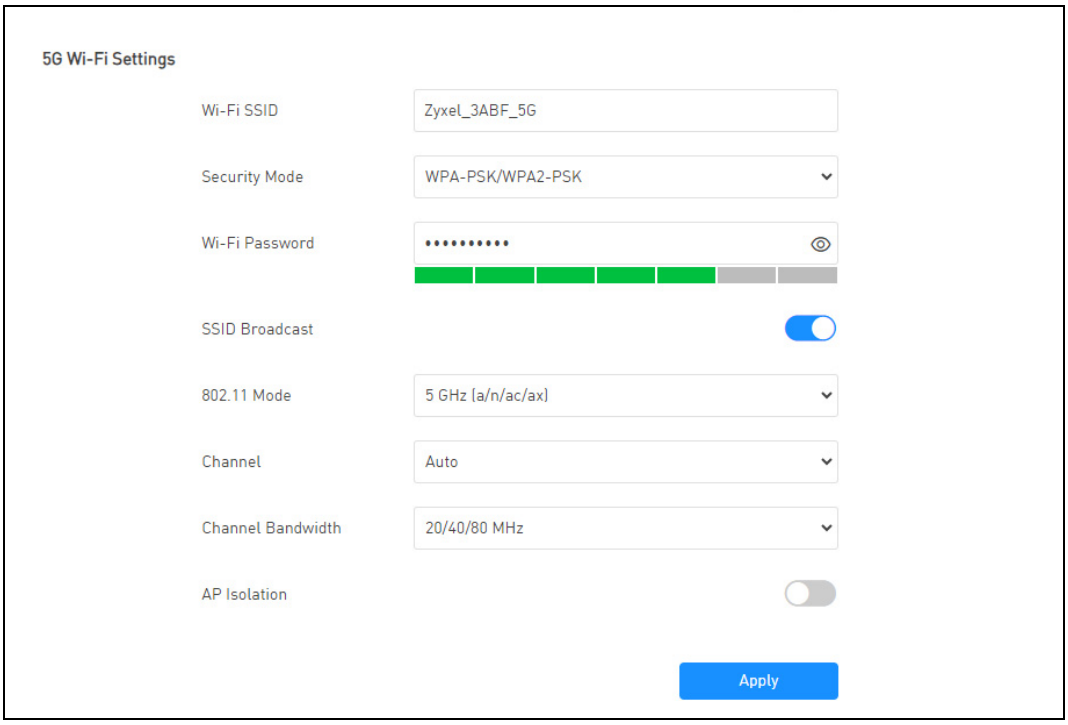
Use this screen to enable the wireless LAN, enter the SSID, and configure security and other WiFi settings.

Note: If you are configuring the NR2301 from a device connected to the wireless LAN and you change the NR2301's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply** to confirm. You must then change the WiFi settings of your device to match the NR2301's new settings.

To access this screen, click **WI-FI SETTINGS** > **Wi-Fi Settings**.

Figure 23 WI-FI SETTINGS > Wi-Fi Settings





The following table describes the labels in this screen.

Table 16 WI-FI SETTINGS > Wi-Fi Settings

LABEL	DESCRIPTION
Master Wi-Fi Control	
Wi-Fi Enable	Turn the switch button on to activate WiFi on the NR2301.
Wi-Fi Band	Select whether the NR2301 uses the 2.4 GHz WiFi band, the 5 GHz WiFi band, or both.
Frequency Combination	Turn the switch button on to have the 2.4G and 5G wireless LAN share the same SSID. Wireless clients can use the same wireless LAN network name to connect to either the 2.4G or 5G WiFi network.
Max User	Specify the maximum number of clients (up to 32) 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 WiFi client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Security Mode	Select **WPA2-PSK**, **WPA-PSK/WPA2-PSK**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE** to add security on this WiFi network. WiFi clients must support one of the selected security modes and use the same WiFi key (password) to connect to the WiFi network. Or you can select **Open** to use no security and allow any client to connect to this network without authentication. The WPA-PSK (WiFi 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 NR2301 and a connecting client at the beginning of a WiFi session. Note: WPS can be used only when the security mode is set to **Open**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK**.

Table 16 WI-FI SETTINGS > Wi-Fi Settings (continued)

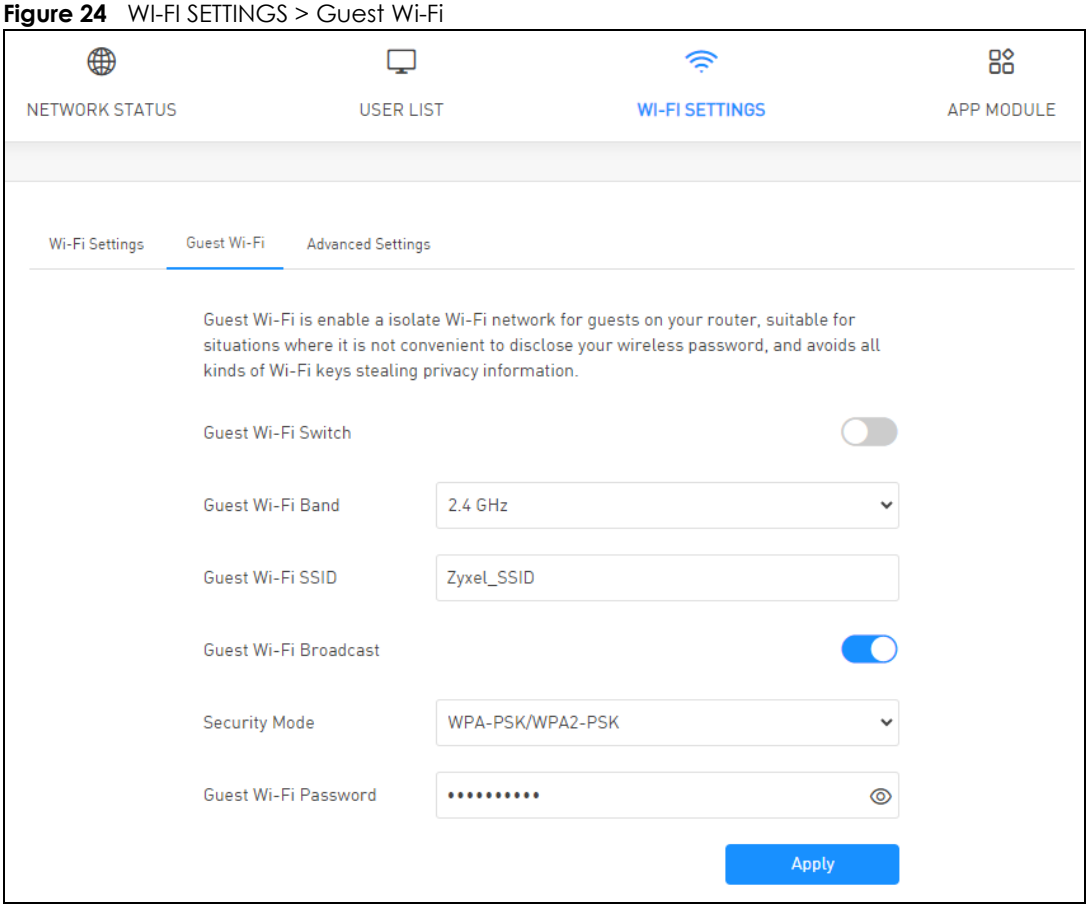
LABEL	DESCRIPTION
Wi-Fi Key	Unless the **Security Mode** is set to **Open**, you need to configure a WiFi key for this WiFi network. Enter a WiFi key from 8 to 63 case-sensitive keyboard characters. The strength of your password is displayed below.
SSID Broadcast	Turn the switch button on to show the 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: • **2.4 GHz (b)**: allows either IEEE 802.11b compliant WLAN devices to associate with the NR2301. In this mode, all WiFi devices can only transmit at the data rates supported by IEEE 802.11b. • **2.4 GHz (b/g)**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NR2301. The NR2301 adjusts the transmission rate automatically according to the WiFi standard supported by the WiFi devices. • **2.4 GHz (b/g/n)**: allows IEEE802.11b, IEEE802.11g, and IEEE802.11n compliant WLAN devices to associate with the NR2301. The transmission rate of your NR2301 might be reduced. • **2.4 GHz (b/g/n/ax)**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the NR2301. The transmission rate of your NR2301 might be reduced. Select one of the following for the 5G network: • **5 GHz (a)**: allows only IEEE 802.11a compliant WLAN devices to associate with the NR2301. • **5 GHz (a/n)**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NR2301. The transmission rate of your NR2301 might be reduced. • **5 GHz (a/n/ac)**: allows both IEEE802.11a, IEEE802.11n, and IEEE802.11ac compliant WLAN devices to associate with the NR2301. The transmission rate of your NR2301 might be reduced. • **5 GHz (a/n/ac/ax)**: allows both IEEE802.11a, IEEE802.11n, IEEE802.11ac, and IEEE802.11ax compliant WLAN devices to associate with the NR2301. The transmission rate of your NR2301 might be reduced.
Channel	Set the operating frequency/channel depending on your particular region. Select **Auto** for the NR2301 to automatically choose the channel with the least interference. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.
Channel Bandwidth	Select the WiFi channel width the NR2301 uses. 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. Because not all devices support 40 MHz and/or 80 MHz channels, select **20/40/80 MHz** to allow the NR2301 to adjust the channel bandwidth automatically. **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 WiFi 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 WiFi signal. Select **20 MHz** if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding.
AP Isolation	If the switch button is turned on , the clients in the NR2301's network are blocked from connecting to each other directly.
Apply	Click **Apply** to save your changes back to the NR2301.

6.3 Guest Wi-Fi

The **Guest Wi-Fi** screen allows you to enable and configure guest WiFi network settings on the NR2301. This is an isolated network for guest clients accessing the WiFi network to secure the WiFi keys and settings of the NR2301. Clients using the guest WiFi network cannot access the NR2301's Web Configurator. Up to 10 clients may connect to the guest WiFi network at the same time. The maximum number of regular and guest clients connecting to the NR2301 is 32.

To access this screen, click **WI-FI SETTINGS** > **Guest Wi-Fi**.

Figure 24 WI-FI SETTINGS > Guest Wi-Fi



The following table describes the labels in this screen.

Table 17 WI-FI SETTINGS > Guest Wi-Fi

LABEL	DESCRIPTION
Guest Wi-Fi Switch	Turn the switch button on to activate the guest WiFi network. Note: When WiFi is disabled on the NR2301, the guest WiFi network cannot be activated.
Guest Wi-Fi Band	Select whether to use **2.4 GHz** or **5 GHz** for the guest WiFi network.
Guest Wi-Fi SSID	The SSID (Service Set IDentity) identifies the Service Set with which a WiFi client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the guest wireless LAN.

Table 17 WI-FI SETTINGS > Guest Wi-Fi (continued)

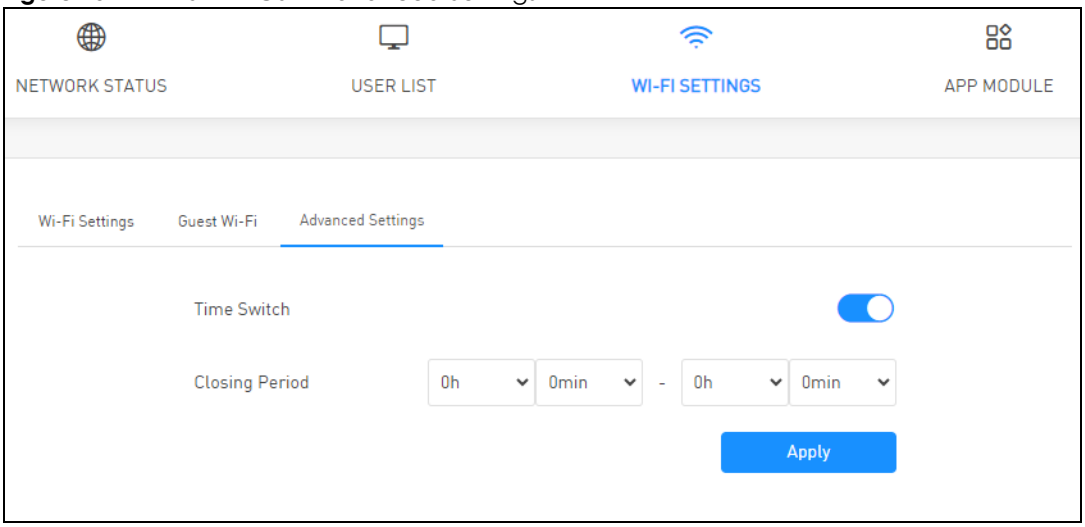
LABEL	DESCRIPTION
Guest Wi-Fi Broadcast	Turn the switch button on to show the guest SSID in the outgoing beacon frame. Turn it off to hide the guest SSID so a station cannot obtain the guest SSID through scanning using a site survey tool.
Security Mode	Select **WPA2-PSK**, **WPA-PSK/WPA2-PSK**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE** to add security on this guest WiFi network. WiFi clients must support one of the selected security modes and use the same WiFi key to connect to the guest wireless network. Or you can select **Open** to use no security and allow any client to connect to the guest network without authentication. The WPA-PSK (WiFi 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 NR2301 and a connecting client at the beginning of a WiFi session. Note: WPS can be used only when the security mode is set to **Open**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK**.
Guest Wi-Fi Password	Type a password the clients need to enter to connect to the guest WiFi network.
Apply	Click **Apply** to save your changes back to the NR2301.

6.4 Advanced Settings

The **Advanced Settings** screen allows you to enable and configure a time schedule to disable the NR2301's WiFi network. The WiFi network is disabled during the configured time period and all clients (including guest WiFi clients) cannot access it. It will be enabled automatically after this time period.

To access this screen, click **WI-FI SETTINGS** > **Advanced Settings**.

Figure 25 WI-FI SETTINGS > Advanced Settings



The following table describes the labels in this screen.

Table 18 WI-FI SETTINGS > Advanced Settings

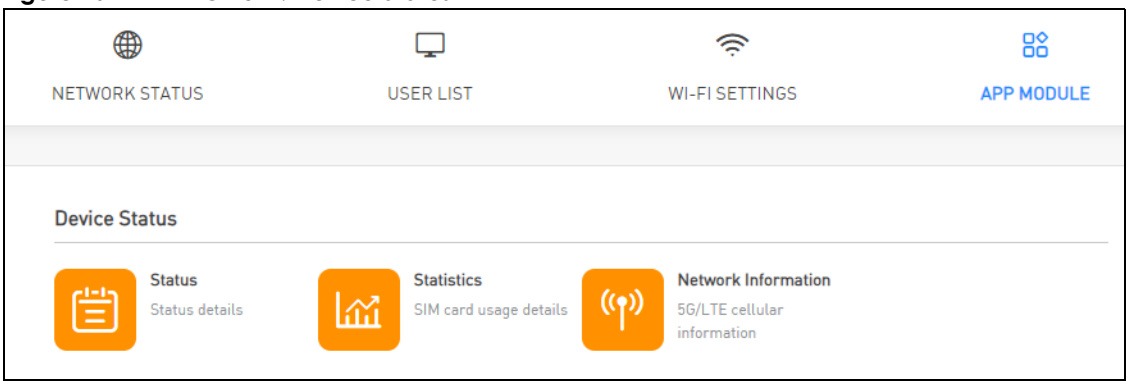
LABEL	DESCRIPTION
Time Switch	Turn the switch button on to activate the schedule for disabling the WiFi network.
Closing Period	Enter the time period in 24-hour format of the schedule. The WiFi network is disabled during the configured time period and all clients (including guest WiFi clients) cannot access it. It will be enabled automatically after this time period.
Apply	Click **Apply** to save your changes back to the NR2301.

CHAPTER 7
Device Status

7.1 Overview

Use the **Device Status** screens to view the NR2301's device status information, network information, and the SIM card usage details.

Figure 26 APP MODULE: Device Status

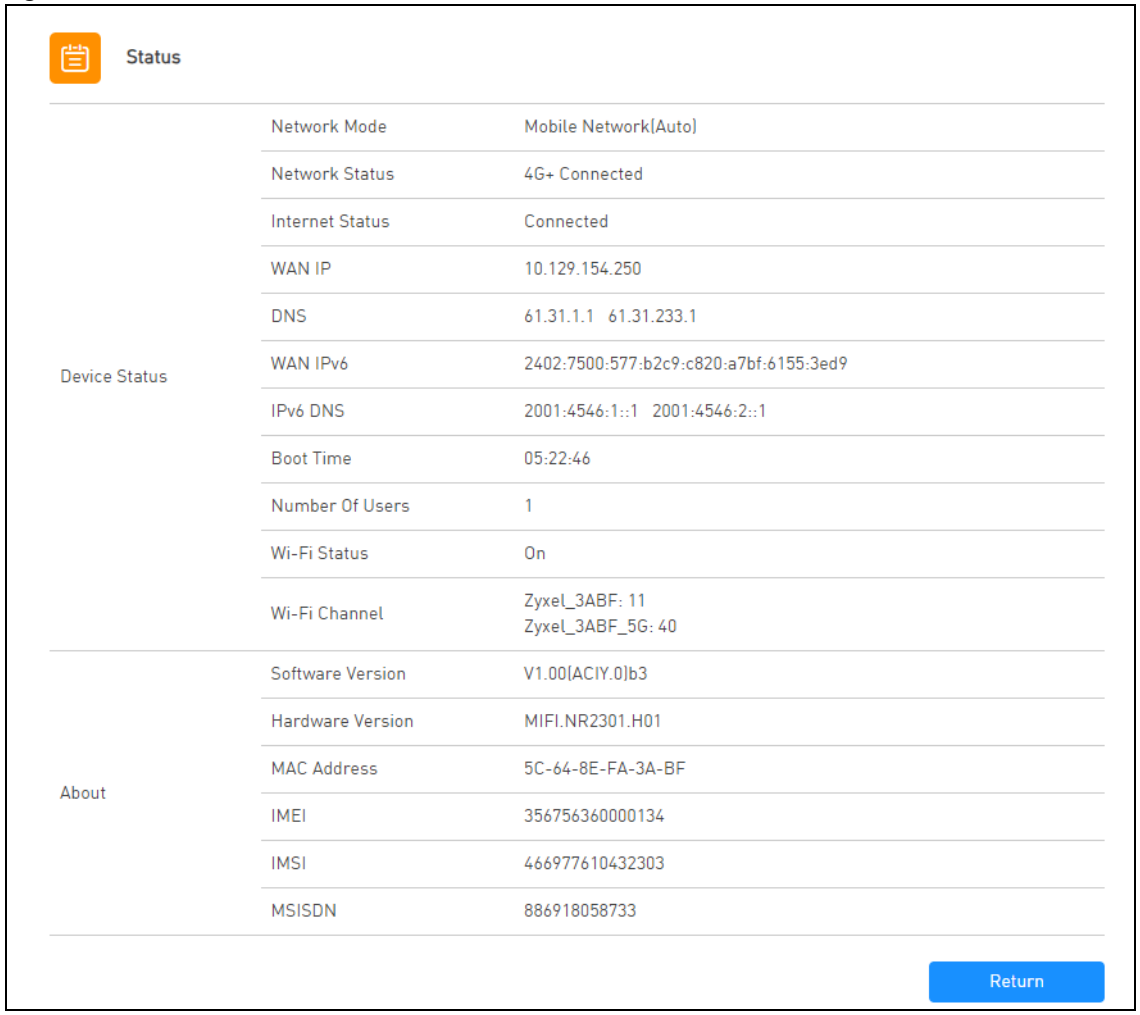


7.2 Status

Use the **Status** screen to check status information about the NR2301.

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

Figure 27 APP MODULE > Status



The following table describes the labels in this screen.

Table 19 APP MODULE > Status

LABEL	DESCRIPTION
Device Status	
Network Mode	This field displays the network mode of the NR2301.
Network Status	This field displays the type of network the NR2301 is using.
Internet Status	This field displays whether the NR2301 is connected to the Internet.
WAN IP	This field displays the current WAN IP address of the NR2301 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 NR2301 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 NR2301.
Wi-Fi Status	This field displays whether WiFi 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 19 APP MODULE > Status (continued)

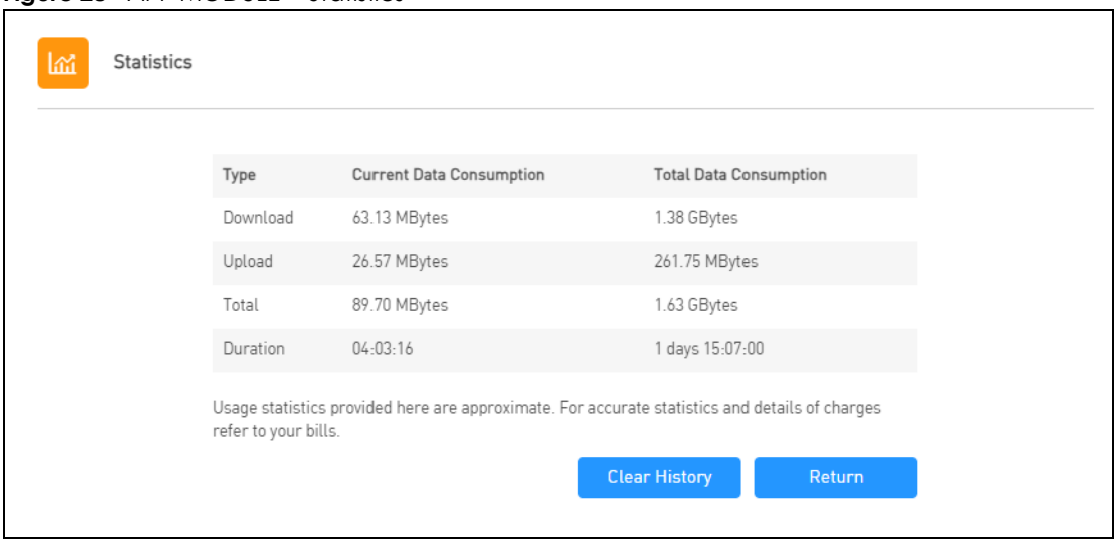
LABEL	DESCRIPTION
Software Version	This field displays the current version of the firmware inside the NR2301.
Hardware Version	This field displays the hardware version of the NR2301.
MAC Address	This field displays the MAC address of the NR2301.
IMEI	This field displays the International Mobile Equipment 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 28 APP MODULE > Statistics



The following table describes the labels in this screen.

