



renkforce

User Manual

N300 Wi-Fi Access Point

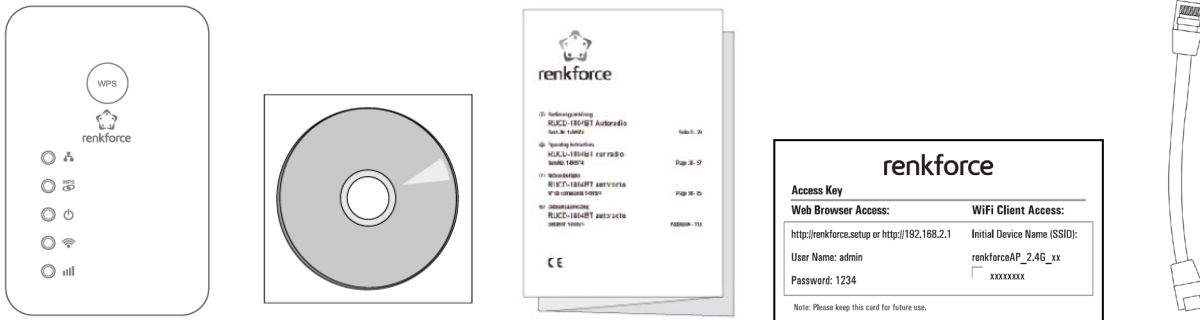
Item No. 1606296

CONTENTS

I	Product Information	1
I-1	Package Contents	1
I-2	System Requirements.....	1
I-3	LED Status	1
I-4	Hardware Overview	3
I-5	Safety Information.....	4
II	Installation	5
III	Reset to Factory Default Settings	6
IV	Browser Based Configuration Interface	8
IV-1	Access Browser Based Interface.....	8
IV-2	Apply Settings.....	8
IV-3	Main Menu	10
V	Access Point Mode	11
V-1	Home	11
V-2	iQ Setup.....	13
V-3	Basic Settings	16
V-3-1	Multiple SSID	16
V-3-2	Show Active Clients.....	17
V-4	WPS Settings	19
V-5	Wireless Advanced.....	21
V-5-1	Security	23
V-5-1-1	Disable	23
V-5-1-2	WEP	24
V-5-1-3	WPA pre-shared key	24
V-5-1-4	WPA RADIUS	25
V-5-2	MAC Filtering	25
V-5-3	Time Settings.....	27
V-5-4	Scheduling Setting	28
V-5-4-1	Add	28
V-5-5	Administration Utility.....	28
V-5-6	Configuration Tools.....	31
V-5-6-1	Manage Settings.....	32
V-5-6-2	Upgrade Firmware	32
V-5-6-3	Reboot	32
V-5-6-4	System Log	32
VI	Appendix	32
VI-1	Connecting to a Wi-Fi network.....	32
VI-2	Troubleshooting	33

I Product Information

I-1 Package Contents








- GRP-438N
- CD with multi-language QIG & user manual
- Quick installation guide (QIG)
- Access key card
- RJ45 cable

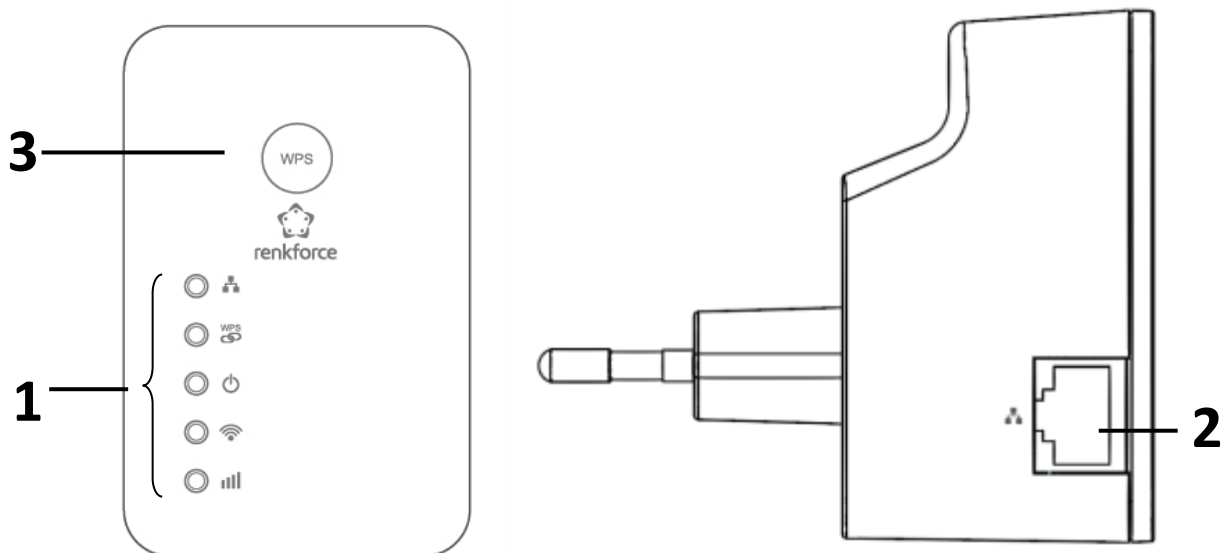
I-2 System Requirements

- Wi-Fi extender/Wi-Fi bridge mode: Existing 2.4GHz wireless network
- Access point mode: Cable/DSL modem router
- Computer with 2.4GHz 802.11/b/g/n Wi-Fi adapter, and web browser for software configuration (Internet Explorer 8® or above, Google Chrome®, Firefox® or Safari® latest version)
- Smartphone setup: iOS 6 or Android 4.x and above

I-3 LED Status

LED	Color	Status	Description
Signal Strength  2.4GHz	Amber	On	Excellent signal Signal strength: 60 – 100%
		Slow Flashing	Good signal Signal strength: 40 – 60%
		Quick Flashing	Poor signal Signal strength: 0 – 40%
		Off	No signal detected, disconnected, or in LED off mode
Wi-Fi 	Green	Flashing	Transferring data
		Off	Wi-Fi not active or in LED off mode
Power 	Green	On	Extender is on
		Flashing	Resetting to factory default settings, or system is booting up
		Off	Extender is off or in LED off mode
WPS 	Green	On	WPS connection established (LED will remain on for 5 minutes to indicate a successful connection)
		Flashing	WPS in progress (waiting for another WPS device)
		Off	No WPS in progress or in LED off mode
LAN 	Green	On	LAN port connected
		Flashing	LAN activity (transferring or receiving data)
		Off	LAN port not connected

