InGateway502
User Manual

Version: V1.2 -- January, 2021

www.inhandnetworks.com
InHand Networks

Declaration

Thank you for choosing our product. Before using the product, read this manual carefully.

The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.

Due to continuous updating, InHand cannot promise that the contents are consistent with the actual product information, and does not assume any disputes caused by the inconsistency of technical parameters. The information in this document is subject to change without notice. InHand reserves the right of final change and interpretation.

Conventions

Symbol	Indication
< >	Content in angle brackets “<>” indicates a button name. For example, the <OK> button.
""	"" indicates a window name or menu name. For example, the pop-up window "New User."
>	A multi-level menu is separated by the double brackets ">". For example, the multi-level menu File > New > Folder indicates the menu item [Folder] under the sub-menu [New], which is under the menu [File].
Cautions	Means reader be careful. Improper action may result in loss of data or device damage.
Note	Notes contain detailed descriptions and helpful suggestions.

Contact Us

Add: 3900 Jermantown Rd., Suite 150, Fairfax, VA 22030 USA
E-mail: support@inhandneworks.com
T: +1 (703) 348-2988
URL: www.inhandnetworks.com

Contents

1. Preface

This document describes how to install and operate the edge computing gateway IG502 series products of Beijing InHand Networks Technology. Before using these products, confirm the product model and the number of accessories inside the package, and purchase a SIM card from the local network operator.

IG502-IO is used as an example. Refer to the actual product during operation.

2. Packing List

Each edge computing gateway product is delivered with accessories (such as standard accessories) frequently used at the customer site. Check the received product against the packing list carefully. If any accessory is missing or damaged, contact the InHand sales personnel promptly.

InHand provides customers with optional accessories based on the characteristics of different sites. For details, see the optional accessories list.

Standard accessories:

Accessory	Quantity	Description
Gateway	1	Edge computing gateway

Product document	1	Quick installation manual and user manual (Obtained by scanning a QR code)
Guide rail installation accessory	1	Used to fix the gateway
Power terminal	1	7-pin industrial terminaland
	2	8- pin industrial terminaland
Network cable	1	1.5 m long
Antenna	1	3G or 4G specification
Product warranty card	1	Warranty period: 1 year
Certificate of conformance	1	Certificate of conformance for the edge computing gateway

Optional accessories:

Accessory	Quantity	Description
AC power cord	1	Power cord for American English Australian or European Standard
Power Adapter	1	VDC Power Adapter
Antenna	1	Wi-Fi Antenna
	1	GPS Antenna
Serial Port	1	Gateway serial port line for debugging

The following sections describe the panel, structure, and dimensions of the edge computing gateway.

2.1. Panel

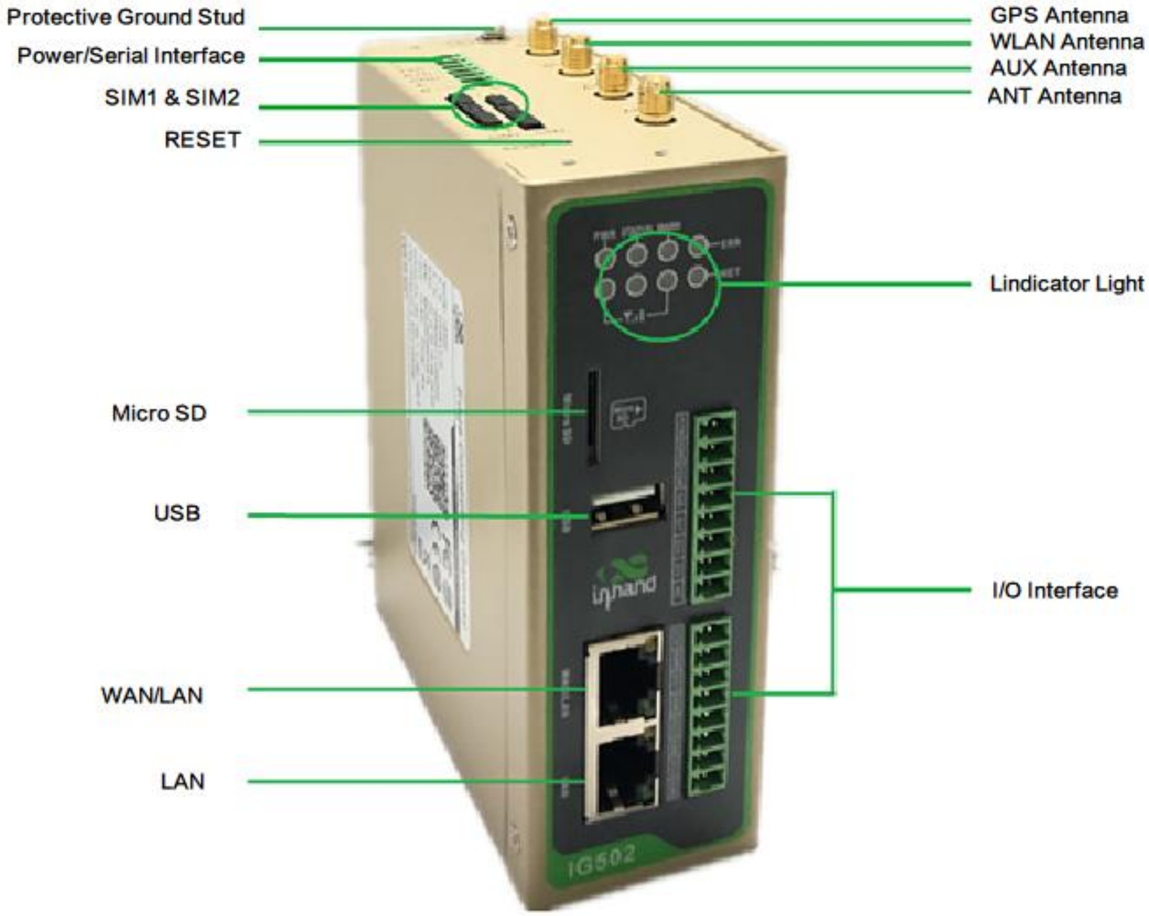


Figure 2-1 IG502

Caution

The IG502 series product is applicable to multiple panel appearances, as they have the same installation method. Refer to the actual product during operation.

2.2. Structure and Dimensions

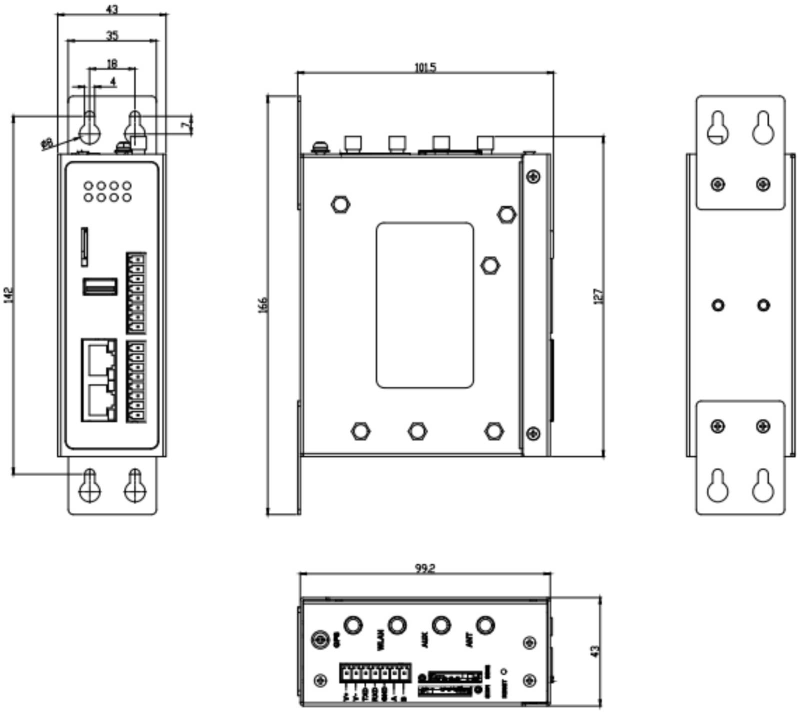


Figure 2-2-1 Wall Mounting (A)

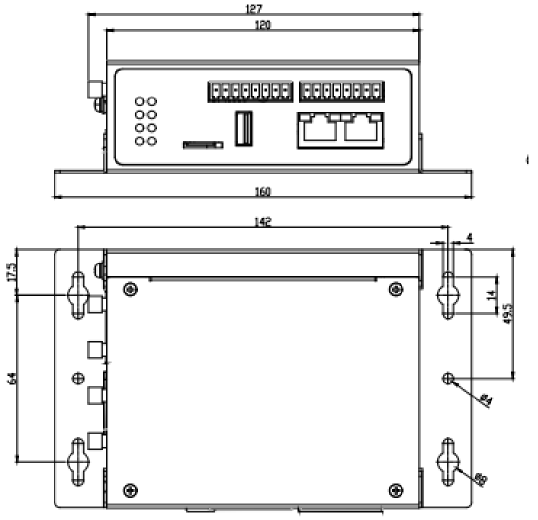


Figure 2-3-2 Wall Mounting (B)

3. Installation

Precautions:

- Power supply requirements: 12V DC (12–48 V DC).
- Environment requirements: operating temperature –25°C to 75°C; storage temperature –40°C to 85°C; relative humidity 5% to 95% (non-condensing). The temperature on the device surface may be high. Install the device in a restricted area and assess the surrounding environment.
- Avoid direct sunlight and keep away from thermal sources or areas with strong electromagnetic interferences.
- Install the gateway product on an industrial DIN-rail.
- Check whether the required cables and connectors are installed.

3.1. Installing and Uninstalling the Device on a DIN-Rail

3.1.1. Installing with a DIN-Rail

Procedure:

Step 1: Select an installation place and reserve enough space for installation.

