

IWR-2458-AC-S-I

Configuration Manual



Beijing Nodes Network Limited

2025

Contents

1. Introduction	2
Overview	2
Power Supply	3
2. First-time Configuration	4
3. Operation Mode	5
3.1 Client Mode	6
Wireless-Radio setup	6
WLAN Security Settings	8
Network Setup	11
Communication Log Setting	14
Connection Info	15
3.2 AP Mode	16
WLAN Setup	16
Network Setup	18
Communication Log Setting	19
Association List	20
4. Maintenance	21
Log Download	21
Change Password	21
Configuration Import and Export	21
Firmware Update	23
Load Factory Default	24

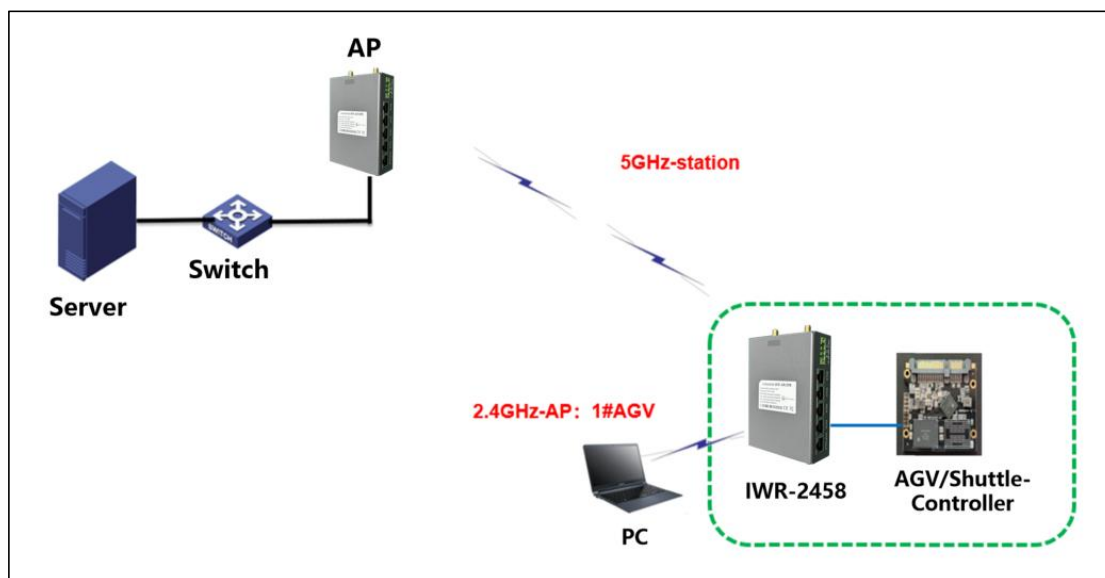
1. Introduction

IWR-2458-AC-S-I is an industrial dual-band equipment, which provides users with an unparalleled WiFi experience and highly reliable wireless connection by adding a number of powerful functions to meet the challenges in the WiFi deployment of the industrial field.

It can be operated on the 2.4 and 5 GHz simultaneously, and supports profinet & modbus protocols. It is built-in advanced interference suppression functional components which can significantly reduce wireless interference in noisy industrial applications.