I-4 Hardware Overview



1. LEDs
2. Ethernet Port
3. WPS/Reset Button

I-5 Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

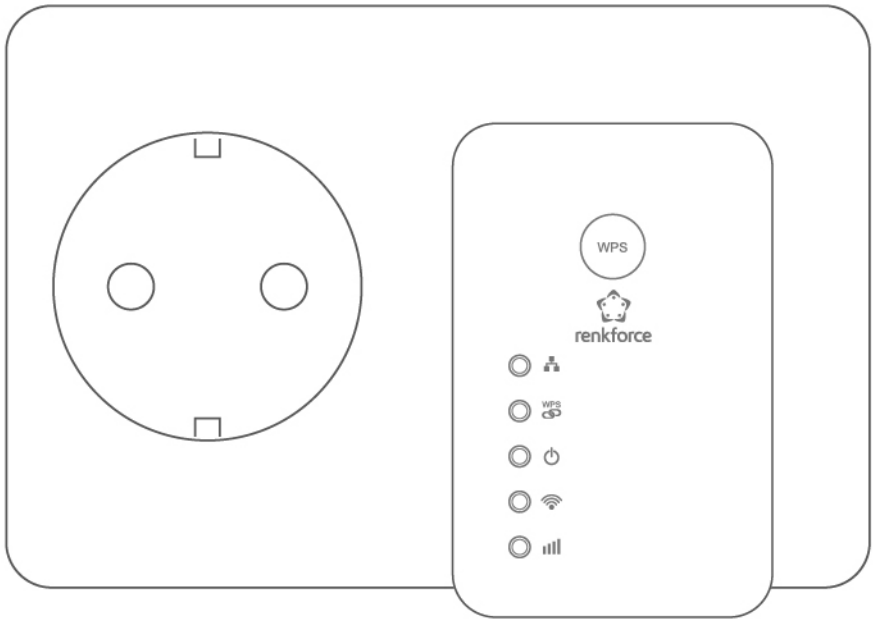
1. The device is designed for indoor use only; do not place it outdoors.
2. Do not place the device in or near hot/humid places, such as a kitchen or bathroom.
3. Do not pull any connected cable with force; carefully disconnect it from the GRP-438N.
4. Handle the device with care. Accidental damage will void the warranty of the device.
5. The device contains small parts which are a danger to small children under 3 years old. Please keep the device out of reach of children.
6. Do not place the device on paper, cloth, or other flammable materials. The device may become hot during use.
7. There are no user-serviceable parts inside the device. If you experience problems with the device, please contact your dealer of purchase and ask for help.
8. The device is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.
9. If you smell burning or see smoke coming from the GRP-438N then unplug the device immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.
10. This product should work for a long time, and provide round-the-clock Wi-Fi service.

II Installation

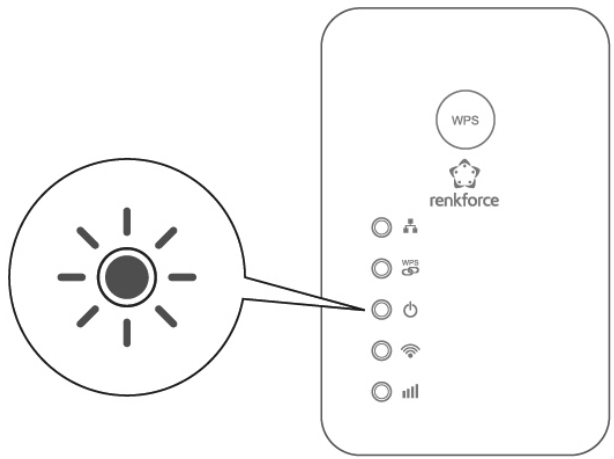
Wi-Fi Access Point	The device connects to an existing router via Ethernet cable and provides wireless Internet access for your network devices. Location: Connected to your router via Ethernet cable.
---------------------------	---

Follow the steps below to setup your access point:

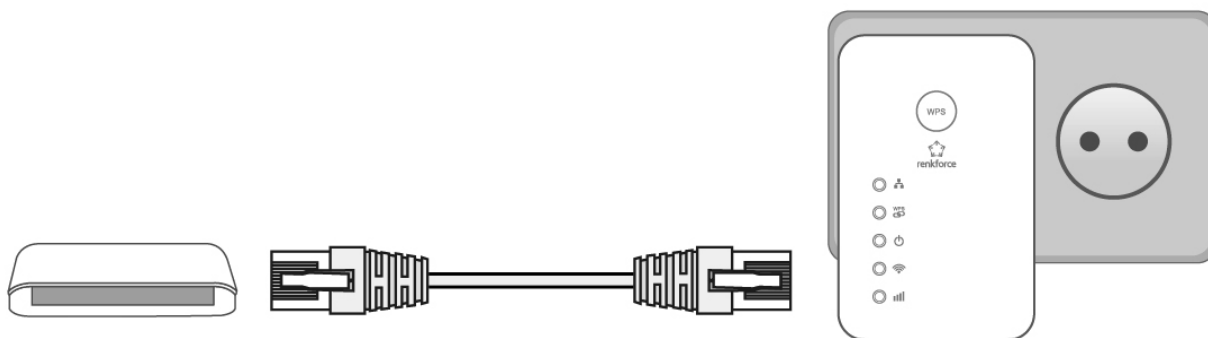
1. Plug the unit into a power socket.



2. The **green** power LED will **flash** while the system is booting up. The unit is ready when the **green** power LED displays **on**.



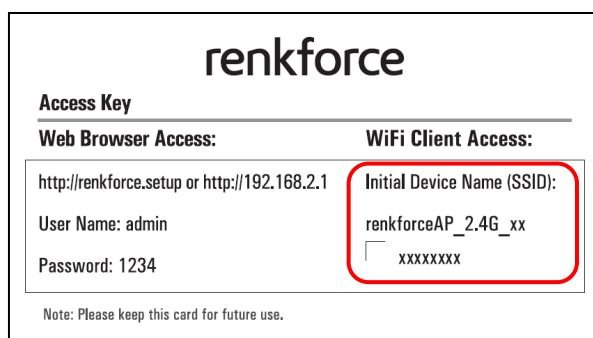
3. Connect the LAN port of the unit to the LAN port of your existing router using an Ethernet cable.