Step 2: Insert the upper part of the DIN rail seat onto the DIN rail. Grab the lower end of the device and revolve it upward in the direction indicated by arrow 2 with gentle force, to insert the DIN rail seat onto the DIN rail. Check that the device is installed reliably on the DIN rail, as shown in Figure 3-1 on the right.

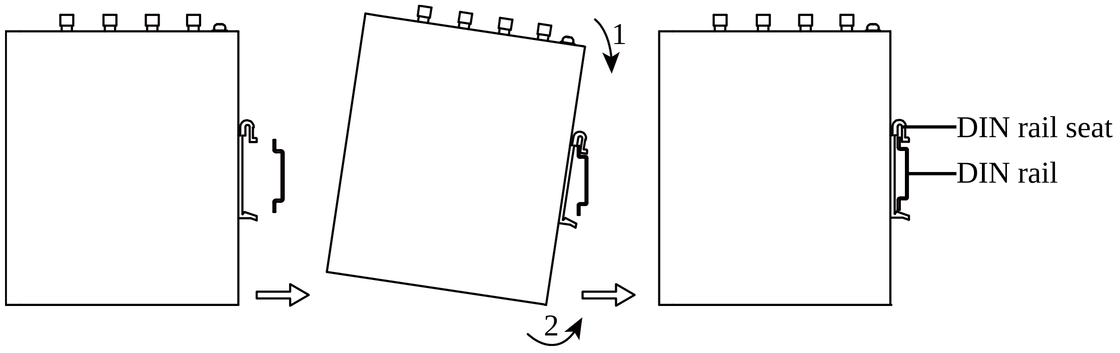


Figure 3-1-1 DIN rail installation schematic diagram

3.1.2. Uninstalling with a DIN-Rail

Procedure:

Step 1: Press the device downward in the direction indicated by arrow 1 in Figure 3-2 to create a gap near the lower end of the device so that the device isolates from the DIN rail.

Step 2: Revolve the device in the direction indicated by arrow 2, and grab the lower end of the device and move the device outward. Lift the device when its lower end isolates from the DIN rail. Then, take off the device from the DIN rail.

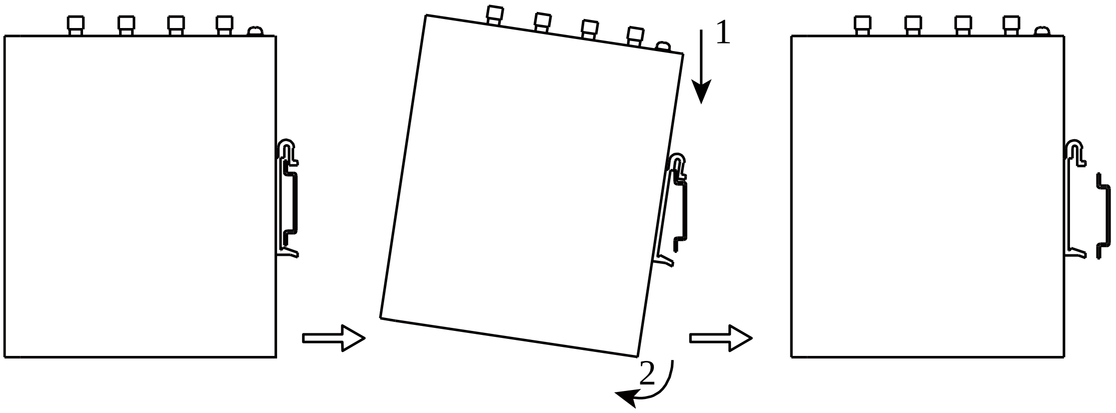
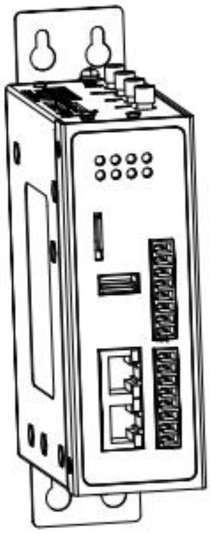


Figure 3-1-2 DIN rail disassembly schematic diagram

3.2. Installing and Uninstalling the Device in Wall-mounted Mode

3.2.1. Installing in Wall-mounted Mode

3.2.1.1. Wall Mounting (A)



Procedure:

Step 1: Select an installation place and reserve enough space for installation.

Step 2: Install the wall mounting bracket on the back of the device by using a screwdriver, as shown in Figure 3-2-1-1.

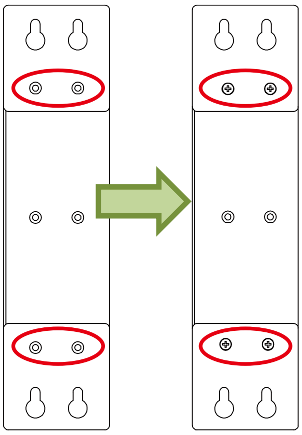


Figure 3-2-1-1 Wall mounted installation diagram

Step 3: Take out the screws (packaged with the wall mounting bracket), fasten the screws in the installation positions by using the screwdriver, and pull down the device to make it secure, as shown in Figure 3-2-1-1-2.

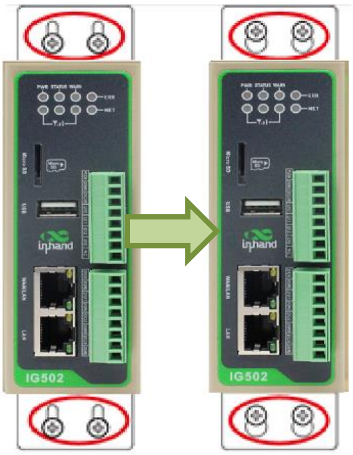
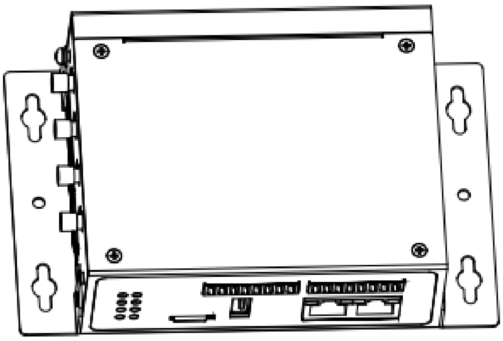


Figure 3-2-1-2 Wall mounted installation diagram

3.2.1.2. Wall Mounting (B)



Step 1: Select an installation place and reserve enough space for installation.

Step 2: Install the wall mounting bracket on the back of the device by using a screwdriver, as shown in Figure 3-2-2-1.

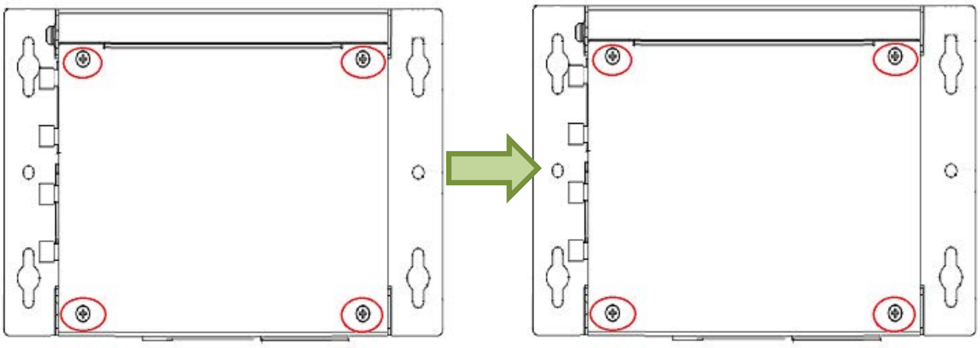


Figure 3-2-1-2-1 Wall mounted installation diagram

Step 3: Take out the screws (packaged with the wall mounting bracket), fasten the screws in the installation positions by using the screwdriver, and pull down the device to make it secure, as shown in Figure 3-2-2-1-2.

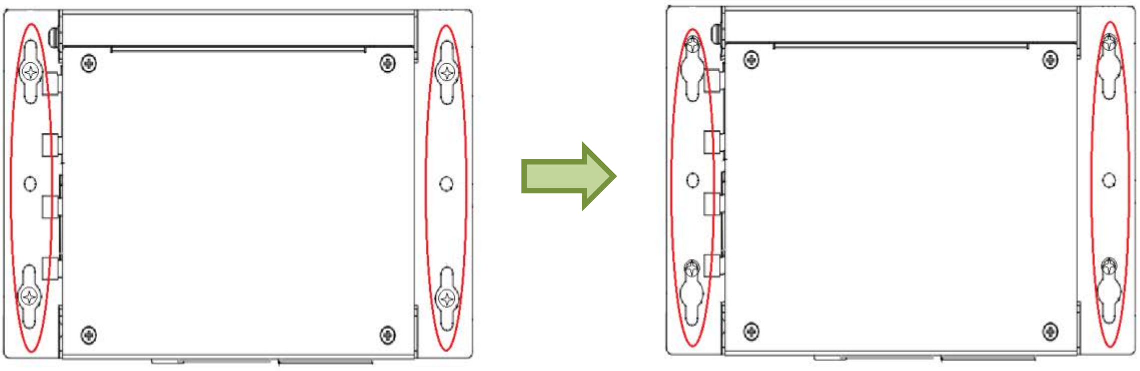


Figure 3-2-1-2 Wall mounted installation diagram

3.2.2. Uninstalling in Wall-mounted Mode

Procedure:

Hold the device with one hand and unfasten the screws that fix the upper end of the device with the other hand, to remove the device from the installation place.

3.3. Installing a SIM Card

IG502 supports Dual SIM card.

