



Wireless Bridge (Client)

User Manual

Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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 Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

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". HIKVISION 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 HIKVISION 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 HIKVISION 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 HIKVISION 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, HIKVISION 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.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see:

<http://www.recyclethis.info>.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:

<http://www.recyclethis.info>.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.




Preface

Applicable Models

This manual is applicable to iVMS-4200 client of the switch.

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.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Danger

- This is a class A product and may cause radio interference in which case the user may be required to take adequate measures.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The serial port of the equipment is used for debugging only.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Keep vertical downward when moving or using the equipment.

Caution

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.

Contents

Chapter 1 Introduction	1
Chapter 2 Device Management.....	2
2.1 Activate the Device	2
2.2 Add the Device	3
Chapter 3 Device Status.....	5
Chapter 4 Network Configuration	7
Chapter 5 Wireless Network Configuration	8
Chapter 6 System Configuration	10
6.1 Device Information.....	10
6.2 User Management.....	10
6.3 Device Maintenance.....	11
6.4 Log Management.....	11
6.5 Security Configuration.....	12
Chapter 7 FAQ.....	13
7.1 Why the device cannot start up?	13
7.2 Why devices pairing failed?	13
7.3 Why the wireless connection rate is relatively low?	13
7.4 Why the signal intensity is too low?	13
7.5 Why the throughput is inadequate even with high signal quality?	14
7.6 Why there are excessive packet loss and time delay when PC Pings the device IP address?	14
Appendix A Communication Matrix.....	15

Chapter 1 Introduction

You can manage and configure the device through iVMS-4200, including device management, network configuration, system configuration, etc.

 **Note**

The wireless bridges vary with different models. The actual device prevails.

Chapter 2 Device Management

The device can be configured and managed through iVMS-4200 software, mainly including network parameter configuration, wireless configuration, system maintenance, and so on.

Note

- This chapter will briefly introduce the device management through iVMS-4200 software. For other functions, please refer to *User Manual of iVMS-4200 Software*.
- All pictures in this manual are for illustration only, and the specific interface is subject to the actual device.

2.1 Activate the Device

For the inactive devices, you are required to create a password to activate them before they can be added to the software and work properly.

Before You Start

Make sure the device to be activated is connected to the network and is in the same network segment with the PC running the client.

Steps

Note

This function should be supported by the device.

1. Run iVMS-4200 software.
2. Go to **Device Management** → **Device**.
3. Click **Online Device** to show the online devices.
The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.

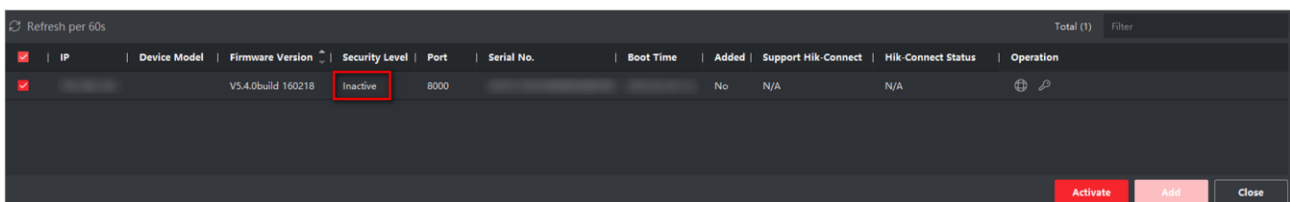


Figure 2-1 Online Inactive Device

5. Click **Activate**.
6. Create a password in the password field, and confirm the password.

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: upper case letters, lower case 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.

7. Click **OK** to activate the device.

2.2 Add the Device

The client provides various device adding modes including IP/domain, IP segment, cloud P2P, ISUP protocol, and HiDDNS. The client also supports importing multiple devices in a batch when there are large amount of devices to be added. The section only introduces one mode, namely, adding a detected online device.

Steps

1. Go to **Device Management** → **Device**.
 2. Click **Online Device** to show the online devices.
The searched online devices are displayed in the list.
 3. Select an online device, and click **Add**.
-

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, see [2.1 Activate the Device](#).

5. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

You can customize the port No. The port No. of the device is obtained automatically in this adding mode.

User Name

By default, the user name is **admin**.

Password

Enter the device password set for activation.

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: upper case letters, lower case 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.
-

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.

7. Click **Add**.

Note

If the country/region code of the device is not configured, you need to select a country/region code after adding the device.

8. Optional: Click  to edit the information of the device.

Chapter 3 Device Status

Click  to view the device status, basic wireless settings, port status, and port statistics.

Note

All pictures in this manual are for illustration only, and the specific interface is subject to the actual device.