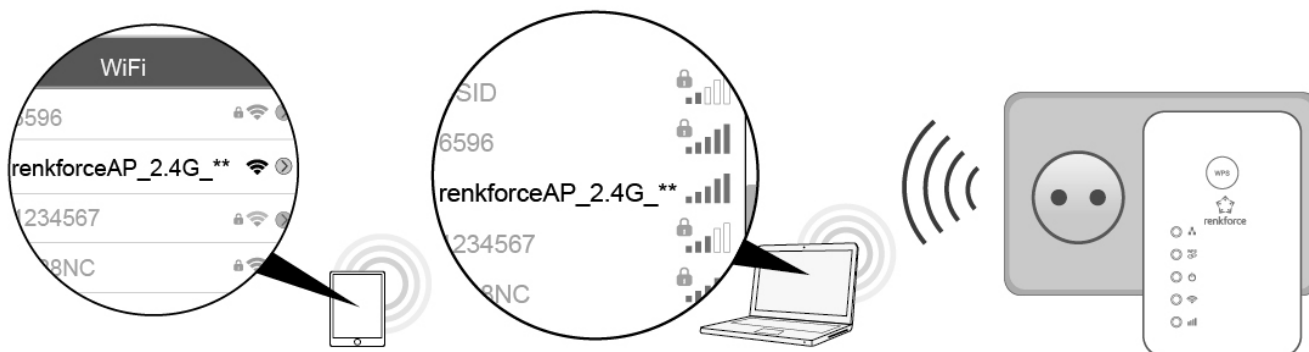
4. Please wait for ~2 minutes for auto network configuration.

Congratulations! You can now use the Access Point to connect to your router's network!

By default, the Access Point's SSID (Wi-Fi name) and password is shown on your Access Key Card. An example of the Access Key Card is shown below:



An example of how some of the devices may see the Access Point's SSID is shown below:

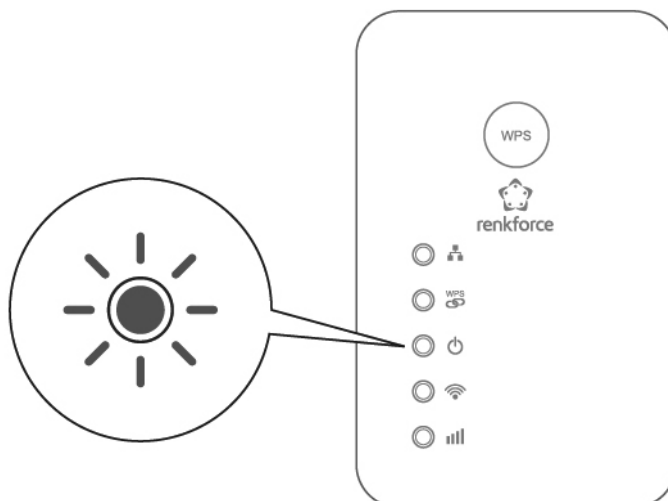


The last two characters of the SSID (renkforceAP_2.4G_**) are unique alphanumeric characters and will vary depending on your device. e.g. "renkforceAP_2.4G_f8".

Should you wish to change the SSID (Wi-Fi name), please follow the instructions in **V-2 iQ Setup** or see the information in **V-3 Basic Settings**.

III Reset to Factory Default Settings

If you experience problems with your access point, you can reset the device back to its factory settings. This resets **all** settings back to default.



1. Press and hold the WPS/Reset button for at least 10 seconds and release when the **green** power LED is **flashing**.
2. Wait for the extender to restart. The extender is ready for setup when the **green** power LED displays **on**.

IV Browser Based Configuration Interface

After you have setup the unit as detailed in **II Installation** or the included **Quick Installation Guide**, you can use the browser based configuration interface to configure advanced settings.

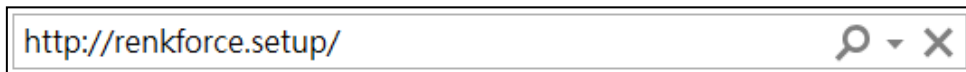


Please ensure that your computer is set to use a dynamic IP address.

IV-1 Access Browser Based Interface

To access the browser based interface, please first make sure that you are connected to the unit's Wi-Fi network and follow the instructions below:

1. Open a web browser and enter the URL **http://renkforce.setup**.



If you cannot access **http://renkforce.setup**, please make sure your computer is set to use a dynamic IP address.

2. You will be prompted a username and password, please type in the username (**admin**) and password (**1234**) shown in the Access Key card.

Authentication required

http://renkforce.setup
Your connection to this site is not private

Username

Password

3. You should be taken to the dash board of the unit as shown below:

renkforce Wi-Fi Access PointEnglish

- Home
- iQ Setup
- Basic Settings
- WPS Setting
- Advanced Setting

Status and Information

You can check the device's MAC address, runtime code, hardware version, and network status below.

System	
Current Time	0:59:26 2000/1/1
Uptime	0Day:0h:54m:22s
Hardware Version	1.1.1
Firmware version	1.0.1 Upgrade Firmware
Mode	AP

Wireless Configuration	
SSID	renkforceAP_2.4G_F8
Channel Number	11
Security	WPA-Shared Key
BSSID (MAC)	11:11:11:11:11:F8
Associated Clients	1 Show Active Clients
State	Connected

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC Address	11:11:11:11:11:F8

IV-2 Apply Settings

For the changes made on the browser interface to take effect, you will have to apply the changes.

1. If you wish to save the changes made on the browser interface, please click "APPLY".

renkforce Wi-Fi Access Point English

Basic Settings

This page allows you to define SSID and channel number for the wireless connection. These parameters are used for wireless stations to connect to the access point.