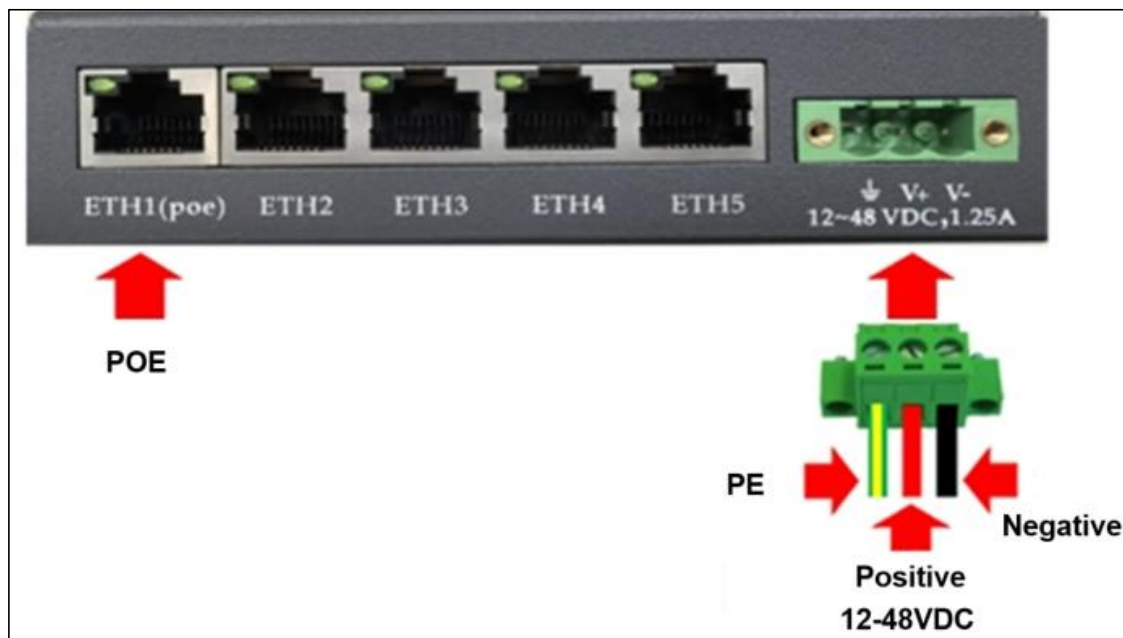
Overview

The IWR-2458-AC-S-I can be used as a dual-band wireless AP to provide WiFi coverage, It can also be used as a wireless client, installed on mobile devices such as AGV/RGV. You can change the work mode to adapt your applications, such as AP/Station/Repeater.



Power Supply

The IWR-2458-AC-S-I supports 12-48V DC power supply,the schematic diagram is as follows:



2. First-time Configuration

Before configuration the CPE-2458, you will need access to a PC equipped with an Ethernet port. The CPE-2458 has a default IP address that must be used when connecting to the device for the first time.

Step 1: Connect a power source.

The CPE-2458 can be powered by a DC(12-48v) power input.

Step 2: Connect the CPE-2458 to PC.

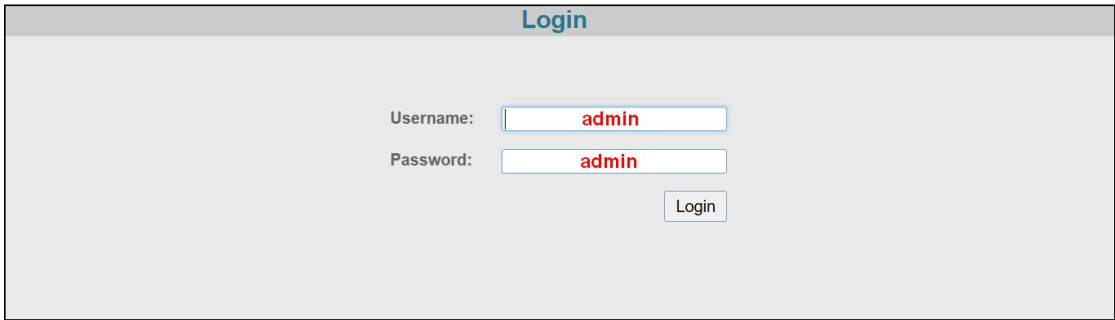
You can use a straight-through cable to connect the CPE-2458 to PC. The LED indicator on the CPE-2458's LAN port will light up when a connection is established.

Step 3: Set up the computer's IP address.

Choose an IP address on the same subnet as the CPE-2458. Since the CPE-2458's default IP address is 192.168.1.222, and the subnet mask is 255.255.255.0, you should set the IP address of the computer to 192.168.1.x.

Step 4: Use the web-based manager to configure the CPE-2458

Open your computer's web browser and type `http://192.168.1.222` in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the Username and Password as shown in the following figure. For first-time configuration, enter the default username and password and then click on the Login button.



Username:

Password:

Login

3. Operation Mode

The CPE-2458 supports four operation modes—AP, Station, Repeater, and Bridge—each of which plays a distinct role in a wireless network.

Enable Radio

Setting	Description	Factory Default
Enable Radio	Use this function to turn the RF (Radio Frequency) module on or off.manually.	Enable

Operation mode

Setting	Description	Factory Default
AP	CPE-2458 plays the role of wireless access point	2.4GHz-AP 5GHz-Station
Station	CPE-2458 plays the role of wireless client	
Repeater	CPE-245 can not only provide a backhaul link as a client but also offer signal coverage as an AP	
Bridge	CPE-245 plays the role of Point To Point link	

3.1 Client Mode

Wireless-Radio setup

The **Wireless-Radio** panel is used to edit the SSIDs and set the RF type for the device. You can choose the Radio0 or Radio1 to configure the CPE-2458 to operate either on the 2.4 GHz or 5 GHz frequency band. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Set the SSID of CPE-2458 to match with the SSID of the AP that you want it to connect to, so that the CPE-2458 will associate with the network defined by the SSID.