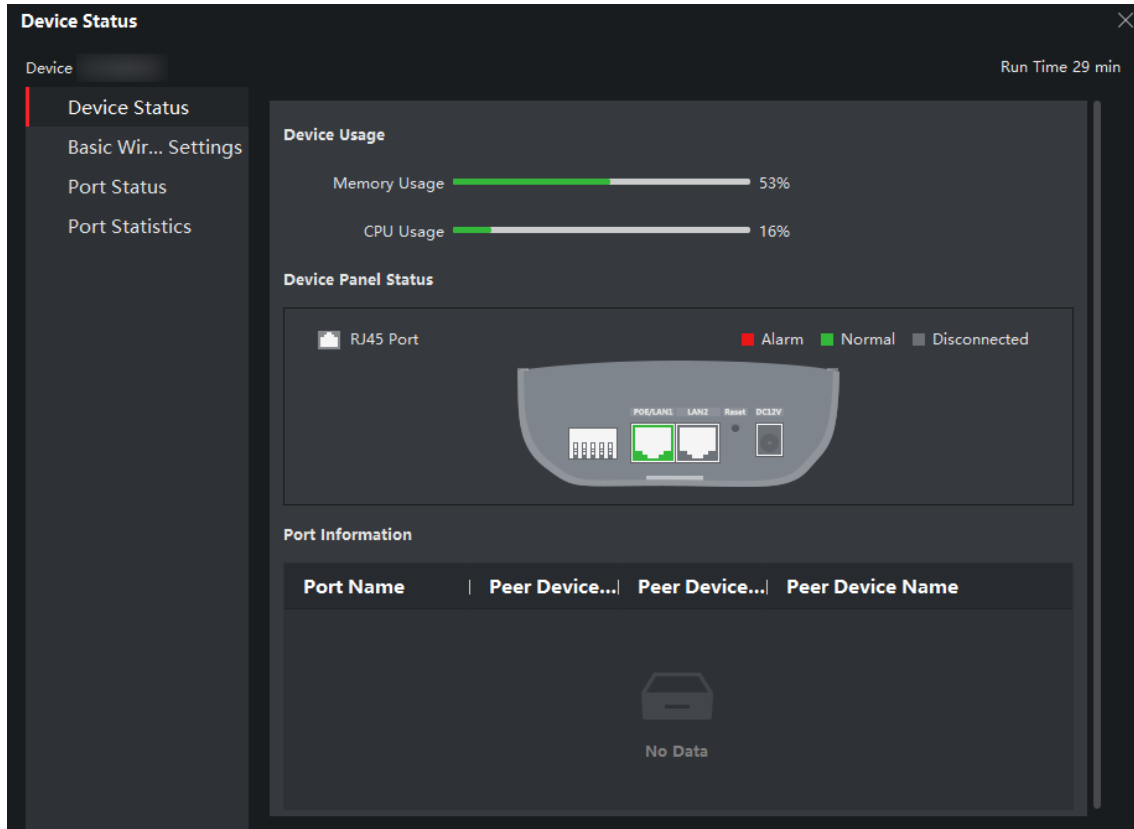


Figure 3-1 Device Status

Device Status

View the device usage, device panel status and port information.

Basic Wireless Settings

View the channel width, channel frequency, working scene, transmit power, etc.

Port Status

View the bitrate, duplex, and flow control of ports.

Port Statistics


View the number of bytes sent or received, the number of packets sent or received, sending or receiving rate, and peak value of sending or receiving rate.

 **Note**

Drag the sliding bar on the bottom to view all data.

Chapter 4 Network Configuration

Basic Settings

Go to  → **Network** → **General** to configure NIC type, IPv4 address, subnet mask, gateway address, MAC address, and device port.

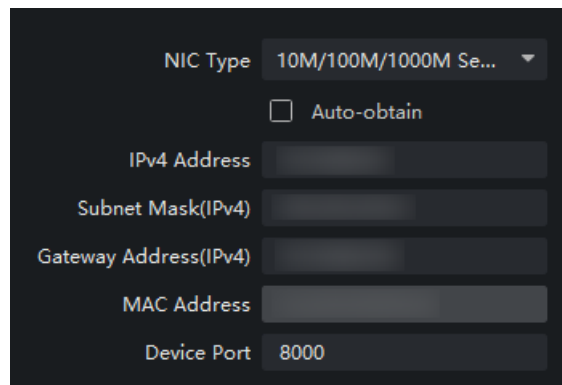



Figure 5-1 Network Configuration

Note

After the IPv4 address is reset, the device IP may not be in the same network segment as the computer IP of the client, so it cannot be configured and managed. It is recommended to use the SADP tool to plan the IP address of the device when the device is activated for the first time.

Advanced Settings

Go to  → **Network** → **Advanced Settings** to configure DNS IP address. DNS server address of your own computer or public address on the internet are both available.

