3onedata

BlueEyesView

Integrated Monitoring and Management System

User Manual

Document Version: 05

Issue Date: 04/11/2022

Industrial Ethernet Communication Solution Expert **3onedata Co., Ltd.**

Trademark statement

3onedata , 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notice

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

The user manual of integrated monitoring and management system introduces BlueEyesView:

- Functional performance
- Installation and configuration method
- Network management and monitoring function

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Fox example “Port number”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Symbols

Format	Description
 Notes	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Notes	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.

Format	Description
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	4/01/2020	First release
02	5/20/2020	Optimize the installation in Windows system
03	9/04/2020	Function optimization, software version upgrade
04	1/26/2021	Web interface optimization
05	4/08/2021	Function optimization, software version upgrade

Contents

1 Overview

BlueEyesView provides a visual and centralized integrated monitoring and management system for industrial internet devices. It can manage all internet devices produced by our company or other manufacturers. The system includes topology diagram, topology management, device management, configuration management, alarm management, statistical analysis, system management and other modules.

Note
Due to version upgrade and other reasons, individual devices may not be recognized. Please contact customer service agent for help.

Based on ICMP, ARP, SNMP, LLDP and 3onedata private protocols, BlueEyesView provides detailed topology diagram, port connection information, bandwidth utilization and other network information for the network environment. Support centralized discovery and unified management of IP devices such as routers, switches, wireless switches, wireless APs, serial servers, CAN servers, Modbus gateways, PCs, cameras, wireless terminals; Support unified management of wireless devices, provide wireless group configuration, and realize batch configuration of WiFi, black and white list, probes and other parameters; Support device firmware management and configuration file backup, and provide remote batch upgrade and recovery backup; Support alarm playback, AP playback and custom alarm level, and provide alarm methods such as e-mail, short message and local voice; Statistical analysis chart and network topology function can realize visual network fault diagnosis, so as to quickly troubleshoot and locate faults.

Support optional installation on Windows and Linux operating systems, which can meet the demands of multiple operating environments and sites. It can be widely used in rail transit, smart city, safe city, new energy, intelligent manufacturing, utility tunnel

monitoring and other industrial fields, providing real-time monitoring and management for industrial Internet devices and ensuring the stable operation of the network system.

1.1 Introduction of Characteristics

- Based on B/S architecture, developed by mainstream Java EE technology and supports multi-system deployment
- Linux system supports stand-alone deployment and distributed deployment
- Provide a powerful authority control system to manage users' functional authority and data authority
- Support remote and centralized device monitoring and management via WEB interface
- Based on the international ICMP, ARP, SNMP, LLDP protocols, it can conduct centralized discovery and unified management of devices
- Support 3onedata private discovery protocol and provide real and visual panel library, and clear network topology
- The network topology diagram provides general view, the 3onedata view and traffic view switching, and the traffic view can view the dynamic distribution state of network traffic load
- Support device performance information, traffic statistics, VLAN information, spanning tree port, 3onedata ring and other information collection
- Support network diagnosis, provide Ping command and Traceroute route tracing that can view network connectivity and network path
- Support access to device CLI interface, provide Telnet client with smooth operation
- Support AP event playback, device alarm playback, and the alarm state change of topology diagram
- Support frequent alarm mechanism to ensure system performance
- Support visual topology, web message, mail, short message, local voice and other alarm methods
- Provide intelligent chart analysis for device type, online status, offline status, CPU/ memory utilization, fault distribution, etc.
- Support WEB proxy server, and access to the WEB interface of device across network segments
- Support the northbound interface RESTful API interface and OPC UA interface to provide information such as network, device, topology and alarm for external applications
- Support log information recording such as user login and user operation
- Based on HTML5 technology, the data analysis table items are displayed dynamically in real time, and the page layout is simple and easy to operate
- Based on the development and operation of free and open source software, low operating cost

2 Installing BlueEyesView on Windows System

BlueEyesView provides different installation packages for Linux system and Windows system. This chapter mainly introduces the operation process of installing integrated monitoring and management system under Windows system. This section provides the operation process of installing, authorizing, upgrading and uninstalling the BlueEyesView integrated monitoring and management system in Windows system.

Note

- This chapter takes Windows10 64-bit operating system as an example to install and configure the system.
- BlueEyesView provides different installation packages for Linux system and Windows system. Please ensure to obtain the installation package matching the operating system.

2.1 System Requirements

Windows operating system requirements:

Hardware	System Requirements
Operating system	Windows Server 2016/2019, Windows 7/10 and other 64-bit operating systems. Note: The built-in database system of the BlueEyesView is MySQL Community Edition8. It can be installed on operating systems such as Windows Server 2016 and above. If you need to install on Windows Server 2012 and earlier operating systems, please contact customer service personnel to customize the installation program.
Browser	In browsers like Chrome, Firefox, Edge, IE10 and above, Chrome browser is recommended. Notice:

Hardware	System Requirements
	If you use a browser whose configuration is lower than that of the above browsers , it may cause abnormal display of the WEB interface.
CPU	Single 4-core 2GHz and above, Core i5/i7/i9 series or XEON series is recommended.
Memory	8GB and above, 16GB is recommended.
Disc	1TB hard disk, redundant configuration and backup disk are recommended.
Monitor	1980x1080 and above resolution is recommended . Note: Resolution lower than this will affect the page layout effect.

2.2 System Firewall Configuration

Note

- If the firewall of the operating system is not enabled, you can skip this subsection "System Firewall Configuration" and refer directly to the next subsection "Installation of Integrated Monitoring System".
- On the premise of ensuring network security, the firewall can be disabled.
- If the firewall of the operating system is enabled, please open the service port used by BlueEyesView; Otherwise, related services will be abnormal.

If the firewall is enabled, please open the following ports:

- 162: port for SNMP protocol to receive Trap messages.
- 8181: port for sending short message application server WEB service.
- 8282/8283: application server WEB service HTTP/HTTPS port.
- 8285: port for Mib Browser tool to use HTTPS port.
- 8686: WEB proxy server port.
- 65534: UDP listening port of management system.
- 50000-60000: port range of Web proxy.

Configuration Instance

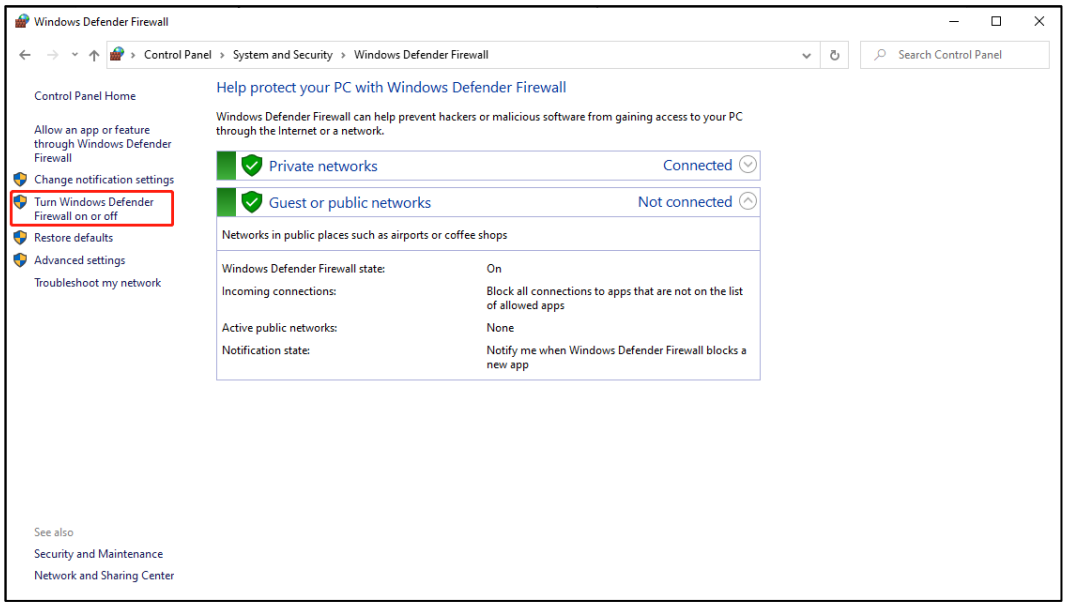
In the Windows10 system, enable the firewall and open the above ports.

Operation Steps

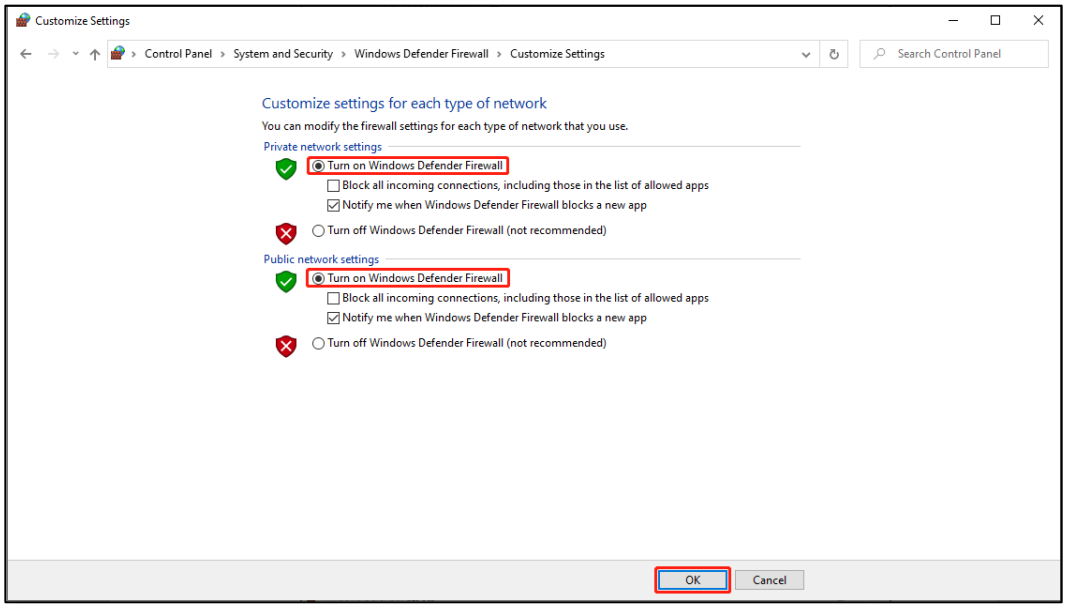
Step 1 On the system menu bar, click “Start > Windows System > Control Panel“ to open the control panel.

Step 2 In the control panel, click to open the ”Windows Defender Firewall”.

Step 3 In the “Windows Defender Firewall” window, click “Turn Windows Defender Firewall on or off”, as shown in the following figure.



Step 4 Turn on the firewall as follows.



1 Under the “Private network settings” configuration bar, select “Turn on Windows Defender Firewall”;

2 Under the “Public network settings” configuration bar, select “Turn on Windows Defender Firewall”;

3 Click the "OK" button, as shown in the above figure.

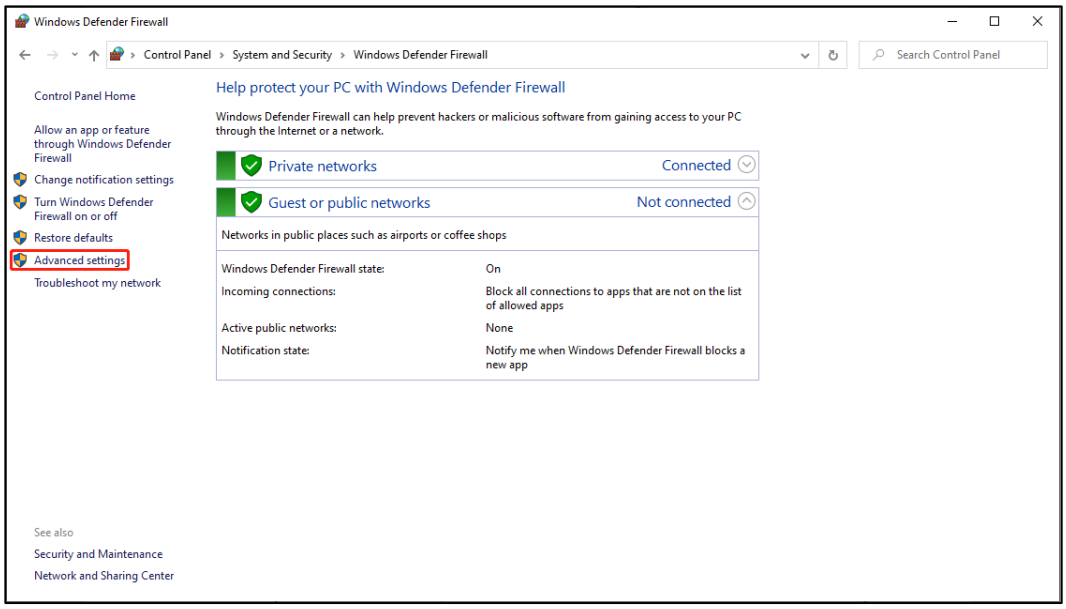
Note:

If the firewall is turned on, do not check "Block all incoming connections …".

Step 5 Open UDP protocol port 162 and 65534.

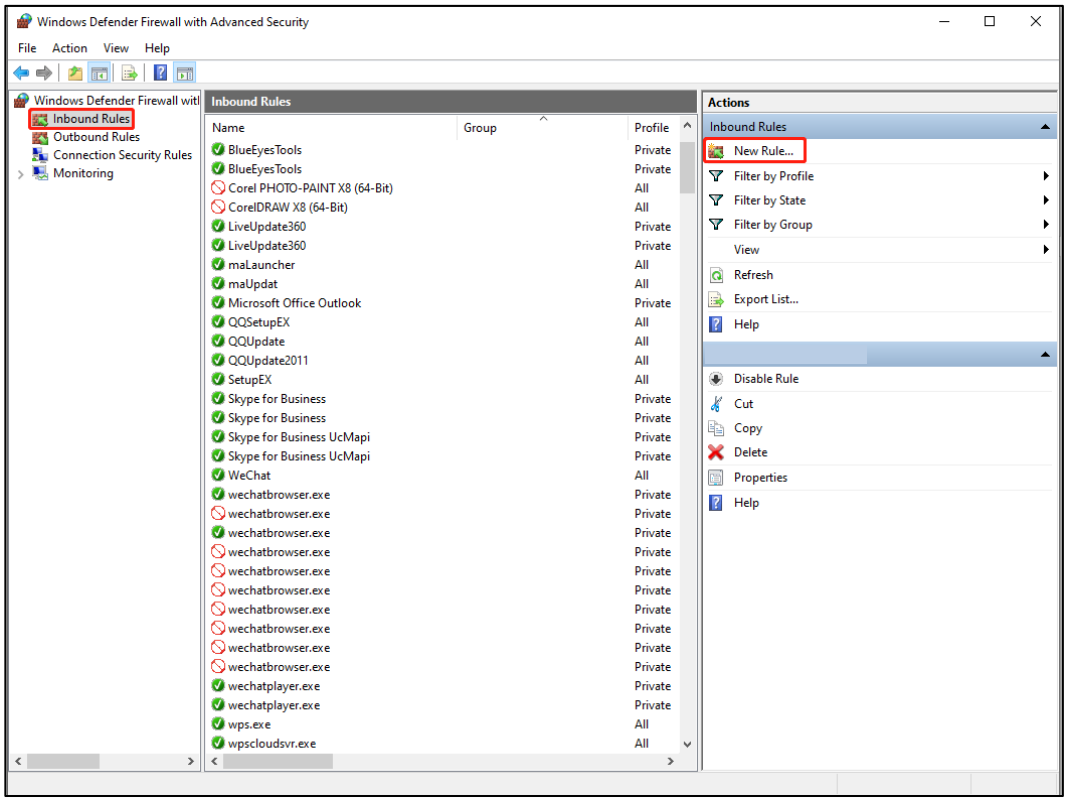
1 In the Windows Defender firewall window, click “Advanced settings”, as shown in

the following figure.



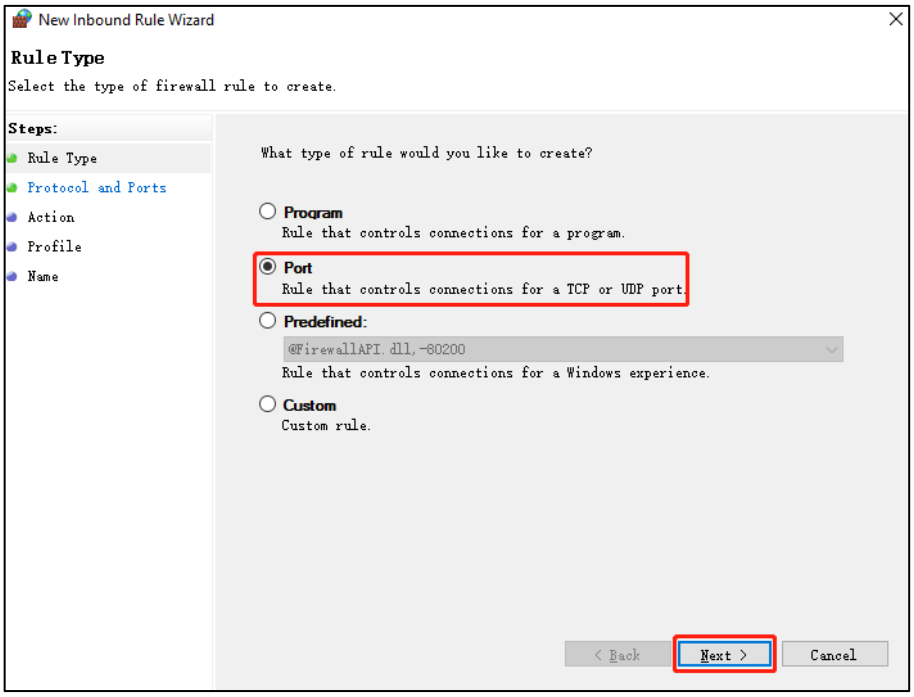
2 In the “Windows Defender Firewall with Advanced Security” window, click “Inbound Rules”, as shown in the following figure.

3 In the “Actions” area of inbound rules, click “New Rule…”.

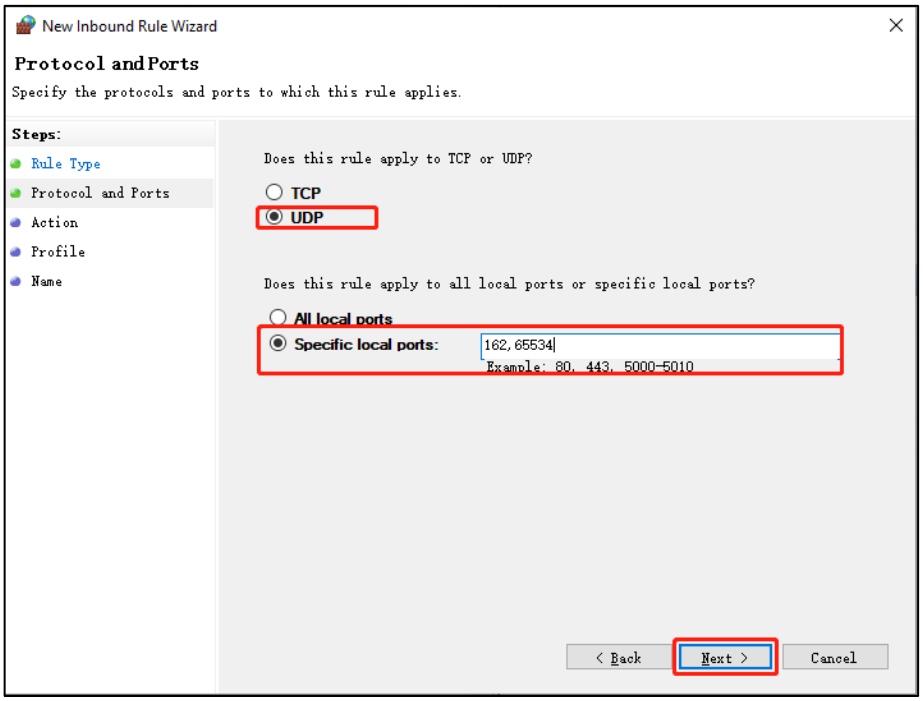


4 Open port 162 and 65534.

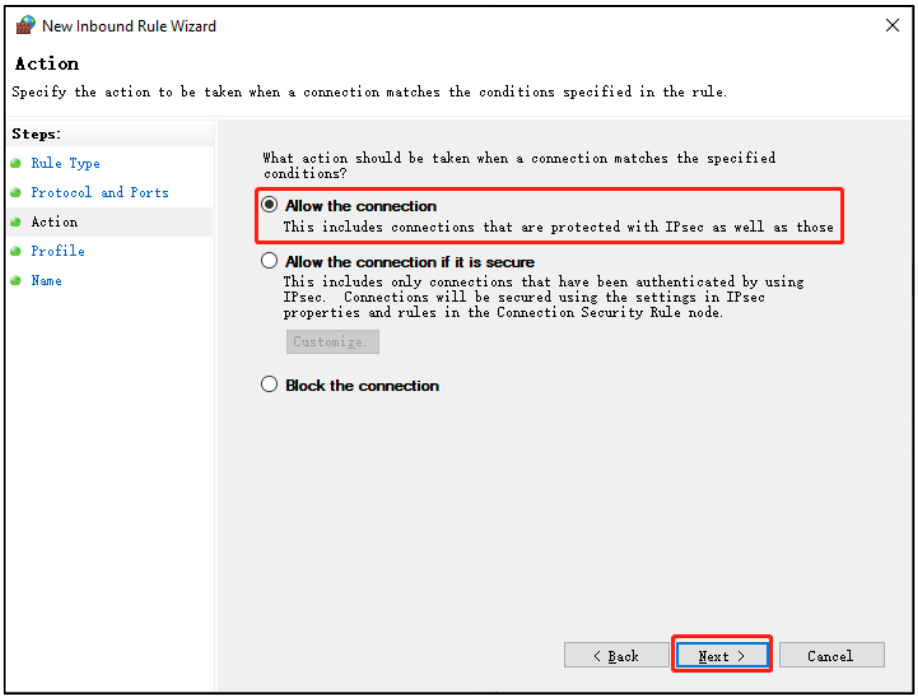
- In the rule type, check the radio box before "Port";
- Click “Next” as shown below;



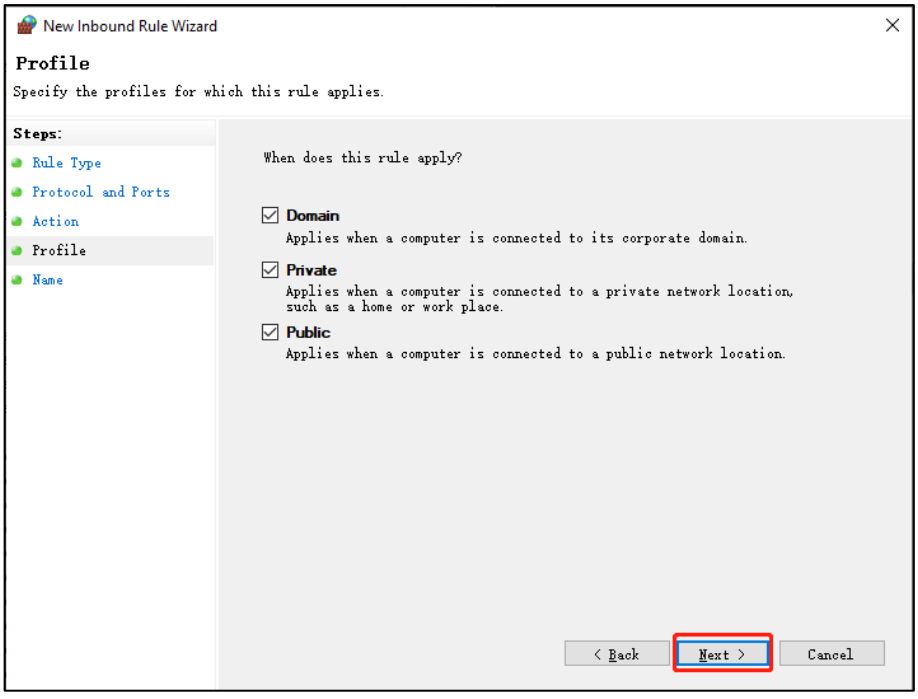
- In the protocol and ports, check the radio box before "UDP";
- Check the radio box before "Specific local port";
- Enter the port "162,65534" in the text box after "Specific local port";
- Click “Next” as shown below.



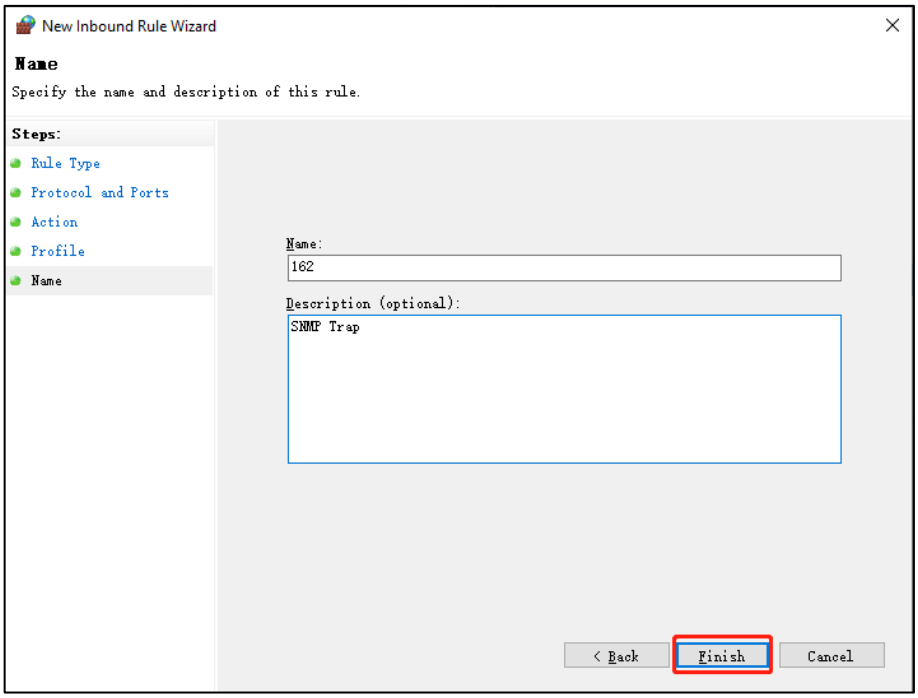
- In action, check the radio box before "Allow the connection";
- Click “Next” as shown below;



- In the profile, check the check boxes before the "Domain", "Private" and "Public" networks;
- Click “Next” as shown below;



- Enter a custom name in the “Name” text box;
- Click “Finish”, as shown in the following figure.



Step 6 Open TCP protocol port 8181, 8282, 8283, 8285, 8686, 50000-60000. The opening process is similar to opening UDP port. Repeat Step 5 to modify the following differences in the rule type:

- In the rule type, check the radio box before "TCP";
- Enter the port "8181, 8282, 8283, 8285, 50000-60000" in the text box after "Specific Local Port";

Step 7 End.

2.3 Install Integrated Monitoring and Management System

Before installation, please obtain the BlueEyesView installer corresponding to the Windows operating system: "BlueEyesViewInstall V2.1.exe".

Install BlueEyesView system on Windows10 64-bit operating system. The operation process is as follows:

Notice

- Before installation, please temporarily exit the system protection software such as 360 Total Security and Tencent PC Manager to prevent these software from blocking the normal installation of BlueEyesView; If you don't exit this kind of software, please choose to allow all the operations of the installer for the pop-up interception window during

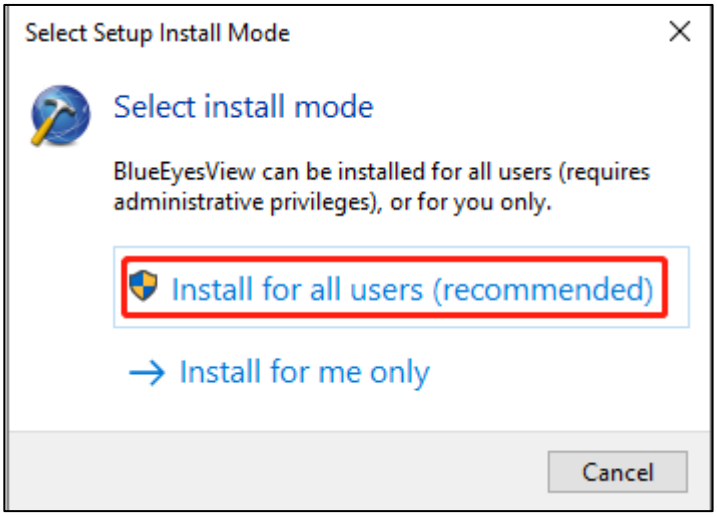
installation; Otherwise, the installation will probably fail and the program will not run normally.

- Before installation, in order to avoid wrong operation of notification message of Windows system, please temporarily adjust "Change User Account Control Settings" in "Control Panel > All Control Panel Items > User Accounts" to "Never Notify".
- When installing, please choose to run the installer as an administrator, otherwise it may cause abnormal installation. You can do this by right-clicking the installer and selecting “Run as Administrator”.

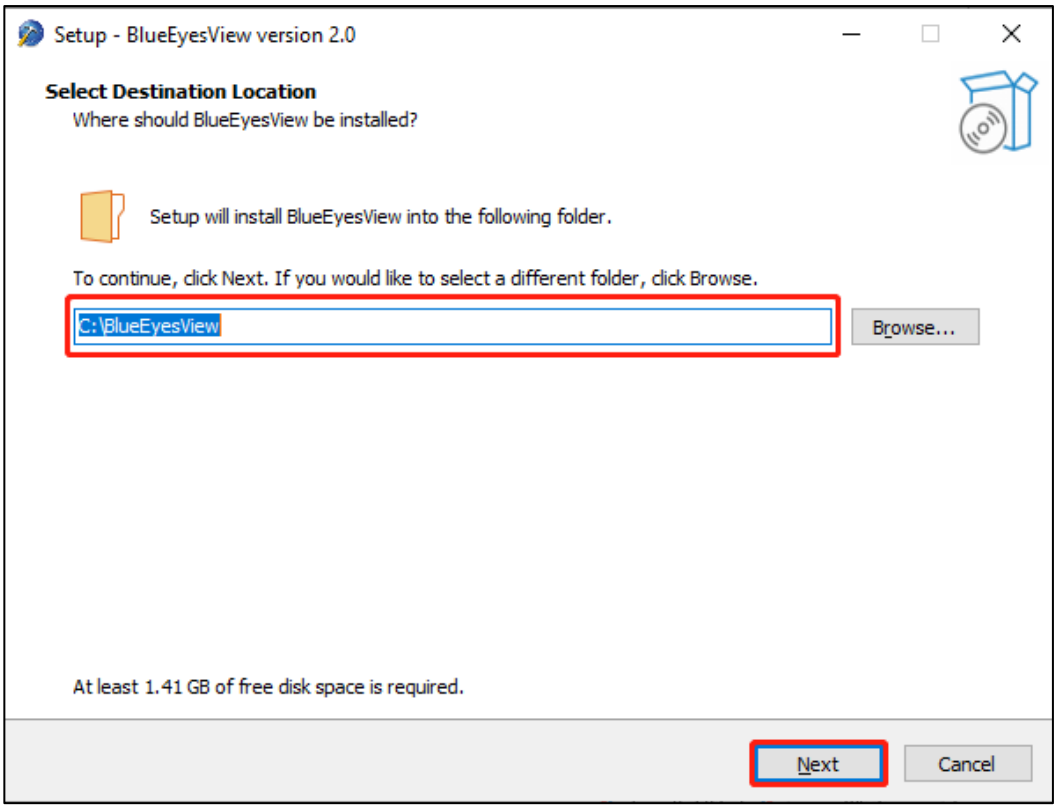
Operation Steps

Step 1 Right-click the installation file "BlueEyesViewInstall V2.1.exe" and select "Run as Administrator” to install the file.

Step 2 Click to select the installation mode "Install for all users (recommended)", as shown in the following figure. If you cannot obtain administrator rights, you can select "Install for me only".



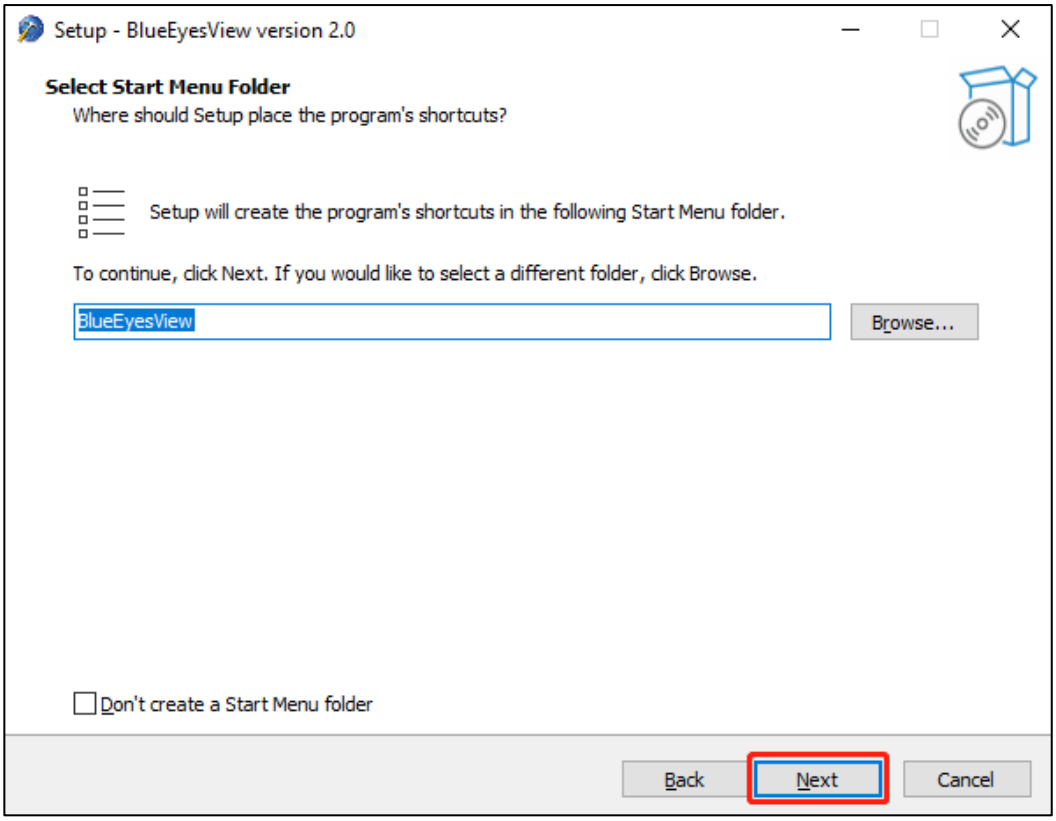
Step 3 Select the installation path of the program.



1 The default installation path is "C:\BlueEyesView", which can be modified manually or click "Browse" button to select another folder as the installation path.

2 Click "Next", as shown in the above figure.

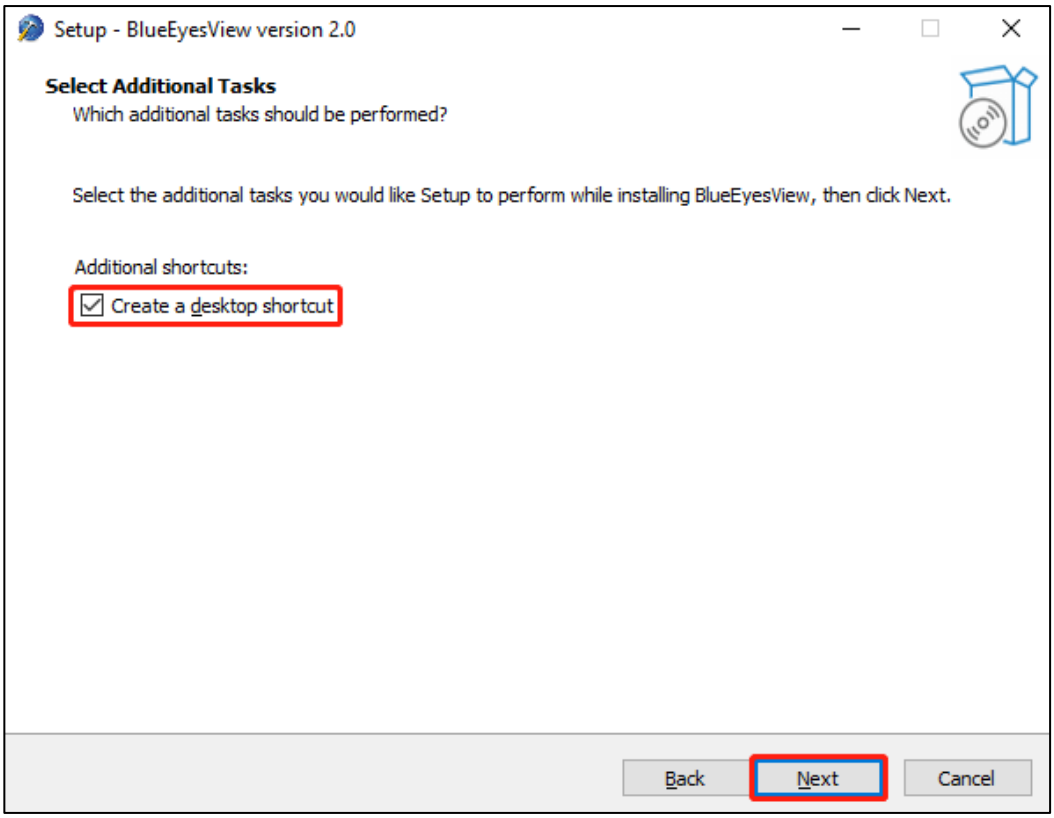
Step 4 Select the shortcut storage path of the program.



1 Shortcuts of programs are installed in the start menu folder of the system by default, and a new "BlueEyesView" folder is created. You can modify it manually or click “Browse” to select another folder, or check “Don’t create a Start Menu folder”.

2 Click "Next", as shown in the above figure.

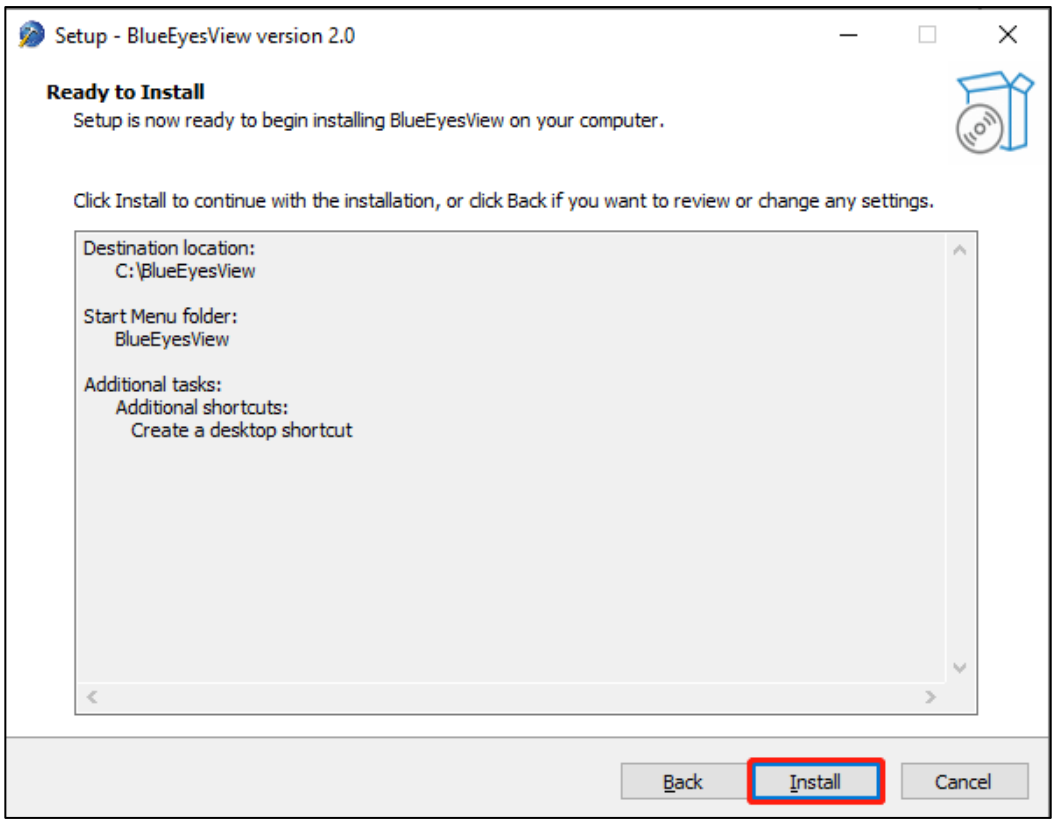
Step 5 Create a desktop shortcut.

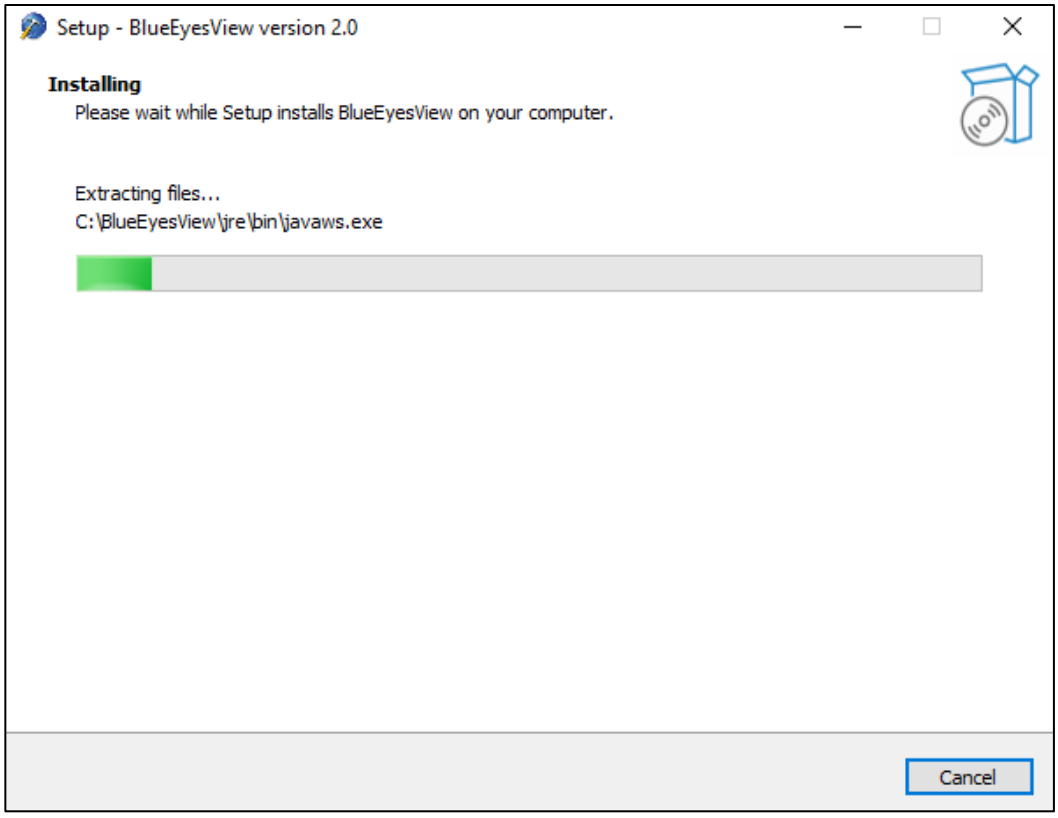


1 "Create a desktop shortcut" is unchecked by default and can be selected according to requirements;

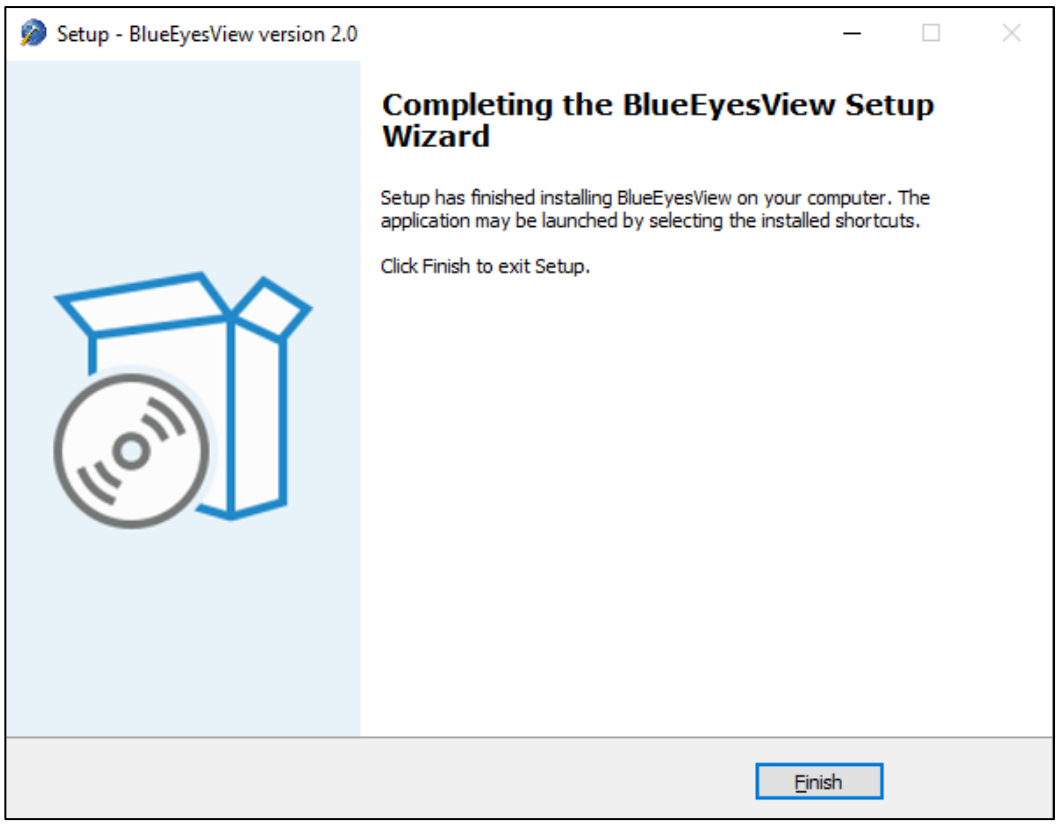
2 Click "Next", as shown in the above figure.

Step 6 Click the "Install" button to start the installation, as shown in the following figure. You can view the installation configuration information in the "Prepare for Installation" interface. If you need to modify the configuration, you can click "Back" to return to other configuration interfaces to modify the configuration information.





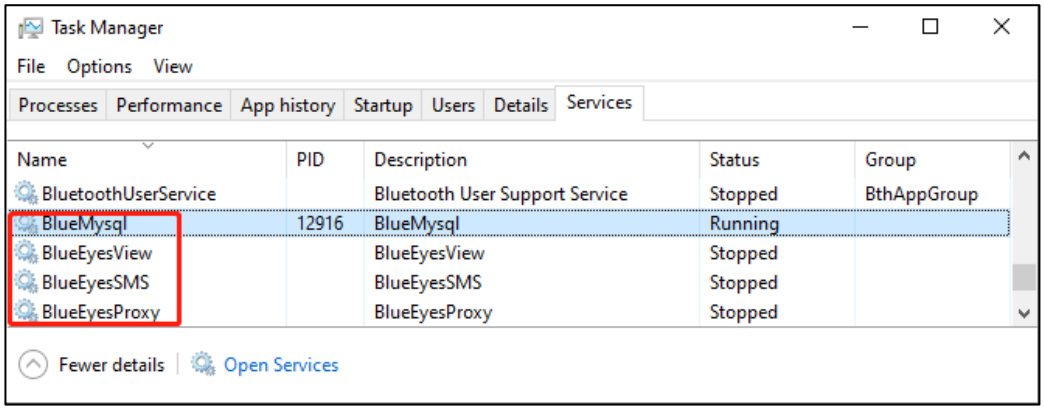
Step 7 After the installation is completed, click “Finish” to exit the installation wizard, as shown in the following figure.



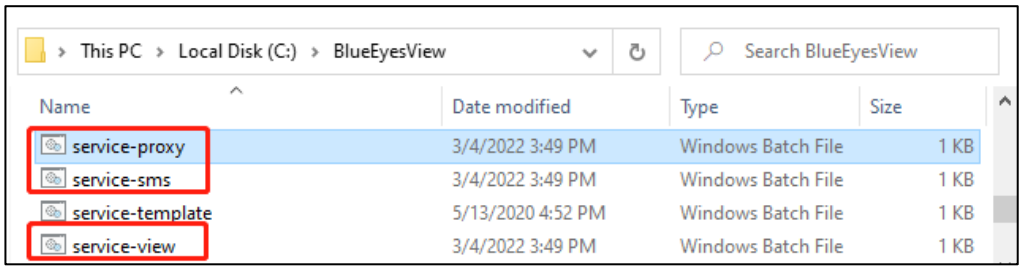
Step 8 End.

Notice

- After the system initialization is completed, right-click on the system taskbar, and then select “Task Manager” to enter the “Services” option to view the system services. As shown in the following figure, when the four types of services: "BlueEyesProxy", "BlueEyesSMS", "BlueEyesView" and "BlueMysql” appear, it indicates that the installation is complete.



- If "BlueEyesProxy", "BlueEyesSMS" or "BlueEyesView" services are found missing, you can right-click the corresponding bat file "Run as Administrator" under the installation path, as shown in the following figure. (Be sure to choose to run bat file as administrator).



2.4 System Initialization, Authorization, Startup and Upgrade

After the installation is completed, the following operations are required to ensure the operation of the system.

- System initialization: after the installation of BlueEyesView is completed, the system will be initialized for the first time.
- System authorization: after initialization, according to the temporary authorization file "licenseTemp.bin" generated in the default installation path "C:\BlueEyesView", obtain the authorization file from the customer service personnel to complete the system authorization.
- System startup: After the system is authorized, the system is started without initialization and authorization.
- (Optional) system upgrade: select when necessary.

Note
If you use the trial version of the system, you can visit the page of "System Management > System Security > Authorization Information", download the hardware information "licenseTemp.bin", upload the authorization file, and authorize the system through the webpage.

2.4.1 System Initialization

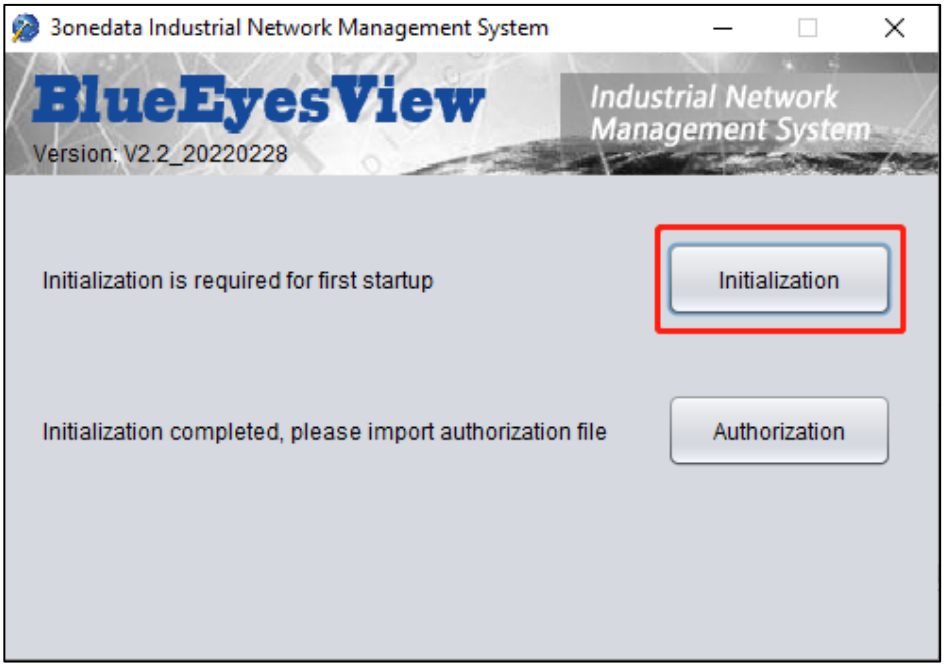
Operation Steps

Step 1 Double-click the “ 

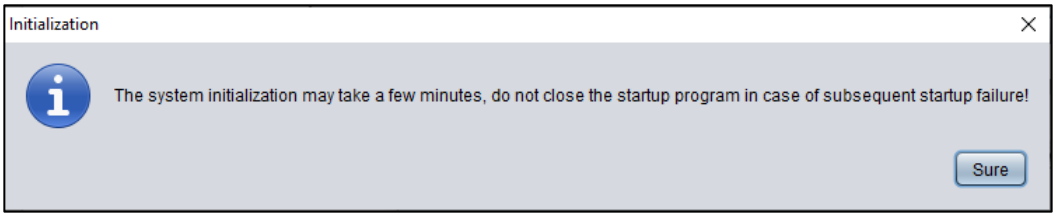
” icon to open the BlueEyesView system.

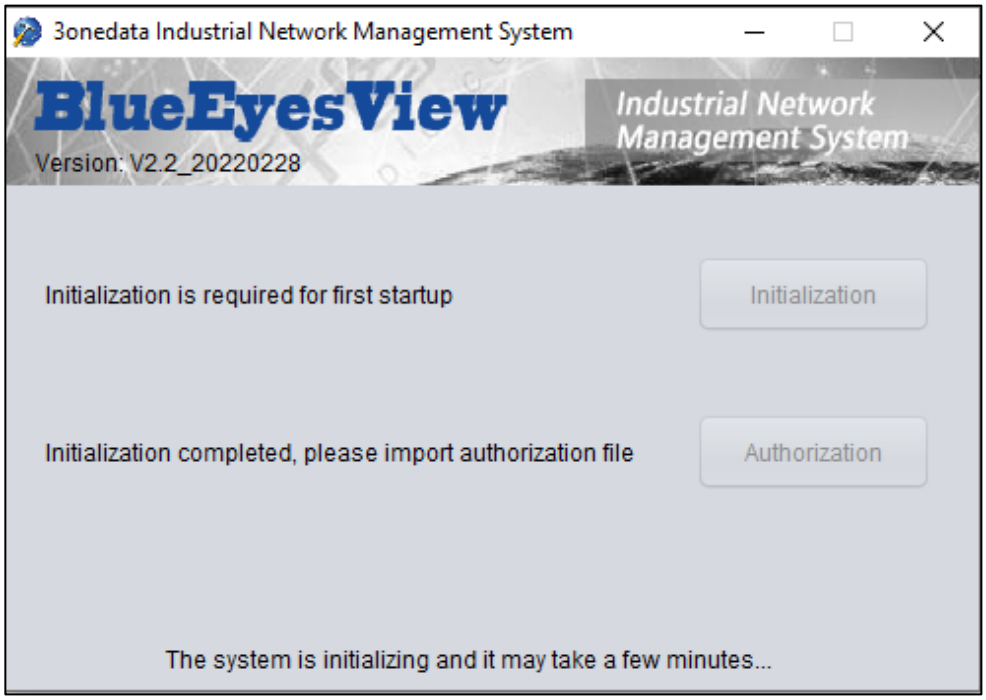
Step 2 In the pop-up dialog box of “3onedata Integrated Monitoring and Management System”,

click the “Initialization” button, as shown in the following figure.

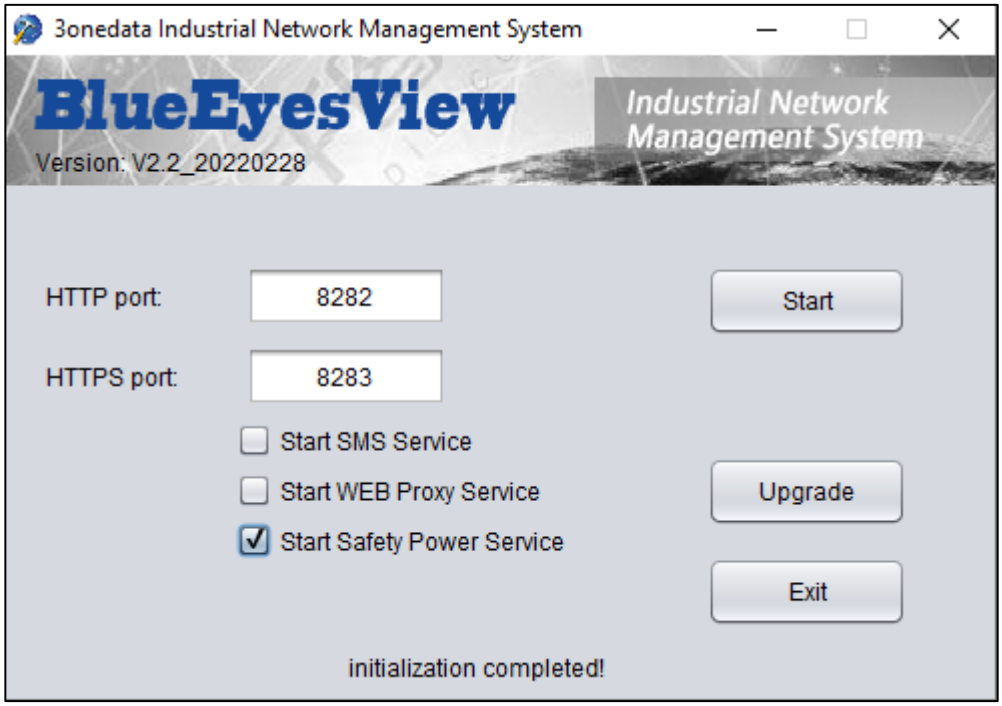


Step 3 In the pop-up “Initialization” Prompt window, click “Sure”. At the bottom of the "3onedata Integrated Monitoring and Management System" window, "The system is initializing and it may take a few minutes …" is displayed. As the picture below.