Table 20 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 20 APP MODULE > Statistics (continued)

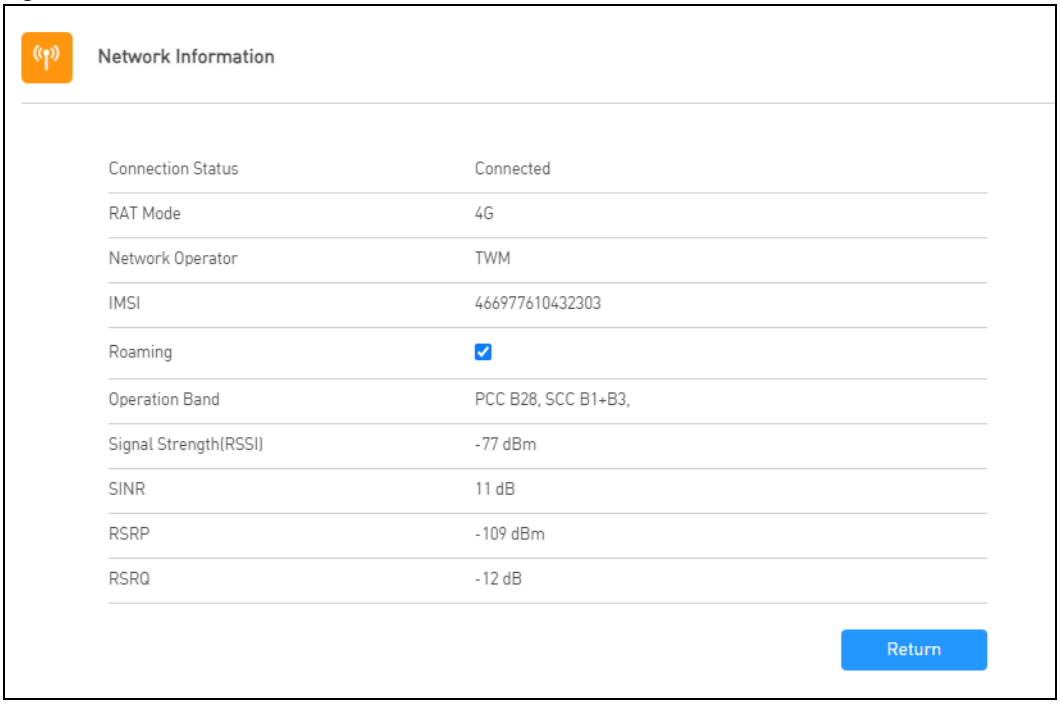
LABEL	DESCRIPTION
Download	This field displays the number of received packets on the SIM card for the current connection session or in total.
Upload	This field displays the number of transmitted packets on the SIM card for the current connection session or in total.
Total	This field displays the total 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 NR2301's network information.

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

Figure 29 APP MODULE > Network Information



The following table describes the labels in this screen.

Table 21 APP MODULE > Network Information

LABEL	DESCRIPTION
Connection Status	This displays whether the NR2301 is connected to the Internet.
RAT Mode	This displays the network mode that the NR2301 used to register with the service provider's mobile network.
Network Operator	This displays the name of the service provider.

Table 21 APP MODULE > Network Information (continued)

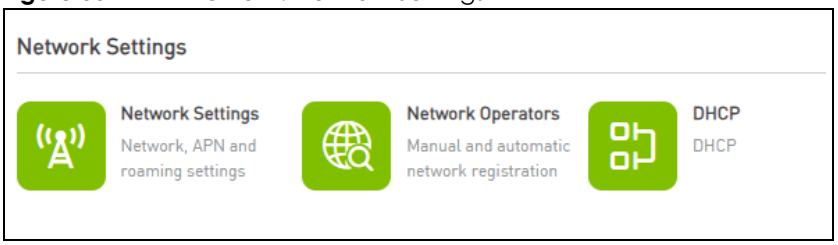
LABEL	DESCRIPTION
IMSI	This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network.
Roaming	This displays whether the NR2301 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 NR2301 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 NR2301's network, APN, roaming, and DHCP settings. You can also view available Public Land Mobile Networks (PLMNs) and select your preferred network.

Figure 30 APP MODULE: Network Settings

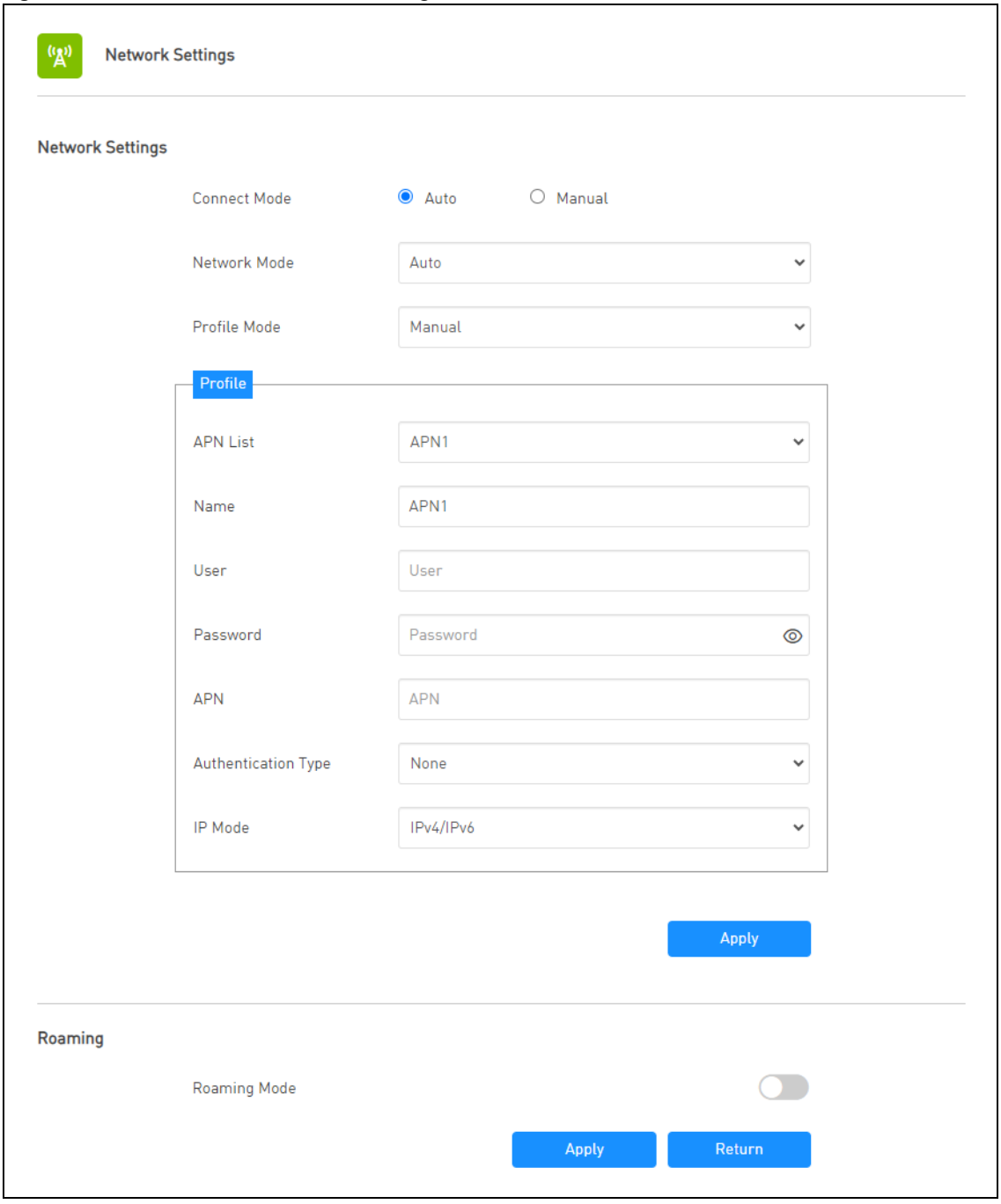


8.2 Network Settings

Use the **Network Settings** screen to configure the NR2301's network, APN, and roaming settings.

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

Figure 31 APP MODULE > Network Settings



The following table describes the labels in this screen.

Table 22 APP MODULE > Network Settings

LABEL	DESCRIPTION
Network Settings	
Connect Mode	Select **Auto** to have the NR2301 connect to the mobile network automatically after it has been restarted or registered. If you select **Manual**, you can manually connect or disconnect the NR2301's mobile network connection in the **NETWORK STATUS** screen. See Chapter 4 on page 38 for more information.

Table 22 APP MODULE > Network Settings (continued)

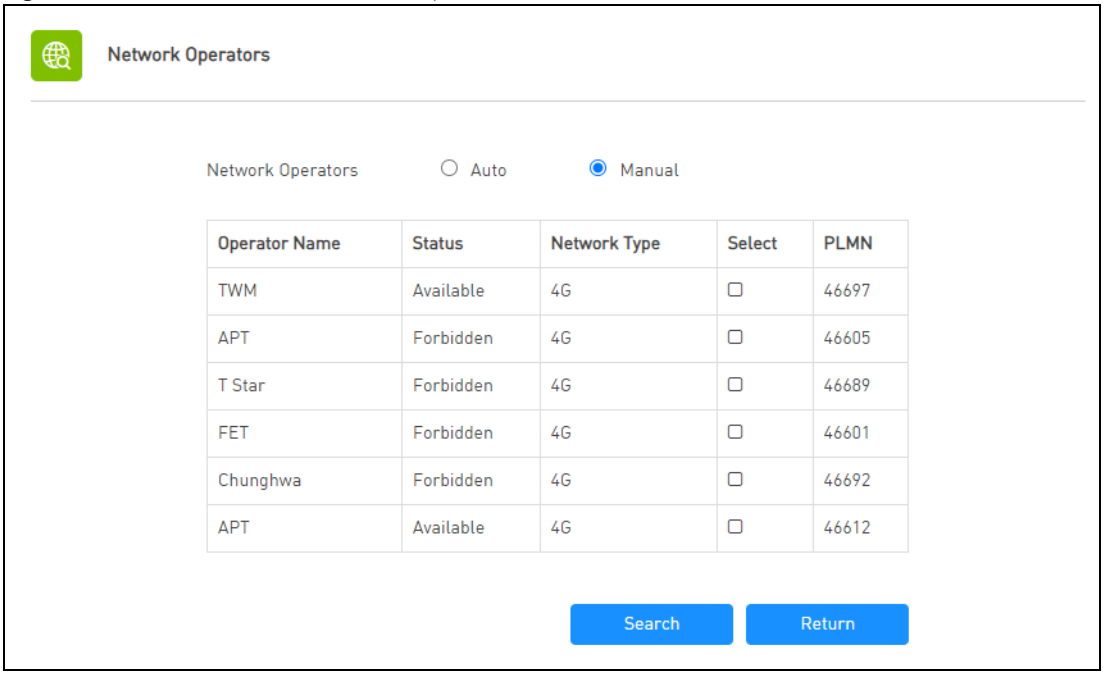
LABEL	DESCRIPTION
Network Mode	Select the type of the network (**5G-SA**, **5G-NSA**, or **4G**) to which you want the NR2301 to connect. Otherwise, select **Auto** to have the NR2301 connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the NR2301 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. Select **Auto** to have the APN information automatically configured. 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	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type 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 NR2301 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 Select an authentication protocol (**PAP**, or **CHAP**) used by the service provider. Otherwise, select **Auto** to have the NR2301 accept either CHAP or PAP.
IP Mode	Select **IPv4/IPv6** to allow the NR2301 to run IPv4 and IPv6 at the same time. Select **IPv4** if you want the NR2301 to run IPv4 only. Select **IPv6** if you want the NR2301 to run IPv6 only.
Apply	Click **Apply** to save your changes back to the NR2301.
Roaming	
Roaming Mode	Turn the switch button on to enable roaming on the NR2301. 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 NR2301 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 back to the NR2301.
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 NR2301 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 32 APP MODULE > Network Operators



The following table describes the labels in this screen.

Table 23 APP MODULE > Network Operators

LABEL	DESCRIPTION
Auto	Select **Auto** to have the NR2301 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 NR2301 is currently connected. This displays **Available** to display other PLMNs available from your ISP. 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 NR2301 establish a connection to the selected mobile network.
PLMN	This shows the PLMN number.
Search	Click **Search** so the NR2301 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.

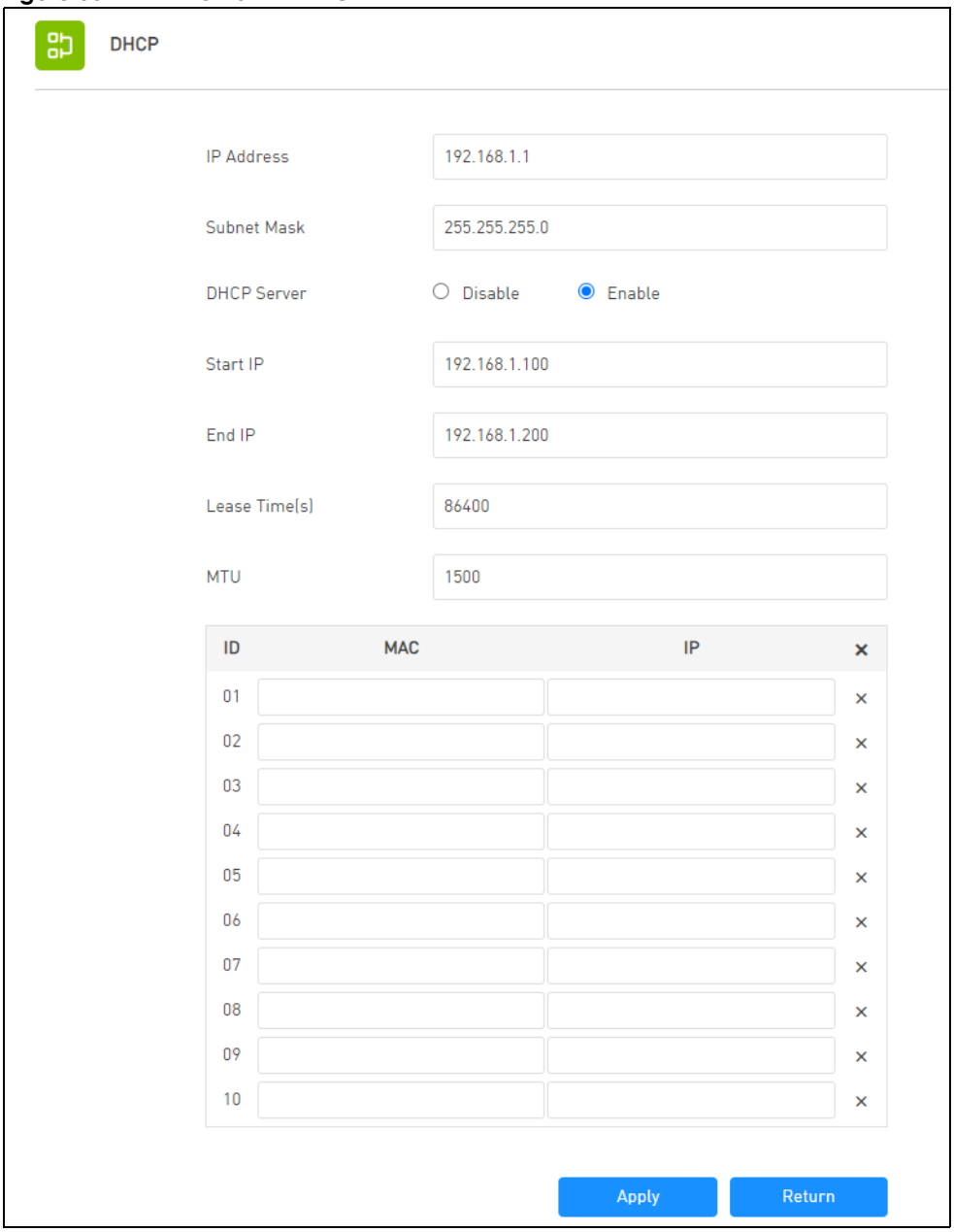
8.4 DHCP

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 NR2301's WLAN as a DHCP server or disable it. When configured as a server, the NR2301 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 NR2301 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.

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

Figure 33 APP MODULE > DHCP



The following table describes the labels in this screen.

Table 24 APP MODULE > DHCP

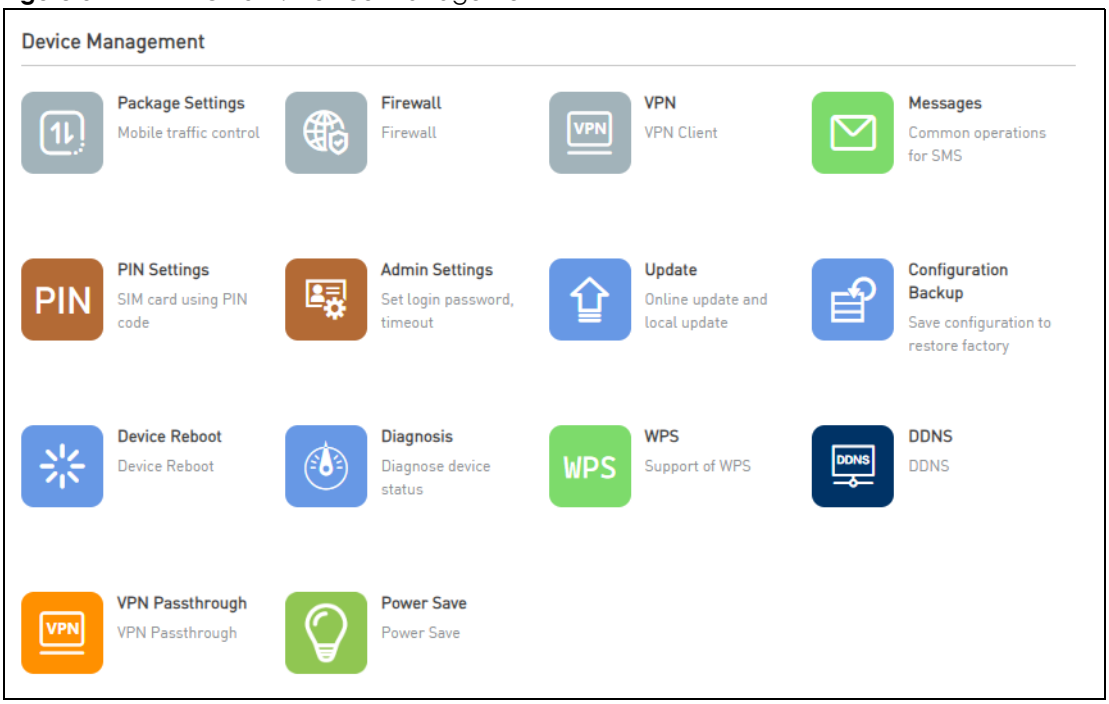
LABEL	DESCRIPTION
IP Address	Enter the LAN IPv4 IP address you want to assign to the NR2301 in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). The NR2301 automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server	Select **Disable** to stop the DHCP server on the NR2301. Select **Enable** to have the NR2301 act as a DHCP server or DHCP relay agent. When configured as a server, the NR2301 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.
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
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	Type the MAC address (with colons) of a computer on your LAN.
IP	Type the LAN IP address of a computer on your LAN.
X	Click the **X** next to an entry to clear it.
Apply	Click **Apply** to save your changes back to the NR2301.
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 NR2301.