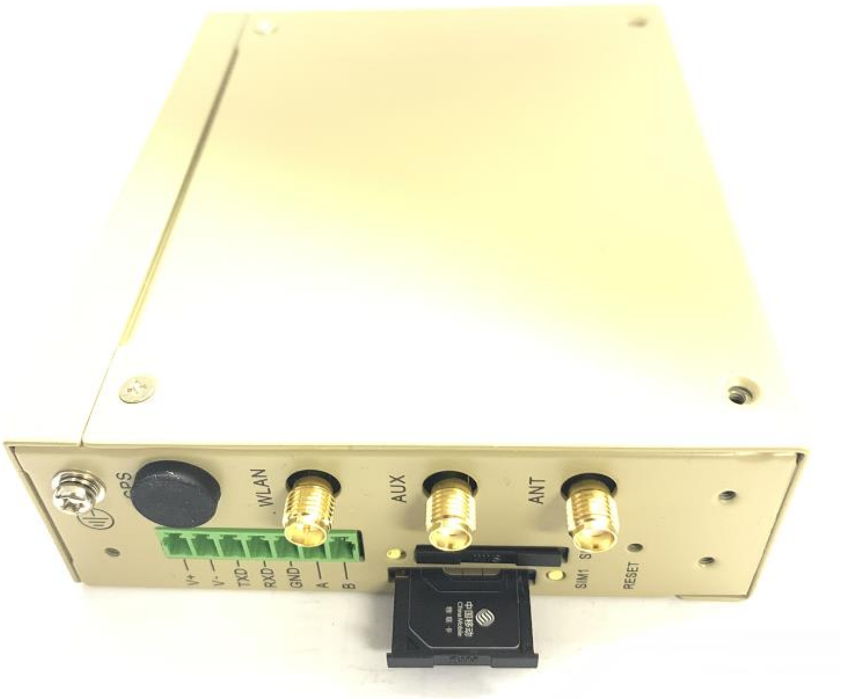


Figure 3-3 Install SIM card

3.4. Installing an Antenna

Revolve the movable part of the metal SMAJ interface with gentle force until it cannot be revolved, in which state the outer thread of the antenna connection cable is invisible. Do not wring the antenna with force by grabbing the black plastic cover.

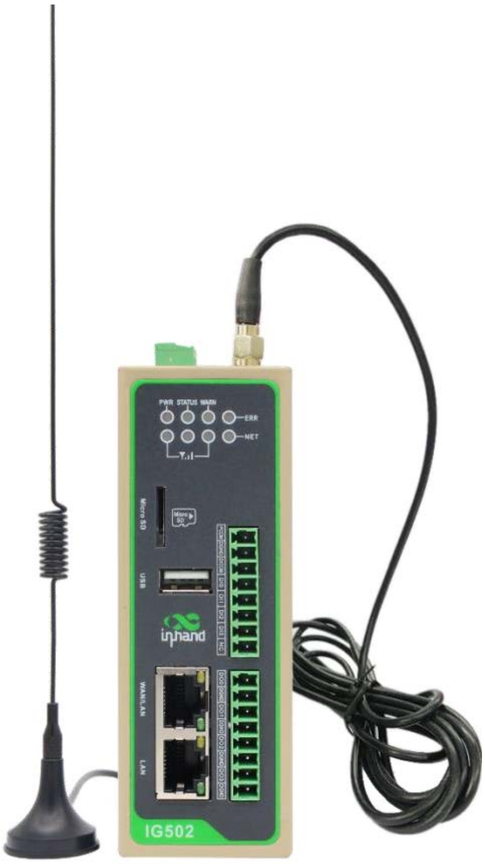


Figure 3-4 Installing an Antenna

Note

- IG502 supports dual antenna: ANT antenna and AUX antenna. The ANT antenna sends and receives data. The AUX antenna only increases the antenna signal strength and cannot be used independently for data transmission.
- Only the ANT antenna is used in normal cases. It is used with the AUX antenna only when signal is poor and signal strength must be improved.

3.5. Installing the Power Supply

Procedure:

Step 1: Remove the terminal from the gateway.

Step 2: Unfasten the locking screw on the terminal.

Step 3: Connect the power cable to the terminal and fasten the locking screw.

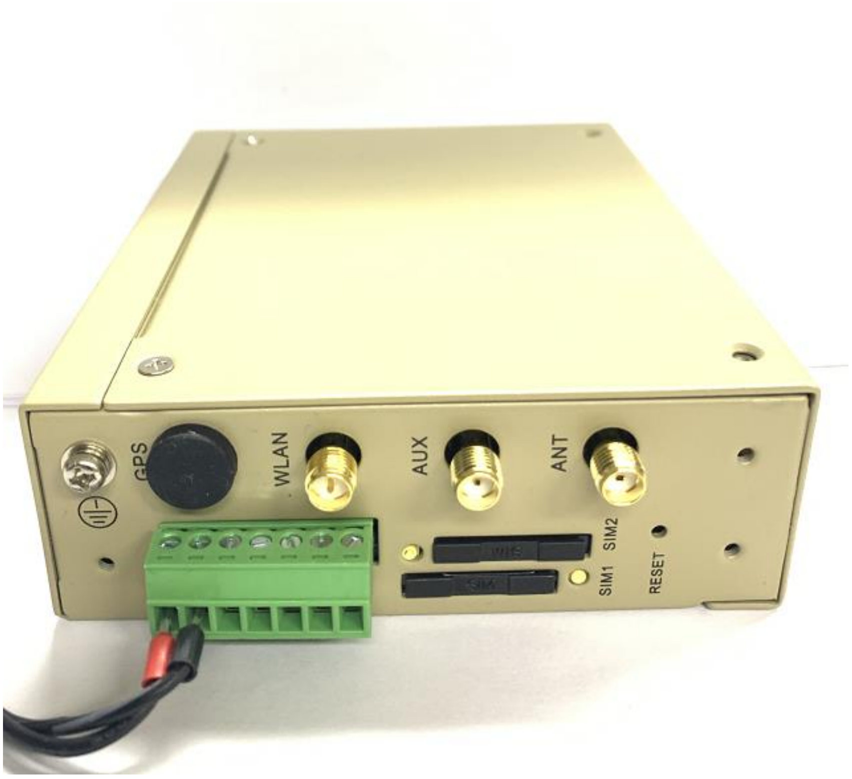


Figure 3-5 Installing the Power Supply

3.6. Installing the Ground Protection

Procedure:

Step 1: Unfasten the ground screw cap.

Step 2: Put the ground loop of the cabinet ground cable onto the ground post.

Step 3: Fasten the ground screw cap.

⚠ **Caution**

Ground the gateway to improve its interference resistance. Connect the ground cable to the ground post of the gateway based on the operation environment.

3.7. Connecting the Network Cable

Connect the gateway to a PC directly by using the Ethernet cable.

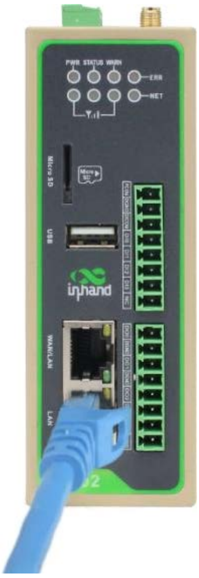


Figure 3-7 Network connection

3.8. Connecting Terminals

3.8.1. Power/serial Terminals

Terminals provide the RS232 and RS485 interface modes. Connect cables to the corresponding terminals before using the interfaces. During installation, remove the terminals from the device, unfasten the locking screws on the terminals, connect cables to the corresponding terminals, and fasten the screws. Sort the cables in order.

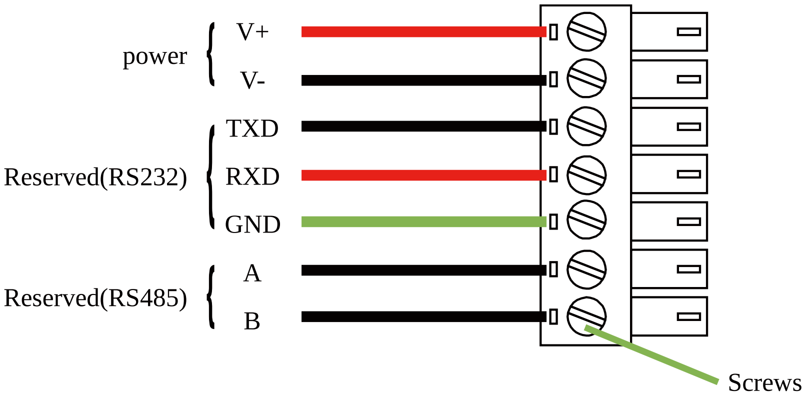


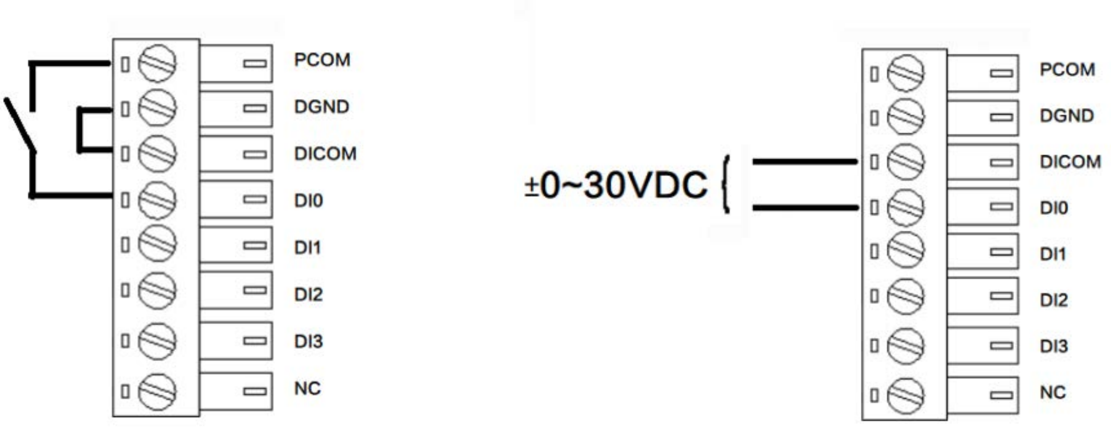
Figure 3-8 Terminal line

3.8.2. IO Terminal

IG502 supports the digital input, pulse counting, digital output, and pulse output functions. In addition, IG502 can remotely read I/O status data or report it to the cloud platform through Modbus TCP. I/O in each mode is defined as follows:

3.8.2.1. Digital input

Dry contacts and wet contacts are specified based on actual connections.



