Wireless Bridge (Web)

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the company website Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

Trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL OUR COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Preface

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠**Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
⚠**Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
ℹ**Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction

You can manage and configure the wireless bridge (hereinafter referred to as the device) through the web browser, including network settings, wireless network settings, and system management.

Note

Functions vary with device models. Pictures used for illustration here are for example purposes. The actual interface prevails.

Chapter 2 Activation and Login

2.1 Activate the Device

For the security of your privacy and system data, you are required to set a password for your first use. After the password is set, you can log in to the web for further configuration.

Before You Start

Ensure that your PC and the device are on the same network segment.

Steps

1. Run the web browser.
2. Enter the IP address of the device in the address bar, and press **Enter**.

- AP default IP address: 192.168.1.35
- CPE default IP address: 192.168.1.36
- Default user name: admin

3. Set your password and confirm.

⚠**Caution**

- The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: uppercase letters, lowercase letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system. Changing the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Select the desired **Country/Region Code** and confirm.

Note

Only when **Country/Region Code** is set, can the device work normally.

2.2 Log in to the Device

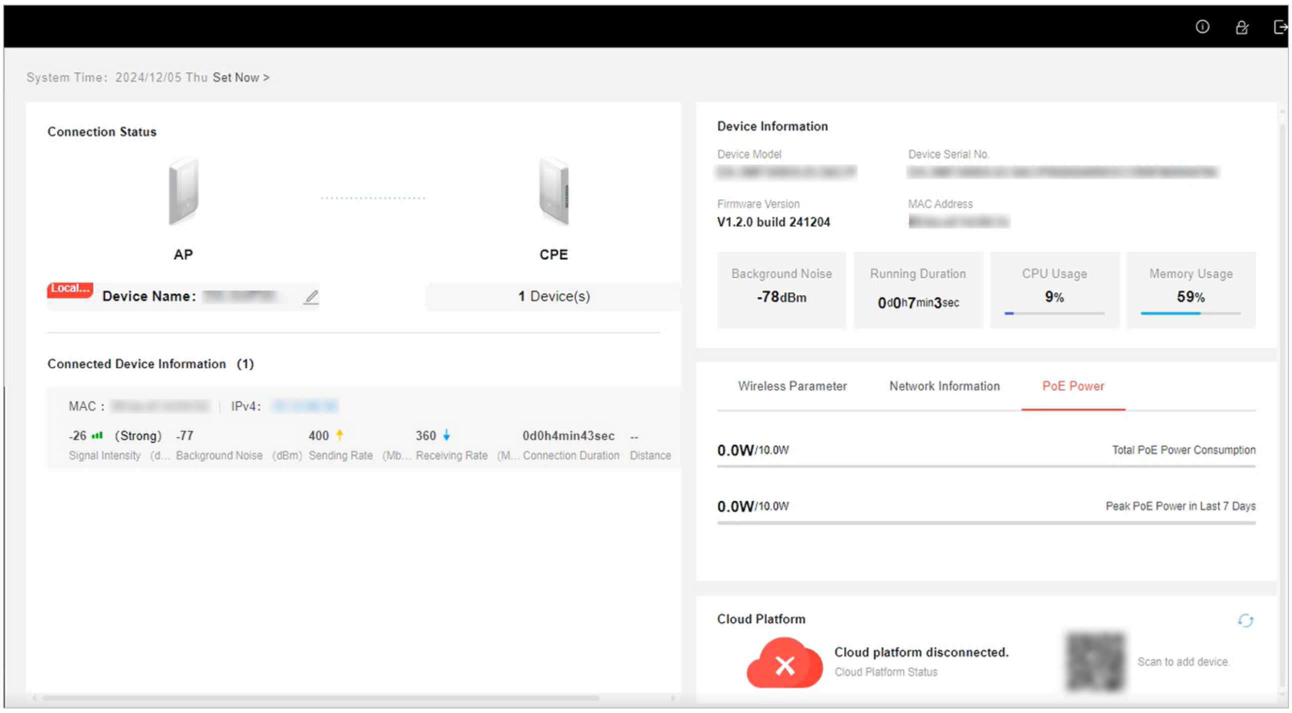
Log in to the device to check device information and configure related parameters.

Steps

1. Enter the IP address in the address bar of the web browser, and press **Enter**.
2. Enter the user name and password.
3. Click **Login**.

Chapter 3 Overview

You can view the basic information, connection status, network status, and wireless status for routine check or device maintenance.



System Time: 2024/12/05 Thu Set Now >

Connection Status

AP

CPE

Local... Device Name: [redacted]

1 Device(s)

Connected Device Information (1)

MAC : [redacted] | IPv4: [redacted]

-26 (Strong) Signal Intensity (d... | -77 Background Noise (dBm) | 400 Sending Rate (Mb... | 360 Receiving Rate (M... | 0d0h4min43sec Connection Duration | -- Distance

Device Information

Device Model: [redacted]

Device Serial No.: [redacted]

Firmware Version: V1.2.0 build 241204

MAC Address: [redacted]

Background Noise: -78dBm

Running Duration: 0d0h7min3sec

CPU Usage: 9%

Memory Usage: 59%

0.0W/10.0W Total PoE Power Consumption

0.0W/10.0W Peak PoE Power in Last 7 Days

Cloud Platform

Cloud platform disconnected.

Cloud Platform Status

Scan to add device.

Figure 3-1 Overview

Table 3-1 Overview Description

Information&Operation	Description
Device Information	Check device name, device model, serial No., program version, MAC address, CPU usage, memory usage, running time, and background noise condition of the device, etc.
Connection Status	Check the connection status of the device.
Connected Device Information	Check MAC/IP address, signal intensity, sending rate, receiving rate, connection duration of the connected device (e.g. the peer bridge device).
Wireless Parameter	Check working scene, SSID, wireless mode, channel, channel width, security mode of the device. The LAN parameters are configurable. See ***4.2 LAN Settings*** for details.
Network Information	Check IPv4, subnet mask, gateway, DNS, alternate DNS of the device.
PoE Power	Check total PoE power consumption and peak PoE power in the last

	7days. See ***Chapter 7 PoE Management*** for details.
Cloud Platform	Check clound platform connection status. This function varies with models. The actual interface prevails.
Quick Set Time	Click Set Now to set system time. See ***9.7 Set Time*** for details.
Quick Modify Device Name	Click ✎ to modify device name. Or go to **System** → **System Configuration** → **Basic Information**.
Check User Manul	Click ⓘ to check the Web User Munal.
Modify System Password	Click 🔏 to modify system password. See ***9.8 Change Password*** for details.
Log Out	Click ⇥ to log out.

Note

Information on this page varies with models. The actual interface prevails.