Figure 34 APP MODULE: Device Management

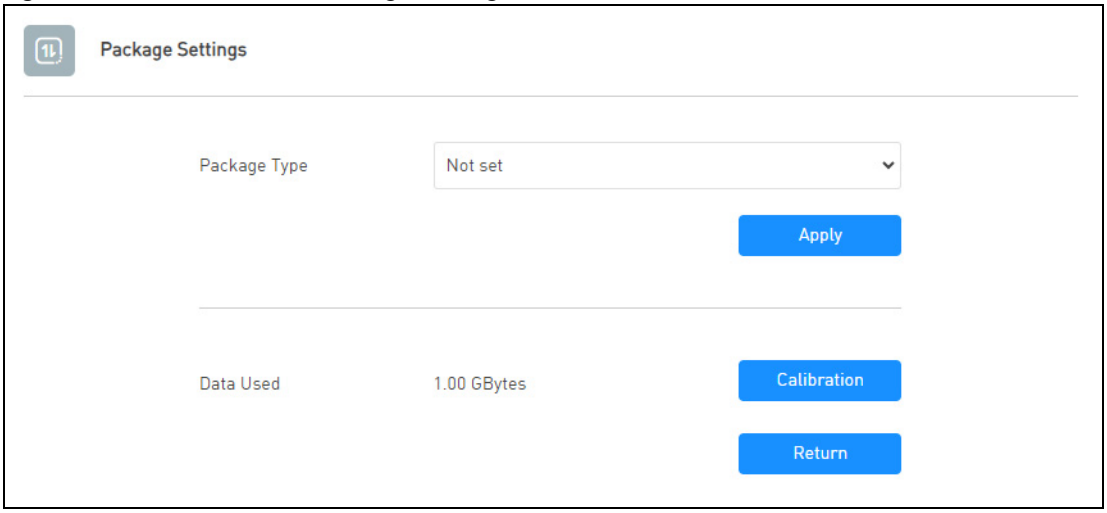


9.2 Package Settings

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 35 APP MODULE > Package Settings: Not set

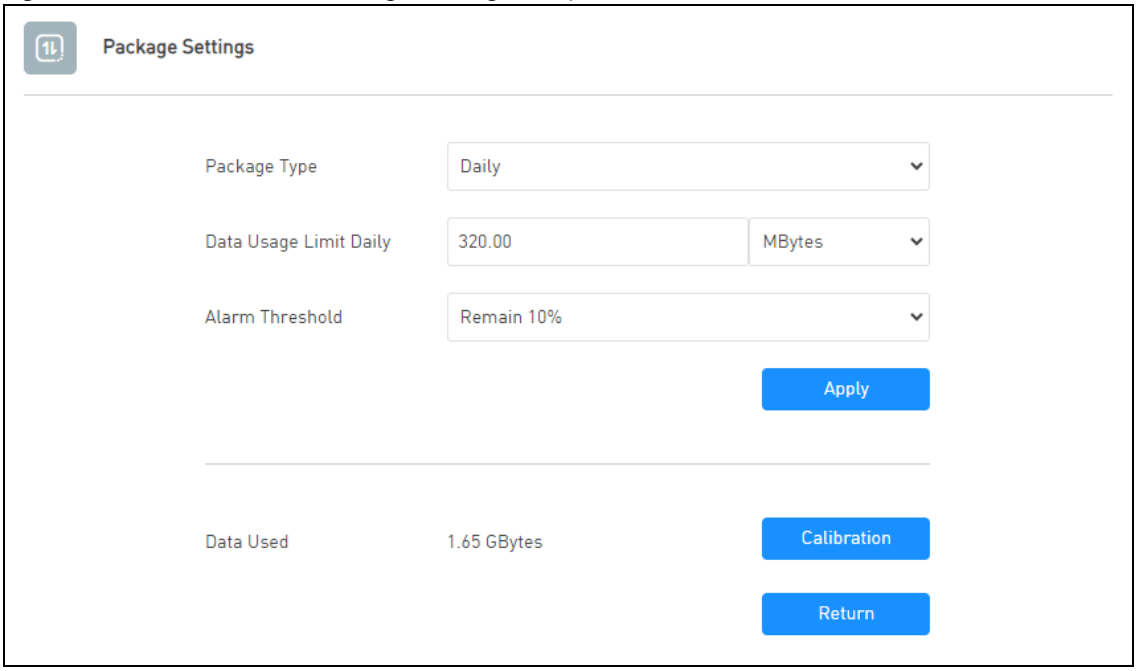


The following table describes the labels in this screen.

Table 25 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 NR2301.
Apply	Click **Apply** to save your changes back to the NR2301.
Data Used	This displays the mobile data used by the NR2301 so far.
Calibration	Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting. 
Return	Click this button to return to the **APP MODULE** list.

Figure 36 APP MODULE > Package Settings: Daily

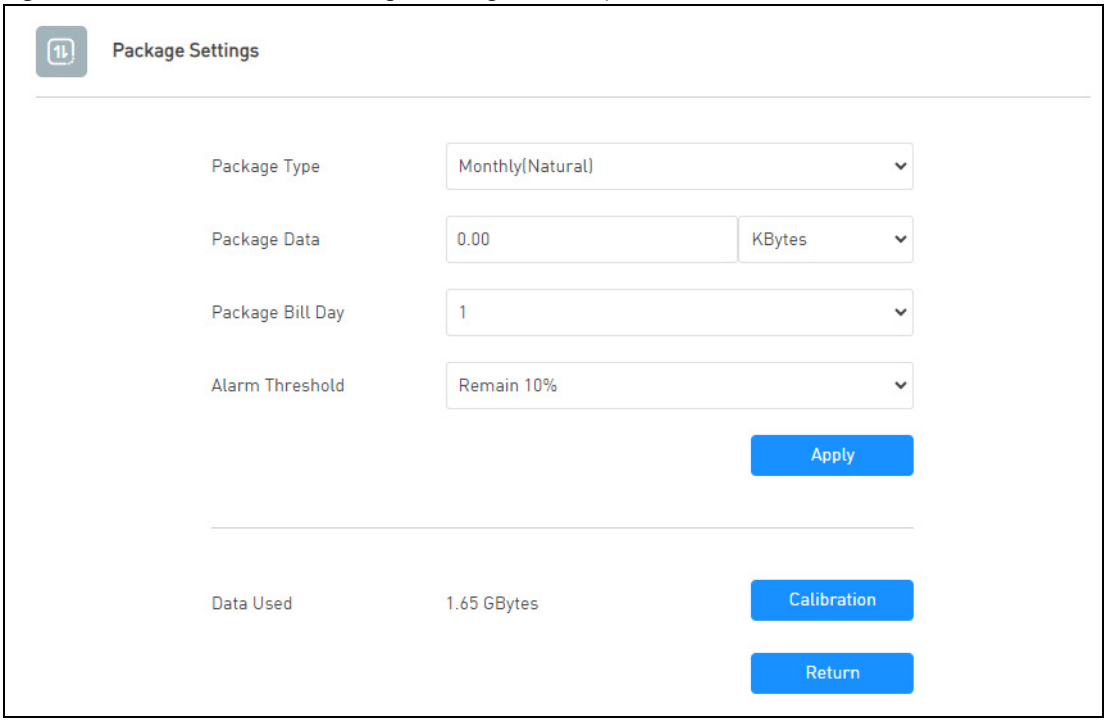


The following table describes the labels in this screen.

Table 26 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 NR2301 has to reach to display a notification on the NR2301's LCD **Home** screen and Web Configurator's **Main** screen.
Apply	Click **Apply** to save your changes back to the NR2301.
Data Used	This displays the mobile data used by the NR2301 so far.
Calibration	Click this to manually set the amount of data used in the following screen and click **Save** to apply the setting. 
Return	Click this button to return to the **APP MODULE** list.

Figure 37 APP MODULE > Package Settings: Monthly

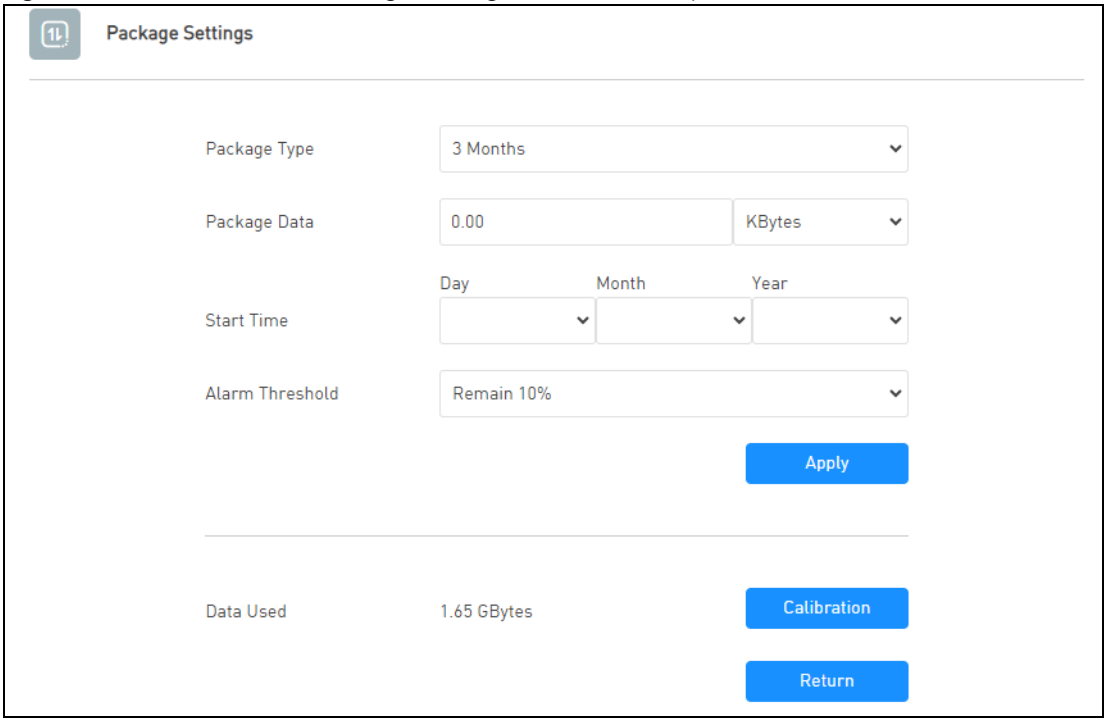


The following table describes the labels in this screen.

Table 27 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 NR2301 restarts calculating the amount of data per month.
Alarm Threshold	Select the percentage of data usage the NR2301 has to reach to display a notification on the NR2301's LCD **Home** screen and Web Configurator's **Main** screen.
Apply	Click **Apply** to save your changes back to the NR2301.
Data Used	This displays the mobile data used by the NR2301 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. 
Return	Click this button to return to the **APP MODULE** list.

Figure 38 APP MODULE > Package Settings: 3 Months/Half year/Year

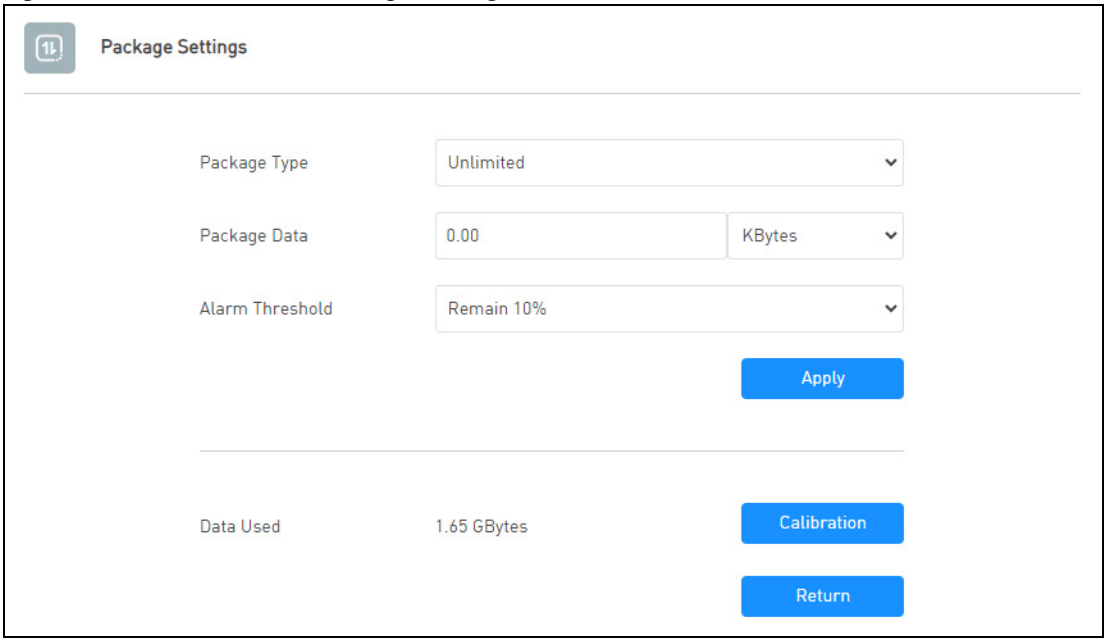


The following table describes the labels in this screen.

Table 28 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 NR2301 restarts calculating the amount of data.
Alarm Threshold	Select the percentage of data usage the NR2301 has to reach to display a notification on the NR2301's LCD **Home** screen and Web Configurator **Main** screen.
Apply	Click **Apply** to save your changes back to the NR2301.
Data Used	This displays the mobile data used by the NR2301 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. 
Return	Click this button to return to the **APP MODULE** list.

Figure 39 APP MODULE > Package Settings: Unlimited



The following table describes the labels in this screen.

Table 29 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 NR2301 has to reach to display a notification on the NR2301's LCD **Home** screen and Web Configurator's **Main** screen.
Apply	Click **Apply** to save your changes back to the NR2301.
Data Used	This displays the mobile data used by the NR2301 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. 
Return	Click this button to return to the **APP MODULE** list.

9.3 Firewall

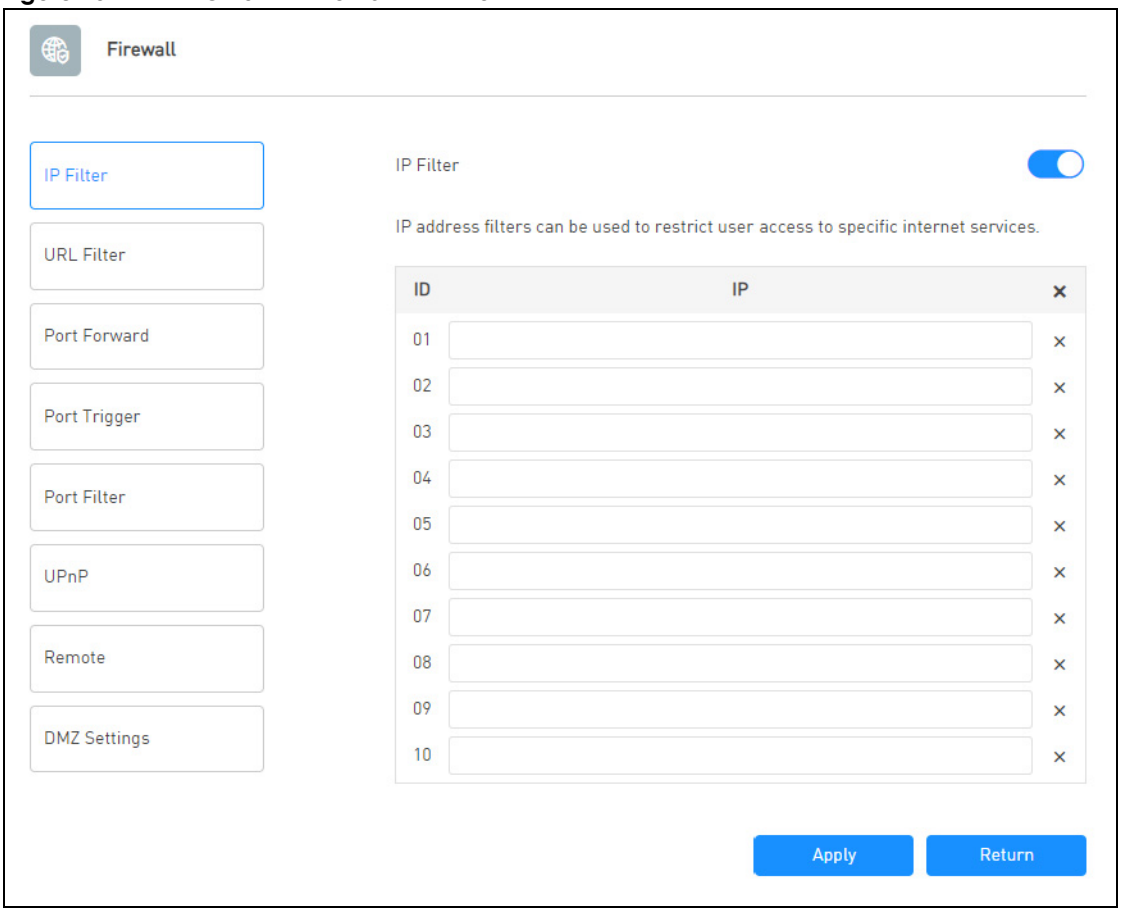
Use the **Firewall** screens to configure IP and URL filters, port forward, port trigger, UPnP, remote management, and DMZ.

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 40 APP MODULE > Firewall > IP Filter



The following table describes the labels in this screen.

Table 30 APP MODULE > Firewall > IP Filter

LABEL	DESCRIPTION
Turn the switch button on to enable IP filter on the NR2301. 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 NR2301'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 back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

9.3.2 URL Filter

Keyword Blocking URL Checking

The NR2301 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

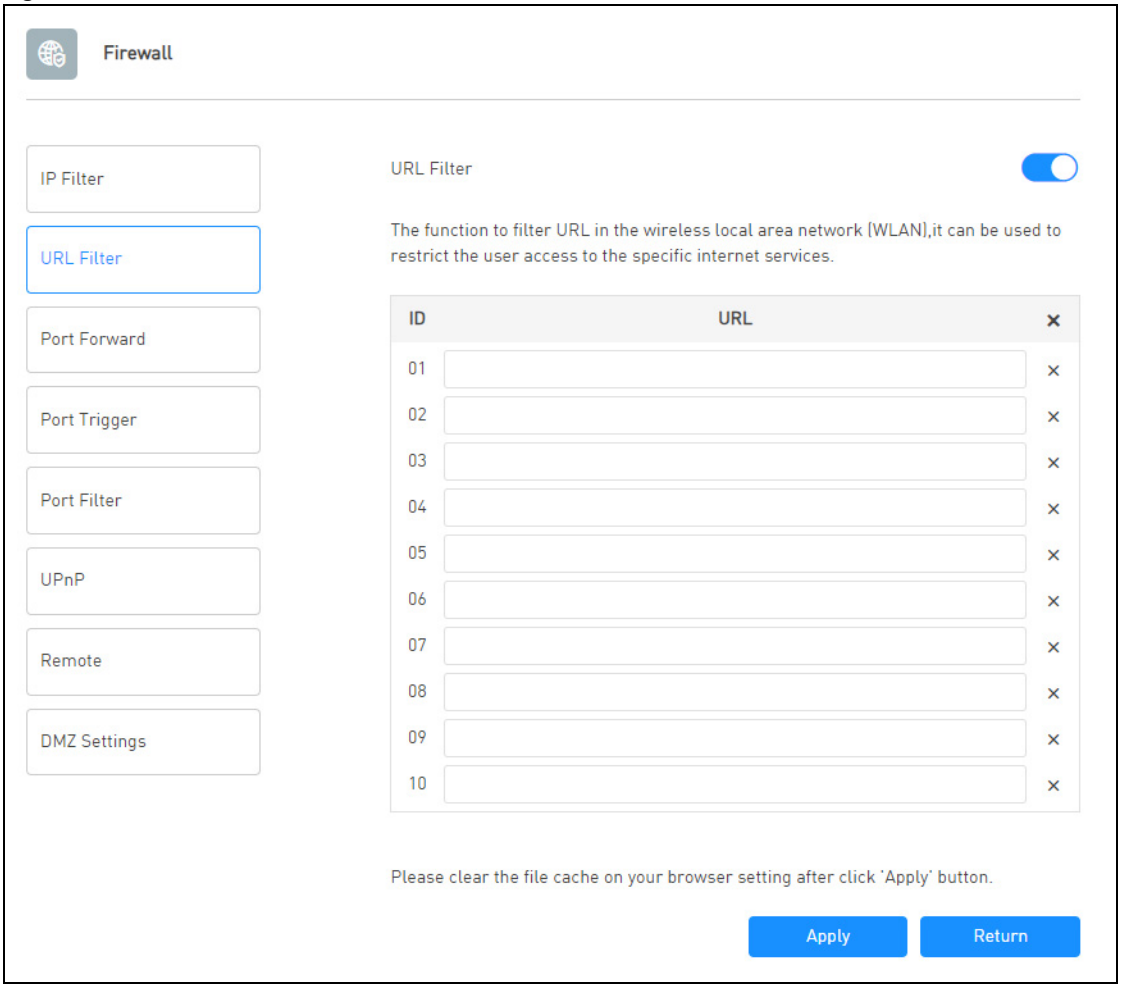
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the NR2301 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the NR2301 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

Use the **URL Filter** screen to configure URL filtering settings to block the users on your network from accessing certain web sites.

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

Figure 41 APP MODULE > Firewall > URL Filter



The following table describes the labels in this screen.