Click in sequence, "Configuration→Wireless→Radio1(5G)→General" to enter the following configuration interface:

The screenshot displays the 'Radio1(5G) Setting' configuration page. On the left sidebar, the 'Configuration' menu is expanded, showing 'Wireless' and 'Radio1(5G)' selected, with 'General' as the active sub-tab. The main content area has three tabs: 'General', 'Backhaul', and 'Advanced'. Under the 'General' tab, the following settings are visible: 'Enable Radio' is checked; 'Radio Mode' is set to 'Station'; 'Country/Region Code' is set to 'HONG KONG (CHINA)'; and 'Transmit Power' is set to '25'. A 'Submit' button is located at the bottom left of the configuration area. A small note below the power setting states: 'The effective Tx Power may be different, depends on the selected Channel.'

- Enable Radio: The RF (Radio Frequency) module can be manually turned on or off. When you check it, the RF turns on.
- Radio Mode: Station
- Transmit Power: Click on the options bar. Scroll down to the bottom and select the maximum value
- Click Submit

Click on "Backhaul" to enter the following basic configuration interface:

- Remote SSID: Fill in the SSID (you can scan and select)
- Authentication Mode: Select the corresponding mode
- Cipher Mode: Select the corresponding mode
- Pass Phrase: Fill in the connection password
- Enable Roaming: check
- Roaming Threshold: 20
- Roaming Sensitivity: Medium
- Allow DFS Channels: Check . (To ensure that the device supports 5GHz full frequency band)
- Scan Channel List: No need to check
- Click Submit

WLAN Security Settings

The CPE-2458 provides four standardized wireless security modes: Open, Shared (Shared Key), WPA (Wi-Fi Protected Access), and WPA2. Several security modes are available in the CPE-2458 by selecting Security mode and WPA type:

The screenshot shows the 'Security Setting' interface. On the left, there are labels for 'Authentication Mode:', 'Cipher Mode:', 'EAP Method:', 'Username:', and 'Password:'. To the right, a dropdown menu is open, displaying a list of options: 'Open', 'Shared', 'WPA2 Enterprise' (which is highlighted in blue), 'WPA2 Personal', 'WPA Enterprise', and 'WPA Personal'. A 'Show' checkbox is visible to the right of the dropdown list.

WPA/WPA2 Personal :

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. A Passphrase is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.

The screenshot shows the 'Security Setting' interface with 'WPA2 Personal' selected in the 'Authentication Mode' dropdown. The 'Cipher Mode' dropdown is set to 'AES'. The 'Pass Phrase' field is empty, and a 'Show' checkbox is to its right. Below the 'Pass Phrase' field, there is a note: 'Length:8-63(ASCII Characters); Length:64(HEX Characters)'. At the top of the interface, there is a label 'IP Only: XXX.XXX.XXX.XXX'.

WPA/WPA2 Enterprise :

When used as a client, the CPE-2458 can support three EAP methods (or EAP protocols): EAP-TLS, EAP-TTLS, and EAP-PEAP, corresponding to WPA/WPA-Enterprise settings on the AP side.

Security Setting

Authentication Mode: WPA2 Enterprise

Cipher Mode: AES

EAP Method: PEAP-MSCHAPV2

Username: PEAP-MSCHAPV2

Password: TTLS-PAP

Bandwidth Setting

TTLS-CHAP

TLS

Show

EAP Protocol

Setting	Description	Factory Default
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	PEAP
TTLS	Specifies Tunneled Transport Layer Security	
TLS	Specifies Transport Layer Security protocol	

Before choosing the EAP protocol for your WPA/WPA2-Enterprise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections.

➤ PEAP&TTLS:

Security Setting

Authentication Mode: WPA2 Enterprise

Cipher Mode: AES

EAP Method: PEAP-MSCHAPV2

Username:

Length:0-128(Ascii Characters)

Password:

Length:1-128(Ascii Characters)

Show

TTLS and PEAP work in a similar way. First, they establish a TLS tunnel (EAP-TLS for example), and validate whether the network is trustworthy with digital certificates on the authentication server. This step establishes a tunnel that protects the next step (or “inner” authentication), and consequently is

sometimes referred to as “outer” authentication. The TLS tunnel is then used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

➤ TLS:

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange.

EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

Security Setting

Authentication Mode: WPA2 Enterprise

Cipher Mode: AES

EAP Method: TLS

Identity:

Length:1-128(Ascii Characters)

Private key passwd: ☐ Show

Length:1-128(Ascii Characters)

CA Certificate:

选择文件

未选择任何文件

Upload

Client Certificate:

选择文件

未选择任何文件

Upload

Certificate Status: Not installed

Network Setup

The network mode includes:

- ① Switch Mode
- ② Gateway Mode

Switch Mode:

Adapt to the Nodes AP and other fat AP , in which the CPE module and AGV controller use the same network segment IP.(Each AGV will occupy multiple IP addresses, making it more suitable for self-organizing LAN environments)

Click on "Configuration→Network→General":

- Network Setting:Switch Mode
- Static IP address modification:
 - ✧ Fill in the IP address, subnet mask, and gateway
 - ✧ Choose whether to modify the DNS server based on the project
 - ✧ Click Summit
- Dynamic IP address modification:
 - ✧ Internet connection type:DHCP
 - ✧ Click Submit

Gateway Mode:

If you need to access to fit AP, and the number of IP addresses is limited, CPE can use gateway mode. Each AGV/RGV only occupies one IP address, and the controller's configuration is simple and unified.