Mode	AP
Band	2.4 GHz (B+G+N)
Main SSID	renkforceAP_2.4G_18 Multiple SSID
AP Isolation (Client user isolation)	Disabled
Channel Number	11
Associated Clients	Show Active Clients

Cancel APPLY

A "Settings saved successfully" message will be shown

Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE APPLY

2. Select "CONTINUE" to save current changes, return to the previous page, and continue the browser configuration.
Or select "APPLY" to restart the unit and bring the changes into effect. The following is shown when the unit is being restarted:

System restarting. Please wait for a moment.

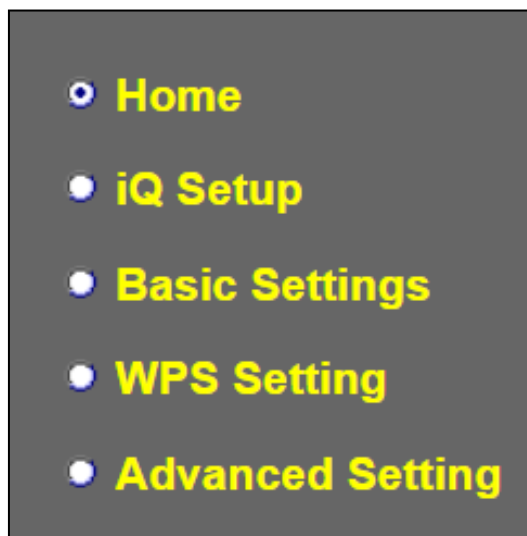
4%



Tip: The unit needs to restart in order to apply and bring any changes into effect. Use the "CONTINUE" button to make several changes and apply them all together in one restart.

IV-3 Main Menu

The Access Point main menu is displayed as shown below:



V Access Point Mode

V-1 Home

The "Status and Information" page displays basic system information about the device, arranged into three categories: system, wireless configuration & LAN configuration.



Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

Status and Information

You can check the device's MAC address, runtime code, hardware version, and network status below.

System	
Current Time	0:59:26 2000/1/1
Uptime	0Day:0h:54m:22s
Hardware Version	
Firmware version	<input type="button" value="Upgrade Firmware"/>
Mode	AP

Wireless Configuration	
SSID	renkforceAP_2.4G_f8
Channel Number	11
Security	WPA-Shared Key
BSSID (MAC)	
Associated Clients	1 <input type="button" value="Show Active Clients"/>
State	Connected

LAN Configuration	
IP Address	
Subnet Mask	
Default Gateway	
MAC Address	

System	
Current Time	Displays the current time and date.
Uptime	Displays the total time since the device was turned on.
Hardware Version	Displays the hardware version.
Firmware Version	Displays the firmware version.
Mode	Displays the operating mode.
Wireless Configuration	
SSID	Displays the access point's SSID. The SSID is the name used to identify a wireless network.
Channel Number	Displays the current wireless channel number.
Security	Displays the current wireless security setting.
BSSID (MAC)	Displays the unit's BSSID. The BSSID identifies this access point in the network, and is the same as the device's MAC address.
Associated Clients	Displays the number of clients connected to the access point. Click "Show Active Clients" to display a new window showing information about wireless clients.
State	Displays the current connection state of the unit.
LAN Configuration	
IP Address	Displays the IP address of this unit.
Subnet Mask	Displays the subnet mask of the IP address.
Default Gateway	Displays the IP address of the default gateway.
MAC address	Displays the device's MAC address. The MAC address is a unique, fixed ID for this device, it cannot be modified.

V-2 iQ Setup

Follow the step-by-step process to go through the basic settings of the access point.
For more detailed information of the settings shown below, please refer to the following chapters.

- 1. Management IP:** Manage the IP settings of your network.
Select "Obtain an IP address automatically" or "Use the following IP address" for your GRP-438N.
If you are using a static IP, enter the IP address, subnet mask, default gateway and DNS. Click "Next" to proceed to the next step.



"Obtain an IP address automatically" is the recommended setting for most users.

Management IP

Please set the IP address of the access point. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click Next to proceed to the next step.

Obtain an IP address automatically.

Use the following IP address.

IP Address : . . .

Subnet Mask : . . .

Gateway Address : . . .

DNS : . . .

- 2. Change Basic Setting**
Enter / edit the Wi-Fi network name and select whether the network requires a password. If required, enter a password.

Change Basic Setting

Wi-Fi Network Name	<input type="text" value="renkforceAP_2.4G_f8"/>
Wi-Fi Network Password	Enabled ▼ <input type="text" value="baccfbcf"/>
Enable Guest Network	<input type="radio"/> Yes <input checked="" type="radio"/> No


Enable Guest Network: Check the "Yes" checkbox to enable. Enter / edit the guest network name and select whether the network requires a password. If required, enter a password.

Change Basic Setting	
Wi-Fi Network Name	renkforceAP_2.4G_f8
Wi-Fi Network Password	Enabled ▾ baccfbcf
Enable Guest Network	<input checked="" type="radio"/> Yes <input type="radio"/> No
Guest Network Name	Guest Network
Guest Wi-Fi Password	Enabled ▾ 12345678
<input type="button" value="BACK"/> <input type="button" value="NEXT"/>	

3. The page will show its basic settings, click "APPLY" to apply the settings (the system will restart) or click "BACK" to go to the previous step.

Settings saved successfully!	
Please click APPLY to restart the system and make the changes take effect.	
Wi-Fi Network Name :	renkforceAP_2.4G_f8
Wi-Fi Network Password :	baccfbcf
Guest Network Name :	Guest Network
Guest Wi-Fi Password :	12345678
<input type="button" value="BACK"/> <input type="button" value="APPLY"/>	

4. Please wait a moment for the unit to be ready.

System is restarting. Please wait for a moment.	
	
Reminder: Your Wi-Fi will disconnect from the extender during the system restart (approximately 1 minute). When the system is complete, please connect to the extender's new SSID using the password below.	
Wi-Fi Network Name :	renkforceAP_2.4G_f8
Wi-Fi Network Password :	baccfbcf
Guest Network Name :	Guest Network
Guest Wi-Fi Password :	12345678

5. A final congratulations screen will indicate that setup is complete. The unit is working and ready for use. You can now reconnect to the unit's network.

Congratulations.

You have successfully completed the configuration. You can close this browser window and reconnect to this AP device with new wireless security key now.