Table 31 APP MODULE > Firewall > URL Filter

LABEL	DESCRIPTION
Turn the switch button on to enable URL filter on the NR2301 and block the users on your network from accessing certain web sites.	
ID	This is the index number of the entry.
URL	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address. 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 back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

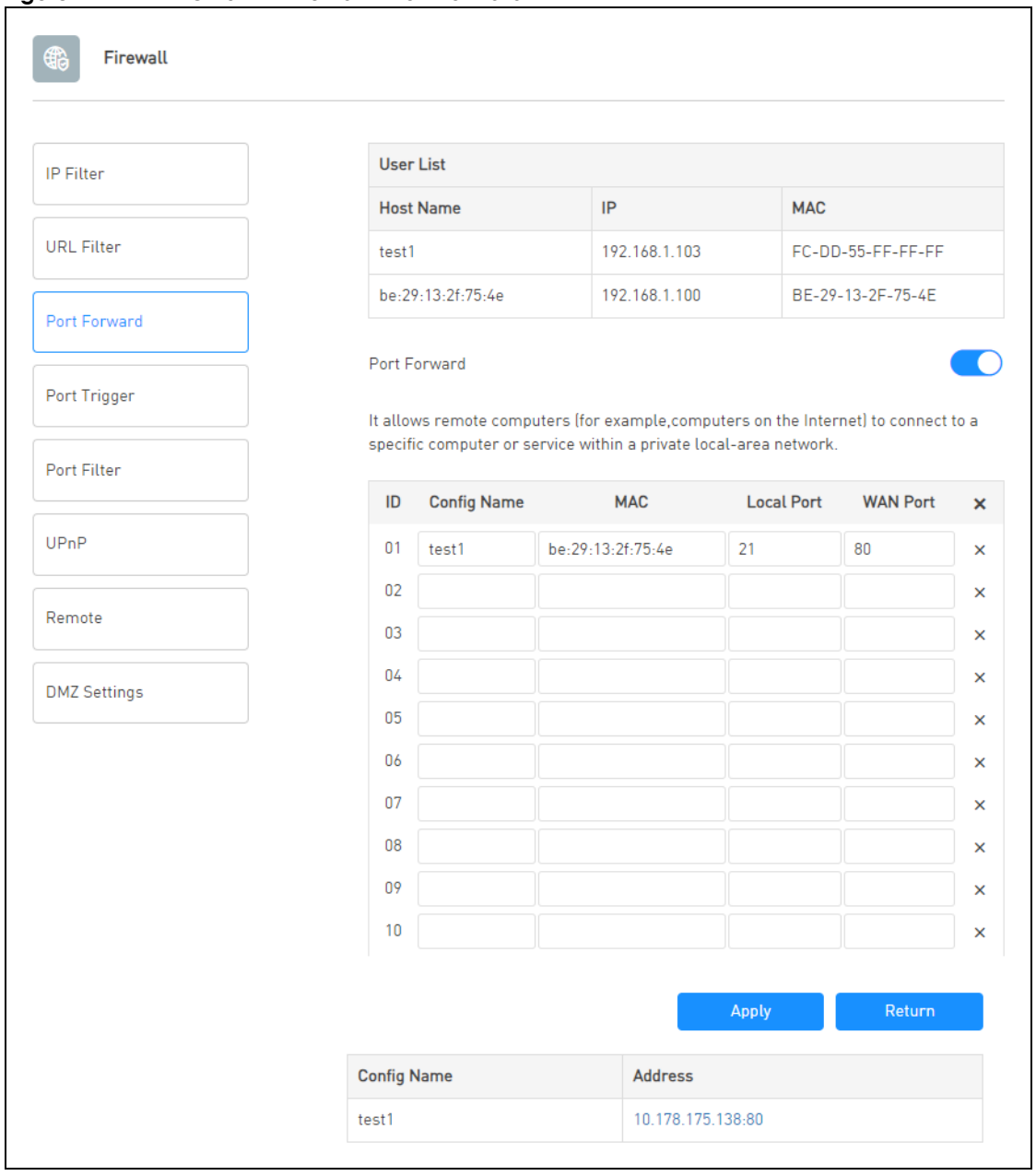
9.3.3 Port Forward

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 9.16.1 on page 98 for more information.

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

Figure 42 APP MODULE > Firewall > Port Forward



The following table describes the labels in this screen.

Table 32 APP MODULE > Firewall > Port Forward

LABEL	DESCRIPTION
User List	This section displays information of the NR2301'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.
MAC	This displays the MAC address of the service server.
Turn the switch button on to enable port forwarding on the NR2301. 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 back to the NR2301. 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.

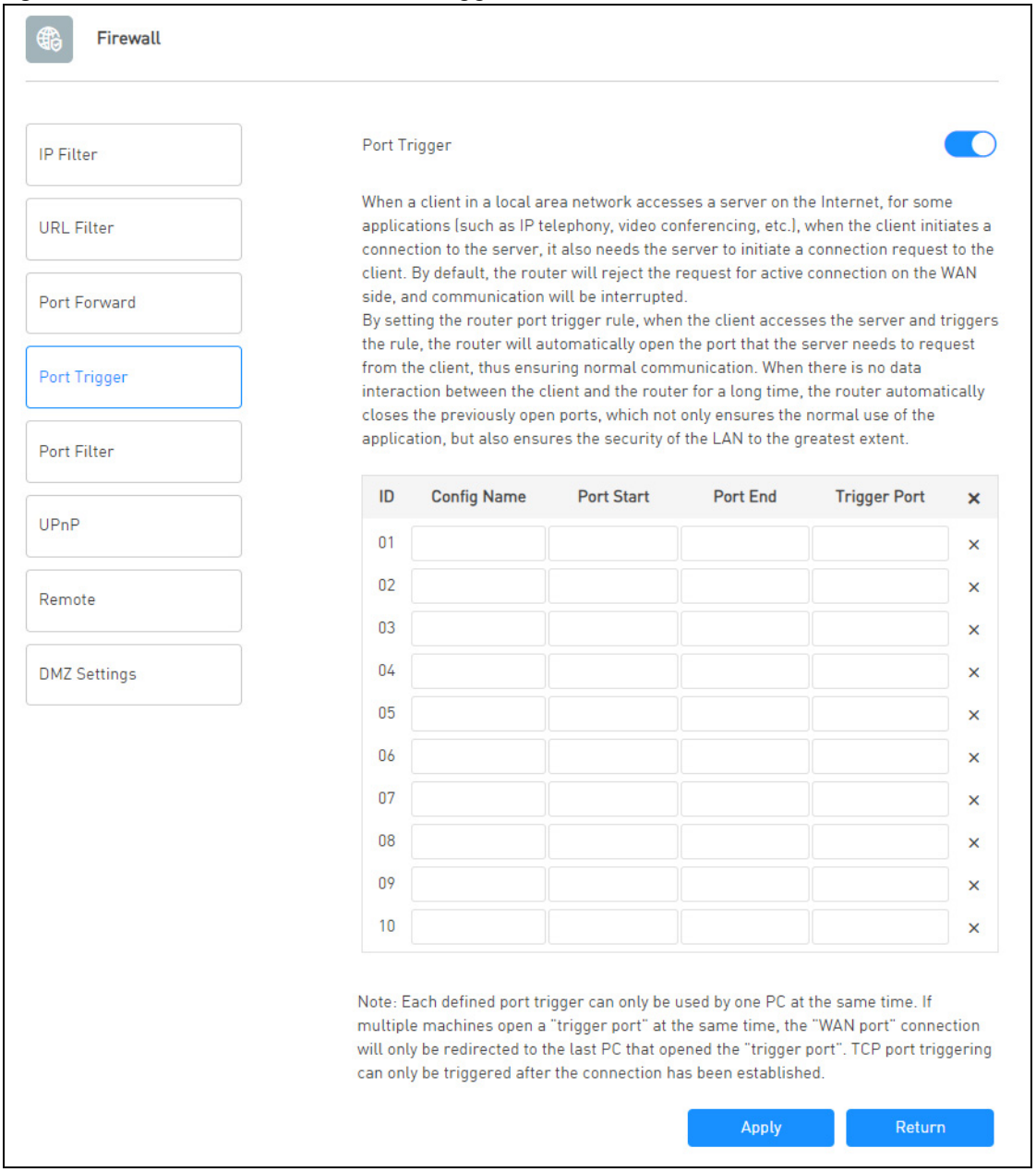
9.3.4 Port Trigger

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The NR2301 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 NR2301's WAN port receives a response with a specific port number, the NR2301 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 9.16.3 on page 99 for more information.

To change your NR2301'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 43 APP MODULE > Firewall > Port Trigger



The following table describes the labels in this screen.

Table 33 APP MODULE > Firewall > Port Trigger

LABEL	DESCRIPTION
Turn the switch button on to enable port trigger on the NR2301.	
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 NR2301 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.

Table 33 APP MODULE > Firewall > Port Trigger (continued)

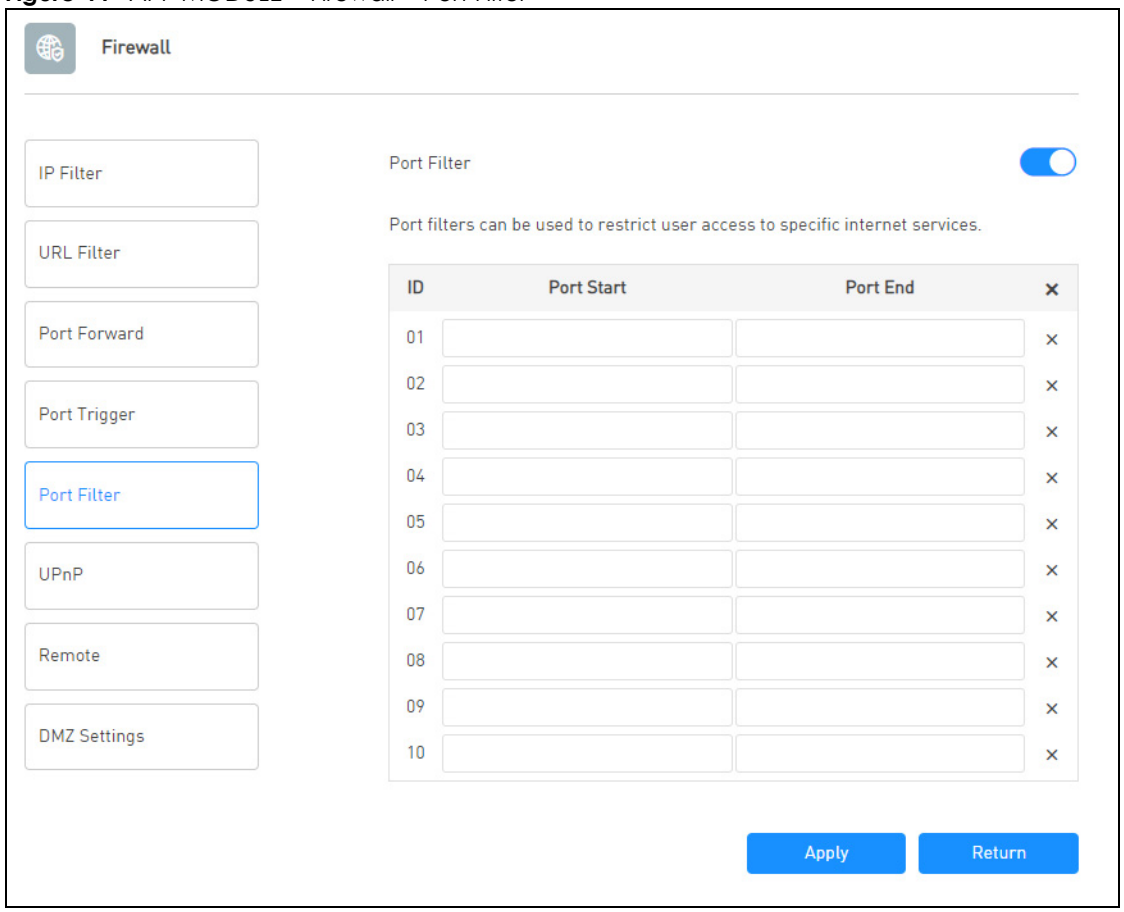
LABEL	DESCRIPTION
X	Click the **X** next to an entry to clear it.
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

9.3.5 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 44 APP MODULE > Firewall > Port Filter



The following table describes the labels in this screen.

Table 34 APP MODULE > Firewall > Port Filter

LABEL	DESCRIPTION
Turn the switch button on to enable port filter on the NR2301. 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.

Table 34 APP MODULE > Firewall > Port Filter (continued)

LABEL	DESCRIPTION
X	Click the **X** next to an entry to clear it.
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

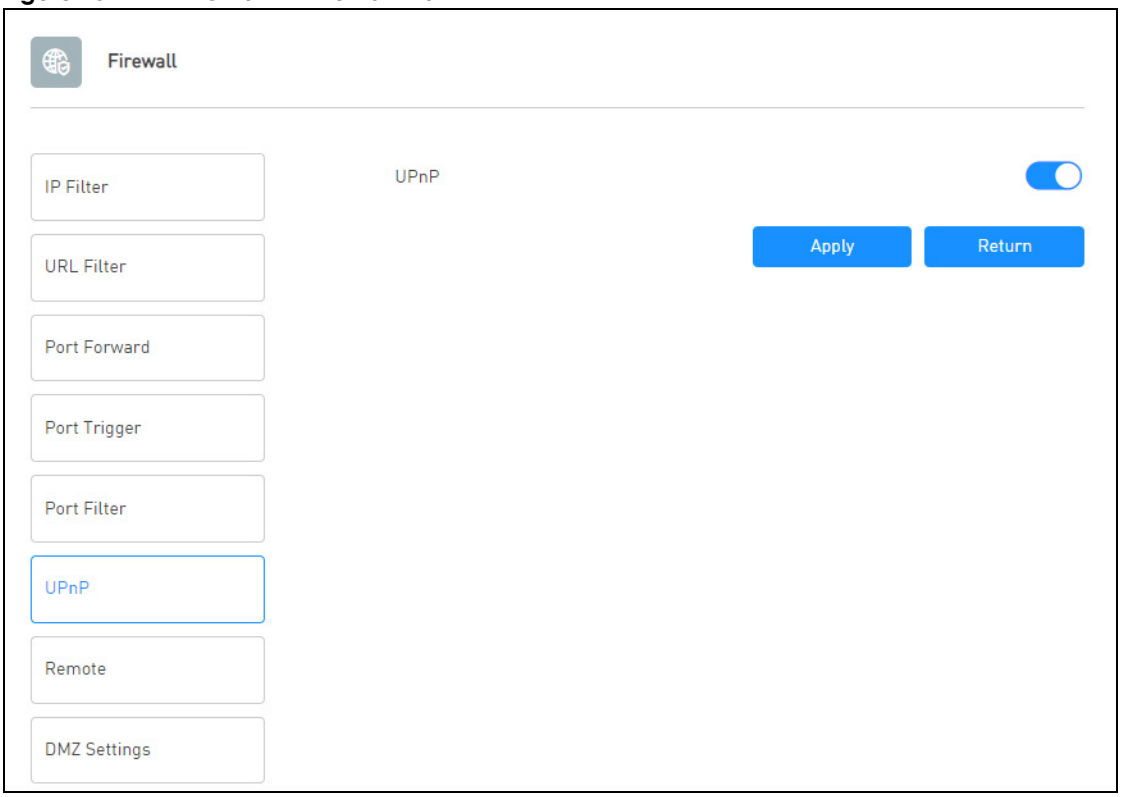
9.3.6 UPnP

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. See Section 9.16.6 on page 100 for more information.

Use the **UPnP** screen to enable or disable UPnP on the NR2301.

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

Figure 45 APP MODULE > Firewall > UPnP



The following table describes the labels in this screen.

Table 35 APP MODULE > Firewall > UPnP

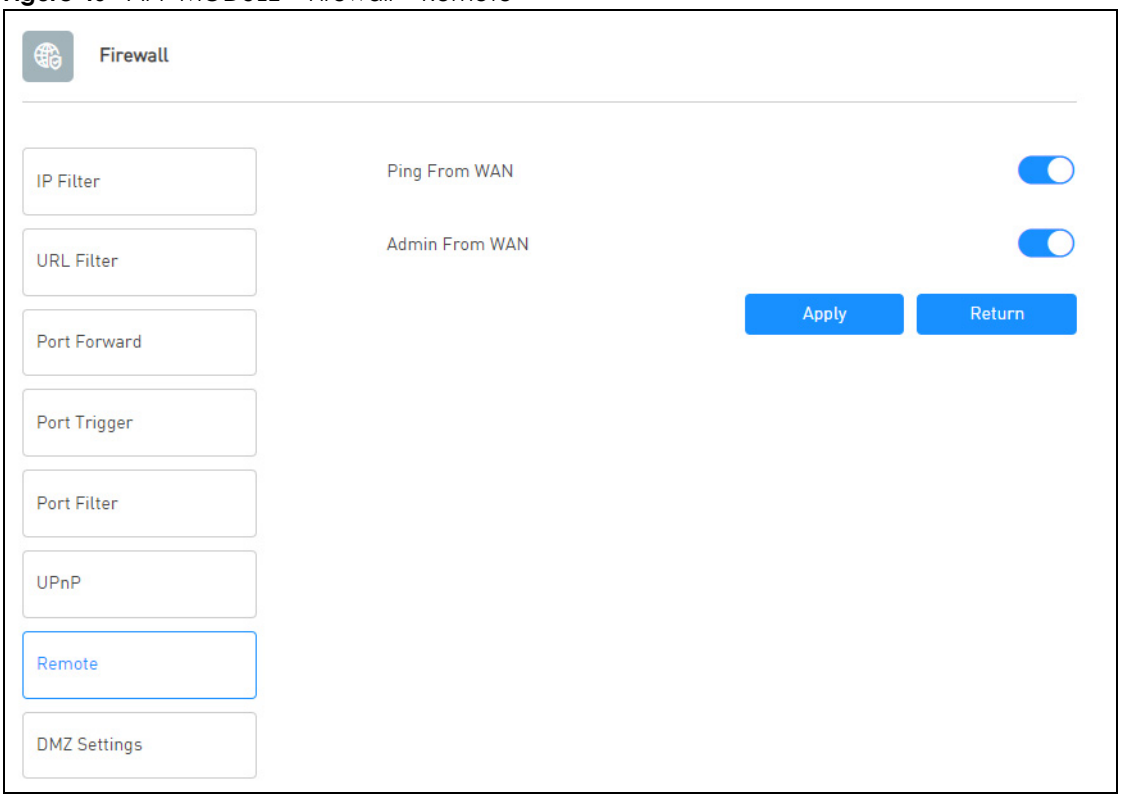
LABEL	DESCRIPTION
Turn the switch button on to enable UPnP on the NR2301. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NR2301's IP address (although you must still enter the password to access the Web Configurator).	
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

9.3.7 Remote

Use the **Remote** screen to allow or forbid WAN users from pinging or configuring the NR2301.

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

Figure 46 APP MODULE > Firewall > Remote



The following table describes the labels in this screen.

Table 36 APP MODULE > Firewall > Remote

LABEL	DESCRIPTION
Ping From WAN	Turn the switch button on to allow WAN users to ping the NR2301.
Admin From WAN	Turn the switch button on to allow WAN users to access the NR2301's Web Configurator.
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

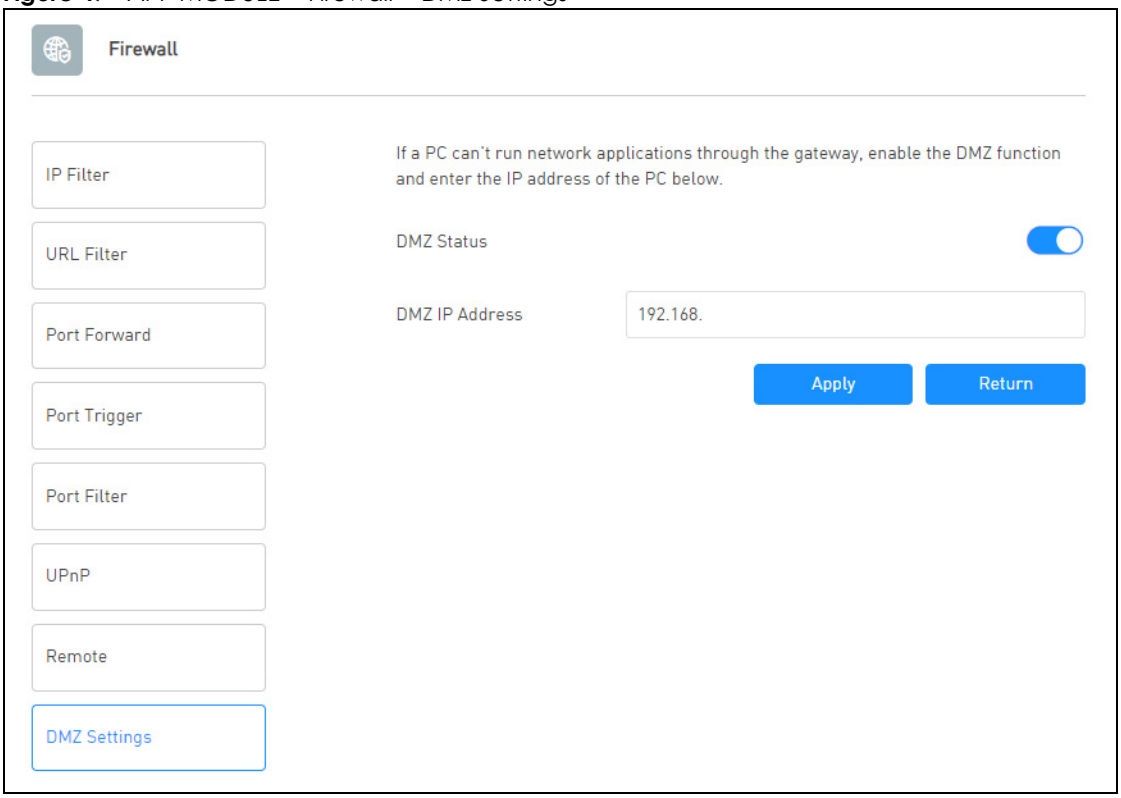
9.3.8 DMZ Settings

A client in the Demilitarized Zone (DMZ) is no longer behind the NR2301 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 NR2301.