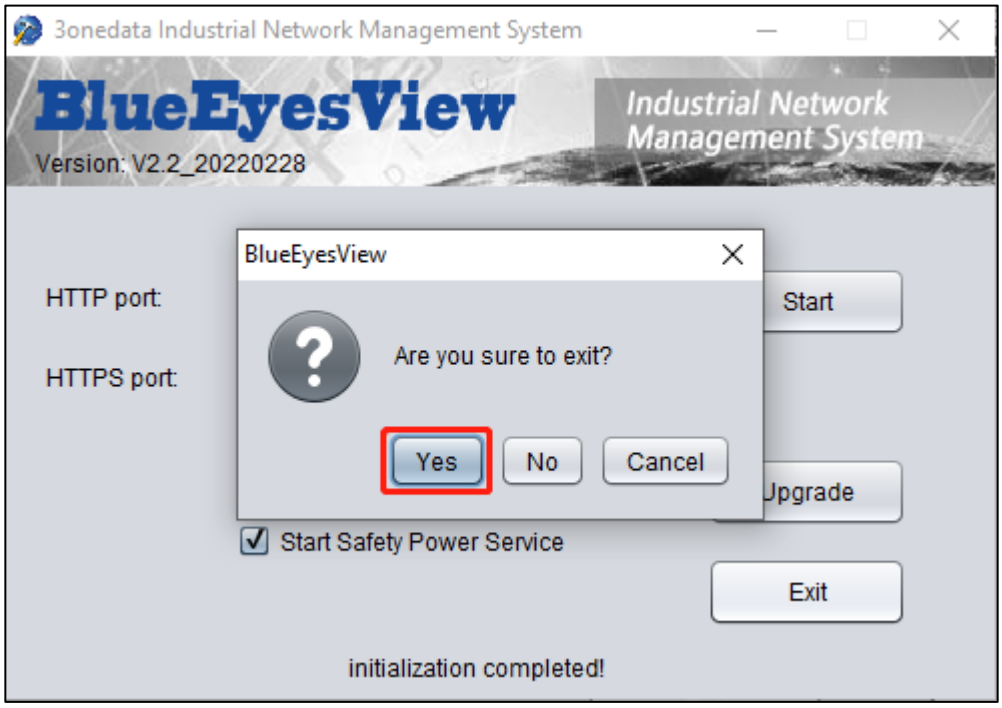




Step 4 When the window displays “initialization completed!”, click the "Exit" button, as shown in the following figure.



Step 5 In the pop-up "BlueEyesView" window, click the "Yes(Y)" button to exit the system.



Step 6 End.

After initialization is completed, authorization service operation can be performed. At the same time, the system will automatically generate a trial version of the authorization file, which by default supports the management of up to 50 network nodes and the use of the two-year validity period. After authorizing the service operation, the user can cancel the restrictions on the number of nodes and the validity period.

2.4.2 Authorization Service

The file "licenseTemp.bin" will be generated under the installation path after the system is initialized. Please send this file to the customer service staff for authorization. After receiving the "licenseTemp.bin" file, the customer service staff will provide the authorization file.

Notes

- After the initialization is completed, the authorization file will be detected before the system starts, and the authorization interface will be skipped when the current time is found to be within the validity period; Otherwise, authorization is required before entering the startup interface.
- To authorize service operation, you need to exit the running system and delete the original trial version authorization file; Then, enter the authorization interface and import the obtained official authorization file for authorization.

Authorization process is as follows:

Note

If you use the trial version of the system, you can visit the page of "System Management > System Security > Authorization Information", download the hardware information "licenseTemp.bin", upload the authorization file, and authorize the system through the webpage.

Operation Steps

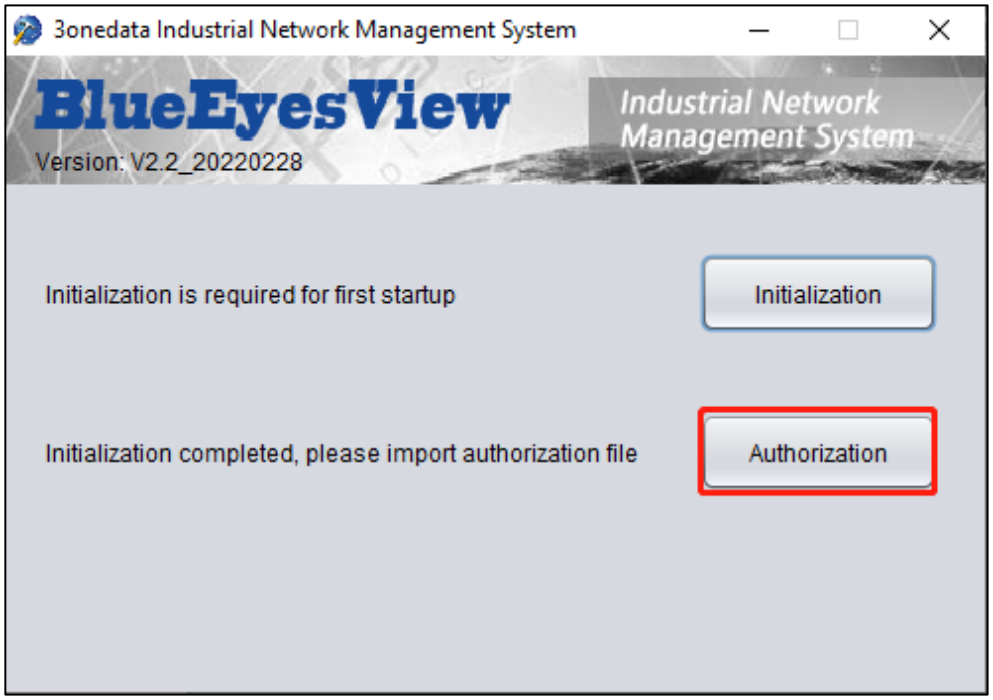
Step 1 Contact the customer service staff and provide the "licenseTemp.bin" file under the "BlueEyesView" folder of the installation path to obtain the authorization file "license.bin".

Step 2 Delete the trial license file "license.bin" under the installation path. The default installation path is "C:\BlueEyesView".

Step 3 After obtaining the authorization file, double-click the icon " 

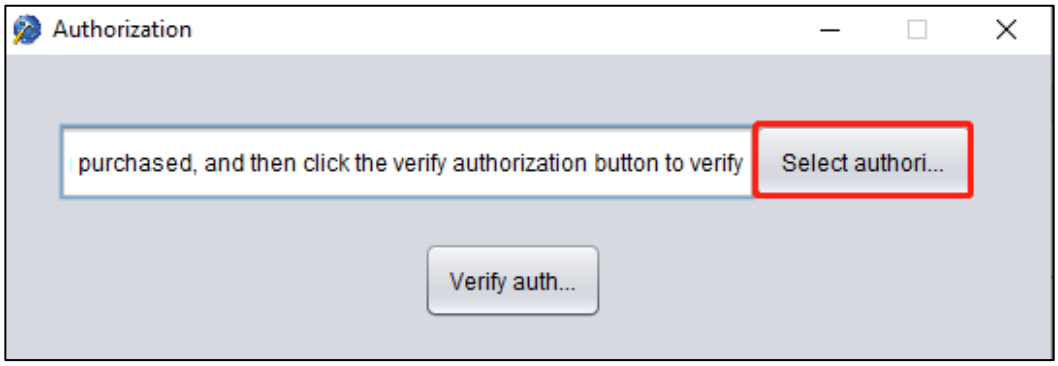
"to open the BlueEyesView system.

Step 4 Click the "Authorization" button, as shown in the following figure.

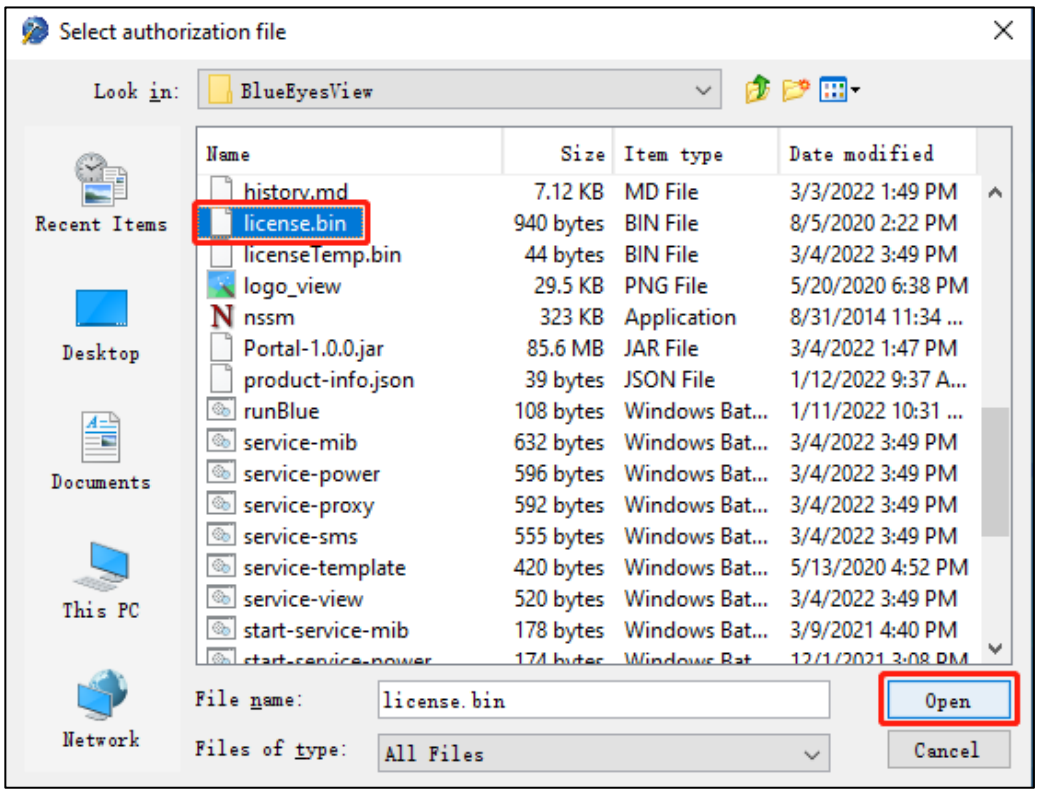


Step 5 Select the authorization file to authorize the system.

1 In the “Authorization” window, click the “Select Authorization File” button, as shown in the following figure.

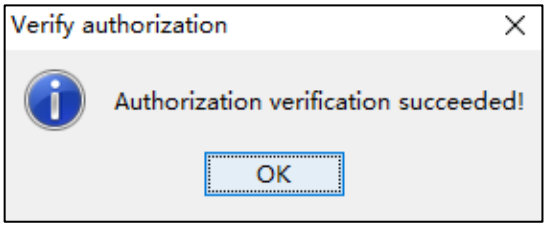


- In the pop-up "Select Authorization File" window, click to select the local authorization file "license.bin";
- Click the “Open” button, as shown in the following figure.



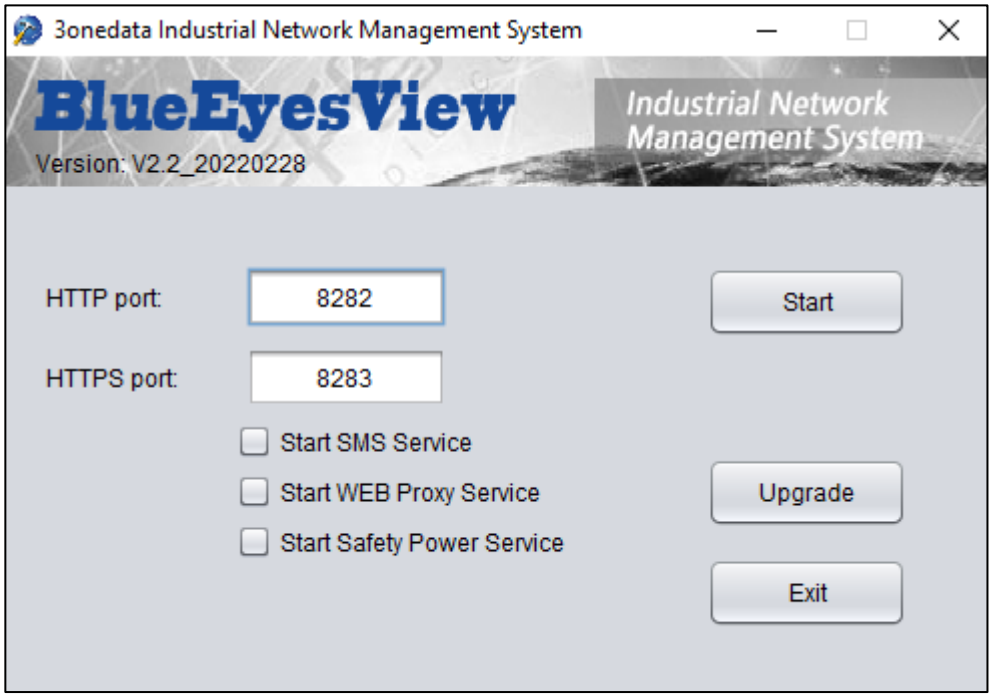
2 In the “Authorization” window, click the “Verify Authorization” button, as shown in the following figure.

- In the pop-up “Verify Authorization” window, click “OK”, as shown in the following figure.



Step 6 End.

After authorization is completed, enter the system startup interface, as shown in the following figure. Run the system again without initialization and authorization, and enter the startup interface directly.



After starting the system, you can log in to the WEB server and view the relevant information in “System Management > System Settings > Authorization Information”.

2.4.3 Start/Exit System

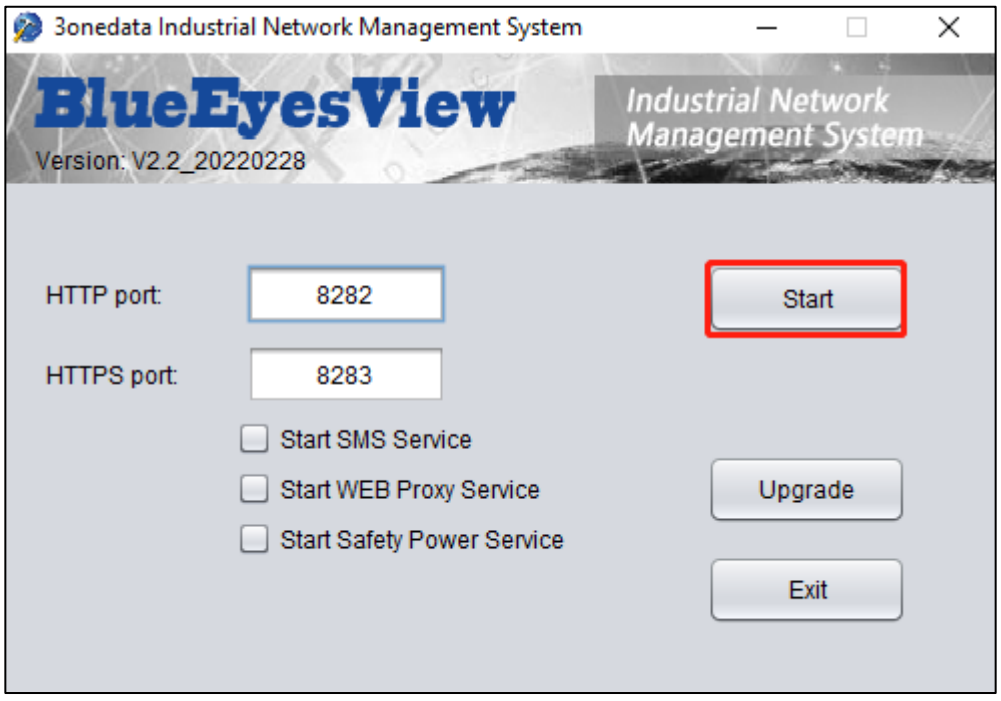
After completing the system initialization and authorization service, you can enter the system startup interface. Support the configuration of HTTP and HTTPS port number when starting the system. At the same time, you can choose to open SMS service and WEB proxy service. After the system is started, it will automatically access the local WEB server through the default browser using HTTPS protocol and enter the integrated monitoring and management system. Clients on the same network segment as the WEB server can access the WEB server through a browser using HTTP or HTTPS protocol according to specific addresses and ports, and enter the integrated monitoring and management system. When the host installing the system is in different network segments using dual network cards, the system can start the WEB proxy server, so that the client of one network segment can directly access the WEB interface of the device under the other network segment.

Start System

Step 1 Double-click the " 

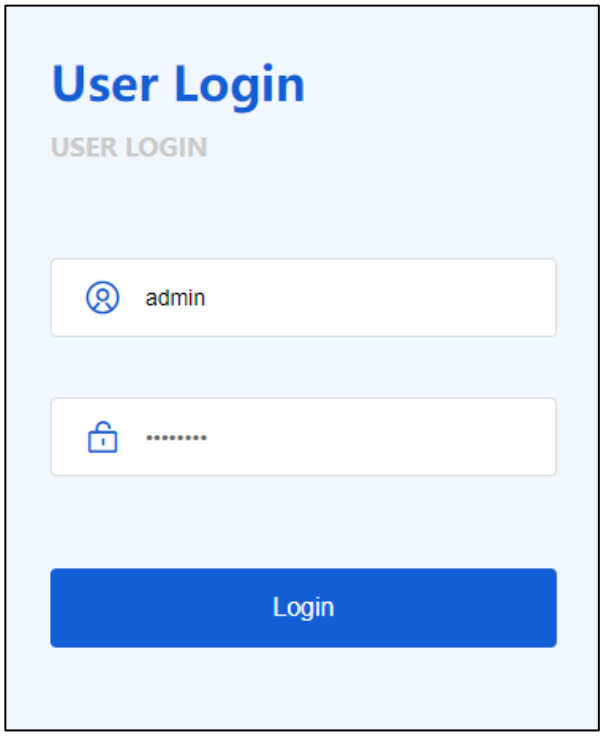
"icon to open the BlueEyesView system.

Step 2 In the "3onedata Industrial Network Management System" window, click the "Start" button. "HTTP port" defaults to 8282 and "HTTPS port" defaults to 8283, which is recommended to remain unchanged, as shown in the following figure.



Step 3 In the pop-up browser login window, enter the user name and password. The default

user name is "admin" and the password is "admin123".



Note:

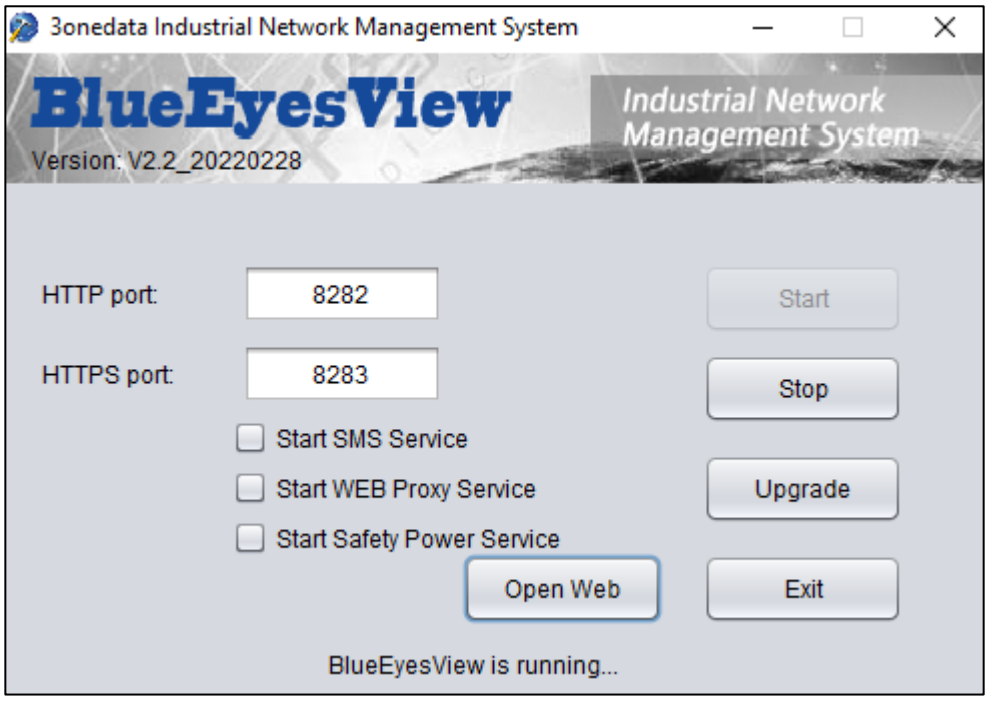
- After starting the system, access the BlueEyesView system through the default system browser by default; To switch to other browsers, enter the local IP and HTTP/HTTPS service port in the address bar, such as "http://127.0.0.1:8282/" or "https://127.0.0.1:8283/".
- 127.0.0.1 is the loopback address of this host. When accessing through the browser of the remote client, it needs to be modified to be the IP address bound by the system and be in the same LAN as the system.
- 8282/8283 is the default service port number, which can be modified when the port number conflicts; At this time, the access address needs to be modified synchronously.

Step 4 Click the “login” button.

Step 5 End.

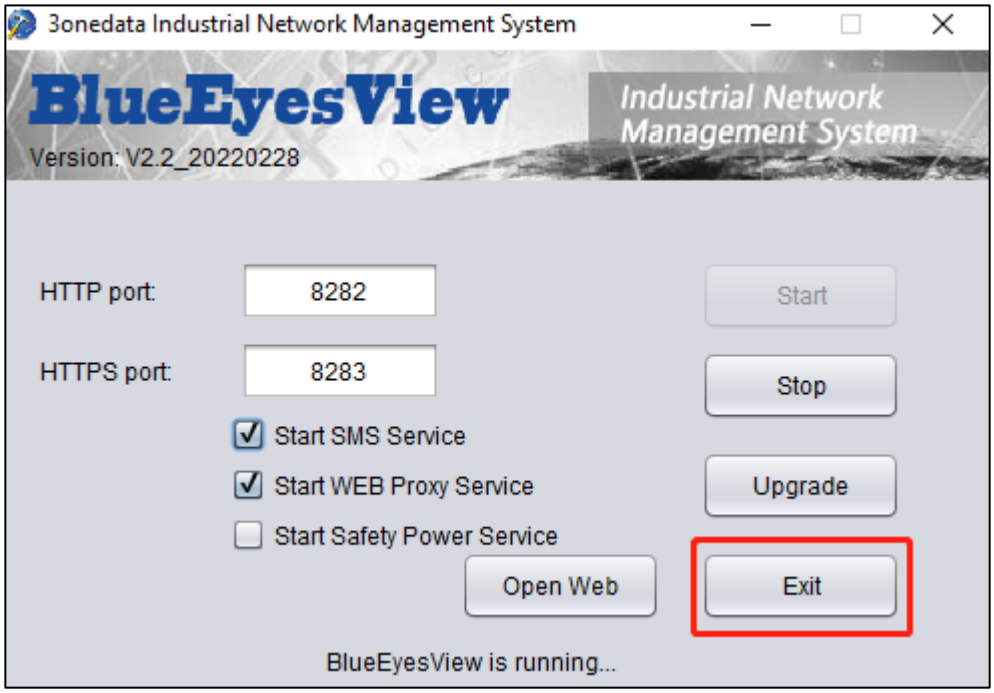
Notice

When the system is running, keep the "3onedata Integrated Monitoring and Management System" window open, as shown in the following figure. If you close or exit this window, the system will also close and stop running.



Exit System

In the "3onedata Industrial Network Management System" window, click the "Exit" button or close the window directly to exit the system, as shown in the following figure.



Note
Closing the client browser web page does not affect the BlueEyesView service.

2.4.4 System Upgrade

Before upgrading the system, please obtain an upgrade package such as "update.zip" from the customer service staff.

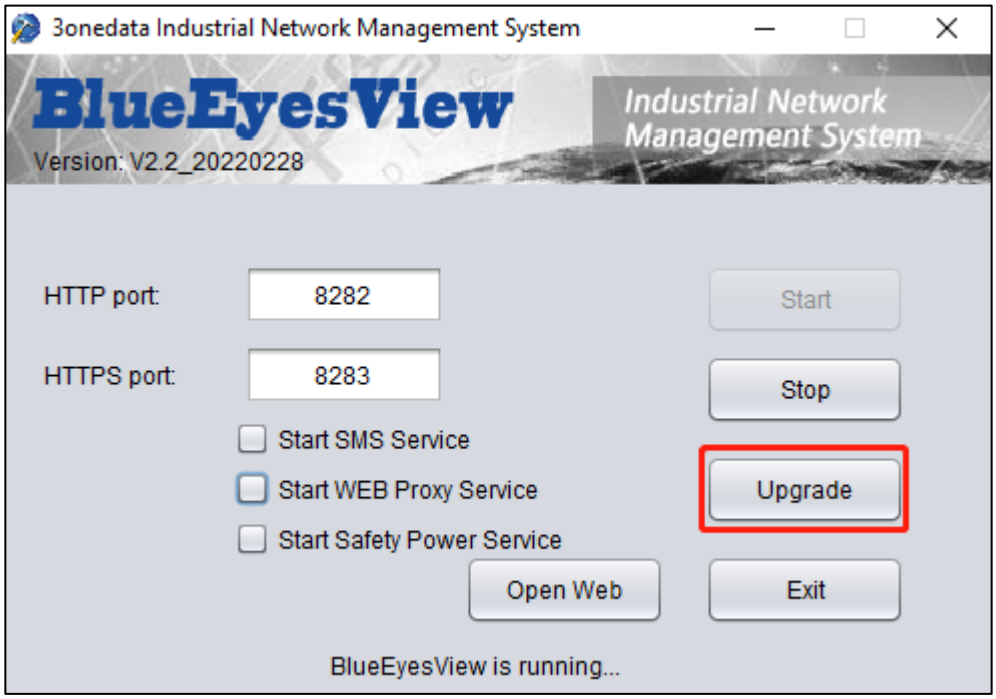
Note
Before upgrading the system, you need to exit the system.

Operation Steps

Step 1 Double-click the " 

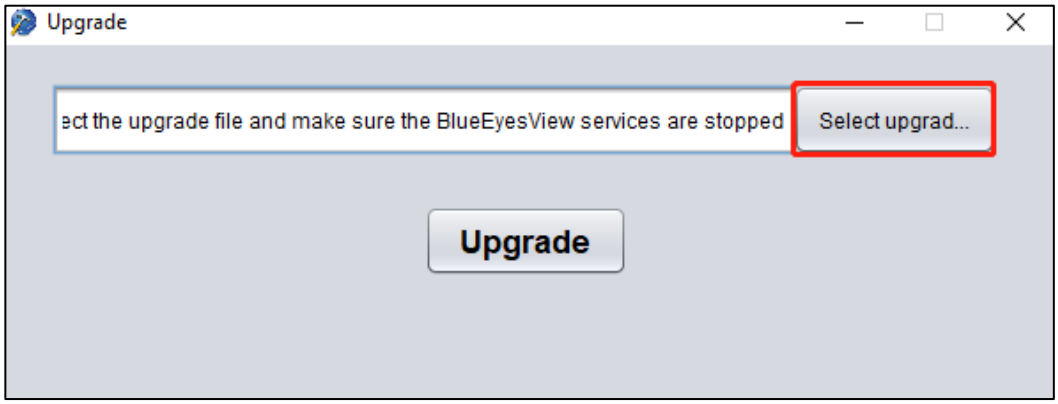
" icon to open the BlueEyesView system.

Step 2 In the "3onedata Industrial Network Management System" window, click the "Upgrade" button, as shown in the following figure.

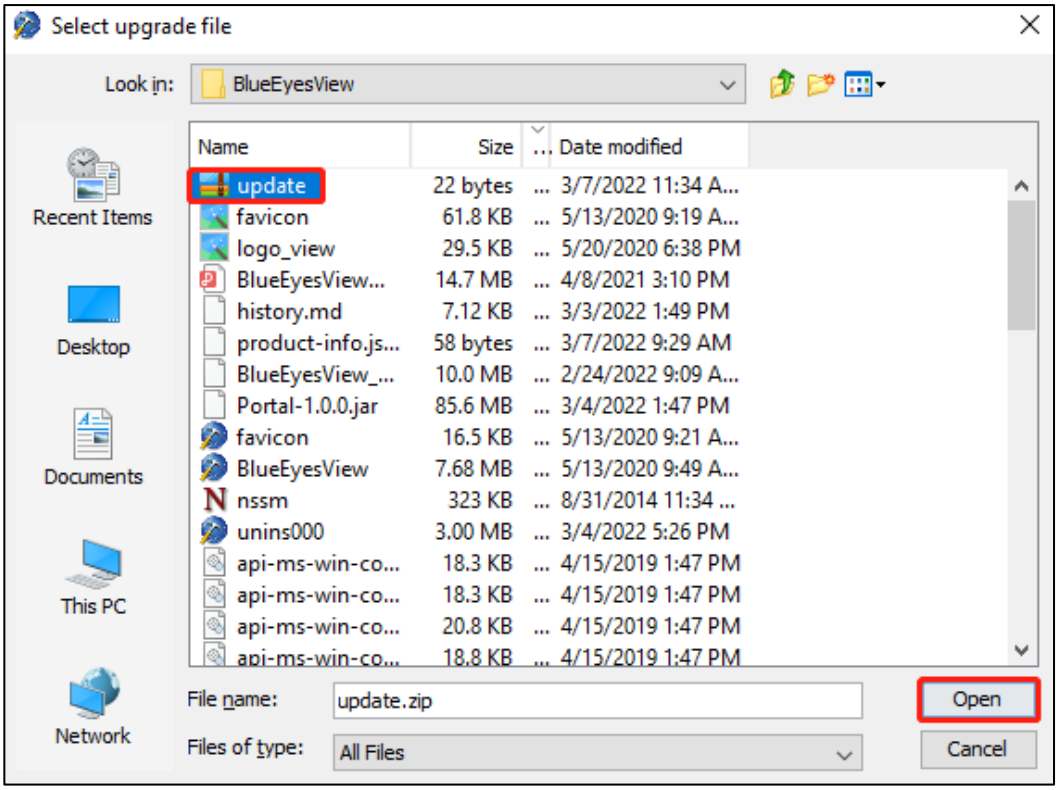


Step 3 Select the upgrade file to upgrade the system.

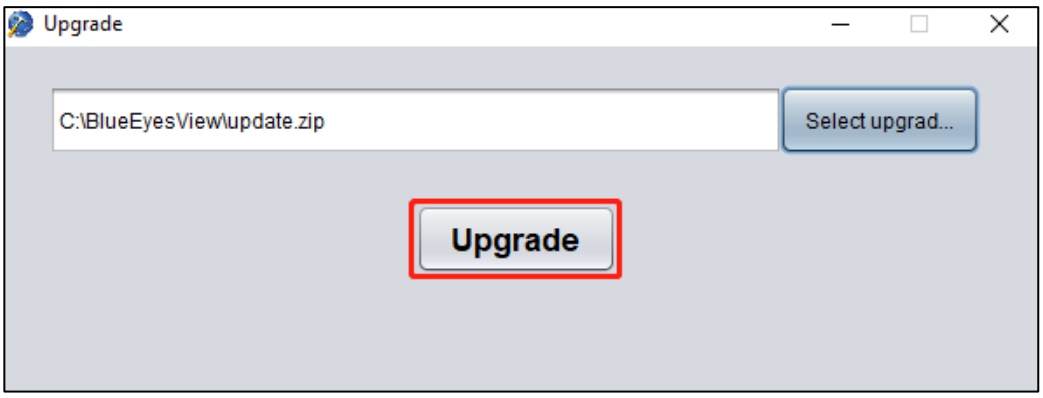
1 In the “Upgrade” window, click the “Select Upgrade File” button, as shown in the following figure;



- In the pop-up "Select Upgrade File" window, click to select the upgrade file stored locally;
- Click the “Open” button, as shown in the following figure.



2 In the “Upgrade” window, click the “Upgrade” button, as shown in the following figure;



Step 4 End.

2.5 Uninstall System

After uninstalling the system, all local configuration information and log records will be deleted.

Notice

- Before uninstalling, you need to exit the running system. You can check the running status of "BlueEyesProxy", "BlueEyesSMS", "BlueEyesView" and "BlueMysql" services under "Services" in Task Manager, or stop running services.
- Uninstall the BlueEyesView V1 version system by using the “uninstall.bat” uninstall wizard under the installation path, and right-click "Run as Administrator" when uninstalling.
- Uninstall the BlueEyesView V2 version system, which can be uninstalled by the shortcut "Uninstall BlueEyesView" in the start menu bar.
- If uninstallation fails, you can find "Command Prompt" in the start menu bar, and right-click to select "Run as Administrator". On the "Administrator: command prompt" interface, enter and execute the commands “sc delete BlueEyesProxy”, “sc delete BlueEyesSMS”, “sc delete BlueEyesView” and “sc delete BlueMysql” to delete the service from the registry, and then delete the files and folders under the installation path to complete the uninstallation.

Operation Steps

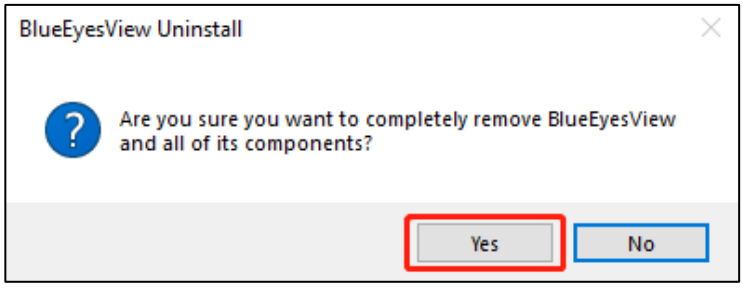
Step 1 Enter the installed "BlueEyesView" folder, and the default installation path is "C:\BlueEyesView". Please enter the "BlueEyesView" folder according to the actual installation path.

Step 2 Right-click the “uninstall.bat” uninstall wizard and select “Run as Administrator”.

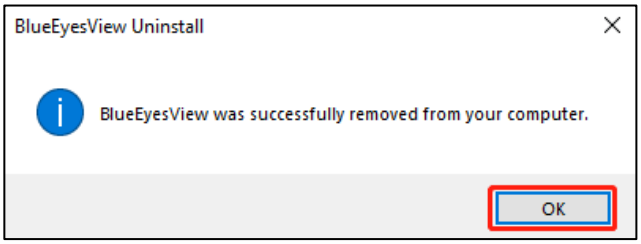
Note:

If you do not run the uninstaller as an administrator, it may result in incomplete uninstallation of the program.

Step 3 In the pop-up “BlueEyesView Uninstall” dialog box, click “Yes” to start uninstalling, as shown in the following figure.



Step 4 Click "OK" button, and the uninstallation is completed, as shown in the following figure.



Step 5 End.

3 Install BlueEyesView on Linux

This chapter provides the process of installing BlueEyesView integrated monitoring and management system in Linux system. The installation procedure is applicable to CentOS7/6, RHEL7/6 and Fedora28/29/30 systems. If install BlueEyesView under other Linux versions, this installation process can be used as a reference.

Notes

- In this chapter, CentOS7 physical machine is used as Linux operating system for system installation and configuration.
- BlueEyesView provides different installation packages for Linux system and Windows system. Please ensure to obtain the installation package matching the operating system.

3.1 Linux System Requirement

3.1.1 Hardware Requirement

Hardware requirements of Linux operating system:

Hardware	System Requirements
CPU	Single 4-core 2GHz and above, Core i5/i7/i9 series or XEON series is recommended.
Memory	8GB and above, 16GB is recommended.
Disc	1TB hard disk, redundant configuration and backup disk are recommended.
Monitor	1980x1080 and above resolution is recommended. Note: Below this resolution will affect the page layout.

Note

In the production environment, it is recommended that the application server and database server be deployed separately.

3.1.2 Software Requirement

Server

Server software requirements of Linux operating system:

Software	System Requirements
Operating system	Linux series 64-bit operating system
JVM	Oracle JDK 8/Open JDK 8 and above
Database	MySQL Community Server 8

Note

- The database used by BlueEyesView is MySQL, and its version is compatible with 5.7~8.x. The installed database in this manual is MySQL Community 8.0.
- The installation methods of MySQL and Oracle JDK 8/Open JDK 8 are described in the subsequent sections of this chapter. If installed, please ignore the installation process.

Client

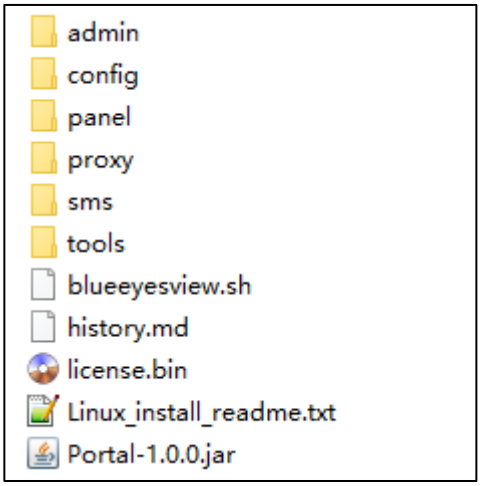
Client software requirements of Linux operating system:

Software	System Requirements
Browser	In browsers like Chrome, Firefox, Edge, IE10 and above, Chrome browser is recommended.

3.2 Installation and Deployment

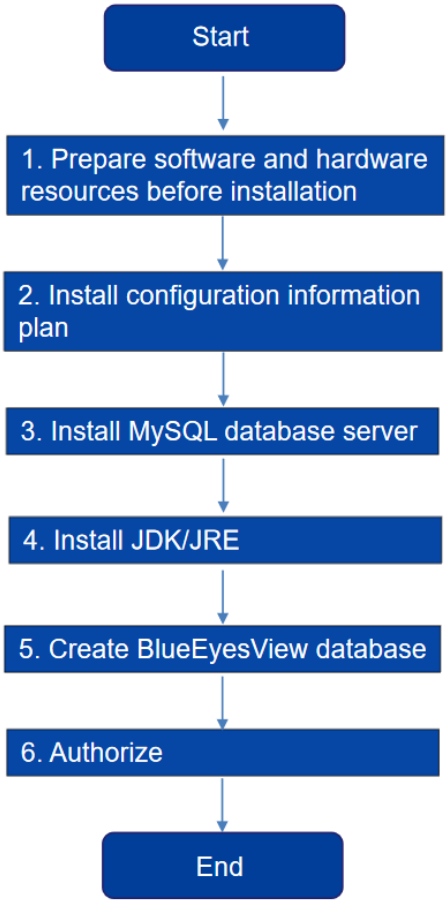
Obtain Installation Package

Before installation, please contact the business personnel to obtain the BlueEyesView installation package of Linux system. This chapter mainly introduces the operation process of installing integrated monitoring and management system under Linux system. The Linux system installation composition files of BlueEyesView are as follows.



Installation Process

The installation process is as follows:



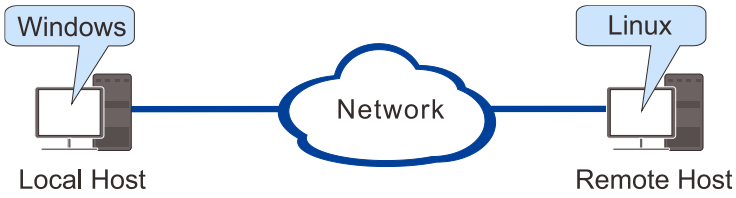
The installation process is described as follows:

Installation Process	Note
1. Prepare software and hardware resources before	Before installation, the system installation program, Linux operating system, hardware devices and

Installation Process	Note
installation	network environment should be prepared in advance.
2. Install configuration information plan	It is recommended to plan the installation path and database account number in advance before installation. If it is inconsistent with the default configuration, it needs to be modified synchronously in relevant configuration files.
3. Install MySQL database server	MySQL is a free and safe relational database management system, which supports multiple development systems and languages. The BlueEyesView business database is created on the basis of MySQL.
4. Install JDK/JRE	BlueEyesView system depends on JRE/JDK, JRE is Java runtime environment, JDK is Java development kit, both of which support the operation of the system.
5. Create BlueEyesView database	Creating the BlueEyesView database requires the assistance of database tools.

Network Environment

The integrated monitoring and management system can be installed locally on Linux system or through remote control. This manual introduces Windows system to remotely control Linux system to complete installation. The network topology is shown in the following figure.



Notice

- Before making remote configuration, make sure that the route between the computers is reachable.
- Before making a local configuration, make sure that the computers are on the same subnet.

On the Windows operating system of Local Host, a free third-party MobaXterm_Personal or application program with similar function should be installed

in advance to assist in the installation of the system. MobaXterm_Personal is an installation-free desktop remote terminal management software, which is suitable for Windows system to access Linux server, and can manually upload Windows local files to Linux system directory.

On the Linux operating system of Remote Host, SSH service should be started in advance to establish remote secure encrypted connection. The Linux system uses Centos7 as a configuration example, and SSH is enabled by default. Linux system needs to access the Internet normally to obtain installation resources.

Note

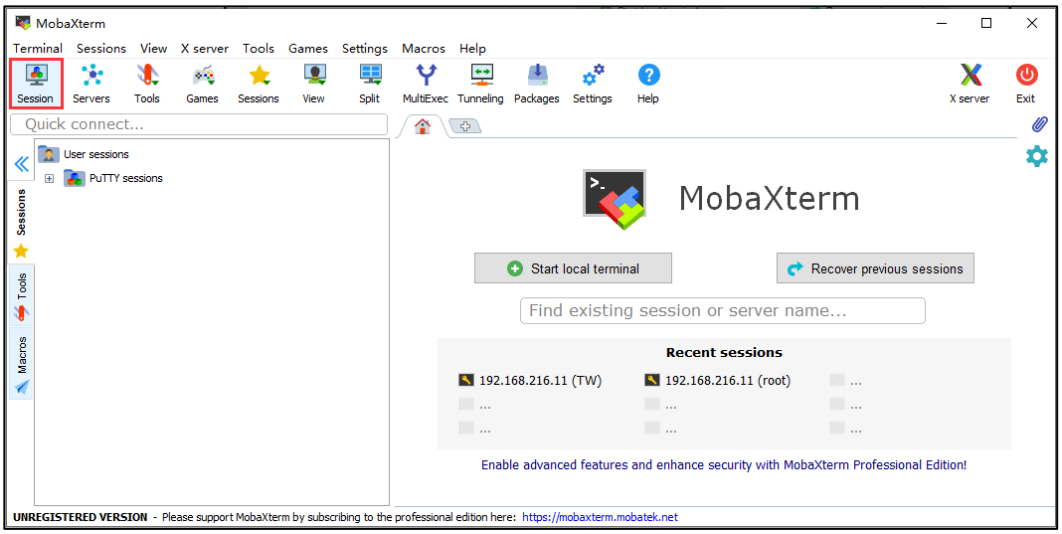
Linux system generally supports SSH server function, which is enabled by default. If SSH function is disabled, please re-enable. You can enable SSH service through the command "service sshd start" at the local terminal.

3.3 Enter the Linux Terminal Interface

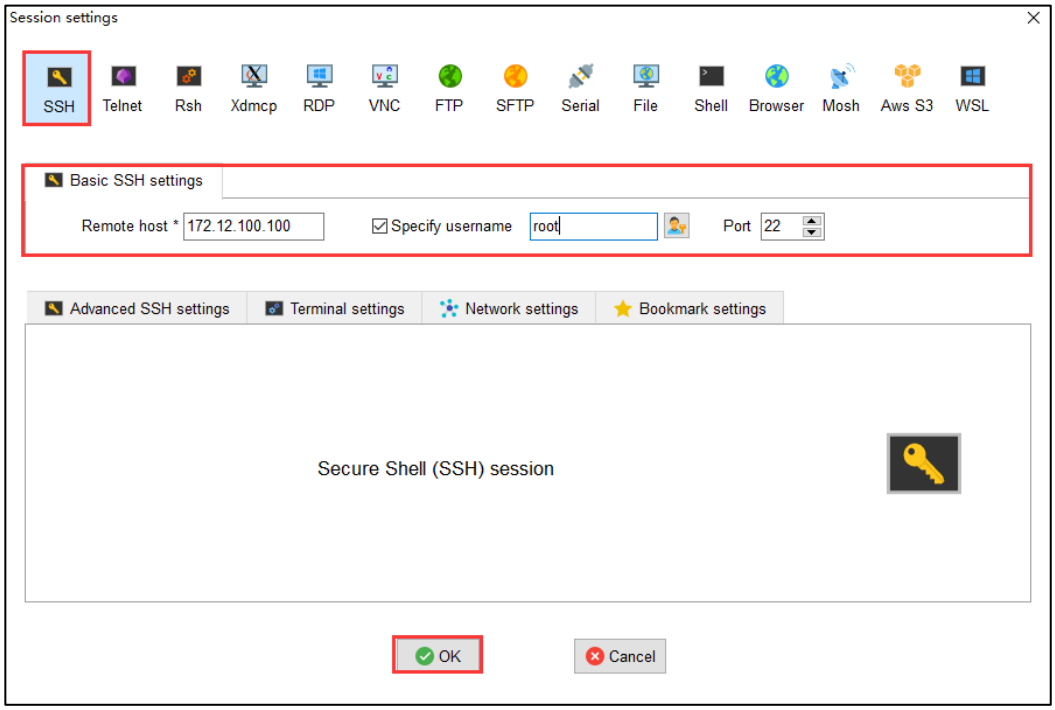
Windows system uses application MobaXterm to create remote connection with Linux system. And upload the system installation package to Linux system.

Step 1 Open “MobaXterm” program.

Step 2 Click the "Session" icon to create a remote session, as shown in the following figure.



Step 3 In the “Session settings” window, create an SSH session, as shown in the following figure:



1 Click the “SSH” icon;

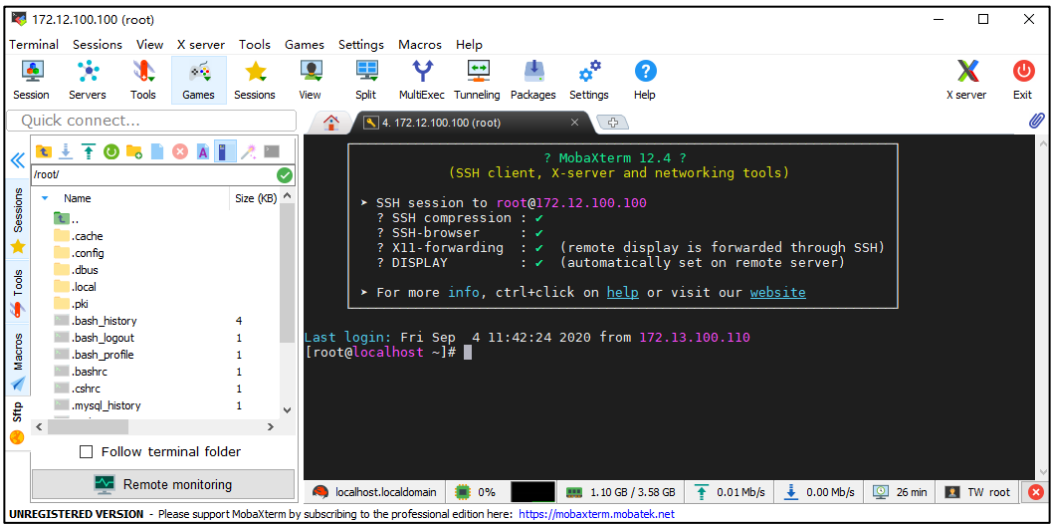
2 Enter the IP address or name of the remote Linux host in the "Remote host" text box;

3 Check the check box before "Specify username" and enter the name of the user who logs in to Linux system;

Note:
The user name for logging in to Linux system can be a user name with different permissions.

4 Enter the specified Port number in the "port" text box. If the server is not modified, it is the default port 22 of the protocol;

5 Click the "OK" button, as shown in the following figure, to successfully establish a remote connection and enter the Linux terminal interface.



Step 4 End.

3.4 Firewall Configuration of Linux System

To ensure the security of the server, it is recommended to open the firewall of the server. If the firewall is not enabled, skip this section; If the firewall is enabled, please open the following ports:

- 3306: port for MySQL database.
- 8282/8283: application server WEB service HTTP/HTTPS port.
- 8285: port for Mib Browser tool to use HTTPS port.
- 162: port for SNMP protocol to receive Trap messages.
- 65534: UDP listening port of management system.

Note

- Independent database server, only need to open Port 3306.
- Independent application servers, need to open Port 8282, 8283, 8285, 162 and 65534.
- All the above ports will be opened when the single machine is deployed integrally.

3.4.1 Enable Firewall

Check the firewall status by entering the following command:

```
firewall-cmd --state
```

If "running" is returned, the firewall is enabled.

If the firewall is not enabled, you can open the firewall with the following command:

```
systemctl enable firewalld
systemctl start firewalld
systemctl status firewalld
```

3.4.2 Open Port

After enabling the firewall, open the designated ports according to the installation environment and requirements.

Open database Port 3306 with the following command:

```
sudo firewall-cmd --zone=public --add-port=3306/tcp --
permanent
```

Open HTTP Port 8282 of WEB service, the command is as follows:

```
sudo firewall-cmd --zone=public --add-port=8282/tcp --
permanent
```

Open HTTPS Port 8283 of WEB service, the command is as follows:

```
sudo firewall-cmd --zone=public --add-port=8283/tcp --
permanent
```

Open HTTPS Port 8285 of Mib Browser service, the command is as follows:

```
sudo firewall-cmd --zone=public --add-port=8285/tcp --
permanent
```

Open Port 162 of SNMP Trap, the command is as follows:

```
sudo firewall-cmd --zone=public --add-port=162/udp --permanent
```

Open Port 65534 of system listening, the command is as follows:

```
sudo firewall-cmd --zone=public --add-port=65534/udp --
permanent
```

After opening the port, you need to reload the configuration. The command is as follows:

```
sudo firewall-cmd --reload
```

After the configuration is completed, you can view the configuration of the opened port. The command is as follows:

```
firewall-cmd --list-all
```

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# firewall-cmd --state
running
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=3306/tcp --permanent
success
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=8282/tcp --permanent
success
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=8283/tcp --permanent
success
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=162/udp --permanent
success
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=65534/udp --permanent
success
[root@localhost ~]# sudo firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp2s0
  sources:
  services: dhcpv6-client ssh
  ports: 3306/tcp 8282/tcp 8283/tcp  162/udp 65534/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

3.5 Install MySQL Database Server

BlueEyesView database is compatible with MySQL version 5.7~8.x This section provides the installation method of MySQL Community 8.0 under CentOS/RHEL7, 6 and Fedora 28, 29 and 30.


Note
MySQL Community 8.0 is a free version. If you have purchased MySQL Enterprise Edition, you can contact Oracle service personnel to help install it, or you can install it by yourself according to official guidelines.

3.5.1 Prepare Yum Library

If you use CentOS/RHEL 7 system to obtain and install database files, the command is as follows:

```
rpm -Uvh https://repo.mysql.com/mysql80-community-release-el7-3.noarch.rpm
```

If you use CentOS/RHEL 6 system to obtain and install database files, the command is as follows:

```
rpm -Uvh https://repo.mysql.com/mysql80-community-release-el6-3.noarch.rpm
```

If you use Fedora 30 system to obtain and install database files, the command is as follows:

```
rpm -Uvh https://repo.mysql.com/mysql80-community-release-fc30-1.noarch.rpm
```

If you use Fedora 29 system to obtain and install database files, the command is as follows:

```
rpm -Uvh https://repo.mysql.com/mysql80-community-release-fc29-2.noarch.rpm
```

If you use Fedora 28 system to obtain and install database files, the command is as follows:

```
rpm -Uvh https://repo.mysql.com/mysql80-community-release-fc28-2.noarch.rpm
```


Note
If you are prompted with "error: package: akonadi-MySQL-1.9.2-4.el7.x86 _ 64 (@ anaconda)", you can use the command yum -y remove mariadb-libs, and then obtain and install the database file again.

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# rpm -Uvh https://repo.mysql.com/mysql80-community-release-el7-3.noarch.rpm
…
# # The dependency processing procedure is omitted here # #
…
Transaction summary
================================================================
Install 1 package (+3 dependent packages)
Total download volume: 472 M
Installation size: 2.1 G
Is this ok [y/d/N]: y
…
# # Download process is omitted here # #
…
Fingerprint: a4a9 4068 76fc bd3c 4567 70c8 8c71 8d3b 5072 e1f5
Package: mysql80-community-release-el7-3.noarch (installed)
From:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Do you want to continue? [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing: mysql-community-common-8.0.18-1.el7.x86_64     1/4
Installing: mysql-community-libs-8.0.18-1.el7.x86_64       2/4
Installing: mysql-community-client-8.0.18-1.el7.x86_64     3/4
Installing: mysql-community-server-8.0.18-1.el7.x86_64     4/4
Authenticating: mysql-community-client-8.0.18-1.el7.x86_64
1/4
Authenticating: mysql-community-common-8.0.18-1.el7.x86_64
2/4
Authenticating: mysql-community-libs-8.0.18-1.el7.x86_64
3/4
Authenticating: mysql-community-server-8.0.18-1.el7.x86_64
4/4

Installed:
  mysql-community-server.x86_64 0:8.0.18-1.el7

Installed as dependence:
  mysql-community-client.x86_64 0:8.0.18-1.el7
```

```
  mysql-community-common.x86_64 0:8.0.18-1.el7
  mysql-community-libs.x86_64 0:8.0.18-1.el7

Finished!
```

3.5.2 Install MySQL Community Server

Disable all repositories in the MySQL repo file with the following command:

sed -i 's/enabled=1/enabled=0/' /etc/yum.repos.d/mysql-community.repo

If CentOS/RHEL system is used, install the database file MySQL Community Server with the following command:

yum --enablerepo=mysql80-community install mysql-community-server

If Fedora system is used, install the database file MySQL Community Server with the following command:

dnf --enablerepo=mysql80-community install mysql-community-server

3.5.3 Enable MySQL Service

If you use the SysVinit command, the command is as follows:

service mysqld start

If you use the Systemd command, the command is as follows:

systemctl start mysqld.service

3.5.4 Change the Default root Password

Get the temporary password of MySQL database root with the following command:

grep "A temporary password" /var/log/mysqld.log

According to the above command, the system will feedback a temporary password, as shown below. "o/rhs3#%amhL" after "root@localhost:" is the temporary password of root.

```
A temporary password is generated for root@localhost:
o/rhs3#%amhL
```

Notice

MySQL8 requires that the password must contain capital and small letter and special characters and numbers. Please record the new password you set to avoid forgetting!

Run MySQL security configuration wizard with the following command:

```
mysql_secure_installation
```

Change the password as follows:

```
Enter password for user root:            #Enter temporary
password#
The existing password for the user account root has expired.
Please set a new password.
New password:                            #Enter new password#
Re-enter new password:                   #Enter the new
password again#
Change the password for root ? ((Press y|Y for Yes, any other
key for No): n
Remove anonymous users? (Press y|Y for Yes, any other key for
No) : y                                    #Enter y#
Disallow root login remotely? (Press y|Y for Yes, any other
key for No) : y                          #Enter y#
Remove test database and access to it? (Press y|Y for Yes, any
other key for No) : y                      #Enter y#
Reload privilege tables now? (Press y|Y for Yes, any other key
for No) : y                              #Enter y#
```

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# grep "A temporary password"
/var/log/mysqld.log
2019-12-18T07:21:30.652808Z 5 [Note] [MY-010454] [Server] A
temporary password is generated for root@localhost:
Iv+P;2rBKsk7

[root@localhost ~]# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:
The existing password for the user account root has expired.
Please set a new password.
New password:
```

```
Re-enter new password:
The &apos;validate_password&apos; component is installed on
the server.
The subsequent steps will run with the existing configuration
of the component.
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other
key for No) : n

Do you wish to continue with the password provided?(Press y|Y
for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for
No) : y
Success.


Normally, root should only be allowed to connect from
&apos;localhost&apos;. This ensures that someone cannot guess
at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other
key for No) : y
Success.

By default, MySQL comes with a database named &apos;test&apos;
that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any
other key for No) : y
```

```
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key
for No) : y
Success.
```

3.5.5 Modify the Default Setting of sql-mode

Search for my.cnf file, the command is as follows

whereis my.cnf

Back to the path "my: /etc/my.cnf ",enter the file VIM mode, and the command is as follows:

vim /etc/my.cnf

Back to my.cnf file as follows:

```
dir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

Press i to enter edit mode and add the following command at the end:

sql-mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION"

Press Esc to exit edit mode, enter ":wq" to save and exit VIM mode.

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# whereis my.cnf
my: /etc/my.cnf
[root@localhost ~]# vim /etc/my.cnf
# For advice on how to change settings please see
# http://dev.mysql.com/doc/refman/8.0/en/server-configuration-
defaults.html

[mysqld]
#
```

```
# Remove leading # and set to the amount of RAM for the most
important data
# cache in MySQL. Start at 70% of total RAM for dedicated
server, else 10%.
# innodb_buffer_pool_size = 128M
#
# Remove the leading "# " to disable binary logging
# Binary logging captures changes between backups and is
enabled by
# default. It's default setting is log_bin=binlog
# disable_log_bin
#
# Remove leading # to set options mainly useful for reporting
servers.
# The server defaults are faster for transactions and fast
SELECTs.
# Adjust sizes as needed, experiment to find the optimal
values.
# join_buffer_size = 128M
# sort_buffer_size = 2M
# read_rnd_buffer_size = 2M
#
# Remove leading # to revert to previous value for
default_authentication_plugin,
# this will increase compatibility with older clients. For
background, see:
# https://dev.mysql.com/doc/refman/8.0/en/server-system-
variables.html#sysvar_default_authentication_plugin
# default-authentication-plugin=mysql_native_password

datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
# Add sql-mode here, or there will be a pop-up prompt on the
home page when Windows remotely accesses the system on the
web.
sql-mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION"
```

3.5.6 Restart MySQL Service

If you use the SysVinit command, the command is as follows:

```
service mysqld restart
Chkconfig mysqld on
```

If you use the Systemd command, the command is as follows:

```
systemctl restart mysqld.service
Systemctl enable mysqld.service
```

3.5.7 Enable Remote Access of MySQL root Account

Open remote access for MySQL root account. You can use root in database tool to remotely access MySQL database and then create BlueEyesView business database.

Enter MySQL shell, command is as follows:

```
mysql -u root -p
```

Select MySQL database, command is as follows:

```
USE mysql;
```

Note:

Do not omit the semicolon in the command.