Dry contacts

Wet contacts

0: disconnected

1: connected

0: 0 V DC to 3 V DC/-3 V DC to 0 V DC

1: 10 V DC to 30 V DC/-30 V DC to -10 V DC (4 mA min)

Figure 3-8-2-1. Digital input

3.8.2.2. Pulse counting

A maximum of 3000 Hz pulse signal counting is supported, up to 4294967296.

The following figure shows the connection modes

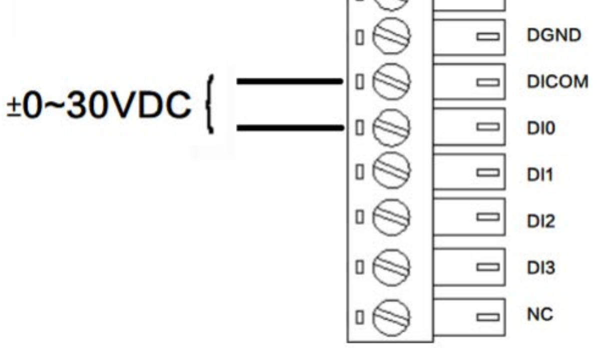


Figure 3-8-2-2 Pulse counting

3.8.2.3. Digital output

According to the external power output voltage, if no external power supply is connected, no voltage is output. The maximum voltage output is 30 V, 500 mA.

The following figure shows the connection modes.

0: OFF

1: ON.

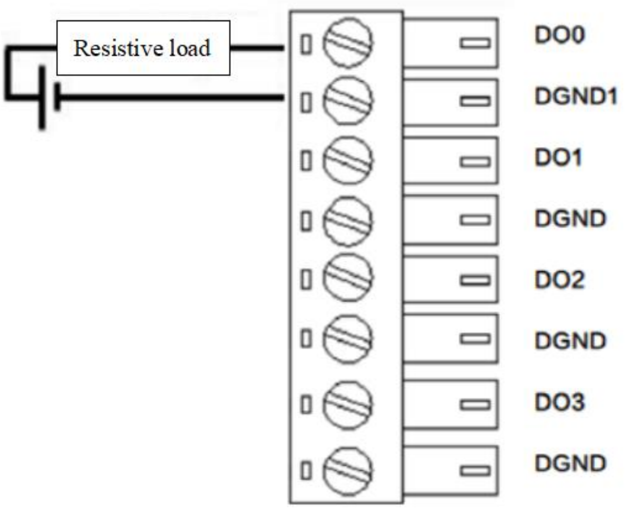


Figure 3-8-2-3 Digital output

3.8.2.4. Pulse output

A maximum of 5000 Hz pulse signal output is supported.

The following figure shows the connection modes.

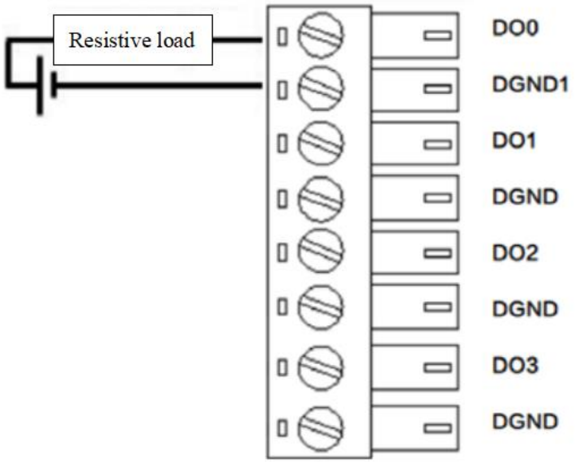


Figure 3-8-2-4 Pulse output

Note

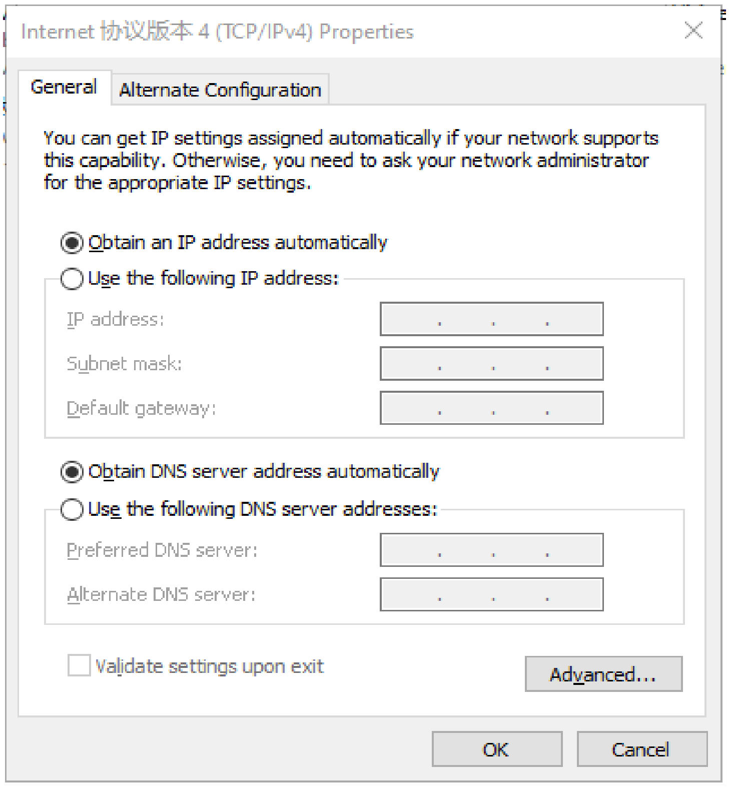
This section is only applicable to IG500 with industrial interfaces.

4. Configuring Network Connection for a Wireless Gateway

4.1. Connecting to the Gateway

Step 1: By default, the IP address of WAN/LAN on IG502 is 192.168.1.1; the IP address of LAN on IG502 is 192.168.2.1. This document uses the LAN port to access the IG502 as an example. Set the PC’s IP address to be on the same subnet with LAN.

Method 1: Enable the PC to obtain an IP address automatically (recommended)



Internet 协议版本 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

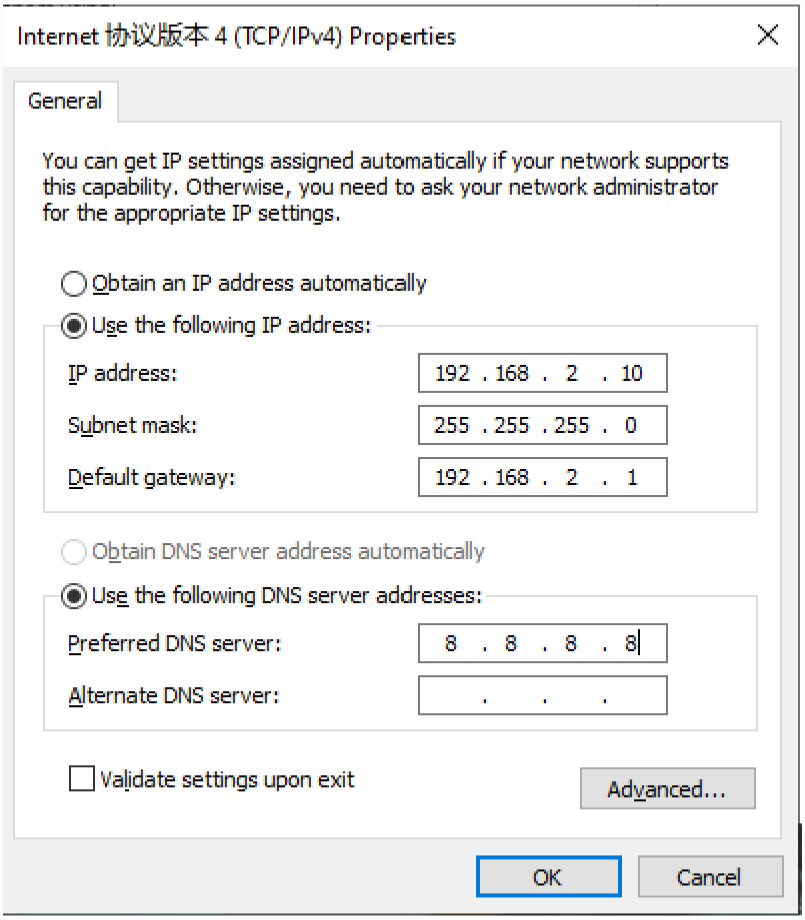
Alternate DNS server: . . .

□ Validate settings upon exit

Figure 4-1-1 Gateway Settings(1)

Method 2: Set a fixed IP address

Select Use the following IP address, enter an IP address (By default,any from 192.168.2.2 to 192.168.2.254), subnet mask (By default,255.255.255.0), default gateway (By default,192.168.2.1), and DNS server address, and click OK.



Internet 协议版本 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

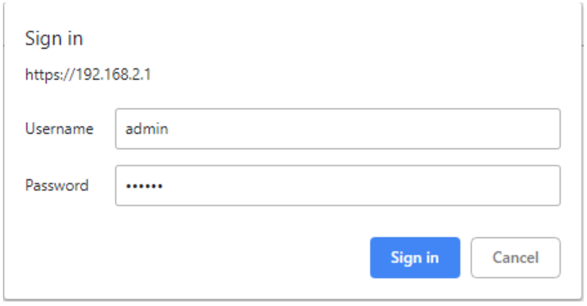
Alternate DNS server: . . .