Use the **DMZ Settings** screen to enable DMZ on the NR2301.

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

Figure 47 APP MODULE > Firewall > DMZ Settings



The following table describes the labels in this screen.

Table 37 APP MODULE > Firewall > DMZ Settings

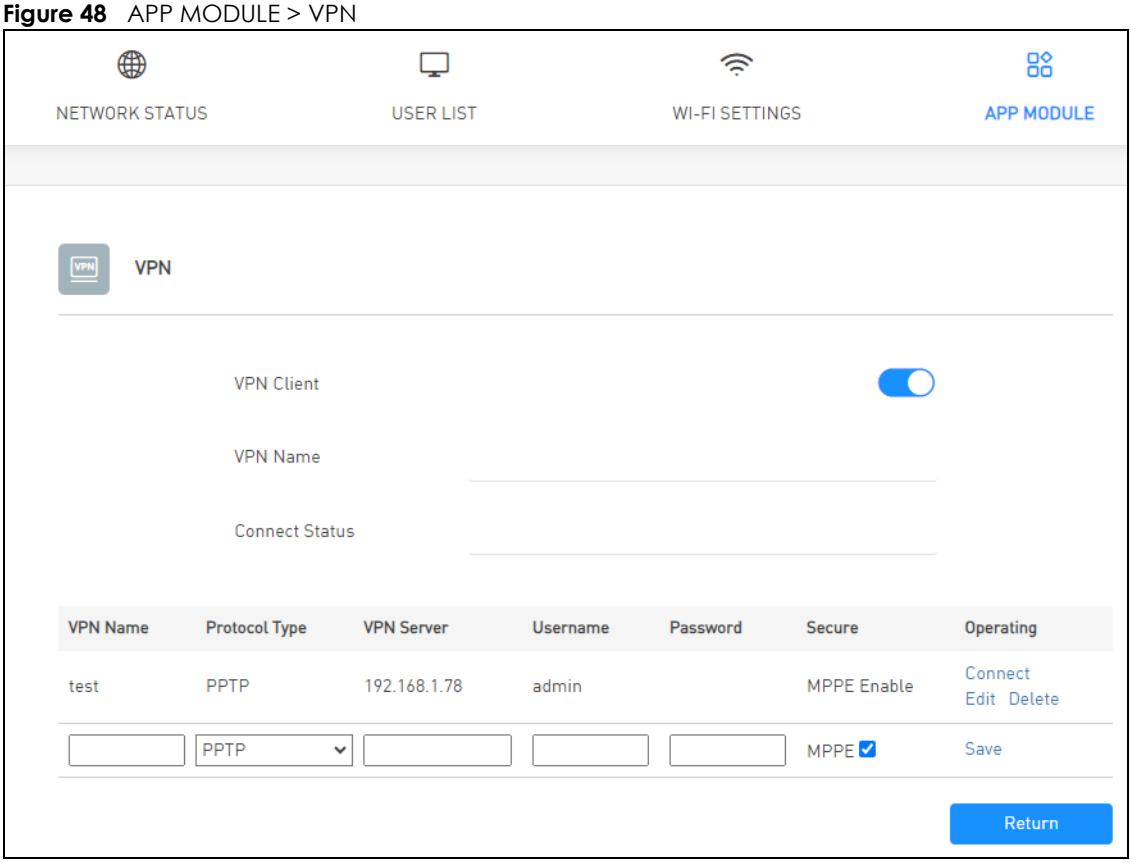
LABEL	DESCRIPTION
DMZ Status	Turn the switch button on to enable DMZ on the NR2301.
DMZ IP Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign the DMZ IP Address, the NR2301 discards all packets received for ports that are not specified in the **Port Forwarding** screen.
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

9.4 VPN

Use the **VPN** screen to enable and configure VPN client settings. You can configure up to 10 VPN client rules but only one rule can be used at a time. A VPN client rule has the NR2301 use VPN to connect through the Internet to a remote private network and let the NR2301's LAN devices also access the remote private network. Essentially you install VPN clients on the NR2301 instead of on the LAN devices. See Section 9.16.8 on page 100 for more information.

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

Figure 48 APP MODULE > VPN



The following table describes the labels in this screen.

Table 38 APP MODULE > VPN

LABEL	DESCRIPTION
VPN Client	Turn the switch button on to enable VPN client on the NR2301.
VPN Name	This field displays the client's login name.
Connect Status	This field displays the current connection status.
VPN Name	Enter a descriptive name for the VPN connection rule.
Protocol Type	Select **PPTP**, **L2TP**, or **L2TP/IPSEC** as the network protocol. See Section 9.16.9 on page 101 and Section 9.16.10 on page 102 for more information.
VPN Server	Enter the IP address of the VPN server.
Username	Enter the username of the VPN server.
Password	Enter the password of the VPN server.

Table 38 APP MODULE > VPN (continued)

LABEL	DESCRIPTION
Secure	Select if you want to use Microsoft Point-to-Point Encryption (MPPE) encryption for this VPN connection rule.
Operating	Click **Save** to save the settings as a new VPN connection rule. If the VPN connection rule is already configured, click **Connect** to start the connection and click **Unselect** to disconnect it. You can also click **Edit** to edit the rule or **Delete** to remove it.
Return	Click this button to return to the **APP MODULE** list.

9.5 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 NR2301.

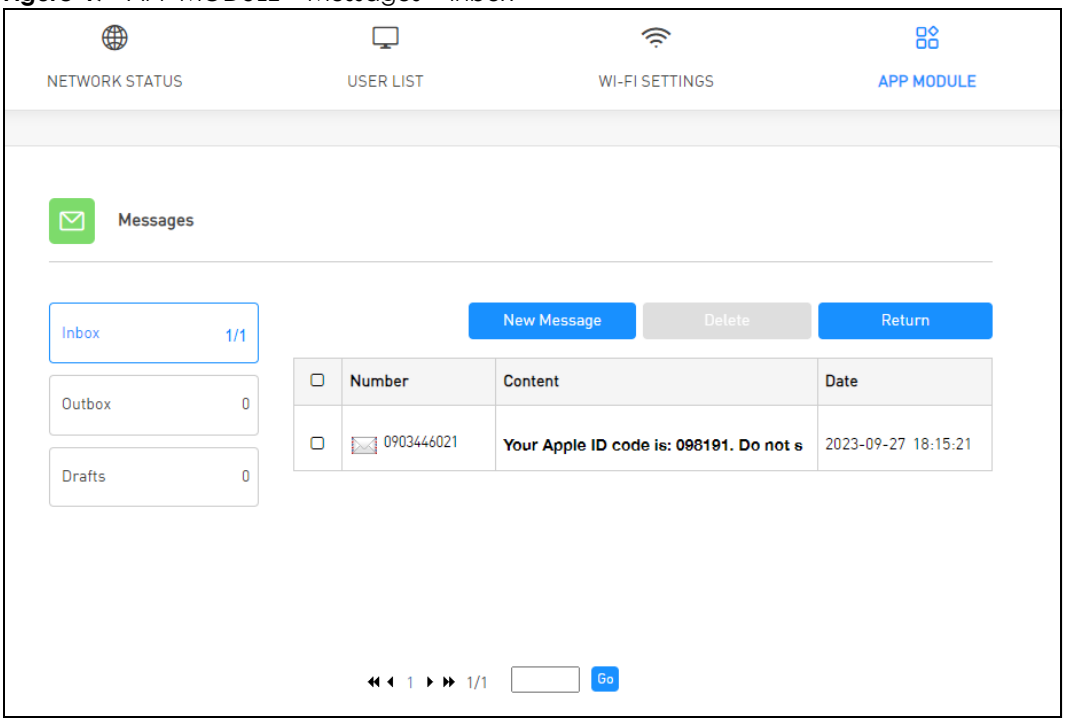
To access this screen, click **APP MODULE** > **Messages**.

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

9.5.1 Inbox

Use this screen to view messages received by the NR2301. To access this screen, click **APP MODULE** > **Messages** > **Inbox**.

Figure 49 APP MODULE > Messages > Inbox



The following table describes the labels in this screen.

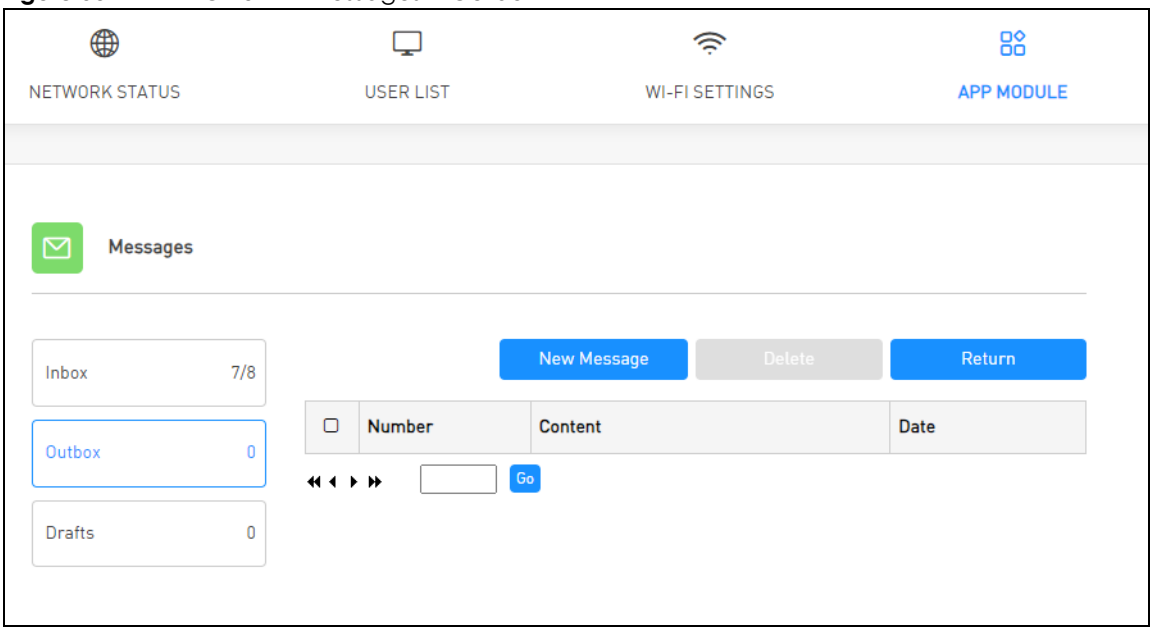
Table 39 APP MODULE > Messages > Inbox

LABEL	DESCRIPTION
New Message	Click this button to send messages using the NR2301. See Section 9.5.4 on page 85 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.

9.5.2 Outbox

Use this screen to view messages sent from the NR2301. To access this screen, click **APP MODULE** > **Messages** > **Outbox**.

Figure 50 APP MODULE > Messages > Outbox



The following table describes the labels in this screen.

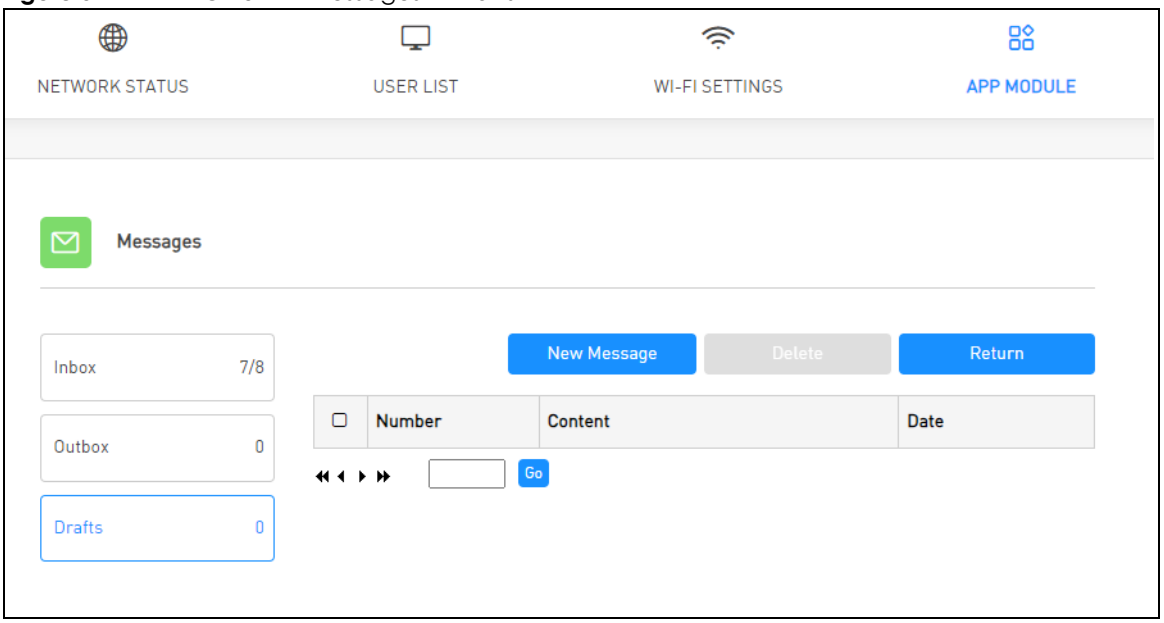
Table 40 APP MODULE > Messages > Outbox

LABEL	DESCRIPTION
New Message	Click this button to send messages using the NR2301. See Section 9.5.4 on page 85 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.

9.5.3 Drafts

Use this screen to view messages not yet sent from the NR2301. To access this screen, click **APP MODULE** > **Messages** > **Drafts**.

Figure 51 APP MODULE > Messages > Drafts



The following table describes the labels in this screen.

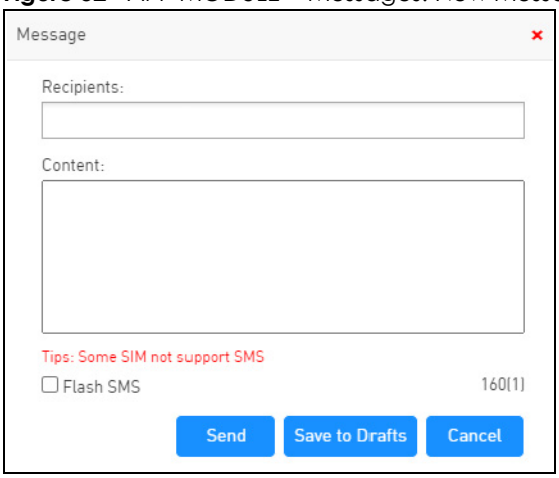
Table 41 APP MODULE > Messages > Drafts

LABEL	DESCRIPTION
New Message	Click this button to send messages using the NR2301. See Section 9.5.4 on page 85 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.

9.5.4 New Messages

Use this screen to send messages using the NR2301. To access this screen, click the **New Messages** button in the **Messages** screen.

Figure 52 APP MODULE > Messages: New Messages



The following table describes the labels in this screen.

Table 42 APP MODULE > Messages: New Messages

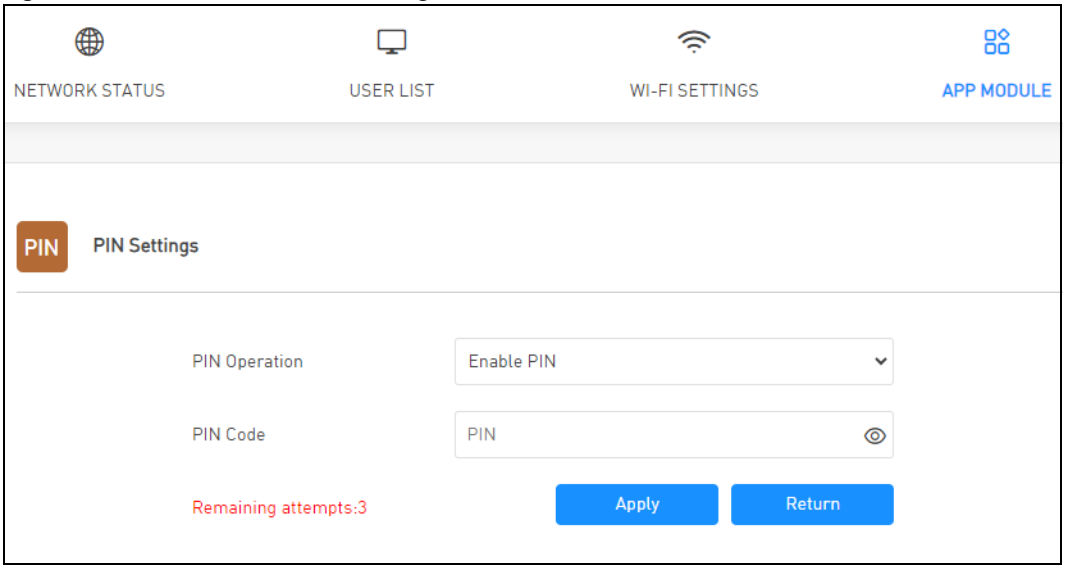
LABEL	DESCRIPTION
Recipients	Enter the phone number to which to send the message. Press **Enter** on your keyboard if you want to add another phone number. You can add up to 5 phone numbers.
Content	Enter the message content. You can send up to 160 characters in one message. If the message exceeds 160 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.

9.6 PIN Settings

Use the **PIN Settings** screens to enable PIN code authentication on the NR2301.

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

Figure 53 APP MODULE > PIN Settings



The following table describes the labels in this screen.

Table 43 APP MODULE > PIN Settings

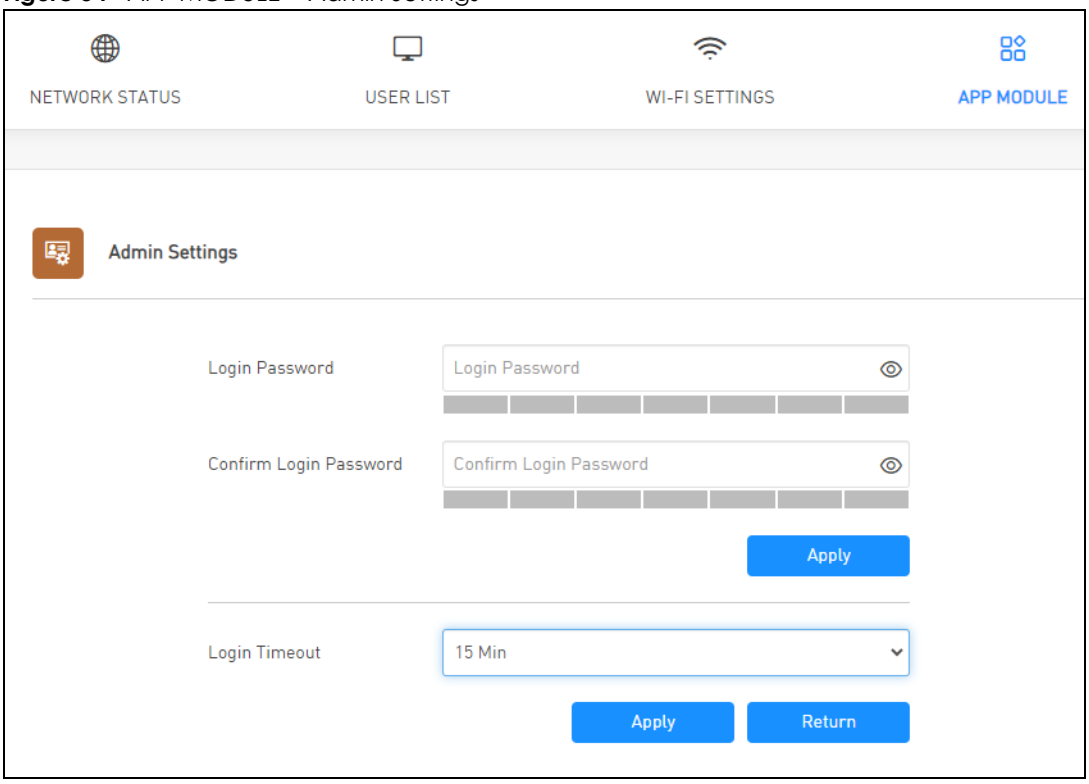
LABEL	DESCRIPTION
PIN Operation	This displays **Enable PIN** so that PIN code authentication is enabled. You need to enter the PIN code every time the NR2301 reboots.
PIN Code	Enter a 4-digit PIN code (0000 for example) provided by your ISP for the inserted SIM card. If you have entered the wrong PIN 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 back to the NR2301
Return	Click this button to return to the **APP MODULE** list.

9.7 Admin Settings

Use the **Admin Settings** screens to change the NR2301's system password and time-out setting. It is strongly recommended that you change your NR2301's system password.

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

Figure 54 APP MODULE > Admin Settings



The following table describes the labels in this screen.

Table 44 APP MODULE > Admin Settings

LABEL	DESCRIPTION
Login Password	Type 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	Type 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 back to the NR2301
Return	Click this button to return to the **APP MODULE** list.

9.8 Update

Use the **Update** screens to upload new firmware to your NR2301. You can download new firmware releases or check for new firmware online to use to upgrade your NR2301's performance.

Only use firmware for your device's specific model.