Check the information about the current root user in the user table of MySQL database. The command is as follows:

```
SELECT host, user, authentication_string, plugin FROM user;
```

Set the remote access of root user , and the command is as follows:

```
update user set host = '%' where user ='root';
```

Refresh privileges, and the command is as follows:

```
FLUSH PRIVILEGES;
```

Grant all permissions to root, and the command is as follows:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';
```

Update the root password and encryption rules (if the client does not support encryption plug-in), the command is as follows:

```
ALTER USER 'root'@'%' IDENTIFIED WITH mysql_native_password BY
'NewPassword12#$';
```

Notice:

- Command "NewPassword12#$" is the password for root to remotely access the database. To ensure the security of the database, it is recommended to change the password.
- The password consists of uppercase and lowercase characters, numbers and special characters, otherwise, the password is not safe.
- After the password is modified, the "application.properties" file in the folder "tools\config" in the installation package needs to be modified synchronously. Add the set password after "spring.datasource.password=".

Refresh privileges, and the command is as follows:

```
FLUSH PRIVILEGES;
```

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.18 MySQL Community Server - GPL

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All
rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or
its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current
input statement.
mysql> USE mysql;
Database changed
mysql> SELECT host, user, authentication_string, plugin FROM
user;
…
5 rows in set (0.00 sec)

mysql> update user set host = '%' where user ='root';
Query OK, 1 row affected (0.09 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';
Query OK, 0 rows affected (0.06 sec)
```

```
mysql> ALTER USER 'root'@'%' IDENTIFIED WITH
mysql_native_password BY 'NewPassword12#$';
Query OK, 0 rows affected (0.06 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)
```

3.6 Install JDK/JRE

The operation of BlueEyesView system depends on JDK/JRE 8, so it is necessary to install JDK or JRE. JRE(Java Runtime Environment) is an environment needed to run an application based on Java language. JDK(Java Development Kit) includes JRE, and also supports tools and databases needed for developing Java programs. The most widely used JDK/JRE is Oracle JDK/JRE. Since Oracle changed the free policy of JDK/JRE in 2019, it is necessary to purchase Oracle authorization to use the JDK/JRE released by Oracle 2019 in commercial environment. Therefore, it is recommended to use the free Open JDK/JRE 8. If Oracle JDK/JRE is used, please use the version released in 2018.

Only one version of JDK and JRE needs to be installed, and the related installation methods are as follows.

Open JDK

Install Open JDK 8.0, the command is as follows:

```
sudo yum install java-1.8.0-openjdk
```

Open JRE

Install Open JRE 8.0, the command is as follows:

```
sudo yum install java-1.8.0-openjdk-devel
```

Oracle JDK

Get Oracle JDK 8.0 resources, and the command is as follows:

```
wget "https://mirrors.huaweicloud.com/java/jdk/8u192-b12/jdk-
8u192-linux-x64.rpm"
```

Install Oracle JDK 8.0, and the command is as follows:

```
sudo yum localinstall jdk/8u192-b12/jdk-8u192-linux-x64
```

Configure Java_Home and modify the profile file. The command is as follows:

```
sudo vim /etc/profile
```

Add the following three lines to the open file:

```
export JAVA_HOME=/usr/java/jdk1.8.0_192-amd64
export PATH=$JAVA_HOME/bin:$PATH
export
CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib/tools.jar
```

Then reload the configuration file with the following command:

```
source /etc/profile
```

Oracle JRE (omitted)

The Oracle JRE installation can refer to the official Oracle guidelines.

After the installation, enter the command "**java -version**". If the type and version of jdk/jre can be displayed normally, the installation is successful.

Configuration Instance

The installation configuration of Open JDK 8.0 in CentOS7 terminal is as follows:

```
[root@localhost ~]# sudo yum install java-1.8.0-openjdk-devel
…
##The resolution of dependencies is omitted here##

…
Install 1 software package

Total download volume: 9.8 M
Installation size: 40 M
Is this ok [y/d/N]: y
Downloading packages:
java-1.8.0-openjdk-devel-1.8.0.232.b09-0.el7_7.x86_64.rp | 9.8
MB   00:11
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing: 1:java-1.8.0-openjdk-devel-1.8.0.232.b09-
0.el7_7.x86_64 1/1
Authenticating: 1:java-1.8.0-openjdk-devel-1.8.0.232.b09-
0.el7_7.x86_64   1/1
Installed:
java-1.8.0-openjdk-devel.x86_64 1:1.8.0.232.b09-0.el7_7

Finished!
[root@localhost ~]# java -version
openjdk version "1.8.0_232"
```

```
OpenJDK Runtime Environment (build 1.8.0_232-b09)
OpenJDK 64-Bit Server VM (build 25.232-b09, mixed mode)
```

3.7 Install the Integrated Monitoring and Management System Database

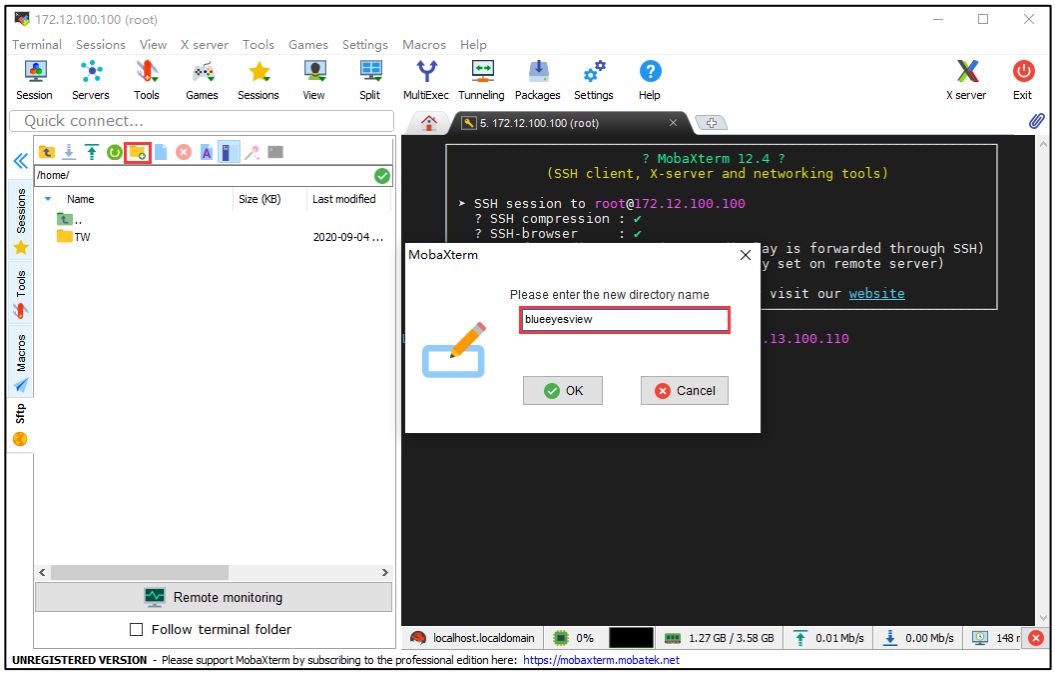
3.7.1 Upload Installation File

Upload Installation File

Create a new folder "blueeyesview" under the "\home" directory of Linux system via MobaXterm, and then upload the compressed package of system installation to the folder "blueeyesview".

Step 1 Use MobaXterm to establish remote connection with Linux system, please refer to the description of Chapter "3.3".

Step 2 Create the "blueeyesview" folder as follows:



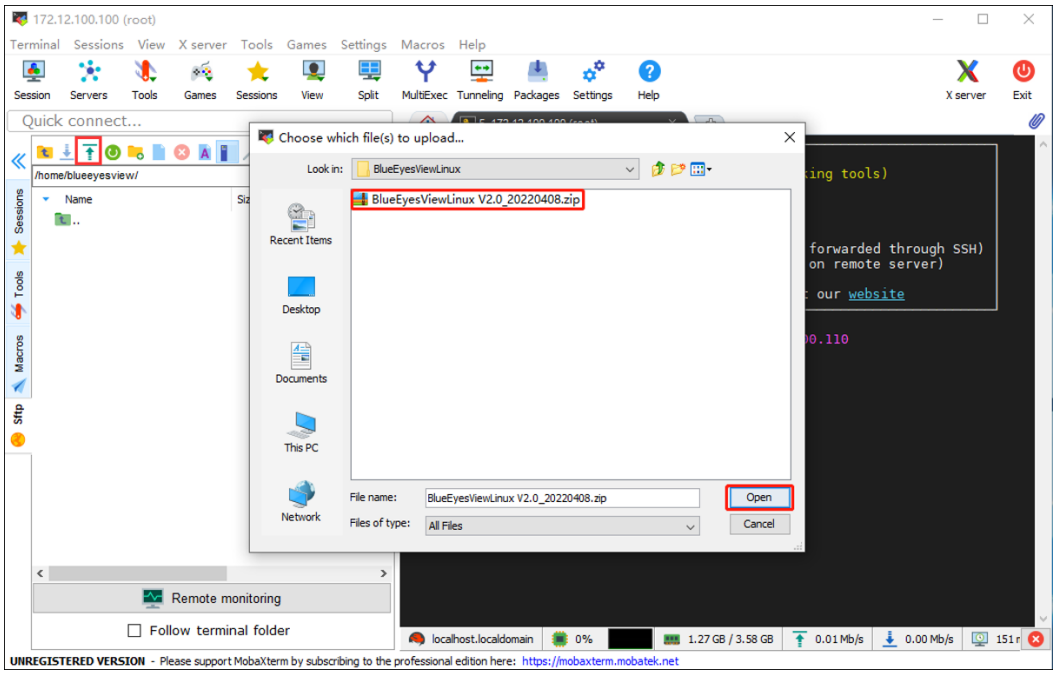
1 Click “Sftp” in the left navigation bar to enter the file management page;

2 Double-click the "home" folder and enter the "\home" directory;

3 Click the "" icon to create a new "blueeyesview" folder;

- Enter "blueeyesview" in the text box "Please enter the new directory name";
- Click the "OK" button, as shown in the above figure;

Step 3 Upload the installation package to the "blueeyesview" folder:



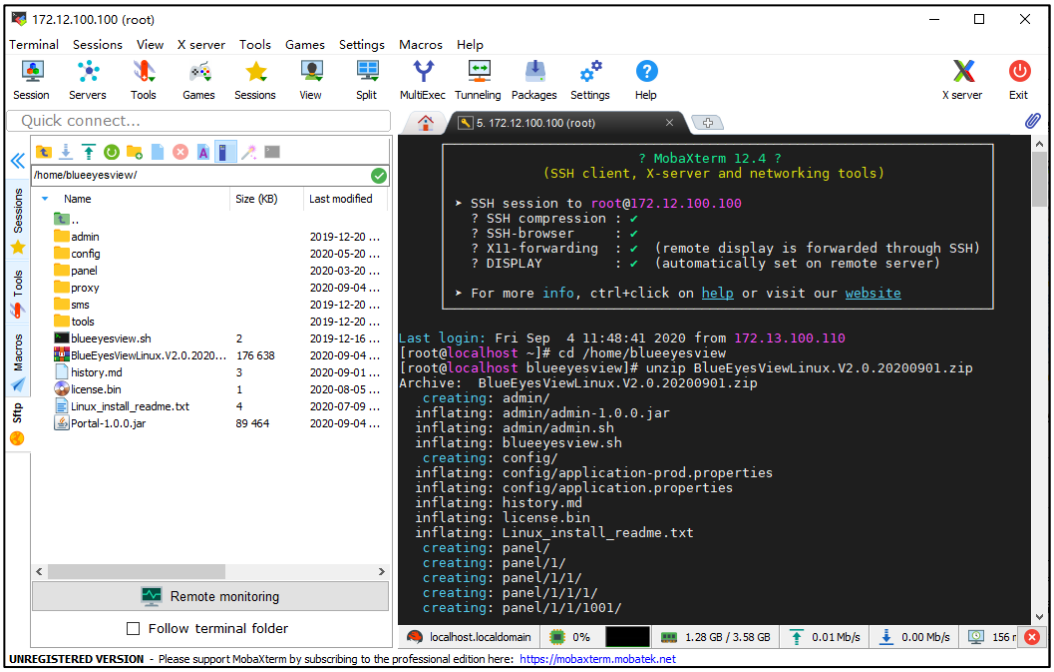
1 Double-click the "blueeyesview" folder to enter the "blueeyesview" directory;

2 Click the " " "icon;

3 In the "Choose which file(s) to uplad ..." window, click to select the installation package

4 Then click the "Open" button to start uploading, as shown in the above figure.

Step 4 Unzip the installation package.



1 Enter the command "cd /home/blueeyesview" in the terminal interface to enter the "blueeyesview" directory;

2 Enter the command “unzip BlueEyesViewLinux.V2.0.20200901.zip” to unzip the installation package, and “blueeeyesviewlinux.v2.0.20200901.zip” is the installation package name, as shown in the above figure.

Note:

If there are no zip and unzip commands on Linux system, please install zip and unzip manually.

Step 5 End.

User Privilege for Files

After the file is uploaded, it is necessary to set the user rights of the "blueeyesview" directory. The command is as follows:

```
chmod -R 777 /home/blueeyesview
```

Add MySQL root Account Password

The MySQL root account password created in the MySQL database needs to be added to the "application.properties" file under the directory "blueeyesview\tools\config" synchronously.

In the terminal interface of Linux system, the operation is as follows.

Enter VIM mode of "application.properties" file with the following command:

```
vim /home/blueeyesview/tools/config/application.properties
```

Go back to the "application.properties" file, press the "i" key to enter the VIM editing mode, and enter the root password after "spring.datasource.password=" in the seventh line as follows:

```
logging.level.org.springframework=info
logging.level.com._3onedata=INFO
logging.level.root=INFO

spring.datasource.url=jdbc:mysql://localhost:3306/?useSSL=fals
e&allowPublicKeyRetrieval=true&serverTimezone=Asia/Shanghai&us
eUnicode=true&characterEncoding=UTF-8
spring.datasource.username=root
spring.datasource.password=NewPassword12#$
spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver

ds.url=jdbc:mysql://localhost:3306/blueeyesdb?useSSL=false&all
owPublicKeyRetrieval=true&serverTimezone=Asia/Shanghai&useUnic
ode=true&characterEncoding=UTF-8
ds.username=3onedata
ds.password=_3oneData!@#
ds.driver=com.mysql.cj.jdbc.Driver
```

Press Esc to exit edit mode, enter ":wq" to save and exit VIM mode.

File Path and Java Name

The created folder name, file path and Java name are changed. Please modify them synchronously in the "blueeyesview.sh" script. It is recommended to use the default path and name.

Enter VIM mode of "blueeyesview.sh" file with the following command:

```
vim /home/blueeyesview/blueeyesview.sh
```

Go back to the "blueeyesview.sh" file as follows:

```
# service name, used for display. it is recommended to use English and spaces
SERVICE_NAME=BlueEyesView

# Directory where # JAR package is located, please modify it to actual directory
APP_HOME=/home/blueeyesview

# JAR package name, please modify it to the actual name
JAR_NAME=Portal-1.0.0.jar
```

Press the "i" key to enter VIM editing mode, and modify the path and name. Press "Esc" to exit edit mode, and enter ":wq" to save and exit VIM mode.

3.7.2 System Initialization

Use BlueEyesViewTool to initialize the system and create the system database.

On the Linux system terminal interface, enter the "tools" directory, and the command is as follows:

```
cd /home/blueeyesview/tools
```

Run the database installation tool with the following command:

```
java -jar BlueEyesViewTool-1.0.0.jar
```

The system will prompt you to select the operation to be performed, such as:

- 1: System initialization
- 2. Import the system authorization file
- 3. Upgrade the system

Enter 1 to enter system initialization.

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost blueeyesview]# cd /home/blueeyesview/tools
[root@localhost tools]# java -jar BlueEyesViewTool-1.0.0.jar
# The loading process is omitted here #
Choose the operation to be performed:
```

```
1 -- System initialization
2 -- Import the system authorization file
3 -- Upgrade the system
Please select:
1
# The system automatic initialization process is omitted here
#
```

3.7.3 System Authorization

After initialization is completed, authorization service operation can be performed. At the same time, the system will automatically generate a trial version of the authorization file, which by default supports the management of up to 50 network nodes and the use of the two-year validity period. After authorizing the service operation, the user can cancel the restrictions on the number of nodes and the validity period.

Notes

- After the initialization is completed, the authorization file will be detected before the system starts. When the current time is found to be within the validity period, the authorization service will be skipped. Otherwise, authorization is required before entering the WEB interface.
- To authorize service operation, you need to exit the running system and delete the original trial version authorization file; Then, enter the authorization interface and import the obtained official authorization file for authorization.

The file "licenseTemp.bin" will be generated in the directory "/home/blueeyesview/tools/" when the system is initialized. Please contact relevant customer service staff and provide the file "licenseTemp.bin" to obtain relevant authorization files. The file "licenseTemp.bin" can be downloaded to local Windows through MobaXterm. After obtaining the authorization file, you can delete "”the trial version of the authorization file on the Linux system through MobaXterm, and upload "”the obtained official version of the authorization file to the remote Linux system.

The operation mode of system authorization is as follows.

On the Linux system terminal interface, enter the "tools" directory, and the command is as follows:

```
cd /home/blueeyesview/tools
```

Run the database installation tool with the following command:

```
java -jar BlueEyesViewTool-1.0.0.jar
```

The system will prompt you to select the operation to be performed, such as:

- 1: System initialization
- 2. Import the system authorization file
- 3. Upgrade the system

Input 2 to enter the mode of importing the system authorization file

```
You will be prompted "Please enter the full name of the
license file (with path)". Please fill in the real path and
the full name of the license file, such as:
/home/blueeyesview/tools/license.bin
```

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost ~]# cd /home/blueeyesview/tools
[root@localhost tools]# java -jar BlueEyesViewTool-1.0.0.jar
#Omited#
Choose the operation to be performed:
1 -- System initialization
2 -- Import the system authorization file
3 -- Upgrade the system
Please select:
2
Please enter the full name (with the path) of the license
file:
/home/blueeyesview/tools/license.bin
got cmd job : dmidecode -t processor | grep 'ID'
got cmd job : dmidecode |grep 'Serial Number'
got cmd job : ifconfig -a
2019-12-26 15:43:12.679  INFO 7292 --- [          main]
com._3onedata.license.LicenseTools      :The authorization file
was verified successfully!
```

3.7.4 Start/Shut Down the System

On the Linux system terminal interface, enter the "blueeyesview" directory, and the command is as follows:

```
cd /home/blueeyesview
```

The trial run of the system will be displayed at the front end, but cannot be run in the background. The command is as follows:

```
java -jar Portal-1.0.0.jar
```

Note:

- If the system can start normally, it means that BlueEyesView has been successfully installed on Linux!

- Press the "Ctrl+C" key to interrupt the system operation, and quit the terminal system.
- After starting the system, you can enter "Server IP Address: 8282" through the browser to access the WEB interface.
- When the port number conflicts with the WEB service port number of other applications, the port number can be modified to other ports. You can modify the port number by modifying the value of "server.port" in the application configuration file "application-prod.properties". The default storage path of application configuration file is "/home/blueeyesview/config/".

After the system officially runs, it will run in the background. Start the system with the following command:

```
./blueeyesview.sh start
```

Check the system operation with the following command:

```
./blueeyesview.sh status
```

Stop the system operation with the following command:

```
./blueeyesview.sh stop
```

Configuration Instance

CentOS7 terminal configuration is as follows:

```
[root@localhost blueeyesview]# ./blueeyesview.sh start
BlueEyesView is already running, it's pid is 9184.
[root@localhost blueeyesview]# ./blueeyesview.sh status
BlueEyesView is running, it's pid is 9184.
[root@localhost blueeyesview]# ./blueeyesview.sh stop
Stoping BlueEyesView...
BlueEyesView stopped.
```

3.7.5 System Maintenance and Upgrade

The system upgrade process is similar to the system authorization process, which requires obtaining the upgrade package first and then uploading it to the Linux system. Enter Item 3 "System Upgrade" through BlueEyesViewTool-1.0.0, and then follow the prompts. Before upgrading, please make sure the system is backed up, especially the database.

On the Linux system terminal interface, enter the "tools" directory, and the command is as follows:

```
cd /home/blueeyesview/tools
```

Run the database installation tool with the following command:

```
java -jar BlueEyesViewTool-1.0.0.jar
```

The system will prompt you to select the operation to be performed, such as:

- 1: System initialization
- 2. Import the system authorization file
- 3. Upgrade the system

Input 2 to enter the mode of importing the system authorization file

`You will be prompted with "Please enter the full name of the upgrade file (with path)", such as:`

`/home/blueeyesview/tools/update.zip`

4 Log in to the WEB Management Interface

4.1 System Requirement for WEB Browser

Client browsers should meet the following conditions.

Hardware and Software	System requirements
Resolution	1980x1080 and above.
Color	65536 color and above.
Browser	In browsers like Chrome, Firefox, Edge, IE10 and above, Chrome browser is recommended. Note: When logging in using browsers other than Chrome and Firefox, the message "This site is unsafe" will pop up. At this point, click “Details” and select “Go to this webpage (not recommended)”.

4.2 Log in the Web Configuration Interface

Confirm the IP address of the host where BlueEyesView software is installed before logging in to the WEB.

Note
The default binding IP address of BlueEyesView is 0.0.0.0, which can monitor all the networks where the server is located, that is, the WEB of BlueEyesView binds all the network cards of the host by default. Login IP for single network card and multi-network card host:

- For single network card hosts, log in to the WEB directly using the IP address of the host.
- For multi-network card hosts, log in through the IP address of any network card.

Operation Steps

Note
Make sure the BlueEyesView system has been started before logging in to the WEB interface.

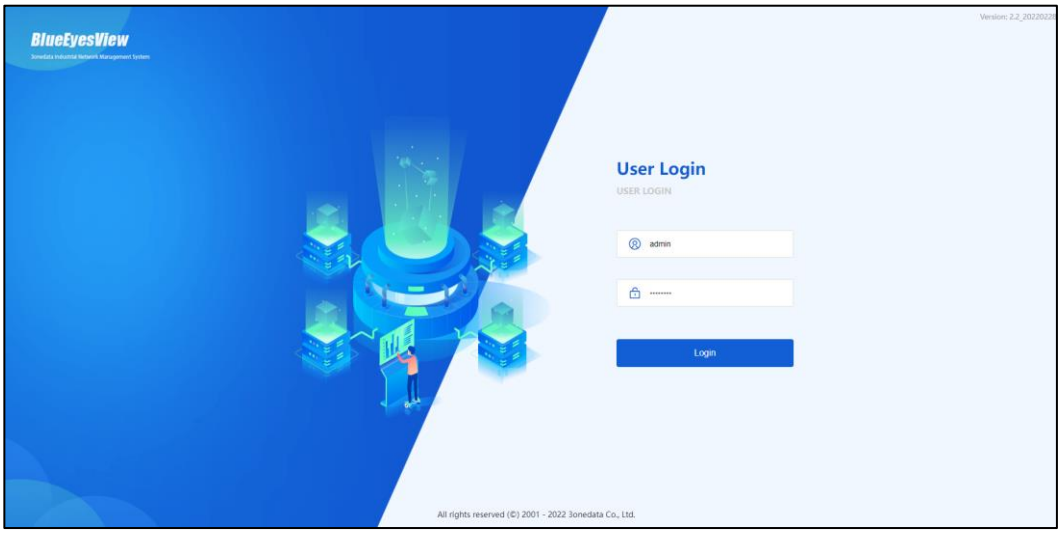
Login in the web configuration interface as follow:

Step 1 Open the computer browser.

Step 2 Enter the system address and port number "http:/http://XX.XX.XX.XX:8282" or "https://xx.xx.xx: 8283" in the address bar of the browser. E.g.: http://192.168.1.100:8282.

Step 3 Click the “Enter” key.

Step 4 Enter the user name and password in the popup login window.



Note:

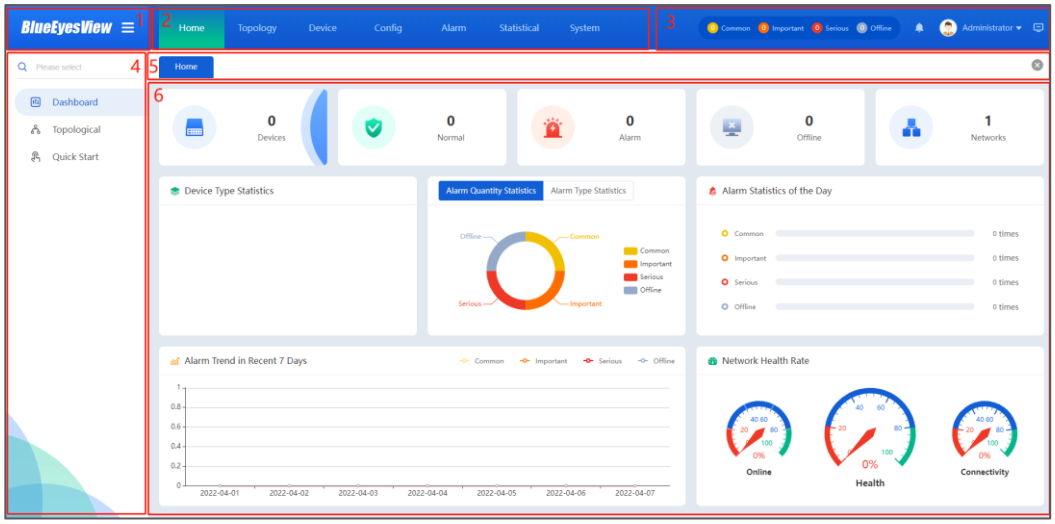
- The default username is “admin” and the password is “admin123”; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privileges.

Step 5 Click "Login".

Step 6 End.

5 Interface Introduction

Common WEB operation interface is shown in the following figure:



Layout description of common WEB operation interface:

Number	Note
1	System name and navigation bar control buttons. Click "☰"or "▥"to close or display the navigation bar.
2	The menu bar. The WEB interface consists of home page, topology management, device management, configuration management, alarm management, statistical analysis and system management.
3	Notification area. It consists of real-time alarm data, alarm messages, current users and large monitoring screens.
4	Fuzzy query and navigation bar. • Fuzzy query: after the user inputs the characteristic characters of the device, the matching device list will be listed for the user to select. • Navigation bar: provides configuration navigation under the current menu.
5	Tab, current and historical operation page tabs are displayed.
6	Status display and operation area. This area displays the current status of the device, and provides operations such as creating, modifying,

Number	Note
	deleting, loading and searching.

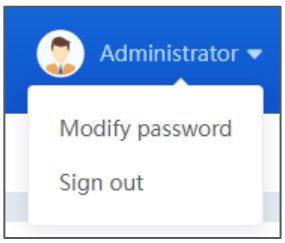
5.1 Current User

Function Description

The name display of the current login user, and the password of the current user can be modified and the system can be logged out.

Interface Description 1: Current User

Click the current user name drop-down list, as shown in the following figure:



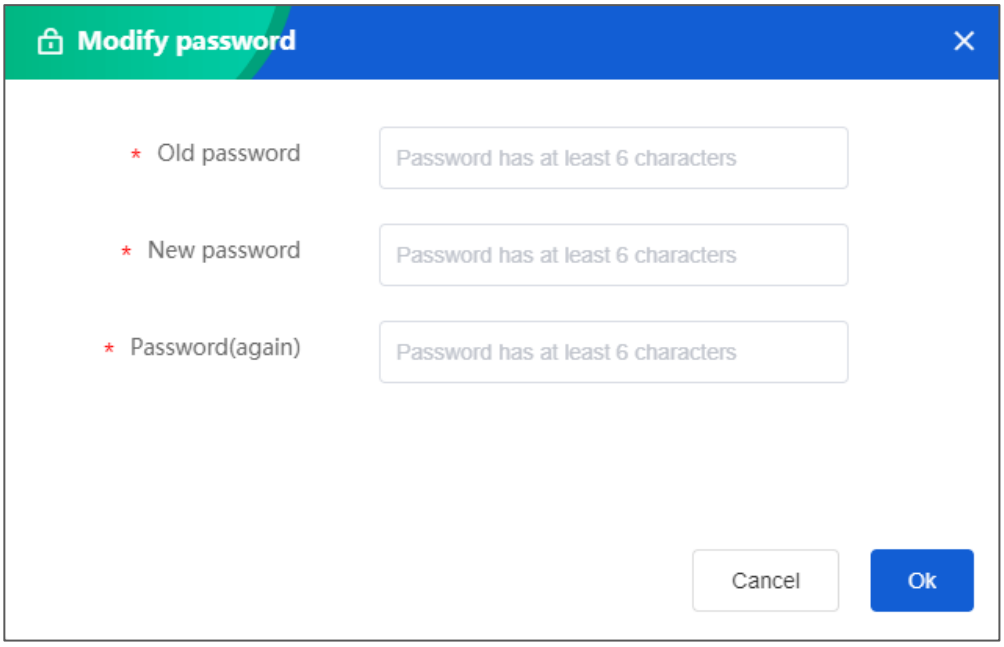
The main element description of current user interface:

Interface Element	Description
Modify password	Modify the password of the current user.
Sign out	Exit the currently logged-in network system.

Interface Description 2: Modify Password

In the current user interface, click “Modify Password” to enter the Modify Password interface.

The Modify Password interface is shown in the following figure:



The element description of Modify Password interface:

Interface Element	Description
Old password	Enter the login password for the current user.
New password	Enter the modified password. The password consists of 6 to 50 characters, and supports the input of letters, numbers, special characters, etc., but does not support spaces.
Password(again)	Enter the new password again.

Notice

- After modifying the password of the current user, you need to log in to the system again.
- The default user "admin" is "Administrator" and has administrator rights. If you change the administrator's password, please keep the password information properly; If the password is lost, please contact the relevant customer service staff and reset to the default password.

5.2 Real-time Alarm Data

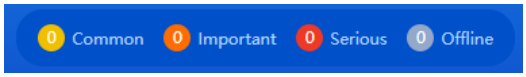
Function Description

In the display area of real-time alarm data function, you can view the alarm level and number of devices in the current network. The alarm levels of the system are divided into four categories that correspond to different colors. The alarm levels and colors are as follows:

- : indicates general alarm;
- : Indicates important alarm;
- : indicates severe alarm;
- : indicates offline alarm.

Interface Description

The real-time alarm data interface is as shown in the following figure:



The element description of real-time alarm data interface:

Interface Element	Description
Common	Displays the number of general alarms generated by devices in the current network, such as flow alarms, CPU utilization alarms, memory utilization alarms and bandwidth utilization alarms.
Important	Displays the number of important alarms generated by devices in the current network, such as power failure.
Serious	Displays the number of serious alarms generated by devices in the current network, such as link failure and ring network storm.
Offline	Displays the number of offline devices in the current network.

Note

- After the network failure corresponding to the real-time alarm is recovered, the corresponding alarm number will be automatically cleared.
- Click the corresponding alarm quantity to enter the page of "Alarm Management > Real-time Alarm List", where you can view the corresponding alarm device information and alarm information processing.
- The alarm level can be modified in "Alarm Management > Alarm Configuration > Alarm Definition".

5.3 Alarm Message

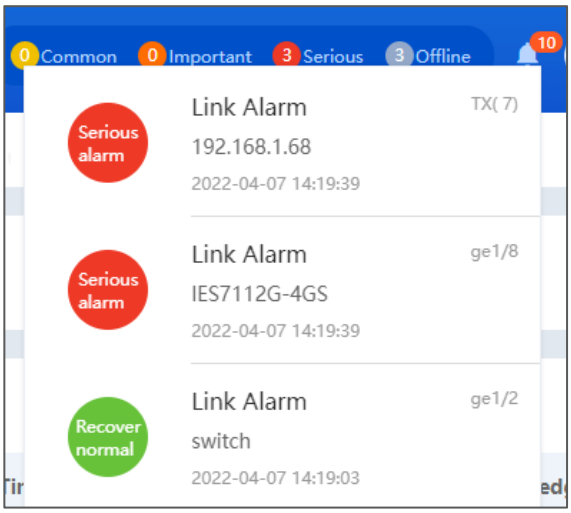
Function Description

The alarm message is displayed with the icon "".When the alarm message appears, it will automatically prompt and record the current alarm information.

Interface Description 1: Alarm Message

Click the alarm message icon "" to enter the alarm message interface and view the network alarm information.

The alarm message interface is shown in the following figure:



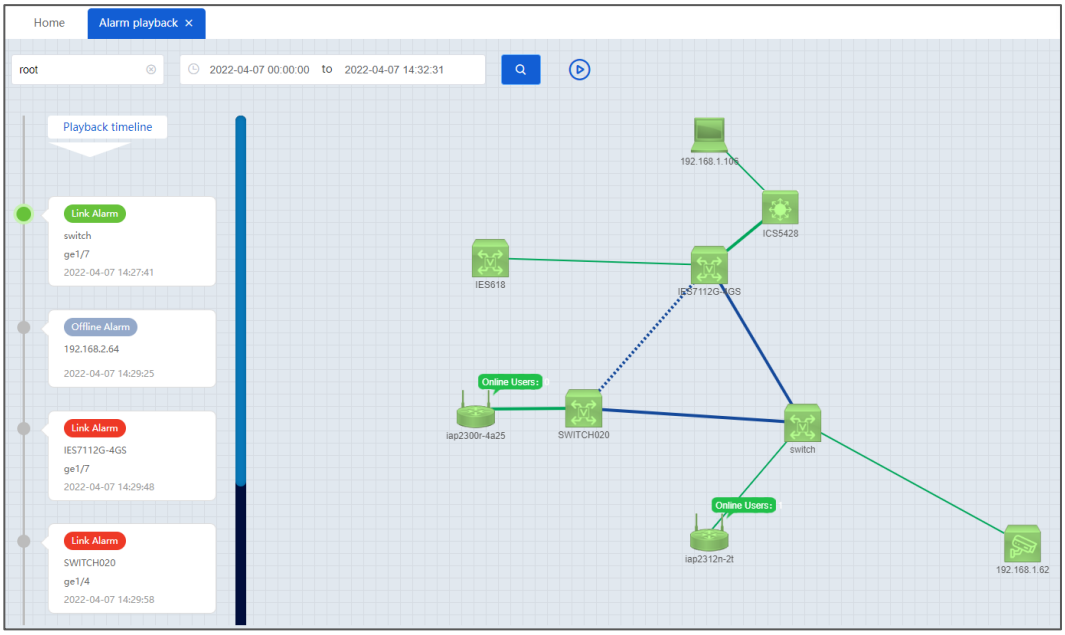
The element description of alarm message interface:

Interface Element	Description
Alarm Message	Display general, important, serious, offline and other alarm events, as well as alarm events returning to normal.
Alarm playback	After an alarm occurs, you can view the state change of the network topology diagram when an alarm message occurs through the alarm playback function. Notice: The alarm playback function of the system is disabled by default, and can be enabled under "Playback Switch" under "System Management > System Settings > System Configuration"; After enabling the playback switch, it will affect the performance of the system. Please use it with care!
Clear	Clear alarm messages.
View all	Check the alarm message list.

Interface Description 2: Alarm Playback

In "Alarm Message", click "Alarm Playback" button to enter the alarm playback interface. Turn on the "Playback switch" in "System Management > System Configuration > System Configuration" in advance to use the playback function.

The alarm playback interface is shown in the following figure:



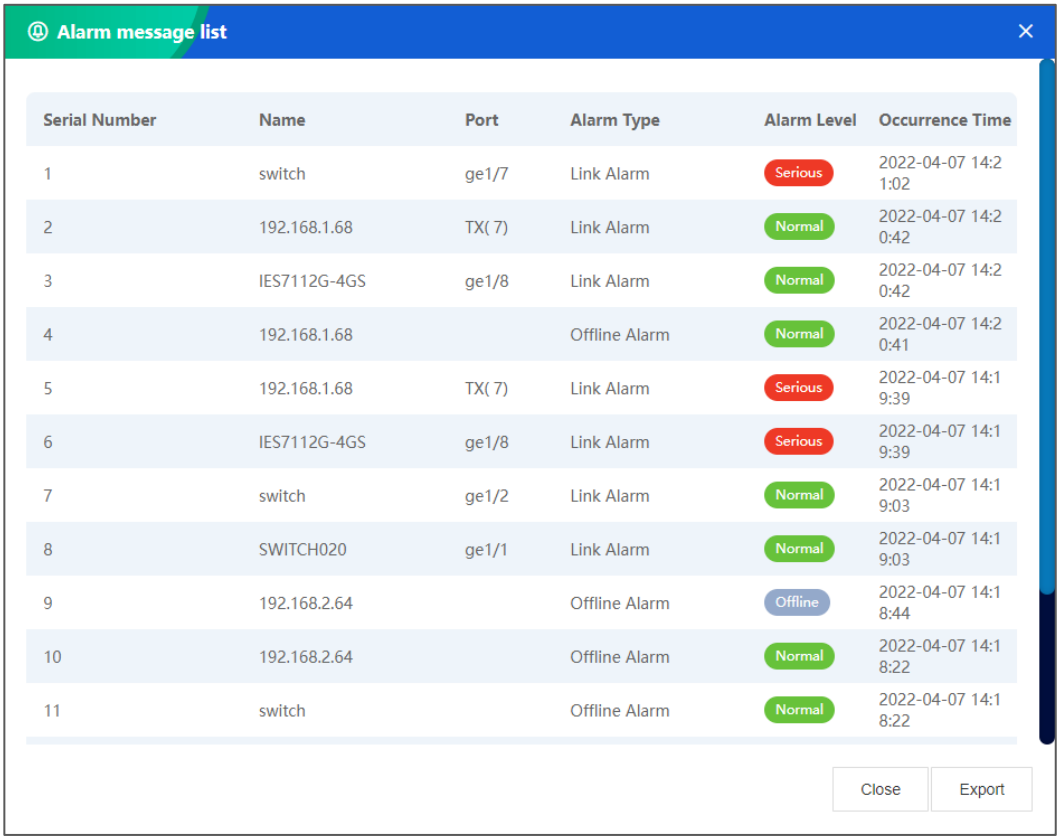
The element description of alarm playback interface:

Interface Element	Description
	Click the Query "  " button to query the alarm message playback within the specified network and time period.
	Click the Play "  " button to view the changes of network topology diagram under different alarm messages.
	Pause button.
	Replay button.
Playback timeline	On the Playback timeline, click to select an alarm event, and view the network topology diagram after the alarm event occurs.

Interface Description 3: Alarm Message List

In "Alarm Messages", click "View All" button to enter the alarm message list.

The alarm message list interface is as shown in the following figure:

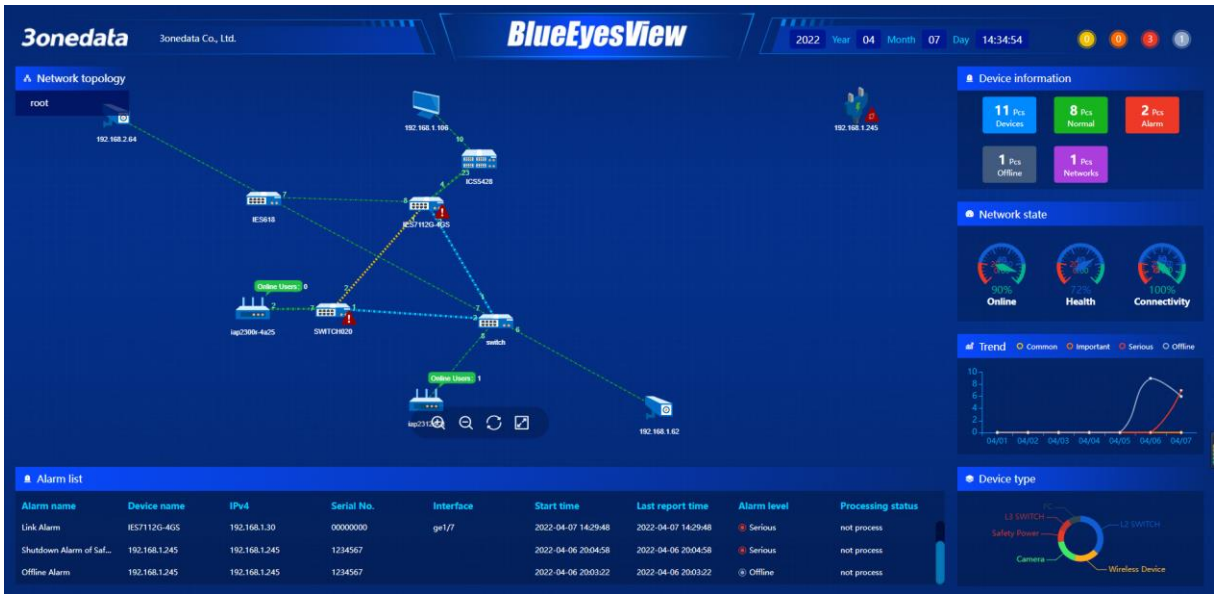


The element description of alarm message list interface:

Interface Element	Description
Serial Number	Serial number of alarm message.
Name	The name of the device where the alarm occurred in the network.
Port	Device port corresponding to the alarm in the network.
Alarm Type	The event type of the alarm message.
Alarm Level	The alarm level corresponding to the alarm message.
Occurrence time	The time when the alarm event is detected.
Close	Close the alarm message list.
Export	Export the alarm message list.

5.4 Full Screen

On the WEB interface, click the full screen icon “ ” in the upper right corner to enter the full screen monitoring page of the integrated monitoring management system. On the monitoring page, you can view information such as network topology diagram, device information, network status, alarm trend, device type statistics and alarm list.



6 Home Page

6.1 Home Page

Function Description

On the “Home” page, you can view the following information:

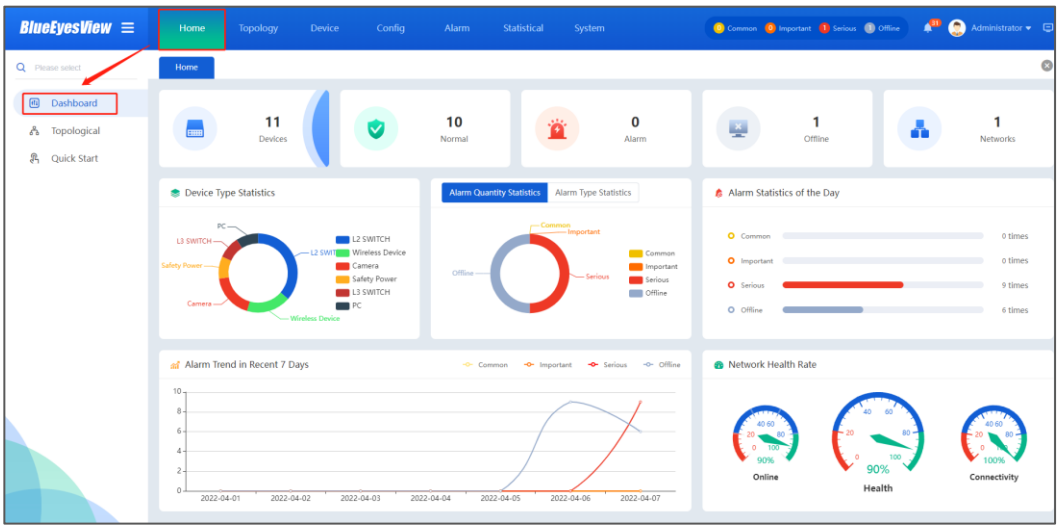
- Number of devices in different alarm states;
- Statistical diagram of the number and proportion of different types of devices;
- Statistical diagram of the number and proportion of alarms of different levels and types;
- The alarm statistics chart of the day and the historical alarm trend chart;
- Network health rate.

Operation Path

Open in order: "(Menu bar) Home > (Navigation bar) Home page".

Interface Description

Screenshot of homepage interface:



Main elements configuration descriptions of the home interface:

Interface Element	Description
Devices	The total number of devices in all networks, regardless of the type of devices.
Normal	The number of devices with normal status (no alarm) in all networks.
Alarm	The number of devices with alarm status of general, important and severe in all networks.
Offline	Number of devices with offline status in all networks. Note: Offline means that the device is disconnected, the network management system cannot communicate with the device or the response is timed out.
Networks	Total number of root networks in the system, excluding subnetworks.
Device type statistics	Pie chart of device types, counting the number and proportion of various types of devices.
Alarm quantity statistics	Pie chart of alarm quantity, indicating the alarm quantity and proportion of each alarm level in the system at present.
Alarm type statistics	Histogram of alarm type, showing the number of various alarms in the current system.
Alarm statistics of the day	Bar chart of alarm statistics of the day, showing the alarm times of the system such as general, important, serious and offline.
Alarm trend in recent 7 days	Trend chart of alarm level in recent 7 days supports general, important, serious and offline alarms.
Network health rate	The dashboard graph of network health rate supports the

Interface Element	Description
	following statistics: • Device online rate: the ratio of real-time online device to the total number of device (online device includes alarm device); • Device health rate: the ratio of real-time normal device to the total number of device (excluding alarm device); • Link connectivity rate: the ratio of normal links to the total links of the system, which is counted in real time.

Note

- Click the number of various devices to enter the device management menu and view the corresponding devices.
- Click "Networks" to enter the topology management menu and view all the networks.
- Move the mouse pointer to the statistical chart to view the corresponding data information.

6.2 Topological Graph

Function Description

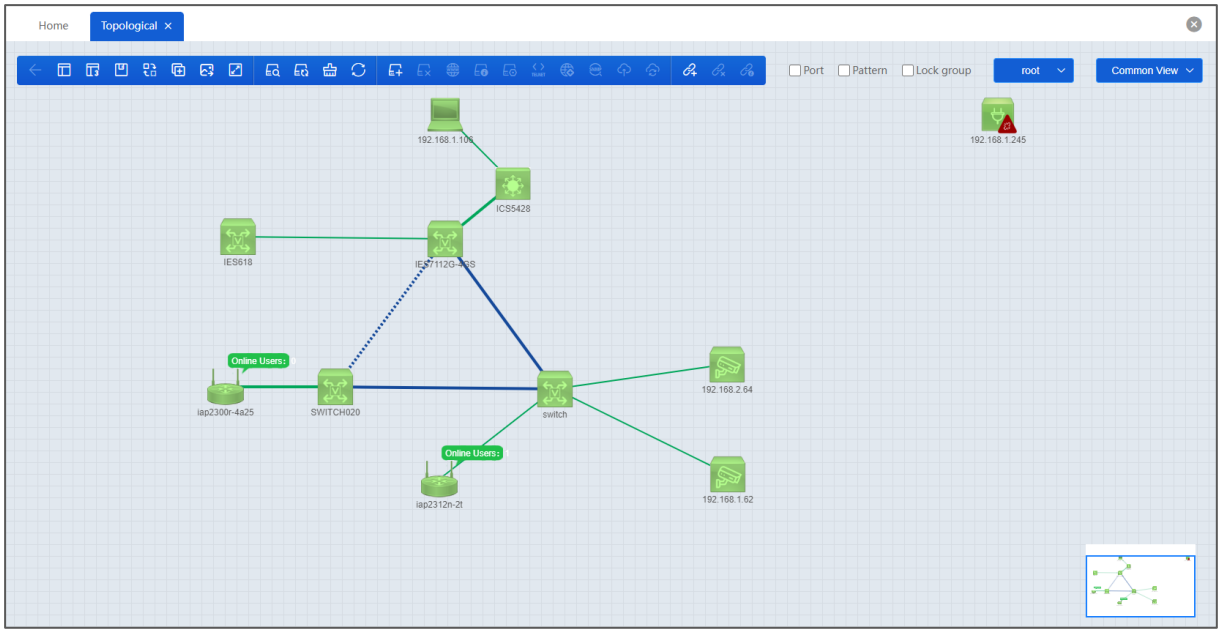
On the "Topology Diagram" page, you can view the network topology diagram to realize device discovery, topology diagram management and real-time alarm.

Operation Path

Open in order: "(Menu bar) Home > (navigation bar) Topology Diagram".

Interface Description

Screenshot of topology diagram interface:



Element description of topology diagram interface:

Interface Element	Description
Topology layout	**Operation button of topology layout**
	Back: return to the previous topology of this sub-topology. You can also double-click in the blank place on the subnet topology to return to the previous topology of this subnet topology.
	Save layout: save the current network topology layout.
	Restore layout: Restore the original network topology layout.
	Full screen: the network topology diagram is displayed in full screen.
	Exit full screen: exit full screen display.
	Classic layout: the topology diagram layout is displayed from left to right.
	3onedata layout: the topological graph layout is displayed from top to bottom.
Device Discovery	**Operation button of device discovery**
	Device discovery: support device discovery configuration of 3onedata private protocol and general protocol.
	Rediscovery: Rediscover link relationships between devices.
	Clear: Clears the current network topology diagram.
	Refresh: Refresh the topology map.
Device Management	**Click the device icon to check the operation button of current device.**

Interface Element	Description
	Add Device: Manually add device.
	Delete Device: Device can be deleted only when they are offline.
	WEB configuration: access device WEB interface. Notice: • When the client and the device are in the same network segment or the network is reachable, the WEB interface of the device can be accessed normally; • When the BlueEyesView system is configured for multi-network (e.g. multi-network card), the function of local WEB proxy server in "System Management > System Settings > WEB Agent" can be used to realize client cross-network segment or network access device WEB interface.
	Device information: modify device information, such as serial number, device name, device type, installation address, remark and other information.
	Device configuration: Modify the basic configuration of the device, such as IP address, device name, factory reset and device restart. Note: Only 3onedata devices are supported temporarily, and the device and network management system are in the same local area network.
	Telnet: The CLI interface of the device be accessed through Telnet protocol. Note: When accessing a device through the Telnet protocol, the device must have the Telnet service function enabled in advance.
	Network Diagnosis: Supports PING and TRACEROUTE detection.
	SNMP query: according to the MIB list related to the public SNMP protocol, get the information of the corresponding node of the device, and support the query of customized OID node.
	Configuration Backup: Download the configuration file of the current device.
	Configuration Recovery: Upload configuration file to the current device.
Topological connection	**Click the topology connection to view the action button for the connection**
	Add Connection: Manually add the topology connection.

Interface Element	Description
	Delete Connection: The connection can be deleted only when it is offline.
	Connection Information: The topology connection can be modified, such as the port, link type, interface type, bandwidth and other information of the device.
Event Playback	**Click to select a wireless device and view its alarm information.**
	AP Event Playback: You can view the status changes of the wireless device and mobile client topology diagram within a specified period of time. Notice: The AP event playback function of the system is disabled by default which can be enabled in the "Playback Switch" under "System Management > System Settings > System Configuration"; When the switch is enabled, it will affect the performance of the system. Please use it with care!
Display Port	**Check the "Display Port" check box to display the port number to which the network topology diagram device is connected**
Drawing Description	**Check the "Drawing Description" check box to display the information description of device icon and topology connection in the network topology diagram.**
Network Switching	**Click the drop-down list of Network Name to switch to a different network or subnet topology**
View Switching	**Click the drop-down list of View to switch the network topology view**
Common View	In the network topology diagram, the system uses common icons to identify various network devices.
3onedata View	In the network topology diagram, the system uses 3onedata icons to identify various network devices.
Traffic View	In the network topology diagram, the system identifies the network link in different colors to reflect the traffic load.

 Note

- When the device establishes the link, select the device to freely drag the device location. If you select the blank area within the network, you can drag the entire network location.
- In the topology diagram, according to the area where the mouse cursor is located, slide the

mouse wheel to zoom in and zoom out the topology diagram accordingly.

- Double-click the connection in the topology diagram to enter the "Modify topology connection" editing interface and modify the connection configuration.
- ▪▪▪▪▪▪▪: Indicates that the topology link is offline.
-  : Indicates the device offline alarm.
-  : Yellow icon indicates common alarm.
-  : Orange icon indicates important alarm.
-  : Red icon indicates serious alarm.

6.2.1 Network Topology Discovery

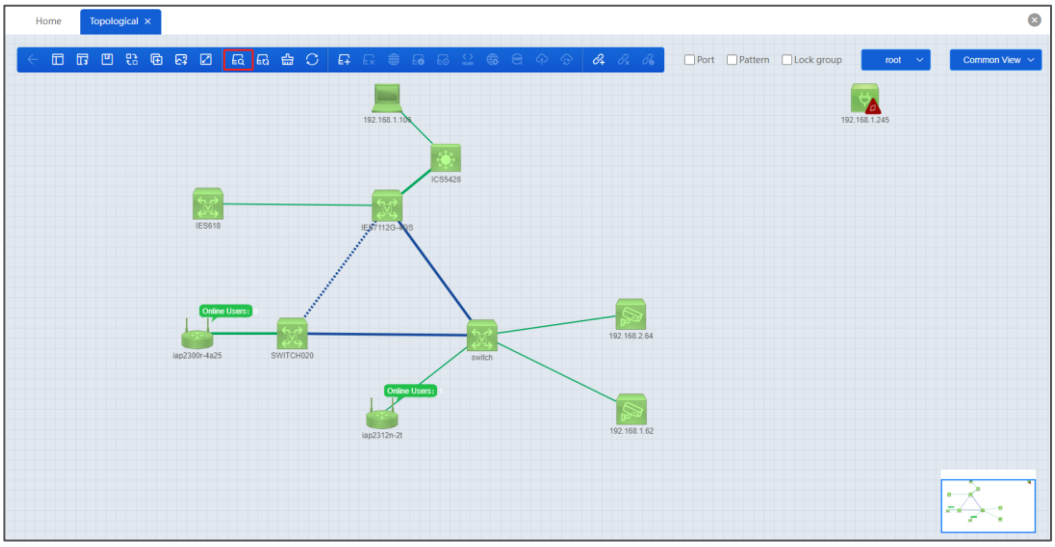
The network topology consists of Devices, links and alarms. Among them, the device discovery supports 3onedata private protocol, intelligent discovery and specified IP range discovery. 3onedata managed industrial Internet devices not only support public ICMP/ARP/SNMP protocol for intelligent device discovery, but also support 3onedata private second-generation and third-generation network management protocols for device discovery. Other network devices of manufacturers that do not support the private network management protocol of 3onedata can discover and manage all network devices through the public ICMP/ARP/SNMP protocol for device intelligent discovery or specified IP range discovery. LLDP discovery protocol and SNMP management protocol shall be enabled for device link discovery and management.

 Notice

- Before the network topology discovery, you can configure the network card, UDP, SNMP settings and other related parameters in the system settings of the system management menu. If there is no special modification, you can keep the default parameters.
- Device's LLDP and SNMP functions should be enabled in advance to ensure link discovery and management.

Operation Path

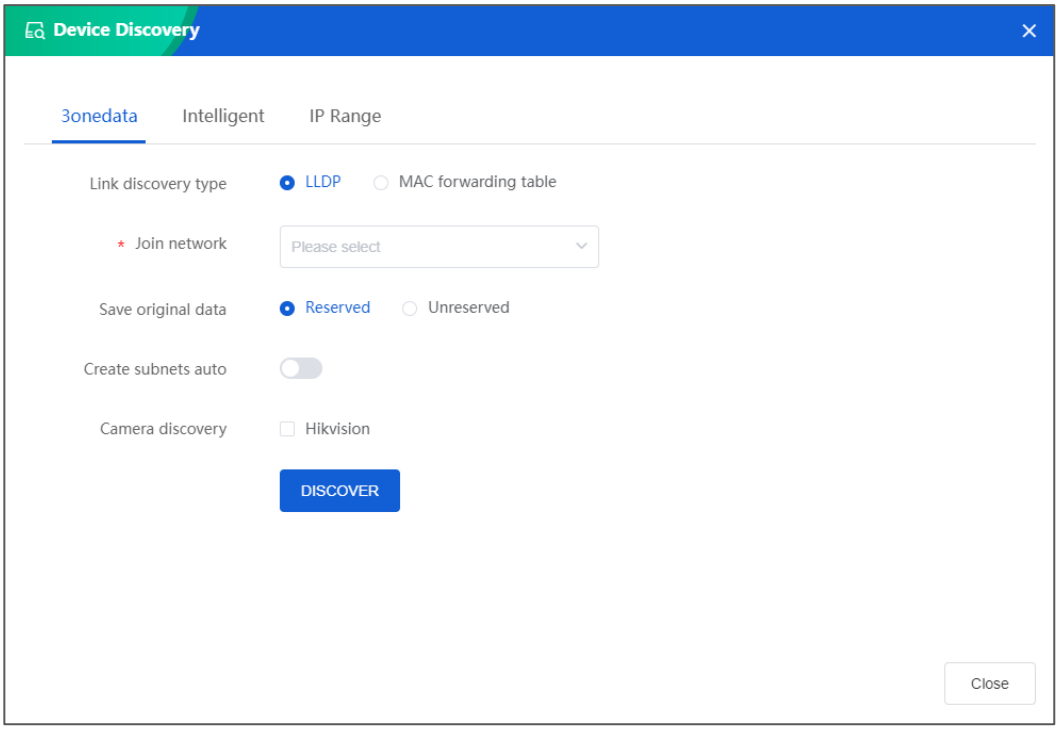
Open in order:(Menu Bar) Home >(Navigation Bar) Topology Diagram, select Device Discovery icon  .



Interface Description 1: 3onedata Discovery

In the device discovery page, select the "3onedata " tab to enter the 3onedata Discovery interface. In the network segment where the server of the integrated monitoring and management system is located, 3onedata discovery discovers the devices through the second and third generation 3onedata private network management protocols. When Layer 3 switch/router device is found in the network, the subnet device of the Layer 3 switch/router is to be discovered according to the routing table of the Layer 3 switch/router. Using this method until discovery is complete. 3onedata private protocol uses UDP broadcast packet for data transmission. Make sure the device is in the same LAN during device discovery.