Wi-Fi Network Name : renkforceAP_2.4G_f8

Wi-Fi Network Password : baccfbcf

Guest Network Name : Guest Network

Guest Wi-Fi Password : 12345678

V-3 Basic Settings

The “Basic Settings” screen displays various settings for your wireless network.

Basic Settings

This page allows you to define SSID and channel number for the wireless connection. These parameters are used for wireless stations to connect to the access point.

Mode	AP
Band	2.4 GHz (B+G+N) ▼
Main SSID	renkforceAP_2.4G_f8 <input type="button" value="Multiple SSID"/>
AP Isolation (Client user isolation)	Disabled ▼
Channel Number	11 ▼
Associated Clients	<input type="button" value="Show Active Clients"/>

Mode	The unit’s operation mode is displayed here.
Band	Displays the wireless standard used for the unit. “2.4GHz (B+G+N)” means that 802.11b, 802.11g, and 802.11n wireless clients can connect to the unit.
MAIN SSID	This is the name of your Wi-Fi network for identification, also known as “SSID”. The SSID can be consisted of any combination of up to 32 alphanumerical characters.
Multiple SSID	Click “Multiple SSID” to open a new window and assign one more SSID to this access point. Please see below for more details.
AP Isolation	When “Enabled”, wireless clients will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.
Channel Number	Select a wireless radio channel or use the default “Auto” setting from the drop-down menu.
Associated Clients	Click “Show Active Clients” to display a new window showing information about wireless clients. Please disable any pop-up blockers if you have difficulty using this function.

V-3-1 Multiple SSID

This page allows you to configure an extra SSID's wireless settings.

Multiple SSID

This page allows you to configure the wireless settings for Multiple SSIDs. The wireless security settings for these SSIDs can be configured in Security page.

No.	Enabled	Associated Clients	Basic Settings		Advanced Setting		
			SSID	Broadcast SSID	WMM	Band	AP Isolation (Client user isolation)
SSID1	<input type="checkbox"/>	Show Active Clients	Guest Network	Enabled ▼	Disabled ▼	2.4 GHz (B+G+N) ▼	Disabled ▼

No.	Identification number of the additional SSID.
Enable	Check the box to enable or disable the SSID.
Associated Clients	Click "Show Active Clients" to display a new window showing information about wireless clients.
SSID	Enter / edit the SSID (the name used to identify this wireless network). You can input up to 32 alphanumerical characters. Please note that the SSID is case sensitive.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When WMM is enabled, the access point will prioritize different kinds of data and give higher priority to applications which require instant responses. This improves the performance of such network applications.
Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Clients can only connect to the selected wireless bands.
AP Isolation	When "Enabled", wireless clients will be able to access the Internet, but will not be able to communicate with each other.

V-3-2 Show Active Clients

This page displays information of the connected wireless clients.

Active Wireless Client Table

This table shows the MAC address, transmitted packets, and received packet of each connected wireless client.

MAC Address	Mode	Tx Packets	Rx Packets	Tx Rate (Mbps)	Power saving	Expire Time
56:3e:3b:7d:90:a0	11n	190978	96733	270	no	300
56:3e:3b:7d:90:01	11n	190978	96733	270	no	300
56:3e:3b:7d:90:a1	11n	190978	96733	270	no	300

Click "Refresh" to refresh the client list.

Click "Close" to close the window.

V-4 WPS Settings

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. PIN code WPS includes the use of a PIN code between the two devices for verification.

The WPS Settings page displays settings for WPS between your extender and a **wireless client**.

WPS (Wi-Fi Protected Setup) Settings

This page allows you to configure WPS (Wi-Fi Protected Setup) settings. WPS allows wireless clients to connect to this device automatically.

Note: WPS function will be disabled if your wireless security uses WEP or WPA (TKIP) encryption.

WPS Setting	<input checked="" type="radio"/> 2.4GHz
-------------	---

- 2.4G Wi-Fi Protected Setup Information**

WPS Status	Configured
Self PinCode	04015284
Device SSID	renkforceAP_2.4G_f8
Security Type	WPA pre-shared key
Passphrase Key	baccfbcf

- Device Configure**

Configuration Mode Device is as an AP	Registrar
Configure via Push Button	<input type="button" value="Start PBC"/>
Input Client PIN Code	<input type="text"/> <input type="button" value="Send PIN"/>

WPS Status	Displays "Configured" or "unConfigured" depending on whether WPS and SSID/security settings for the unit have been configured or not, either manually or using the WPS button.
Self PIN Code	Displays the WPS PIN code of the unit.
Device SSID	Displays the SSID of the unit.
Security Type	Displays the wireless security authentication mode of the device.
Passphrase Key	Displays the wireless security authentication key (or the password of the Wi-Fi network).
Device Configure	
Configuration Mode	The configuration mode of the unit's WPS setting is displayed here. "Registrar" means the unit acts as an access point for a wireless client to connect to and the wireless client(s) will follow the unit's wireless settings.
Configure via Push Button	Click "Start PBC" (Push-Button Configuration) to activate WPS on the unit. WPS will be active for 2 minutes.
Input Client PIN Code	Enter the wireless client's PIN code here and click "Send PIN" to send PIN code to the WPS-enabled device. Refer to your WPS-enabled device's documentation if you are unsure how to obtain its PIN code.

V-5 Wireless Advanced

Using the “Advanced Setting” menu, you can configure security, MAC filtering and various other settings.

The settings on the “Advanced Setting” page shown below are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.



Changing these settings can adversely affect the performance of your access point.

Wireless Advanced Setting

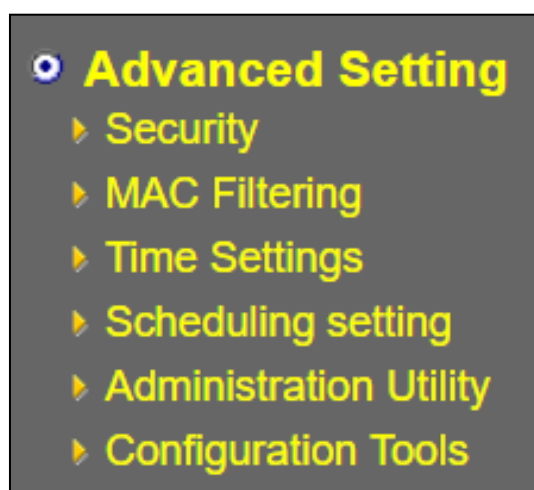
These settings are only for more technical advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effects the changes will have.

Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(0-2347)
Beacon Interval	100	(20-1024 ms)
DTIM Period	3	(1-10)
Data Rate	Auto ▼	
N Data Rate	Auto ▼	
Channel Width	<input checked="" type="radio"/> Auto 20/40MHz <input type="radio"/> 20MHz	
Preamble Type	<input checked="" type="radio"/> Short Preamble <input type="radio"/> Long Preamble	
Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
CTS Protect	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power	100 % ▼	

Fragment Threshold	Set the Fragment threshold of the wireless radio. The default value is 2346.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM period of wireless radio. The default value is 3.
Data Rate	Set the wireless data transfer rate. The default is set to auto.
N Data Rate	Set the data rate of 802.11n. The default is set to auto.
Channel Width	Select wireless channel width (bandwidth used by wireless signals from the device) – the recommended value is Auto 20/40MHz.

Preamble Type	Set the wireless radio preamble type. The default value is "Short Preamble".
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID. WPS (Wi-Fi Protected Setup) is also disabled when SSID broadcast is disabled.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It's recommended to set this option to "Auto".
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.

The menu of the Advanced Setting is shown below, with the following sections containing the viewable / configurable information.



V-5-1 Security

The access point provides a variety of wireless security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the encryption key. The "Security" screen displays security settings for the unit.

Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- Select SSID**

Device SSID	renkforceAP_2.4G_f8 ▼
-------------	-----------------------
- Security Settings**

Security Type	WPA pre-shared key ▼
WPA Unicast Cipher Suite	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-Shared Key Format	Passphrase ▼
Security Key	baccfbcf

Select SSID	
Device SSID	Select which SSID to configure security settings for.
Security Settings	
Security Type	Select a security type and refer to the next sections for more details about each security type.

V-5-1-1 Disable

“Disable” is selected as the security type where no password/key is required to connect to the unit.



Disabling wireless encryption is not recommended. When disabled, anybody within range can connect to your device’s SSID.

• Security Settings	
Security Type	Disable ▼
<input type="checkbox"/> Enable 802.1x Authentication	

Enable 802.1x Authentication	Check the box to enable the 802.1x authentication. A RADIUS server is required to perform 802.1x authentication.
-------------------------------------	--

V-5-1-2 WEP

“WEP” is selected as the security type. WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security, please consider using WPA encryption.



WEP supports data rates up to 54Mbps.

• Security Settings	
Security Type	WEP ▼
Key Length	64-bit ▼
Key Format	HEX (10 Characters) ▼
Default Key	Key 1 ▼
Security Key	<input type="text"/>
<input type="checkbox"/> Enable 802.1x Authentication	

Key Length	Select 64-bit or 128bit. 128-bit is more secure than 64-bit.
Key Format	Choose from “ASCII” (any alphanumeric character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Encryption Key	Enter your encryption key/password according to the format you selected above. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.
Enable 802.1x Authentication	Check the box to enable the 802.1x authentication. A RADIUS server is required to perform 802.1x authentication.

V-5-1-3 WPA pre-shared key

WPA pre-shared key is the recommended and most secure encryption type.



WPA (TKIP) supports data rates up to 54Mbps.

• Security Settings	
Security Type	WPA pre-shared key ▼
WPA Unicast Cipher Suite	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-Shared Key Format	Passphrase ▼
Security Key	baccfbcf

WPA Unicast Cipher Suite	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP). Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
Pre-shared Key Format	Choose from "Passphrase" (8 – 63 alphanumeric characters) or "Hex" (up to 64 characters from 0-9, a-f and A-F).
Pre-shared Key	Enter / edit key according to the format you selected above. A complex, hard-to-guess key is recommended. Check the "Hide" box to hide your password from being displayed on-screen.

V-5-1-4 WPA RADIUS

WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can authenticate the identity of every wireless client against a user database.

• Security Settings	
Security Type	WPA RADIUS ▼
WPA Unicast Cipher Suite	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

WPA Unicast Cipher Suite	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP). Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
RADIUS Server IP address	Input the IP address of the RADIUS authentication server here.
RADIUS Server Port	Input the port number of the RADIUS authentication server here. The default value is 1812.
RADIUS Server Password	Input the password of the RADIUS authentication server here.

V-5-2 MAC Filtering

The MAC filtering feature allows you to define a list of wireless devices permitted to connect to this access point, identified by their unique MAC address. When this feature is enabled, devices which are not on the list of permitted MAC addresses cannot connect to the access point.

MAC Address Filtering

With MAC address filtering set up, only authorized MAC addresses can be associated to this device.

Select SSID renkforceAP_2.4G_f8 ▼

- MAC Address Filtering Table**
 Only 32 entries are allowed.

NO.	MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			
- Enable Wireless Access Control**

New	MAC Address: <input style="width: 95%;" type="text"/>	Comment: <input style="width: 95%;" type="text"/>	<input type="button" value="Add"/> <input type="button" value="Clear"/>
-----	--	--	---

MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.

Delete Selected/ Delete All	Delete selected or all entries from the table.
Reset	De-select all selected entries.

To enable the MAC filtering function, check the box labeled "Enable Wireless Access Control".

MAC address	Enter a MAC address of computer or network device without dashes or colons e.g. for MAC address 'aa-bb-cc-dd-ee-ff' enter 'aabbccddeeff'.
Comment	Enter a comment for reference/identification consisting of up to 16 alphanumerical characters.
Add	Click "Add" to add the MAC address to the MAC address filtering table.
Clear	Clear all fields.

V-5-3 Time Settings

Time Zone

Set the time zone of the extender by synchronizing with Network Time Protocol server, the time will be used for Wi-Fi scheduling function.

Set Time Zone	(GMT-12:00)Eniwetok, Kwajalein ▼
Time Server Address	pool.ntp.org ▼
Daylight Savings	<input type="checkbox"/> Enable Function January ▼ 1 ▼ To January ▼ 1 ▼

Set Time Zone	Select the time zone of your country or region.
Time Server Address	The access point supports NTP (Network Time Protocol), select a time server from the drop down menu.
Daylight Savings	If your country/region uses daylight saving time, please check the "Enable Function" box, and select the start and end date.