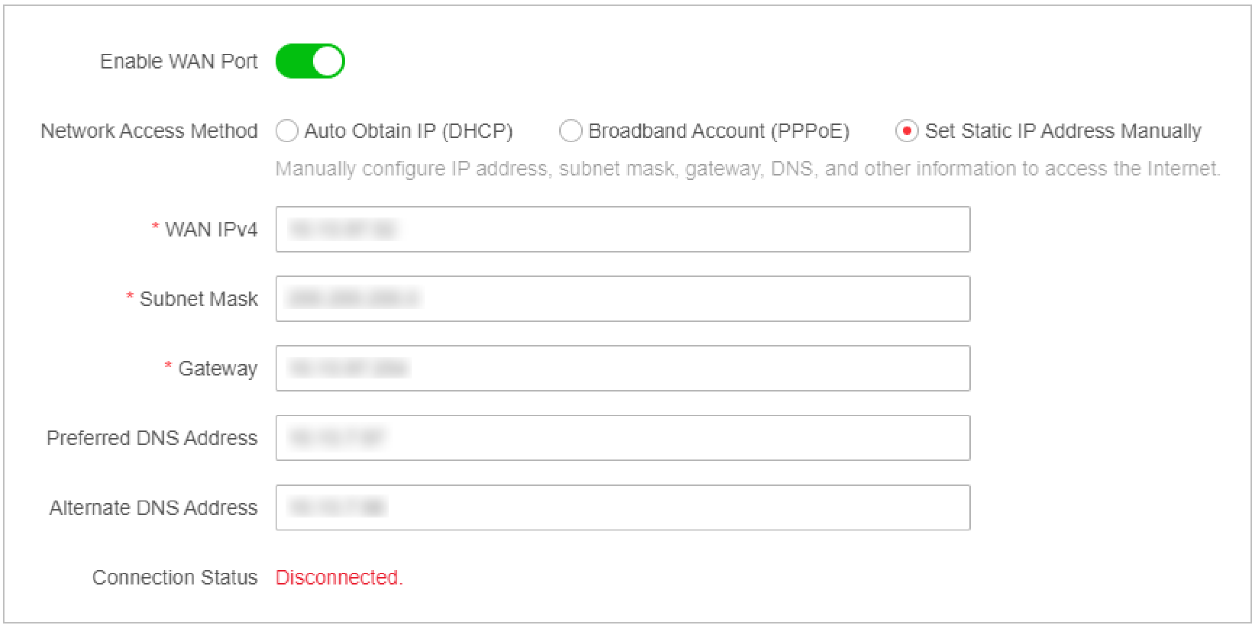
Chapter 4 Network Settings

4.1 WAN Settings

Go to **Network Settings** → **LAN Settings** to set relevant parameters, such as **Network Access Method** and **WAN IPv4**.

Note

The function varies with models, and it is only supported when some devices are set as **AP** site. The actual interface prevails.



Enable WAN Port: ● on

Network Access Method: ○ Auto Obtain IP (DHCP) ○ Broadband Account (PPPoE) ● Set Static IP Address Manually

Manually configure IP address, subnet mask, gateway, DNS, and other information to access the Internet.

* WAN IPv4: [redacted]

* Subnet Mask: [redacted]

* Gateway: [redacted]

Preferred DNS Address: [redacted]

Alternate DNS Address: [redacted]

Connection Status: Disconnected.

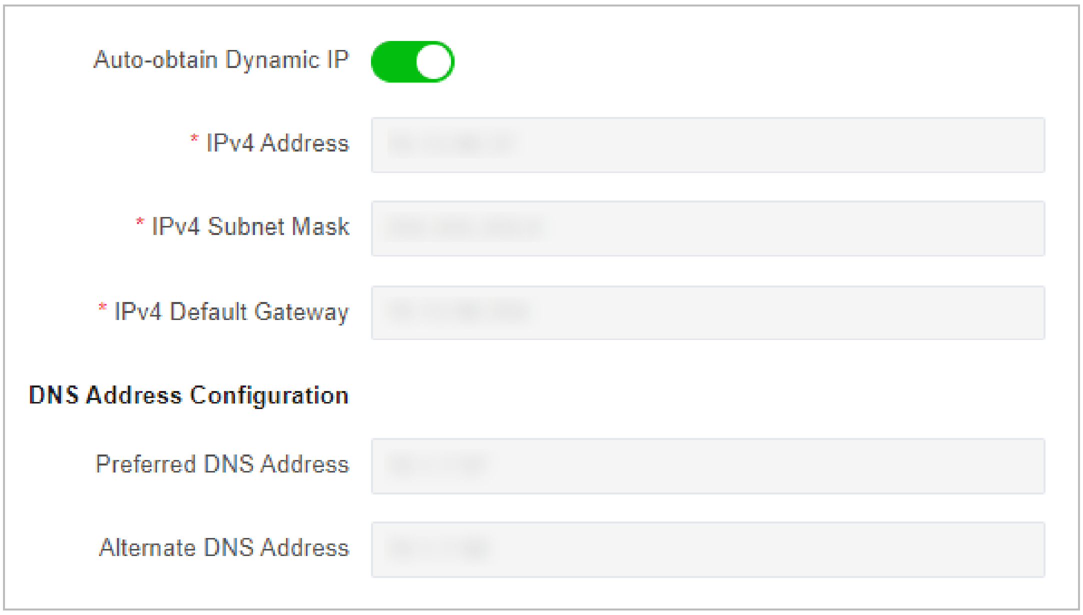
Figure 4-1 WAN Port Settings

Table 4-1 Parameter Description

Parameter	Description
DHCP	No additional configuration is required if you choose this mode.
PPPoE	Select this mode if your ISP (Internet Service Provider) has provided a broadband account and password.
Static IP	Select this mode if your ISP has provided an IP address and other information related.

4.2 LAN Settings

Go to **Network Settings** → **LAN Settings** to configure detailed network parameters.
If you enable **Auto-obtain Dynamic IP**, other parameters will be set automatically.



Auto-obtain Dynamic IP

* IPv4 Address

* IPv4 Subnet Mask

* IPv4 Default Gateway

DNS Address Configuration

Preferred DNS Address

Alternate DNS Address

Figure 4-2 LAN Settings

Note

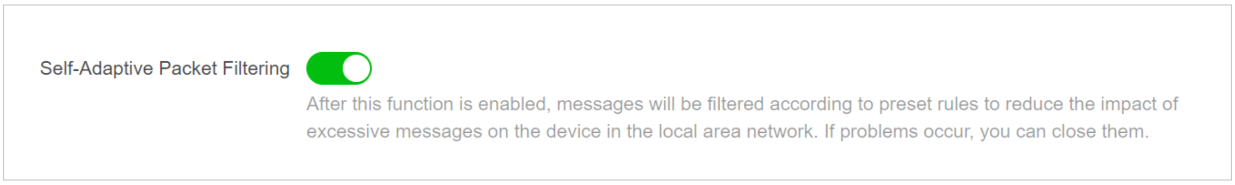
- The function varies with models. Devices with WAN port is supported to configure DHCP server. The actual interface prevails.
- After the IP address is reset, the web page redirects to the new login interface of the newly set IP address.
- To prevent IP address conflict, it is recommended to use SADP tool when you set the device IP address.