Screenshot of 3onedata discovery interface:



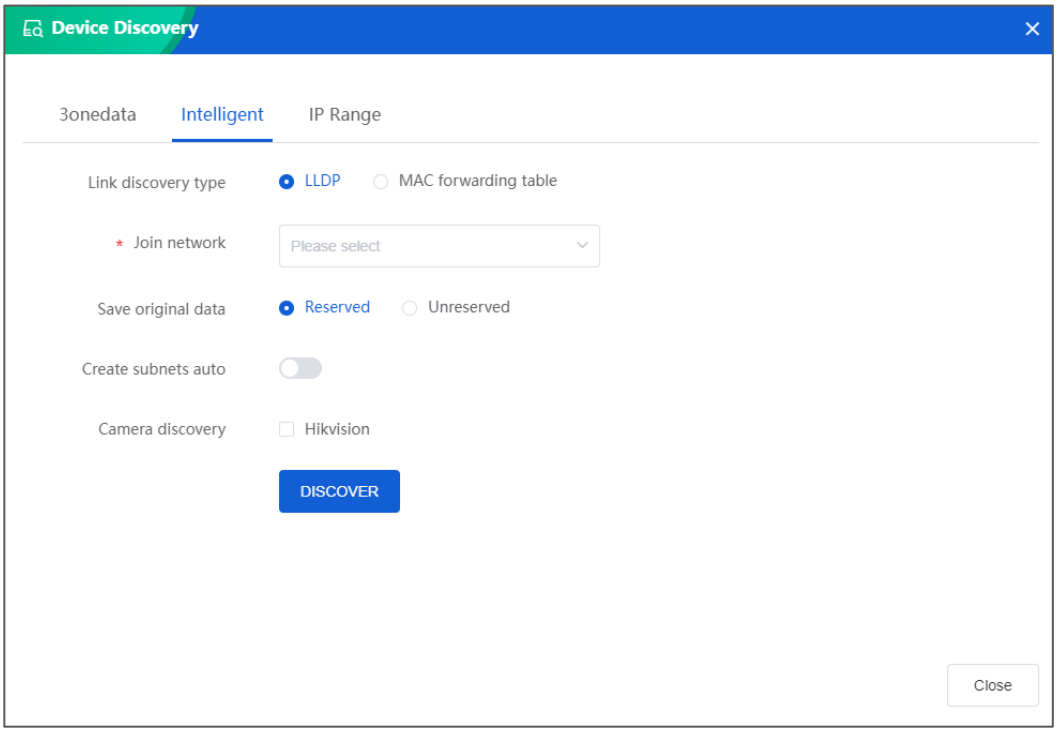
Element Description of 3onedata Discovery Interface:

Interface Element	Description
Link discovery type	Link discovery type, options are as follows: • LLDP: Link Layer Discovery Protocol; • MAC forwarding table: device MAC address forwarding list.
Join network	The network to which devices discovered through the protocol will join.
Save original data	Data storage, options are as follows: • Save: Existing or manually added device and link data will be saved in the new network topology diagram. When the original data does not exist, it is displayed with a gray offline icon. • Remove: Re-establish the network topology based on the discovered data and manually added links will be removed.
Create subnets auto	The feature of automatically creating subnet is disabled by default; And all discovered devices join the specified network automatically. After automatically create subnet is enabled, during 3onedata Discovery and Intelligent Discovery: • When the device IP address found matches the subnet created, the system adds the matching device to the subnet; • When multiple devices in the same network segment do not match the created subnet, the system automatically creates a subnet based on the device IP and adds the device to the subnet. Other devices will join the specified network.

Interface Description 2: Intelligent Discovery

In the device discovery page, select the "Intelligent " tab to enter the Intelligent Discovery interface.

Screenshot of Intelligent Discovery interface:



Element Description of Intelligent Discovery Interface:

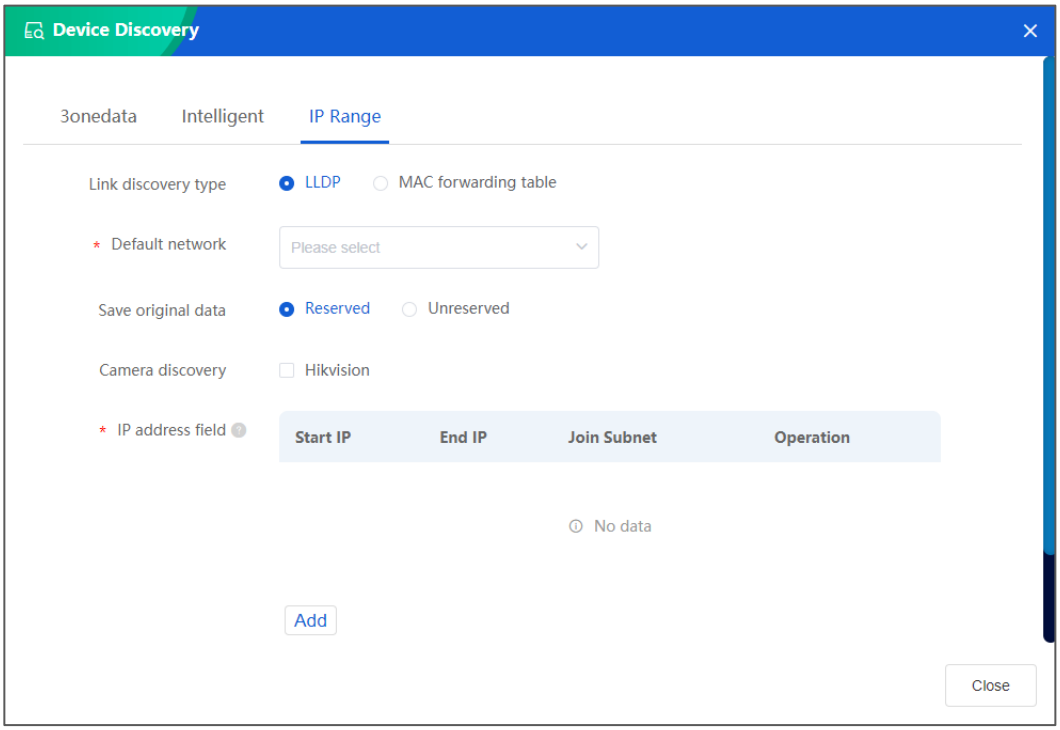
Interface Element	Description
Link discovery type	Radiobox options are as follows: • LLDP: obtain the data of LLDP (Link Layer Discovery Protocol) to calculate the link. • MAC forwarding table: device MAC address forwarding list.
Join network	The network to which devices discovered through the protocol will join.
Save original data	Data storage, options are as follows: • Save: Existing or manually added device and link data will be saved in the new network topology diagram. When the original the device or the link does not exist, it is displayed with a gray offline icon. • Remove: Re-establish the network topology based on the discovered data and manually added links will be removed.
Create subnets auto	The feature of automatically creating subnet is disabled by default; And all discovered devices join the specified network automatically. After automatically create subnet is enabled, during 3onedata Discovery and Intelligent Discovery: • When the device IP address found matches the subnet created, the system adds the matching device to the subnet;

Interface Element	Description
	• When multiple devices in the same network segment do not match the created subnet, the system automatically creates a subnet based on the device IP and adds the device to the subnet. Other devices will join the specified network.

Interface Description 3: Specified IP Range Discovery

In the device discovery page, select the "IP Range " tab to enter the Specified IP Range Discovery interface.

Screenshot of Specified IP Range Discovery interface:



Element Description of Specified IP Range Discovery Interface:

Interface Element	Description
Link discovery type	Radiobox options are as follows: • LLDP: obtain the data of LLDP (Link Layer Discovery Protocol) to calculate the link. • MAC forwarding table: device MAC address forwarding list.
Default network	The network that devices discovered through the IP range will join.
Save original data	Data storage, options are as follows: • Reserved: Existing or manually added device and link data will be saved in the new network topology diagram.

Interface Element	Description
	When the original the device or the link does not exist, it is displayed with a gray offline icon. • Unreserved: Re-establish the network topology based on the discovered data and manually added links will be removed.
IP address filed	Specify IP address range for device discovery, and add addresses of different network segment ranges.
Start IP	The start address of IP address range, which is mandatory, such as 192.168.1.1.
End IP	The end address of IP address range, which is mandatory, such as 192.168.1.254.
Join subnet	Subnet name, optional. Specify the subnet that the devices discovered in IP range will join. If the subnet does not exist, it will be created automatically. When not filled in, the discovered device will join the default network.
Operation	"Delete" button is used for deleting the current IP address range entry.

Network topology discovery shows the progress of discovery through five processes, as follows:

- Start;
- Device discovery;
- Link discovery;
- Data storage;
- End.

After the device discovery is completed, the discovered devices will be automatically displayed in the topology diagram. The topology diagram is displayed in networks. Different networks will be displayed separately, and the subnets of the network will be displayed as subnets icon in the topology diagram. In the topology diagram, the color of the device element represents the real-time state of the device. When the mouse moves to the element, the basic information and status of the device will be displayed. The thickness of the link represents different bandwidth. The thicker the link, the greater the bandwidth. The general link is generally displayed in green. When the link is displayed in blue, it means 3onedata ring network. When the mouse moves to the link, the connection information and link information at both ends of the link will be displayed.

6.2.2 Device Panel

6.2.2.1 Switch Device Panel

Function Description

In the switch device panel, you can view the panel information, system information, performance information, traffic statistics, VLAN information, 3onedata ring and spanning tree port status of the specified switch devices.

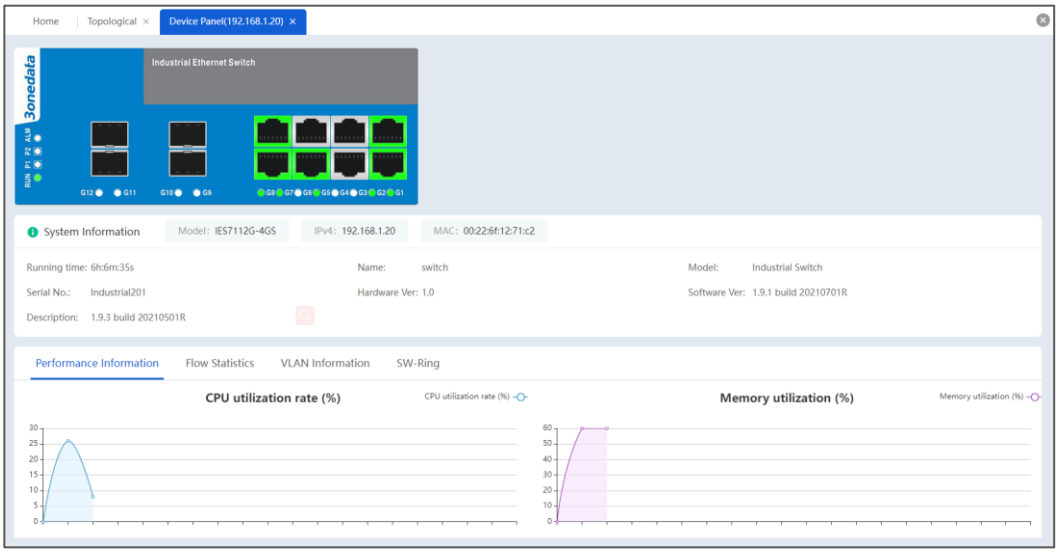
- Panel information includes common logical panel and customized physical panel.
  - The logic panel is the default panel, which is automatically arranged according to the port number.
  - The layout of the physical panel is the same as the actual port of the device. The developer completes the template development according to the actual situation of the device panel, and then uploads it through the system to take effect. The physical panel also supports logo and other customized information.
- The system information comes from the relevant parameters configured by the switch device itself. BlueEyesView will read the information parameters of the device periodically. If the relevant parameters are not defined, it will not be displayed.

Operation Path

In the "Topology Diagram" interface, double-click the switch device icon to enter the switch device panel.

Interface Description

The interface of the device panel is shown in the figure below:



The element description of Device Panel interface:

Interface Element	Description
Model	Only the defined device models are displayed, and the corresponding model can be selected in the device management menu.
IPv4	The IPv4 address information of the device. If it is a layer 3 device, the IP address information of all kinds of layer 3 interfaces will be displayed.
MAC	The MAC address information of this device.
Device status	The current alarm status of the device, including normal, general, important, serious, offline, etc.
Device Panel	The device panel provides logical panel and physical panel, in which the port type and status are represented by different icons and colors. •  : indicates that the port type is copper port; •  : indicates that the port type is SFP fiber port; •  : indicates that the port type is 1×9 fiber port; • Green: indicates that the port is connected; • Gray: indicates that the port is disconnected. Note: Move the mouse to the port to view • The port number, port name, connection status, rate, physical address, RX/TX bandwidth utilization and other information of the port. • The device name, IP and port number of the connected peer

Interface Element	Description
	device; if the port is an optical module, the real-time temperature, voltage, current, input power and output power of the module will be displayed.
System Information	**System Information State Bar**
Running time	The current device's running time after startup.
Name	The name or network ID of the device.
Model	Model of the device.
Serial No.	Device SN.
Hardware Ver	Hardware version information of the device.
Software Ver	Software version information of the device.
Description	Related description information of the device.
Performance Information	**Performance Information State Bar**
CPU Utilization (%)	The CPU utilization of the device is dynamically displayed in blue line chart. Click the icon to close the display.
Memory Utilization (%)	The Memory utilization of the device is dynamically displayed in purple line chart. Click the icon to close the display.
Flow Statistics	**Status bar of received and transmitted flow statistics**
Port	Display the number of the device interface in sequence.
Number of bytes	Number of bytes sent / received by port.
Unicast message	Number of unicast messages sent / received by the port.
Multicast message	Number of multicast messages sent / received by the port.
Broadcast message	Number of broadcast messages sent / received by the port.
Discarded Packets	Number of dropped packets sent / received by the port.
Error packet	Quantity of error packets transmitted/received by the port.
VLAN information	**VLAN Information State Bar**
VLAN ID	VLAN ID number.
VLAN name	VLAN ID name or description information.
Access port	Access port member.
Untagged port	Untagged port member.
Tagged port	Tagged port member.
Status	VLAN Status.
STP Port State	**STP Port State Bar (STP needs to be enabled first)**
Port	Display the number of the device interface in sequence.

Interface Element	Description
Priority	Port priority.
Status	Port status in spanning-tree.
Enable	Port enable status.
Path Cost	The path cost from network bridge to root bridge.
Designated Root	The bridge ID of the root bridge.
Designated Cost	The path cost from this port to the root bridge.
Designated Bridge	The bridge ID of the designated bridge.
Designated Port	The port ID with which the designated bridge interacts.
Forward Transitions	Forwarding status.
SW-Ring	**SW-Ring Status Bar (SW-Ring needs to be enabled first)**
Group ID	Ring group ID.
Ring ID	Ring Network ID. When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Local Port	Local port number of ring port 1/ring port 2.
Remote port	Port number of the opposite end of ring port 1/ ring port 2.
Remote MAC	MAC address of the opposite end of ring port 1/ ring port 2.
Status	Port state of Ring Port 1/Ring Port 2.
Ring Status	SW-Ring state.

6.2.2.2 Wireless Device Panel

Function Description

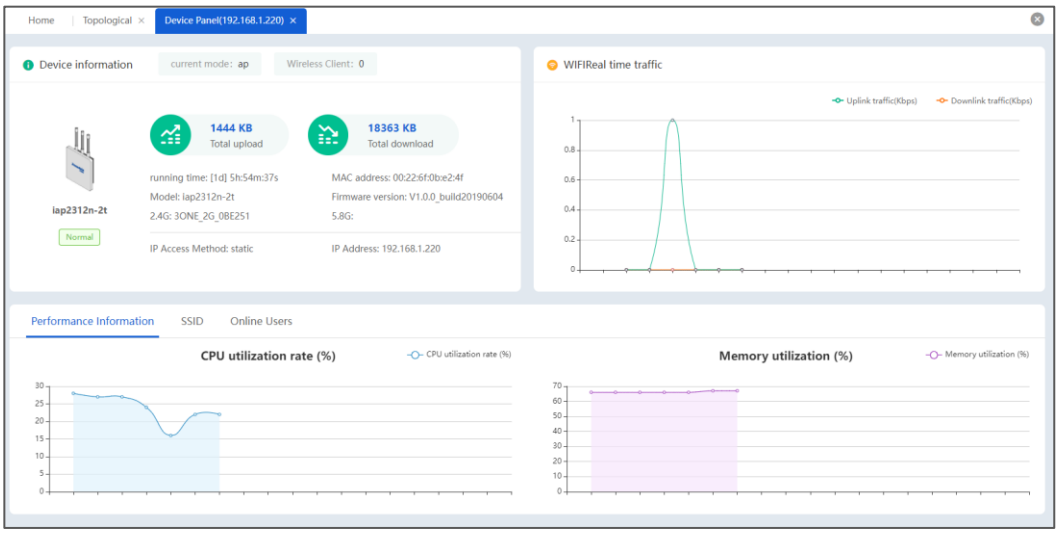
In the wireless device panel, you can view the WiFi up/down real-time traffic of the wireless device; View the information of wireless devices, wireless users and wireless networks; CPU utilization and memory utilization of wireless devices; Details of online users.

Operation Path

In the "Topology Diagram" interface, double-click the wireless device icon to enter the wireless device panel.

Interface Description

The interface of the wireless device panel is shown in the figure below:



The element description of wireless device panel interface:

Interface Element	Description
Device information	**Wireless Device Basic Information Bar**
Current Mode	Working mode of wireless device, such as AP.
Wireless Client	The number of wireless devices currently accessed.
Device information	**Equipment information column.**
Total upload	Total traffic of WiFi upload.
Total download	Total traffic of WiFi download.
Running time	The running time of wireless device after power on.
MAC address	The MAC address information of this wireless device.
Model	Only the defined wireless device model is displayed, and the corresponding model can be selected from the device management menu.
Firmware version	Software version number of the wireless device.
2.4G	WiFi name of 2.4G band.
5.8G	WiFi name of 5.8G band.
IP Access Method	IP acquisition of wireless devices. Such as static acquisition, dynamic acquisition.
IP Address	The IP address of the wireless device.
WiFi real time traffic	**WiFi real time traffic status bar**
Uplink traffic	Real-time monitoring of wireless device WiFi uplink traffic (kbps), which is dynamically displayed in green curve.
Downlink traffic	Real-time monitoring of wireless device WiFi downlink traffic (kbps), which is dynamically displayed in orange curve.

Interface Element	Description
Performance Information	**Performance Information State Bar**
CPU Utilization (%)	The CPU utilization of the wireless device is dynamically displayed in blue line chart. Click the icon to close the display.
Memory Utilization (%)	The Memory utilization of the wireless device is dynamically displayed in purple line chart. Click the icon to close the display.
SSID- 2.4G/ 5.8G	**Wireless information-2.4g/5.8g information column (subject to the frequency band actually supported by the device)**
Switch	Wireless switch status, used to enable 2.4G or 5.8G wireless Wi-Fi network.
Hidden SSID	After enabled, name of SSID from the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Channel	Working channel of wireless network, default "auto" self-adaptation.
Bandwidth	Wireless network channel bandwidth.
Transmitting power	Transmission power of device wireless signal.
Max Links	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.
SSID	Name of wireless network.
Encryption	The encryption method of wireless network.
Password	Password of wireless network.
SSID - Advanced Settings	**Wireless information - Advanced settings information bar**
Short GI	Enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. After disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.

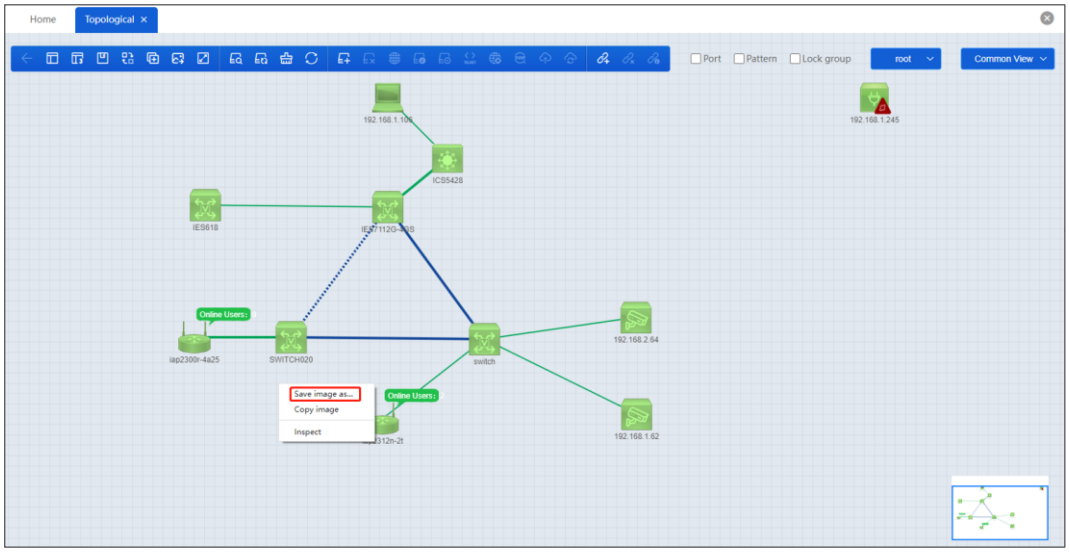
Interface Element	Description
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN.
WMM	After enabling WMM function, the device can process the data packet with priority level, improving the data transmission performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements.
Wireless isolate	After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
Fragment threshold	Fragment threshold of data frame. The data frame will be segmented when its length surpasses fragment threshold.
RTS	Packet RTS (request to send) threshold. The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to response the device, which represents the two stations can conduct wireless communication.
Country	Applied countries and regions of wireless network. Different countries and regions have different open channels.
Authentication method	Wireless network authentication methods, such as personal version of WPA-PSK / WPA2-PSK, enterprise version of WPA-802.1X / WPA2-802.1X authentication.
Online Users	**Online User Information Bar**
Connection Type	The connected wireless frequency band, such as 2.4G and 5.8G.
User IP	IP address of wireless user.
User MAC	MAC address of wireless user.
Username	Device name of wireless user.
Signal	Signal strength received by wireless users. The greater the value, the stronger the signal.
Upload (KB)	Real time traffic of WiFi uplink for wireless users.
Download (KB)	Real time traffic of WiFi downlink for wireless users.
User online time	The time when a wireless user accesses a wireless device.

6.2.3 Save and Copy Topology

Operation Path

In the blank space of the "Topology Diagram" page, right-click to open the shortcut menu. You can choose to save, copy or check the topology diagram.

Interface Description



Element description of shortcut menu:

Interface Element	Description
Save image as	Save the topology diagram in "*. PNG" format.
Copy image	Paste the diagram into the file by "Ctrl + V".
Inspect	Open the code check for the topology diagram.

6.3 Quick Start

Function Description

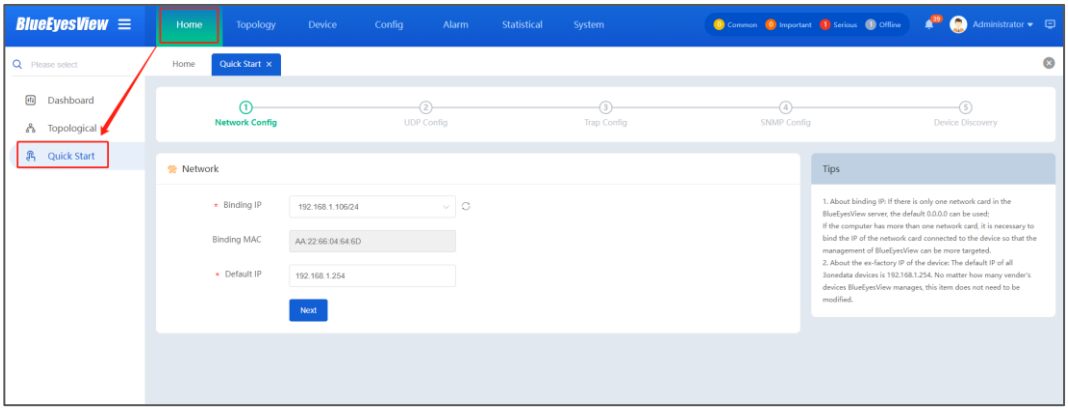
"Quick Start" is a quick start function of the system. When users use BlueEyesView for the first time, they will open it by themselves and guide users to complete a series of operations step by step: Network Card Binding, UDP Configuration, Trap Configuration, SNMP Configuration and Device Discovery. After device discovery is completed, it would automatically switch to the topology.

Operation Path

Open in order: “(Menu Bar) Home > (Navigation Bar) Quick Start”.

Interface Description

Screenshot of Quick Start interface:



Configuration description of Quick Start:

Interface Element	Description
Network Config	See 12.2.1 Network
UDP Config	See 12.2.2 UDP
Trap Config	See 12.2.4 Overview
SNMP Config	See 12.2.3 SNMP General
Device Discovery	See 7.2.1 Device Discovery

7 Topology Management

7.1 Network Management

7.1.1 Network Maintenance

Function Description

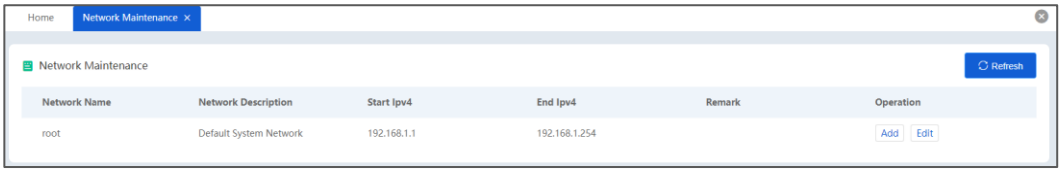
In the "Network Maintenance" page, you can view, modify or add network or sub network information. If the network is complex and contains core network and multiple subnets, and each subnet contains a large number of devices, it is recommended to add the subnet data corresponding to the actual network in this function according to the actual network situation. In this way, after rediscovering the network, the devices in the subnet will be automatically classified into the subnet according to their IP, which makes the topology look clearer, simpler and closer to the reality.

Operation Path

Open in order: "(Menu Bar)Topology > (Navigation Bar) Network > (Navigation Bar) Network Maintenance".

Interface Description 1: Network Maintenance

Screenshot of network maintenance interface:



Element description of network maintenance interface:

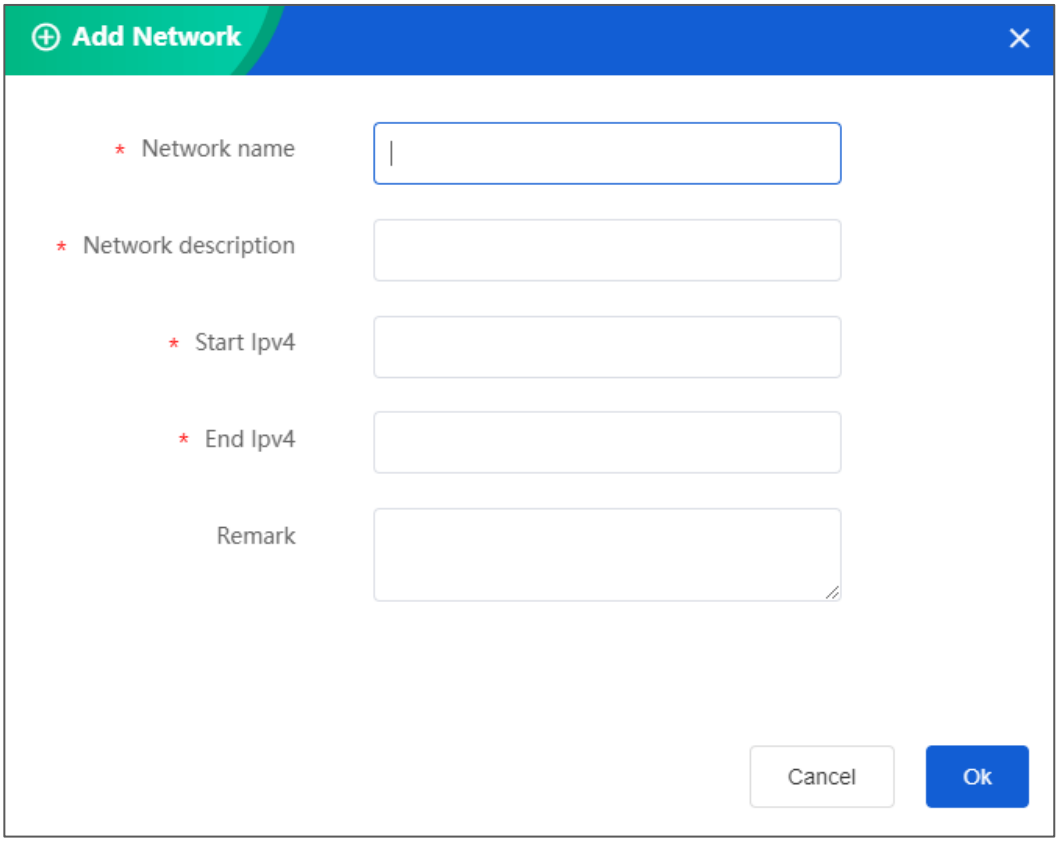
Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Network name	The name of the current network. A default network is built in the system, and the network name is root.
Network description	Description information of the network.
Start IPv4	The start address of the network IPv4 address range.

Interface Element	Description
End IPv4	The end address of the network IPv4 address range.
Remark	Remark information of the network.
Operation	The operation button options are as follows: • Add: click “Add” button to add a subnet of the current network. • Modify: click “Modify” button to modify the current network or subnet information. • Delete: click "Delete" button to delete the subnet of the current network. The deleted network cannot contain subnets and associated devices, otherwise it cannot be deleted.

Interface Description 2: Add Network

Click “Add” button to enter Add Network interface.

Screenshot of Add Network interface:



Element description of Add Network interface:

Interface Element	Description
Network name.	The name of the network. Required, no more than 20 characters.

Interface Element	Description
	Note: One character contains one letter, number or Chinese character.
Network description	Description information of the network. Required, no more than 100 characters.
Start IPv4	The start address of the network IPv4 address range. Required, IPv4 address format, such as 192.168.1.1. The IP address range of each network cannot be repeated.
End IPv4	The end address of the network IPv4 address range. Required, IPv4 address format, such as 192.168.1.254. The end IPv4 address and the start IPv4 address should be in the same network segment and the end IPv4 address should be larger than the start IPv4 address.
Remark	Remark information of the network. Not required, no more than 100 characters.

7.1.2 Subnet Device Management

Function Description

In the "Subnet Device Management" page, you can replan the device list and root device in the network.

Operation Path

Open in order: "Topology Management > Network Management > Subnet Device Management".

Interface Description 1: Subnet Device Management

Screenshot of Subnet Network Device Management interface:

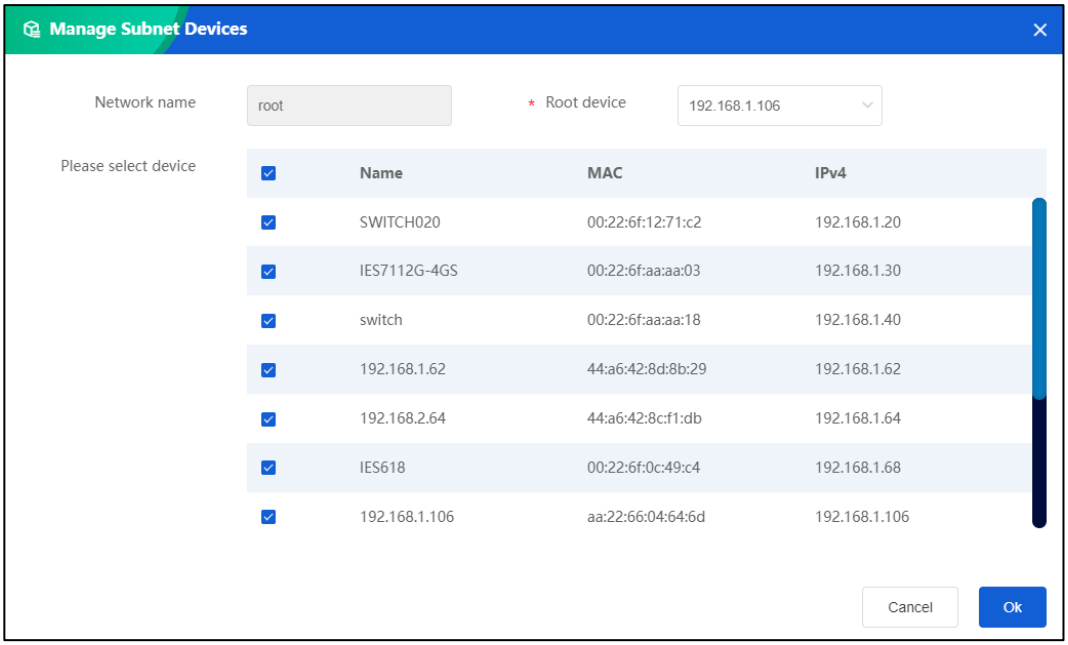
Element description of Subnet Network Device Management interface:

Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Management	Click the “Manage” button to manage the list of network devices and root devices.
Network list	Select a different network and its corresponding device list will be displayed.
Name	Display the device name.
MAC	The MAC address information of this device.
IPv4	The IPv4 address information of this device.
Root	The root device refers to the first device to be displayed when the current network is displayed in the topology diagram. There is only one root device in a network or subnet. When generating the network topology, the system uses the network device with the smallest IP address as the root device, and then creates the network topology from the root device.
Operation	The operation button options are as follows: • Delete: click "Delete" ” button to delete devices in the current network.
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

Interface Description 2: Manage Subnet Device

On the "Subnet Device Management" page, click the "Manage" button to enter the current subnet root device management interface.

Screenshot of Subnet Device Management interface:



Element description of Subnet Device Management interface:

Interface Element	Description
Network name.	The name of the current network.
Root device	From the drop-down list of Root Device, you can select a device as the root device.
Please select device	In the selection area, you can view the list of devices. You can add or delete devices in the current network by checking or unchecking the check box before devices.

7.1.3 Topology Connection Management

Function Description

On the "Topology Connection Management" page, you can customize the topology connection between devices, mainly for devices that do not support LLDP protocol.

Operation Path

Open in order: "Topology > Network > Topology Links ".

Interface Description 1: Topology Links

Screenshot of Topology Topology Links interface:

Element description of Topology Connection Management interface:

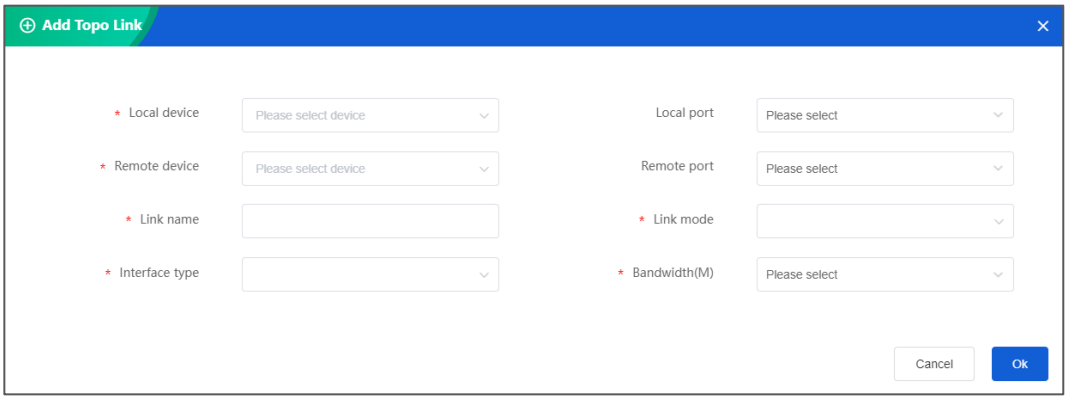
Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click “⊕Add” to create a new device link in the topology.
Network list	Select a different network and its corresponding link list will be displayed.
Local device	Name of the local device.
Local IP	IP address of the local device.
Local port	The port number of the local device connection.
Remote device	Name of the remote device.
Remote IP	IP address of the opposite end.
Remote port	The port number of the opposite end connection.
Link name	Link name, which is composed of device IP address and port number by default.
Link Mode	The network properties of the link support the following types: • Common; • SW-Ring: SW-Ring private ring protocol link; • STP / RSTP / MSTP: spanning tree ring protocol link. • Wireless.
Interface type	The transmission medium of the connection interface supports the following types: • Optical fiber; • Network cable; • unknown; • Wireless.

Interface Element	Description
Bandwidth(Mbit/S)	The link transmission bandwidth supports the following types: • 10Mbit/s; • 100Mbit/s; • 1000Mbit/s; • 10000Mbit/s;
Remark	Remark information of the link.
Operation	The operation button options are as follows: • Modify: click “Modify” to modify the link. • Delete: click “Delete” to delete the link.

Interface Description 2: Add Topology Connection

On the topology connection management page, click “⊕Add“ to enter the interface of Add Topology Connection. If the device does not support SNMP protocol or LLDP protocol, the device would have no link display after it is discovered by the system. At this time, you can add links for devices by manually adding topology connections.

Screenshot of Add Topology Connection interface:



Element description of Add Topology Connection interface:

Interface Element	Description
Local device	Click the drop-down list of “Local Device” and select the local device to which the link is connected.
Local port	Click the drop-down list of “Local Port” and select the local device port to which the link is connected. This option is not required. If the device does not support SNMP or LLDP protocols, the port data will not be able to be read.
Remote device	Click the drop-down list of “Opposite End” and select the Remote device to which the link is connected.
Remote port	Click the drop-down list of “Opposite Port” and select the local

Interface Element	Description
	device port to which the link is connected. This option is not required. If the device does not support SNMP or LLDP protocols, the port data will not be able to be read.
Link name	Link name, no more than 100 characters.
Lik mode	Link type supports the following options: • Common; • SW-Ring: SW-Ring private ring protocol link; • STP/RSTP: spanning tree ring protocol link; • Wireless.
Interface type	Interface type supports the following options: • Optical fiber; • Network cable; • unknown; • Wireless.
Bandwidth (M)	The link transmission bandwidth supports the following options: • 10Mbit/s; • 100Mbit/s; • 1000Mbit/s; • 10000Mbit/s;
Remark	The link remark information, no more than 100 characters.

Note

The communication link has no direction. For a link, the local end and the opposite end are relative. If both devices support LLDP and two pieces of link data are read from the same link, the only difference between them is that the local end and the opposite end are exchanged. It's essentially the same link.

7.2 Topology Discovery

7.2.1 Device Discovery

Function Description

On the page of “Device Discovery”, user can configure the following four device discovery methods.

- 3onedata Discovery: based the second and third generation 3onedata private

network management protocols;

- Intelligent Discovery: Based on common standard protocol ICMP/ARP/SNMP discovery;
- Designated IP Range Discovery: Discover devices within the designated IP range based on ICMP / ARP / SNMP;
- Trap Discovery: Discover devices based on trap information received. When the system receives the SNMP trap information from the unknown device, it adds the device to the network topology according to the device information in the trap information.
- Timing Discovery: Periodically perform device discovery tasks.

3onedata Discovery, Intelligent Discovery and IP Address Range Discovery have been described in the chapter "Network Topology Discovery" of "Topology Diagram", which will not be described here. Trap Discovery and Timing Discovery are described below.

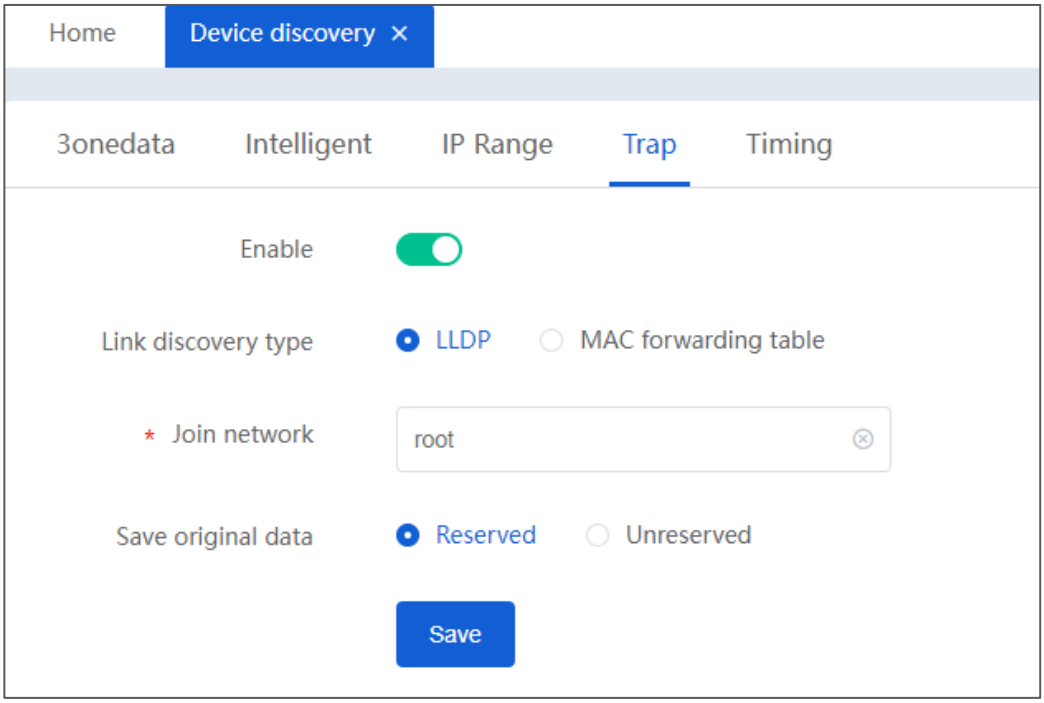
Operation Path

Open in order: "(Menu Bar) Topology > (Navigation Bar) Topology > (Navigation Bar) Device Discovery".

Interface Description 1: Trap Discovery

In the device discovery page, select the "Trap Discovery" tab to enter the Trap Discovery interface.

Screenshot of Trap Discovery interface:



Element description of Trap Discovery interface:

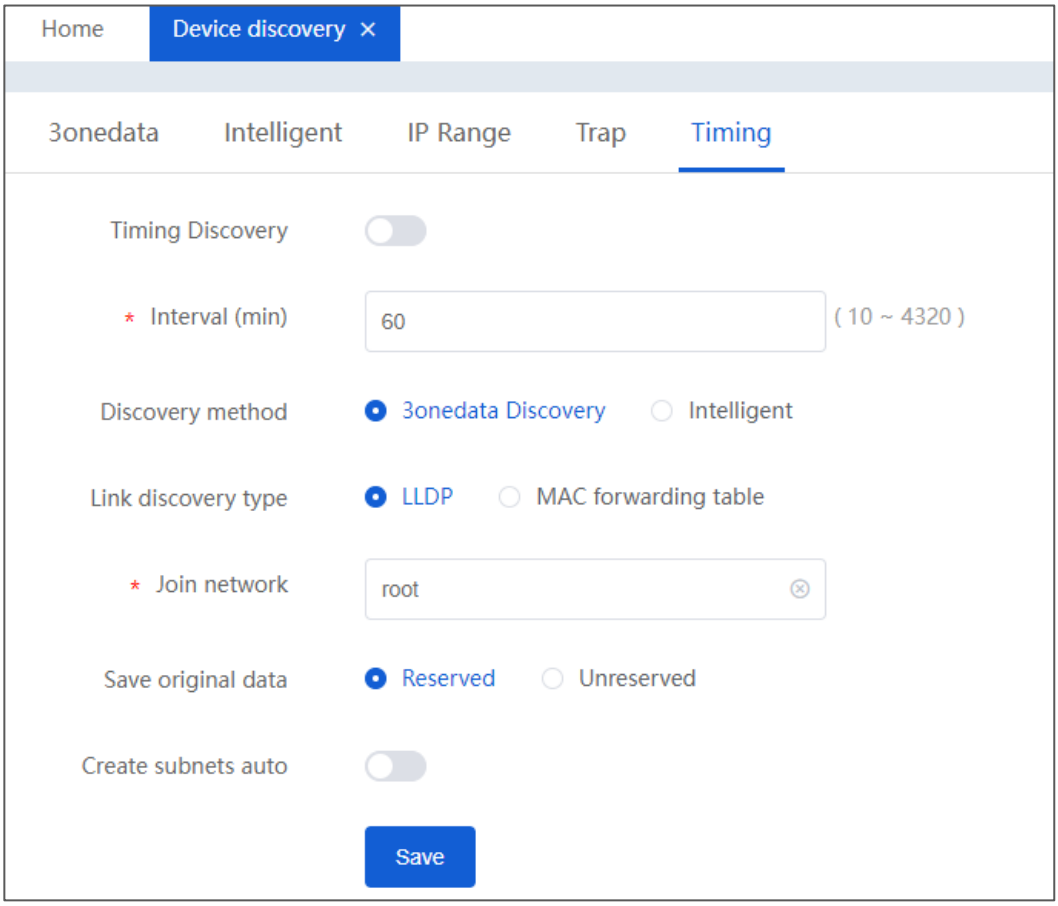
Interface Element	Description
Enable	Trap Discovery switch button, which has triggered device

Interface Element	Description
	discovery by default.
Link discovery type	Link discovery type, options are as follows: • LLDP: Link Layer Discovery Protocol; • MAC forwarding table: device MAC address forwarding list.
Join network	The network to which devices discovered through the protocol will join.
Save original data	Data storage, options are as follows: • Save: Existing or manually added device and link data will be saved in the new network topology diagram. When the original data does not exist, it is displayed with a gray offline icon. • Remove: Re-establish the network topology based on the discovered data and manually added links will be removed.

Interface Description 2: Timing Discovery

In the device discovery page, select the "Timing Discovery" tab to enter the Timing Discovery interface.

Screenshot of Timing Discovery interface:



Element description of Timing Discovery interface:

Interface Element	Description
Timing Discovery	Timing Discovery switch button, disabled by default. When Timing Discovery is enabled, it will periodically discover device and update network topology.
Interval (min)	Time interval of Timing Discovery, unit: minutes.
Discovery method	Discovery methods have the following options: • 3onedata Discovery; • Intelligent Discovery.
Link discovery type	Link discovery type, options are as follows: • LLDP: Link Layer Discovery Protocol; • MAC forwarding table: device MAC address forwarding list.
Join network	The network to which devices discovered through the protocol will join.
Save original data	Data storage, options are as follows: • Save: Existing or manually added device and link data will be saved in the new network topology diagram. When the original data does not exist, it is displayed with

Interface Element	Description
	a gray offline icon. • Remove: Re-establish the network topology based on the discovered data and manually added links will be removed.
Create subnets auto	The feature of automatically creating subnet is disabled by default; And all discovered devices join the specified network automatically. After automatically create subnet is enabled, during 3onedata Discovery and Intelligent Discovery: • When the device IP address found matches the subnet created, the system adds the matching device to the subnet; • When multiple devices in the same network segment do not match the created subnet, the system automatically creates a subnet based on the device IP and adds the device to the subnet. Other devices will join the specified network.

7.2.2 Link Discovery

Function Description

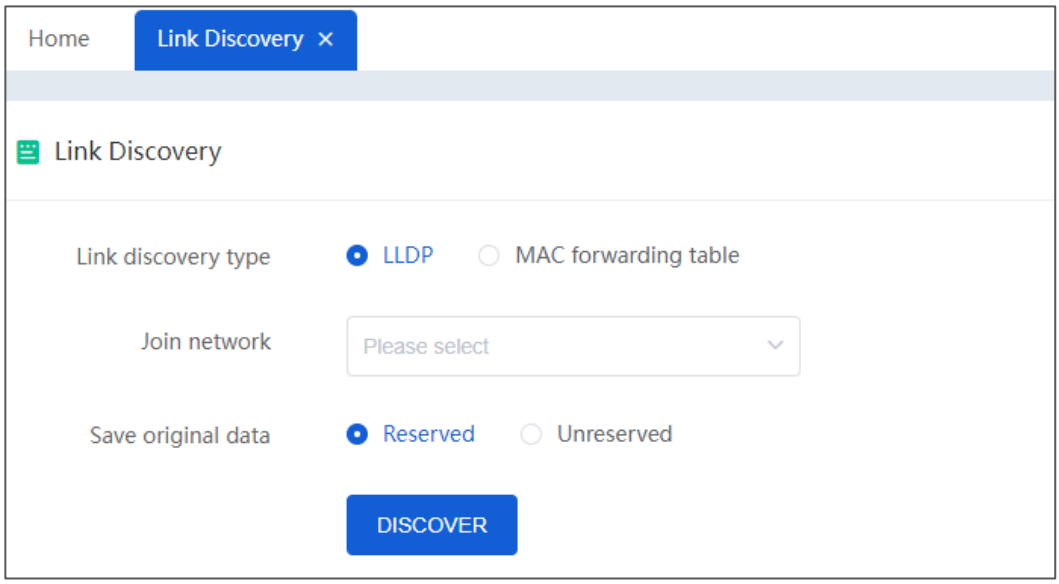
On the “Link Discovery” page, you can rediscover the link. According to the existing devices in the current network, the link between devices is recalculated, but no new devices are found.

Operation Path

Open in order: "(Menu Bar)Topology > (Navigation Bar) Topology > (Navigation Bar) Link Discovery".

Interface Description

Screenshot of Link Discovery interface:



Element description of Link Discovery interface:

Interface Element	Description
Link discovery type	Link discovery type, options are as follows: • LLDP: Link Layer Discovery Protocol; • MAC forwarding table: device MAC address forwarding list.
Join network	The network which the link discovered through the protocol will join.
Save original data	Data storage, options are as follows: • Save: Existing or manually added link data will be saved in the new network topology diagram. When the original data does not exist, it is displayed with a gray offline icon. • Remove: Re-establish the network topology based on the discovered data and manually added links will be removed.

7.3 Panel Management

7.3.1 Panel Configuration

Function Description

On the “Panel Configuration” page, you can view, modify or add device panels. Provide customized physical panel files for some 3onedata devices or customized products.

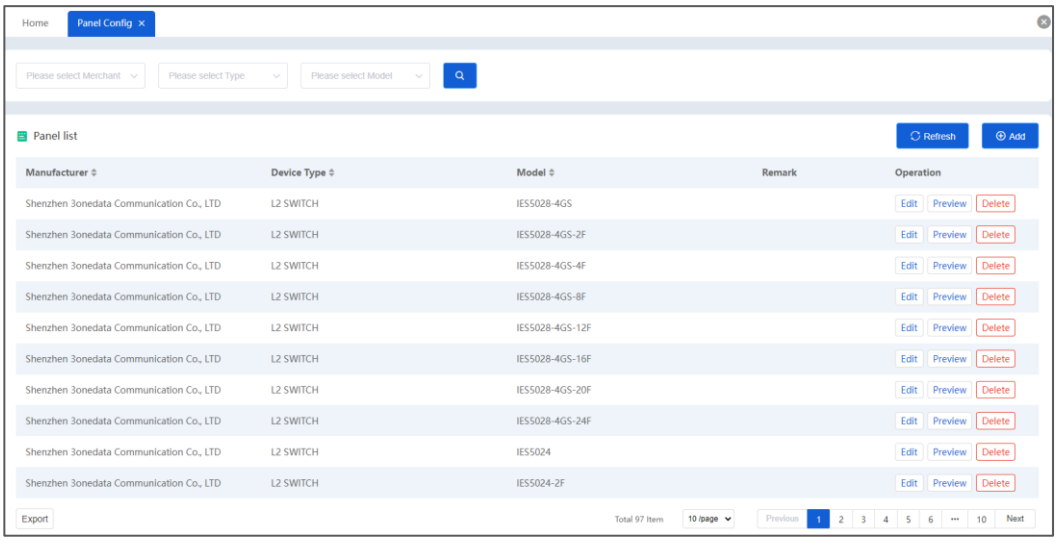
After using the physical panel, when viewing the device panel information, it will be displayed as the physical panel, otherwise it will be the logical panel. The product panel file is saved in the "BlueeyesView\panel" folder by default, and the corresponding panel can be added according to the device model. When you add a new device panel, you need to add the manufacturer, type, model and other related information in "Device Management > Basic Data".

Operation Path

Open in order: "(Menu Bar) Topology > (Navigation Bar) Panel > (Navigation Bar) Panel Config".

Interface Description 1: Panel Configuration

Screenshot of Panel Configuration interface:



Element description of Panel Configuration interface:

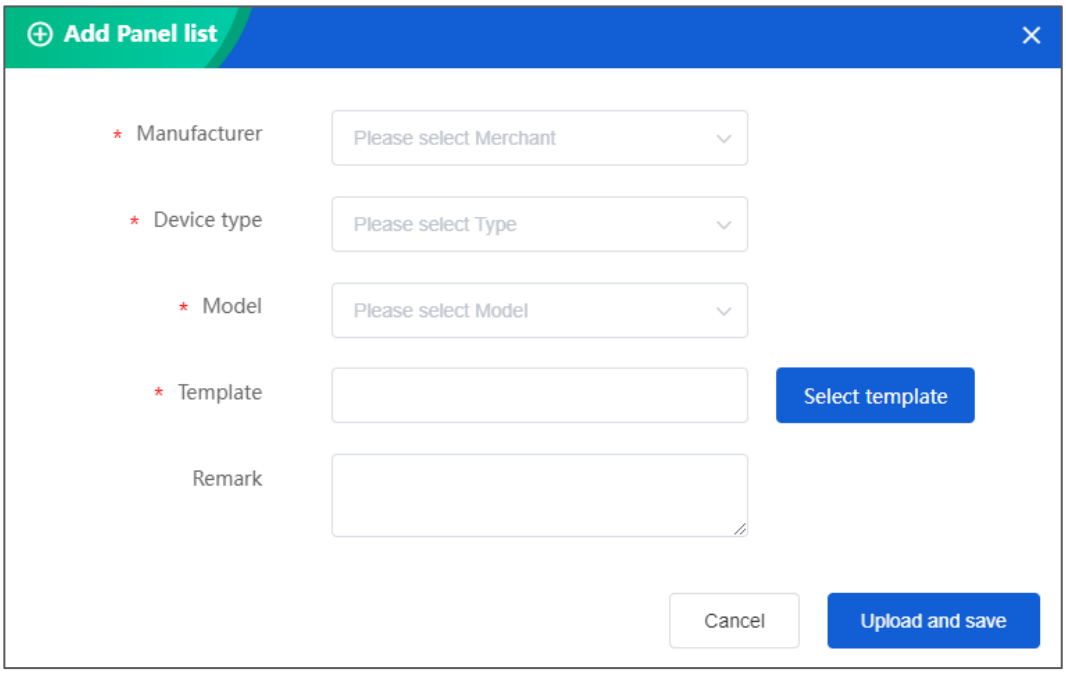
Interface Element	Description
	Click the "  " button to query the panel information of the specified device.
Refresh	Click "Refresh" button to refresh the current page information.
Add	Click the "Add" button to add a device panel.
Manufacturer	Name of device manufacturer or supplier.
Device type	The product type of the device.
Model	Model of the device.
Remark	Remark information of device panel.
Operation	The operation button options are as follows: • Modify: click "Modify" to modify the physical panel of the device.

Interface Element	Description
	• Preview: click “Preview” to view the physical panel of the device. • Delete: click “Delete” to delete the physical panel of the device.

Interface Description 2: Add Panel

On the panel configuration page, click “⊕Add” to enter the add panel interface.

Screenshot of Add Panel interface:



Element description of Add Panel interface:

Interface Element	Description
Manufacturer	Click the drop-down list and select the name of the device manufacturer.
Device type	Click the drop-down list and select the device type.
Model	Click the drop-down list and select the device model.
Template	Click “Select Template” to open the local file dialog box and select the template file in ". ftl" format.
Remark	Remark information of device panel, no more than 100 characters.

Note

- When adding or modifying the device panel, you can contact the customer service

personnel to obtain the template file of the relevant model in advance, and the template file format is ".ftl".

- When adding a new panel, the corresponding manufacturer / type / model should already exist in the list of device models. You can add the manufacturer/type/model by configuring "Device Management > Basic Data".

8 Device Management

8.1 Device

8.1.1 Device List

Function Description

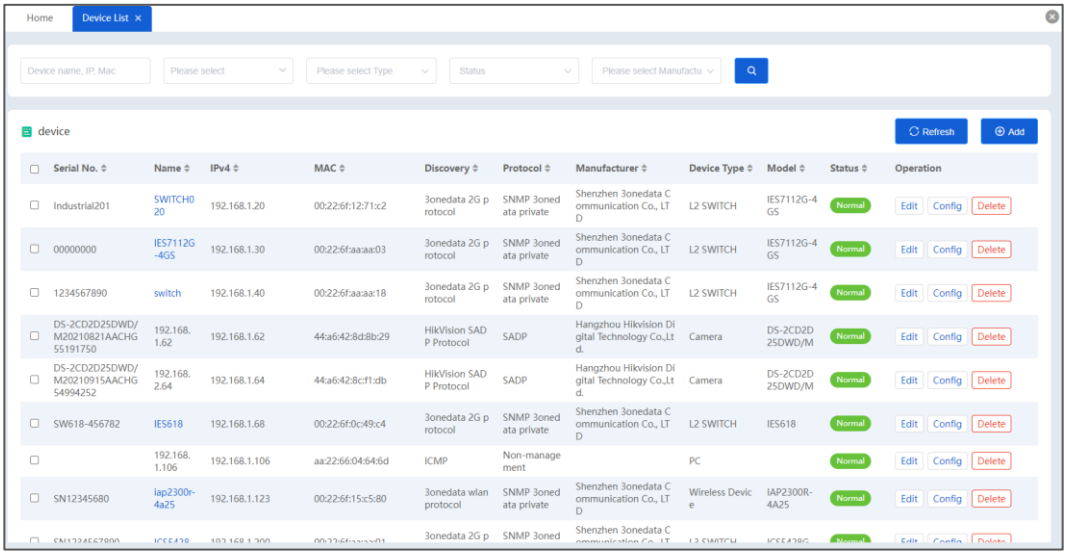
On the "Device List" page, you can view, modify or add various information of the device. The system takes the acquired device system information as the default parameter of the device during device discovery. The modification of device network information here will not involve the change of device parameters. In addition, the device list information supports batch import and export, which can be used as data backup.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Device > (Navigation Bar) Device List".