V-5-4 Scheduling Setting

Scheduling setting

Scheduling function can be configured below for specific service.

Schedule Table (Up to 10 sets) : Enable Disable

NO.	Service	Schedule description	Schedule	Select
1	Wireless off		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Add	Click to add a new schedule in a new window (see below).
Edit	Edit an existing schedule in a new window.
Delete	Delete the specified schedule.

V-5-4-1 Add

When you click "Add" to add a new schedule, a new window will open as shown below:

Service : Schedule description :

	Start Time (hh.mm)	End Time (hh.mm)	Select
Sunday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Monday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Tuesday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Wednesday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Thursday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Friday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Saturday	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>
Every day	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="text" value="0"/> : <input type="text" value="0"/>	<input type="checkbox"/>

1. Select which function to schedule using the "Service" drop down menu.
2. (Optional) Enter a name for the schedule in the "schedule description" box.
3. Specify a start and end time (hours and minutes) using the drop-down menus.
4. Check the day(s) you wish the schedule to apply to in the "Select" column and click "APPLY" to save the schedule, or "Back" to cancel and go back to the previous screen.



If you need to use the access point during a scheduled off period, press the WPS/Reset button once to "wake up" the unit and resume Wi-Fi coverage.

V-5-5 Administration Utility

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes. You can also configure the unit's IP address.



Please make a note of the new password. In the event that you forget the password and are unable to login to the browser based configuration interface, see III Reset to Factory Default Settings for how to reset the device.

Administration Utility

If you wish to customize the login information for your Access Point, please enter the new user name and password in the following columns. If you want to set up a DHCP server, you need to assign this device an unique IP address.

- Password Settings**

Current Password	<input type="text"/>
New Password	<input type="text"/>
Re-Enter Password	<input type="text"/>
- Management IP**

<input checked="" type="radio"/> Obtain an IP address automatically	
<input type="radio"/> Use the following IP address	
IP Address	<input type="text" value="192.168.2.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text"/>
DNS	<input type="text"/>
- DHCP Server**

DHCP Server	<input type="text" value="Disabled"/>
Default Gateway	<input type="text" value="192.168.2.1"/>
Start IP	<input type="text" value="192.168.2.100"/>
End IP	<input type="text" value="192.168.2.200"/>
Lease Time	<input type="text" value="Forever"/>

Password Settings	
Current Password	Enter your current password.

New Password	Enter your new password.
Confirmed Password	Confirm your new password.
Management IP	
IP Address	Specify an IP address here. This IP address will be assigned to your unit.
Subnet Mask	Input the subnet mask of the new IP address.
Gateway Address	Input the network's gateway IP address.
DNS	Enter the DNS address here.
DHCP Server	
DHCP Server	Enable or disable the DHCP server.
Default Gateway	Input the network's gateway IP address.
Start IP	Enter the start IP address for the DHCP server's IP address leases.
End IP	Enter the end IP address for the DHCP server's IP address leases.
Lease Time	Select a lease time for the DHCP leases here. The DHCP client will obtain a new IP address after the period expires.

V-5-6 Configuration Tools

The "Configuration Tools" menu allows you to backup the unit's settings, restore the settings to a previous version or restore the unit back to its factory default state. You can also upgrade the firmware, reboot the device and export system log.

Configuration Tool

Manage Settings

Save the current settings of the device to a .bin file, restore the settings of the device to a previously saved .bin file or reset the device to its factory default settings.

Backup Settings :

Restore Settings : No file chosen

Restore to Factory Defaults :

Upgrade Firmware

Upgrade the firmware to the most recent version - it is recommended that you use a wired connection for the procedure.

No file chosen

Reboot

In the event that the device malfunctions or is not responding, you can perform a system reboot. Click on Apply - this will reboot the device, without affecting your existing settings.

System Log

V-5-6-1 Manage Settings

Backup current settings, restore to a previous setting or restore the unit to the factory default settings in this section.

Backup Settings	Click "Save" to save the current settings on your computer as config.bin file.
Restore Settings	Click "Browse" to find a previously saved config.bin file and then click "Upload" to replace your current settings.
Restore to Factory Default	Click "Reset" to restore settings to the factory default. A pop-up window will appear and ask you to confirm and enter your log in details. Enter your username and password and click "Ok". See below for more information.

V-5-6-2 Upgrade Firmware

Use this section to upgrade the firmware of the unit.



Do not switch off or disconnect the device during a firmware upgrade, as this could damage the device.

Browse	Open a new window to locate and select the firmware file in your computer.
---------------	--

After firmware upgrade, the system will restart.

V-5-6-3 Reboot

In the event that the router malfunctions or is not responding, then it is recommended that you restart the device.



Rebooting the unit will not affect the current configuration / settings of the device.

Apply	Click "Apply" to reboot the device. A status bar will indicate the progress of the reboot and you will see a confirmation screen when the reboot is complete.
--------------	---

V-5-6-4 System Log

Export the system log to a separate file in this section.

Export system log	Click to open a new window and select a location to save the log file.
--------------------------	--




VI Appendix

VI-1 Connecting to a Wi-Fi network

For help connecting to your device's **renkforceAP_2.4G_**** SSID for initial setup, or to connect to your device's new Wi-Fi network (SSID) after setup is complete, follow the guide below:

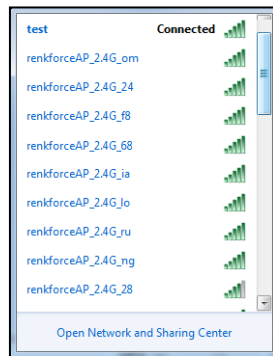


Below is an example of how to connect using Windows 7 – the process may vary slightly for other versions of Windows.