4.3 Data Forwarding Settings

In a complex LAN environment, to reduce the negative impact of certain multicast, broadcast, and unknown unicast packets on the device, you can filter the packets as required. Go to **Network Settings** → **Data Forwarding Settings** to enable/disable the packet filtering features of the device.

Note

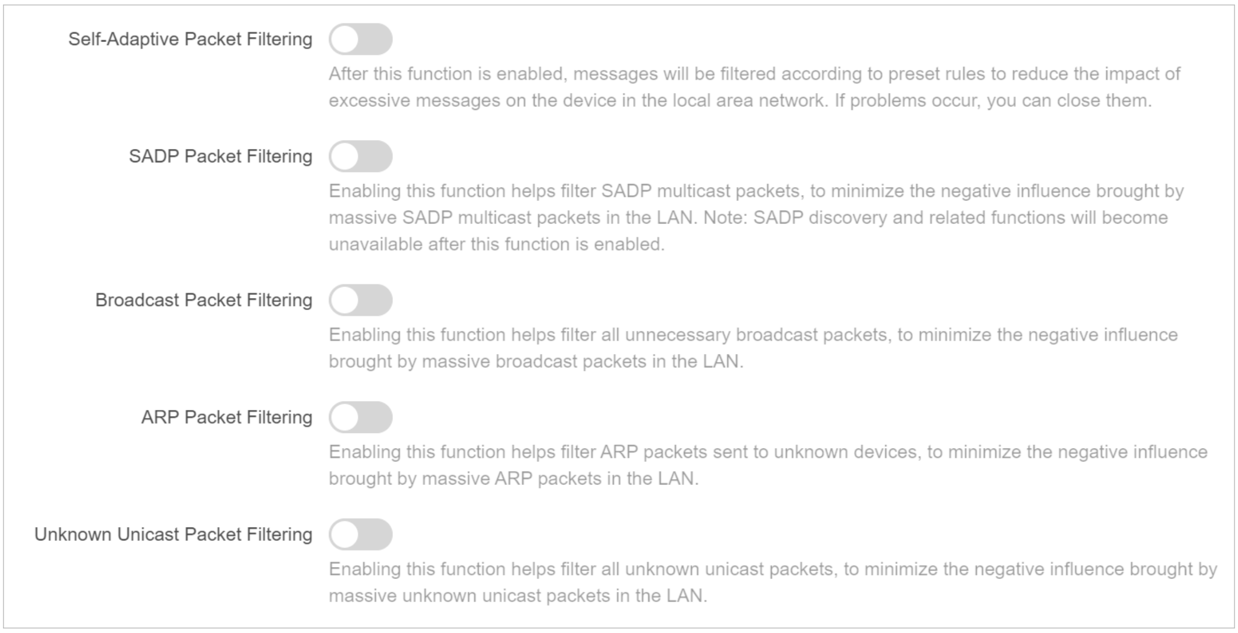
The function varies with models, and it is only supported when some devices are set as AP site. The actual interface prevails.



Self-Adaptive Packet Filtering

After this function is enabled, messages will be filtered according to preset rules to reduce the impact of excessive messages on the device in the local area network. If problems occur, you can close them.

Figure 4-3 Enable Self-Adaptive Packet Filtering



Self-Adaptive Packet Filtering

After this function is enabled, messages will be filtered according to preset rules to reduce the impact of excessive messages on the device in the local area network. If problems occur, you can close them.

SADP Packet Filtering

Enabling this function helps filter SADP multicast packets, to minimize the negative influence brought by massive SADP multicast packets in the LAN. Note: SADP discovery and related functions will become unavailable after this function is enabled.

Broadcast Packet Filtering

Enabling this function helps filter all unnecessary broadcast packets, to minimize the negative influence brought by massive broadcast packets in the LAN.

ARP Packet Filtering

Enabling this function helps filter ARP packets sent to unknown devices, to minimize the negative influence brought by massive ARP packets in the LAN.

Unknown Unicast Packet Filtering

Enabling this function helps filter all unknown unicast packets, to minimize the negative influence brought by massive unknown unicast packets in the LAN.

Figure 4-4 Disable Self-Adaptive Packet Filtering

Table 4-2 Parameter Description

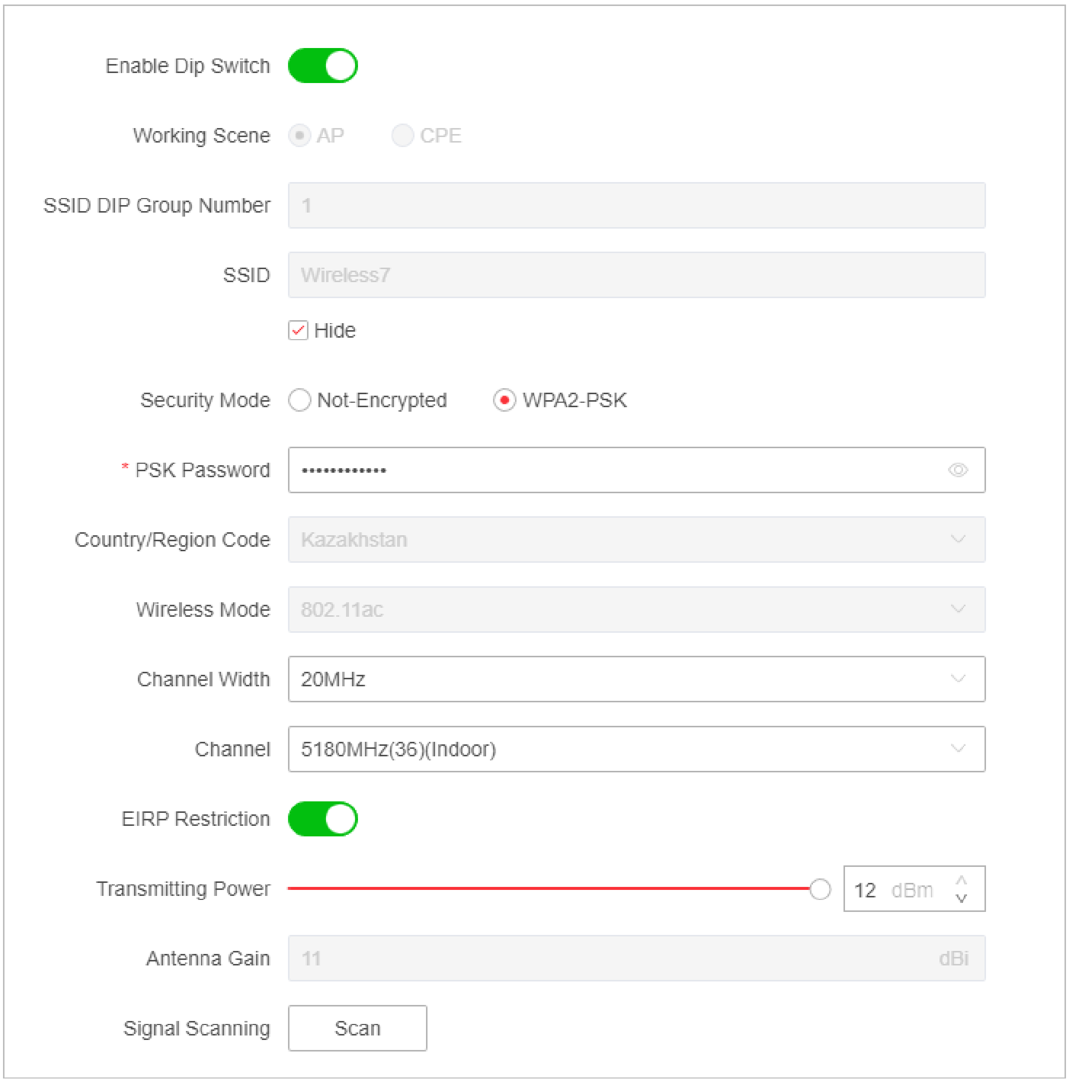
Parameter	Description
Self-Adaptive Packet Filtering	Enabled by default. Filter packets according to present rules, in order to reduce the impact of excessive message on the device in the LAN.
SADP Packet Filtering	Filter SADP multicast packets to minimize the negative influence brought by massive SADP multicast packets in the LAN. **Note** SADP discovery and related functions will become unavailable after this function is enabled.
Broadcast Packet Filtering	Filter all unnecessary broadcast packets to minimize the negative influence brought by massive broadcast packets in the LAN.
ARP Packet Filtering	Filter ARP packets sent to unknown devices, in order to minimize the negative influence brought by massive ARP packets in the LAN.
Unknown Unicast Packet Filtering	Filter all unknown unicast packets to minimize the negative influence brought by massive unknown unicast packets in the LAN.