9.8.1 Online Update

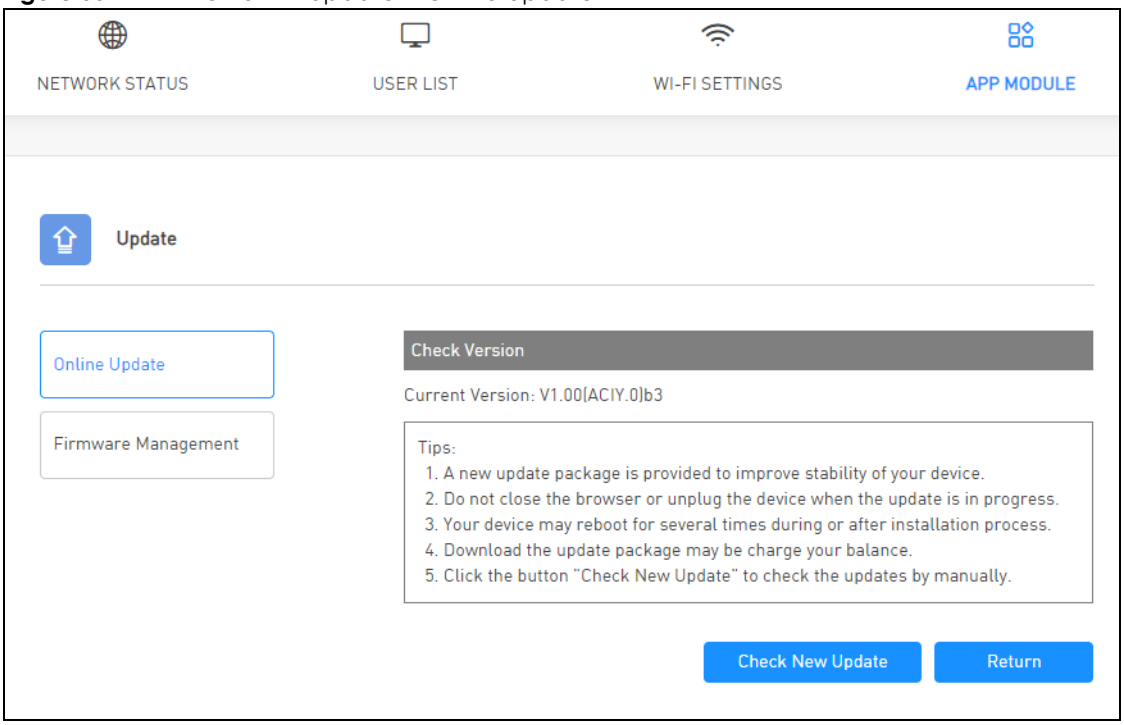
Firmware Over the Air (FOTA) allows for timely and automatic firmware upgrades. By default, FOTA is enabled on the NR2301 and it checks for firmware updates automatically. It will do so each time it is turned on and connected to the Internet. You can disable it in the NR2301's LCD screen. See Chapter 1 on page 19 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 NR2301 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 NR2301 while firmware upload is in progress!

Figure 55 APP MODULE > Update > Online Update



9.8.2 Firmware Management

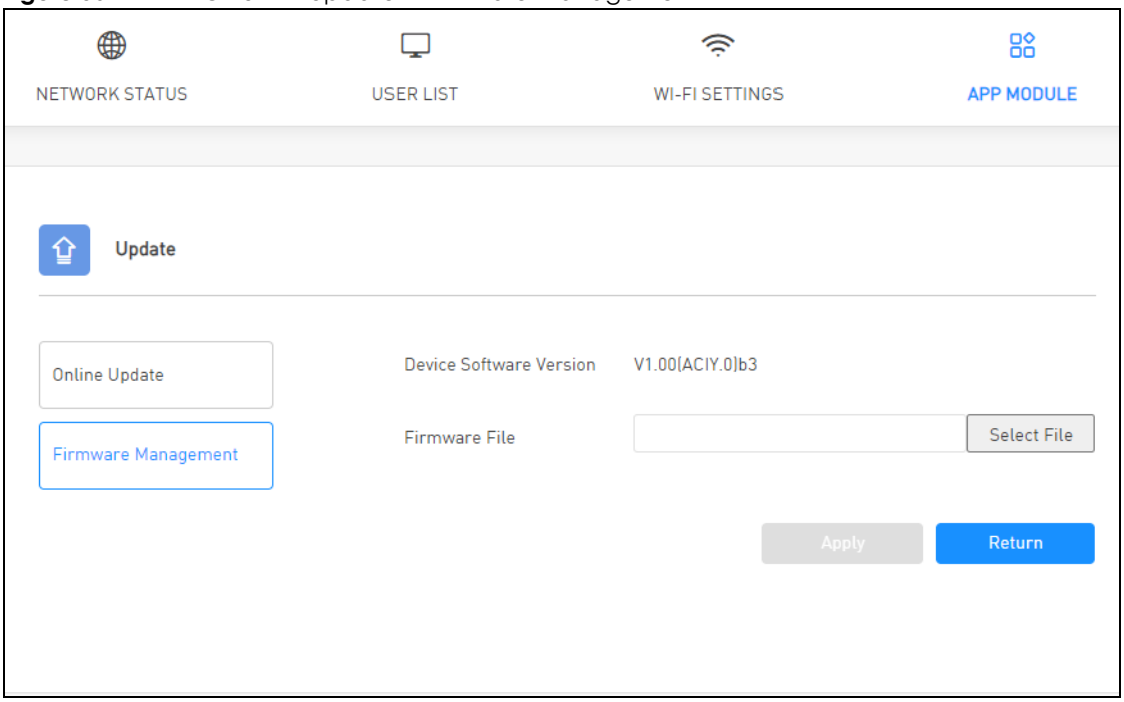
The **Firmware Management** screen allows you to upload new firmware to your NR2301. You can download new firmware releases from the download library at the Zyxel website (www.zyxel.com) to use to upgrade your NR2301's performance.

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 NR2301 while firmware upload is in progress!

Figure 56 APP MODULE > Update > Firmware Management



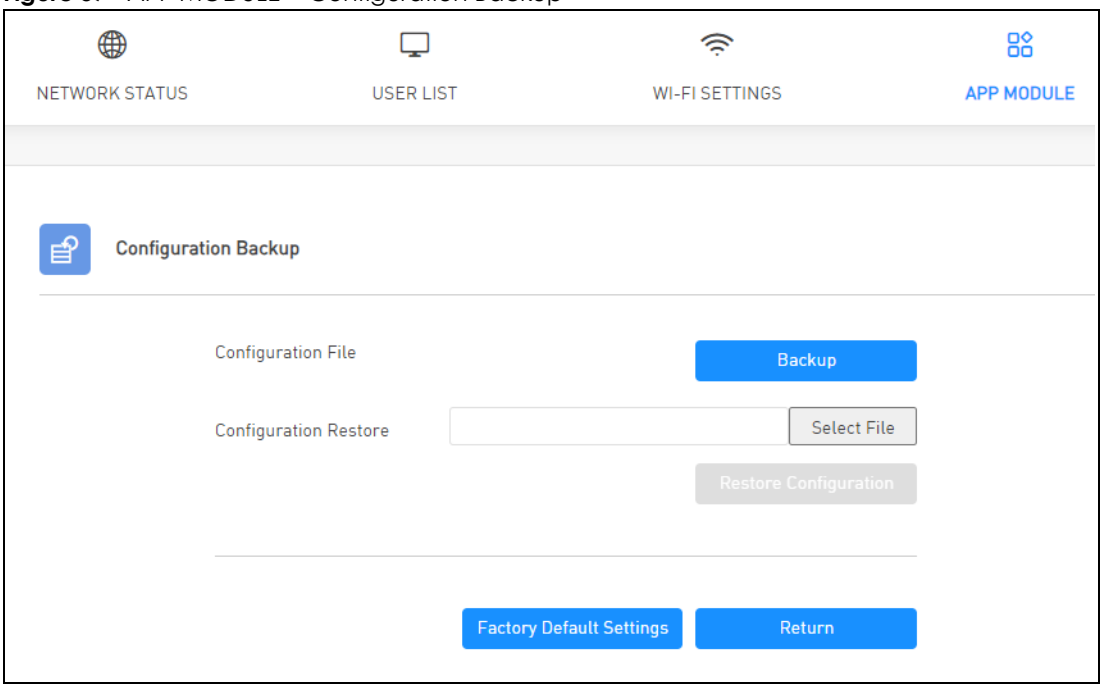
9.9 Configuration Backup

Backup configuration allows you to back up (save) the NR2301's current configuration to a file with a "bin" extension on your computer. Once your NR2301 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 NR2301.

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

Figure 57 APP MODULE > Configuration Backup



The following table describes the labels in this screen.

Table 45 APP MODULE > Configuration Backup

LABEL	DESCRIPTION
Configuration File	Click **Backup** to save the NR2301'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. Note: Do not turn off the NR2301 while configuration file upload is in progress. The NR2301 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 NR2301 to its factory defaults. You can also press the **RESET** button on the side panel to reset the factory defaults of your NR2301. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button. See Section 1.4.3 on page 11.
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 NR2301 IP address (192.168.1.1).

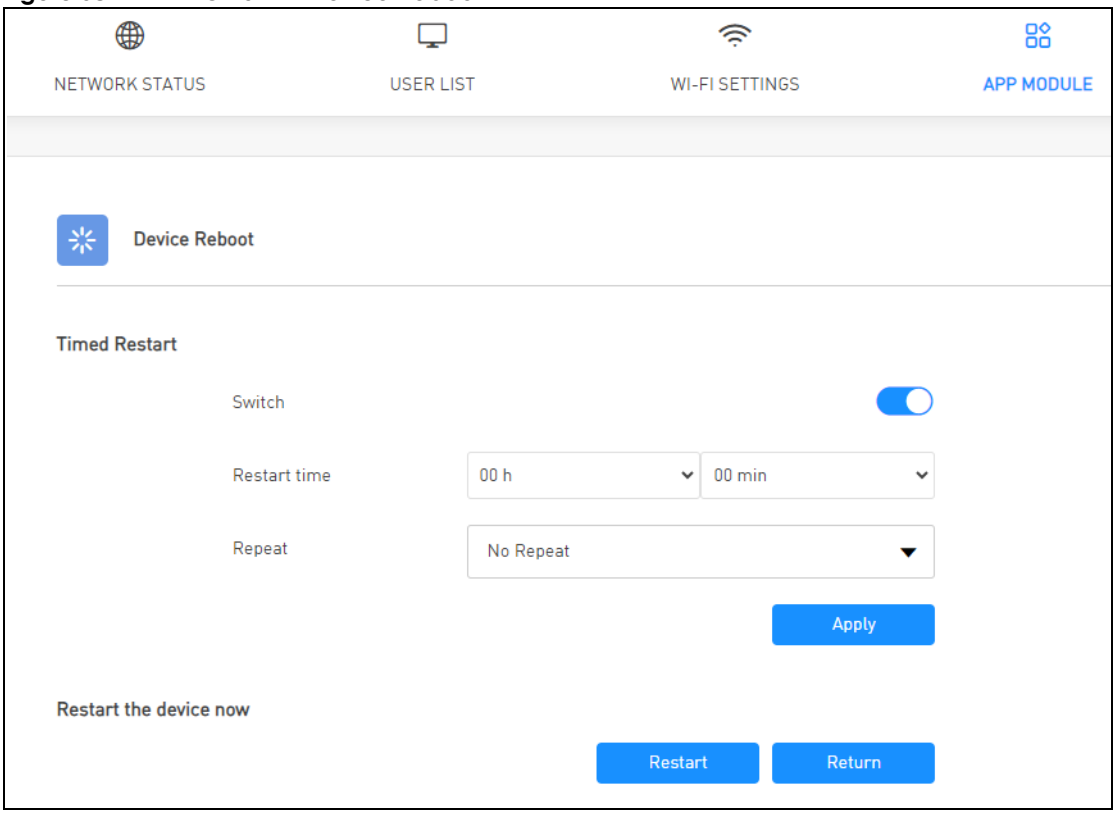
9.10 Device Reboot

Use the **Device Reboot** screen to restart the NR2301. You can also set a schedule to reboot the NR2301. System restart allows you to reboot the NR2301 without turning the power off. Click **Restart** to reboot the

NR2301. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the NR2301 in your Web browser.

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

Figure 58 APP MODULE > Device Reboot



The following table describes the labels in this screen.

Table 46 APP MODULE > Device Reboot

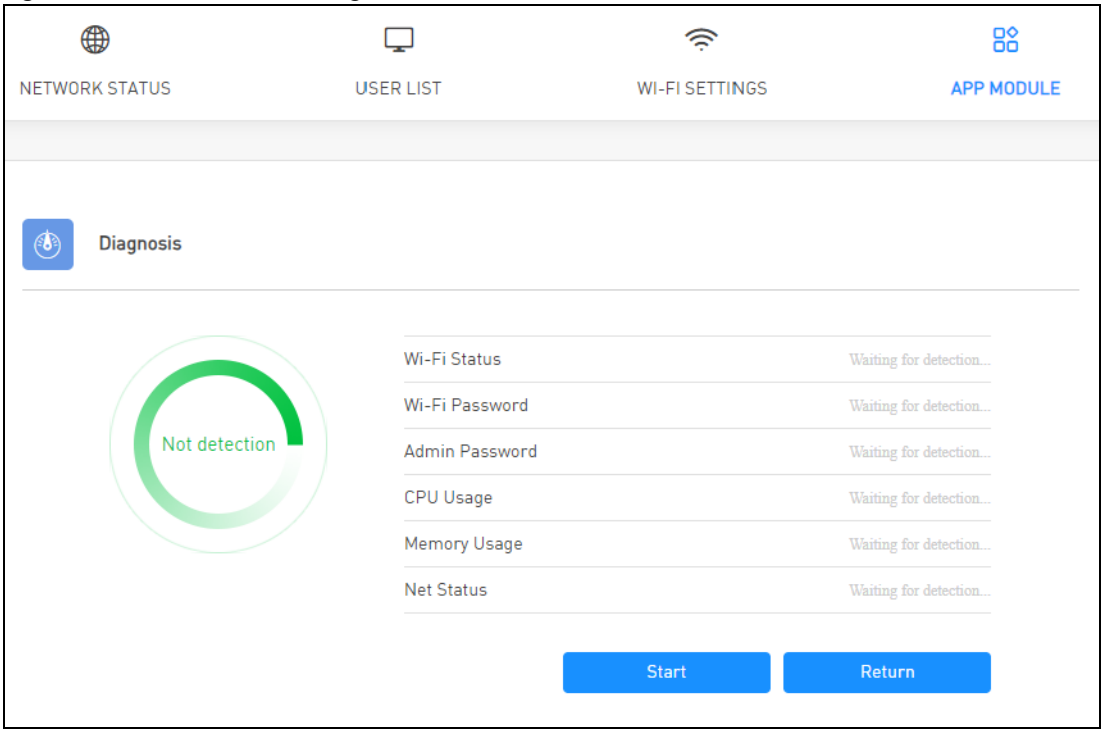
LABEL	DESCRIPTION
Switch	Turn the switch button on to configure and enable a schedule to reboot the NR2301.
Restart time	Set the time that you plan to reboot the NR2301.
Repeat	Select the day of a week to enable the NR2301 to reboot periodically. Select **No Repeat** to reboot the NR2301 just once.
Apply	Click **Apply** to save your changes back to the NR2301.
Restart	Click this button to reboot the NR2301.
Return	Click this button to return to the **APP MODULE** list.

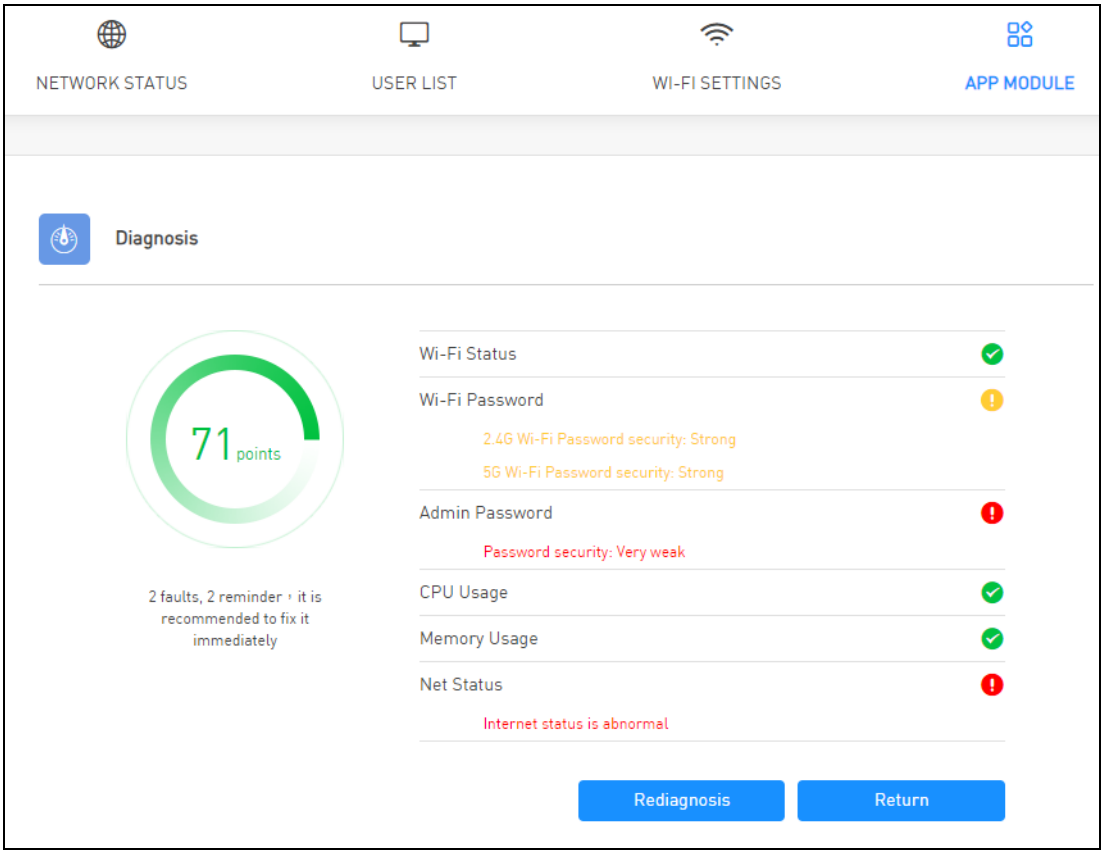
9.11 Diagnosis

Use the **Diagnosis** screen to check the WiFi and status of the NR2301. Click the **Start** button to begin diagnosing. You can check the results displayed in the screen and make changes in the NR2301's settings accordingly. Click **Rediagnosis** to diagnose the NR2301 again or **Return** to return to the **APP MODULE** list.

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

Figure 59 APP MODULE > Diagnosis





9.12 WPS

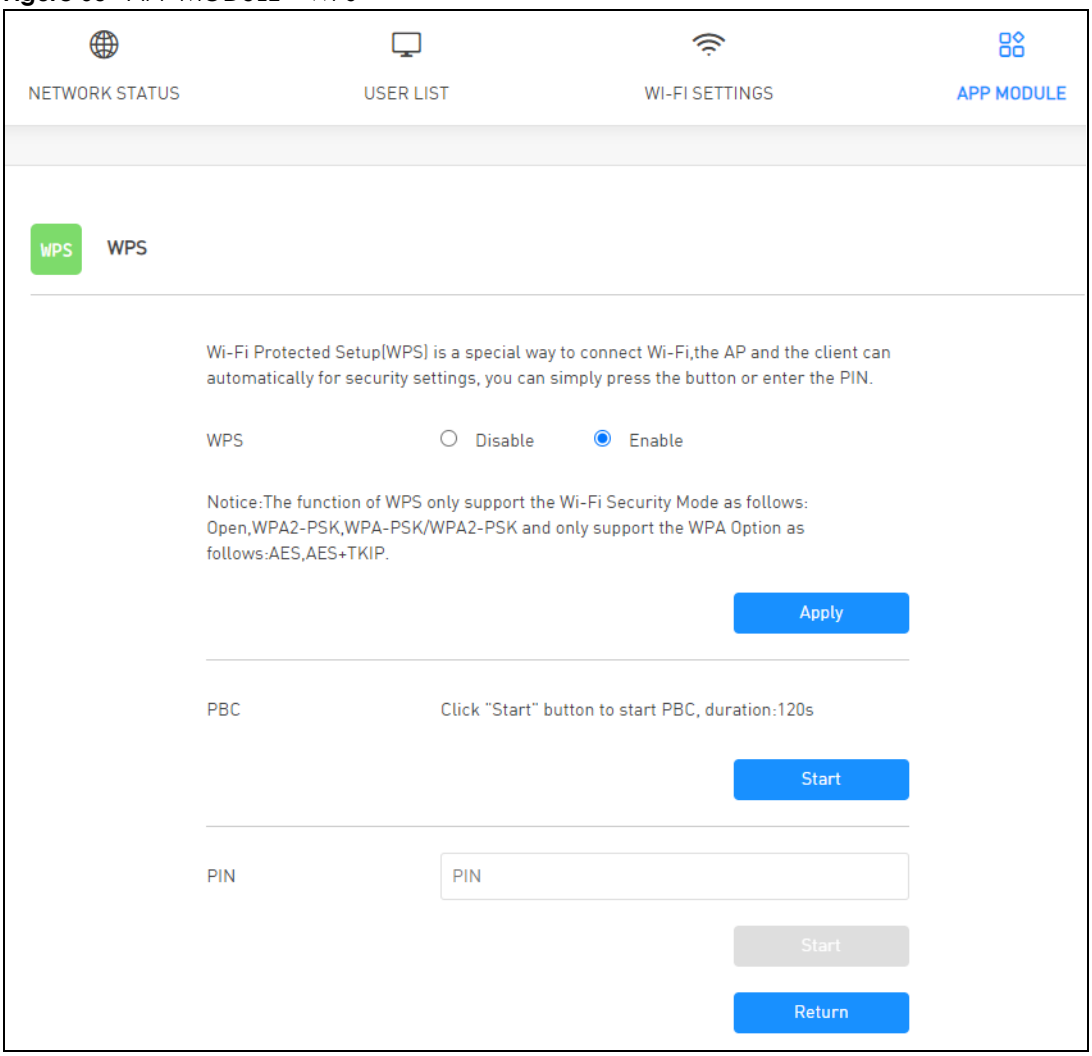
WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it. See Section 9.16.11.3 on page 104 for more information about WPS.