Interface Description 1: Device List

Screenshot of Device List interface:



Element description of Device List interface:

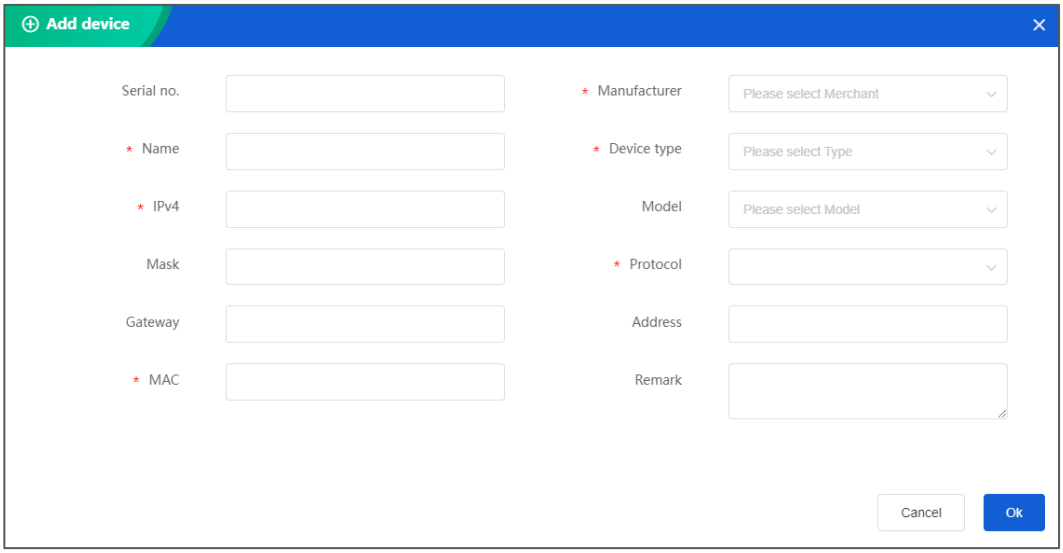
Interface Element	Description
	Click the "  " button to query the information of the specified device. According to the device name, IP address, MAC address and other information, it can match the qualified device information fuzzily, and support the screening of network, device type and device status.
Refresh	Click "Refresh" button to refresh the current page information.
Add	Click the "Add" button to manually add new device information.
Serial No.	SN (product serial number) of the device.
Name	The name of the device. By default, the value read from the node mib2.system.sysname in the device MIB through SNMP protocol is used as the device name. If the value is empty, the IP address of the device is used instead.
IPv4	The IPv4 address of the device.
MAC	The MAC Address of the device.
Discovery	The protocol of discovery device is shown as follows: • ICMP: Internet control message protocol, i.e. universal discovery. • 2nd-generation 3onedata network management protocol: 3onedata private protocol, i.e. 3onedata discovery. • 3rd-generation 3onedata network management protocol: 3onedata private protocol, i.e. 3onedata discovery. The third generation network management protocol adds the discovery of wireless devices. • Manually add: manually added devices.
Protocol	The protocol for managing devices is shown as follows: • SNMP public: devices only support SNMP public MIB. • SNMP 3onedata private: the device supports not only SNMP public MIB, but also 3onedata private MIB. • Private JSON: 3onedata private JSON data protocol. • Non-management: the device does not support SNMP protocol management currently.
Manufacturer	Name of device manufacturer or supplier.
Device type	The product type of the device.
Model	Model of the device.
Status	The status of the device is shown as follows: • Normal: normal, no alarm state; • General: general level alarm; • Important: important level alarm;

Interface Element	Description
	• Serious: serious level alarm; • Offline: the device is offline.
Remark	Remark information of the device.
Operation	The operation button options are as follows: • Modify: click “Modify” to modify the device information. • Delete: click “Delete” to delete the device. • Configure: click the "Configure" button to jump to the "Device Management > Configuration > Basic Configuration" page, and configure the device IP, name, etc.
Download import template	Download and import the device list information template in ". xlsx" file format. The import template contains the device list template and the corresponding manufacturer, type, name and other ID information.
Import	Import the device list information in the file format ". xlsx". To import the equipment list, you need to download the import template first, fill in the device information according to the template requirements, and then import it.
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

Interface Description 2: Add Device

On the Device List page, click “⊕Add” to enter the Add Device interface.

Screenshot of Add Device interface:



Element description of Add Device interface:

Interface Element	Description
Serial No.	SN (product serial number) of the device, which cannot exceed 40 characters.
Name	The name of the device, which cannot exceed 100 characters.
IPv4	The IPv4 address of the device.
Mask	Device subnet mask.
Gateway	Gateway address of the device.
MAC	MAC address of the device. The format of MAC address is as follows: XX: XX: XX: XX: XX: XX: XX.
Manufacturer	Click the drop-down list and select the name of the device manufacturer or supplier.
Device type	Click the drop-down list and select the product type of the device.
Model	Click the drop-down list and select the product model of the device. This item is not required.
Protocol	The protocols of the management device have the following options: • SNMP public: public SNMP protocol MIB database management. • SNMP 3onedata private: 3onedata private SNMP protocol MIB database management. • Private JSON: 3onedata private JSON data packet. • Non-management: i.e. do not support SNMP protocol management.
Address	Installation location information, which cannot exceed 180 characters.
Remark	Remark information of device panel, which cannot exceed 100 characters.

8.2 Wireless Device

In the “Wireless Device” interface, you can view the wireless device list, wireless user list and wireless user log information.

8.2.1 Wireless Device List

Function Description

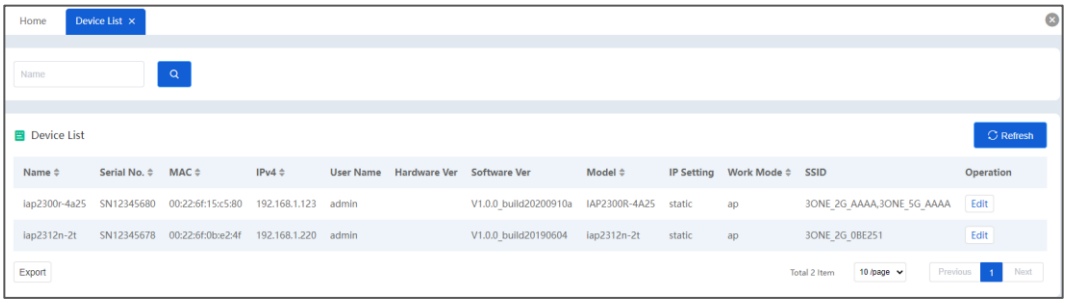
On the "Wireless Device List" page, you can view the operation status of wireless devices in the wireless device list.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Wireless Device > (Navigation Bar) Device List".

Interface Description

Screenshot of wireless device list interface:



Element description of wireless device list interface:

Interface Element	Description
	Query device information according to device name
Refresh	Click “Refresh” button to refresh the current page information.
Name	Name of the wireless device. Note: If there is no device name, the item is displayed as device IPv4.
Serial No.	The number of the wireless device.
MAC	The MAC address information of this wireless device.
IPv4	The IPV4 address information of the wireless device.
User name	User name of the wireless device.
Hardware Ver	Hardware version of the wireless device.
Software Ver	Software version of the wireless device.
Model	Product model of the wireless device.
IP Setting	IP address acquisition method of LAN port of wireless device.
Work mode	Current work mode of wireless device, such as AP.
SSID	SSID name of wireless network, it supports 1-32 characters.
Operation: modify account	Modify the user name and password of the wireless device.

Interface Element	Description
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

8.2.2 Wireless User List

Function Description

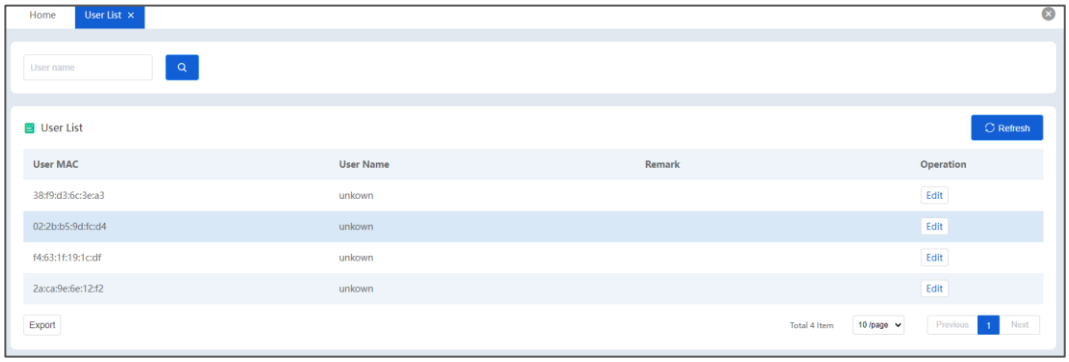
On the "Wireless User List" page, you can see the user information accessing the wireless network; You can modify the user name of the wireless user.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Wireless Device > (Navigation Bar) User List".

Interface Description

Screenshot of wireless user list interface:



Element description of wireless user list interface:

Interface Element	Description
	Query user information according user name
Refresh	Click “Refresh” button to refresh the current page information.
User MAC	MAC address information of the wireless device connected to the wireless network.
User name	Wireless user name connected to the wireless network.
Remark	—
Operation	Modify the wireless user name.

8.2.3 Wireless User Log

Function Description

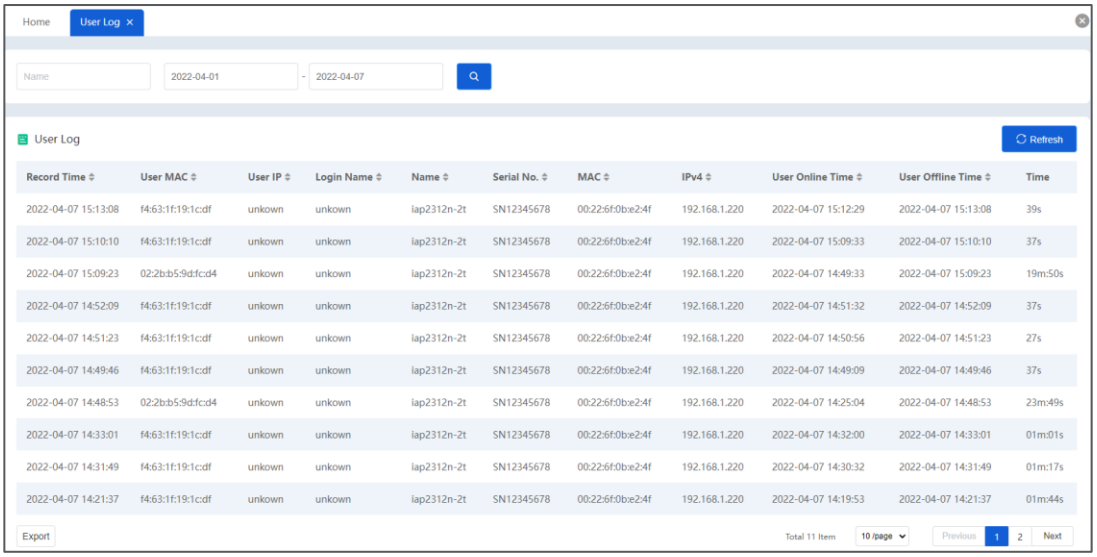
On the "User Log" page, you can view wireless users and their online and offline information.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Wireless Device > (Navigation Bar) User Log".

Interface Description

Screenshot of wireless user log interface:



Element description of wireless device list interface:

Interface Element	Description
	User logs of a time period can be queried.
Refresh	Click “Refresh” button to refresh the current page information.
Record time	Generation time of wireless user log.
User MAC	The MAC address of the wireless user.
User IP	IP address of wireless user.
Login name	Name of wireless user.
Name	The name of the wireless device accessed by the wireless user. Note: If there is no device name, this item is displayed as device IP V4.
Serial No.	The access device number of the wireless user.
MAC	The MAC address information of wireless device accessed by the wireless user.

Interface Element	Description
IPv4	The address information of the wireless device IPv4 accessed by the wireless user.
User online time	The time when a wireless user accesses a wireless device.
User offline time	Time when the wireless user exits the wireless device.
Time	Wireless user online time.
Remark	—

8.3 Basic Data

8.3.1 Manufacturer Management

Function Description

On the "Manufacturer Management" page, you can modify or add manufacturer information.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Basic Data > (Navigation Bar) Manufacturer".

Interface Description

Screenshot of manufacturer management interface:

Element description of manufacturer management interface:

Interface Element	Description
	Click the “  ”button to filter the devices according to the selected information.
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click “Add” to add manufacturer information.
ID	Manufacturer ID number.

Interface Element	Description
Code	Manufacturer's code. The first three sections of the MAC address of the manufacturer's device are used as the manufacturer's code by default. The same manufacturer name or company name can have multiple codes, but the codes cannot be repeated, and the manufacturer or company name can be repeated.
Name	Company name of the manufacturer.
Address	Address information of the manufacturer.
Contact	Name of the manufacturer's contact person.
Tel	Contact number of the manufacturer's contact person.
E-mail	E-mail address of the manufacturer's contact person.
Website	Company website address of the manufacturer.
Remark	Manufacturer management remarks.
Operation	Optional operations are as follows: • Click “Edit” to modify the manufacturer information. • Click “Delete” to delete the manufacturer information.
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

8.3.2 Device Type

Function Description

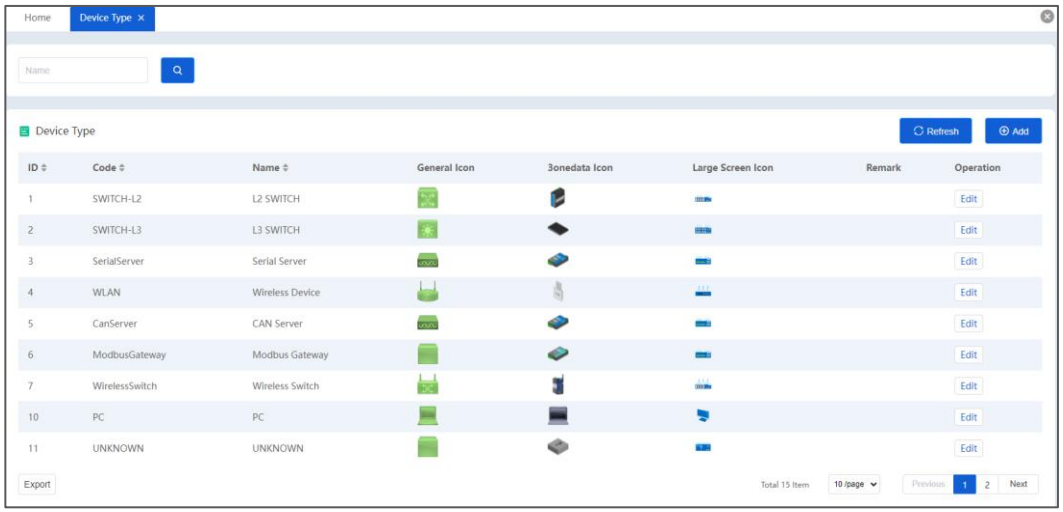
On the “Device Type” page, you can modify or add device type information.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Basic Data > (Navigation Bar) Device Type".

Interface Description

Screenshot of Device Type interface:



Element description of Device Type interface:

Interface Element	Description
	Click the “  ”button to filter the device type according to the selected information.
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click “Add” to add a new device type.
ID	Device type ID number.
Code	Code of device type. Device type codes cannot be the same.
Name	Name of the device type. By default, L2 / L3 switches, serial port servers, wireless routing devices and other device types are supported.
General icon	In general view, the icon displayed for this type of device.
3onedata icon	In 3onedata view, the icon displayed for this type of device.
large screen icon	In the large screen view, the icon displayed for this type of device.
Remark	Remarks of device type.
Operation	Optional operations are as follows: • Click “Edit” to modify the device type information. • Click “Delete” to delete the specified device type. The default type cannot be deleted.
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

8.3.3 Device Model

Function Description

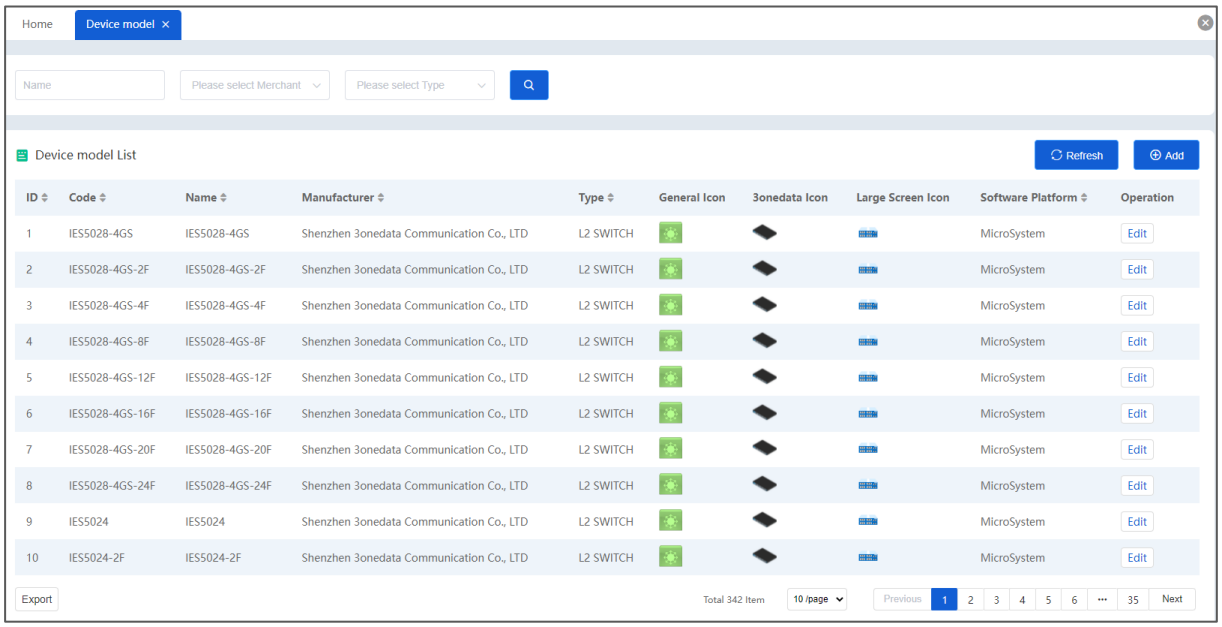
On the “Device Model" page, you can modify or add device model and other information. When adding the device model, ensure that the manufacturer information and device type already exist.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Basic Data > (Navigation Bar) Device Model".

Interface Description

Screenshot of Device Model interface:



Element description of Device Model interface:

Interface Element	Description
	Click the “  ”button to filter the devices according to the selected information.
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click “Add” to add new device models.
ID	ID number of the device model.
Code	The codes of the device model and they cannot be the same.
Name	Product name of the device.
Manufacturer	Name of the manufacturer or supplier of the device.

Interface Element	Description
Type	The product type of the device.
General icon	In general view, the icon displayed for this model of device.
3onedata icon	In 3onedata view, the icon displayed for this model of device.
large screen icon	In large screen view, the icon displayed for this model of device.
Software platform	Software platform of the device.
Remark	Remarks of device type.
Operation	Optional operations are as follows: • Click “Edit” to modify the device type information. • Click “Delete” to delete the specified device type. The default type cannot be deleted.
Export	Export the current list in ". Xlsx" or ". CSV" format. You can modify the file export format under “System Management > System Settings > System Configuration”.

8.3.4 Device Icon

Function Description

On the “Device Icon” page, you can add or delete 3onedata icon library, general icon library and large image icon library.

- 3onedata Icon Library: store the icons displayed in 3onedata view.
- General icon: store the icons displayed in general view.
- Large screen icon: store the icons displayed in large screen view.

Operation Path

Open in order: "(Menu Bar) Device > (Navigation Bar) Basic Data > (Navigation Bar) Device Icon".

Interface Description

Screenshot of Icon Management interface:

Note

- Please add the icon to the corresponding icon library according to the style of the icon.
- It is not allowed to upload pictures with duplicate names in the same icon library.
- Move the mouse over the icon to display the deletion symbol. Click to delete the picture.

9 Configuration Management

9.1 Configuration

9.1.1 Basic Configuration

Function Description

On the "Basic Configuration" page, you can configure the IP address, device name, restore factory setting and restart of 3onedata devices.

Note
Modify the IP address and name of the device, restore factory settings and restart. Only 3onedata devices are supported, and BlueEyesView is in the same LAN as the device.

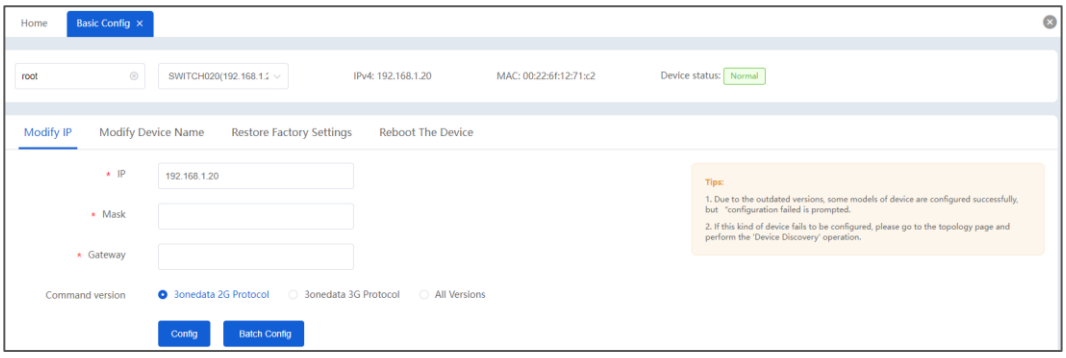
Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Configuration > (Navigation Bar) Basic Configuration".

Interface Description 1-1: Modify IP

On the Basic Configuration page, select the “modify IP” tab to enter the modify IP interface.

Change IP interface screenshots:



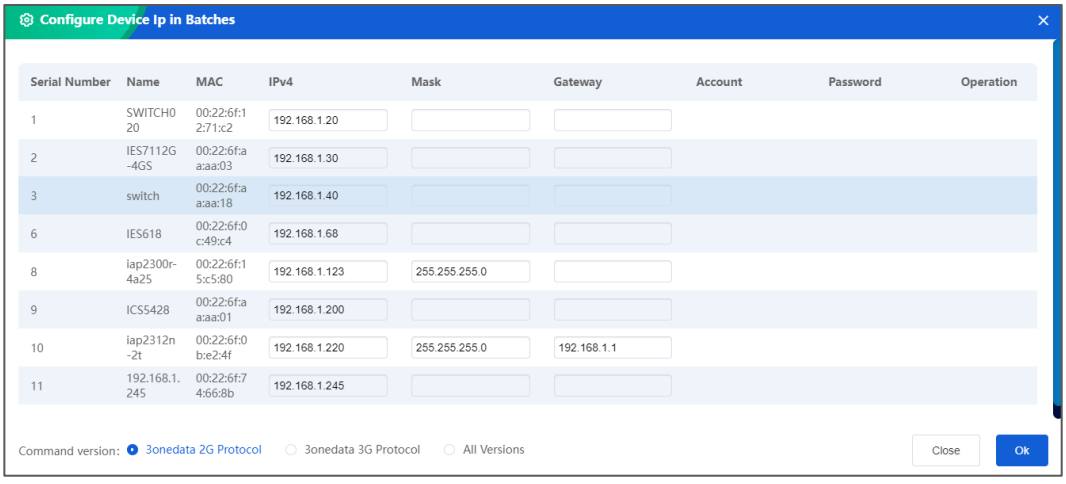
Element description of Modify IP interface:

Interface Element	Description
Please select	Click the drop-down list and select the network where the device is located.
Please select device	Click the drop-down list and select the name of the device.
IPv4	The IPv4 address of the selected device.
MAC	The MAC address of the selected device.
Device status	The alarm status of the selected device.
IP	IPv4 address of the device. The format of IPv4 address is as 192.168.1.254.
Mask	The subnet mask of the device, such as 255.255.255.0.
Gateway	Gateway address of the device, such as 192.168.1.1.
Operation	Optional operations are as follows: • Configure: configure the current device information. • Batch configuration: enter the batch setting page to conduct batch operation of device.

Interface Description 1-2: Batch Configuration of Device IP

On the modify IP page, click “Batch Configuration” to enter the Batch Configuration of Device IP interface. The IP address, subnet mask and gateway of multiple devices can be modified at the same time.

Screenshot of Batch Configuration of Device IP interface:



Element description of Batch Configuration of Device IP interface:

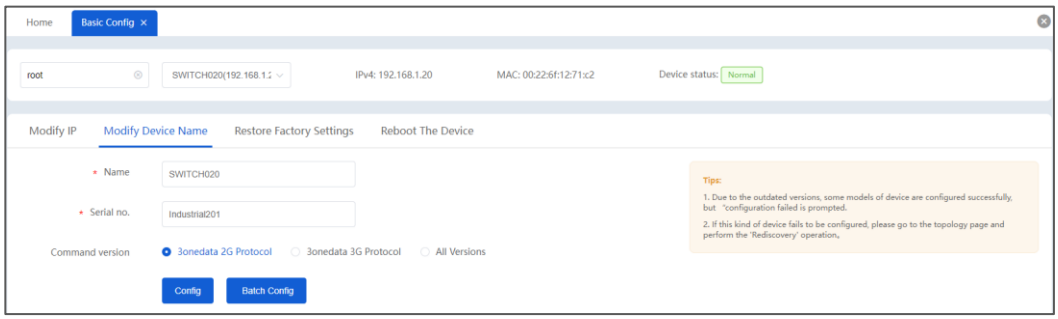
Interface Element	Description
Serial Number	Device list serial number.
Name	Display the device name.
MAC	The MAC Address of the device.

Interface Element	Description
IPv4	IPv4 address of the device. The format of IPv4 address is as 192.168.1.254.
Mask	The subnet mask of the device, such as 255.255.255.0.
Gateway	Gateway address of the device, such as 192.168.1.1.
Operation	Restore: after modifying the IP address, mask or gateway of the device, the "Restore" button is displayed to restore the parameters.

Interface Description 2-1: Modify Device Name

On the basic configuration page, select the “Modify Device Name” tab to enter the modify device name interface.

Screenshot of Modify Device Name interface:



Element description of modify device name interface:

Interface Element	Description
Name	The name of the device, which cannot exceed 20 characters.
Serial No.	SN (product serial number) of the device, which cannot exceed 20 characters.
Operation	Optional operations are as follows: • Configure: configure the current device information. • Batch configuration: enter the batch setting page to conduct batch operation of device.

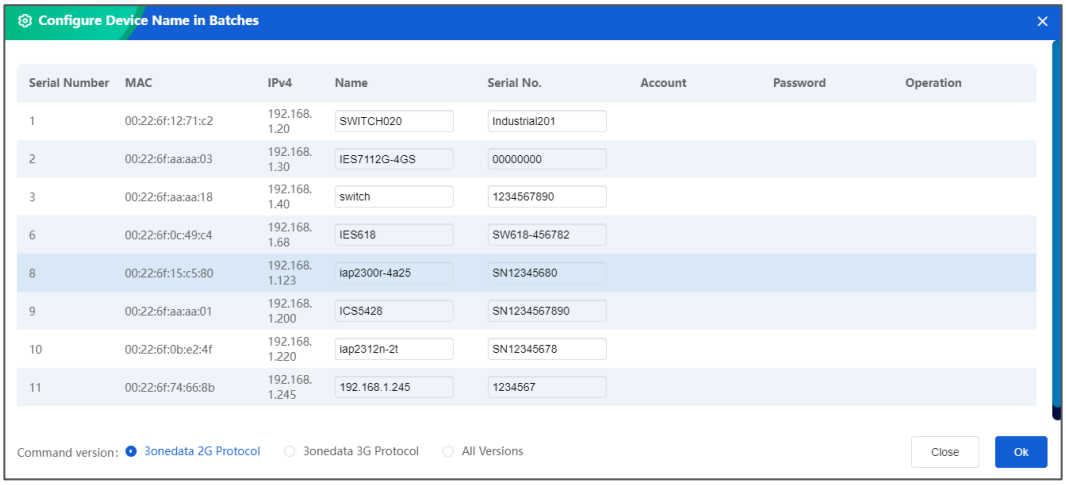
Note

- The device name and SN configuration are related to the device's own system settings.
- The device name defaults to the IP address information of the device in the system, which is different from the default device name in the device's own system. After modification, the device name and SN in the device system will be overwritten.

Interface Description 2-2: Batch Configuration of Device Name

On the modify device name page, click “Batch Configuration” to enter the Batch Configuration of Device Name interface. In the batch configuration device name interface, you can modify multiple device names and device codes at the same time.

Screenshot of Batch Configuration of Device Name interface:



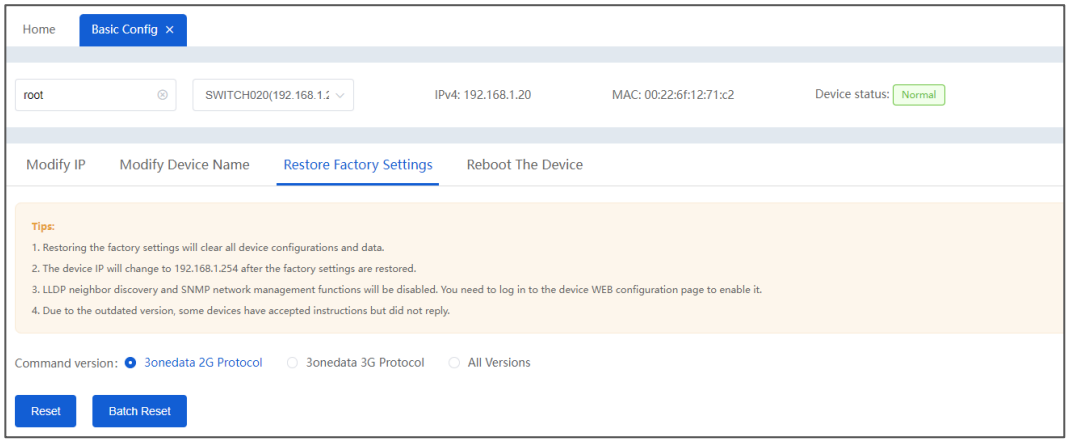
Element description of Batch Configuration of Device Name interface:

Interface Element	Description
Serial Number	Device list serial number.
MAC	The MAC Address of the device.
Name	The name of the device, which cannot exceed 20 characters.
Serial No.	SN (product serial number) of the device, which cannot exceed 20 characters.
Operation	Restore: after modifying the name or code of the device, the "Restore" button is displayed to restore the parameters.

Interface Description 3-1: Restore Factory Settings

On the Basic Configuration page, select the “ Restore Factory Settings” tab to enter the Restore Factory Settings interface.

Screenshot of Restore Factory Settings Interface:



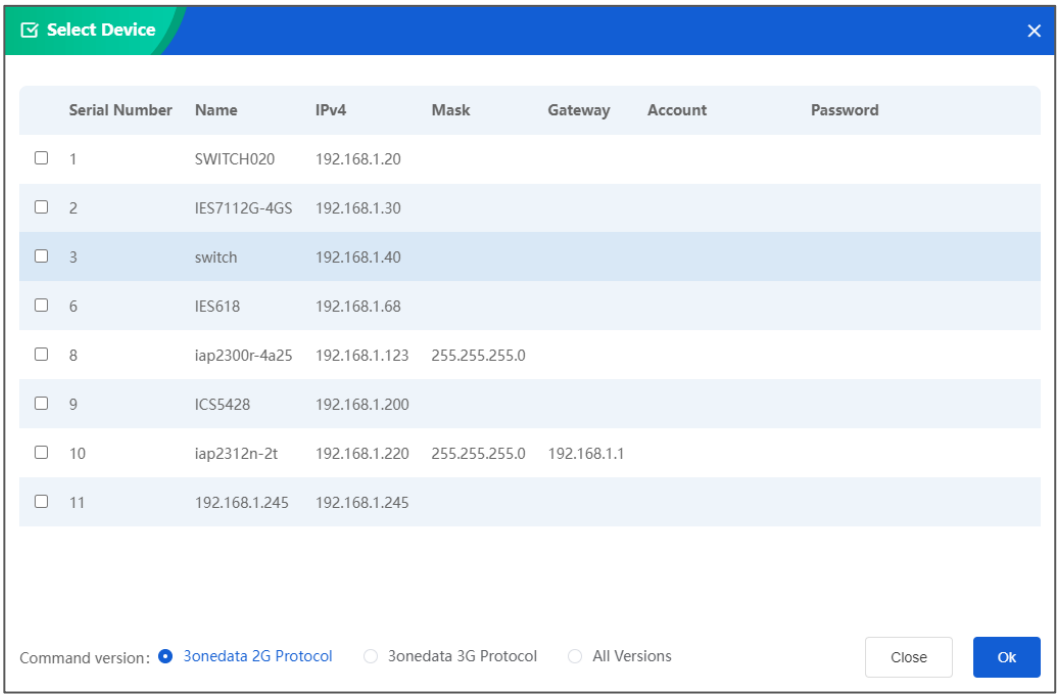
The main element configuration description of restore factory settings interface:

Interface Element	Description
Operation	Optional operations are as follows: • Reset: restore the factory settings of current device. When restoring factory settings, the system will pop up a confirmation dialog box for user to operate; After confirmation, the system will ask to enter the system administrator password for authorization; After authorization, it will restore the factory settings. • Batch Reset: enter the batch settings page to perform batch operation of the device. Notice: When the device is restored to the factory settings, all configured data will be cleared, the IP address of the device will be restored to the default IP address, and the LLDP and SNMP functions will be disabled.

Interface Description 3-2: Restore Factory Settings in Batch

In the interface of restoring factory settings, click " Batch Reset " to enter the interface of device selection. Multiple devices can be selected to restore factory settings at the same time.

Screenshot of Restore Factory Settings in Batch Interface:



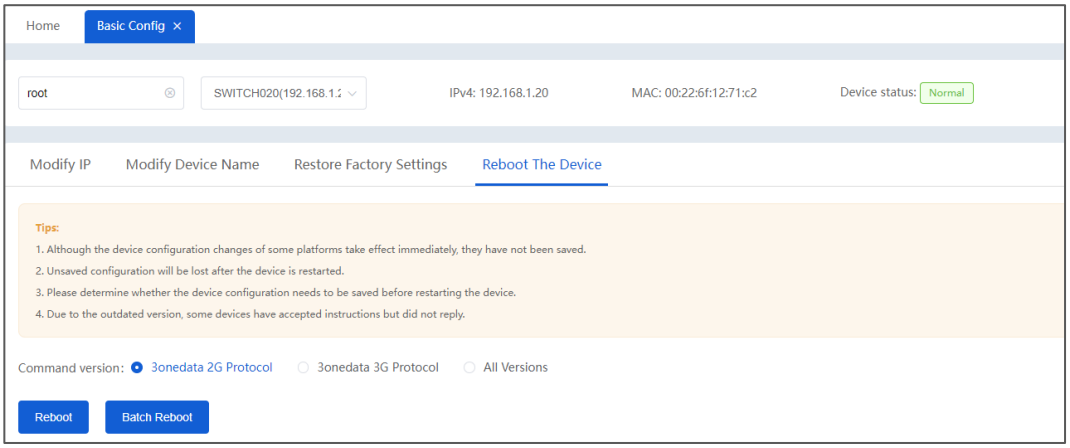
Element description of Restore Factory Settings in Batch interface:

Interface Element	Description
Serial Number	Device list serial number.
Name	Display the device name.
IPv4	The IPv4 address of the device.
Mask	Device subnet mask.
Gateway	Gateway address of the device.
Operation	Check the box in front of the device serial number, and then click “OK”. A confirmation dialog box will pop up for user to operate; After confirmation, the system will ask to enter the system administrator password for authorization; After authorization, multiple devices can be restored to factory settings. Notice: When the device is restored to the factory settings, all configured data will be cleared, the IP address of the device will be restored to the default IP address, and the LLDP and SNMP functions will be disabled.

Interface Description 4-1: Reboot the Device

On the basic configuration page, select the “Device Reboot” tab to enter the Device Reboot interface.

Screenshot of Device Restart interface:



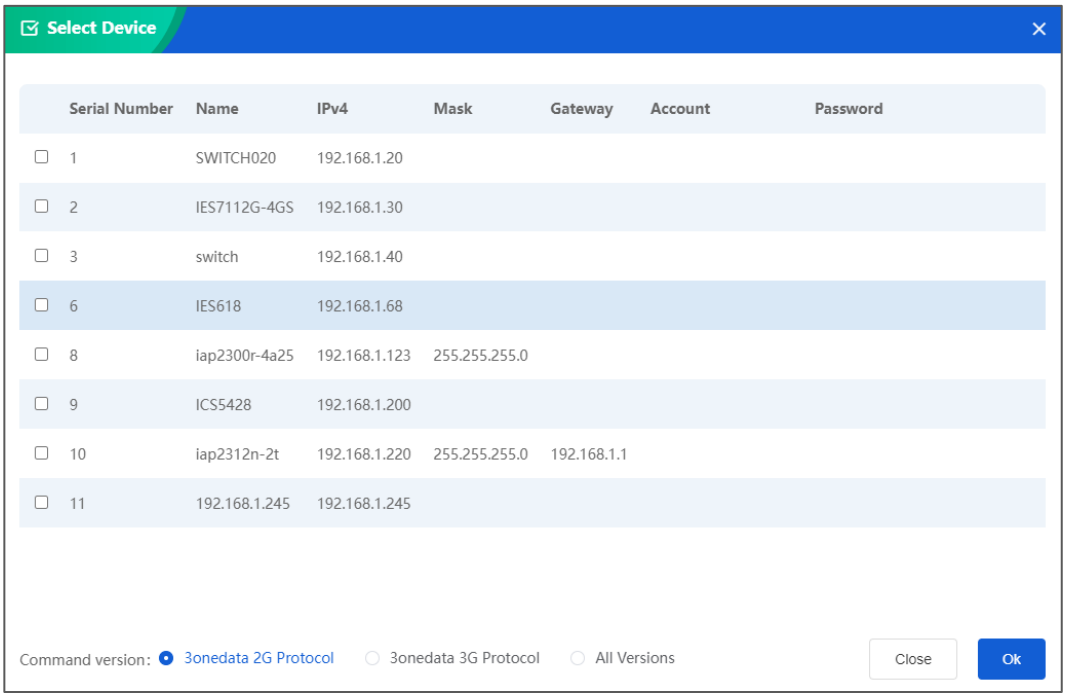
Element description of Device Restart interface:

Interface Element	Description
Operation	Optional operations are as follows: • Reboot: restart the device system. When the device is restarted, the system will pop up a confirmation dialog box for user to operate; After confirmation, the system will ask to enter the system administrator password for authorization; After authorization, it will restart the device. • Batch Reboot: enter the batch setting page to conduct batch operation of devices. Notice: Before restarting the device, please save the current configuration of the device; After restart, the device will run the last saved configuration parameters.

Interface Description 4-2: Batch Device Reboot

In the batch device reboot interface, click “Batch Reboot” to enter the device selection interface. Multiple devices can be selected to reboot at the same time.

Screenshot of Batch Device Restart interface:



Element description of Batch Device Restart interface:

Interface Element	Description
Serial Number	Device list serial number.
Name	Display the device name.
IPv4	The IPv4 address of the device.
Mask	Device subnet mask.
Gateway	Gateway address of the device.
Operation	Check the box in front of the device serial number, and then click “OK”. A confirmation dialog box will pop up for user to operate; After confirmation, the system will ask to enter the system administrator password for authorization; After authorization, you can restart multiple devices. Notice: Before restarting the device, please save the current configuration of the device; After restart, the device will run the last saved configuration parameters.

9.1.2 Telnet/SSH

Function Description

On the “Telnet/SSH” page, the TELNET client access the CLI interface of the device. The telnet client supports all devices that have enabled Telnet service.

Note

When accessing the device through Telnet protocol, the device shall have enabled Telnet service function and access permission in advance; At the same time, BlueEyesView and the device are in the same LAN or reachable by route.

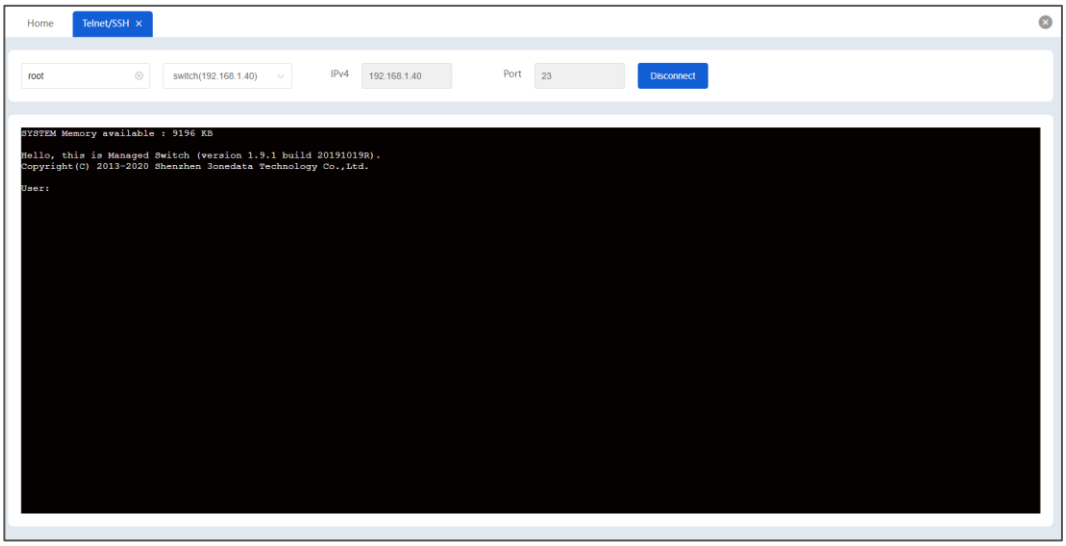
Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Configuration > (Navigation Bar) Telnet/SSH".

Interface Description

On the basic configuration page, select the "Telnet" tab to enter the Telnet interface.

Screenshot of Telnet interface:



Element description of Telnet interface:

Interface Element	Description
IPv4	SN (product serial number) of the device, which cannot exceed 20 characters.
Port	Telnet protocol port number. The default port is 23.
Operation	Optional operations are as follows: • Connect: click the “Connect” button to establish a Telnet connection with the device. • Disconnect: click the “Disconnect” button to disconnect the Telnet connection with the device.

9.1.3 SNMP Configuration

Function Description

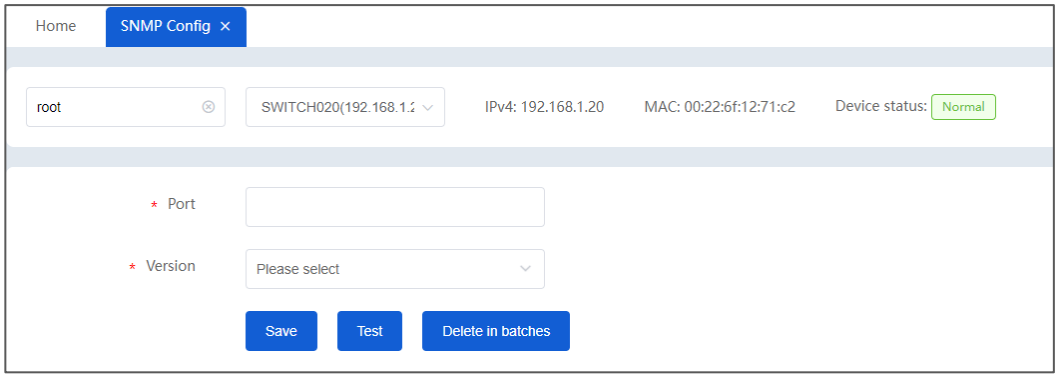
On the “SNMP Configuration” page, you can configure the SNMP protocol information used by the management device. When the device supports SNMP protocol, but its agent port, SNMP version and security mechanism are inconsistent with the default configuration of the system, normal SNMP communication with the system will not be possible. Personalized configuration can be made for such devices.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Configuration > (Navigation Bar) SNMP Configuration".

Interface Description

Interface screenshot of SNMP configuration as follows:



Element description of SNMP configuration interface:

Interface Element	Description
Please select	Click the drop-down list and select the network where the device is located.
Please select device	Click the drop-down list and select the name of the device.
IPv4	The IPv4 address of the selected device.
MAC	The MAC address of the selected device.
Device status	The alarm status of the selected device.
Port	The SNMP protocol listening port of the device is UDP Port 161 by default.
Version	Device SNMP protocol version, with the following options: • v1: use authentication based on community name; • v2c: enhanced on the basis of SNMPv1, it supports more operations, more data types, richer error handling codes and a variety of transmission protocols.

Interface Element	Description
	• v3: added a new security mechanism for authentication service and encryption service.
SNMPv1: v2c authentication	**SNMPv1/v2c authentication information**
Read community	The readable community name, which is used to complete the authentication between Agent and NMS, and supports 4-20 characters. When using SNMPv1/v2c version, it is necessary to fill in the community name for authentication.
Write community	The writable community name, which is used to complete the authentication between Agent and NMS, and supports 4-20 characters. When using SNMPv1/v2c version, it is necessary to fill in the community name for authentication.
SNMPv3 certification	**SNMPv3 authentication information**
Security name	SNMPv3 user name, supporting 4-20 characters.
Security level	SNMPv3 user identity authentication and data encryption level, with the following options: • NOAUTH_ NOPRIV: No authentication and no encryption. • AUTH_ NOPRIV: authentication without encryption. • AUTH_ PRIV: authentication with encryption.
Auth protocol	SNMPv3 user identity authentication protocol, with the following options: • MD5: secure hash function MD5, using 128-bit key as input. • SHA: secure hash function SHA-1, using 160-bit key as input.
Auth password	Authentication password information, supporting 8-20 characters.
Privacy protocol	SNMPv3 user data encryption algorithm, options as follows: • DES: encrypt a 64-bit plaintext block with a 56-bit key. • DES3: use three 56-bit DES keys (total 168-bit keys) to encrypt plaintext. • AES-128: encrypt plaintext using AES algorithm with 128bit key length. • AES-256: encrypt plaintext using AES algorithm with 256bit key length.
Privacy password	Encrypt password information and support 8-20 characters.

Interface Element	Description
Operation	Optional operations are as follows: • Save: Click “Save” to save the SNMP parameters of the current device. • Test: click “Test” to test the SNMP connection between the system and the device. • Delete: click “Delete” to delete the SNMP parameters of the current device. • Copy: click “Copy” to copy the configuration information to the specified device. • Batch delete: click “Batch delete” to delete the SNMP parameters of the specified device. Note: In batch deletion, if only the manufacturer is selected and the device type and device model are blank, it means that all devices of the manufacturer would be selected; If the manufacturer and device type are selected and the device model is blank, it means that all models under the device type of the manufacturer would be selected.

9.1.4 SNMP Query

Function Description

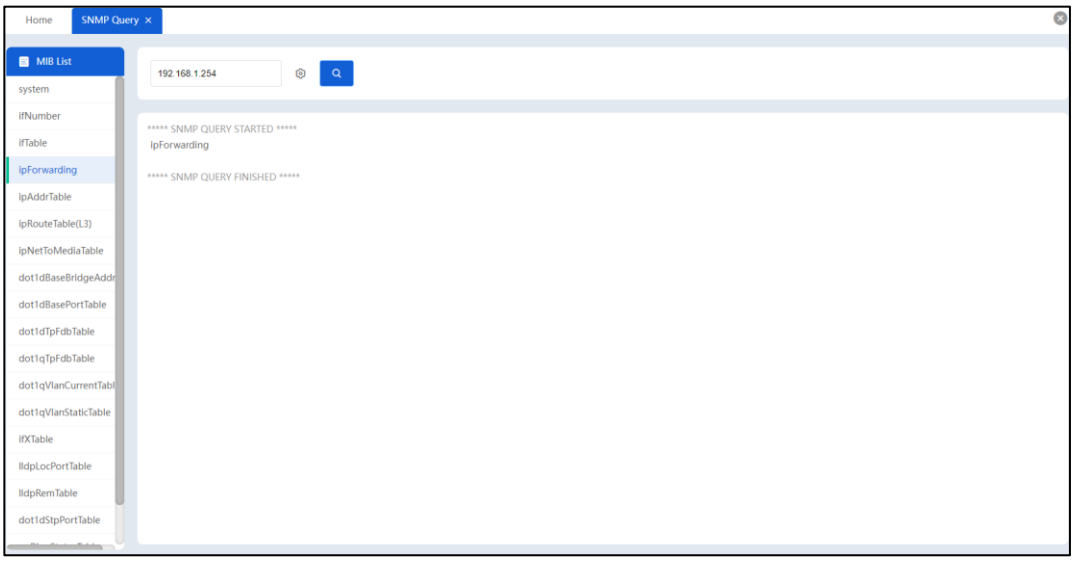
For SNMP query, you can view the device MIB list information through SNMPv1/v2c/v3 protocol.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Configuration > (Navigation Bar) SNMP Query".

Interface Description

Screenshot of SNMP query interface:



Element description of SNMP query interface:

Interface Element	Description
MIB list	MIB (Management Information Base) list contains some data items of managed devices and they can be queried through SNMP protocol. For undefined data items in the list, you can query through the user-defined OID.
IPv4 address	IPv4 address of the queried device.
	After selecting the MIB list data item, click the “  ”button to query the corresponding object information.
	Click the advanced configuration “  ”icon to modify the SNMP protocol port, version, authentication and other related information.
MIB Tree	Enter the query tool of MIB Browser, which allows network and system engineers to load standard or some vendor-specific MIBs, and retrieve data about software and hardware configuration through SNMP agent running on the device.

9.1.5 Network Diagnosis

Function Description

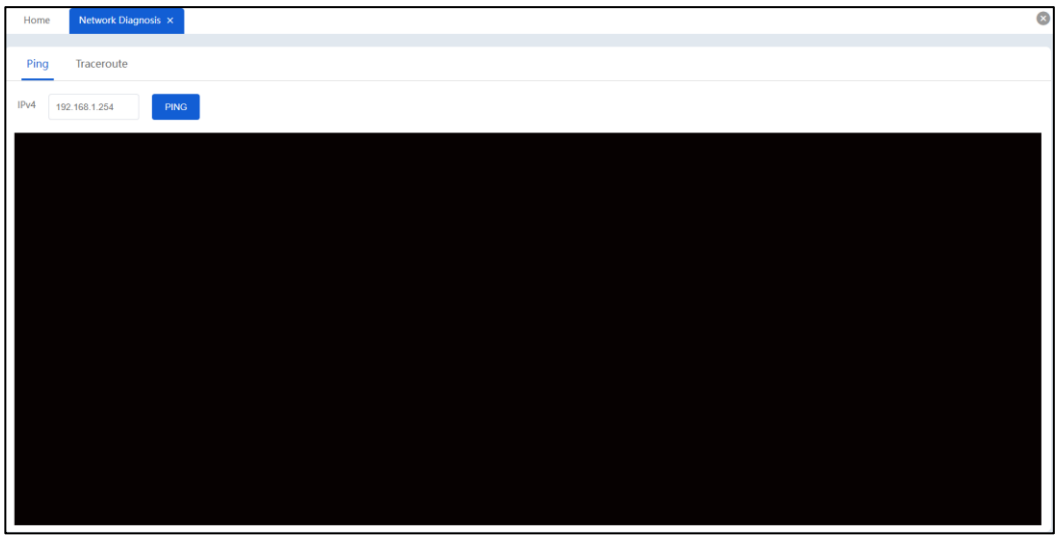
The system supports Ping and Traceroute commands to diagnose the network and check the network connectivity and routing path.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Configuration > (Navigation Bar) Network Diagnosis".

Interface Description

Screenshot of Network Diagnosis interface:



Main elements configuration description of network diagnosis interface:

Interface Element	Description
Please select	Click the drop-down list and select the network where the device is located.
Please select device	Click the drop-down list and select the name of the device.
IPv4	The IPv4 address of the selected device.
MAC	The MAC address of the selected device.
Device status	The alarm status of the selected device.
PING	Ping command, click “Ping” to detect the network connectivity between the system and the specified device.
TRACEROUTE	TRACEROUTE tracing: click "TRACEROUTE" to detect the path between the system and the specified device. It supports up to 30 nodes.

9.1.6 Configuration Record

Function Description

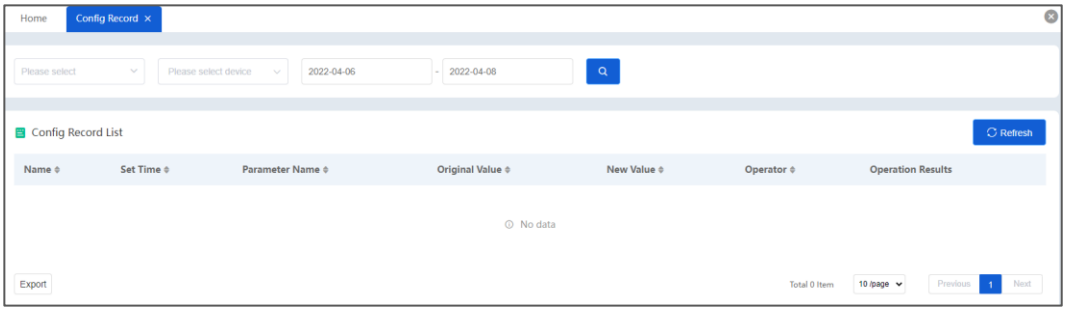
On the "Configuration Record" page, you can view the basic configuration records of the device, such as modifying the device IP, modifying the device name, Telnet configuration, restoring factory settings, restarting, etc.

Operation Path

Open in order: "(Menu Bar) Configuration Management > (Navigation Bar) Configuration > (Navigation Bar) Configuration Record".

Interface Description

Screenshot of configuration record interface:



Element description of configuration record interface:

Interface Element	Description
	Click the "  "button to query the basic configuration record of the device.
Refresh	Click "Refresh" button to refresh the current page information.
Name	The name of the device where the basic configuration operation occurred.
Set time	The time and date when the basic configuration operation occurred.
Parameter name	Specific parameter name modified in basic configuration operation.
Original value	Parameter value of parameter name before modification.
New value	Parameter value of parameter name after modification.
Operator	Users of basic configuration operations.
Operation results	The result of the basic configuration operation.

9.2 Wireless Configuration

9.2.1 Wireless Group Configuration

Function Description

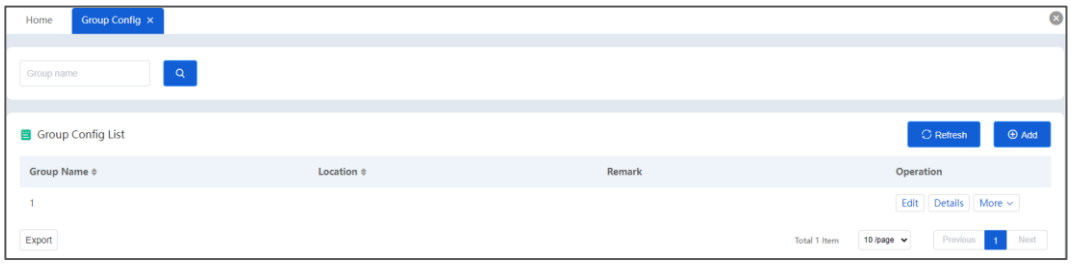
On the "Wireless Group Configuration" page, you can modify or create a wireless group to batch configure and modify the wireless devices in the wireless group.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Wireless Configuration > (Navigation Bar) Group Configuration".

Interface Description

Screenshot of Wireless Group Configuration interface:



Element description of Wireless Group Configuration interface:

Interface Element	Description
	Enter the group name to query, and click " " to filter the wireless group name.
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click the ”Add“ button to add a new wireless group.
Group name	The name of the wireless group.
Location	The geographic location of the wireless group device.
Remark	—
Operation	Optional operations are as follows: • Edit: click “Edit” to modify the configuration information of the current wireless group device. • VDetails: view the configuration information of the current wireless group device. • Config distribution: distribute the wireless group configuration to the devices in the group, that is, batch configure the wireless devices in the group. • Delete: click “Delete” to delete the current wireless group.

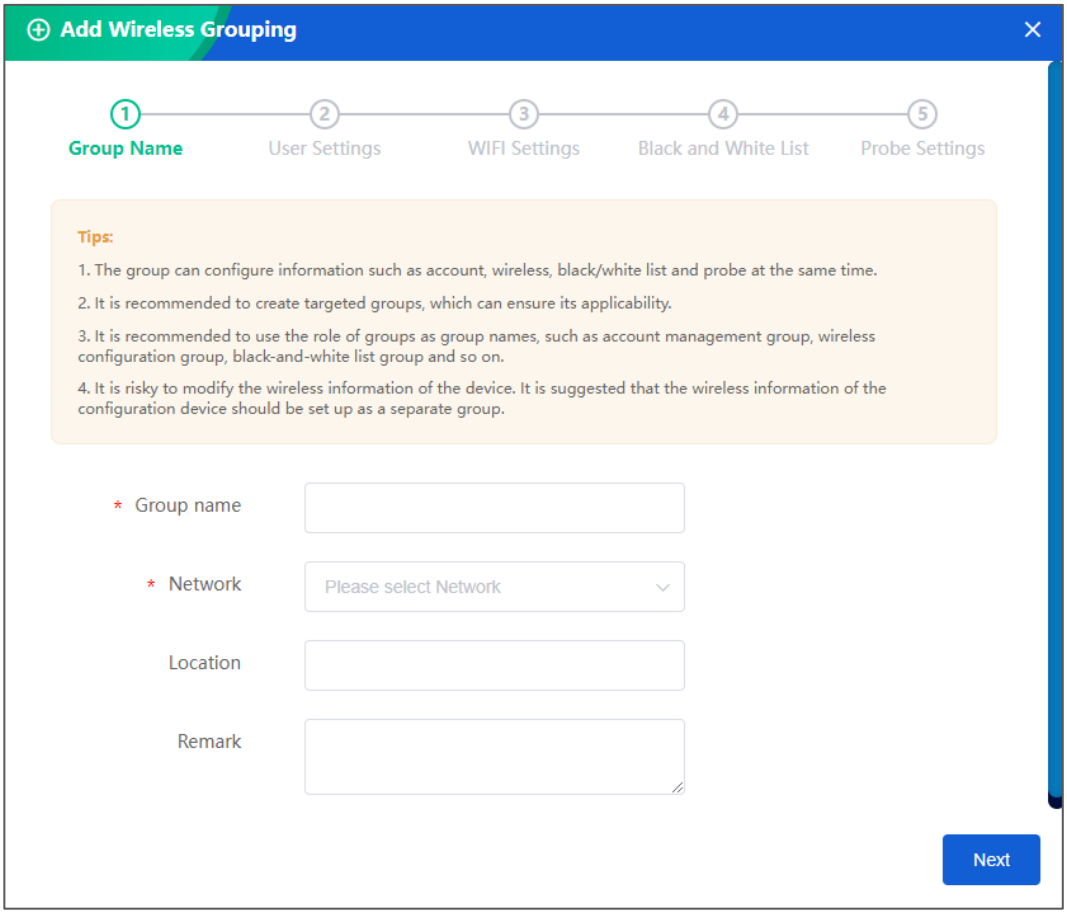
9.2.1.1 Add Wireless Group

This paper mainly introduces the adding process and parameter description of wireless group.

Interface Description 1: Add Wireless Packet - Group Name

On the wireless group page, click "⊕Add" to enter the Add Wireless Group interface.