□ Validate settings upon exit

Figure 4-2-2 Gateway Settings(2)

4.2. Logging in to the Gateway

Connect the PC to the gateway directly by using the network cable, start the web browser, enter **https://192.168.2.1** in the address bar, and press **Enter** to jump to the web login page. Enter the user name (default: **adm**) and password (default: **123456**), and click **OK** or press **Enter** to access the web configuration page.



Sign in

https://192.168.2.1

Username: admin

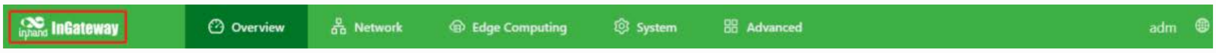
Password: ••••••

Figure 4-2 Login gateway Web management interface

4.3. Navigation Bar Operations

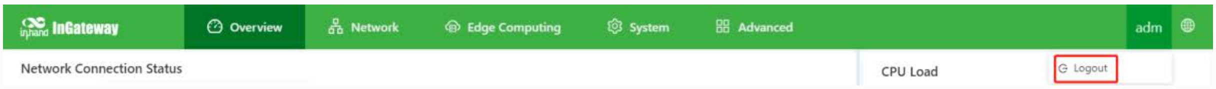
4.3.1. Returning to the Homepage

You can click the InGateway logo in the upper left corner of any web page of the IG502 to return to the **Overview** page quickly.



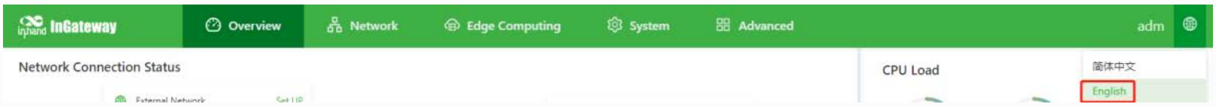
4.3.2. Logging Out

To log out from the IG502, click the user name in the upper right corner.



4.3.3. Changing the Language

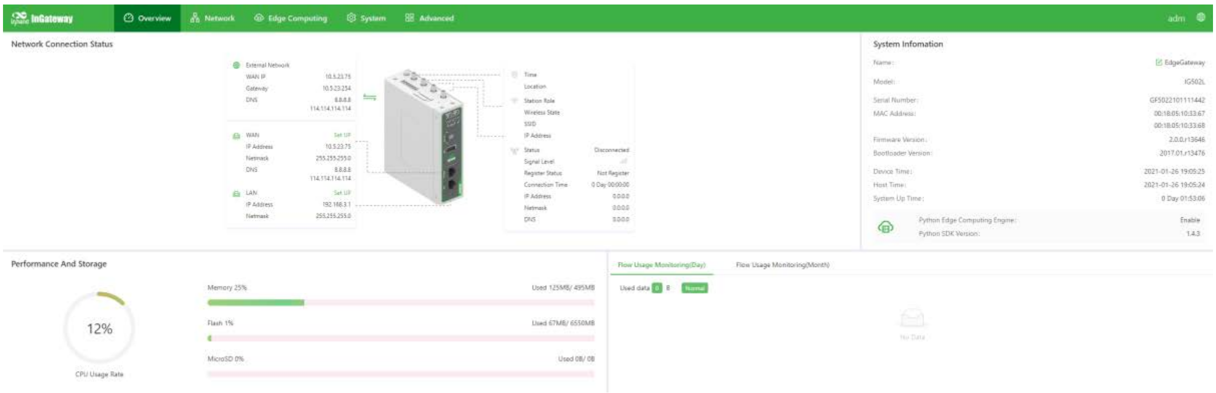
You can click the globe icon in the upper right corner to change the language of web pages. The IG502 supports simplified Chinese and English.



4.4. Overview

The Overview page displays information about the IG502, such as its network connection status, system information, and data usage. You can quickly obtain the IG502 running status on this page.After you log in to the IG502 web page, the Overview page appears by default. You can also click Overview to display this page. This page displays the following information:

Network Connection Status: shows the IG502’ s network connection status and network configuration.



Network Connection Status

External Network
WAN IP 10.5.23.75
Gateway 10.5.23.254
DNS 8.8.8.8
114.114.114.114

WAN Set UP
IP Address 10.5.23.75
Netmask 255.255.255.0
DNS 8.8.8.8
114.114.114.114

LAN Set UP
IP Address 192.168.3.1
Netmask 255.255.255.0

Time
Location

Station Role
Wireless State
SSID
IP Address

Status Disconnected
Signal Level
Register Status Not Register
Connection Time 0 Day 00:00:00
IP Address 0.0.0.0
Netmask 0.0.0.0
DNS 0.0.0.0

System Infomation

Name: EdgeGateway
Model: IG502L
Serial Number: GF5022101111442
MAC Address: 00:18:05:10:33:67
00:18:05:10:33:68
Firmware Version: 2.0.0.r13646
Bootloader Version: 2017.01.r13476
Device Time: 2021-01-26 19:05:25
Host Time: 2021-01-26 19:05:24
System Up Time: 0 Day 01:53:06
Python Edge Computing Engine: Enable
Python SDK Version: 1.4.3

Performance And Storage

12%
CPU Usage Rate
Memory 25% Used 125MB/ 495MB
Flash 1% Used 67MB/ 6550MB
MicroSD 0% Used 0B/ 0B

Flow Usage Monitoring(Day)
Flow Usage Monitoring(Month)
Used data 0 B Normal
No Data

4.5. Network

4.5.1. Network interface

4.5.1.1. Cellular

The **Cellular** page displays the configuration and status of the IG502’ s dial-up interface. You can set dial-up interface parameters to connect the IG502 to a cellular network or view details about the dial-up interface on this page. Follow these steps to configure the dial-up interface:

1. Choose **Network > Network Interfaces > Cellular** to display the **Cellular** page.
2. Select **Enable Cellular**.
3. Set the parameters (default settings recommended). For details about these parameters, see cellular network parameter description.

4. Click **Submit** to complete the configuration of the dial-up interface.

The cellular network parameters are described as follows:

- Enable Cellular: enables or disables the cellular network connection.
- Profile
  - Network Type: specifies the type of the mobile network to which the gateway is connected, which can be GSM or CDMA.
  - APN: specifies the access point name (APN) that identifies the service type of a WCDMA/LTE network. A WCDMA/LTE system provides services based on the APN of the connected WCDMA/LTE network. (This parameter does not need to be set for the CDMA2000 series.)
  - Access Number: specifies the dial string provided by the network operator. Obtain this dial string from your network operator.
  - If your 3G/LTE data card supports WCDMA or LTE, the default dial string is `*99***1#`.
  - If your 3G data card supports CDMA 2000, the default dial string is `#777`.
  - Auth Method
    - Auto: selects an authentication method automatically.
    - PAP: specifies the Password Authentication Protocol, a simple plain-text authentication method implemented through two-way handshakes.

        - CHAP: specifies the Challenge Handshake Authentication Protocol, a security authentication method that verifies message digests through three-way handshakes.
        - MS-CHAP: specifies the CHAP standard defined by Microsoft.
        - MS-CHAPv2: specifies the upgraded version of MS-CHAP, which requires two-way authentication.
    - Username: specifies the user name used for connection to the public data network (PDN). It is provided by your network operator. The default value is `gprs`.
    - Password: specifies the password of the PDN user. It is provided by your network operator. The default value is `gprs`.

Dual SIM Enable: enables or disables the dual-SIM card mode.

- Main SIM: specifies the main SIM card used. Options are SIM1, SIM2, Random, and Sequential.
- Max Number Of Dial: specifies the maximum number of dial-up attempts on SIM1. When the number of dial-up failures reaches this number, the gateway switches to SIM2.
- Min Connected Time: specifies the minimum network connection duration after the gateway dials up successfully. Within this duration, the number of dial-up attempts is counted. When the connection duration exceeds the set

value, the number of dial-up attempts is reset. When the value is set to 0, this function is disabled.

- Backup SIM Timeout: specifies the timeout period of the backup SIM card used currently. The gateway switches to the main SIM card when the timeout period of the backup SIM card is reached.

Network Type: specifies a network type for the SIM card. Options are Auto, 3G, 4G, and 2G. You can select a specific network type suitable for your gateway and SIM card or choose the auto mode, in which the gateway automatically registers to the suitable network.

Profile: specifies the index of the dial-up parameter set.

Roaming: enables the roaming function to allow the gateway to dial up in roaming state or disables the roaming function to prevent the gateway from dialing up in roaming state. When a local SIM card is used, its dial-up capability is not affected whether this option is selected or deselected.

PIN code: specifies the personal identification number of the SIM card. If you enable PIN code but do not set a PIN code or set a wrong PIN code, the gateway cannot dial up. A valid PIN code enables the gateway to dial up to a network.

Static IP: enables or disables the use of a static IP address. If you select this option, specify an IP address manually. Then, the gateway obtains the specified static IP address every time it dials up to a network.

Connection Mode

- Always Online: indicates that the gateway stays online when it is running properly and will be disconnected and redial up only if the dial-up interface does not transmit any traffic in 30 minutes. This is the default connection mode of the system.
- On-demand Dial
- Data Trigger: indicates that the gateway is offline by default and will dial up automatically when data is sent to the Internet.
- Manual Dial: indicates that the network connection can be established or terminated by clicking **Connect** or **Disconnect** in the **Status** area.

Redial Interval: specifies the period that the gateway waits before dialing up again.