Due to the better compatibility and adaptability of the gateway mode, we strongly recommend to use gateway mode!

Click in sequence, "Configuration→Network→General" to enter the following configuration interface:

General Network Setting

Configuration: System, Network, VLAN, Firewall, DHCP, Port Forward, Safe Mode, Device Status Report

Network Setting

Network Setting: Gateway Mode

Enable IPv6: ☐

Secondary IPs: ☒

WAN/LAN Interface Assignment

	Interface(s)	Detail
WAN	Station1	
LAN	eth0 AP0_0(Smartwifi_2.4G_0)	

Enable NAT Mode: ☒

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server IP Address:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 98 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

- Network Setting: Gateway Mode
- WAN/LAN Interface Assignment :
 - ✧ Station interface as WAN port;
 - ✧ eth0 and others as LAN port
- WLAN Setting (IPv4):
 - ✧ Internet Connection Type : Static/DHCP
 - ✧ Fill in the planned IP address, subnet mask, and gateway
 - ✧ Choose whether to modify the DNS server based on the project

- ✧ Click Submit
- LAN Setting(IPv4):
 - ✧ Click to submit the IP address and subnet mask planned for the device
 - ✧ LAN-IPv4 serves as the management IP for the LAN port of the device and the gateway for the backend controller.
- Port Forward :

Click on "Port Forwarding" :

Status		Port Forward						
Configuration		General	VLAN	Firewall	DHCP	Port Forward	Safe Mode	Device Status Report
System								
Network								
General								
VLAN								
Firewall								
DHCP								
Port Forward								
Safe Mode								
Device Status Report								
Wireless								
Remote Mgmt								
Serial Port								
Administration								
Tools								
About								

ID	Local IP	Local Port	Type	Global Port	Enable
1	192 . 168 . 98 . 50	3389	TCP & UDP	3389	☒
2	0.0.0.0	1	TCP & UDP	1	☐
3	0.0.0.0	1	TCP & UDP	1	☐
4	0.0.0.0	1	TCP & UDP	1	☐
5	0.0.0.0	1	TCP & UDP	1	☐
6	0.0.0.0	1	TCP & UDP	1	☐
7	0.0.0.0	1	TCP & UDP	1	☐
8	0.0.0.0	1	TCP & UDP	1	☐
9	0.0.0.0	1	TCP & UDP	1	☐
10	0.0.0.0	1	TCP & UDP	1	☐
11	0.0.0.0	1	TCP & UDP	1	☐
12	0.0.0.0	1	TCP & UDP	1	☐
13	0.0.0.0	1	TCP & UDP	1	☐
14	0.0.0.0	1	TCP & UDP	1	☐
15	0.0.0.0	1	TCP & UDP	1	☐
16	0.0.0.0	1	TCP & UDP	1	☐
17	0.0.0.0	1	TCP & UDP	1	☐
18	0.0.0.0	1	TCP & UDP	1	☐

- Check to enable port
- Local IP: Fill in the IP address of the AGV/RGV controller
- Local Port and Global Port: The communication port used by controller
- Type : TCP or UDP, TCP&UDP
- Click Submit

Communication Log Setting

Click in sequence,"Configuration→System→Logging Setting" to enter the following interface:

The screenshot shows the 'Basic System Setting' interface with the 'Logging Setting' tab selected. The 'Communication Log Setting' section is highlighted with a red box. The settings are as follows:

- Remote Syslog: ☒
- Server IP Address: 0 . 0 . 0 . 0
- System Log Severity: Informational
- Debug Log: Enable
- WiFi Log Severity: Debug
- Historical Statistics: ☒
- Sampling Frequency: 30 (s)
- Communication Log Setting**
 - Log Status: 5GHz Radio
 - Log Work Mode: Station mode
 - Communication IP: 0 . 0 . 0 . 0
- Record Interval: 2 (1-60s)
- Threshold of channel busy: 70 (1-100)
- Abnormal AP Detect: ☐

A 'Submit' button is located at the bottom left of the form.

- Log Status:5GHz RF/2.4GHz RF **(Choose the band of station mode)**
- Log Work Mode:Station mode
- Communication IP:Server of AGV or gateway**(Server is better)**
- Record Interval : 3
- Click Submit
- Save Application

Click on "Save&Apply" in the upper right corner of the page, it will reboot,and the configurations take effect.