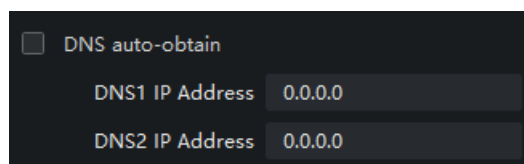


Figure 5-2 Advanced Settings

Note

- **DNS auto-obtain** is available only when you check **Auto-obtain** in **Network** → **General**.
 - It is recommended to configure both DNS1 and DNS2 address to prevent that one of the addresses is invalid.
-


Chapter 5 Wireless Network Configuration

Go to  → **Wireless Configuration** → **General** to configure wireless network parameters as needed.



Figure 5-1 Wireless Network Configuration

Table 5-1 Parameter Description


Parameter	Description
Enable DIP Switch	<p>Enable/Disable the pairing code and scene switching function through the DIP switch.</p> <p>This function is enabled by default.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> • If the numbers of DIP group is not enough, you can disable this function and set SSID accordingly. • Enabling or disabling DIP switch makes the wireless connection disconnected. Please operate carefully.

Wireless Bridge (Client) User Manual

Parameter	Description
Dial Group No.	1 to 16 indicate different numbers of groups. This information is only displayed when DIP switch is enabled.
Working Scene	<ul style="list-style-type: none"> ● DIP switch enabled: The web displays the selected working scene of the device. If AP is selected on the device, the web displays AP in Working Scene. If CPE is selected on the device, the web displays CPE in Working Scene. ● DIP switch disabled: 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	<ul style="list-style-type: none"> ● By default, the SSID is determined by the dial group number, and the CPE pairs with the AP according to SSID. ● If DIP switch is disabled, you can set SSID as desired. ● It is recommended to hide the SSID of APs for security.
Country/Region Code	Set when activating the device. It is unchangeable after selected, unless you restore all the settings to default settings.
Wireless Mode	Default value: 802.11ac . It is not configurable.
Channel Width	<ul style="list-style-type: none"> ● For APs: Three channel widths available: 20 MHz, 40 MHz, and 80 MHz. 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	<ul style="list-style-type: none"> ● For APs: Auto is set by default. You can set a desired one. ● For CPEs: Auto is set by default. It is not configurable.
Security Mode	<ul style="list-style-type: none"> ● 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 Secret Key	The pairing password for CPEs and APs. If WPA2-PSK is set as Security Mode , you should configure PSK Secret Key .

Chapter 6 System Configuration


6.1 Device Information

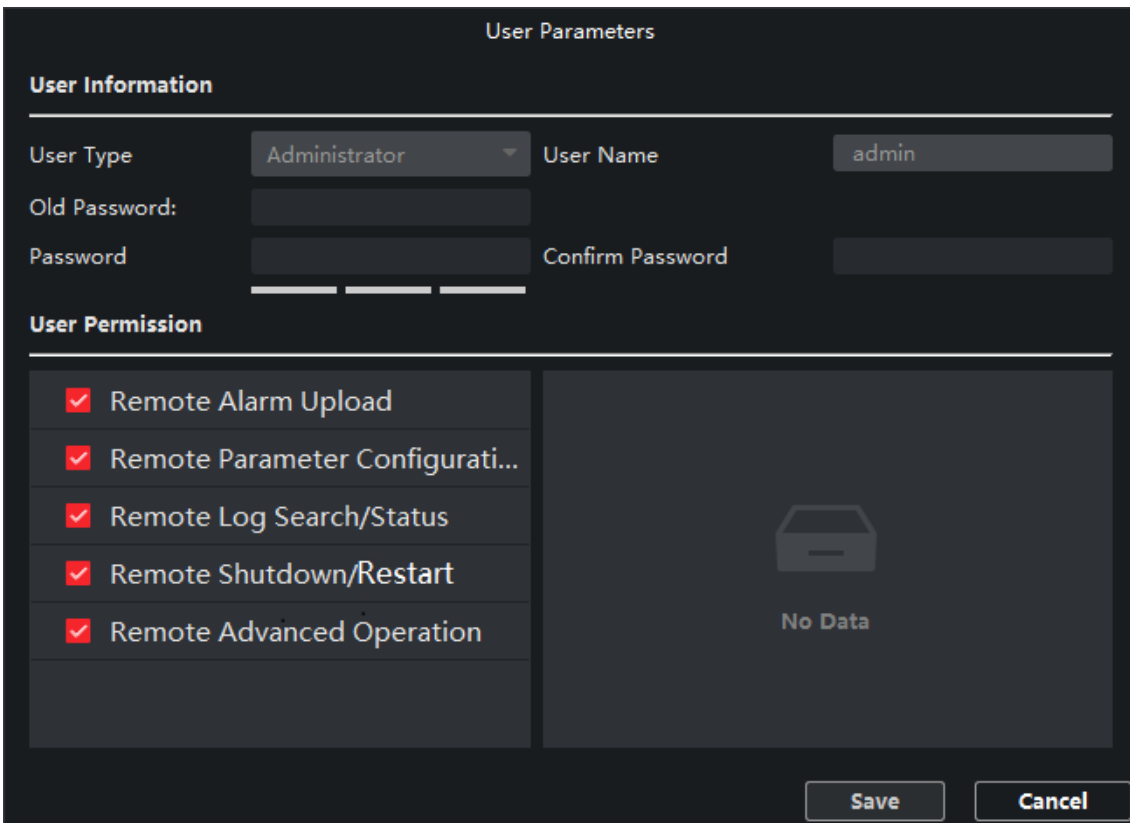
Go to  → **System** → **Device Information** to view the device information, including device name, device model, serial No., and program version.