Chapter 5 Wireless Settings

Click **Wireless Settings** to set basic and advanced parameters of wireless network.

5.1 Basic Wireless Settings

Go to **Wireless Settings** → **Basic Settings** to set wireless network basic parameters.



Enable Dip Switch	●
Working Scene	● AP ○ CPE
SSID DIP Group Number	1
SSID	Wireless7
	☑ Hide
Security Mode	○ Not-Encrypted ● WPA2-PSK
* PSK Password	•••••••••••••
Country/Region Code	Kazakhstan
Wireless Mode	802.11ac
Channel Width	20MHz
Channel	5180MHz(36)(Indoor)
EIRP Restriction	●
Transmitting Power	12 dBm
Antenna Gain	11 dBi
Signal Scanning	Scan

Figure 5-1 Wireless Network Basic Settings

Note

The picture used above is an example of a device with DIP switch function. Parameters of this function vary with models. The actual interface prevails.

Table 5-1 Parameter Description

Parameter	Description
Enable DIP Switch	Enable/disable the pairing code and scene switching function through the DIP switch. This function is enabled by default. Note ● If the DIP group numbers are not enough for use, you can disable this function and set SSID accordingly. ● Enabling or disabling DIP switch makes the wireless connection disconnected. Please operate with caution. ● This parameter is only available for devices with DIP switch function.
Working Scene	You can set **Working Scene** as desired through the web. Select AP to set **AP** as **Working Scene**. Select CPE to set **CPE** as **Working Scene**.
SSID DIP Group Number	1 to 16, used to indicate different group numbers. This information is only displayed when DIP switch is enabled. Note This parameter is only available for devices with DIP switch function.
SSID	● By default, the SSID is determined by the dial group number, and the CPE pairs with the AP according to SSID. ● It is recommended to hide the SSID of APs for security.
Security Mode	● **WPA2-PSK** is set by default, and the encryption method is AES. ● If **Not-Encrypted** is selected, there is no need to set **PSK Secret Key**.
PSK Password	The pairing password for CPEs and APs. If **WPA2-PSK** is set as **Security Mode**, you should configure **PSK Password**.
Country/Region Code	Set when activating the device. It is unchangeable after selected, unless you restore all the settings to default settings.
Wireless Mode	It is not configurable.
Channel Width	● For APs: Channel widths are available for selection. The specific value depends on the country/region code. ● For CPEs: The channel width is automatically changed according to the AP. It is not configurable.
Channel	● For APs: **Auto** is set by default. You can select a desired one. ● For CPEs: **Auto** is set by default. It is not configurable.
EIRP Restriction	Check to limit the EIRP (Effective Isotropic Radiated Power) of the device.
Transmit Power	A key factor affecting the wireless coverage area and the maximum achievable signal-to-noise ratio.

Parameter	Description
Antenna Gain	The power transmitted in the direction of peak radiation to that of an isotropic source.
Signal Scanning	Click **Scan** and select an optimum channel to check the signal intensity of available channels nearby.

5.2 Advanced Wireless Settings

Go to **Wireless Settings** → **Advanced Settings**, enable or disable **TDMA** and **Intelligent Frequency Management** as desired.

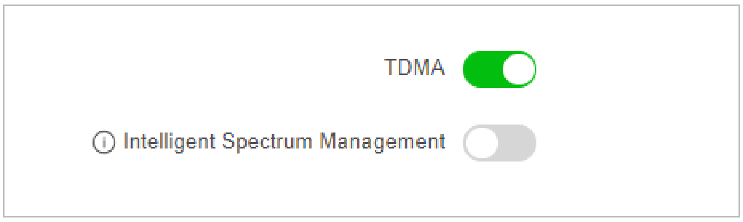


Figure 5-2 Advanced Settings

Table 5-2 Parameter Description

Parameter	Description
TDMA	Enable **TDMA** to improve the throughput performance of the working scene when an AP is connected to multiple devices. **Note** The function varies with models, and it is only supported when some devices are set as AP site. The actual interface prevails.
Intelligent Frequency Management	Enable **Intelligent Frequency Management** to ensure stable video transmission when interference is detected. **Note** ● The function is available for some models only when **AP** is set as the working scene. ● With this function, the working channel will be automatically switched to the optimal channel of all the choices except the DFS (Dynamic Frequency Selection) channels and indoor channels. ● The function varies with countries. For certain countries, this function is not available. ● With this function enabled, you are not able to set the channel and channel width manually. It is recommended that you disable this function if roaming is needed.