This screenshot shows the same 'Basic System Setting' interface, but with the 'Save & Apply' button highlighted in the top right corner. The 'Communication Log Setting' section is still highlighted with a red box. The settings are identical to the previous screenshot.

Attention:Please use the new IP address to login again.

Connection Info

Click in sequence, "Status→Radio1(5G)→Connection Information" to enter the following interface:

Status

Overview

Radio0(2.4G)

Radio1(5G)

Status

Connection Info

Ethernet

Serial Port

Logs

Configuration

Administration

Tools

About

Connection Info

STA Info

MAC Address	Auth Mode	Unicast Cipher	Multicast Cipher	State
a0:62:60:73:2f:79	wpa2-psk	aes	aes	Enabled

AP Info

MAC Address	SSID	SNR (dB)	RSSI (dBm)	Channel	Max DataRate (Mbps)	Throughput	Data Rate	Connected Status
a0:62:60:82:6e:a4	TEST	39	-63	5785MHz(Channel 157)	144	Tx: 4.3Kbps Rx: 7.0Kbps	Tx: 144.0Mbps Rx: 144.0Mbps	Connected

- Connected Status:Connected
- SNR(dB):39
- RSSI(dBm):-63

3.2 AP Mode

WLAN Setup

Click in sequence, "Configuration→Wireless→Radio1(5G)→Basic Information" to enter the following configuration interface:

- Radio Mode:AP
- Wireless Mode : 802.11ac HT20
- Channel:Select based on the project site network planning (Recommend using high-frequency channels 149~165)
- Transmit Power:Click on the options bar, scroll down to the bottom, and select the one with the highest value
- Click Submit

Click in sequence, "Configuration→Wireless→Radio1(5G)→WLAN" to enter the following configuration interface:

Enable WLAN	SSID	Maximum Clients	Isolation	Auth Mode	Cipher Mode	PassPhrase	WLAN Uplink/Downlink Control	Station Uplink/Downlink Control	Detail
☒ 0	TEST ☐ Hide SSID	256	☐	WPA2 Personal	AES	12345678 ☒ Show	0	0	More...
☐ 1	Smartwifi_5G_1 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 2	Smartwifi_5G_2 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 3	Smartwifi_5G_3 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 4	Smartwifi_5G_4 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 5	Smartwifi_5G_5 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 6	Smartwifi_5G_6 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 7	Smartwifi_5G_7 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 8	Smartwifi_5G_8 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...
☐ 9	Smartwifi_5G_9 ☐ Hide SSID	256	☒	Open	Disabled		0	0	More...

- Enable WLAN: Check to activate the corresponding SSID, multiple SSIDs can be checked
- SSID: Fill in the SSID name according to the project
- Isolation: Uncheck
- Auth Mode: Select what you need
- Cipher Mode: Select the corresponding mode
- PassPhrase : Fill in the password
- Click Submit

Network Setup

Click in sequence, "Configuration→Network→General" to enter the following configuration interface:

The screenshot displays the 'General Network Setting' configuration page. On the left sidebar, the 'Configuration' menu is expanded, showing 'System', 'Network', 'VLAN', 'Firewall', 'DHCP', 'Port Forward', 'Safe Mode', 'Device Status Report', 'Wireless', 'Remote Mgmt', and 'Serial Port'. The 'Network' menu is further expanded to show 'General'. The main content area has tabs for 'General', 'VLAN', 'Firewall', 'DHCP', 'Port Forward', 'Safe Mode', and 'Device Status Report'. The 'General' tab is selected, showing the 'Network Setting' section with a dropdown menu set to 'Switch Mode'. Below this, the 'WAN/LAN Interface Assignment' section shows 'Enable NAT Mode' set to 'NA'. The 'WAN Setting(IPv4)' section is highlighted with a red box, showing 'Internet Connection Type' set to 'Static', 'IPv4 Address' as 192.168.1.222, 'IPv4 Subnet Mask' as 255.255.255.0, 'IPv4 Default Gateway' as 192.168.1.1, and 'IPv4 DNS Server IP' as an empty field.

- Network Mode: Switch Mode
- Static IP address modification:
 - ✧ Fill in the IP address, subnet mask, and gateway
 - ✧ Choose whether to modify the DNS server based on the project
 - ✧ Click Summit
- Dynamic IP address modification:
 - ✧ Internet connection type: DHCP
 - ✧ Click Submit

Communication Log Setting

Click in sequence, "Configuration→System→Logging Setting" to enter the following configuration interface:

- Log States: 5GHz RF/2.4GHz RF **(Choose the band of AP mode)**
- Log Work Mode: AP mode
- Record Interval: 5
- Click Submit
- Save Application

Click on "Save&Apply" in the upper right corner of the page, it will reboot, and the configurations take effect.

Attention: Please use the new IP address to login again.