Note: The NR2301 applies the security settings of the main SSID profile (see Chapter 6 on page 48).

Note: If WPS is enabled, UPnP will automatically be turned on.

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

Figure 60 APP MODULE > WPS



The following table describes the labels in this screen.

Table 47 APP MODULE > WPS

LABEL	DESCRIPTION
WPS	Turn the switch button on to enable WPS on the NR2301.
Apply	Click **Apply** to save your changes back to the NR2301.
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 NR2301) 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. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
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. You can find the PIN by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

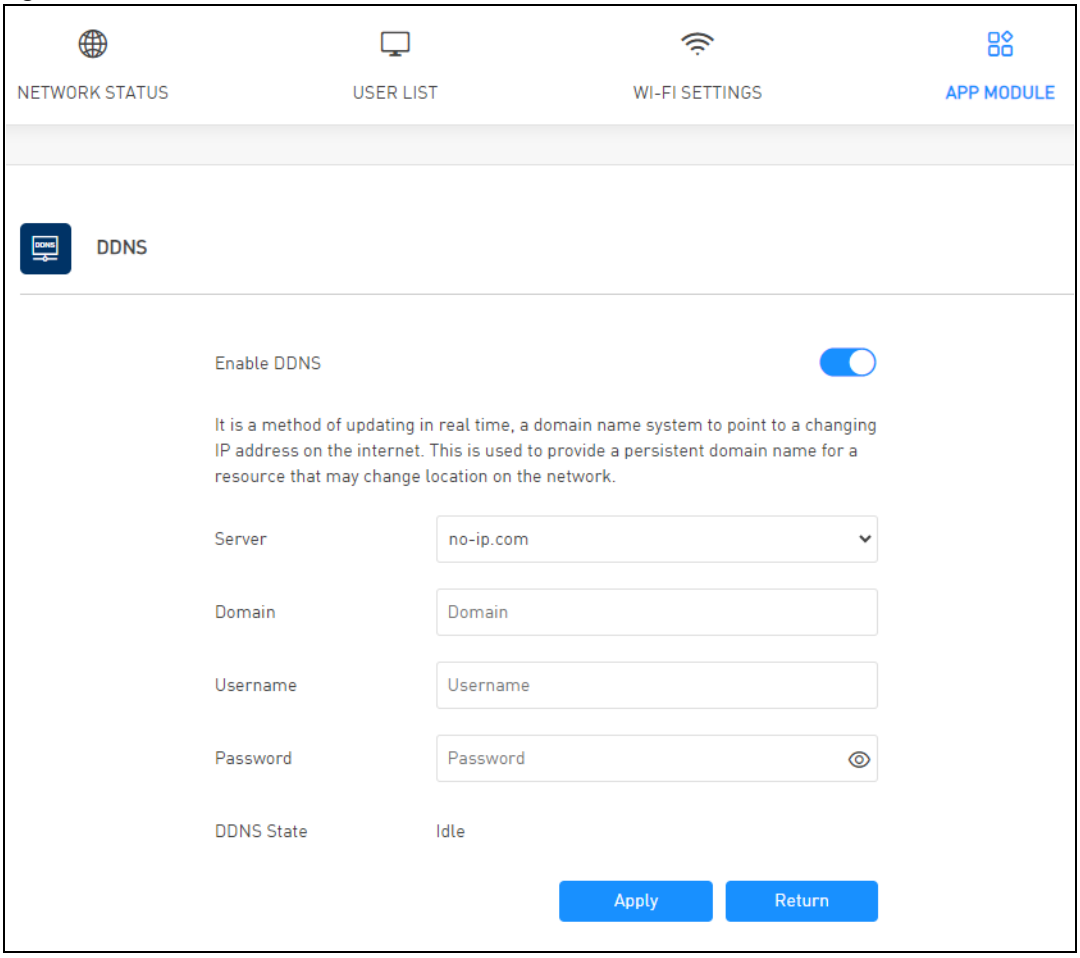
9.13 DDNS

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 NR2301 or a server in your network.

Note: The NR2301 must have a public global IP address and you should have your registered DDNS account information on hand.

To change your NR2301's DDNS, click **APP MODULE** > **DDNS**. The screen appears as shown.

Figure 61 APP MODULE > DDNS



The following table describes the labels in this screen.

Table 48 APP MODULE > DDNS

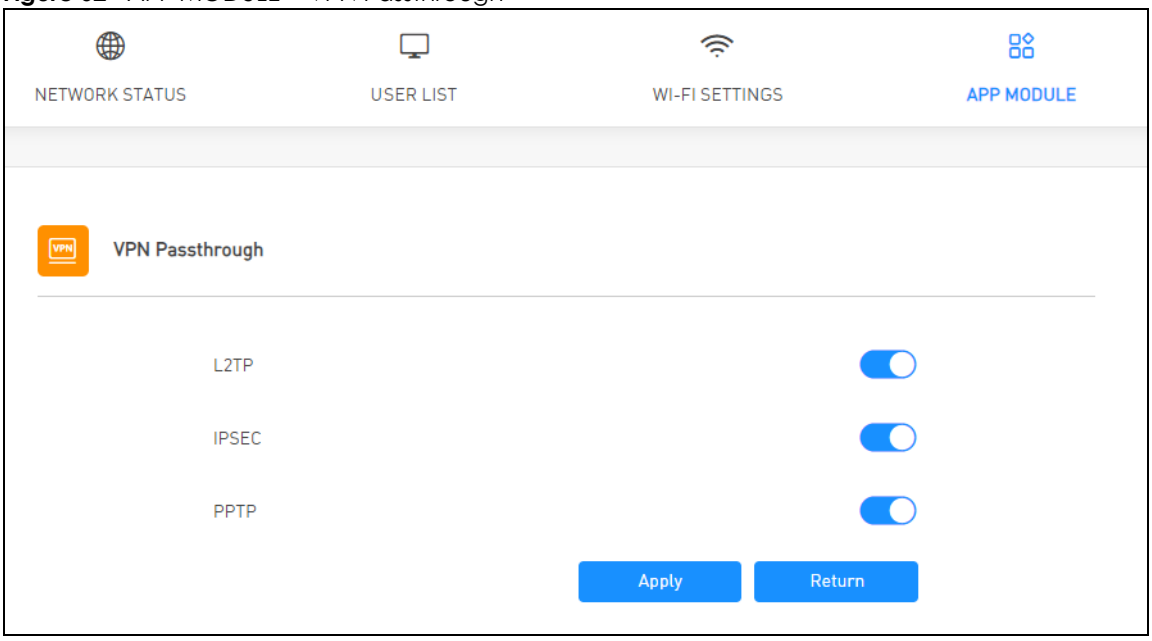
LABEL	DESCRIPTION
DDNS	Turn the switch button on to enable Dynamic DNS on the NR2301.
Server	Select the name of your Dynamic DNS service provider.
Domain	Enter the domain of your Dynamic DNS service provider.
Username	Enter your user name.
Password	Enter the password assigned to you.
DDNS State	This displays the current DDNS status.
Apply	Click **Apply** to save your changes back to the NR2301.
Return	Click this button to return to the **APP MODULE** list.

9.14 VPN Passthrough

Use the **VPN Passthrough** screen to allow VPN traffic including the L2TP, IPSec, and PPTP network protocols to operate through the NR2301. See Section 9.16.8 on page 100 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 back to the NR2301. Click the **Return** button to return to the **APP MODULE** list.

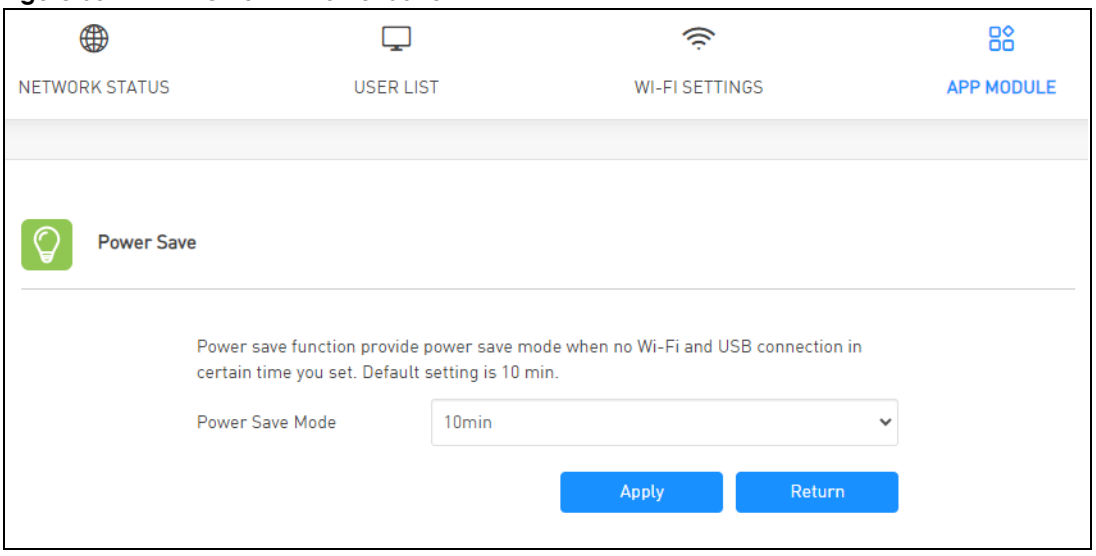
Figure 62 APP MODULE > VPN Passthrough



9.15 Power Save

Use the **Power Save** screen to enable and configure the power saving settings in the NR2301.
Click **APP MODULE** > **Power Save** to display the following screen.
Select the number of minutes after which the NR2301 activates power saving and enters sleep mode. In **Power Saving** the NR2301 turns off its WiFi connections to save battery power when the USB port is not connected, and there are no WiFi clients associating with the NR2301. Then click **Apply** to save your changes back to the NR2301. Click the **Return** button to return to the **APP MODULE** list.

Figure 63 APP MODULE > Power Save



9.16 Technical Reference

The following section contains additional technical information about the NR2301 features described in this chapter.

9.16.1 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.

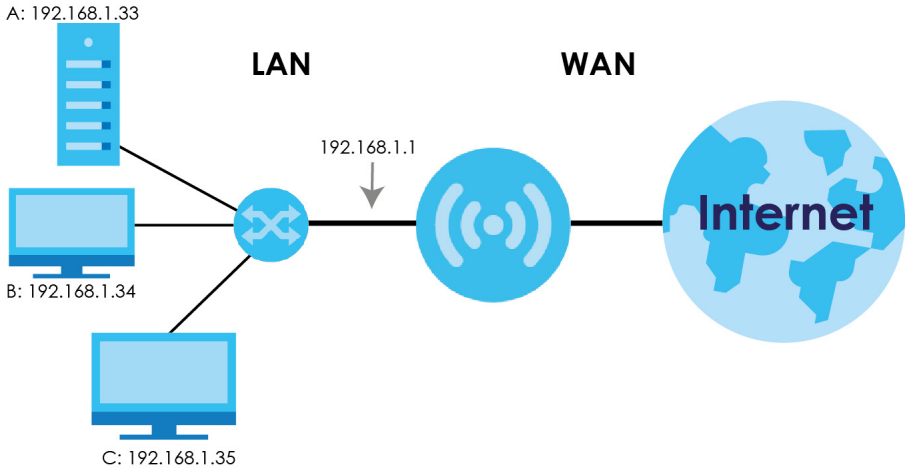
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

9.16.2 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 64 Multiple Servers Behind NAT Example



9.16.3 Trigger Port Forwarding

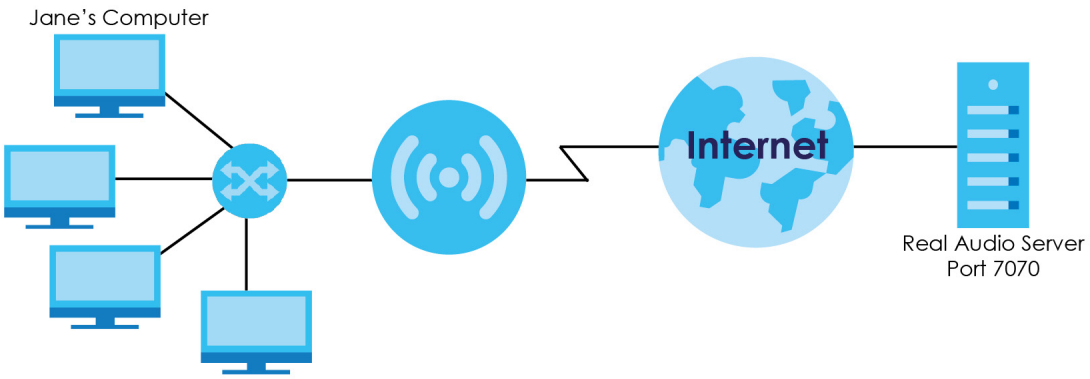
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 NR2301 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 NR2301's WAN port receives a response with a specific port number and protocol ("incoming" port), the NR2301 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.

9.16.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 65 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 NR2301 to record Jane's computer IP address. The NR2301 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 NR2301 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 NR2301 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

9.16.5 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is coming from inside the NR2301 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.

9.16.6 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

9.16.7 Cautions With UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NR2301 allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

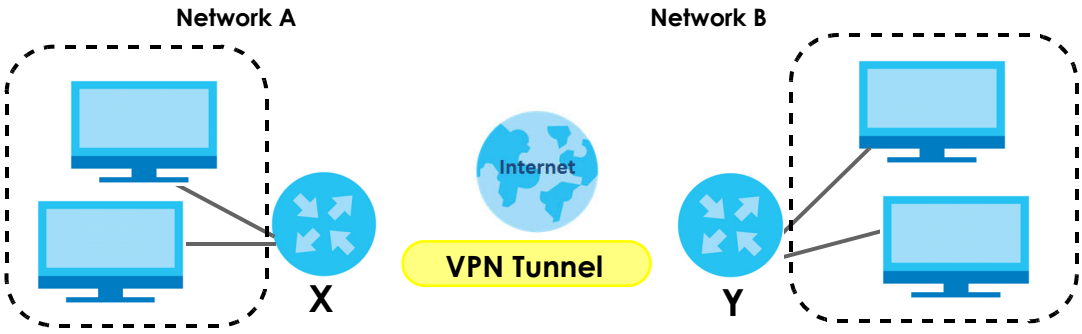
9.16.8 VPN

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 66 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).

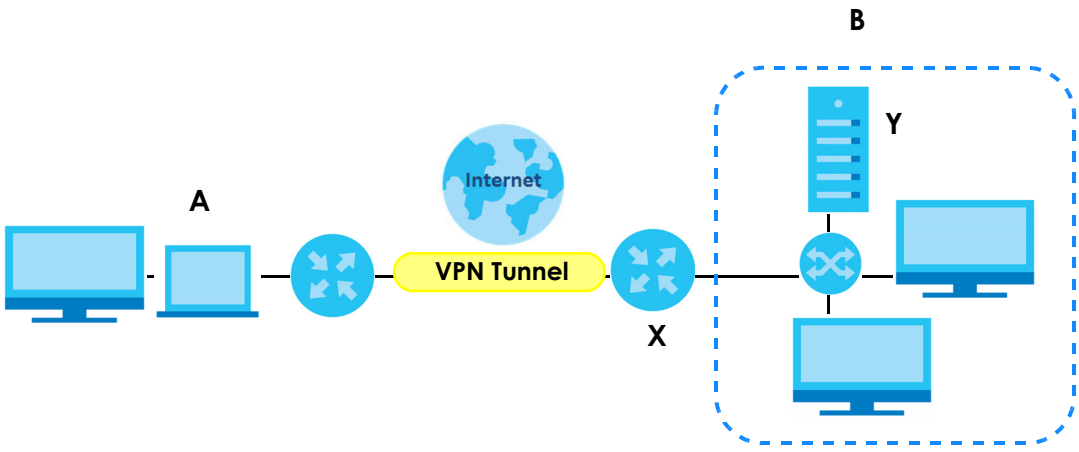
9.16.9 PPTP

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 67 PPTP VPN Example

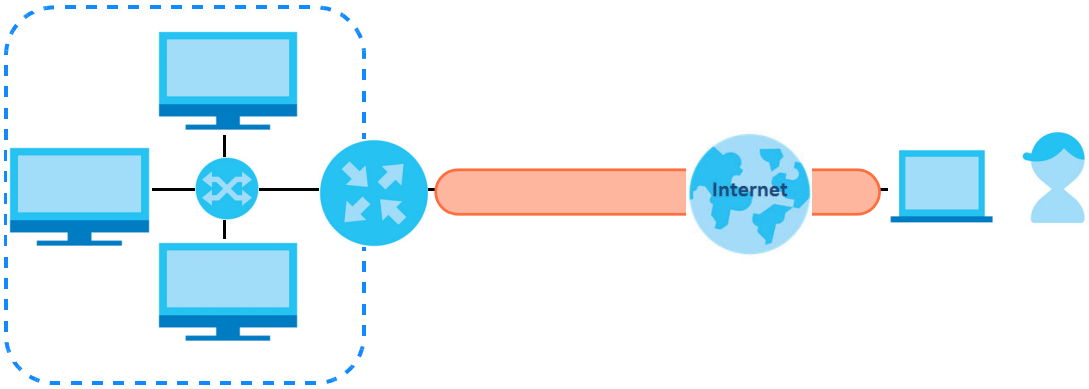


9.16.10 L2TP

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 NR2301. The remote users do not need their own IPSec gateways or VPN client software.

Figure 68 L2TP VPN Overview



9.16.11 WiFi Protected Setup (WPS)

Your NR2301 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi 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.

9.16.11.1 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 NR2301, see Section 9.12 on page 94).

3 Press the button on one of the devices (it does not matter which). For the NR2301 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.

9.16.11.2 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 NR2301, see Section 9.12 on page 94).

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.

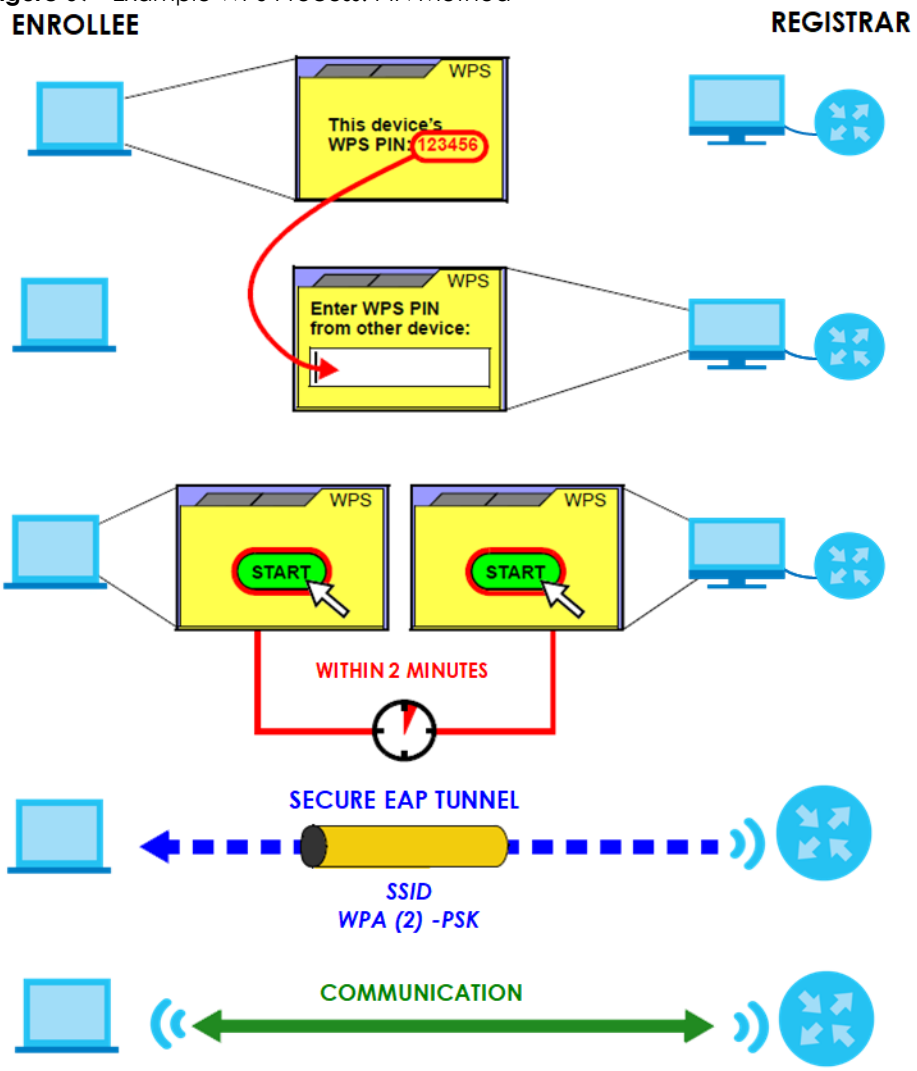
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

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 69 Example WPS Process: PIN Method

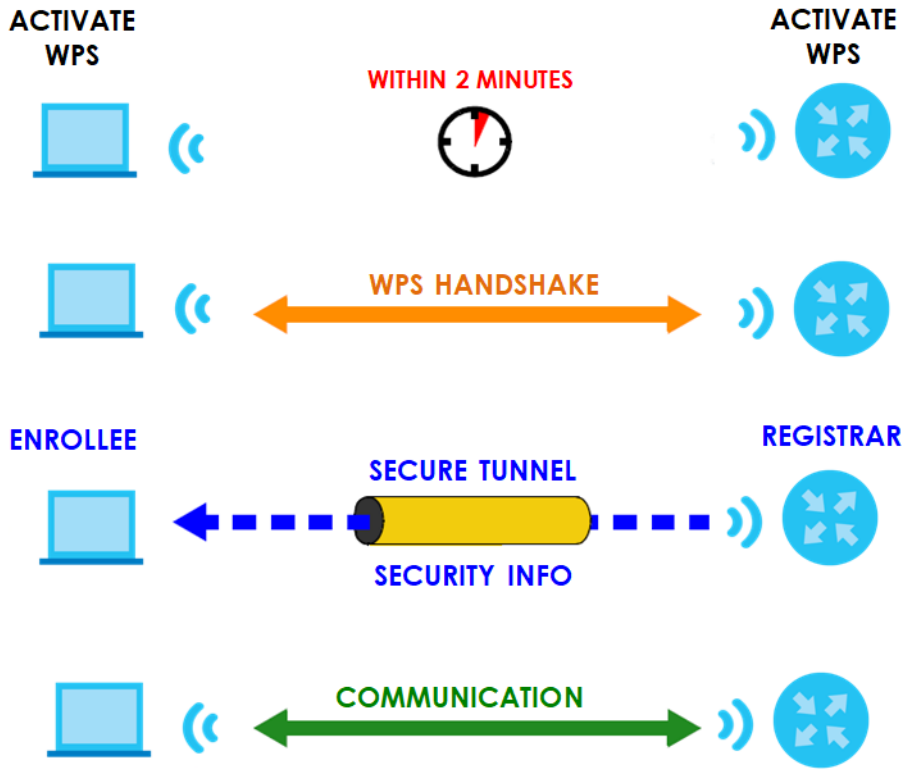


9.16.11.3 How WPS Works

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 70 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.