5.3 Admin SSID

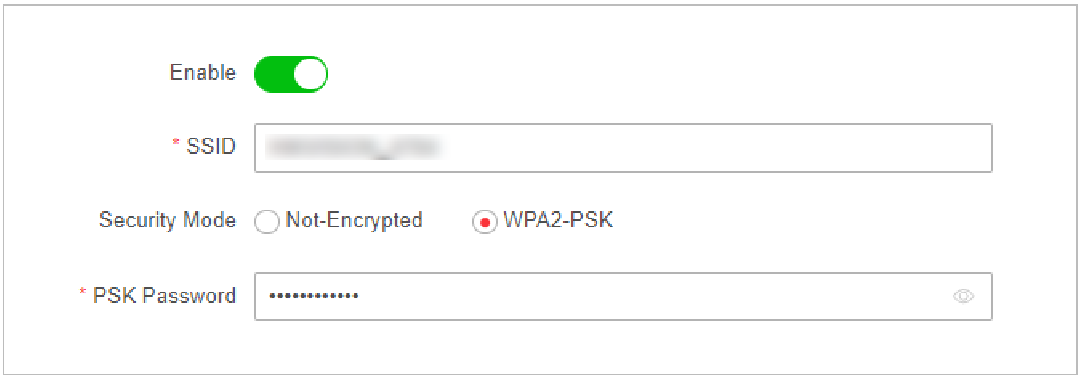
Support mobile phones and PCs to manage AP/CPE device by connecting to the device wireless network, for configuration such as setup and maintenance.

Note

- The function is only available for some models. The actual interface prevails.
- Connecting to the admin SSID cannot make the terminal access to the Internet.
- When the bandwidth is 10 Mbps, admin SSID function is only supported for the device.

Steps

1. Go to **Admin SSID.**
2. Admin SSID is enabled by default. The PSK Password is ***123456789abc*** by default.
3. Customize **SSID** and **PSK Password**. Terminals can connect to the wireless network without password, if the **Security Mode** is set as Not-Encrypted.
4. Go to ***192.168.138.10*** through the browser on your terminal to manage your bridge device.



Enable: ●

* SSID:

Security Mode: ○ Not-Encrypted ● WPA2-PSK

* PSK Password: ••••••••••••

Figure 5-3 Set Admin SSID

Chapter 6 VLAN Management

VLAN (Virtual Local Area Network) is a technology that logically (rather than physically) divides devices within a local area network into individual network segments, thereby achieving the isolation of broadcast domains within a local area network.

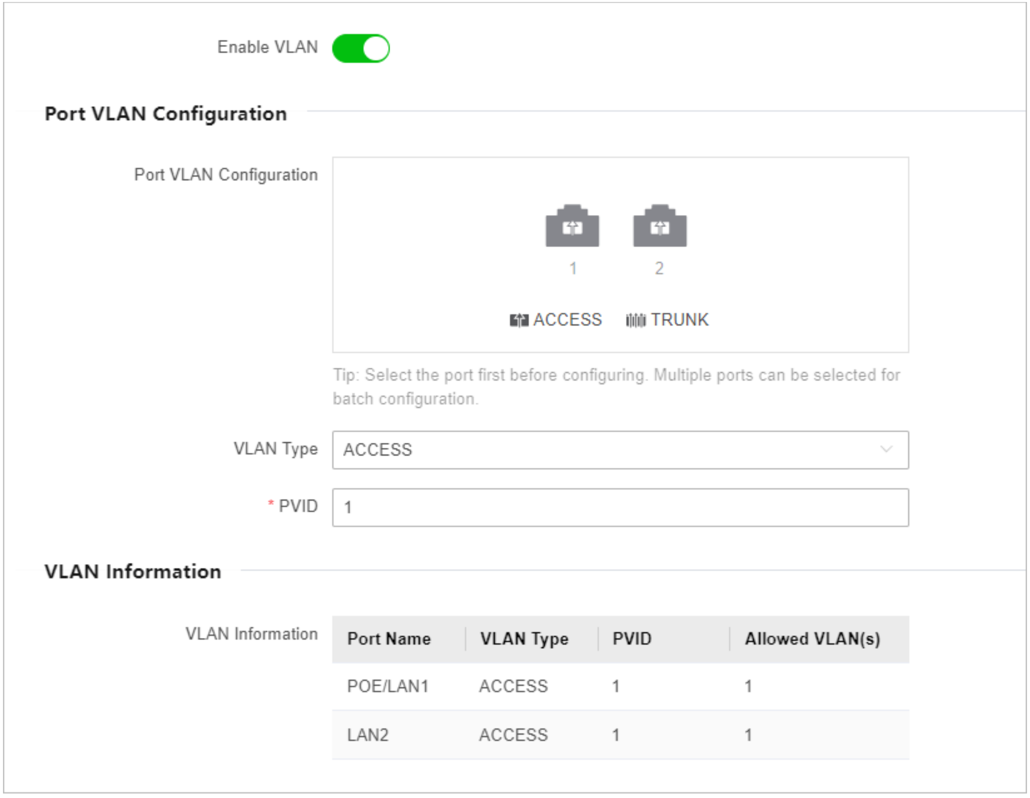
Note

The function is only available for some models. The actual interface prevails.

Steps

1. Go to **VLAN Management**.
2. Enable VLAN.
3. Configure port VLAN.
    a. Select the port to be configured.
    b. Select a VLAN type.
    - TRUNK Port: Used to carry all VLAN traffic, allowing it to pass through all VLANs.
    - ACCESS Port: Only transmits packets for the specified VLAN.

    c. Set PVID. (Range: 1~4093)
4. Click **Save**.
5. (Optional) Check VLAN information of each port.



Enable VLAN

Port VLAN Configuration

Port VLAN Configuration

Tip: Select the port first before configuring. Multiple ports can be selected for batch configuration.