Association List

Click in sequence, "Status→Radio1(5G)→Association List" to enter the following interface:

Status	Association List									
Overview	WLAN Station List Rogue Station List									
Radio0(2.4G)										
Radio1(5G)										
Status										
Association List										
Ethernet										
Serial Port										
Logs										
Configuration										
Administration										
Tools										
About										

WLAN ID	Status	SSID	MAC Address	Auth Mode	Cipher	#Clients	Throughput	Total Traffic
0	On	TEST	a0:62:60:73:2f:79	WPA2 Personal	aes	1	TX: 1.1Kbps RX: 0.3Kbps	TX: 1.0MB RX: 249.6KB
Total						1	TX: 1.1Kbps RX: 0.3Kbps	TX: 1.0MB RX: 249.6KB

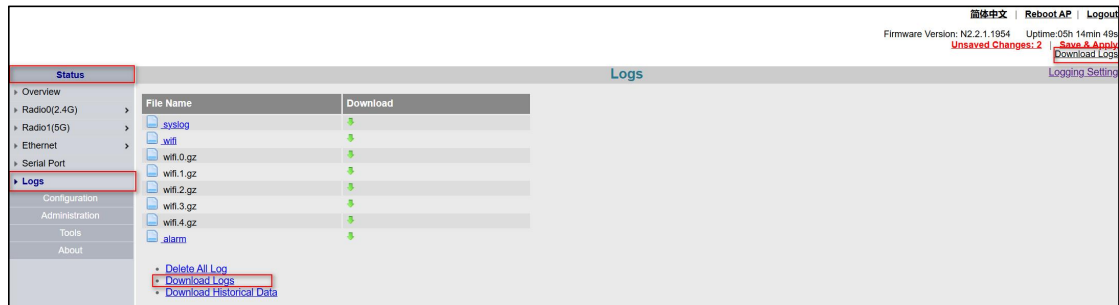
SNR Distribution									
STA ID	MAC Address	IP Address	Hostname	Online Time	SNR(dB)	Throughput	Traffic	Data Rate	
0-1	a0:62:60:82:6e:a4	192.168.1.100		1h 48m 21s	36	TX: 0.9Kbps RX: 0.3Kbps	TX: 723.0KB RX: 249.6KB	TX: 144.0Mbps RX: 144.0Mbps	 

- Total number of connections:1
- Access terminal MAC/IP/SNR/Data Rate

4. Maintenance

Log Download

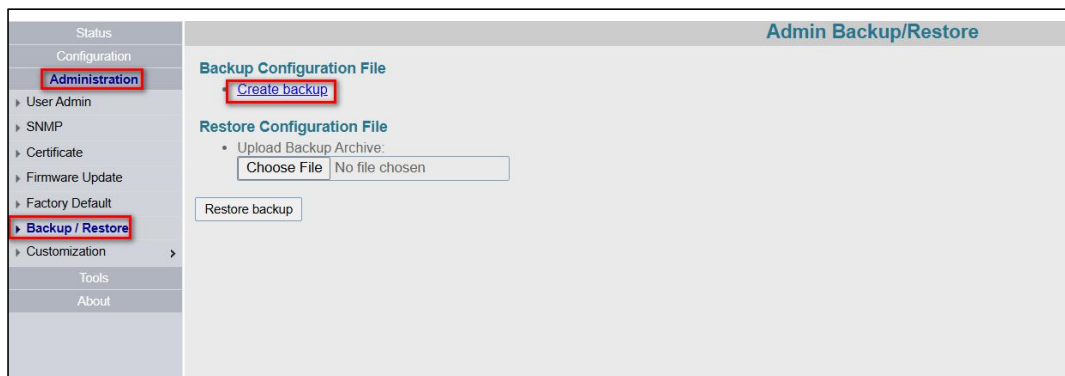
Click on "Download Logs" in the upper right corner of the device interface.



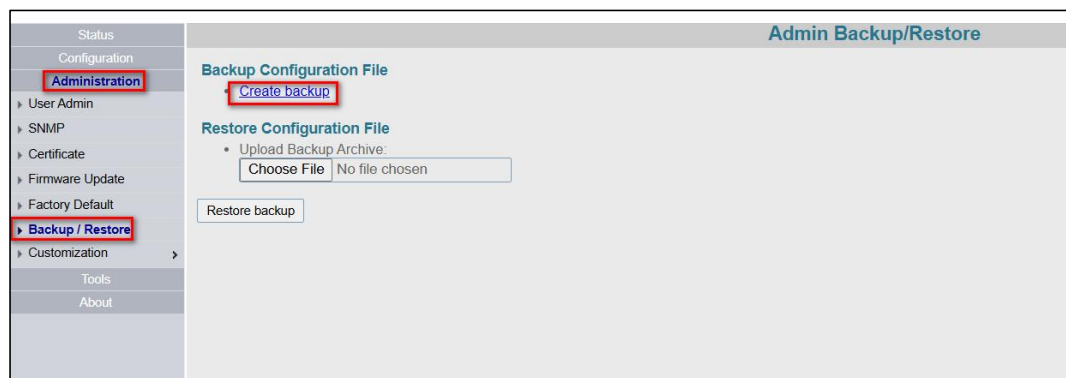
Change Password

Configuration Import and Export

- Backup configuration:
- click in sequence, "Administration→Backup/Restore→Create Backup"