ICMP Probes

- ICMP Detection Server: specifies the IP address or domain name of the remote ICMP server to be probed. (If two ICMP servers are enabled, it is recommended that you enter the IP addresses or domain names of both servers here.) The gateway supports two ICMP servers: a primary server and a backup server. After two servers are configured, the gateway probes the primary server first. It probes the secondary server only when the number of probe retries on the primary server reaches the maximum value. If both the servers fail to be detected, the gateway dials up again and starts a new round of ICMP probe.

- ICMP Detection Interval: specifies the interval between ICMP probe packets sent from the gateway.
- ICMP Detection Timeout: specifies the timeout period of an ICMP probe. If the gateway does not receive any ICMP Reply packet within this period, it considers that the ICMP probe times out.
- ICMP Detection Max Retries: specifies the maximum number of retries after an ICMP probe failure. (The gateway dials up again when the number of retries reaches this value.)
- ICMP Detection Strict: enables or disables the strict ICMP probe mode. In this mode, the gateway does not send ICMP probe packets when its dial-up interface is transmitting data traffic. It sends ICMP probe packets only when the dial-up interface is idle.

Advanced Settings

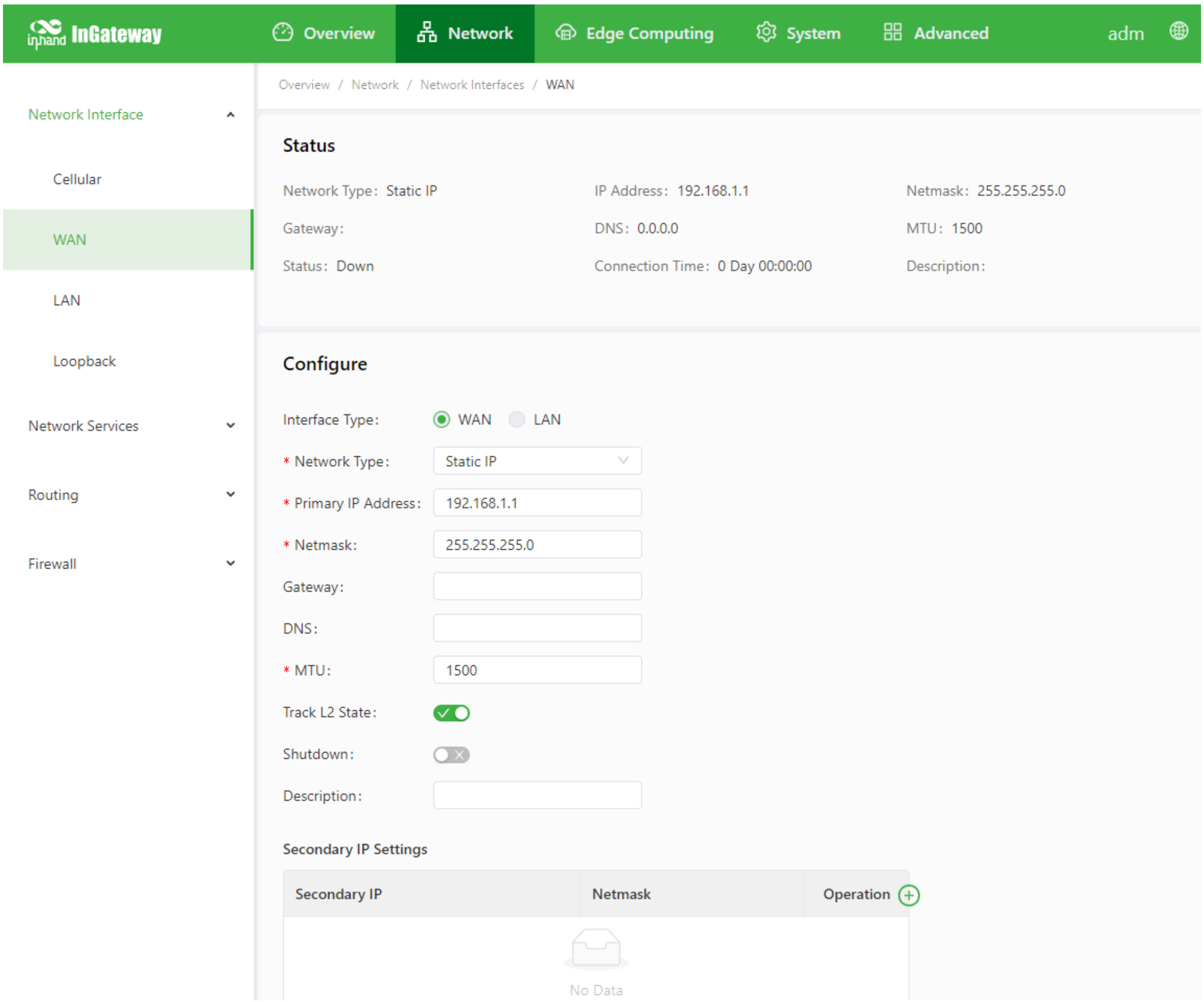
- Initial Commands: specifies some AT commands used to check the module status.

- RSSI Poll Interval: specifies the interval at which the gateway checks the signal status after dialing up successfully. For example, the interval is set to 60s. If you remove the antennas after the gateway dials up successfully, the signal strength will remain unchanged in 60s and decrease 60s later. If the interval is set to 0, RSSI polling is disabled.
- Dial Timeout: specifies the dial-up timeout period. If the gateway fails to dial up to a network within the timeout period, the dial-up times out. In this case, the gateway checks the module status and dials up to the network again.
- MRU: specifies the maximum receive unit, which is expressed in bytes.
- MTU: specifies the maximum transmit unit, which is expressed in bytes.
- Use Default Asyncmap: enables or disables the default Asyncmap.
- Use Peer DNS: enables or disables the use of the DNS server assigned in the connected network.
- LCP Interval: specifies the interval at which the gateway checks whether the cellular connection is normal.
- LCP Max Retries: specifies the maximum number of dial-up retries after the link connection is interrupted.
- Infinitely Dial Retry: enables the gateway to retry unlimited times upon a dial-up failure.
- Debug: enables display of more detailed system logs.

- Expert Options: allows you to set command parameters.

4.5.1.2. WAN

The following figure shows the configuration of **WAN/LAN**, with **Interface Type** set to **WAN**.



Overview / Network / Network Interfaces / WAN

Status

Network Type: Static IP
IP Address: 192.168.1.1
Netmask: 255.255.255.0
Gateway:
DNS: 0.0.0.0
MTU: 1500
Status: Down
Connection Time: 0 Day 00:00:00
Description:

Configure

Interface Type: ● WAN ○ LAN
* Network Type: Static IP
* Primary IP Address: 192.168.1.1
* Netmask: 255.255.255.0
Gateway:
DNS:
* MTU: 1500
Track L2 State: ✓ (on)
Shutdown: (off)
Description:

Secondary IP Settings

Secondary IP	Netmask	Operation ⊕
No Data		

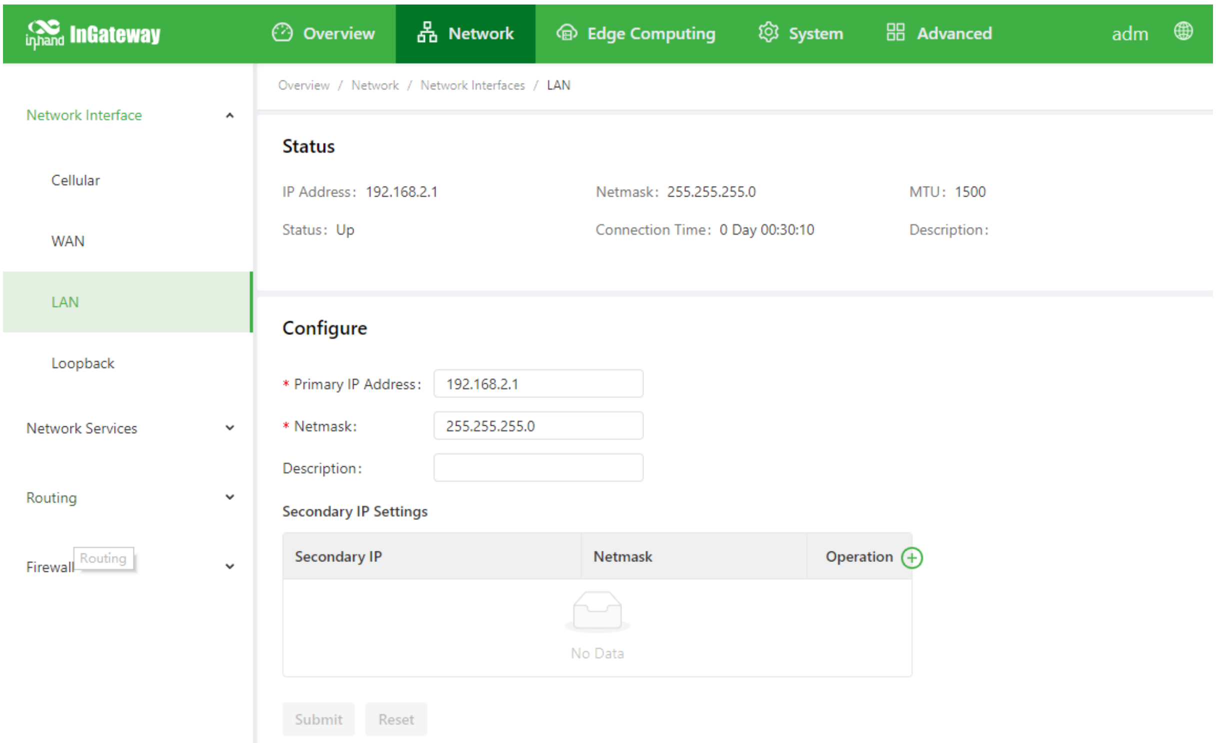
The Ethernet parameters are described as follows:

- Network Type (Static IP by default)
    - Static IP: uses a manually configured IP address, matching subnet mask, and other information for the Ethernet interface.
    - Dynamic Address (DHCP): configures the interface as a DHCP client to obtain an IP address, the matching subnet mask, and other information through DHCP.
- Static IP mode
    - Primary IP: specifies the IP address of the Ethernet interface. By default, the IP address of WAN/LAN is 192.168.1.1, and the IP address of LAN is 192.168.2.1.
    - Netmask: specifies the subnet mask of the Ethernet interface.
    - MTU: specifies the maximum transmit unit, which is expressed in bytes. The default value is 1500.
    - Speed/Duplex, including:
        - Auto Negotiation
        - 1000M Full Duplex
        - 1000M Half Duplex
        - 100M Full Duplex
        - 100M Half Duplex
        - 10M Full Duplex

        - 10M Half Duplex

    - Track L2 State: enables or disables tracking of L2 interface status. After this feature is enabled, the interface is Down when it is not physically connected and is Up when it is physically connected. After this feature is disabled, the interface state is displayed as UP regardless of whether the interface is physically connected.
    - Shutdown: disables the interface.
    - Description: specifies the descriptive information that identifies the Ethernet interface.
    - Secondary IP Setting: allows you to set up to 10 secondary IP addresses in addition to the primary IP address.