VLAN Type: ACCESS

* PVID: 1

VLAN Information

VLAN Information

Port Name	VLAN Type	PVID	Allowed VLAN(s)
POE/LAN1	ACCESS	1	1
LAN2	ACCESS	1	1

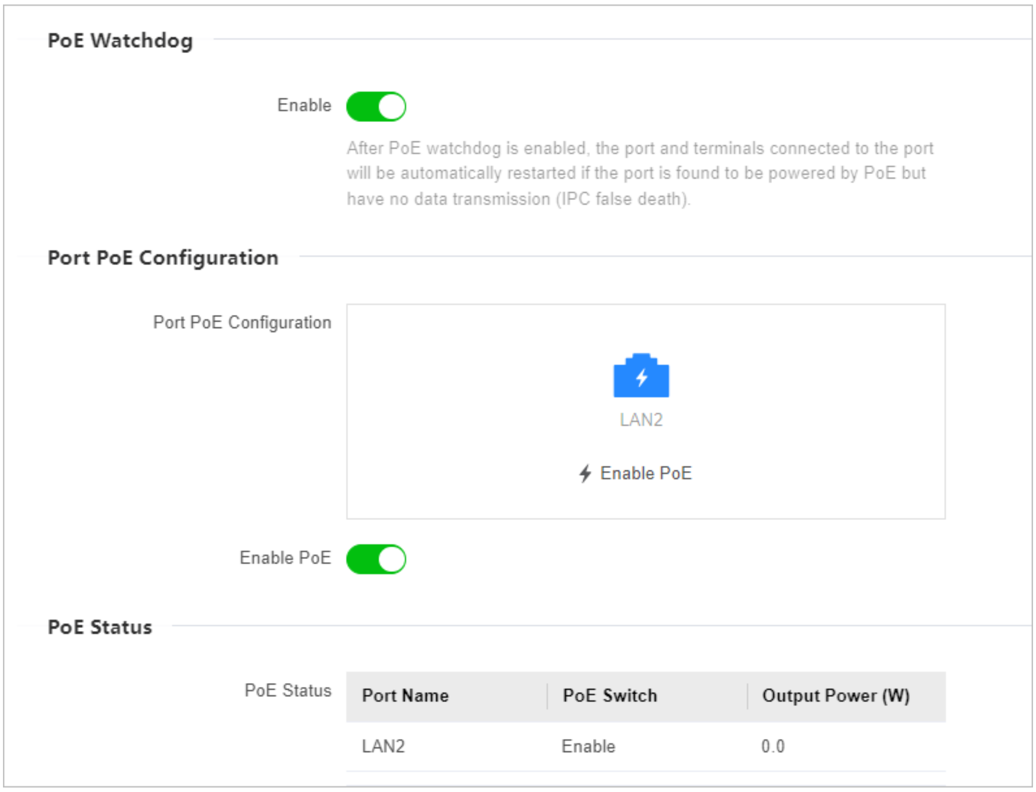
Figure 6-1 VLAN Management

Chapter 7 PoE Management

Click **PoE Management** to manage PoE port as desired.

Note

The function is only available for some models. The actual interface prevails.



PoE Watchdog

Enable: ●

After PoE watchdog is enabled, the port and terminals connected to the port will be automatically restarted if the port is found to be powered by PoE but have no data transmission (IPC false death).

Port PoE Configuration

Port PoE Configuration: LAN2 — Enable PoE

Enable PoE: ●

PoE Status

PoE Status:

Port Name	PoE Switch	Output Power (W)
LAN2	Enable	0.0

Figure 7-1 PoE Management

7.1.1 PoE Watchdog

Enabling PoE watchdog can automatically detect the connection status of devices connected to the PoE port. When a communication failure occurs on a certain port IPC, the PoE will automatically detects and restarts, making sure the normal operation of the device.

7.1.2 PoE Status Control

Select the port icon that needs to be distributed, click to **Enable** or **Disable** the PoE function of that port, and click **OK** to save your settings.

Note

Enabling or disabling PoE will not influent data transmission of the port.

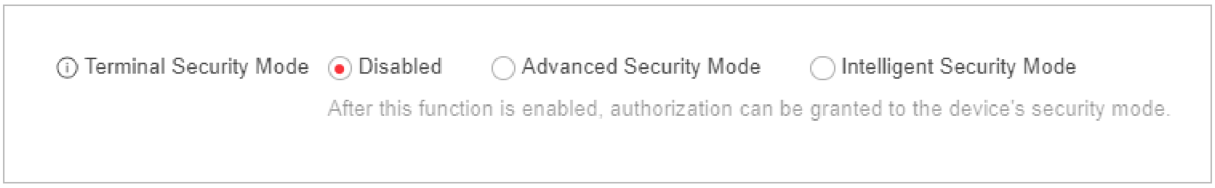
Chapter 8 Terminal Security

Go to **Terminal Security** and select the appropriate mode.

The device can identify the brand of terminals and match security policies to achieve terminal classification management.

Note

The function is only available for some models. The actual interface prevails.



ⓘ Terminal Security Mode ● Disabled ○ Advanced Security Mode ○ Intelligent Security Mode

After this function is enabled, authorization can be granted to the device's security mode.

Figure 8-1 Terminal Security

- Advanced Security Mode: The terminal authorization list displays information of the accessed terminal under this wireless bridge, and users can manually configure those accessed terminals (unauthorized terminals cannot access the network).
- Intelligent Security Mode: The terminal authorization list displays the access terminal information under this network bridge. Terminal devices binding bases on the intelligent security policy of the wireless bridge itself.

Note

After advanced security mode is enabled on the web, it is not supported to modify the configuration on other clients (such as HPP app).

Chapter 9 System Configuration

9.1 System Diagnosis

9.1.1 Manage Log

Export desired logs to your local storage.

Steps

1. Go to **Diagnosis** → **Log Management**.
2. Click **Export** to save the log files.

9.1.2 Ping Tool

Through **Ping Tool**, you can get network status information, which would be useful for the technical support.

Steps

1. Go to **Diagnosis** → **Network Tool** → **Ping Tool**.
2. Enter the IP address.
3. Click **Start Diagnose**. Diagnosis results will display.

9.1.3 Ping Watchdog

By pinging a specific IP address and check the packet loss, technical support professionals can examine the device working status. If the device is in abnormal status, they may reboot the device.

Steps

1. Go to **Diagnosis** → **Network Tool** → **Ping Watchdog**.
2. Enable **Ping Watchdog**.
3. Enter related information.

   Interval

   The interval of Ping packet.

   Start Delay

   The delay time for reboot when the device is in abnormal status.

   Number of Consecutive Failures

   The limit for packet loss times. The device is reckoned as abnormal when the packet loss times reach this limit.
4. Click **Save**.

9.1.4 Wireless Bandwidth Test

Technicians can determine whether the wireless network is smooth through wireless bandwidth testing.

Note

The function is only available for some models. The actual interface prevails.

Steps

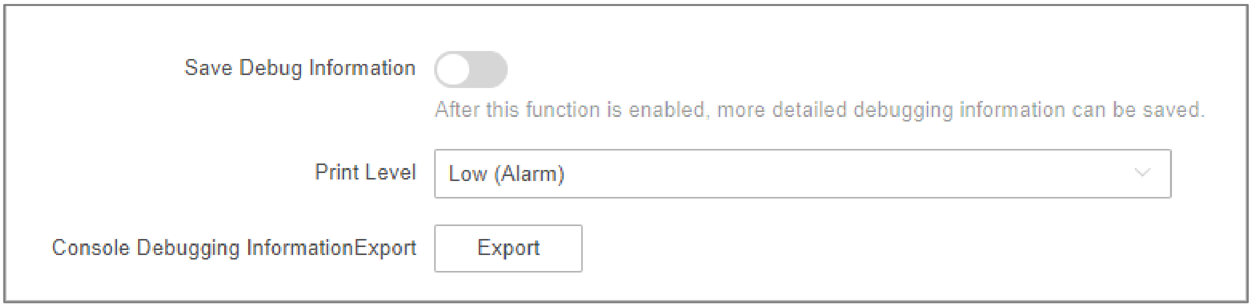
1. Go to **Diagnosis** → **Network Tool** → **Wireless Bandwidth Test**.
2. Click **Test** to get the results (including Source IP, Target IP, Average Bandwidth, and Minimum Bandwidth).

9.1.5 Save Debugging Information

Save debugging information of different print levels to the flash, and the saved information can be restored even after the device is powered off and rebooted, making it easier for technical support personnel to investigate the cause and perform later maintenance.