Screenshot of Add Wireless Packet-Wireless Group interface:



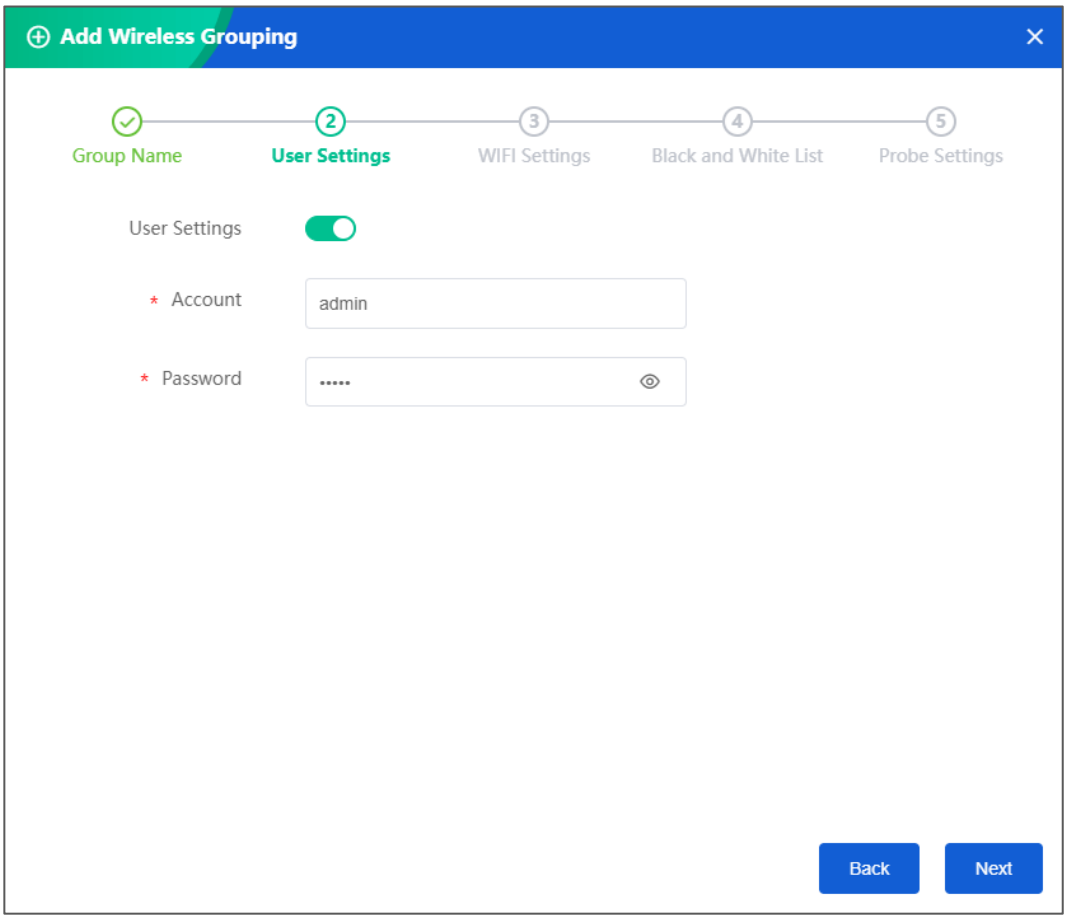
Element description of Add Wireless Packet-Wireless Group interface:

Interface Element	Description
Group name	The name of the wireless group, no more than 50 characters.
Network	Click the drop-down list to select the network where the wireless group is located.
Location	The geographical location of the wireless group device, no more than 100 characters.
Remark	Remarks of wireless group, no more than 100 characters.

Interface Description 2: Add Wireless Packet - User Settings

On the Add Wireless Packet - Wireless Group page, click “Next” to enter the User Settings interface.

Screenshot of Add Wireless Packet - User Settings interface:



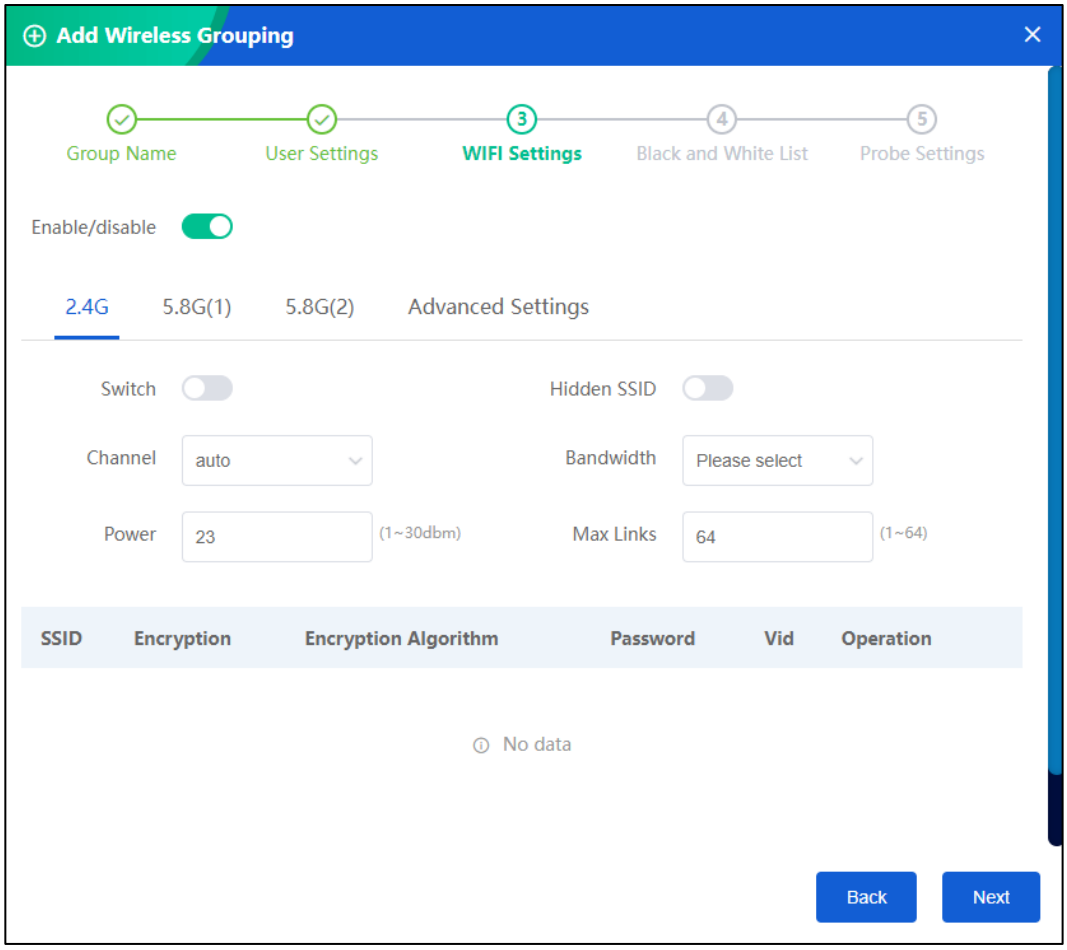
Element description of Add Wireless Packet - User Settings interface:

Interface Element	Description
User Settings	The user can set the move button to modify the user name and password of the AP device.
Account	Modify the login user name of the wireless AP device, no more than 20 characters.
Password	Modify the login password of the wireless AP device, no more than 20 characters.

Interface Description 3: Add Wireless Packet - WiFi Settings

On the add wireless packet - network settings page, click “Next” to enter the WiFi settings interface.

Screenshot of Add Wireless Packet - WiFi Setting interface:



Element description of Add Wireless Packet - WiFi Setting interface:

Interface Element	Description
Enable/disable	Mobile button for WiFi setting, which can modify the WiFi information of AP device.
2.4G	**2.4G configuration bar**
Switch	Mobile button for wireless switch, which can enable or disable the 2.4G wireless WiFi of the AP device.
Hidden SSID	Mobile button for Hidden wireless SSID, which can hide or display the wireless WiFi name. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Channel	Working channel of 2.4G wireless network, default to "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz;

Interface Element	Description
	• 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 3: main frequency band 2422Hz, frequency range 2411~2433Hz; • 4: main frequency band 2427Hz, frequency range 2416~2438Hz; • 5: main frequency band 2432Hz, frequency range 2421~2443Hz; • 6: main frequency band 2437Hz, frequency range 2426~2448Hz; • 7: main frequency band 2442Hz, frequency range 2431~2453Hz; • 8: main frequency band 2447Hz, frequency range 2436~2458Hz; • 9: main frequency band 2452Hz, frequency range 2441~2463Hz; • 10: main frequency band 2457Hz, frequency range 2446~2468Hz; • 11: main frequency band 2462Hz, frequency range 2451~2473Hz; • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in USA, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in USA, so it's temporarily unavailable; Note: In order to improve the network performance, please choose unused channel in the device working environment.
Bandwidth	Channel bandwidth of wireless network, it defaults to 20MHz, options as follows: • 20MHz; • 40MHz: bind two adjacent 20MHz channels together.
Power	Transmit power of 2.4G wireless signal. Value range is 1~30dBm. Note: • The greater the transmission power, the stronger the transmission capacity and the farther the transmission distance; Excessive power may cause unnecessary interference to other wireless devices. • Different device has different transmitting power range.

Interface Element	Description
Max links	Maximum user number of the device 2.4G wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected user number.
Add	Click “Add” to create wireless SSID and encryption method.
SSID	SSID name of 2.4G wireless network.
Encryption	The encryption modes of 2.4G wireless network display as follows: • WPA: WPA (Wi-Fi Protected Access) Wi-Fi protected access, using a pre shared key. • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA-MIXED: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
Encryption	The encryption modes of 5.8G wireless network display as follows: • WPA: WPA (Wi-Fi Protected Access) uses a pre-shared key. • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA-MIXED: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: • AES: advanced encryption standard; • TKIP: (temporary Key Integrity Protocol) encryption algorithm; • TKIP/AES: TKIP/AES encryption algorithm.
Password	Wireless encryption password.
Operation	Optional operations are as follows: • Modify: click “Modify” to modify SSID, encryption

Interface Element	Description
	method and password. • Delete: click “Delete” button to delete WiFi.
5.8G(1) / 5.8G(2)	**5.8G (1) / 5.8G (2) configuration bar**
Wireless switch	Mobile button for wireless switch, which can enable or disable the 5.8G wireless WiFi of the AP device.
Hidden wireless SSID	Mobile button for Hidden wireless SSID, which can hide or display the wireless WiFi name. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Channel	Working channel of 5.8G wireless network, default to "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 36: main frequency band 5180Hz, frequency range 5170~5190Hz; • 40: main frequency band 5200Hz, frequency range 5190~5210Hz; • 44: main frequency band 5220Hz, frequency range 5210~5230Hz; • 48: main frequency band 5230Hz, frequency range 5210~5250Hz; • 52: main frequency band 5260Hz, frequency range 5250~5270Hz; • 56: main frequency band 5280Hz, frequency range 5270~5290Hz; • 60: main frequency band 5300Hz, frequency range 5290~5310Hz; • 64: main frequency band 5320Hz, frequency range 5310~5330Hz; • 149: main frequency band 5745Hz, frequency range 5735~5755Hz; • 153: main frequency band 5765Hz, frequency range 5755~5775Hz; • 157: main frequency band 5785Hz, frequency range 5775~5795Hz; • 161: main frequency band 5805Hz, frequency range 5795~5815Hz; • 165: main frequency band 5825Hz, frequency range 5815~5835Hz; Note:

Interface Element	Description
	In order to improve the network performance, please choose unused channel in the device working environment.
Bandwidth	5.8G wireless network channel bandwidth, options are as follows: • 20MHz; • 40MHz; • 80MHz.
Power	Transmit power of 5.8G wireless signal. Value range is 1~30dBm. Note: • The greater the transmission power, the stronger the transmission capacity and the farther the transmission distance; Excessive power may cause unnecessary interference to other wireless devices. • Different device has different transmitting power range.
Max links	Maximum user number of the device 5.8G wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected user number.
Add	Click “Add” to create wireless SSID and encryption method.
SSID	SSID name of 5.8G wireless network.
Encryption	The encryption modes of 5.8G wireless network display as follows: • WPA: WPA (Wi-Fi Protected Access) Wi-Fi protected access, using a pre shared key. • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA-MIXED: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: • AES: advanced encryption standard; • TKIP: (temporary Key Integrity Protocol) encryption algorithm; • TKIP/AES: TKIP/AES encryption algorithm.
Password	Wireless encryption password.
Vid	Wireless network VLAN ID.

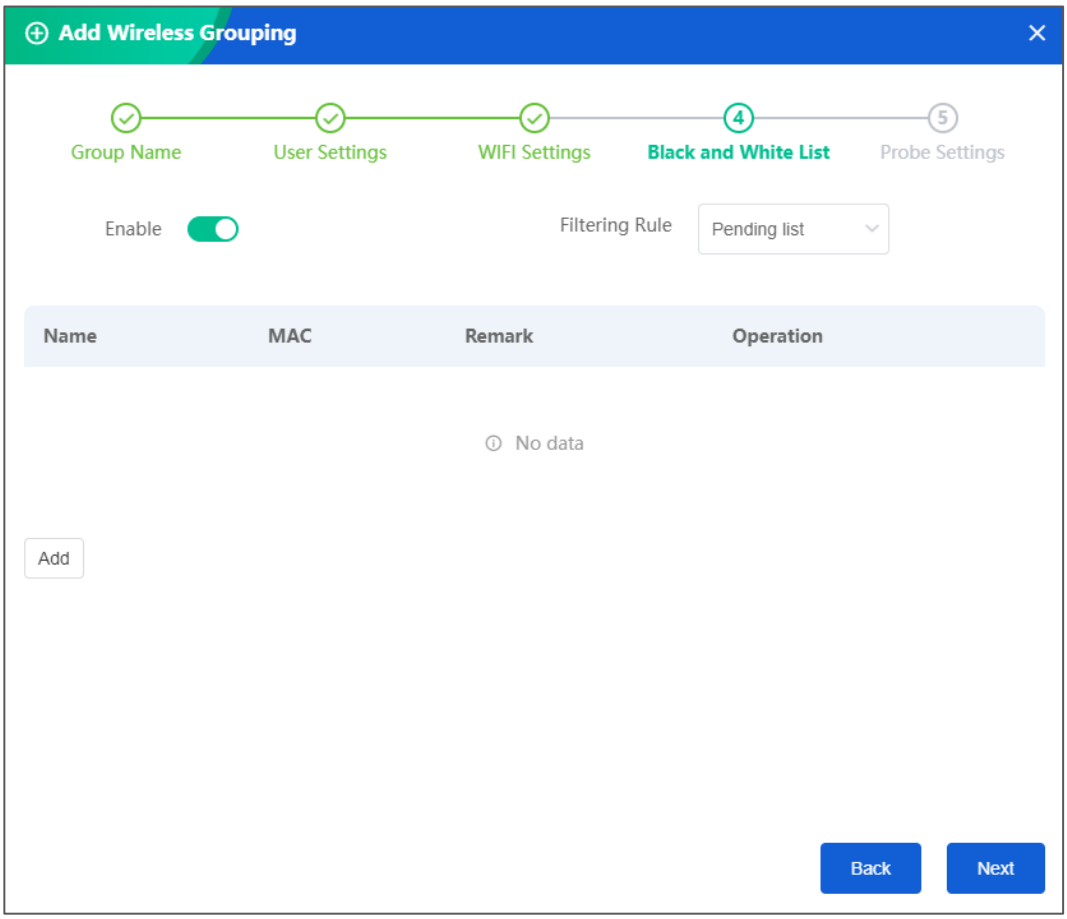
Interface Element	Description
Operation	Optional operations are as follows: • Modify: click “Modify” to modify SSID, encryption method and password. • Delete: click “Delete” button to delete WiFi.
Advanced Settings	**Advanced settings bar**
Short GI	Short GI (Short Guard Interval) enabling switch, click the right button to switch between ON and OFF. • ON: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. • OFF: after disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN. Note: Please enable WDS function while bridging the device and other wireless devices.
WMM	WMM (WiFi Multimedia) function, defaults to enabled. Note: After enabling WMM function, the device can process the data packet with priority level, improving the data transmission performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements.
80211r	Enable fast roaming of the terminal.
Wireless isolate	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
Fragment threshold	Fragment threshold of data packet, value range is 256-2346, defaults to 2346. Note: • The data frame will be segmented when its length surpasses fragment threshold. • With large interference or high utilization ratio of wireless network, user can adopt smaller fragmentation threshold to increase the transmission reliability; but it is low efficiency. • The wireless network is easy to be interfered while adopting

Interface Element	Description
	large fragment threshold; but it is high efficiency.
RTS	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal; • 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. • The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to response the device, which represents the two stations can conduct wireless communication.
Country code	Countries and regions of wireless network application, with the following options: • China • USA Note: Different country opens different channels.

Interface Description 4: Add Wireless Packet - Black/White List

On the add wireless packet-WiFi setting page, click “Next” to enter the blacklist / whitelist interface.

Screenshot of add wireless packet - blacklist / whitelist interface:



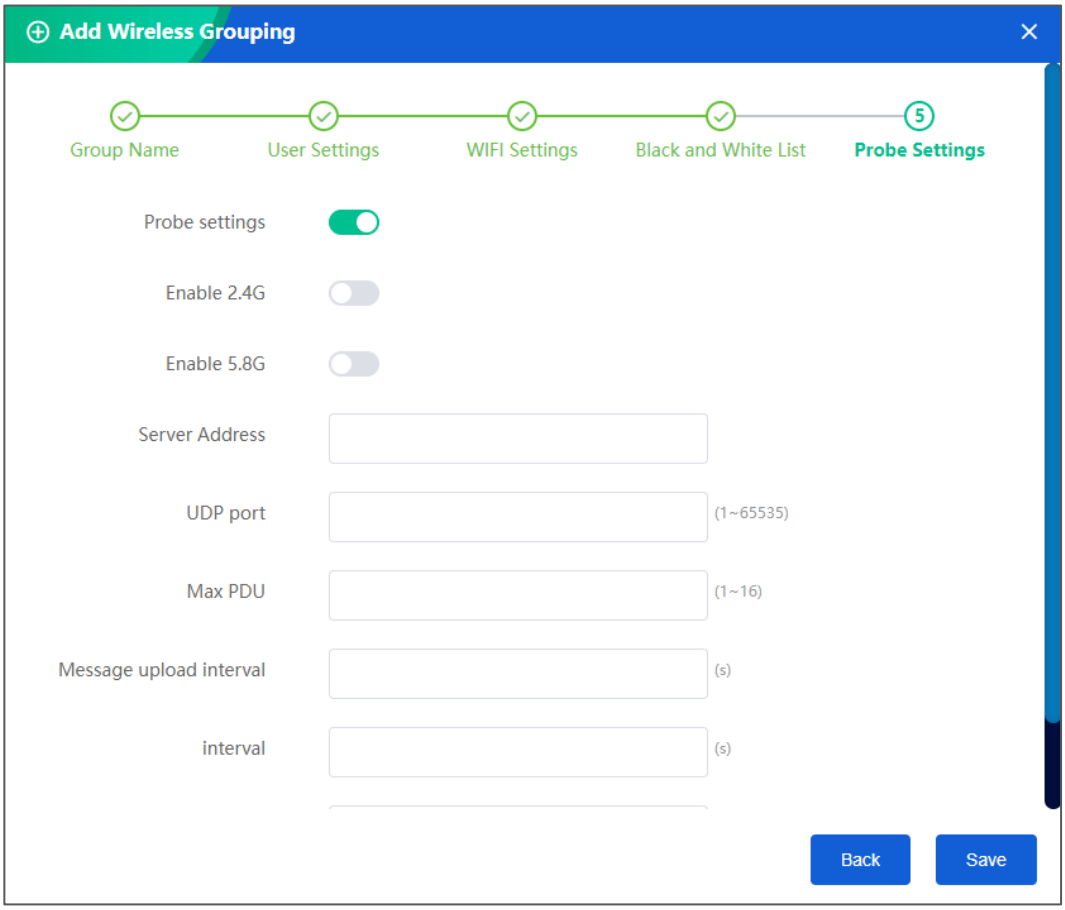
Element description of add wireless packet - blacklist / whitelist interface:

Interface Element	Description
Enable	Enable black / white list mobile button to enable wireless access filtering rules.
Filtering rule	The filter rule options are as follows: • Pending list: the list to be checked, which could be set to white list or black list. • Black list: list of wireless client forbidden to visit wireless network; • White list: list of wireless client allowed to visit wireless network; wireless clients out of white list are forbidden to visit; Note: The filter rule is only effective for the current filter list.
Add	Click “Add” to add a blacklist / whitelist.
Name	Name of the device to be filtered.
MAC	MAC address of the device to be filtered.
Remark	Remark description of the list
Operation	Click “Delete” to delete the list.

Interface Description 5: Add Wireless Packet - Probe Settings

On the add wireless packet - blacklist / whitelist page, click “Next” to enter the probe setting interface.

Screenshot of add wireless packet - probe setting interface:



Element description of add wireless packet - probe setting interface:

Interface Element	Description
Probe settings	The probe setting and moving button can be opened to set the parameters of the probe server.
Enable 2.4G	Probe set move button. After the probe function is started, the wireless terminal equipment information detected in the 2.4G frequency band can be sent to the specified server.
Enable 5.8G	Probe set move button. After the probe function is started, the detected 5.8G band wireless terminal equipment information can be sent to the specified server.
Server address	The address of the server that receives probe information.
UDP port	The port number of the server receiving probe information. The value range is 1-65535.

Interface Element	Description
Max PDU	The number of information in a single message sent by the probe, with a valid value range of 1-16.
Message upload interval	The time interval for uploading data messages of the same device, in seconds, is less than 3600.
Interval	Time interval of the same device data upload, unit is second.
Valid signal threshold	Effective signal threshold，unit is dBm，value range：<0. Note: If the signal strength of wireless client is less than threshold, it will be regarded as invalid signal.

9.2.2 Group Maintenance

Function Description

On the "Group Maintenance" page, you can add wireless devices to the wireless group or delete wireless devices in the wireless group.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Wireless Configuration > (Navigation Bar) Group Maintenance ".

Interface Description

Screenshot of Group Maintenance interface:

Element description of Wireless Group Configuration interface:

Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Management	Click the “Manage” button to add wireless devices to the specified wireless group.
Group list	Wireless group information.
Group name	The name of the wireless group.

Interface Element	Description
Name	Name of the wireless device.
Network card address	The physical MAC address of the wireless device.
IP address	The network IP address of the wireless device.
Model	Product model of the wireless device.
SSID2.4G	Name of 2.4G wireless WiFi.
SSID5.8G	Name of 5.8G wireless WiFi.
Work mode	Working mode of wireless device.
Operation	Optional operations are as follows: • Delete: click “Delete” to delete the specified devices in the current wireless group.

9.2.3 AP Playback

Function Description

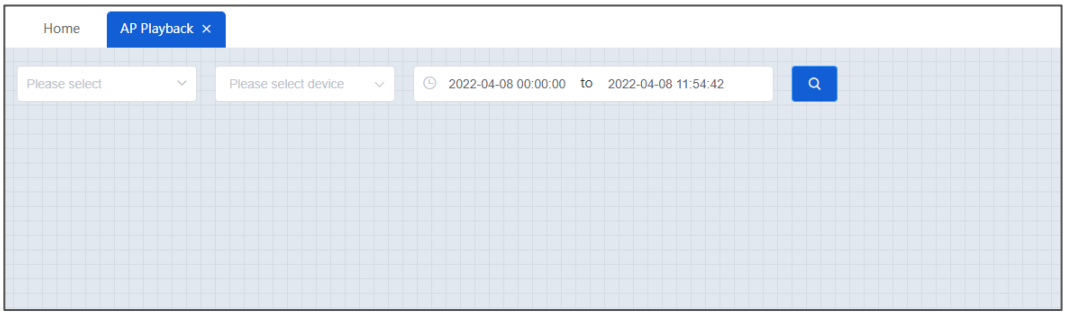
On the “AP Playback” page, you can view the alarm events between the wireless device and the wireless client. The alarm playback function of the system is disabled by default and can be enabled in the "playback switch" under "System Management > System Settings > System Configuration"; After the playback switch is enabled, the alarm playback and AP playback functions are enabled, and the system starts to record alarm events. The playback function has a certain impact on the performance of the system. Please use it according to the site environment.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Wireless Configuration > (Navigation Bar) AP Playback".

Interface Description

Screenshot of AP playback interface:



Element description of AP playback interfaces:

Interface Element	Description
Please select	Click the drop-down list and select the network where the device is located.
Please select device	Click the drop-down list and select the name of the device.
	Click "  " to query the history alarm records of the current device.
	Click the "  " button to play back the history alarm events.
	Pause button.
	Replay button.
	Speed up button.
	Slow down button.

9.3 Software

9.3.1 Firmware

Function Description

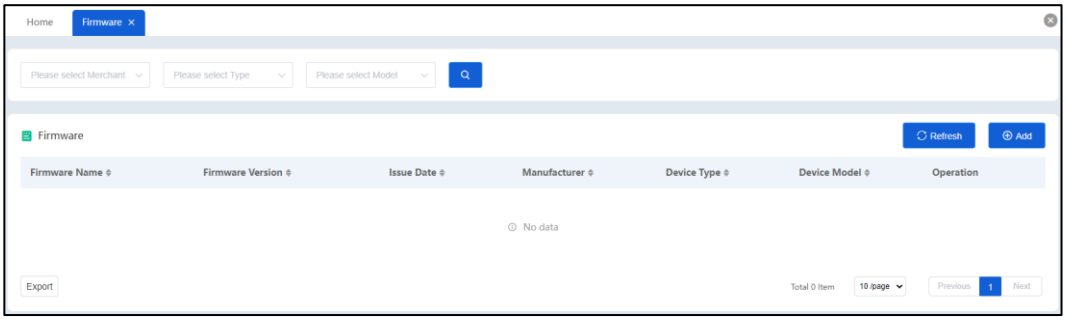
On the "Firmware " page, you can save the upgrade file of the device for remote batch upgrade.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Software > (Navigation Bar) Firmware".

Interface Description 1: Firmware

Screenshot of Firmware Management interface:



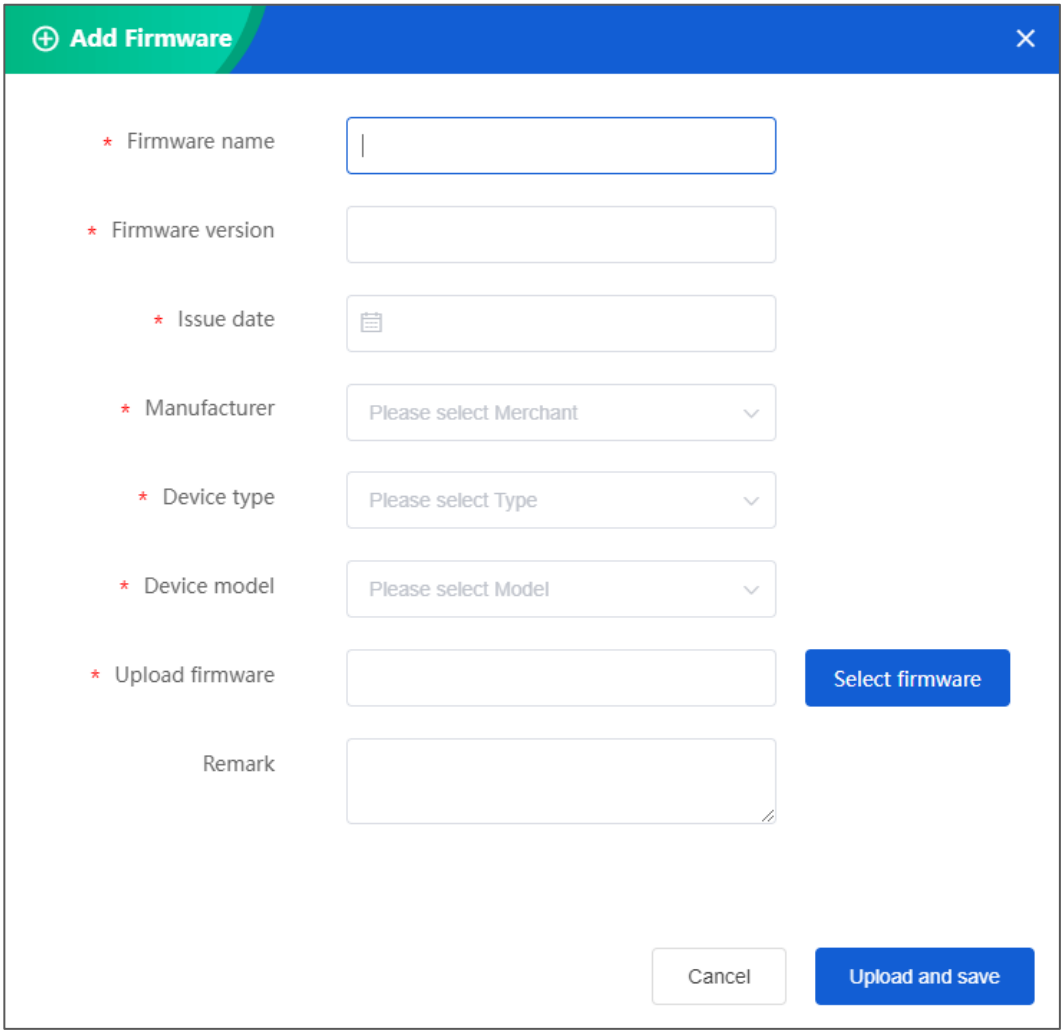
Element description of firmware management interface:

Interface Element	Description
Please select merchant	Click the drop-down list and select the device manufacturer to query.
Please select type	Click the drop-down list and select the device type to query.
Please select model	Click the drop-down list and select the device model to query.
	Click the "  "button to filter the devices according to the selected information.
Refresh	Click "Refresh" button to refresh the current page information.
Add	Click the "Add" button to upload the device firmware file.
Firmware name	Name of the device firmware.
Firmware version	Device firmware version.
Issue Date	The release date of the firmware.
Manufacturer	Name of device manufacturer.
Device type	The product type of the device.
Device model	Device model name.
Operation	Optional operations are as follows: • Modify: click "Modify" to modify the current firmware management information. • Delete: click "delete" to delete the current firmware.

Interface Description 2: Add Firmware

On the firmware management page, click "Add" to enter the Add Firmware interface.

Screenshot of Adding Firmware interface:



Element description of Add Firmware interface:

Interface Element	Description
Firmware name	The name of the device firmware, no more than 50 characters.
Firmware version	The version of the device firmware, no more than 50 characters.
Issue Date	Select the release date of firmware through the time plug-in.
Manufacturer	Click the drop-down list and select the manufacturer name of the firmware upgrade device.
Device type	Click the drop-down list and select the product type of the firmware upgrade device.
Device model	Click the drop-down list and select the product model name of the firmware upgrade device.
Upload firmware	Click the "Select Firmware" button to select the firmware file to be uploaded. The formats such as ".bin", ".img" and ".file" are supported.

Interface Element	Description
Remark	Firmware management remarks information, no more than 100 characters.

9.3.2 Upgrade

Function Description

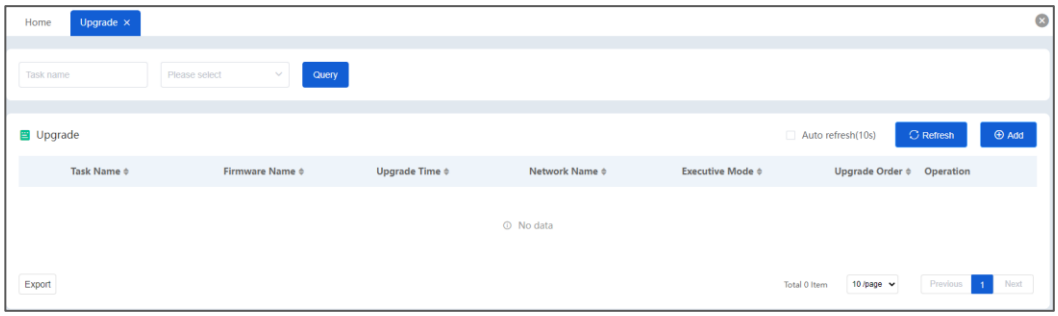
On the "Upgrade" page, you can perform scheduled remote batch upgrade of the devices.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Software > (Navigation Bar) Upgrade".

Description 1: Upgrade

Screenshot of upgrade interface:



Element description of remote upgrade interface:

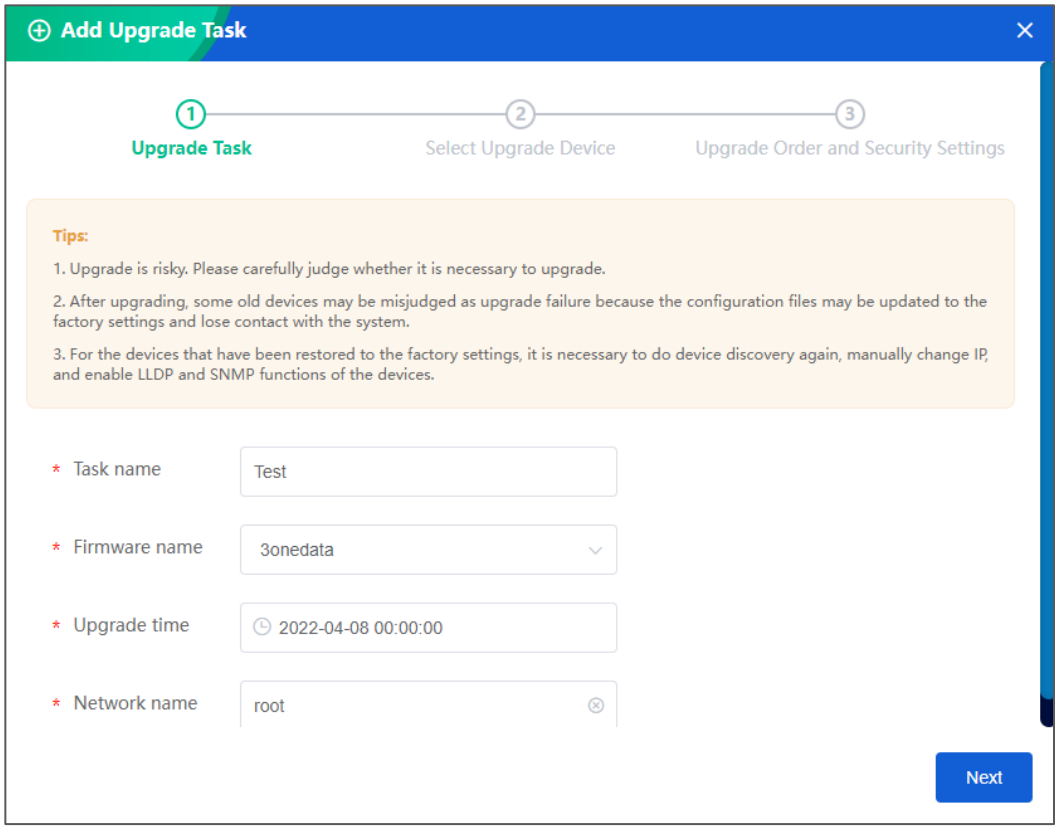
Interface Element	Description
Task name	Enter the name of the upgrade task to query.
Please select	Click the drop-down list and select the network name to query.
	Click the "  "button to filter tasks according to the selected information.
Refresh	Click “Refresh” button to refresh the current page information.
Add	Click “Add” button to add remote upgrade tasks.
Task name	The name of the upgrade task.
Firmware name	The name of the upgrade firmware.
Upgrade time	Schedule the time to perform the upgrade task.
Network name	The network name of the firmware upgrade device.

Interface Element	Description
Group name	The wireless group name of the firmware upgrade device. Batch upgrade only supports single model upgrade.
Executive mode	The executive mode of the remote upgrade task.
Upgrade order	Upgrade order of the device.
Operation	Optional operations are as follows: • Modify: Click the “Modify” button to modify the current task configuration information. • Delete: Click the “Delete” button to delete the current task.

Interface Description 2-1: Add Upgrade Task-Upgrade Task

On the remote upgrade page, click "Add" button to enter the interface of adding upgrade tasks.

Screenshot of upgrade task interface:



Element description of upgrade task interface:

Interface Element	Description
Task name	The name of the upgrade task, no more than 100 characters.
Firmware name	Click the drop-down list and select the firmware name to be

Interface Element	Description
	upgraded. Upload firmware to firmware management before upgrading remotely.
Upgrade time	Select the execution time of the task through the time plug-in. Please avoid the use peak period of wireless AP device use when upgrading.
Network name	Click the drop-down list and select the network name for firmware upgrade.

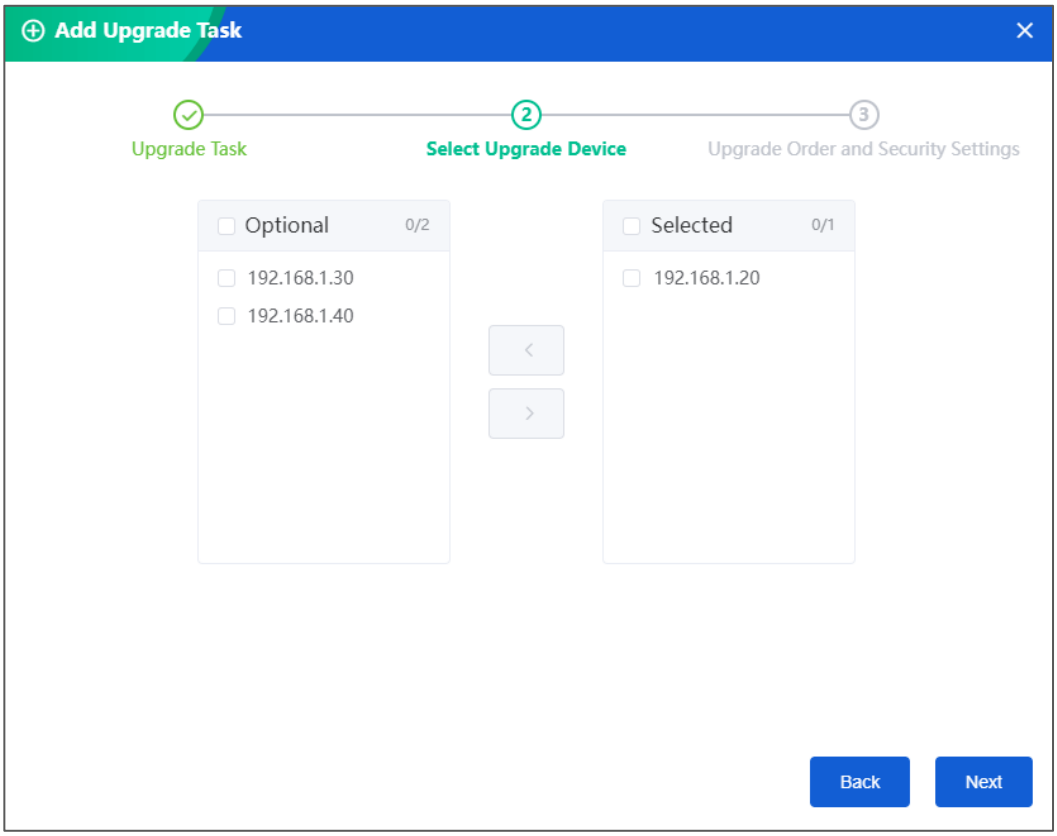
Note

- In batch upgrade, only one model of equipment can be upgraded at a time.
- Do not do anything else during the upgrade if there is no abnormality.

Interface Description 2-2: Add Upgrade Task-Select Upgrade Device

In the upgrade task interface, click "Next" button to enter the interface of selecting upgrade device.

Screenshot of select upgrade device interface:



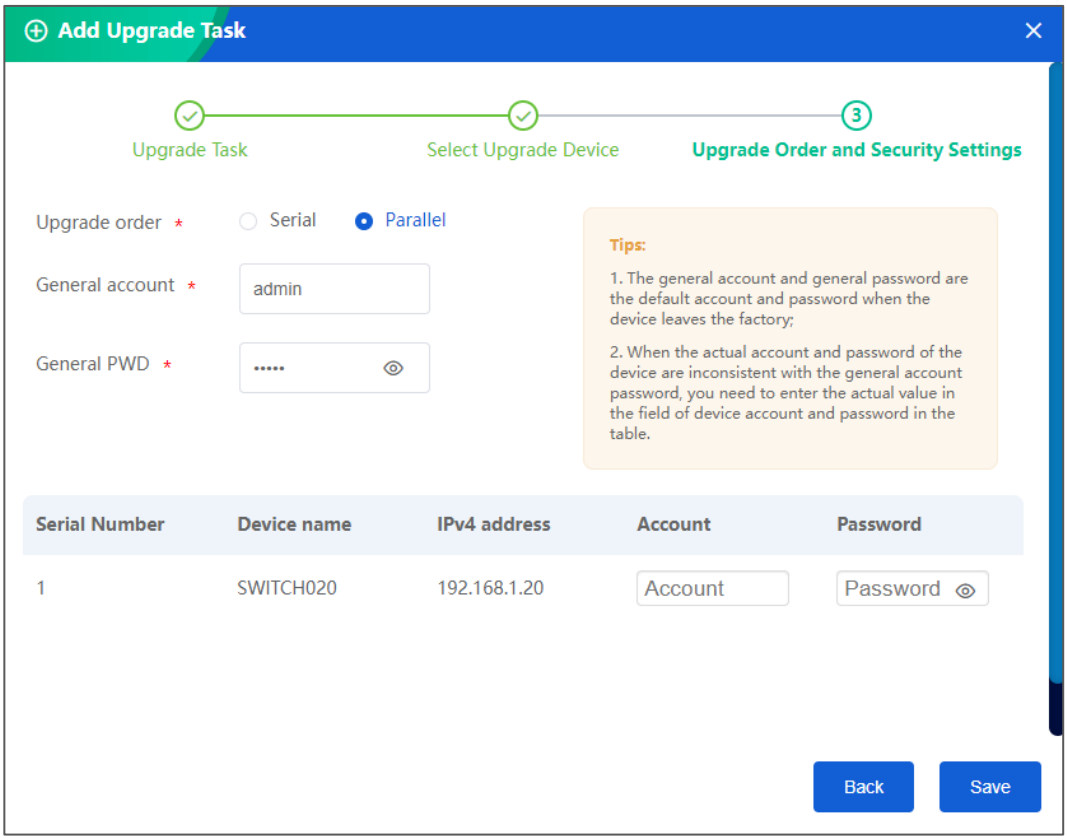
Element description of select upgrade device interface:

Interface Element	Description
Select upgrade device	Upgrade device list: the system screens the upgradable devices according to firmware and network information, and the screened devices will be displayed in the "Optional" device list. Check the device to be upgraded in the "optional" device list, and move it to the "Selected" device list through the ">" button, and these devices will be upgraded in firmware as planned.

Interface Description 2-3: Adding Upgrade Tasks-Upgrade Order and Security Settings

In the interface of upgrading device, click "Next" button to enter the interface of upgrading order and security settings.

Screenshot of upgrade order and security settings interface:



Element description of upgrade order and security settings interfaces:

Interface Element	Description
Upgrade order	Device firmware upgrade mode, options are as follows:

Interface Element	Description
	• Serial: the system upgrades the firmware of all devices one by one according to the order. • Parallel: the system upgrades the firmware of for all devices at the same time.
General account	The login user account of the device. When the device account and password are not specified in the device account list, use the general account and password to upgrade the device. Note: If the user name and password of most devices are the same, the user name and password can be used as the universal account and password.
General password	The login user password of the device. When the device account and password are not specified in the device account list, use the general account and password to upgrade the device. Note: If the user name and password of most devices are the same, the user name and password can be used as the universal account and password.
Serial number	The serial number of the list.
Device name	Display the device name.
IPv4 address	The IP Address of the device.
Account	The login user name of the device.
Password	The login user password of the device.
Sort	When there is a serial upgrade mode, the upgrade order can be adjusted.

9.3.3 Backup

Function Description

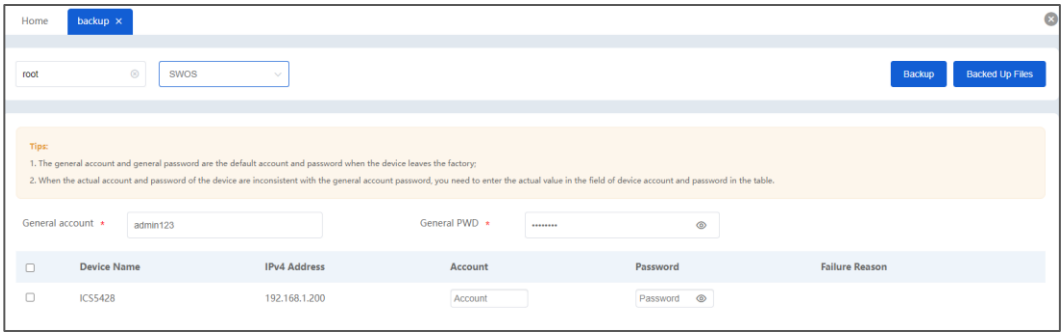
On the "Backup" page, you can save the configuration files of devices in batches.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Software > (Navigation Bar) Backup".

Interface Description

Screenshot of backup interface:



Element description of configure backup interface:

Interface Element	Description
Please select	Click the drop-down list and select the network where the device is located.
Please select software platform	Click the drop-down list and select the software platform to which the device belongs. After selecting the software platform, the system will automatically screen the devices of the same type system.
Backup	Check the device to be backed up, and click the "Backup" button to back up the configuration files of the device in batches.
Backed up files	Click "Backed-up Files" to enter the backup list, view the device configuration files backed up by the system, and support local batch download.
General account	The login user account of the device. When the device account and password are not specified in the device account list, use the general account and password to upgrade the device. Note: If the user name and password of most devices are the same, the user name and password can be used as the universal account and password.
General password	The login user password of the device. When the device account and password are not specified in the device account list, use the general account and password to upgrade the device. Note: If the user name and password of most devices are the same, the user name and password can be used as the universal account and password.
Device name	Display the device name.
IPv4 address	The IP Address of the device.
Account	The login user name of the device.

Interface Element	Description
Password	The login user password of the device.
Failure reason	Cause of backup failure

9.3.4 Recovery

Function Description

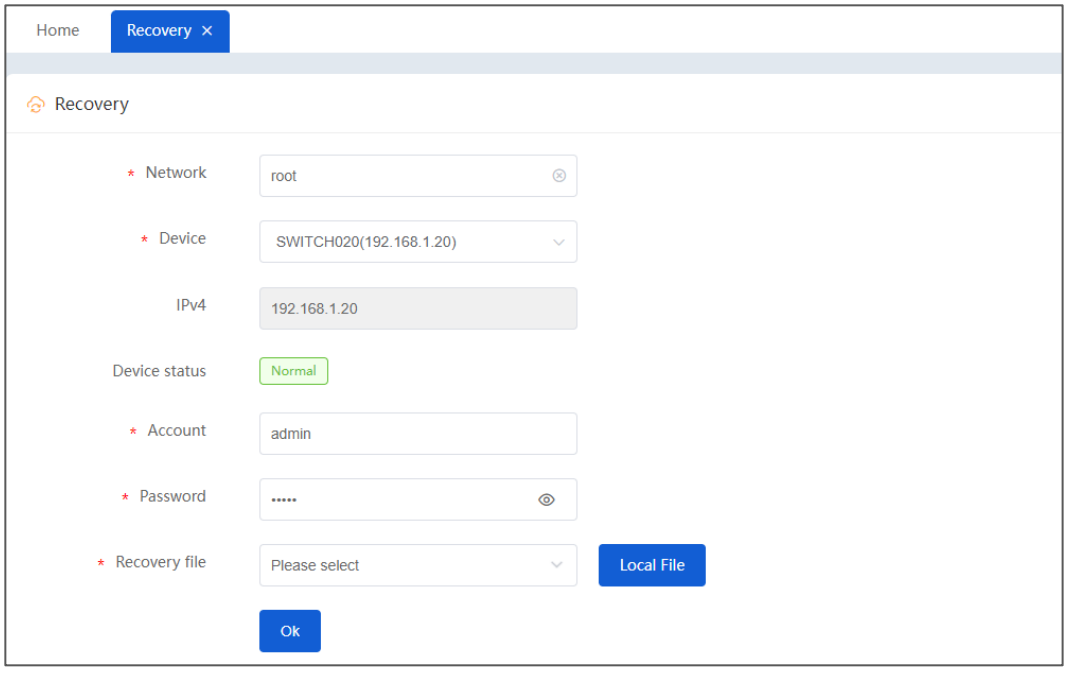
On the “Recovery” page, you can upload the configuration file of the device.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Software > (Navigation Bar) Recovery".

Interface Description

Screenshot of recovery interface:



Description of configuration recovery interface elements:

Interface Element	Description
Network	Click the drop-down list and select the network where the device is located.
Device	Click the drop-down list and select the name of the device.
IPv4	The IP address information of this device.
Device status	The alarm status information of the device.

Interface Element	Description
Account	The login user name of the device.
Password	The login user password of the device.
Recovery file	Backup configuration file of the device or configuration file of the same series model. If the configuration file has been backed up, click the drop-down list to select the configuration file; If the configuration file is not backed up, you can upload the local configuration file to the device by clicking the "Local File" button. Notice: Upload the configuration file to the device, and the current configuration of the device will be overwritten.

9.4 Polling

9.4.1 Interface Polling

Function Description

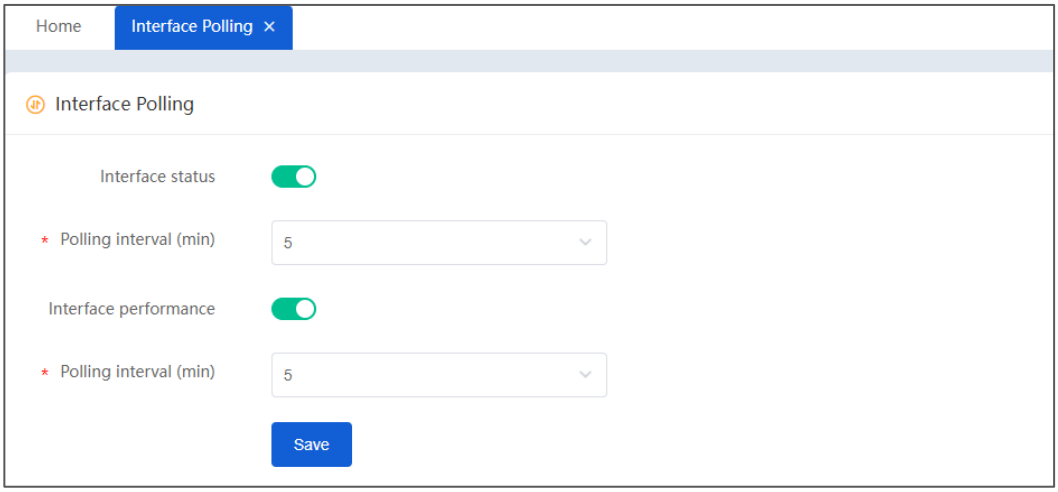
On the “Interface Polling” page, users can configure the system's status and performance polling and polling interval for the interface, and view the status and performance of the interface.

Operation Path

Open in order: "(Menu Bar) Configuration > (Navigation Bar) Polling > (Navigation Bar) Interface Polling".

Interface Description

Screenshot of interface polling interface:



Description of Interface Polling interface element:

Interface Element	Description
Interface status	Interface status polling switch, the system queries the connection status of the interface according to the polling time, so as to avoid the absence or loss of reported information of the device.
Polling interval (min)	Drop-down list of interface polling time interval, unit: minutes, with the following options: • 3; • 5; • 10; • 15; • 30; • 60.
Interface performance	Interface polling switch, the system queries the bandwidth utilization of the interface according to the polling time, such as the traffic load in the traffic view.
Polling interval (min)	Drop-down list of interface polling interval, unit: minutes, with the following options: • 3; • 5; • 10; • 15; • 30; • 60.

Note

Suggested polling interval:

- Quantity of devices (1-200): 5 minutes;
- Quantity of devices (200-500): 10 minutes;
- Quantity of devices (500-2000): 15 minutes;
- Quantity of devices (over 2000): 30 minutes.

9.4.2 Device Polling

Function Description

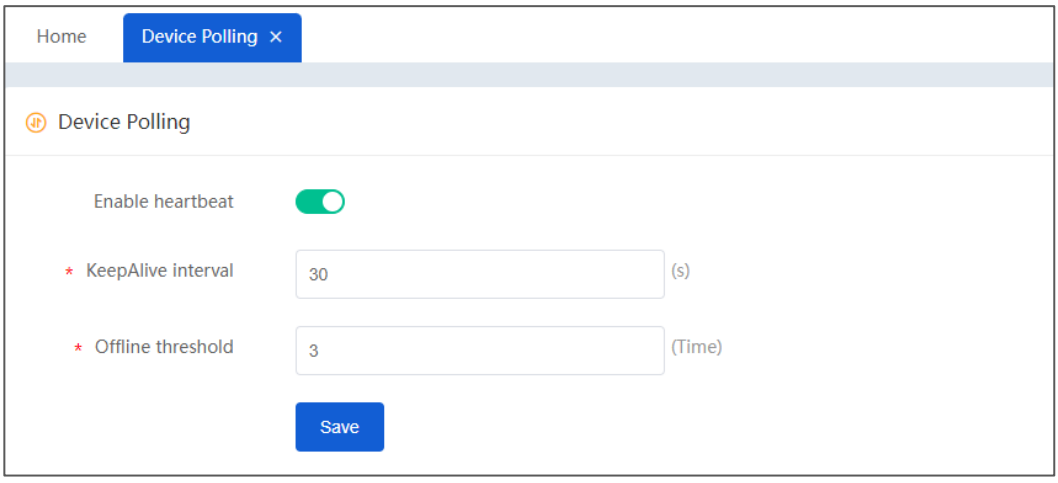
On the "Device Polling" page, you can configure the parameters of heartbeat packet sent by the system to the device and check the online status of the device.

Operation Path

Open in order: (Menu Bar) Configuration > (Navigation Bar) Polling > (Navigation Bar) Device Polling.

Interface Description

Screenshot of device polling interface:



Description of device polling interface elements:

Interface Element	Description
Enable Heartbeat	Heartbeat enable switch.
KeepAlive Interval	Time interval for the system to send heartbeat packet, ranging from 5 to 7200, unit: seconds.
Offline threshold	Off-line threshold of device, ranging from 1 to 5. According to the heartbeat interval, the system sends Ping packets. When

Interface Element	Description
	the device is found to be unresponsive, it continues to send heartbeat packet. When the number of unresponsive times reaches the threshold number of offline times, it is considered that the device is offline.

10 Alarm Management

10.1 Alarm List

10.1.1 Real-time Alarm List

Function Description

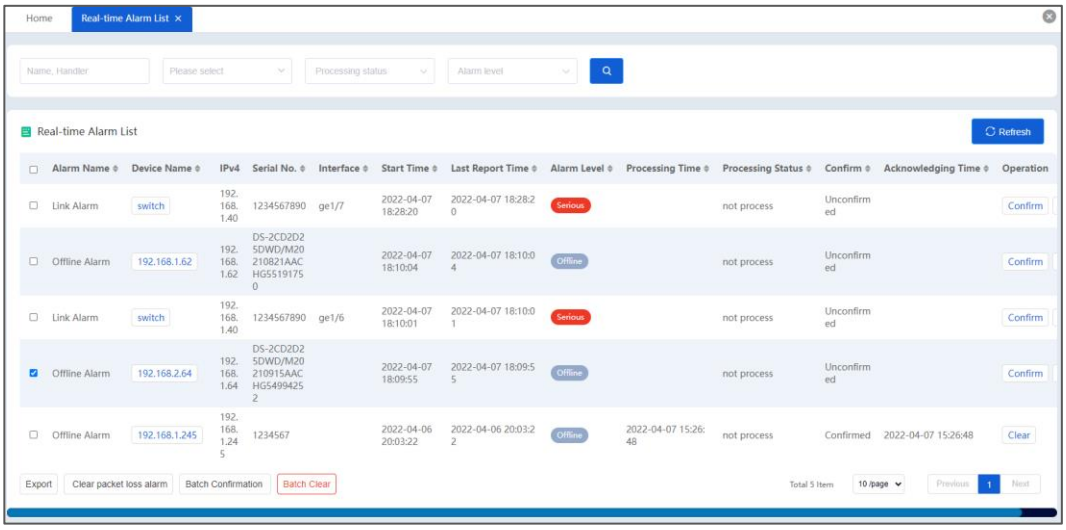
On the “Real-time Alarm List” page, users can view or process the current alarm events. When the system detects that the fault returns to normal, it will automatically cancel the alarm.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm List > (Navigation Bar) Real-time Alarm List".

Interface Description

Screenshot of real-time alarm list interface:



Description of real-time alarm list interface elements:

Interface Element	Description
	Click the "  "button to filter the alarm according to the selected information.

Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Alarm name	The name of the alarm event generated by the device in the current network.
Device name	The name of the device that generated the alarm.
IPv4	The IP address information of the device that generates the alarm.
Serial No.	SN of the device that generated the alarm.
Interface	Port of the device that generates the alarm.
Start time	The time when the device generated the alarm event.
Last report time	The time when the device finally reports the alarm event is suitable for multiple alarms.
Alarm level	The alarm level corresponding to the alarm message is shown as follows: • General • Important • Serious • Offline
Processing time	Time for processing alarm events.
Processing status	The processing status of alarm events is shown as follows: • Unprocessed: indicates that the alarm event is unprocessed.
Confirm	The viewing status of alarm events is shown as follows: • Unconfirmed: indicates that the alarm event information has not been confirmed. • Confirmed: indicates that the alarm event information has been confirmed.
Acknowledging time	Confirmation or processing time of alarm events.
Operation	Optional operations are as follows: • Click the "Confirm" button to indicate that the event is known, but nothing will be done. • Click the "Clear" button to delete the specified alarm event. When deleting, you need to verify the administrator's permission password. Offline alarms and self-loop alarms cannot be deleted manually.