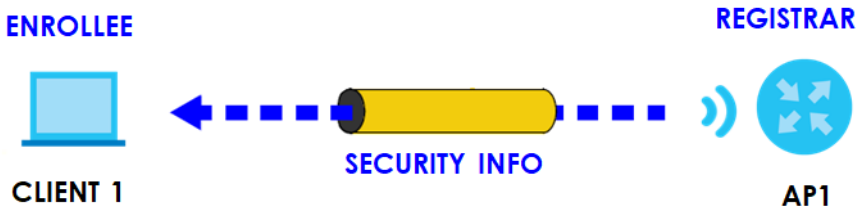
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled 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.

9.16.11.4 Example WPS Network Setup

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

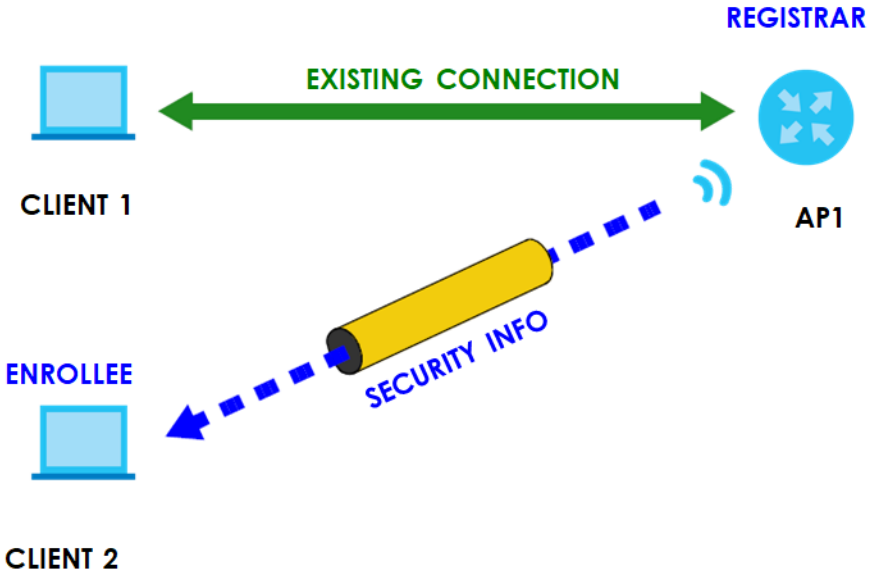
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 71 WPS: Example Network Step 1



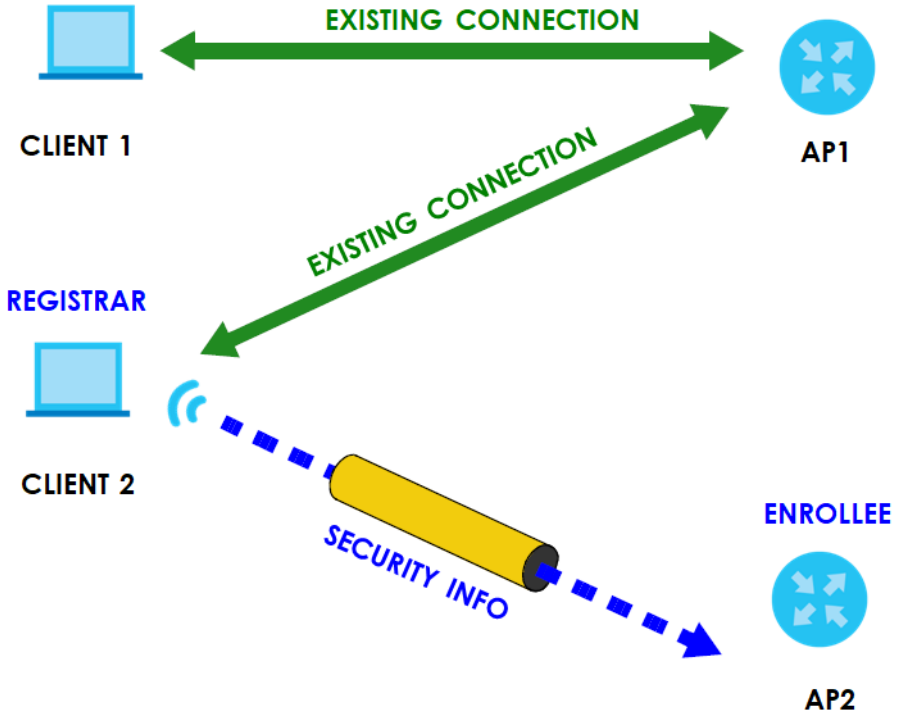
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 72 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 73 WPS: Example Network Step 3



9.16.11.5 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.

- Power
- NR2301 Access and Login
- Internet Access
- IP Address Setup

10.2 Power

The NR2301 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 NR2301 on. See (Chapter 1 on page 11.)
2. If the problem continues, contact the vendor.

10.3 NR2301 Access and Login

I forgot the IP address for the NR2301.

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 NR2301 press the **RESET** button for 3 seconds.

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 NR2301.

2 Make sure the NR2301 is correctly installed and turned on. See the Quick Start Guide and Chapter 1 on page 11.

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 NR2301 and is in the same subnet as the NR2301.

5 Make sure the NR2301's WiFi LAN is enabled. You can enable or disable the NR2301's WiFi network using WiFi Setting on the NR2301. See Chapter 1 on page 17.

6 Reset the device to its factory defaults, and try to access the NR2301 with the default IP address. To reset your NR2301 press the **RESET** button for 3 seconds. See Chapter 1 on page 11.

7 Disconnect your computer from the NR2301 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 NR2301's LCD **About** screen for the default password (see Chapter 1 on page 14 for more information).

2 If this does not work, you have to reset the device to its factory defaults. To reset your NR2301 press the **RESET** button for 3 seconds.

I can access the **Login** screen, but I cannot log in to the NR2301.

1 Make sure you have entered the user name and password correctly. The default user name is **admin** and check the NR2301's LCD **About** screen for the default password (see Chapter 1 on page 14 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 NR2301 again.

4 If this does not work, you have to reset the device to its factory defaults. To reset your NR2301 press the **RESET** button for 3 seconds.

10.4 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 NR2301.
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 NR2301's **About** screen for the default password (see Chapter 1 on page 14 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 NR2301), but my Internet connection is not available anymore.

1. Reboot the NR2301.
2. Make sure the NR2301's WiFi network is enabled. You can enable NR2301's WiFi 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 66).
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 NR2301), 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 43).
2. Make sure your SIM card's mobile data is enabled. Check this on the Web Configurator (See Chapter 4 on page 38).
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 NR2301.

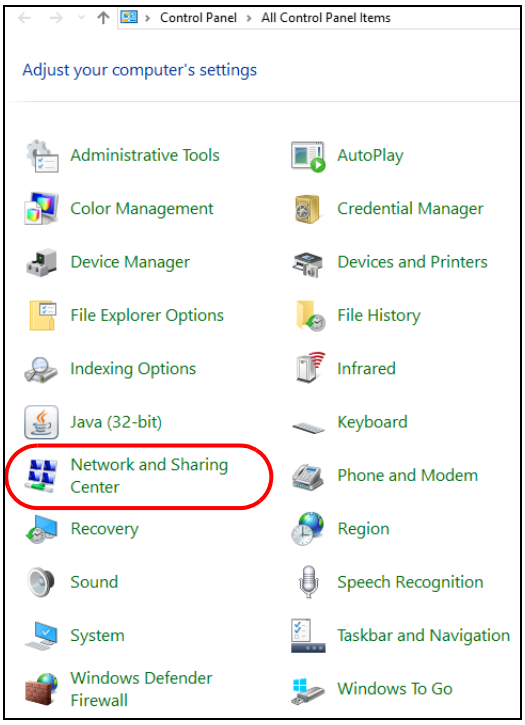
The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. If the NR2301 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 NR2301 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 WiFi network (for example, microwaves, other WiFi networks, and so on).
3. Reboot the NR2301.
4. If the problem continues, contact the network administrator or vendor.

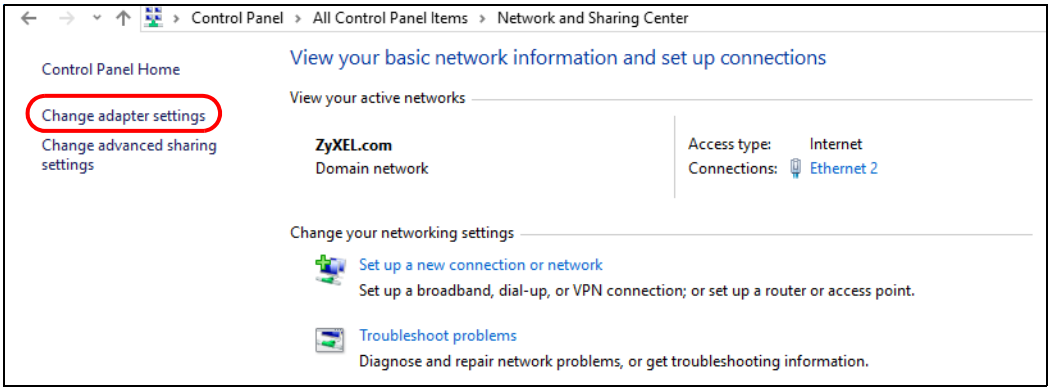
10.5 IP Address Setup

I need to set the computer's IP address to be in the same subnet as the NR2301.

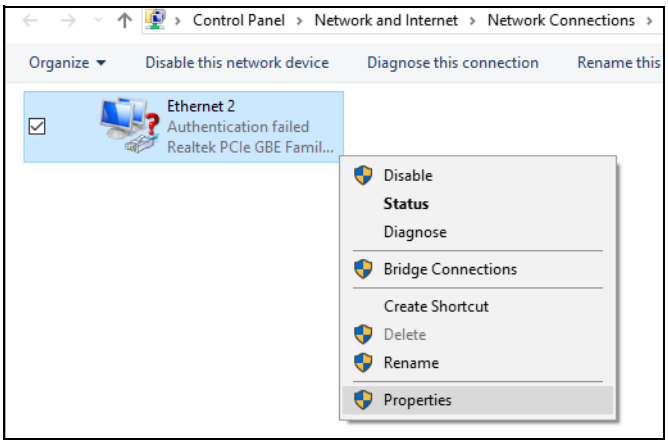
1. In Windows 10, open the **Control Panel**.
2. Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.



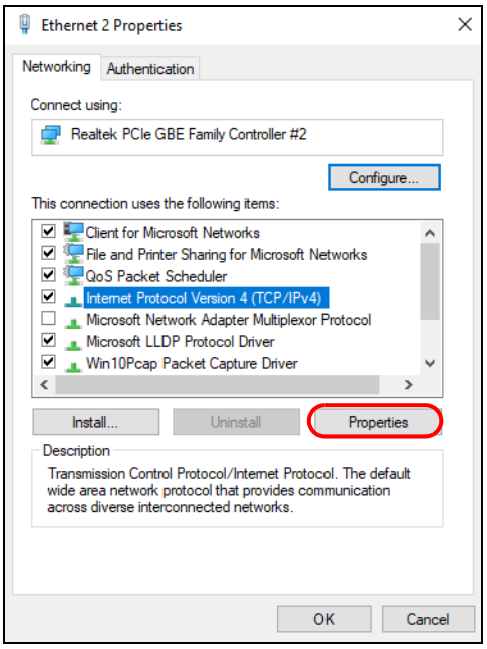
3 Click **Change adapter settings**.



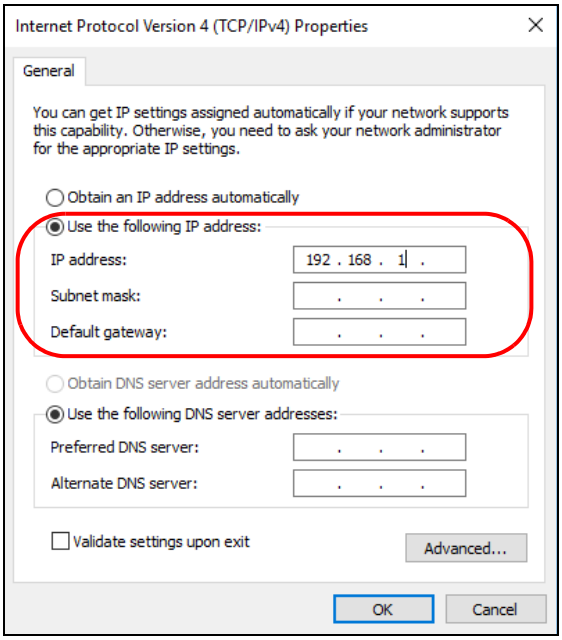
4 Right-click the **Ethernet** icon, and then select **Properties.**



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



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.



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

10.6 WiFi Connections

I cannot access the NR2301.

1. Make sure WiFi is enabled on the NR2301. You can enable or disable the NR2301's WiFi network using the **Wi-Fi Setting** screen on the NR2301's LCD screen. See Chapter 1 on page 17.
2. Make sure the WiFi adapter (installed on your computer) is IEEE 802.11 compatible and supports the same WiFi standard as the NR2301's active radio.
3. Make sure your device (with a WiFi adapter installed) is within the transmission range of the NR2301.
4. Make sure you are using the correct WiFi network name and password to connect to your NR2301. Check your WiFi network settings by reexamining the network name **Wi-Fi SSID** and/or **Wi-Fi Key** in the Web Configurator (Chapter 6 on page 48).
5. If you changed your network **Wi-Fi SSID** and/or **Wi-Fi Key** you will be automatically disconnected from the NR2301. Try reconnecting to the network wirelessly with the new **Wi-Fi SSID** and/or **Wi-Fi Key**.

One of my clients cannot access the NR2301.

1. Make sure the WiFi LAN is enabled on the NR2301. You can enable or disable the NR2301's WiFi network using the **WiFi Setting** screen on the NR2301's LCD screen. See Chapter 1 on page 17.
2. Make sure the WiFi adapter (installed on your computer) is IEEE 802.11 compatible and supports the same WiFi standard as the NR2301's active radio.
3. Make sure your client's device (with a WiFi adapter installed) is within the transmission range of the NR2301.
4. Make sure your client is using the correct WiFi network name **(Wi-Fi SSID)** and password **(Wi-Fi Key)** to connect to your NR2301 (Chapter 6 on page 48).

10.7 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

APPENDIX A
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

European Union

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/V/VIII is 24 dBm
  - LTE band 1/3/5/7/8/20/28/40 is 23 dBm
  - LTE band 38/41/42/43 is 26 dBm
  - NR band n1/n3/n5/n7/n8/n20/n28/n40 is 23 dBm
  - NR band n38/n41/n77/n78 is 26 dBm
  - WiFi:

    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) België (Flemish) Belgique (French)	**National Restrictions** • 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. • 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. • 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/ΕΕ.
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. National Restrictions • 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. • 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 alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
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/ЕС.

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 use this product near water, for example, in a wet basement or near a swimming pool.
- 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, use, 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, 110V 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.

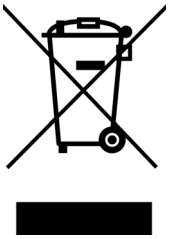
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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，使用或維修此設備。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。
- 請插在正確的電壓供給插座 (如 : 北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 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): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: 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

Numbers

802.11 Mode 51

A

access
troubleshooting 109
AP Isolation 51
APN settings 62
applications
wireless WAN 9
Authentication Type 62

B

Backup 90
Bandwidth 51
Battery 24
Black List 43

C

Calibration 67
certifications 118
Channel 51
channel 47
Configuration
restore 91, 92
Connect Mode 38
content filtering
by keyword (in URL) 73
copyright 116
CPU Occupancy 39
Current SIM Volume 39

D

DDNS 95
see also Dynamic DNS
DHCP 63
see also Dynamic Host Configuration Protocol
DHCP server 63
Diagnosis 92
disclaimer 116
Dynamic DNS 95
Dynamic Host Configuration Protocol 63

E

ESSID 115

F

filters
MAC address 45
Firewall 71
Firmware Management 89
Firmware Over the Air 19, 89
FOTA 19, 89

G

General wireless LAN screen 48
guest WiFi network 52

I

IMSI 59
International Mobile Subscriber Identity 59

Internet
no access 111
Internet access 9
Internet connection
slow or erratic 112
IP Filter 72
IP Mode 62

L

L2TP 102
L2TP VPN 102
LCD Screen Interface 10
LCD Screens 12
LEDs 12
limitations
WPS 107
Login screen
no access 110

M

MAC address
filter 45
MAC address filter 47
MAC authentication 45
MAC Filter Mode 43
Maximum Transfer Unit 65
mobile data usage control 66
MTU 65

N

NAT Traversal 100
Network Information 58
Network Mode 62
Network Status 38

O

Online Update 89
overview 9

P

password
admin 110
lost 110
user 110
PBC 102
PIN, WPS 103
example 104
PLMNs 62
Point-to-Point Tunneling Protocol 101
Port Filter 78
Port Forward 74, 98
Port forwarding
example 98
Port Trigger 76
power button 11
PPTP 101
Public Land Mobile Networks 62
Push Button Configuration, see PBC
push button, WPS 102

R

RAT Mode 58
Reboot 91
Received Signal Strength Indicator
RSSI 59
Reference Signal Receive Power
RSRP 59
Reference Signal Received Quality
RSRQ 59
Remote management 80
Restore configuration 91, 92
Roaming 59
Roaming Mode 62
router features 9

S

Security Mode 50
Service Set 50, 52
Service Set IDentification 50, 52
Service Set IDentity. See SSID.
Short Message Service 83
Signal Strength 24
Signal to Interference plus Noise Ratio
  SINR 59
SMS 83
SSID 47, 50, 52
SSID Broadcast 51
Statistics 57
status 38

T

TCP/IP configuration 63
The Layer 2 Tunneling Protocol 102
time schedule 53
Transmission 24
trigger port 99
Trigger port forwarding 99
  example 99
  process 99
troubleshooting 109

U

Universal Plug and Play 79
  Application 100
  Security issues 100
UPnP 79
URL Filter 73
USB Tethering 10
User List 40
User Name 96

V

VPN 82
VPN Passthrough 96

W

warranty 120
  note 120
Web Configurator 22
White List 44
Wi-Fi 47
WiFi
  WPS 102, 104
    example 105
    limitations 107
    PIN 103
    push button 102
wireless channel 115
wireless LAN 47, 115
  MAC address filter 45
Wireless network
  channel 47
  MAC address filter 47
  security 47
  SSID 47
Wireless security 47
  overview 47
  type 47
wireless security 115
Wireless tutorial 28
WPS 102, 104
  example 105
  limitations 107
  PIN 103
    example 104
  push button 102