Steps

1. Go to **System** → **System Maintenance** → **Device Debugging**.



Save Debug Information ○

After this function is enabled, more detailed debugging information can be saved.

Print Level: Low (Alarm)

Console Debugging InformationExport: Export

Figure 9-1 Device Debugging

2. Select the Print Level. The higher the level, the more detailed the saved information.
3. Enable **Save Debug Information**. After 7 days, the function will be disabled automatically.
4. Click Save.
5. (Optional) Export the debugging information file.

9.2 System Security

9.2.1 SSH

SSH protocol can prevent information leakage caused by remote management. If SSH service is enabled, you can manage the device remotely. SSH service is disabled by default.

To improve network security, it is recommended to disable SSH services. This configuration is only for professional personnel to debug equipment.

Steps

1. Go to **System** → **System Maintenance** → **Device Debugging**.

2. Enable **SSH**.

Note

The user name of **SSH Client** is **root**, and the password is the same as that of web login.

9.2.2 HTTP(S)

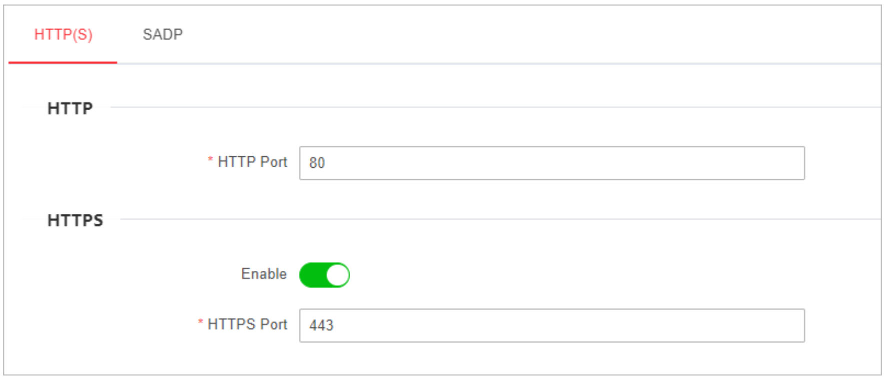
The HTTP protocol (Hypertext Transfer Protocol) is an application layer transport protocol based on the TCP protocol, while the HTTPS protocol (Secure Hypertext Transfer Protocol) is a network protocol built on SSL+HTTP protocol that can perform encrypted transmission and identity authentication.

Note

HTTP port information is only available for some models. The actual interface prevails.

Steps

1. Go to **System** → **Security Management** → **HTTP(S)**.
2. Enable HTTPS service.
3. Enter the server port number for HTTPS or HTTP connection.



HTTP

* HTTP Port: 80

HTTPS

Enable: ●

* HTTPS Port: 443

Figure 9-2 HTTP(S) Service

Note

- HTTPS service is available on port 443 by default when enabled.
- HTTP service is available on port 80 by default.
- The server port number for HTTPS service can be set as 443 or any number from 2000 to 65535.

9.2.3 SADP Service

If SADP service is enabled, you can activate the device, change password, and modify IP address through the software. SADP service is enabled by default.

Steps

1. Go to **System** → **Security Management** → **SADP**.
2. Enable **SADP**.

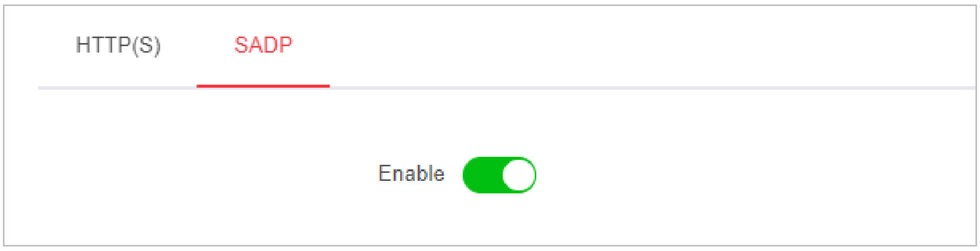


Figure 9-3 SADP Service

Note

If SADP service is disabled, some of the functions may become unavailable. It is recommended to enable this service.

9.3 Reboot the Device

You can reboot the device remotely through the web page.

Steps

1. Go to **System** → **System Maintenance** → **Reboot**.
2. Click **Reboot**.

9.4 Backup and Restore

Go to **System** → **System Maintenance** → **Backup and Restore** for backup or default settings restoration.

- **Backup: Click Export and set Password for device parameter file.**
- **Import Device Parameter: Click 🗀 and select the device parameter file that exported before.**
- **Simple Restore**: Restore the parameters to the default settings, except network settings and user settings.
- **Restore All**: Restore all the parameters to the default settings.

Caution

- Restoring all the parameters will clear all the settings, please operate with caution.
- It is recommended to export all the configuration files before restoration.
- Password is required for importing device parameter file, and the device will restart automatically after device parameter file has been imported.

9.5 Upgrade the Device

Use the newest firmware for available upgrades, and upgrade the device through web page remotely.

Before You Start

Copy the upgrade package to the local directory of the PC used for remote access.

Steps

1. Go to **System** → **System Maintenance** → **Upgrade**.
2. Click 🗀 to go to the local directory, and select the desired upgrade package.
3. Click **Upgrade**.

Note

- The device will reboot automatically after upgrade, and you need to log in again.
- If upgrade fails and the device cannot work normally, please contact the supplier for restoration.

9.6 Intelligent Power Management

When the intelligent power management feature is enabled, the device would power off automatically in condition of insolvable device failure.
Go to **System Management** → **Device Maintenance**. Enable **Intelligent Power Management** as needed.

Note

This function is only available for some models. The actual interface prevails.

9.7 Set Time

Both manual time synchronization and NTP time synchronization are supported.

9.7.1 Manual Setting

You can set a desired specific time, or synchronize the time with that of the computer.

Steps

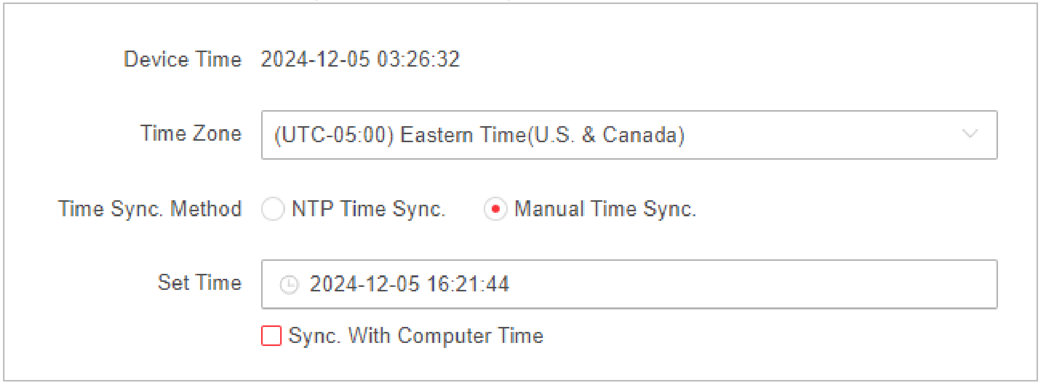
1. Go to **System** → **System Configuration** → **Time Configuration**.
2. Select a **Time Zone**.