4.5.1.3. LAN



Overview / Network / Network Interfaces / LAN

Status

IP Address: 192.168.2.1 Netmask: 255.255.255.0 MTU: 1500

Status: Up Connection Time: 0 Day 00:30:10 Description:

Configure

* Primary IP Address: 192.168.2.1

* Netmask: 255.255.255.0

Description:

Secondary IP Settings

Secondary IP	Netmask	Operation

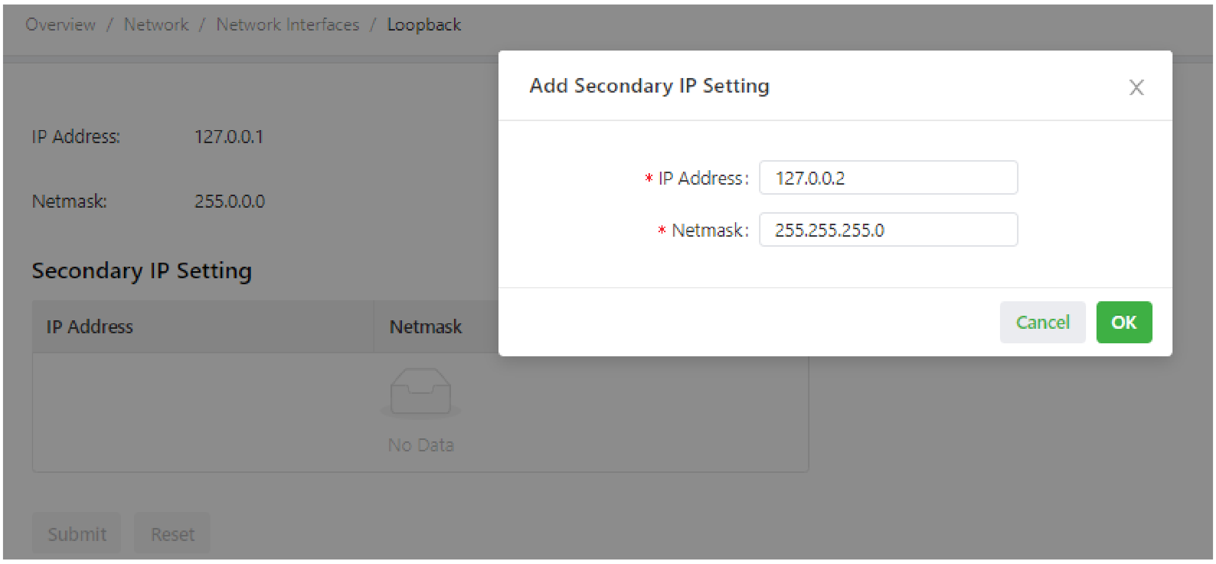
- Primary IP: specifies the primary IP address of the interface.
- Netmask: specifies the subnet mask of the interface.
- Secondary IP Setting: allows you to set up to 10 secondary IP addresses in addition to the primary IP address.

4.5.1.4. Loopback

The loopback interface is a logical, virtual interface on the IG502. After you create and configure the loopback interface, you can ping its IP address or set up a Telnet connection to it to test the network connectivity. You can set or view loopback interface parameters on the **Loopback** page. Follow these steps to configure the loopback interface:

1. Choose **Network** > **Network Interfaces** > **Loopback** to display the **Loopback** page. You can set or view loopback interface parameters on this page.
2. Click the Add icon in the table under **Secondary IP Setting** to add a secondary IP address for the loopback interface. (The default IP address is 127.0.0.1.)
3. Enter the secondary IP address and subnet mask.
4. Click **Submit** to complete the configuration of the loopback interface.

As shown in the following figure, a secondary IP address 127.0.0.2 is set for the loopback interface.



Overview / Network / Network Interfaces / Loopback

IP Address: 127.0.0.1

Netmask: 255.0.0.0

Secondary IP Setting

IP Address	Netmask
No Data	

Add Secondary IP Setting

* IP Address: 127.0.0.2

* Netmask: 255.255.255.0

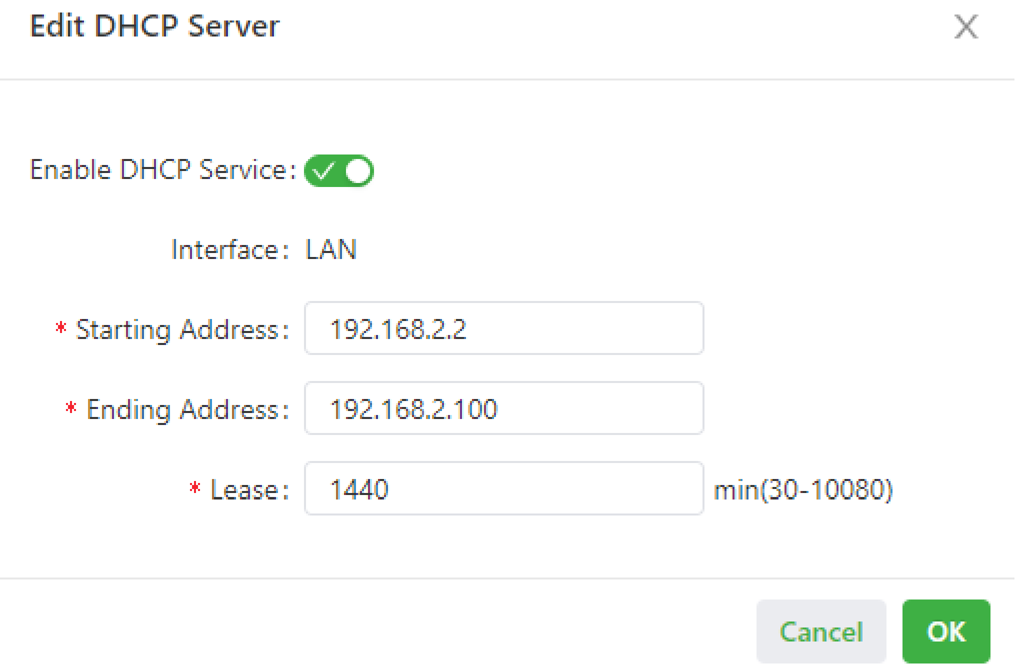
4.5.2. Network Services

4.5.2.1. DHCP

The Dynamic Host Configuration Protocol (DHCP) uses the client/server communication model. The client sends a configuration request to the server, and the server replies with the IP address allocated to the client and other configuration information. In this way, the client IP address and other configuration is assigned dynamically. You can configure a DHCP server and view its configuration on the **DHCP Server** page. Follow these steps to configure a DHCP server:

1. Choose **Network** > **Network Services** > **DHCP** > **DHCP Server** to display the **DHCP Server** page.
2. Click the **Add** or **Edit** icon to configure the DHCP server.
3. Set the parameters. For details about these parameters, see DHCP server parameter description.
4. Click **OK** to save the configuration, and then click **Submit** to apply the configuration.

The following figure shows the DHCP server configuration.



Edit DHCP Server

Enable DHCP Service: ✓

Interface: LAN

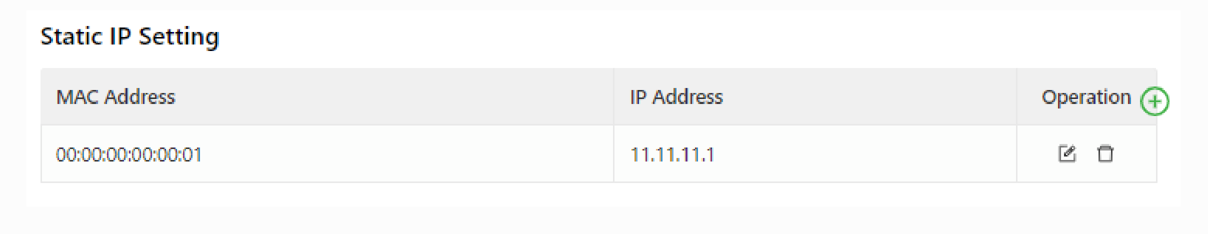
* Starting Address: 192.168.2.2

* Ending Address: 192.168.2.100

* Lease: 1440 min(30-10080)

- The DHCP server parameters are described as follows:
  - Enable DHCP Service: enables or disables the DHCP service.
  - Interface: LAN
  - Starting Address: specifies the start IP address of the IP address pool for address allocation to DHCP clients.
  - Ending Address: specifies the end IP address of the IP address pool for address allocation to DHCP clients.
  - Lease: specifies the validity period of allocated IP addresses. The DHCP server will reclaim the expired IP addresses for reallocation. This field cannot be left blank.
- Windows Name Server (WINS): specifies the IP address of the WINS server.