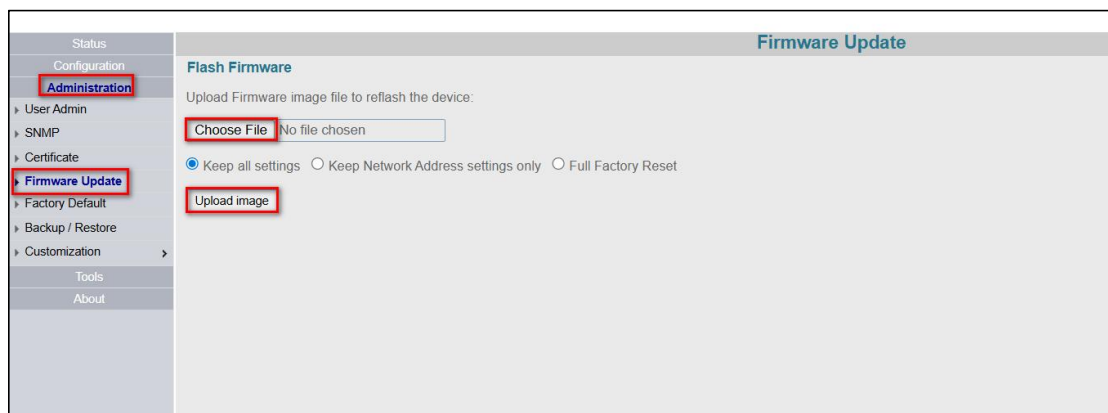
- Restore configuration: click in sequence, "Administration→Backup/Restore→Upload Backup Archive→Restore Configuration"



Attention: Please change the IP address for the device.

Firmware Update

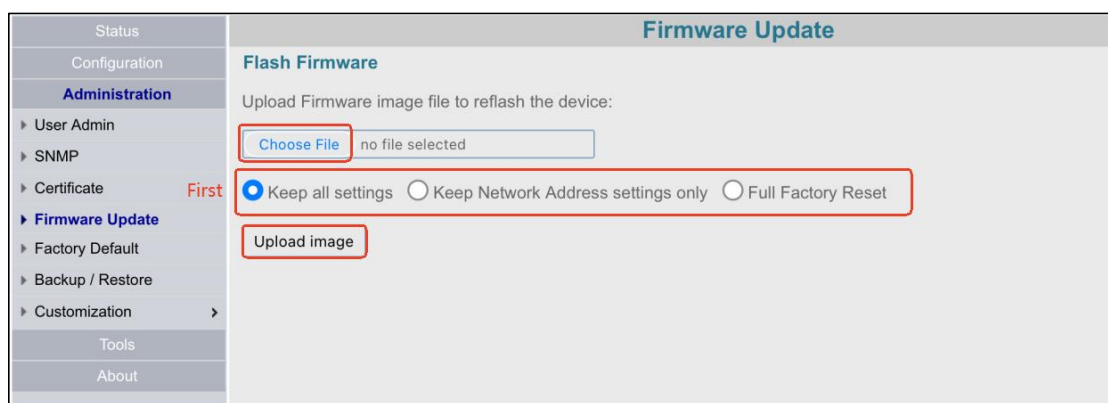
Click “Administration→ Firmware Upgrade”:



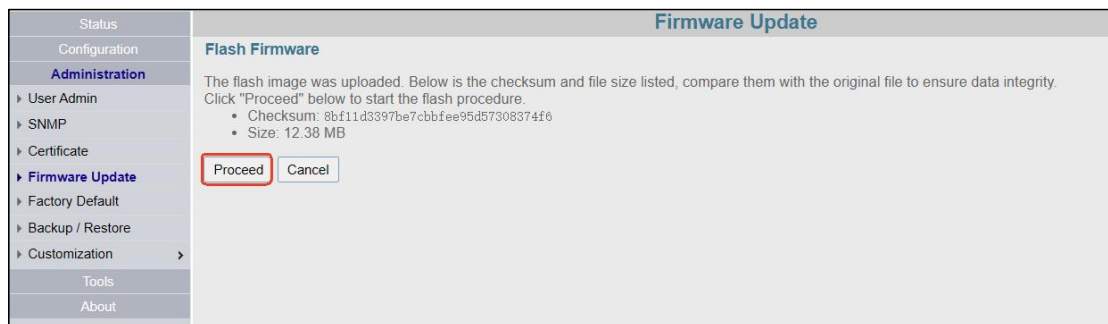
Before clicking “Choose File” to upload the firmware, choose one of the three configuration retention strategies based on your actual needs:

- Keep All Settings: The upgrade will keep all configurations;
- Keep Network Address settings Only: The upgrade will only keep the network-related configurations.
- Full Factory Reset: The upgrade will restore the device to its factory configuration simultaneously.