Note

The time zone is automatically selected after you set the country/region code. You can also select the desired time zone as needed.

3. Select **Manual Time Sync.** as **Time Sync. Method**.

4. Set the desired time or check **Sync. With Computer Time**.



Device Time 2024-12-05 03:26:32

Time Zone (UTC-05:00) Eastern Time(U.S. & Canada)

Time Sync. Method ○ NTP Time Sync. ● Manual Time Sync.

Set Time 2024-12-05 16:21:44

□ Sync. With Computer Time

Figure 9-4 Manual Setting

5. Click **Save**.

9.7.2 NTP Setting

NTP time synchronization is used to synchronize the time with that of a specific NTP server.

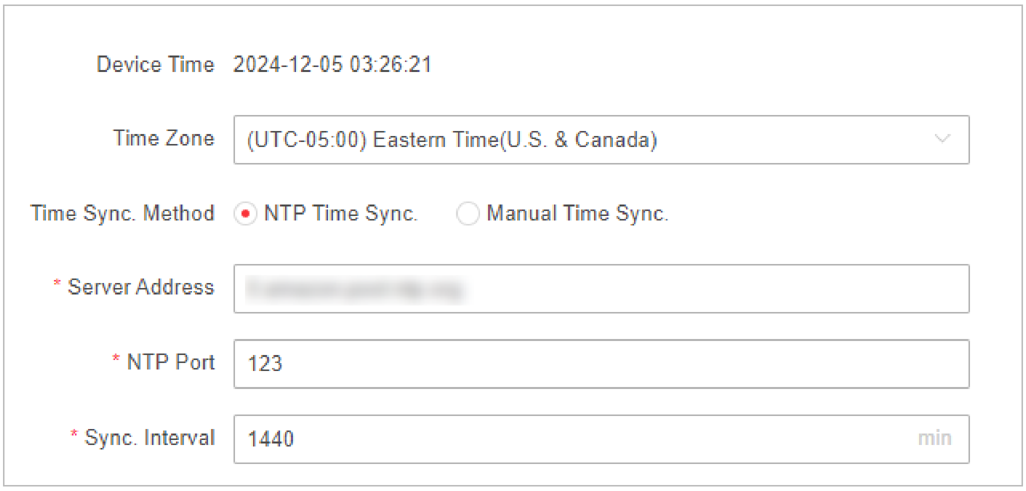
Steps

1. Go to **System** → **System Configuration** → **Time Configuration**.
2. Select a **Time Zone**.

Note

The time zone is automatically selected after you set the country/region code. You can also select the desired time zone as needed.

3. Select **NTP Time Sync.** as **Time Sync. Method**.



Device Time 2024-12-05 03:26:21

Time Zone (UTC-05:00) Eastern Time(U.S. & Canada)

Time Sync. Method ● NTP Time Sync. ○ Manual Time Sync.

* Server Address [redacted]

* NTP Port 123

* Sync. Interval 1440 min

Figure 9-5 NTP Setting

4. Enter NTP server information.

Server Address

The IP address of the NTP server.

NTP Port

Monitoring port of the NTP server. Default value: 123. Value range: 1 to 65535.

Sync. Interval

The frequency for the device to synchronize with the NTP server. Value range: 1 to 10080 minutes.

9.8 Change Password

For data security, we highly recommend you to change your password regularly.

Steps

1. Click 🔒 at the upper-right corner.

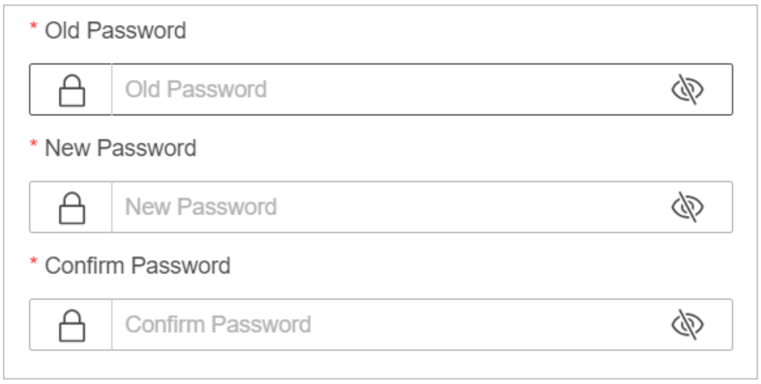


Figure 9-6 Change admin Password

2. Enter the original password, new password and confirm.
3. Click **Save**.
   The web page redirects to the login interface.

Chapter 10 FAQs

10.1 Why the device cannot start up?

Reason

1. The network cable length connecting the wireless bridge to the PoE module exceeds 60 m.
2. The network cable cannot meet the standard of Category 5e.
3. The registered jack of the network cable is not firmly connected, or the connection order is improper.

Solution

1. Use a network cable shorter than 60 m.
2. Use a network cable with Category 5e or higher standard.
3. Remake the registered jack.

10.2 Why devices pairing failed?

Reason

The devices pairing status depends on the distance, direction, SSID name, and PSK password.

Solution

You can check as follows:

1. Check distance and direction: Ensure the AP and CPE are directly faced to each other, and the distance between them is within the limit.
2. Check SSID name and PSK password: Ensure the SSID name and PSK password are correct.

10.3 Why the wireless connection rate is relatively low?

Reason

The wireless system makes connection with its maximum working rate, and the actual rate depends on the distance and environment.

Solution

You can check as follows to ensure the highest connection rate:

1. Device position: Adjust the device position and direction.
2. Wireless channel or frequency: Change to another signal channel or frequency to reduce interference.
3. Wireless interference: Adjust, shield, or disable the device causing interference.

10.4 Why the signal intensity is too low?

Reason

1. There is a large-sized obstruction between the CPE and the AP.
2. The CPE is not directly faced to the AP.

Solution

1. Remove the obstruction or bypass it.
2. Adjust the angle of the CPE and the AP.

10.5 Why the throughput is inadequate even with high signal quality?

Reason

1. Excessive interference or multipath interference.
2. Wired device error.

Solution

1. Remove the interference or change the device frequency.
   Method of changing frequency: Reboot the AP of wireless bridge to allow auto search of available signal channels.
2. Change a network cable or use another PC.

10.6 Why there are excessive packet loss and time delay when PC pings the device IP address?

Reason

1. The registered jack of the network cable is not firmly connected.
2. The IP addresses of multiple devices conflict.

Solution

Port isolation should be conducted for APs connected to the same switch.

1. Remake the registered jack.
2. Modify the IP addresses of different devices.