10.1.2 History Alarm List

Function Description

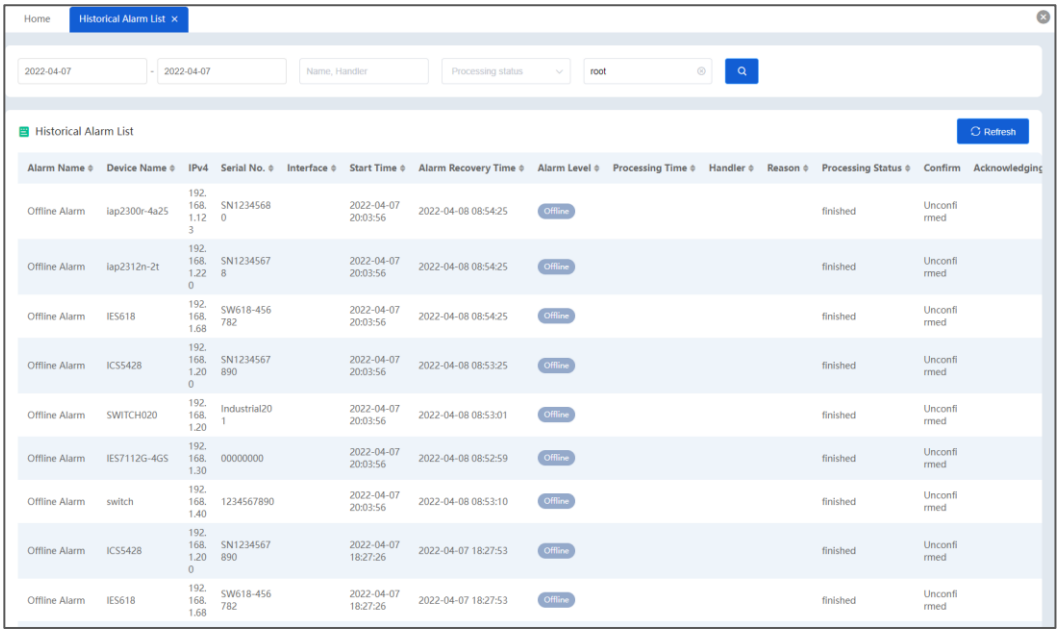
On the "History Alarm List" page, you can view the completed alarm events.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm List > (Navigation Bar) History Alarm List".

Interface Description

Screenshot of history alarm list interface:



Description of history alarm list interface elements:

Interface Element	Description
	Click the "  "button to filter the alarm according to the selected information.
Refresh	Click “Refresh” button to refresh the current page information.
Alarm name	The name of the alarm event generated by the device in the current network.
Device name	The name of the device that generated the alarm.
IPv4	The IP address information of the device that generates the alarm.
Serial No.	SN of the device that generated the alarm.
Interface	Port of the device that generates the alarm.

Interface Element	Description
Start time	The time when the device generated the alarm event.
Alarm recovery time	Device failure recovery time.
Alarm level	The alarm level corresponding to the alarm message is shown as follows: • General • Important • Serious • Offline
Processing time	Time for processing alarm events.
Handler	User information for processing alarm events.
Reason	The reason for processing the alarm event.
Processing status	The processing status of alarm events is shown as follows: • Completed: indicates that the alarm event has been processed or the alarm event has been eliminated.
Confirm	The viewing status of alarm events is shown as follows: • Unconfirmed: indicates that the alarm event information has not been confirmed or suspended. • Confirmed: indicates that the alarm event information has been confirmed or processed.
Acknowledging time	Confirmation or processing time of alarm events.

10.1.3 Device Reporting Event

Function Description

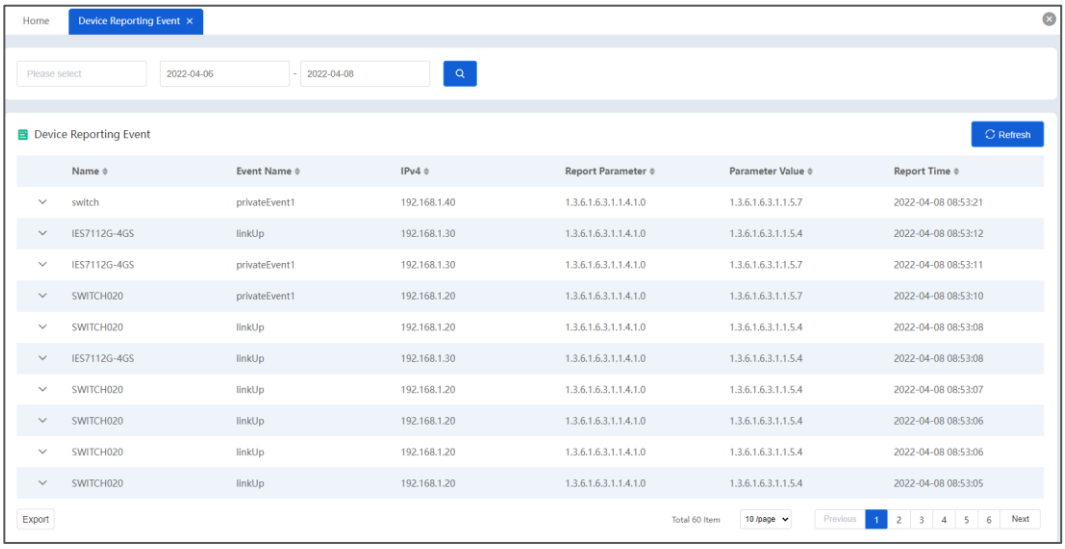
On the "Device Reporting Event" page, you can view the records of device report events. The device actively sends Trap information to the system to report the event.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm List > (Navigation Bar) Device Reporting Events".

Interface Description

Screenshot of device reporting event interface:



Description of device report event interface element:

Interface Element	Description
Fuzzy query box	After the user inputs the characteristic characters of the device, the matching device list will be listed for the user to select.
	Click the "  "button to query the reported event record.
Refresh	Click “Refresh” button to refresh the current page information.
Name	The name of the device that reported the event.
Event Name	The name of the report event. In "Alarm Management > Alarm Configuration > Alarm Definition", you can customize the report events.
IPv4	IP address of the device that reported the events.
Report parameter	The reported event or management object defined in the SNMP MIB library of the device.
Parameter value	Parameter values of report events.
Report time	Time information of the occurred event.

10.1.4 Alarm playback

Function Description

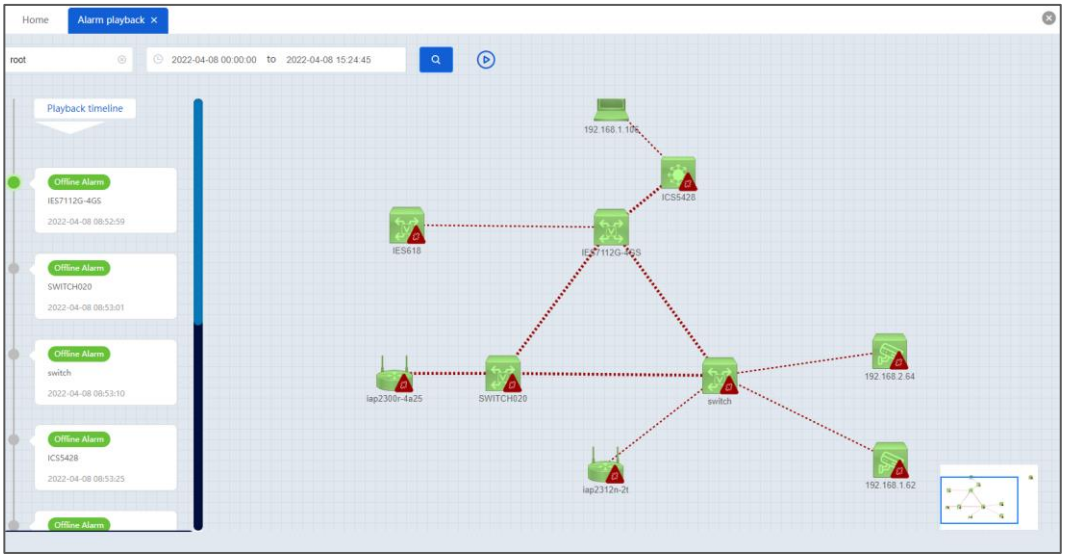
On the "Alarm Playback" page, you can view the topology changes when history alarm events occur. To use the playback function, turn on the "Playback Switch" in “System Configuration” in advance.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm List > (Navigation Bar) Alarm Playback".

Interface Description

Screenshot of alarm playback interface:



The element description of alarm playback interface:

Interface Element	Description
	Click the "  " button to query the alarm message playback within the specified network and time period.
	Click the Play "  " button to view the changes of network topology diagram under different alarm messages.
	Pause button.
	Replay button.

10.2 Alarm Configuration

10.2.1 Event Configuration

Function Description

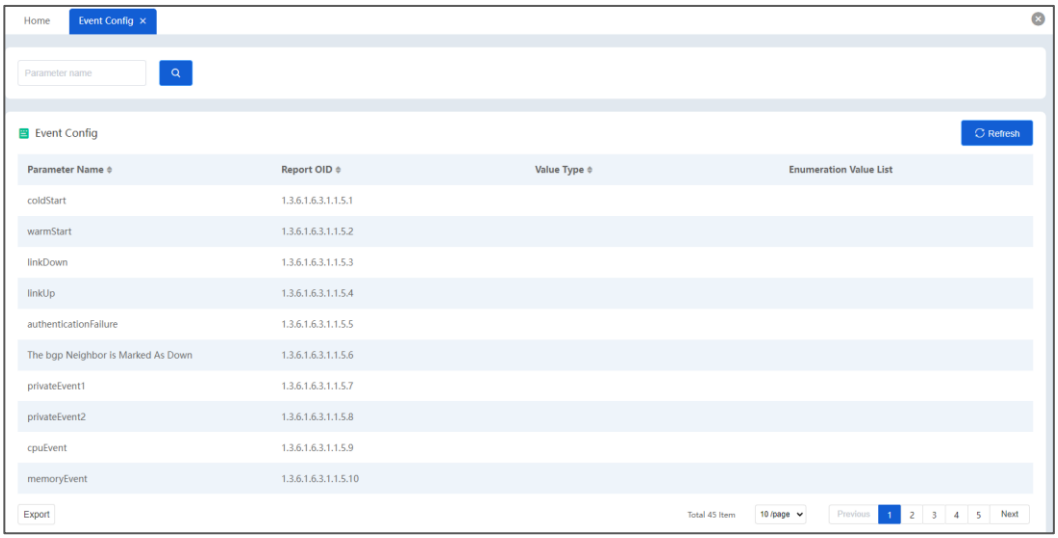
On the “Event Configuration” page, you can view the report events. The network monitoring and management system records and completes the corresponding processing according to the received Trap information of the device.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm Configuration > (Navigation Bar) Event Configuration".

Interface Description

Screenshot of event configuration interface:



Description of event configuration interface elements:

Interface Element	Description
	Click "" button to filter the parameter name.
Refresh	Click “Refresh” button to refresh the current page information.
Parameter name	The parameter name of the report event.
Report OID	The reported event or management object defined in the SNMP MIB library of the device.
Value Type	Type of report event parameter value, such as integer, character string, quantity type, time type or address type, etc.
Enumeration value list	The listed report event parameter values.

10.2.2 Alarm Definition

Function Description

On the "Alarm Definition" page, you can modify or add information such as alarm generation mode, alarm level and alarm notification. At present, the system supports four ways to generate alarms:

- System calculation: refers to the alarms generated, cleared and completely controlled by the system independently with relatively solidified business logic, such as offline alarms.
- Active report: it means that the triggering and clearing of the alarm are reported to the system independently by the device, and the triggering and clearing are of the same report type. Such as power failure alarm, ring network storm alarm, etc.
- Event trigger: it means that the trigger of the alarm is one report type, and the clearing is another report type. Such as link alarm, the trigger is reported by the linkDown event, and the clearing is reported by the linkUp event.
- Performance alarm: the system actively collects device performance data in real time, and then judges whether an alarm is needed according to the defined alarm threshold.

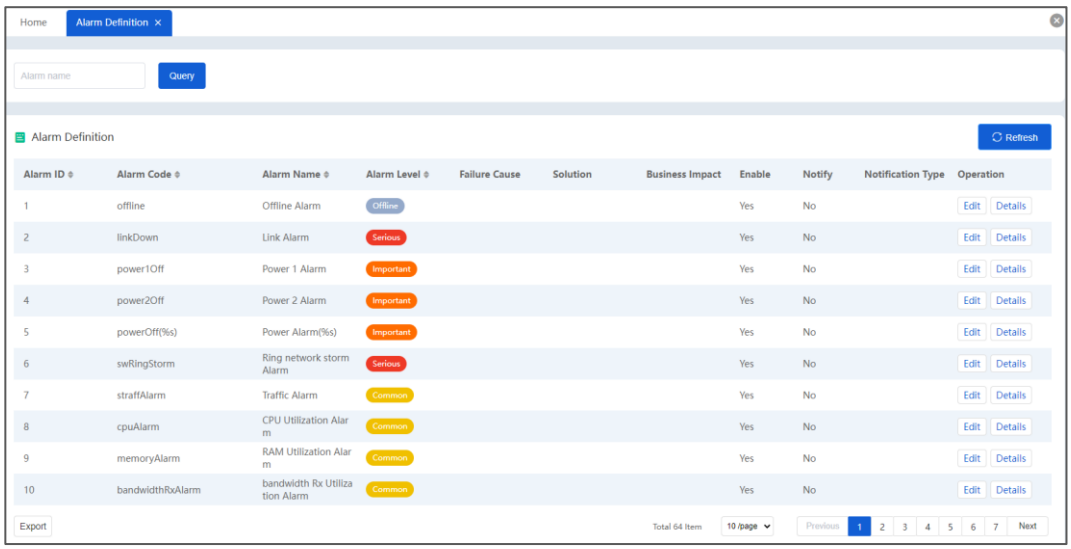
The system supports the user to define the alarm type according to the above rules, and also supports the configuration of device alarm level, causes, solutions, business impact, push rules, etc. At present, most of the main alarms supported by our device have been initialized to the system platform. Users only need to modify the alarm level and push rules according to their needs.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm Configuration > (Navigation Bar) Alarm Definition".

Interface Description

Screenshot of alarm definition interface:



Description of defining alarm interface elements:

Interface Element	Description
Query	Click "Query"button to filter the alarm name.

Interface Element	Description
Refresh	Click “Refresh” button to refresh the current page information.
Alarm ID	The ID number of the alarm event is automatically generated when adding an event.
Alarm code	The codes of alarm events cannot be the same.
Alarm name	The name of the alarm event. Different codes can correspond to the same name.
Alarm level	The level of alarm events, supporting offline, general, important, severe and other alarms.
Failure cause	Record the cause of the alarm event.
Solution	Provide solutions to alarm events.
Business impact	The impact of alarm events.
Enable	The enabled state of the alarm events.
Notify	Notification status of the alarm event. After the alarm and notification are enabled, the corresponding maintenance personnel of each device will be automatically notified by email or SMS after the device generates an alarm.
Notification type	Notification mode of alarm events, which supports SMS or email.
Operation	Optional operations are as follows: • Click Edit to modify the configuration information of the alarm event. • Click the " Details" button to view detailed configuration information.

10.2.3 Relay Configuration

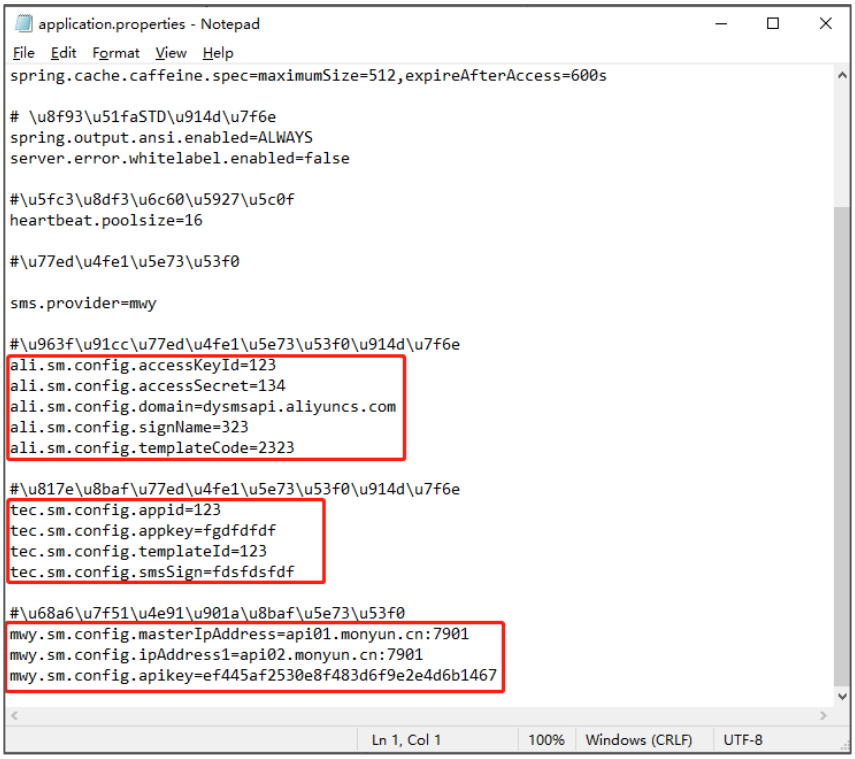
Function Description

On the "Notification Configuration" page, you can configure the notification mode of the alarm, such as email, SMS, sound, etc.

The SMS platform adopts the third-party SMS platform, which currently supports Alibaba Cloud, Tencent Cloud, Monternet Cloud, etc. If customers use other short message platforms, please contact 3onedata customer service for secondary development of the new short message platform.

When using the SMS platform, it is necessary to obtain the authentication or key information of the SMS platform in advance, and modify the application configuration

file. The file to be modified is "application.properties", which is located in the installation path folder "BlueeyesView\sms\config". As shown in the figure below, from top to bottom, there are Alibaba Cloud SMS configuration information, Tencent Cloud SMS configuration information and Monternet Cloud SMS configuration information.



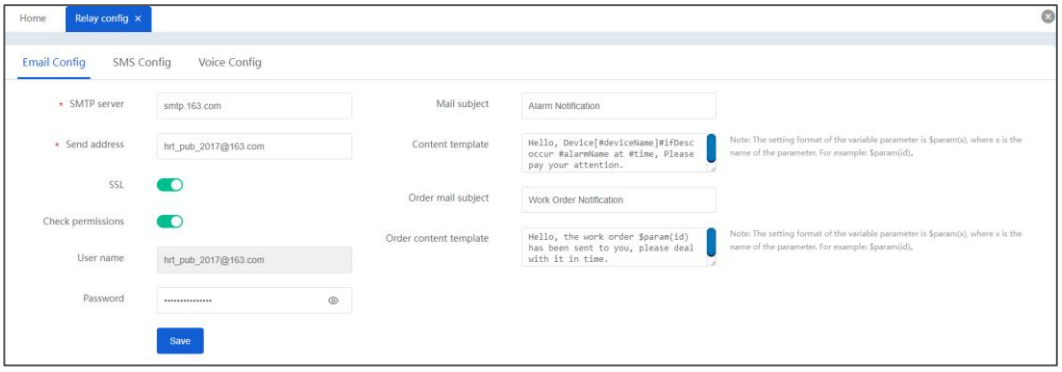
Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm Configuration > (Navigation Bar) Relay Configuration".

Interface Description 1: Emailx Configuration

On the notification configuration page, select the " Emailx Configuration" tab to enter the mailbox configuration interface.

Screenshot of Emailx configuration interface:



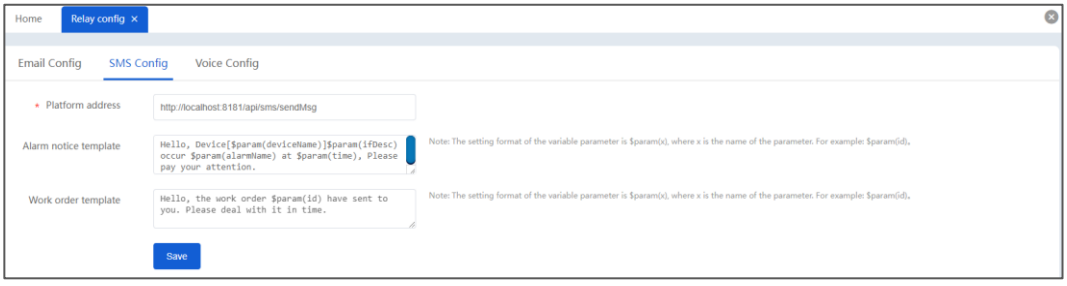
Description of mailbox interface elements:

Interface Element	Description
SMTP server.	Mailbox server address using SMTP simple mail transfer protocol provided by mailbox service provider, and mailbox server address used by sender when sending mail.
Send address	Sender's email account name.
SSL	Use SSL security protocol to encrypt data, maintain data integrity and ensure that data is sent to the correct client and server.
Check permissions	Whether the mail server needs personal identification when sending mail.
User name	Displays the sender's email account name.
Password	Sender's email account password. When checking permission is enabled, the password needs to be verified.
Mail subject	In the automatic alarm triggered by the alarm event, the email title of the mail used to to notify relevant personnel.
Content template	In the automatic alarm triggered by the alarm event, the email content template of the mail used to notify relevant personnel. The mail content can customize variables and other related parameters.
Order mail subject	In the dispatch, the email title of the mail used to to notify relevant personnel.
Order content template	In the dispatch, the email content template of the mail used to notify relevant personnel. The mail content can customize variables and other related parameters.

Interface Description 2: SMS Configuration

On the relay configuration page, select the “SMS configuration” tab to enter the SMS configuration interface.

Screenshot of SMS configuration interface:



Description of short message interface elements:

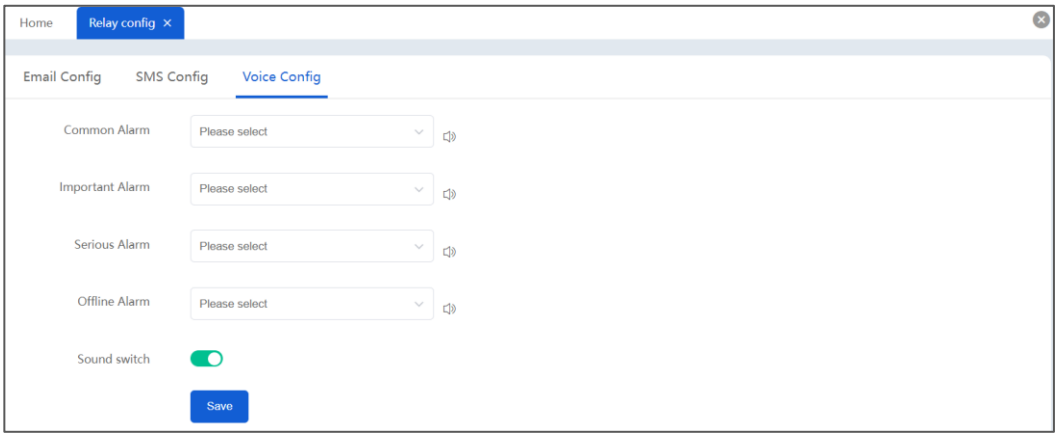
Interface Element	Description
Platform address	URL address of SMS platform. The default is the local host and port number 8181.
Alarm notice template	In the automatic alarm triggered by the alarm event, the SMS content template of the SMS used to notify relevant personnel. The variables and other related parameters of SMS content can be customized .
Work order template	In the dispatch, the SMS content template of the SMS used to notify relevant personnel. The variables and other related parameters of SMS content can be customized .

Notice
Most SMS platforms require approval of SMS templates, and SMS templates without approval cannot send SMS messages.

Interface Description 3: Voice Configuration

On the relay configuration page, select the "Voice Configuration" tab to enter the sound configuration interface.

Screenshot of voice interface configuration:



Description of short message interface elements:

Interface Element	Description
Common alarm	The sound reminder of general alarm, and 8 alarm sound choices are supported.
Important alarm	The sound reminder of important alarm, and 8 alarm sound choices are supported.

Interface Element	Description
Serious alarm	The sound reminder of severe alarm, and 8 alarm sound choices are supported.
Off-line alarm	The sound reminder of offline alarm, and 8 alarm sound choices are supported.
Sound switch	The sound switch button can open the alarm sound prompt of the local browser, and when an alarm occurs, the set alarm sound will be played.

10.2.4 Frequent Alarm

Function Description

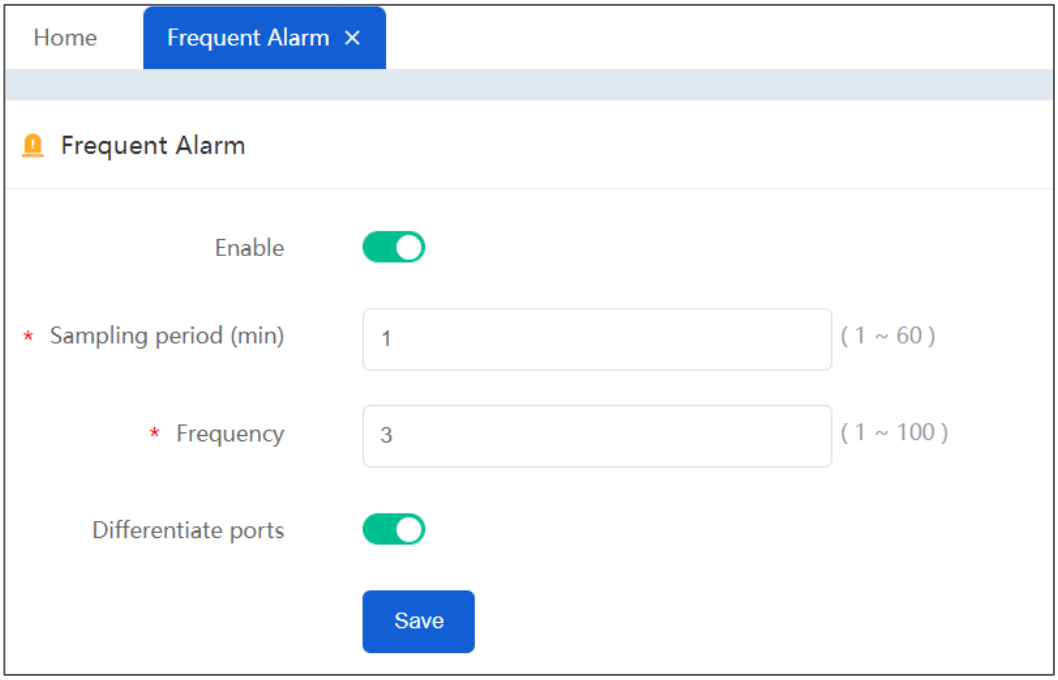
On the "Frequent Alarm" page, you can turn on the frequent alarm function and configure parameters such as sampling period and frequency. Frequent alarm is a severe alarm level, which is a protection mechanism to avoid system performance degradation caused by frequent alarms of the device. When the alarm of a certain device is detected by the system, and it occurs/recovers repeatedly for a certain number of times within the set time, it is decided that the device has frequent alarms. After frequent alarms occur, the system only records the new alarms/restores of this device, without processing them, so as to avoid the impact on the system caused by the intensive reporting of a single device. When the frequency of this new alarm/recovery of the device is lower than the frequent alarm rule, the frequent alarm of the device will be cancelled.

Operation Path

Open in order: "(Menu Bar) Alarm > (Navigation Bar) Alarm Configuration > (Navigation Bar) Frequent Alarm".

Interface Description

Screenshot of frequent alarm interface:



Description of short message interface elements:

Interface Element	Description
Enable	Frequent alarm enable switch button, the default state is on.
Sampling period (min)	The sampling period of the system for the same alarm event of the device ranges from 1 to 60, with unit minutes.
Frequency	The number of times that the same alarm event occurs in the device within the adoption period.
Differentiate ports	Switch button of differentiate port When enabled, the system's judgment of frequent alarms will be specific to the port of the device.

11 Statistical Analysis

11.1 Device Statistics

Function Description

On the "Device Statistics" page, you can view the following information:

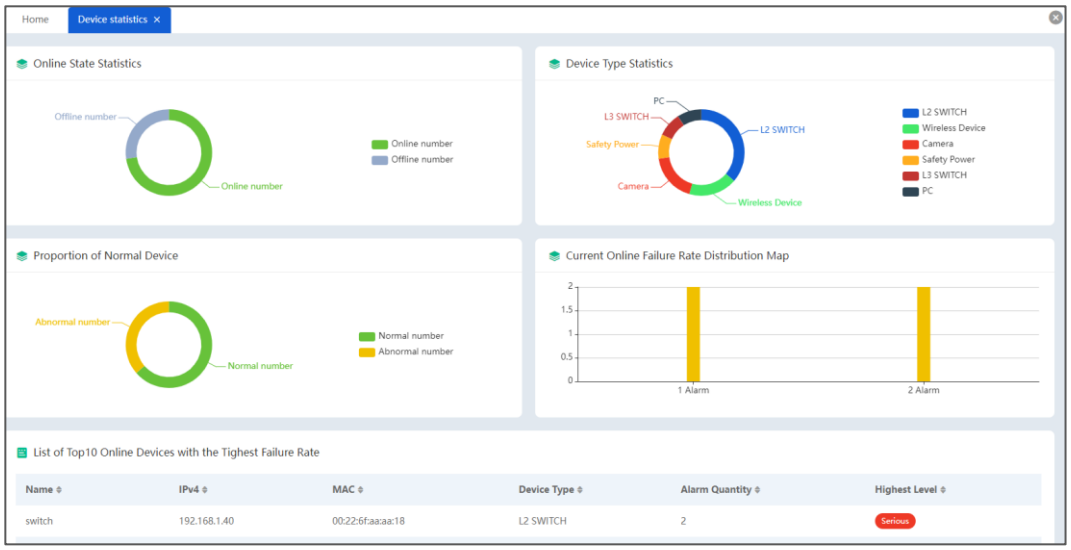
- Circular statistical chart of online state;
- Circular statistical chart of device type;
- Circular statistical chart of normal device proportion;
- Bar chart of current online failure rate distribution;
- Top10 list of online devices with the highest failure rate.

Operation Path

Open in order: (Menu Bar) Statistical Analysis > (Navigation Bar) Device Statistics.

Interface Description

Screenshot of device statistics interface:



The main element configuration description of device statistical interface：

Interface Element	Description
Online state statistics	Online statistical chart, which counts the proportion of online devices and offline devices. Move the mouse to the corresponding area to view the quantity and percentage.

Interface Element	Description
Device type statistics	Online statistical chart, which counts the types of devices in the network. The device type can be defined and modified in "Device Management > Basic Data > Device Type".
Proportion of normal device	Statistical chart of normal devices, which counts the proportion of the number of normal devices in the network and the number of devices in the alarm.
Current online failure rate distribution map	Count the distribution of the number of alarms generated by devices in the network. Move the mouse to the corresponding area to determine the number of devices and alarms.
List of Top10 online devices with the highest failure rate	**Status bar of Top10 online devices with the highest failure rate**
Name	The name of the device, which defaults to the IP address.
IPv4	The IPv4 address of the device.
MAC	The MAC Address of the device.
Device type	The product type of the device.
Alarm quantity	Number of alarms generated by the device.
Highest level	The highest level of alarm generated by the device.

11.2 Alarm Analysis

Function Description

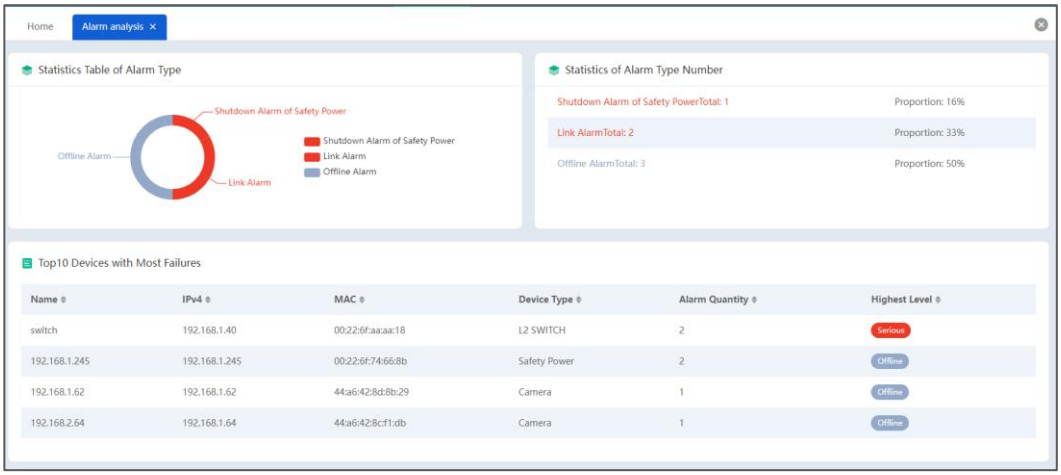
On the "Alarm Analysis" page, you can view the statistics and distribution of online alarm types of devices in the network.

Operation Path

Open in order: "(Menu Bar) Statistical Analysis > (Navigation Bar) Alarm Analysis".

Interface Description

Screenshot of alarm analysis interface:



The main element configuration description of current alarm analysis interface:

Interface Element	Description
Statistics table of alarm type	Count the proportion of alarm types and alarm numbers of device in the network by ring graph. Move the mouse to the corresponding area to view the quantity and percentage.
Statistics of alarm type number	Count the alarm types, alarm numbers and number percentage of device in the network.
Top10 devices with the most failures	**Status bar of Top10 devices with the most failures**
Name	The name of the device, which defaults to the IP address.
IPv4	The IPv4 address of the device.
MAC	The MAC Address of the device.
Device type	The product type of the device.
Alarm quantity	Number of alarms generated by the device.
Highest level	The highest level of alarm generated by the device.

11.3 History Alarm

Function Description

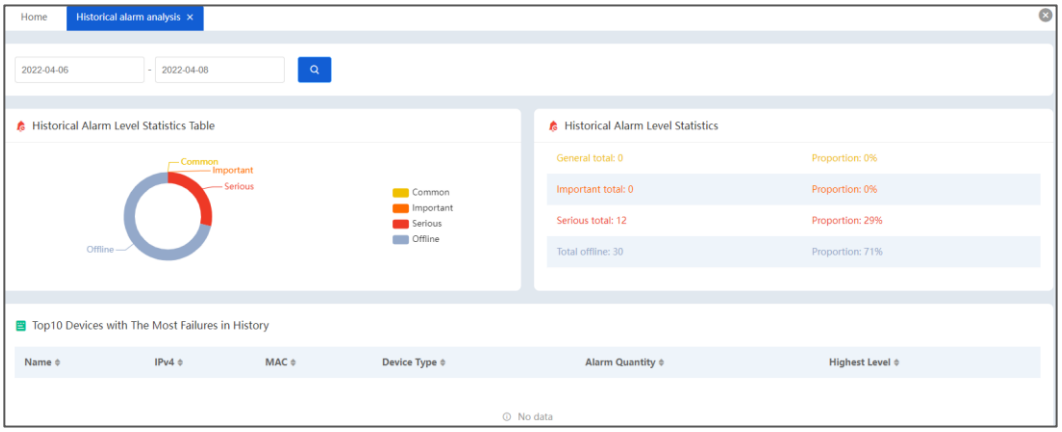
On the "History Alarm" page, you can view the statistical analysis of the alarm numbers of general, important, severe and offline levels of history alarms of device in the network.

Operation Path

Open in order: "(Menu Bar) Statistical Analysis > (Navigation Bar) History Alarm".

Interface Description

Screenshot of history alarm interface:



The main element configuration description of history alarm analysis interface:

Interface Element	Description
	Click the "" button to filter the alarm time range.
History alarm level statistics table	Count the level and proportion of history alarms in the network by circular graph. Move the mouse to the corresponding area to view the quantity and percentage.
History alarm level statistics	Count the number and percentage of each alarm level of device in the network.
Top10 devices with the most history failures	**Status bar of Top10 devices with the most history failures**
Name	The name of the device, which defaults to the IP address.
IPv4	The IPv4 address of the device.
MAC	The MAC Address of the device.
Device type	The product type of the device.
Alarm quantity	Number of alarms generated by the device.
Highest level	The highest level of alarm generated by the device.

12 System Management

12.1 Security

12.1.1 User Maintenance

Function Description

On the "User Maintenance" page, you can query or add administrators and operation and maintenance users, and modify passwords, user information, assign roles, assign data permissions and delete existing users.

Note

- System administrators can manage all users.
- Other users can only manage users created by themselves.
- Other users can't authorize more than their own permissions.

Operation Path

In the function selection area, click "System" and select "Security > User Maintenance" in the left navigation bar to enter the user maintenance interface.

Interface Description

Screenshot of user maintenance:

The main element configuration description of user maintenance interface:

Interface Element	Description
Account	User account name
Full name	The full account name of the user.
Status	Enabled state of this account: • Enabled • Disabled
User type	User account type: • Management • Operation and maintenance
Cellphone	User's mobile phone number
Mailbox	The mailbox number of the user
Remark	The remark information of the user
Operation-Edit Password	Click the "Edit Password" button and enter the "Old Password", "New Password" and "Password(again)" to modify the user password.
Operation-Edit User	Click “Modify” to modify the user's full name, user type, company name, cellphone, email address, status, notes and other information on the “Modify User” page.
Operation-Assign Role	Click "Assign Role" to select the role corresponding to the user on the "Assign Role" page and confirm.
Operation-Data Permission	Each user can independently assign data permission, and data permission can manage the specified device by controlling the network that users can access. Note: It is recommended to set the data permissions after the network planning is completed.
Operation-Delete	Click “Delete” to delete this user data information.
	Enter the user name in the "User Name" input box and click the "  "button to query the user.
Refresh	Click the "Refresh" button to update and display the latest user information.
Add	Click the “Add” button to add user information, such as user information, role information and data permission.

12.1.2 Role Maintenance

Function Description

On the “Role Maintenance” page, you can add roles.

- Role-based authorization management enables unified allocation of operation permissions through the role;
- Users get operation permission by assigning roles, and one user can have multiple roles, and its permission is the union of the permissions of all roles;

Note

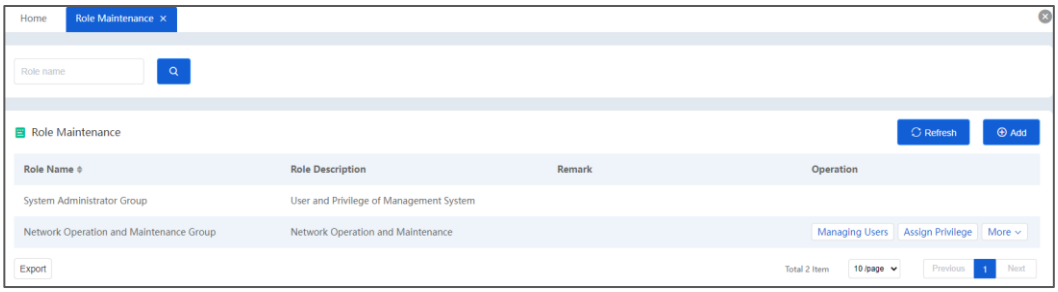
- System administrators can manage all roles;
- Other users can only manage their own created roles.
- Users can't authorize roles beyond their own permissions.

Operation Path

In the function selection area, click “System”, and select: “Security > Role Maintenance” in the left navigation bar to enter the role management interface.

Interface Description

The screenshot of Role Maintenance:



Main element configuration description of role management interface:

Interface Element	Description
Role name	Role name of the user
Role description	The user's role description, such as the permissions assigned by the role, etc
Remark	Remark information of the role
Operation-Managing Users	Click the " Managing Users " button to add existing users to this role
Operation-Assign Privilege	Click " Assign Privilege " to select functional permissions, such as home, topology diagram, topology management,

Interface Element	Description
	device management, fault management, performance monitoring, statistical analysis, system management, etc.
Operation-Edit Role	Click " Edit Role" to modify the role name, role description and remarks, etc.
Operation-Delete	Click "Delete" to delete this role information.
	You can enter the name of the role in the input box of "Role Name" and click the "button to query the role
Refresh	Click the "Refresh" button to update and display the latest role information
Add	Click the "Add" button to add the role name, role description, remarks, etc.

12.1.3 Online User List

Function Description

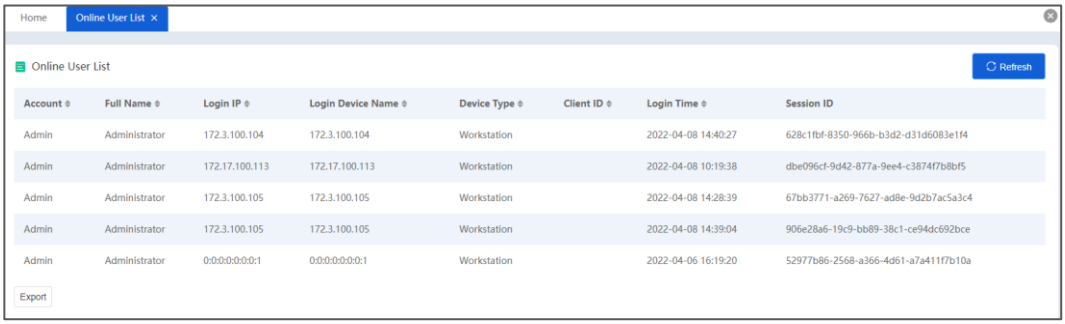
On the “Online User List” page, you can view online user information.

Operation Path

In the function selection area, click "System" and select " Security > Online User List" in the left navigation bar to enter the online user list interface.

Interface Description

Screenshot of online user list interface:



The main element configuration description of online user list interface:

Interface Element	Description
Account	User account name
Full name	The full account name of the user.
Login IP	IP address information of online users

Interface Element	Description
Login device name	Device name of online user.
Device type	Device type of online user
Client ID	Client ID number of online user
Login time	Login time of online users, format: year-month-day hour: minute: second
Session ID	Session ID number of online user assigned by the system

12.1.4 Authorization Information

Function Description

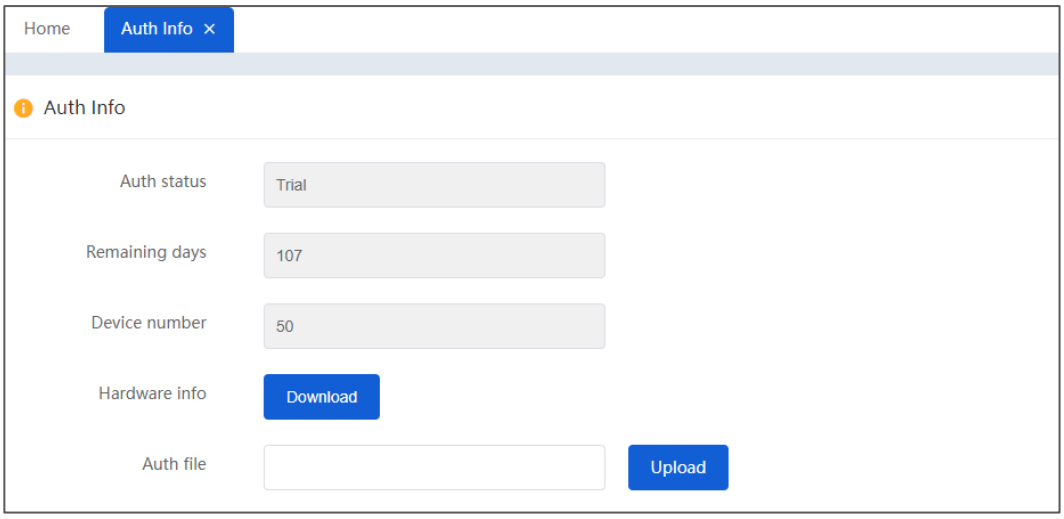
On the "Authorization Information" page, you can view the relevant authorization information of this network management system.

Operation Path

In the function selection area, click "System" and select " Security > Authorization Information" in the left navigation bar to enter the authorization information interface.

Interface Description

Screenshot of authorization information interface:



The main element configuration description of authorization information interface:

Interface Element	Description
Authorization status	Authorization status of network management system
Remaining days	Remaining days of authorization authority
Device number	Number of devices that can be managed by the network

Interface Element	Description
	management system
Hardware information	Click the "Download" button to download the hardware information "licenseTemp.bin" of the host. When obtaining the formal authorization file of the system, the system and the host will be bound according to the provided hardware information.
Authorization file	Click the "Upload" button, and select the obtained authorization file "license.bin" for system authorization.

12.2 Configuration

12.2.1 Network

Function Description

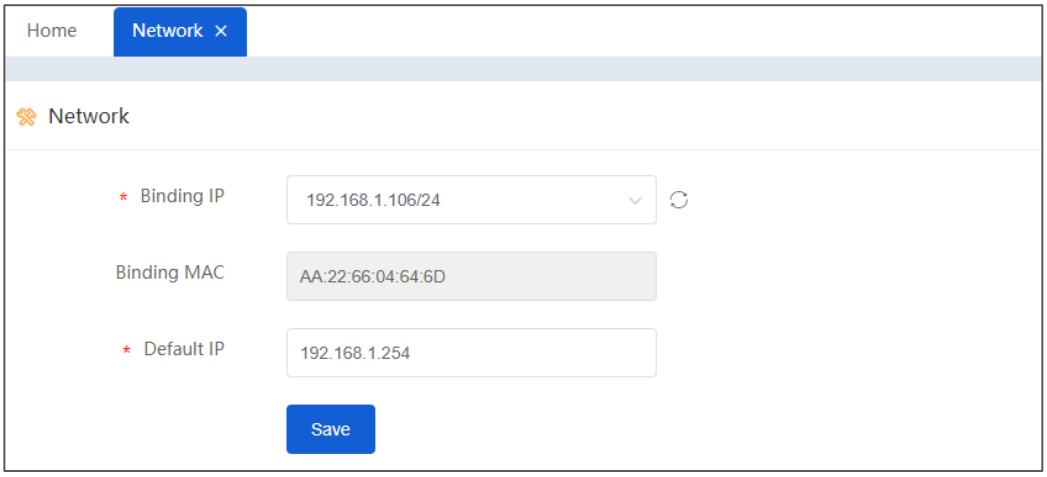
The default binding IP address of BlueEyesView is 0.0.0.0, which can monitor all the networks where the server is located. However, if the server is located in multiple networks, and make BlueEyesView only monitor the managed network in a targeted manner, it is necessary to set the binding network card of BlueEyesView system to the one that accesses the managed network.

Operation Path

In the function selection area, click "System" and select " Configuration > Network " in the left navigation bar to enter the network card settings interface.

Interface Description

Screenshot of network card settings interface:



The main element configuration description of network card settings interface:

Interface Element	Description
Binding IP	Binding IP information of the specified network card
Binding Mac	Binding Mac address corresponding to the network card
Default IP	Default factory IP address information of the device

12.2.2 UDP

The communication protocols between BlueEyesView and devices include the second generation protocol and the third generation protocol of 3onedata network management, which are all based on UDP. Therefore, before discovering devices, it is necessary to check the configuration of UDP to check whether the preset configuration is consistent with the actual situation and whether the corresponding monitoring service is started normally.

UDP configuration is for 3onedata devices, mainly to check whether the monitoring port of the platform and the monitoring port of the devices are consistent with the reality. Whether the default configuration of the platform is the same as the factory configuration of our device, if the user changes the UDP communication configuration of the device, it is necessary to make corresponding changes on the platform; Otherwise, keep the default configuration.

Function Description

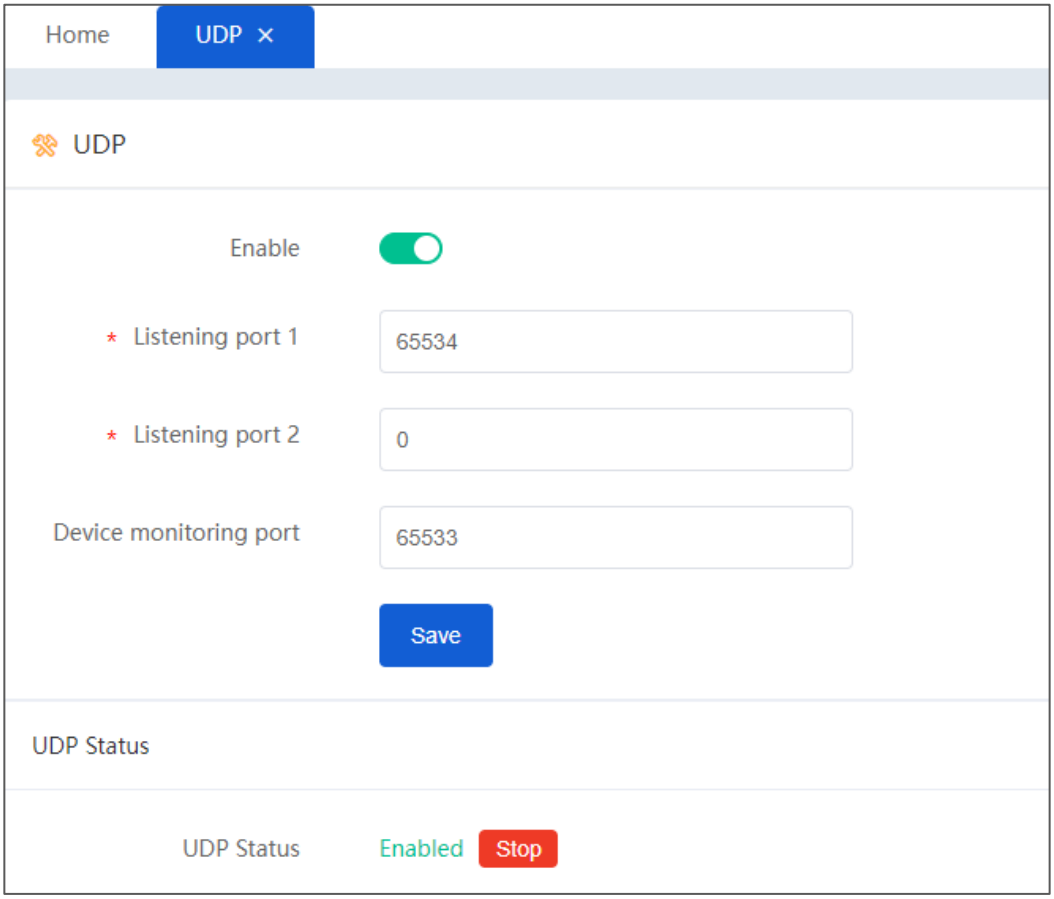
On the “UDP” page, you can configure UDP monitoring ports and device monitoring ports.

Operation Path

In the function selection area, click "System" and select "Configuration > UDP " in the left navigation bar to enter the UDP settings interface.

Interface Description

Screenshot of UDP interface:



The main element configuration description of UDP settings interface:

Interface Element	Description
Enable	UDP enable switch • Enable • Disable
Listening port 1	Set the monitoring port 1 of network management, which is 65534 by default and the value range is 0-65535. Note: This parameter needs to be set to 65534 when the connected device is 3onedata device.
Listening port 2	Set the monitoring port 2 of network management, which is 0 by default and the value range is 0-65535. Note:

Interface Element	Description
	• When the accessed devices are not 3onedata devices, and UDP network management monitoring port needs to be set, it can be set here. • Network management monitoring port 2 and network management monitoring port 1 cannot be duplicated.
Device monitoring port	The monitoring port of the device, 3onedata device needs to be set to 65533, and the value range is 0-65535.
UDP Status	Display UDP status: • Enabled; • Stop

12.2.3 SNMP General

Function Description

The default SNMP access configuration of the device is the access configuration of the SNMP Agent enabled on the device, including SNMP version, security information, etc. The platform tries to connect devices based on this configuration when performing device discovery.

SNMP Protocol Version

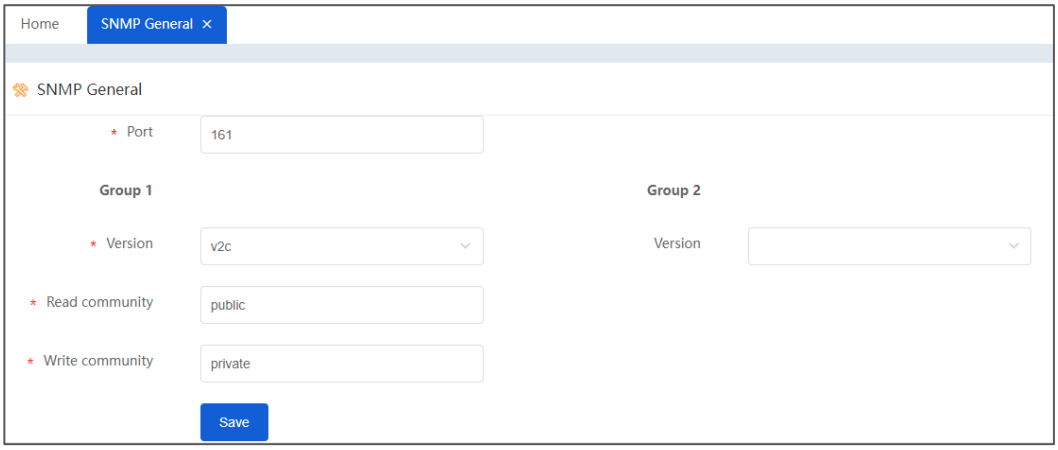
At present, SNMP Agent in the device supports SNMP v1 version, SNMP v2c and SNMP v3 version. SNMP v1, SNMP v2c adopt community name authentication, SNMP message of community name without device authentication will be discarded. SNMP community name is used for defining the relationship of SNMP, NMS and SNMP Agent. Community name plays a role similar to password, and can limit SNMP NMS to access SNMP Agent in device.

Operation Path

In the function selection area, click "System ", and select "Configuration > SNMP General " in the left navigation bar to enter the SNMP general settings interface.

Interface Description

Screenshot of SNMP General interface:



The main element configuration description of SNMP configuration interface:

Interface Element	Description
Port	SNMP protocol monitoring port of the device, the default is: 161
Group 1/Group 2	When different default SNMP versions appear in the network management, they can be set in different groups. Note: When there are more than two groups of default SNMP versions in the network management, it is recommended to set the device version to be less than or equal to the two groups of default SNMP versions before setting the device SNMP.
Version	Default SNMP version of the device, options: • V1 • V2C • V3
Read community	Read only privilege view name selection. Note: This function is only supported when the default SNMP version is V1 or V2C.
Write community	Read-write privilege view name selection. Note: This function is only supported when the default SNMP version is V1 or V2C.
Account number	Device SNMP account information Note: This function is only supported when the default SNMP version is V3.
Security level	Security level of device SNMP, options: • NOAUTH_NOPRIV • AUTH_NOPRIV • AUTH_PRIV Note: This function is only supported when the default SNMP version is V3.

Interface Element	Description
Authentication protocol	Authentication information filling, two authentication methods optional: • MD5: Information abstract algorithm 5; • SHA: Secure hash algorithm.
Authentication password	Authentication password information cannot exceed 20 characters.
Privacy protocol	V3 user data encryption algorithm, options: • DES: data encryption algorithm; • DES: the encryption algorithm for the transition from DES to AES; • AES-128: Advanced encryption algorithm with key length of 128; • AES-256: Advanced encryption algorithm with key length of 256;
Privacy password	V3 user data encryption password information, no more than 20 characters.

12.2.4 Trap Settings

Function Description

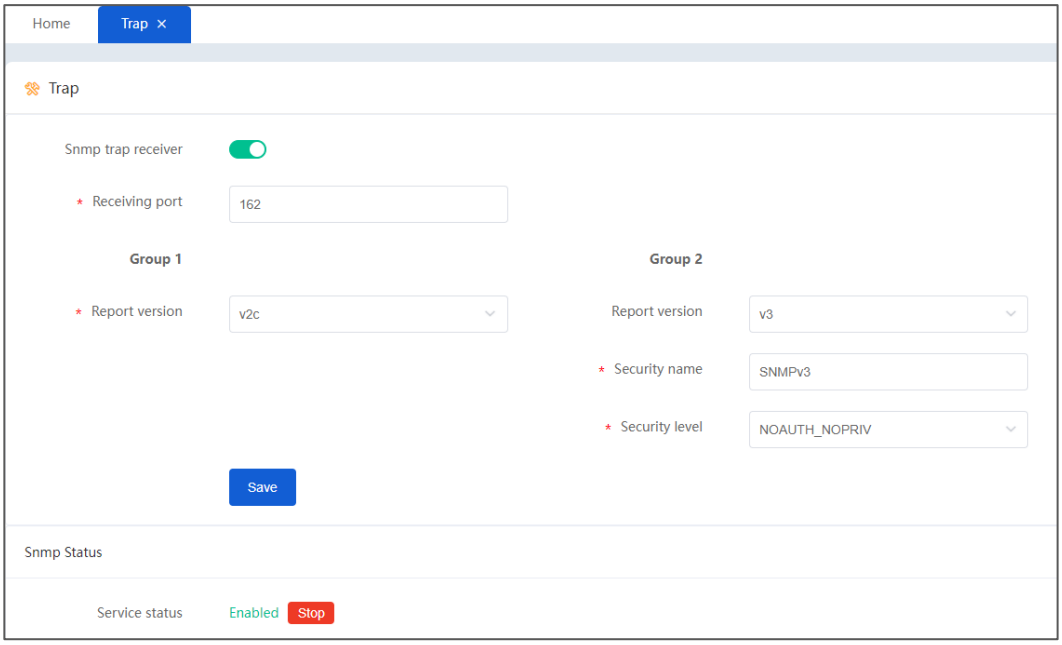
The SNMP Trap Receiver configuration is used to set the report port and security information when the platform receives the report of the Trap device. Once this configuration is set, the trap configuration on the device must be consistent with that here. Otherwise, the reported information of the device cannot be reported to the network management normally.

Operation Path

In the function selection area, click "System ", and select "Configuration > Trap" in the left navigation bar to enter the Trap Settings interface.

Interface Description

Screenshot of Trap setting interface:



The main element configuration description of Trap settings interface:

Interface Element	Description
Snmp Trap Receiver	Enabled switch of Trap Settings: • Started; • Stop
Receiving port	Monitoring port for network management, the default is 162
Group 1/Group 2	When different default SNMP versions appear in the network management, they can be set in different groups.
Report version	Default SNMP version of network management, options: • V1 • V2C • V3
Security Name	User name corresponding to report version V3
Report level	Reported security level: • NOAUTH_NOPRIV • AUTH_NOPRIV • AUTH_PRIV
Authentication protocol	Authentication information filling, two authentication methods optional: • MD5: Information abstract algorithm 5; • SHA: Secure hash algorithm.
Authentication password	Authentication password information cannot exceed 20 characters.
Privacy protocol	V3 user data encryption algorithm, options:

Interface Element	Description
	• DES: data encryption algorithm; • DES: the encryption algorithm for the transition from DES to AES; • AES-128: Advanced encryption algorithm with key length of 128; • AES-256: Advanced encryption algorithm with key length of 256;
Privacy password	V3 user data encryption password information, no more than 20 characters.
Service status	Trap service status: • Started; • Stop
Save	Click the "Save" button to save the Trap setting information.