6.2 User Management

The device only supports one admin user. Users cannot be added or deleted. You can only edit the passwords, IP addresses and permissions of the user.

Steps

1. Go to  → **System** → **User**.
2. Click **Edit** or double-click the user to edit the password, IP address or permission of the user.



The screenshot shows the 'User Parameters' configuration window. It is divided into two sections: 'User Information' and 'User Permission'. In the 'User Information' section, the 'User Type' is set to 'Administrator' and the 'User Name' is 'admin'. There are input fields for 'Old Password', 'Password', and 'Confirm Password'. The 'User Permission' section contains a list of permissions with checkboxes: 'Remote Alarm Upload', 'Remote Parameter Configurati...', 'Remote Log Search/Status', 'Remote Shutdown/Restart', and 'Remote Advanced Operation'. All these checkboxes are checked. To the right of this list is a large grey area with a car icon and the text 'No Data'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 7-1 User Parameters

Note



8 to 16 characters is allowed for the password, including at least 2 of the following types: digits, lower-case letters, upper-case letters, and special characters. The password strength of the device can be automatically checked. We highly recommend you change your password regularly in order to increase the security of your product.

3. Optional: Click the user name at the upper-right corner on the client for more user operations.

6.3 Device Maintenance

You can restart the device, restore the defaults, and upgrade your device.

Steps

1. Go to  → **System** → **System Maintenance**.
 2. Select function button to realize different functions.
 - **Reboot**: Click **Reboot** to remotely restart the device.
 - **Restore Default Settings**: Except network configuration and user parameters, all of the other parameters are restored to the default settings.
 - **Restore All**: All parameters are restored to the default settings. After restoration, the device needs to be activated again.
 - **Import Configuration File**: Select the configuration file, and enter the password for file export. After import, the devices will be restarted automatically.
 - **Export Configuration File**: Set and confirm the password for file export, and click **OK**. Select a storage path, and click **Save**.
 - **Upgrade**: Click  to select the upgrade file, and click **Upgrade**. The upgrading progress is shown below.
-

Note

If upgrading failed or the device cannot function, please contact our technical support professionals.

6.4 Log Management

System operation logs can be searched and exported for backup.

Steps

1. Click **System Log** on the left area.
2. Set search conditions.

Time

Set the start time and end time for the logs to be searched.

User Name

Select the user to be searched.

Log Type

Operation Log and System Log can be selected. Minor type is different under different major type. If you select the search mode as by time, the major type cannot be set.

3. Click **Search**.
4. Click **Back Up Logs**, and select a backup path.
5. Click **Backup**.


6.5 Security Configuration

If the IP is locked because you enter a wrong password, the admin user can log in to the client at the PC (the IP is not locked) and enter the **Security** interface to unlock the locked IP.

Steps

Note

If you need to unlock it immediately, you can contact the admin user.

1. Select  → **System** → **Security**.
 2. Unlock the desired IPs.
 - Click unlock icon to unlock a single IP.
 - Click **Unlock All** to unlock all of the IPs.
-

Note

- If the admin user is locked, you need to change the IP to log in admin again and unlock the locked IP.
 - Up to 5 trials of password are allowed for ordinary users, and 7 for the admin user.
-

Chapter 7 FAQ

7.1 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.

7.2 Why devices pairing failed?

Reason

The devices pairing status depends on the distance, direction, and DIP switch setting.

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. DIP switch enabled: Ensure the pairing codes of the AP and CPE are consistent.
3. DIP switch disabled: Ensure the SSID name and PSK password are correct.

7.3 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.

7.4 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.

7.5 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 channel.
2. Change a network cable or use another PC.

7.6 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 address 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.

Appendix A Communication Matrix

Please scan the QR code below to view the communication matrix document.



Figure A-1 Communication Matrix



See Far, Go Further