Example: Select “Keep All Settings”, choose the corresponding firmware file and click “Upload image”, as shown below:



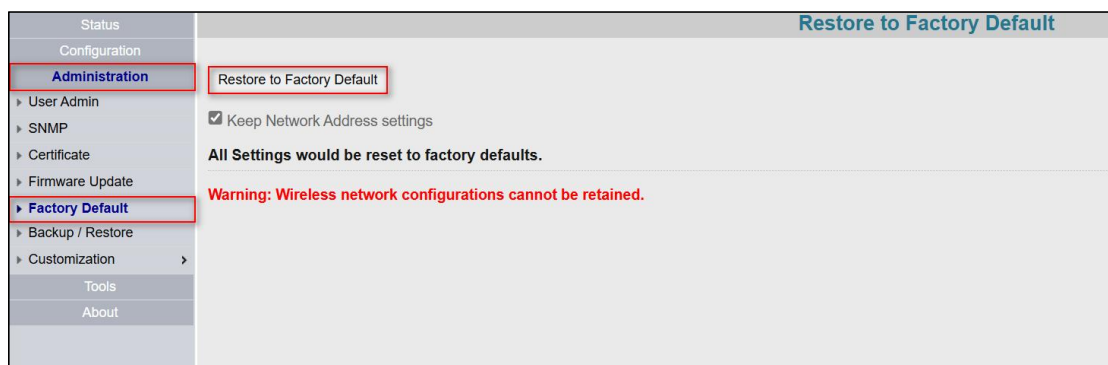
After the firmware file is successfully uploaded, click “Proceed” and wait for the AP upgrade to complete, as shown below:



Attention: Please do not power off the device under any circumstances during this process. Otherwise it will be sent to the factory for repair!

Load Factory Default

Click "Administration→Factory Default":



- 1) Restore to Factory Default.
- 2) Keep Network Address settings:
 - Check, the device will restore the factory settings but retain the network configurations;
 - Uncheck, the device will be fully restored to factory settings, the device's IP address is restored to the default 192.168.1.222.

FCC Warning

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.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure Statement

To maintain compliance with FCC'S RF Exposure guidelines, This equipment should be installed and operated with minimum 20cm between the radiator and your body. This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

EU Declaration of Conformity (DoC)

Company name	Beijing Nodes Network Technology Co., Ltd.
Address	Rm705, Shenzhou Building, No.31 Zhongguancun, South Street, Haidian District, Beijing, 100081, China
Name of Contact	Su Xie
Title	Manager
Phone number	13601232288
E-mail address	xiesu@nodes.com.cn

We declare that the DoC is issued under our sole responsibility and belongs to the following product:

Equipment manufacturer	Beijing Nodes Network Technology Co., Ltd.
Model Type	IWR-2458-AC-5P
Product description	AP/CPE
HW version	1.5
SW version	2.2.1.1956T17
Optional accessories or System components	/

The object of the declaration described above is in conformity with the relevant Union Harmonization Legislation:

RE Directive 2014/53/EU	

The Notified Body Name: **Compliance Testing, LLC**, has conducted the conformity assessment according to module B of Directive 2014/53 / EU (RED) and issues the EU type certificate [XXXXXXX].

The following standards and technical specifications have been applied for

RE Directive 2014/53/EU:

Article 3.1a: Safety and Health	EN IEC 62368-1:2024+A11:2024 EN 50665:2017
Article 3.1b: EMC	EN 301489-1 V2.2.3 (2019-11) EN 301489-17 V3.3.1 (2024-09) EN 55032 :2015+A11 :2020+A1 :2020 EN 55035 :2017+A11 :2020 EN IEC 61000-3-2:2019+A2:2024 EN 61000-3-3:2013+A2:2021+ AC:2022-01
Article 3.2: RF Spectrum Efficiency	EN 300328 V2.2.2 (2019-07) EN 301893 V2.2.1 (2024-11)
Article 3.3: Special requirements invoked	Not applicable

The following standards and technical specifications have been applied for the other European Legislation:

N/A	

Signed on behalf of: Beijing Nodes Network Technology Co., Ltd.

2/3/2026

Print name: Su Xie

Title: Manager

Signature: *Su Xie*