12.2.5 WEB Proxy

Function Description

On the “WEB Proxy” page, you can configure the IP address and port number of the proxy server. Users can access the WEB interface of devices in other network segments of the system through the WEB proxy function.

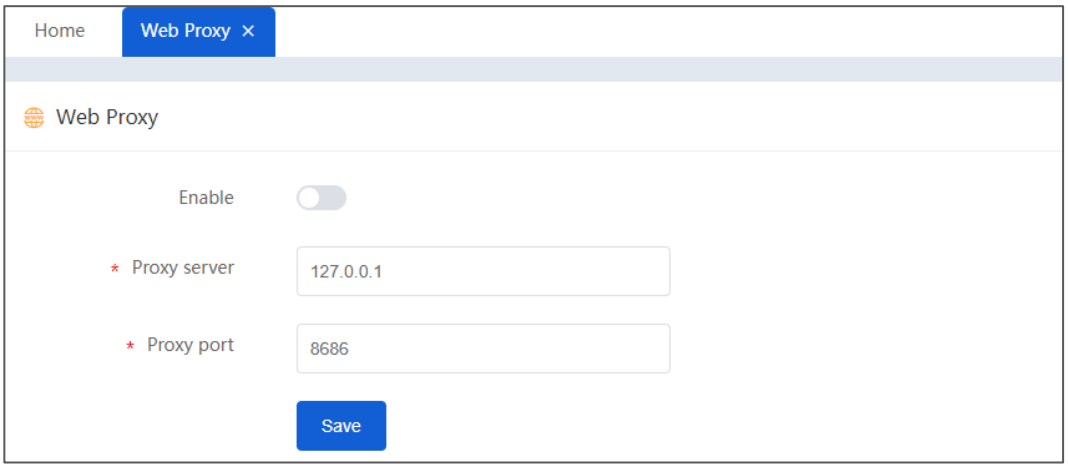
When there is isolation between user network and device network, the user will not be able to directly access the local configuration page of the device through the browser. If the system is equipped with dual network cards, which belong to network segment A and network segment B respectively, when the client in network A wants to access the device WEB in network B, it can directly access it after using the WEB proxy. After enabling the local WEB proxy, when users want to view the local web page of a certain device, the front end first submits an application to the back end, and the back end will dynamically create an access proxy to the device, and then return the proxy address to the front end. The front end can access the local webpage of the device according to the returned proxy address. When the proxy connection is idle for a certain period of time, the system will disconnect the proxy connection actively.

Operation Path

In the function selection area, click "System", and select "Configuration > WEB Proxy" in the left navigation bar to enter the WEB proxy interface.

Interface Description

Screenshot of WEB proxy interface:



Main elements configuration descriptions of WEB proxy interface:

Interface Element	Description
Enable	Proxy enable switch button. Notice: In Windows system, to start the WEB proxy function, check "Enable WEB proxy server" in the system startup interface, and then click "Enable button to start the proxy service.
Proxy server	IP address of proxy server. Note: • IP address of the proxy server, generally the IP address of the currently accessed system. • When accessing other network segment devices through proxy server, you need to access them through IE icon in topology diagram.
Proxy port	Port number of proxy server.

12.2.6 Database Backup

Function Description

On the “Database Backup” page, you can back up the database files manually or automatically. Database backup is only applicable to BlueEyeView service and database deployed on the same computer. The system uses MySQL database and MySQL's own logical backup tool mysqldump to realize data backup.

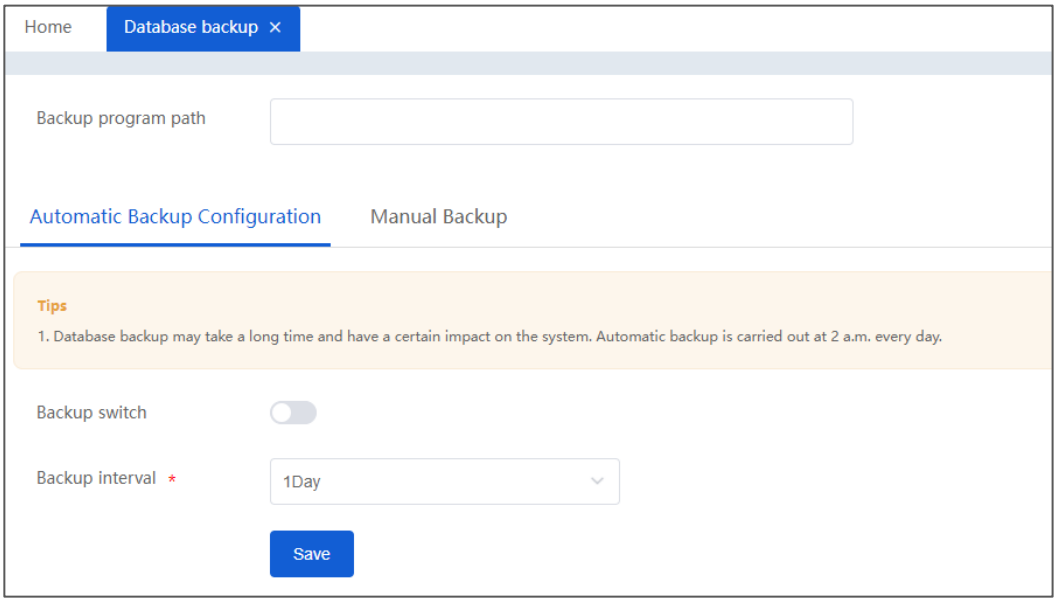
Operation Path

In the function selection area, click "System" and select "Configuration > Database Backup" in the left navigation bar to enter the database backup interface.

Interface Description 1: Automatic Backup Configuration

In the database backup interface, select the “Automatic Backup Configuration” tab.

Screenshot of automatic backup configuration interface:



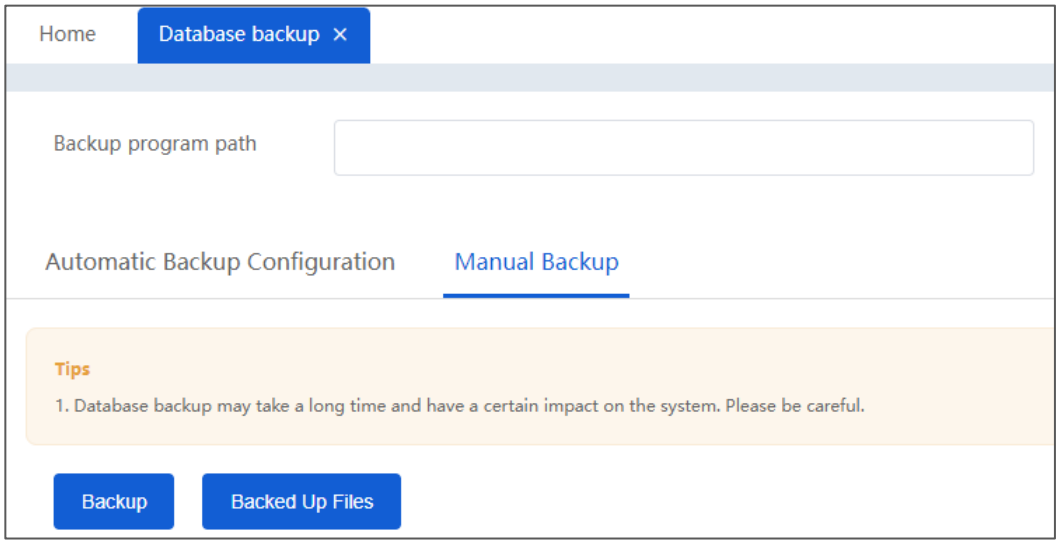
The main element configuration description of automatic backup configuration interface:

Interface Element	Description
Backup program path	The storage path of the backup tool can be left blank, but when the system cannot automatically identify the backup tool mysqldump, you need to manually enter the storage path of the backup program. Note: • Under the Windows system, you can find the location of the configuration program through the command "where mysqldump /R C:\" in the command line. • Under Linux system, the location of the configuration program can be found by the command "whereis mysqldump" in the terminal.
Backup switch	Backup switch button of database, which is off by default.
Backup interval	Time interval for system backup database, with the value range of 24-8760, unit: hour.

Interface Description 2: Manual Backup

In the database backup interface, select the “Manual Backup” tab.

Screenshot of manual backup configuration interface:



The main element configuration description of manual backup configuration interface:

Interface Element	Description
Backup program path	The storage path of the backup tool can be left blank, but when the system cannot automatically identify the backup tool mysqldump, you need to manually enter the storage path of the backup program. Note: • Under the Windows system, you can find the location of the configuration program through the command "where mysqldump /R C:\" in the command line. • Under Linux system, the location of the configuration program can be found by the command "whereis mysqldump" in the terminal.
Backup	Click “Backup” button to implement manual backup.
Backed up files	Click the "Backed Up File" button to view the file name, size and backup time of the backed up database.

12.2.7 Data Clean

Function Description

On the “Data Clean” page, you can clean up log files and database files.

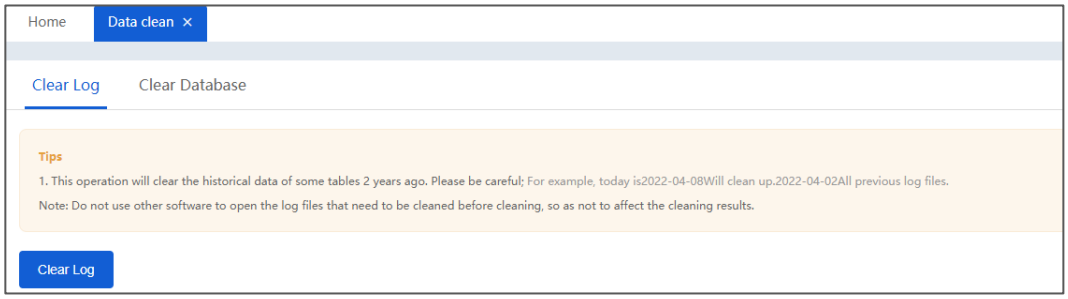
Operation Path

In the function selection area, click "System ", and select "Configuration > Data Clean" in the left navigation bar to enter the data cleaning interface.

Interface Description 1: Clear Log

In the data clean interface, select the “Clear Log” tab.

Screenshot of log cleaning interface:



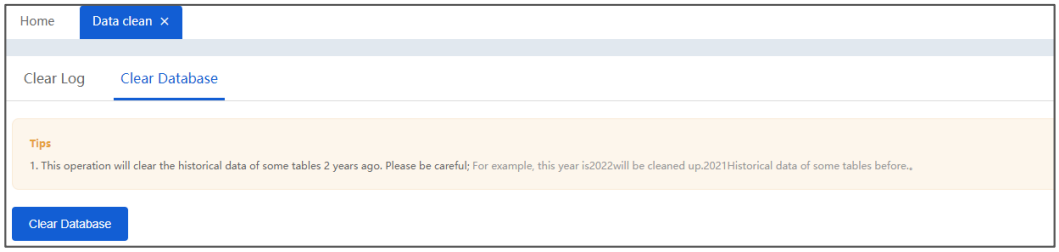
The main elements configuration description of log cleaning interface:

Interface Element	Description
Clear Log	Click the "Clear Log" button to clean up all log files before 7 days.

Interface Description 2: Clear Database

In the data clean interface, select the “Clear Database” tab.

Screenshot of clear database interface:



The main element configuration description of database cleaning interface:

Interface Element	Description
Clear Database	Click the "Clear Database" button to clean up the history data of some tables 2 years ago.

12.2.8 North Interface

Function Description

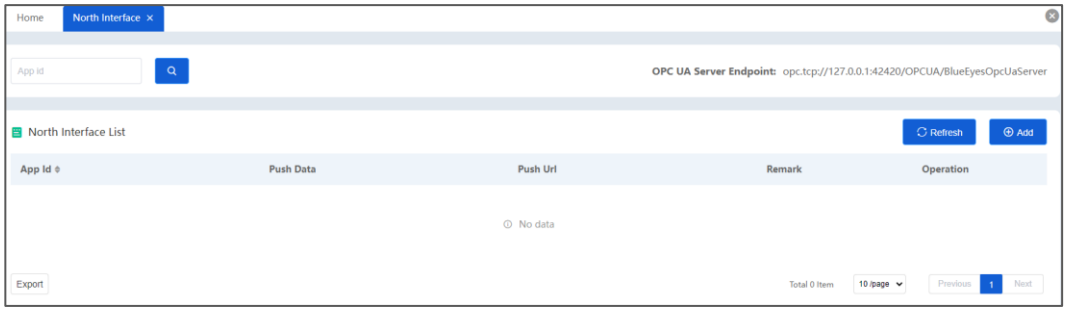
BlueEyesView provides a series of RESTful API interfaces for the next-level network management system as northbound interfaces. Through the northbound interface, external applications can obtain network interface information, device information, topology information and alarm information, etc. When obtaining the authorization service, the system can assign an APPID and an APPSecurity to users, and then realize data communication according to certain calling methods and signature calculation algorithms. See Appendix Northbound Interface Configuration for details.

Operation Path

In the function selection area, click "System" and select "Configuration > North Interface" in the left navigation bar to enter the northbound interface.

Interface Description

Screenshot of north interface:



The main element configuration description of northbound interface:

Interface Element	Description
	Click the "  "button to query the specified APP ID.
Refresh	Click “Refresh” button to refresh the current page.
Add	Click "Add" button to add APPID and APPSecurity, and open the northbound interface application.
App Id	Application ID, the APPID assigned by the system obtained at the time of authorization.
Push data	The status of push data, after it is enabled, it can send data to the specified URL address, and this function is temporarily reserved.
Push URL	URL address for receiving push data.

Interface Element	Description
Remark	Remarks information.
Operation	Optional operations are as follows: • Edit; • Delete.

12.2.9 Data Dictionary

Function Description

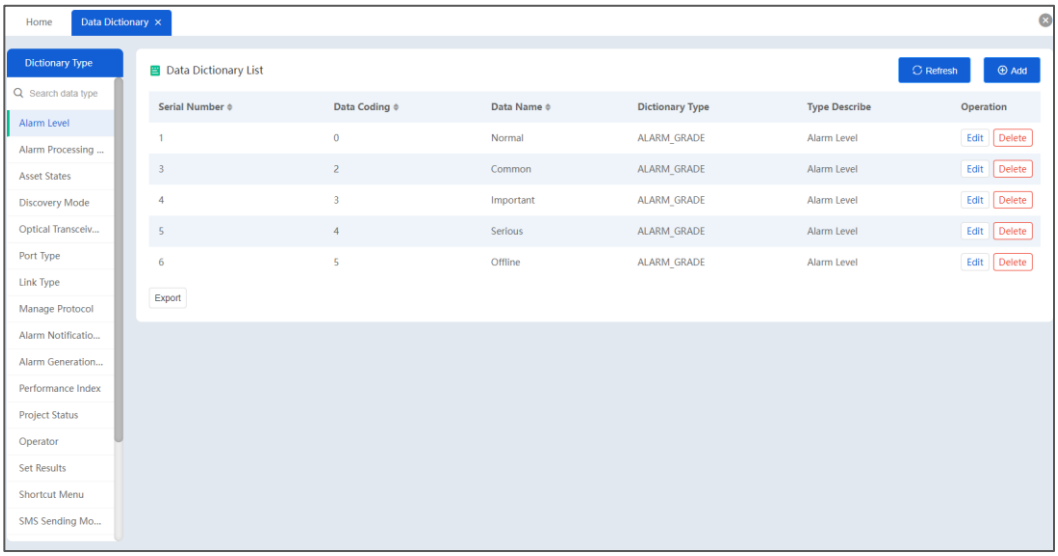
On the "Data Dictionary" page, you can view the types of various data for encoding translation of database in network management system.

Operation Path

In the function selection area, click "System" and select "Configuration > Data Dictionary" in the left navigation bar to enter the data dictionary interface.

Interface Description

Screenshot of data dictionary:



12.2.10 System Configuration

Function Description

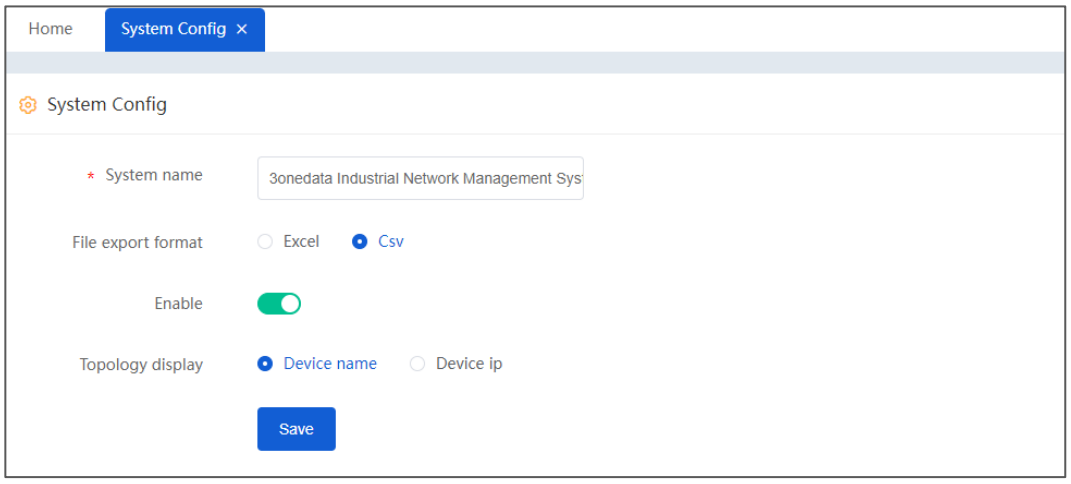
On the “System Configuration” page, you can set the name of the management system, the file format of all export lists, and the event playback switch control.

Operation Path

Open (Menu Bar) System > (Navigation Bar) Configuration > (Navigation Bar) System Configuration" to enter the system configuration interface.

Interface Description

Screenshot of system configuration interface:



The main elements configuration description of system configuration interface:

Interface Element	Description
System Name	Set the name of this network management system.
File export format	The format of exported files in this network management system can be selected as follows: • Excel format • Csv format
Enable	The default state of the playback switch is off. After the playback function is enabled, the system will support alarm playback and AP playback.
Topology display	The label of the selected device in the topology diagram is displayed as "Device Name" or "Device IP". Note: It displays as "Device Name" by default.
Save	Click "Save" button to save the configuration of this page.

12.3 System Log

12.3.1 User Login

Function Description

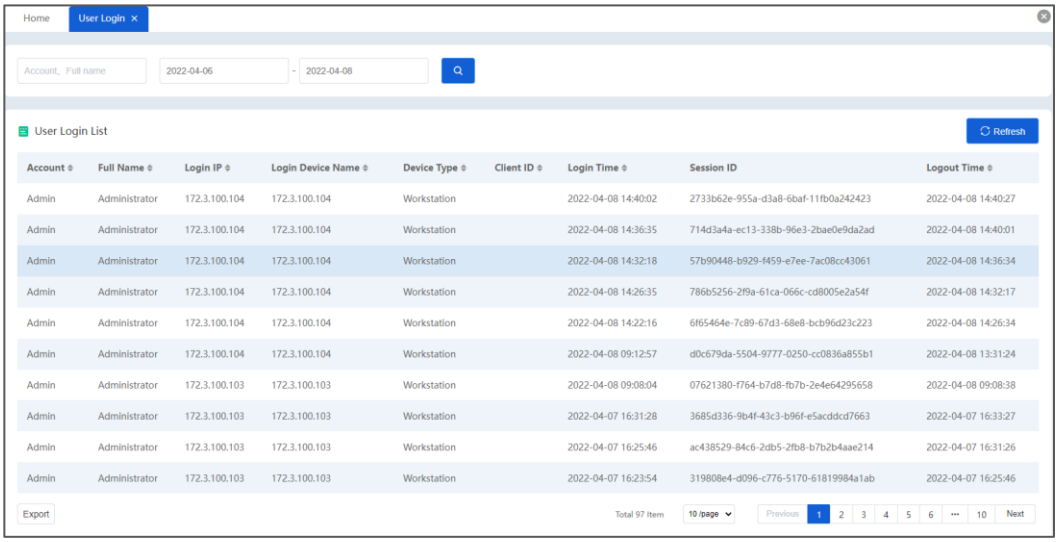
On the “User Login” page, you can view information about user login.

Operation Path

In the function selection area, click “System”, and select “Logs > User Login” in the left navigation bar to enter the user login log interface.

Interface Description

Screenshot of user login interface:



The main element configuration description of user login log interface:

Interface Element	Description
Account	Account name of logged-in user
Full name	Full account name of logged-in user
Login IP	IP address of logged-in user
Login device name	Device name of logged-in user
Device type	Device type of logged-in user
Client ID	ID of logged-in user
Login time	User login time, the format: year-month-day hour: minute: second.
Session ID	Session ID number of the logged-in user assigned by the system

Interface Element	Description
Logout time	The time when the user logs out of the system, the format: year-month-day-hour: minute: second.
	Enter the account number or full name, select the time period, and click "  " to query the corresponding user login log.
Refresh	Click “Refresh” to update the latest user login log.

12.3.2 User Operation

Function Description

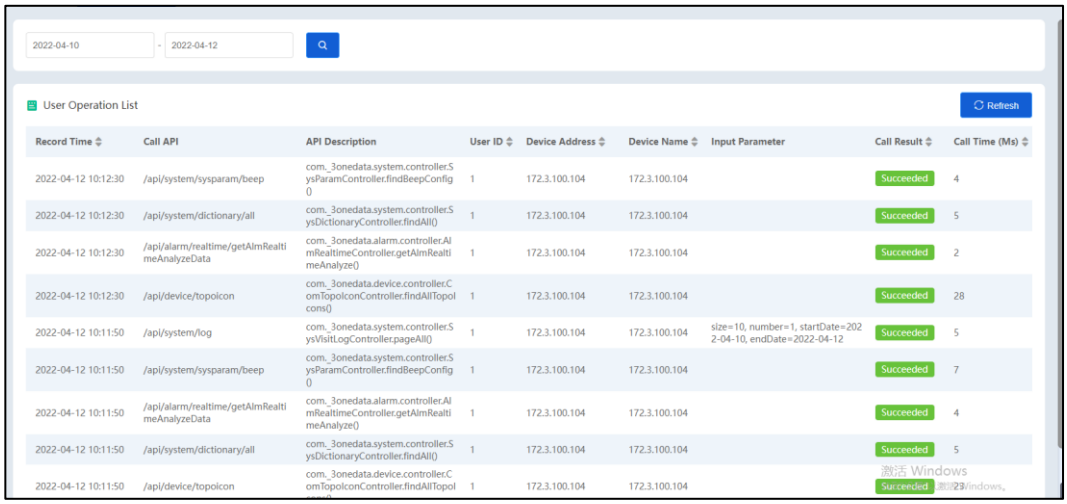
On the “User Operation” page, you can view information about user operations.

Operation Path

In the function selection area, click “System”, and select “Logs > User Operation” in the left navigation bar to enter the user operation log interface.

Interface Description

Screenshot of user operation interface:



The main element configuration description of user operation log interface:

Interface Element	Description
Record time	Record the time of user operation in the format of: year-month-day-hour: minute: second.
Call API	The API path corresponding to the function
API description	Class corresponding to API information
User ID	ID number of the operation user

Interface Element	Description
Device address	Device IP address of the operation user
Device name	Device name of the operation user
Input parameter	Parameter information of the operation user
Call result	Result information of whether the operation is successful or not.
Call time (ms)	Time of operation call, unit: milliseconds
Remark	Operation remark information

13 Appendix 1: Northbound Interface Configuration

13.1 Interface Security Specification

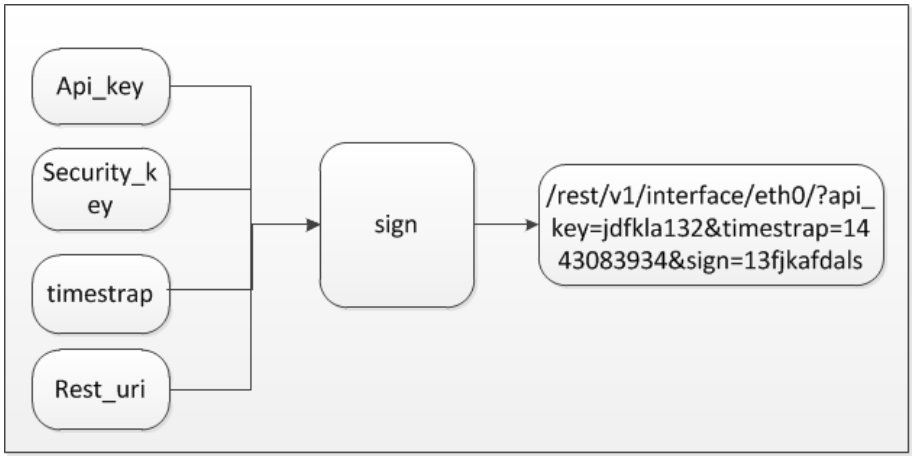
13.1.1 Introduction

The northbound interface is a series of RESTFul API interfaces provided by BlueEyesView for the next-level network management system. Through these interfaces, the superior network management can actively acquire the network information, device information, real-time alarm and history alarm information of device, performance data and other data of BlueEyesView. If the superior network management implements the push interface according to the BlueEyesView agreement, then BlueEyesView can also push the alarm information to the superior network management in real time.

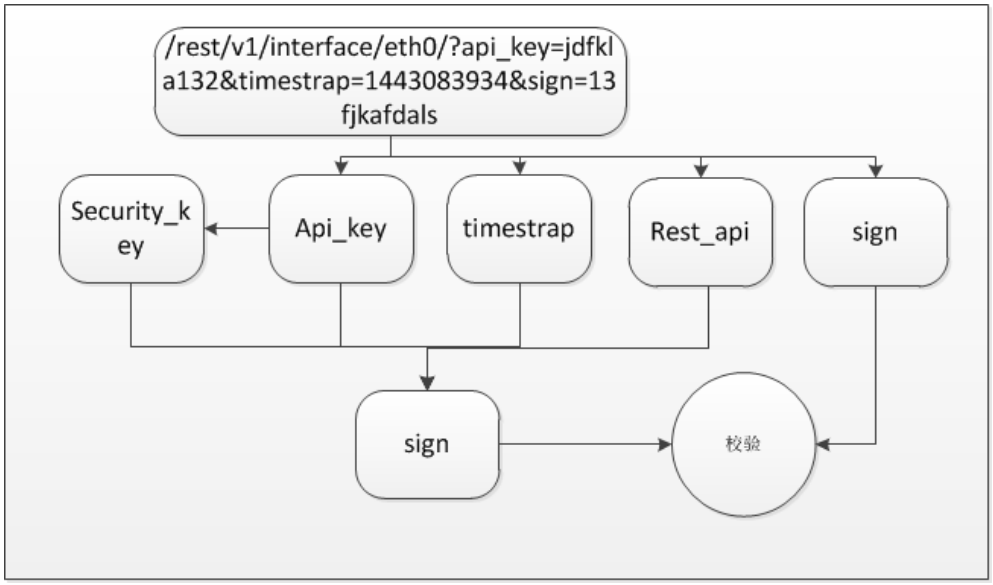
13.1.2 Interface Security Mechanism

The northbound interface of BlueEyesView uses a signature-based security mechanism.

The caller calculates the signature and attaches it to the request.



The responder receives the request, calculates the signature with the same algorithm, and then compares it with the signature in the request. If the verification passes, the interface request content will be returned; if it fails, the error code will be returned.



Notes

The instance does not show the actual algorithm, and the transmission mode of the actual parameters is not completely consistent with the reality.

13.1.2.1 Global Error Code

Error code	Error description
404	Request address error
420	The request header lacks necessary check information.
421	Illegal northbound interface user
422	Signature value calculation error

Example:

```
{
  "timestamp": "2020-06-28 11:25:33",
  "status": 420,
  "error": "Method Failure",
```

```
  "message": "The request header lacks necessary check
information",
  "path": "/north/network"
}
}
```

13.1.2.2 Acquire Authorization

All northbound interface users must get authorization from BlueEyesView: BlueEyesView will assign an appId and an appSecurity to each user. AppId is the identity of the caller, and appSecurity is the key for the caller to calculate the signature, and the key must not be leaked.

13.1.2.3 Signature Calculation Algorithm

Suppose there is a request: GET http://192.168.1.1: 8080/north/device? domainId=x

User appId = 12345678

User appSecurity = Vtce8TO82C1azMhW

Signature calculation method:

1、Break down the request into URL and parameter. For example, it can be broken down into:

url = http://192.168.1.1:8080/north/device

Parameter：domainId = x

2、Get current timestamp: timestamp = 1234567890

3、Put appId, appSecurity, url, timestamp and all parameters into one map, then sort the map according to key

4、Output the sorted map as characters in the format of key=value, and connect them with commas ","

5、Calculate MD5 of the connected string, which is the value of the signature.

6、Finally, put appId, timestamp and sign into the request header and send the request.

Code:

```
/**
 * Signature algorithm
 * @param appId northbound user
 * @param appSecurity northbound user key
 * @param timestamp timestamp
 * @param url request URL
```

```
 * @param parameters request parameters
 * @return signature calculation result
 */
private String calculateSign(String appId, String appSecurity, String timestamp, String url, Map<String, String[]>
parameters) {
    Map<String, String> map = new HashMap<>();
    map.put("appId", appId);
    map.put("appSecurity", appSecurity);
    map.put("timestamp", timestamp);
    map.put("url", url);
    Set<Map.Entry<String, String[]>> entrySet = parameters.entrySet();
    for (Map.Entry<String, String[]> entry: entrySet) {
        map.put(entry.getKey(), entry.getValue()[0]);
    }

    // sort
    map = MapSortUtil.sortByKeyAsc(map);
    //
    StringBuffer sb = new StringBuffer(256);
    map.entrySet().forEach(entry -> {
        sb.append(entry.getKey()).append("=").append(entry.getValue()).append("&");
    });
    String orgin = sb.toString();
    if (orgin.endsWith("&")) {
        orgin = orgin.substring(0, orgin.length() - 1);
    }

    // calculate MD5
    return Md5Utils.getMD5(orgin);
}
```

13.2 API Interface Description

13.2.1 Network interface

Brief Description

BlueEyesView can manage multiple networks, and this interface is used to return the network information managed by BlueEyesView.

Request URL

http://ip:port/north/network

Request Mode

GET

Request Parameter

None

Return Instance


```
[
  {
    "id": 1,
    "domainName": "root",
    "parentId": 0,
    "domainDescp": "System default network",
    "leafNode": false,
    "levelId": 1,
    "icon": null,
    "fromIpv4": "192.168.105.1",
    "toIpv4": "192.168.105.254",
    "rootDeviceId": 69,
    "parentDeviceId": 0,
    "alarmStatus": 0,
    "remark": null,
    "children": null
  },
  {
    "id": 5,
    "domainName": "vlan20",
    "parentId": 1,
    "domainDescp": "vlan20",
    "leafNode": true,
    "levelId": 2,
    "icon": null,
    "fromIpv4": "192.168.20.1",
    "toIpv4": "192.168.20.254",
    "rootDeviceId": null,
    "parentDeviceId": 0,
    "alarmStatus": 0,
    "remark": null,
    "children": null
  },
```

```
  {
    "id": 7,
    "domainName": "vlan30",
    "parentId": 1,
    "domainDescp": "vlan30",
    "leafNode": true,
    "levelId": 2,
    "icon": "",
    "fromIpv4": "192.168.3.1",
    "toIpv4": "192.168.3.254",
    "rootDeviceId": null,
    "parentDeviceId": 0,
    "alarmStatus": 0,
    "remark": null,
    "children": null
  }
]
```


Return Parameter Description

Field name	Type	Note
id	Int	Network ID
domainName	String	Network name
parentId	Int	Parent Network ID And ID can form a hierarchical relation
domainDescp	String	Network description
leafNode	Boolean	Is it leaf node Is it the last level in the hierarchy
levelId	Int	Hierarchical ID Counting from 1
icon	String	-
fromIpv4	String	Start IP range
toIpv4	String	End IP range
rootDeviceId	Int	Root device ID
parentDeviceId	Int	Parent device ID Subnet's associated parent network device
alarmStatus	Int	Subnet status: 0-Normal 2-General 3-Important 4-Severe 5-Off-line (take the maximum alarm status of all devices in the subnet)

Field name	Type	Note
Remark	String	Remark
children	[]	-

13.2.2 Obtain Topological Graph

Brief Description

The topology data of some networks can be returned via this interface to display topological graph.

Request URL

http://ip:port/north/topo

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
domainId	Yes	int	Network ID

Return Instance


```
[
    {
      "domainId": null,
      "nodes": [
        {
          "nodeType": 1,
          "nodeId": 69,
          "nodeName": "DESKTOP-U79S2P2",
          "ipv4": "192.168.105.100",
          "mac": null,
          "vendorId": 3,
          "prodTypeId": 10,
          "modelName": null,
          "discoveryType": 3,
          "alarmGrade": 0,
          "removeFlag": 0,
          "children": [],
          "level": 1,
          "order": 1,
```

```
    "x": null,
    "y": null,
    "workmode": null,
    "ssid": null,
    "onlineTime": null,
    "assocSum": null,
    "key": "1_69"
  },
  {
    "nodeType": 1,
    "nodeId": 66,
    "nodeName": "switch20",
    "ipv4": "192.168.1.20",
    "mac": null,
    "vendorId": 1,
    "prodTypeId": 1,
    "modelName": "IES7112G-4GS",
    "discoveryType": 1,
    "alarmGrade": 0,
    "removeFlag": 0,
    "children": [],
    "level": 2,
    "order": 1,
    "x": null,
    "y": null,
    "workmode": null,
    "ssid": null,
    "onlineTime": null,
    "assocSum": null,
    "key": "1_66"
  },
  {
    "nodeType": 1,
    "nodeId": 68,
    "nodeName": "iap2312n-2t",
    "ipv4": "192.168.1.250",
    "mac": null,
    "vendorId": 1,
    "prodTypeId": 4,
    "modelName": "IAP2312N-2T",
    "discoveryType": 2,
    "alarmGrade": 0,
    "removeFlag": 0,
```

```
    "children": [],
    "level": 3,
    "order": 1,
    "x": null,
    "y": null,
    "workmode": "",
    "ssid": "3ONE_GROUP_TEST",
    "onlineTime": null,
    "assocSum": 0,
    "key": "1_68"
  },
  {
    "nodeType": 1,
    "nodeId": 67,
    "nodeName": "IndustrialSwitch",
    "ipv4": "192.168.1.68",
    "mac": null,
    "vendorId": 1,
    "prodTypeId": 1,
    "modelName": "IES618",
    "discoveryType": 1,
    "alarmGrade": 0,
    "removeFlag": 0,
    "children": [],
    "level": 3,
    "order": 2,
    "x": null,
    "y": null,
    "workmode": null,
    "ssid": null,
    "onlineTime": null,
    "assocSum": null,
    "key": "1_67"
  },
  {
    "nodeType": 1,
    "nodeId": 65,
    "nodeName": "IWS2300",
    "ipv4": "192.168.1.254",
    "mac": null,
    "vendorId": 1,
    "prodTypeId": 11,
    "modelName": null,
```

```
      "discoveryType": 1,
      "alarmGrade": 0,
      "removeFlag": 0,
      "children": [],
      "level": 4,
      "order": 1,
      "x": null,
      "y": null,
      "workmode": null,
      "ssid": null,
      "onlineTime": null,
      "assocSum": null,
      "key": "1_65"
    }
  ],
  "links": [
    {
      "linkId1": 58,
      "linkId2": null,
      "localNodeId": 69,
      "localMacAddr": "00:e0:4c:68:7c:b0",
      "localIpv4Addr": "192.168.105.100",
      "localIfIndex": null,
      "localPort": null,
      "localPortRingStatus": null,
      "remNodeType": 1,
      "remNodeId": 66,
      "remMacAddr": "00:22:6f:12:71:c2",
      "remIpv4Addr": "192.168.1.20",
      "remIfIndex": 3,
      "remPort": "ge1/3",
      "remPortRingStatus": null,
      "linkName": "switch20[ge1/3] - DESKTOP-U79S2P2",
      "linkType": 1,
      "linkMetrial": 2,
      "linkBandwidth": "100000000",
      "removeFlag": 0,
      "ringStatus": null,
      "alarmStatus": 0
    },
    {
      "linkId1": 59,
      "linkId2": null,
```

```
  "localNodeId": 66,
  "localMacAddr": "00:22:6f:12:71:c2",
  "localIpv4Addr": "192.168.1.20",
  "localIfIndex": 5,
  "localPort": "ge1/5",
  "localPortRingStatus": null,
  "remNodeType": 1,
  "remNodeId": 68,
  "remMacAddr": "00:1f:6f:ff:d7:bb",
  "remIpv4Addr": "192.168.1.250",
  "remIfIndex": null,
  "remPort": null,
  "remPortRingStatus": null,
  "linkName": "switch20[ge1/5] - iap2312n-2t",
  "linkType": 1,
  "linkMetrial": 2,
  "linkBandwidth": "100000000",
  "removeFlag": 0,
  "ringStatus": null,
  "alarmStatus": 0
},
{
  "linkId1": 57,
  "linkId2": null,
  "localNodeId": 66,
  "localMacAddr": "00:22:6f:12:71:c2",
  "localIpv4Addr": "192.168.1.20",
  "localIfIndex": 6,
  "localPort": "ge1/6",
  "localPortRingStatus": null,
  "remNodeType": 1,
  "remNodeId": 67,
  "remMacAddr": "00:22:6f:d1:aa:ac",
  "remIpv4Addr": "192.168.1.68",
  "remIfIndex": 3,
  "remPort": "TX( 3)",
  "remPortRingStatus": 0,
  "linkName": "switch20[ge1/6] - IndustrialSwitch[3]",
  "linkType": 2,
  "linkMetrial": 2,
  "linkBandwidth": "100000000",
  "removeFlag": 0,
  "ringStatus": 1,
```

```
        "alarmStatus": 0
      },
      {
        "linkId1": 60,
        "linkId2": null,
        "localNodeId": 67,
        "localMacAddr": "00:22:6f:d1:aa:ac",
        "localIpv4Addr": "192.168.1.68",
        "localIfIndex": 4,
        "localPort": "TX( 4)",
        "localPortRingStatus": 0,
        "remNodeType": 1,
        "remNodeId": 65,
        "remMacAddr": "00:22:66:12:21:12",
        "remIpv4Addr": "192.168.1.254",
        "remIfIndex": null,
        "remPort": null,
        "remPortRingStatus": null,
        "linkName": "IndustrialSwitch[TX( 4)] - IWS2300",
        "linkType": 2,
        "linkMetrial": 2,
        "linkBandwidth": "100000000",
        "removeFlag": 0,
        "ringStatus": 1,
        "alarmStatus": 0
      }
    ],
    "rings": [],
    "rowCount": 4,
    "columnCount": 2
  }
]
```


Return Parameter Description

Topology object

Field name	Type	Note
domainId	int	Network ID
nodes	[]	Node array
links	[]	Link array
rings	[]	Ring array
rowCount	Int	Total number of layers

Field name	Type	Note
columnCount	int	Total number of columns

Node object

Field name	Type	Note
nodeType	int	Node types: 1- Device, 2- subnet
nodeId	int	When nodeType==1, it indicates the device ID; when nodeType== 2, it indicates the network ID
nodeName	String	Node name
ipv4	String	Node IP (Device only)
mac	String	Node MAC (Device only)
vendorId	Int	Device manufacturer (check manufacturer interface)
prodTypeId	Int	Device type (check device type interface)
modelName	String	Device model
discoveryType	Int	Discovery mode: 1-3onedata 2th-generation, 2-3onedata 3rd-generation, 3-ICMP, 4-Manual add
alarmGrade	Int	Alarm level: 0-Normal 2-General 3-Important 4-Severe 5-Offline
removeFlag	Int	Remove flag 1- Remove
children	[]	Lower node
level	Int	Hierarchy
order	Int	Column
x	Int	User saves x of Topo
Y	Int	User saves y of Topo
workmode	String	Work mode (only wireless device)
ssid	String	SSID (only wireless device)
onlineTime	String	-
assocSum	Int	Online user number (only wireless device)
key	String	nodeType+"_"+nodeId

Connected object

Field name	Type	Note
linkId1	Int	Link ID1

Field name	Type	Note
linkId2	Int	Link ID2
localNodeId	Int	Local device ID The NodeType of this terminal is fixed to 1, that is, the device.
localMacAddr	String	Local MAC
localIv4Addr	String	Local IP
localIfIndex	Int	Local port number
localPort	String	Local port name
localPortRingStatus	Int	Status of the local ring network port: 0-blocked 1-forwarding
remNodeType	Int	Remote nodeType
remNodeId	Int	Opposite nodeId
remMacAddr	String	Opposite end MAC
remIpv4Adr	String	Opposite end IP
remIfIndex	Int	Opposite port number
remPort	String	Opposite port name
remPortRingStatus	Int	Status of the opposite end ring network port: 0-blocked 1-forwarding
linkName	String	Link name
linkType	Int	Link type: 1-Common 2-3onedate ring 3-STP/RSTP/MSTP 4-Wireless
linkMetrial	Int	1-Optical fiber 2-Network cable 3-Unknown 4-Wireless
linkBandwidth	String	Bandwidth, bits/s
removeFlag	Int	Remove flag
ringStatus	Int	Ring status 1-stable 2-nostable
alarmStatus	Int	Alarm state 0-Normal 2-General 3-Important 4-Severe 5-Offline

13.2.3 Device List (Paging)

Brief Description

Through this interface, device data that meets requirements can be returned.

Request URL

http://ip:port/north/device

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
number	Yes	int	Page number, starting at 1
size	Yes	int	Rows-per-page
searchKey	No	String	Fuzzy query key
vendorId	No	Int	Manufacturer ID
prodTypeId	No	Int	Product type ID
domainId	No	Int	Network ID
alarmGrade	No	Int[]	Alarm level array

Return Instance


```
{
   "records": [
     {
       "deviceId": 66,
       "deviceName": "switch20",
       "deviceCode": "Industrial0",
       "macAddress": "00:22:6f:12:71:c2",
       "ipv4Address": "192.168.1.20",
       "ipv4Mask": null,
       "ipv4Gateway": null,
       "vendorId": 1,
       "vendorCode": "00226F",
       "vendorName": "3onedata Co., Ltd.",
       "prodTypeId": 1,
       "prodTypeCode": "SWITCH-L2",
       "prodTypeName": "L2 switch",
       "modelId": 1021,
       "modelCode": "IES7112G-4GS",
       "modelName": "IES7112G-4GS",
       "discoveryType": 1,
       "discoveryTypeDesc": null,
       "manageProtocol": 2,
       "manageProtocolDesc": null,
       "driverClass": 0,
```

```
    "address": null,
    "longitude": null,
    "latitude": null,
    "remark": null,
    "alarmGrade": 0,
    "alarmGradeDesc": null,
    "lastUpdateTime": "2020-06-28 09:29:05"
  },
  {
    "deviceId": 67,
    "deviceName": "IndustrialSwitch",
    "deviceCode": "1234567890\n\n\n\n\n\n\n",
    "macAddress": "00:22:6f:d1:aa:ac",
    "ipv4Address": "192.168.1.68",
    "ipv4Mask": null,
    "ipv4Gateway": null,
    "vendorId": 1,
    "vendorCode": "00226F",
    "vendorName": "3onedata Co., Ltd.",
    "prodTypeId": 1,
    "prodTypeCode": "SWITCH-L2",
    "prodTypeName": "L2 switch",
    "modelId": 31,
    "modelCode": "IES618",
    "modelName": "IES618",
    "discoveryType": 1,
    "discoveryTypeDesc": null,
    "manageProtocol": 2,
    "manageProtocolDesc": null,
    "driverClass": 0,
    "address": null,
    "longitude": null,
    "latitude": null,
    "remark": null,
    "alarmGrade": 0,
    "alarmGradeDesc": null,
    "lastUpdateTime": "2020-06-28 09:29:05"
  },
  {
    "deviceId": 68,
    "deviceName": "iap2312n-2t",
    "deviceCode": null,
    "macAddress": "00:1f:6f:ff:d7:bb",
```

```
    "ipv4Address": "192.168.1.250",
    "ipv4Mask": "255.255.255.0",
    "ipv4Gateway": "192.168.1.1",
    "vendorId": 1,
    "vendorCode": "00226F",
    "vendorName": "3onedata Co., Ltd.",
    "prodTypeId": 4,
    "prodTypeCode": "WLAN",
    "prodTypeName": "wireless device",
    "modelId": 4005,
    "modelCode": "IAP2312N-2T",
    "modelName": "IAP2312N-2T",
    "discoveryType": 2,
    "discoveryTypeDesc": null,
    "manageProtocol": 2,
    "manageProtocolDesc": null,
    "driverClass": 0,
    "address": null,
    "longitude": null,
    "latitude": null,
    "remark": null,
    "alarmGrade": 0,
    "alarmGradeDesc": null,
    "lastUpdateTime": "2020-06-28 09:29:05"
  },
  {
    "deviceId": 65,
    "deviceName": "IWS2300",
    "deviceCode": "000012345678",
    "macAddress": "00:22:66:12:21:12",
    "ipv4Address": "192.168.1.254",
    "ipv4Mask": null,
    "ipv4Gateway": null,
    "vendorId": 1,
    "vendorCode": "00226F",
    "vendorName": "3onedata Co., Ltd.",
    "prodTypeId": 11,
    "prodTypeCode": "UNKNOWN",
    "prodTypeName": "unknown type",
    "modelId": null,
    "modelCode": null,
    "modelName": null,
    "discoveryType": 1,
```

```
      "discoveryTypeDesc": null,
      "manageProtocol": 254,
      "manageProtocolDesc": null,
      "driverClass": 0,
      "address": null,
      "longitude": null,
      "latitude": null,
      "remark": null,
      "alarmGrade": 0,
      "alarmGradeDesc": null,
      "lastUpdateTime": "2020-06-28 09:29:05"
    },
    {
      "deviceId": 69,
      "deviceName": "DESKTOP-U79S2P2",
      "deviceCode": null,
      "macAddress": "00:e0:4c:68:7c:b0",
      "ipv4Address": "192.168.105.100",
      "ipv4Mask": null,
      "ipv4Gateway": null,
      "vendorId": 3,
      "vendorCode": "PEN_311",
      "vendorName": "Microsoft",
      "prodTypeId": 10,
      "prodTypeCode": "PC",
      "prodTypeName": "PC",
      "modelId": null,
      "modelCode": null,
      "modelName": null,
      "discoveryType": 3,
      "discoveryTypeDesc": null,
      "manageProtocol": 1,
      "manageProtocolDesc": null,
      "driverClass": 0,
      "address": null,
      "longitude": null,
      "latitude": null,
      "remark": null,
      "alarmGrade": 0,
      "alarmGradeDesc": null,
      "lastUpdateTime": "2020-06-19 09:37:36"
    }
  ],
```

```
  "total": 5,
  "size": 15,
  "current": 1,
  "searchCount": true,
  "pages": 1
}
```


Return Parameter Description

Paging object

Field name	Type	Note
records	[]	Device data
total	int	Total number of rows
size	int	Rows-per-page
current	int	Current page number
searchCount	boolean	-
pages	int	Total number of pages

Device object

Field name	Type	Note
deviceId	int	Device ID
deviceName	int	Device name
deviceCode	String	Device Serial Number
macAddress	String	MAC
ipv4Address	String	IP
ipv4Mask	Int	Mask
ipv4Gateway	Int	Gateway
vendorId	String	Manufacturer ID
vendorName	Int	Name of manufacturer
prodTypeId	Int	Device Type ID
prodTypeCode	Int	Device type code
prodTypeName	[]	Device type name
modelId	Int	Device model ID
modelCode	Int	Device model code
modelName	Int	Device model name.
discoveryType	Int	Discovery method 1-3onedata 2th-generation, 2-3onedata 3rd-generation, 3-ICMP, 4-Manual add

Field name	Type	Note
discoveryTypeDesc	String	Empty
manageProtocol	String	Management protocol 1-Public MIB 2-Private MIB 3-JSON 254-Unmanaged
manageProtocolDesc	String	Empty
driverClass	Int	Meaningless
address	String	Address
longitude	number	Longitude
latitude	number	Latitude
Remark	String	Remark
alarmGrade	Int	Alarm level 0-Normal 2-General 3-Important 4-Severe 5-Offline
alarmGradeDesc	String	Empty
lastUpdateTime	String	Last update time

13.2.4 Query Single Device Data

Brief Description

Through this interface, device data that meets requirements can be returned.

Request URL

http://ip:port/north/device/{deviceId}

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
deviceId	Yes	int	Device ID

Return Instance


```
{
  "deviceId": 66,
  "deviceName": "switch20",
  "deviceCode": "Industrial0",
  "macAddress": "00:22:6f:12:71:c2",
  "ipv4Address": "192.168.1.20",
```

```
    "ipv4Mask": null,
    "ipv4Gateway": null,
    "vendorId": 1,
    "vendorCode": "00226F",
    "vendorName": "3onedata Co., Ltd.",
    "prodTypeId": 1,
    "prodTypeCode": "SWITCH-L2",
    "prodTypeName": "L2 switch",
    "modelId": 1021,
    "modelCode": "IES7112G-4GS",
    "modelName": "IES7112G-4GS",
    "discoveryType": 1,
    "discoveryTypeDesc": null,
    "manageProtocol": 2,
    "manageProtocolDesc": null,
    "driverClass": 0,
    "address": null,
    "longitude": null,
    "latitude": null,
    "remark": null,
    "alarmGrade": 0,
    "alarmGradeDesc": null,
    "lastUpdateTime": "2020-06-28 09:29:05"
}
```


Return Parameter Description

Device object

Field name	Type	Note
deviceId	int	Device ID
deviceName	int	Device name
deviceCode	String	Device Serial Number
macAddress	String	MAC
ipv4Address	String	IP
ipv4Mask	Int	Mask
ipv4Gateway	Int	Gateway
vendorId	String	Manufacturer ID
vendorName	Int	Name of manufacturer
prodTypeId	Int	Device Type ID
prodTypeCode	Int	Device type code

Field name	Type	Note
prodTypeName	[]	Device type name
modelId	Int	Device model ID
modelCode	Int	Device model code
modelName	Int	Device model name.
discoveryType	Int	Discovery method 1-3onedata 2th-generation, 2-3onedata 3rd-generation, 3-ICMP, 4-Manual add
discoveryTypeDesc	String	Empty
manageProtocol	String	Management protocol 1-Public MIB 2-Private MIB 3-JSON 254-Unmanaged
manageProtocolDesc	String	Empty
driverClass	Int	Meaningless
address	String	Address
longitude	number	Longitude
latitude	number	Latitude
Remark	String	Remark
alarmGrade	Int	Alarm level 0-Normal 2-General 3-Important 4-Severe 5-Offline
alarmGradeDesc	String	Empty
lastUpdateTime	String	Last update time

13.2.5 Real-time Alarm List

Brief Description

The current real-time alarm can be returned through this interface.

Request URL

http://ip:port/north/alarm/realtime

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
number	Yes	int	Page number, starting at 1

Parameters	Must	Type	Note
size	Yes	int	Rows-per-page
searchKey	No	String	Fuzzy query key
deviceId	No	Int	Device ID
alarmGrade	No	Int	Alarm level 2-General 3-Important 4-Severe 5-Offline
domainId	No	Int	Network ID

Return Instance


```
{
    "records": [
      {
        "id": 41,
        "deviceId": 65,
        "deviceName": "IWS2300",
        "deviceCode": "000012345678",
        "ifIndex": 0,
        "ifDescr": null,
        "alarmId": 1,
        "alarmCode": "offline",
        "alarmName": "Offline alarm",
        "startTime": "2020-06-28 16:19:45",
        "lastTime": "2020-06-28 16:19:45",
        "recount": 1,
        "alarmGrade": 5,
        "status": 1,
        "dealUser": 0,
        "dealTime": null,
        "workBillId": 0,
        "confirmed": false,
        "confirmUser": 0,
        "confirmTime": null,
        "remark": "192.168.1.254"
      },
      {
        "id": 40,
        "deviceId": 67,
        "deviceName": "IndustrialSwitch",
        "deviceCode": "1234567890\n\n\n\n\n\n\n",
        "ifIndex": 4,
        "ifDescr": "TX( 4)",
```

```
        "alarmId": 2,
        "alarmCode": "linkDown",
        "alarmName": "Link alarm",
        "startTime": "2020-06-28 16:19:39",
        "lastTime": "2020-06-28 16:19:39",
        "recount": 1,
        "alarmGrade": 4,
        "status": 1,
        "dealUser": 0,
        "dealTime": null,
        "workBillId": 0,
        "confirmed": false,
        "confirmUser": 0,
        "confirmTime": null,
        "remark": "192.168.1.68"
      }
    ],
    "total": 2,
    "size": 10,
    "current": 1,
    "searchCount": true,
    "pages": 1
}
```


Return Parameter Description

Paging object

Field name	Type	Note
records	[]	Device data
total	int	Total number of rows
size	int	Rows-per-page
current	Int	Current page number
searchCount	boolean	-
pages	Int	Total number of pages

Alarm object

Field name	Type	Note
id	int	Real-time alarm serial number
deviceId	int	Device ID
deviceName	String	Device name

Field name	Type	Note
deviceCode	String	Device Serial Number
ifIndex	Int	Port
ifDescr	Int	Port name
alarmId	Int	Alarm definition ID
alarmCode	String	Alarm number
alarmName	String	Alarm name
startTime	String	Alarm start time
lastTime	String	Last report time of alarm
recount	Int	Cumulative report times
alarmGrade	Int	Alarm level 2-General 3-Important 4-Severe 5-Offline
status	Int	Processing state 1-Not processed 2-Processing 5-Completed
dealUser	Int	Process users
dealTime	String	Processing time
workBillId	Int	Work order number
confirmed	Boolean	Confirm?
confirmUser	Int	Confirm user
confirmTime	String	Confirmation time
remark	String	Remark

13.2.6 History Alarm List

Brief Description

The history alarm within the specified time range can be returned through this interface.

Request URL

http://ip:port/north/alarm/history

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
number	Yes	int	Page number, starting at 1
size	Yes	int	Rows-per-page

Parameters	Must	Type	Note
startTime	Yes	String	Start time range (yyyy-MM-dd format)
endTime	Yes	String	End time range (yyyy-MM-dd format)
searchKey	No	String	Fuzzy query key
deviceId	No	Int	Device ID
alarmGrade	No	Int	Alarm level 2-General 3-Important 4-Severe 5-Offline
domainId	No	Int	Network ID

Return Instance

```
{
    "records": [],
    "total": 0,
    "size": 10,
    "current": 1,
    "searchCount": true,
    "pages": 1
  }
```

Return Parameter Description

Paging object

Field name	Type	Note
records	[]	Device data
total	int	Total number of rows
size	int	Rows-per-page
current	Int	Current page number
searchCount	boolean	-
pages	Int	Total number of pages

History alarm object

Field name	Type	Note
id	int	History alarm serial number
deviceId	int	Device ID
deviceName	String	Device name
deviceCode	String	Device Serial Number
ifIndex	Int	Port
ifDescr	Int	Port name

Field name	Type	Note
alarmId	Int	Alarm definition ID
alarmCode	String	Alarm number
alarmName	String	Alarm name
startTime	String	Alarm start time
endTime	String	Alarm end time
recount	Int	Cumulative report times
alarmGrade	Int	Alarm level 2-General 3-Important 4-Severe 5-Offline
status	Int	Processing state 1-Not processed 2-Processing 5-Completed
dealUser	Int	Process users
dealTime	String	Processing time
workBillId	Int	Work order number
confirmed	Boolean	Confirm?
confirmUser	Int	Confirm user
confirmTime	String	Confirmation time
remark	String	Remark

13.2.7 Device Type

Brief Description

The device type data managed by the system can be returned through this interface.

Request URL

http://ip:port/north/prodtype

Request Mode

GET

Request Parameter

Parameters	Must	Type	Note
vendorId	No	int	Manufacturer ID

Return Instance

```
[
    {
```

```
    "prodTypeId": 1,
    "prodTypeCode": "SWITCH-L2",
    "prodTypeName": "L2 switch",
    "defaultImg": "",
    "remark": null
  },
  {
    "prodTypeId": 2,
    "prodTypeCode": "SWITCH-L3",
    "prodTypeName": "L3 switch",
    "defaultImg": "",
    "remark": null
  },
  {
    "prodTypeId": 3,
    "prodTypeCode": "SerialServer",
    "prodTypeName": "Serial server",
    "defaultImg": "",
    "remark": null
  },
  {
    "prodTypeId": 4,
    "prodTypeCode": "WLAN",
    "prodTypeName": "wireless device",
    "defaultImg": "",
    "remark": null
  }
]
```


13.2.8 Manufacturer Information

Brief Description

All manufacturer information can be returned through this interface.

Request URL

http://ip:port/north/verdor

Request Mode

GET

Request Parameter

None

Return Instance


```
[
    {
      "id": 1,
      "code": "00226F",
      "name": "3onedata Co., Ltd.",
      "address":”3/B, Zone 1, Baiwangxin High Technology
Industrial Park, Song Bai Road, Nanshan District, Shenzhen,
518108, China”,
      "linkman": null,
      "telphone": "400-880-4496/0755-26702688",
      "email": "sale@3onedata.com",
      "website": "www.3onedata.com.cn",
      "remark": null
    },
    {
      "id": 4,
      "code": "00E04C",
      "name": "REALTEK SEMICONDUCTOR CORP.",
      "address": null,
      "linkman": null,
      "telphone": null,
      "email": null,
      "website": null,
      "remark": null
    },
    {
      "id": 5,
      "code": "002266",
      "name": "Nokia Danmark A/S",
      "address": null,
      "linkman": null,
      "telphone": null,
      "email": null,
      "website": null,
      "remark": null
    }
  ]
```

Return Parameter Description

Field name	Type	Note
id	int	ID
code	String	Code
name	String	Name
address	String	Address
linkman	String	Contact
telphone	String	Contact number
email	String	Mailbox
website	String	Website
remark	String	Remark

3onedata

3onedata Co., Ltd.

Headquarter Address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com