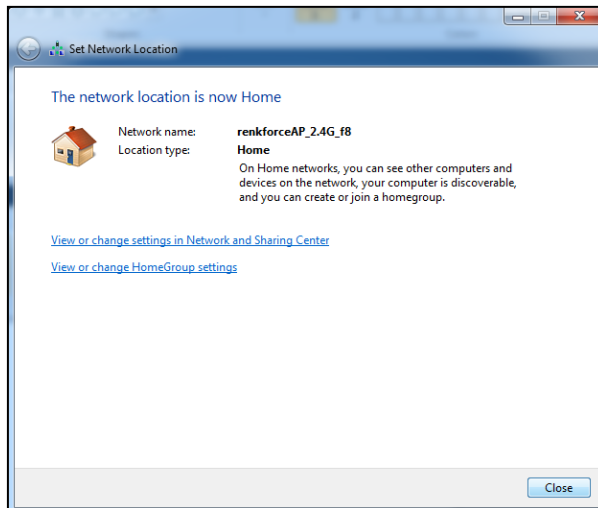
1. Click the network icon (, , or ) in the system tray and select **"Connect to a network"**.



2. Search for the SSID of the unit and then click **"Connect"**. If you set a password for your network, you will then be prompted to enter it.



3. After correctly entering your password, you will be successfully connected to the GRP-438N's wireless network.



VI-2 Troubleshooting

If you are experiencing problems with your unit, please refer to this troubleshooting guide before contacting your dealer of purchase for help.

Scenario	Solution
----------	----------

<p>I can't log onto the browser-based configuration interface.</p>	<ul style="list-style-type: none"> a. Please check that the unit is correctly inserted into a power socket and check the LEDs on the front panel. If the unit is initializing after being switched off or restarted, wait for a 2 minutes and try again. b. Make sure you are using the full, correct URL: http://renkforce.setup c. If you are using a MAC or IP address filter, try to connect the unit using a different computer. d. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can obtain an IP address. e. Ensure that all other Wi-Fi/Ethernet adapters are disabled or disconnected. f. Password is case-sensitive. Make sure the "Caps Lock" light is not illuminated. g. b. If you do not know your password, restore the device to factory settings.
<p>I can't establish a connection to my unit.</p>	<ul style="list-style-type: none"> a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client. The password is case-sensitive. Make sure the "Caps Lock" light is not illuminated. b. Try moving closer to the unit. c. Switch off the unit and switch it back on after 10 seconds. h. Please check that the unit is correctly inserted into a power socket and check the LEDs on the front panel.
<p>File downloads are very slow or frequently interrupted.</p>	<ul style="list-style-type: none"> a. Reset the unit. b. Try again later. Your local network may be experiencing technical difficulties or very high usage. c. Change channel number.
<p>The unit is extremely hot.</p>	<ul style="list-style-type: none"> a. It is normal for the unit to heat up during frequent use. If you can safely place your hand on the unit, the temperature is at a normal level. b. If you smell burning or see smoke coming from the unit, disconnect it immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.
<p>My network device can't access the Internet.</p>	<ul style="list-style-type: none"> a. Ensure that your broadband router is fully functional. b. Power off both your network device and the access point and switch back on again. c. Ensure that the unit is powered on (check the PWR LED). d. On the browser based configuration interface home page, check "Status" under "Wireless Configuration". It should be "Connected" – if it is "Disconnected" then this means the unit is not connected to your router/access point.
<p>Can I use the same SSID as my current gateway router for my Wi-Fi access point?</p>	<p>Yes, but it is not recommended as it will be difficult to distinguish between two SSIDs with the same name.</p>
<p>A firmware upgrade failed and the GRP-438N isn't working.</p>	<p>Firmware upgrade failures can happen occasionally due to power cuts or unstable connections. In this scenario, you need to first connect a computer to your GRP-438N's LAN port using an Ethernet cable. Then you need to modify your computer's IP address to 192.168.2.x where x</p>

is any value between **3** and **254**.

From there, you need to go to 192.168.2.1 in a web browser, and you will see the page below:

Firmware Recovery Mode

Please select the correct firmware file than click Upload once and wait for the next screen to display that the upgrade is in progress.

A screenshot of a web interface for firmware recovery. It features a horizontal file input field on the left, followed by a 'Browse...' button and an 'Upload' button on the right.

Click "Browse" to locate the firmware file on your computer and then click "Upload" to upload the new firmware. It may take several minutes to complete, please wait and follow the instructions on screen.

COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such as PDAs or lap pads is not authorized. This transmitter is restricted for use with the specific antenna tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency Range (MHz)	Max. Transmit Power (dBm) EIRP
2400~2483.5	19.74

A simplified DoC shall be provided as follows: Article 10(9)

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type **300N Wi-Fi Access Point** is in compliance with Directive 2014/53/EU

The full text of the EU declaration of conformity is available at the following internet address: <http://www.edimax.com/edimax/global/>

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

- English:** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/35/EU.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU.
- Polski:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU.
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/35/EU.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/35/EU).
- Türkçe:** Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/35/EU.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU.
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 2014/53/EU, 2014/35/EU.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/35/EU.
- suomen kieli:** Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR DE GR HU
IE IT LV LT LU MT NL PL PT SK SI ES SE
GB IS LI NO CH BG RO RU TR UA



EU Declaration of Conformity

Conrad Electronic SE, Klaus-Conrad-Straße 1, D-92240 Hirschau hereby declares that this product conforms to the 2014/53/EU directive.

Click on the following link to read the full text of the EU declaration of conformity:

- www.conrad.com/downloads

Enter the product item number in the search box. You can then download the EU declaration of conformity in the available languages.

Disposal



This symbol must appear on any electrical and electronic equipment placed on the EU market. This symbol indicates that this device should not be disposed of as unsorted municipal waste at the end of its service life.

Owners of WEEE (Waste from Electrical and Electronic Equipment) shall dispose of it separately from unsorted municipal waste. Spent batteries and accumulators, which are not enclosed by the WEEE, as well as lamps that can be removed from the WEEE in a non-destructive manner, must be removed by end users from the WEEE in a non-destructive manner before it is handed over to a collection point.

Distributors of electrical and electronic equipment are legally obliged to provide free take-back of waste. Conrad provides the following return options free of charge (more details on our website):

- in our Conrad offices
- at the Conrad collection points
- at the collection points of public waste management authorities or the collection points set up by manufacturers or distributors within the meaning of the ElektroG

End users are responsible for deleting personal data from the WEEE to be disposed of.

It should be noted that different obligations about the return or recycling of WEEE may apply in countries outside of Germany.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent

license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

11. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GRP-438N
V2023-03-15