- Static IP Setting: allows you to bind a fixed IP address to a MAC address, as shown in the following figure.



Static IP Setting

MAC Address	IP Address	Operation ⊕
00:00:00:00:00:01	11.11.11.1	✎ 🗑

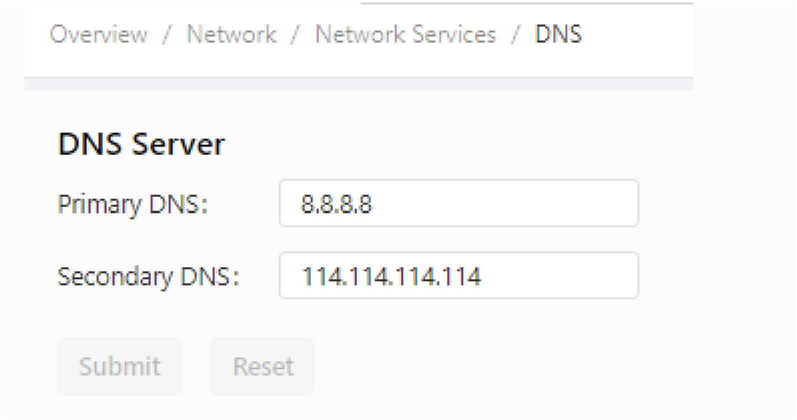
4.5.2.2. DNS

A domain name system (DNS) is a distributed database used for TCP/IP applications and provides translation between domain names and IP addresses. DNS allows users to access some applications by using easy-to-remember, meaningful domain names, which are then translated into the correct IP addresses by a DNS server on the network. You can configure a DNS server and the DNS relay service and view the configuration on the **DNS** page.

- Follow these steps to configure a DNS server:

  1. Choose **Network** > **Network Services** > **DNS** to display the **DNS** page.
  2. Enter the IP address of the DNS server.
  3. Click **Submit** to apply the configuration.

The following figure shows the DNS server configuration.



Overview / Network / Network Services / DNS

DNS Server

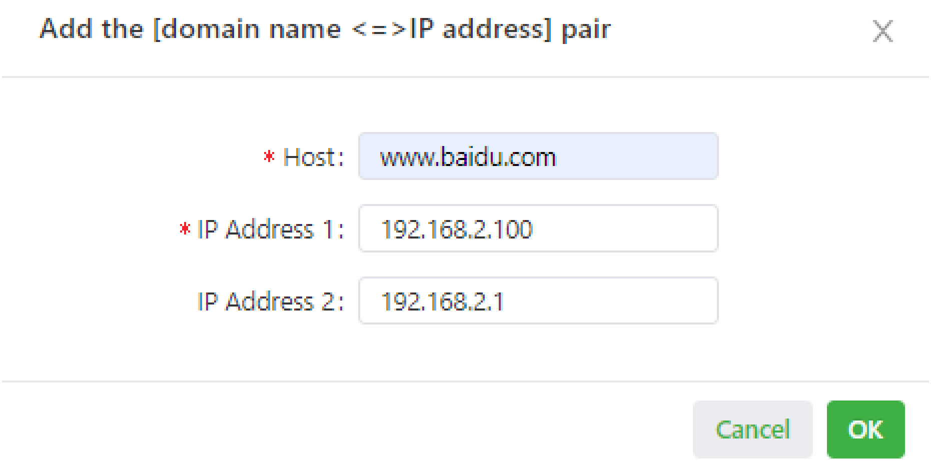
Primary DNS: 8.8.8.8

Secondary DNS: 114.114.114.114

Follow these steps to configure the DNS relay service:

1. Choose **Network > Network Services > DNS** to display the **DNS** page.
2. Enable the DNS relay service. The DNS relay service cannot be disabled when the DHCP server feature is enabled.
3. Click the Add icon to add a **[domain name <=> IP address] pair**.
4. Enter the domain name or IP address of a host and specify the matching IP address.
5. Click **OK** to save the configuration, and then click **Submit** to apply the configuration.

The following figure shows the configuration of the DNS relay service.



Add the [domain name <=>IP address] pair

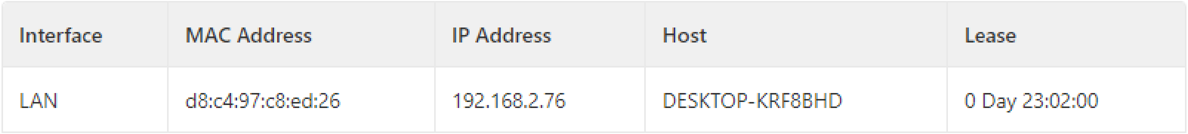
* Host: www.baidu.com

* IP Address 1: 192.168.2.100

IP Address 2: 192.168.2.1

4.5.2.3. Host List

You can view information about hosts connected to the IG502 on the **Host List** page. Choose **Network** > **Network Services** > **Host List** to display the **Host List** page, as shown in the following figure.

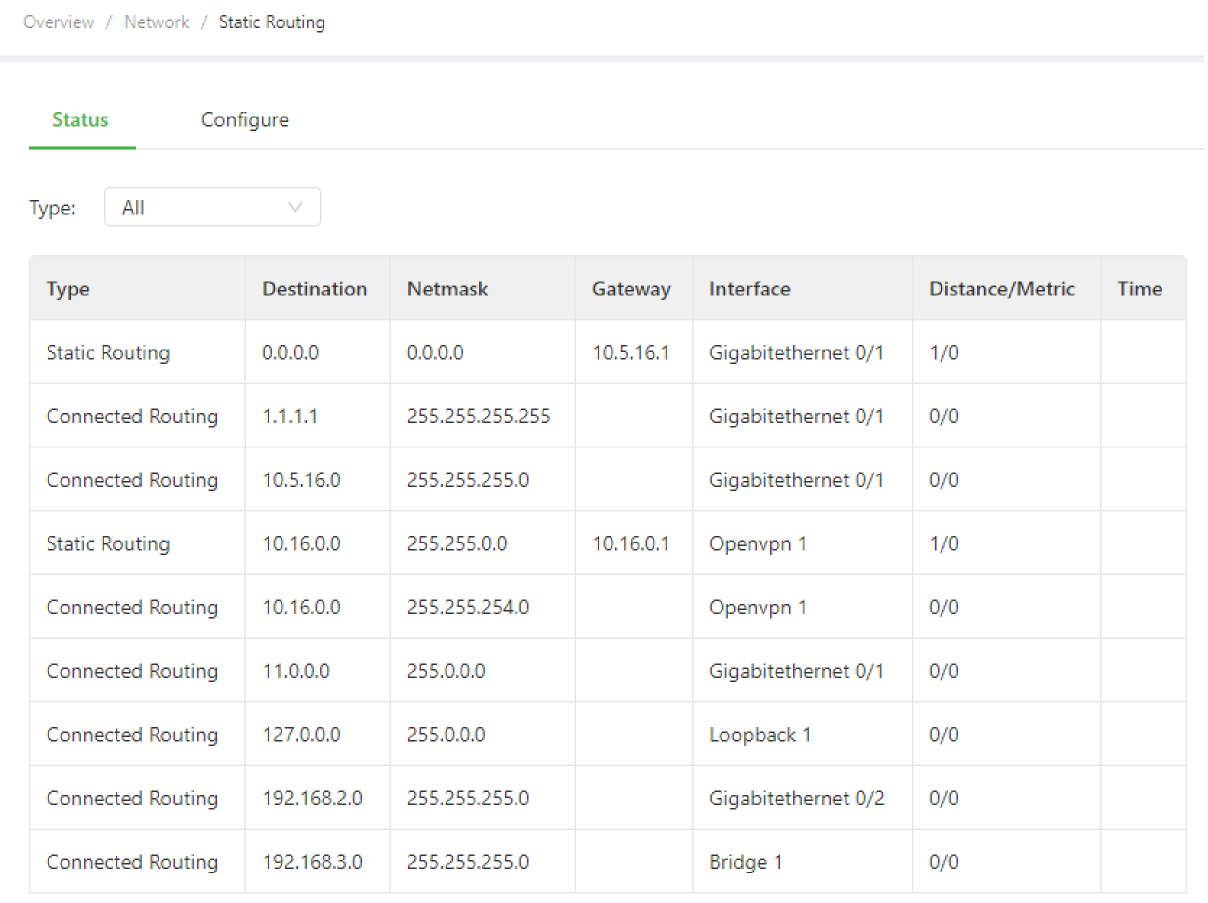


Interface	MAC Address	IP Address	Host	Lease
LAN	d8:c4:97:c8:ed:26	192.168.2.76	DESKTOP-KRF8BHD	0 Day 23:02:00

4.5.3. Routing

4.5.3.1. Routing Status

Choose **Network** > **Routing** > **Routing Status** to display the **Routing Status** page. This page displays information about static routes configured on the IG502, as shown in the following figure.



Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
Static Routing	0.0.0.0	0.0.0.0	10.5.16.1	Gigabitethernet 0/1	1/0	
Connected Routing	1.1.1.1	255.255.255.255		Gigabitethernet 0/1	0/0	
Connected Routing	10.5.16.0	255.255.255.0		Gigabitethernet 0/1	0/0	
Static Routing	10.16.0.0	255.255.0.0	10.16.0.1	Openvpn 1	1/0	
Connected Routing	10.16.0.0	255.255.254.0		Openvpn 1	0/0	
Connected Routing	11.0.0.0	255.0.0.0		Gigabitethernet 0/1	0/0	
Connected Routing	127.0.0.0	255.0.0.0		Loopback 1	0/0	
Connected Routing	192.168.2.0	255.255.255.0		Gigabitethernet 0/2	0/0	
Connected Routing	192.168.3.0	255.255.255.0		Bridge 1	0/0	

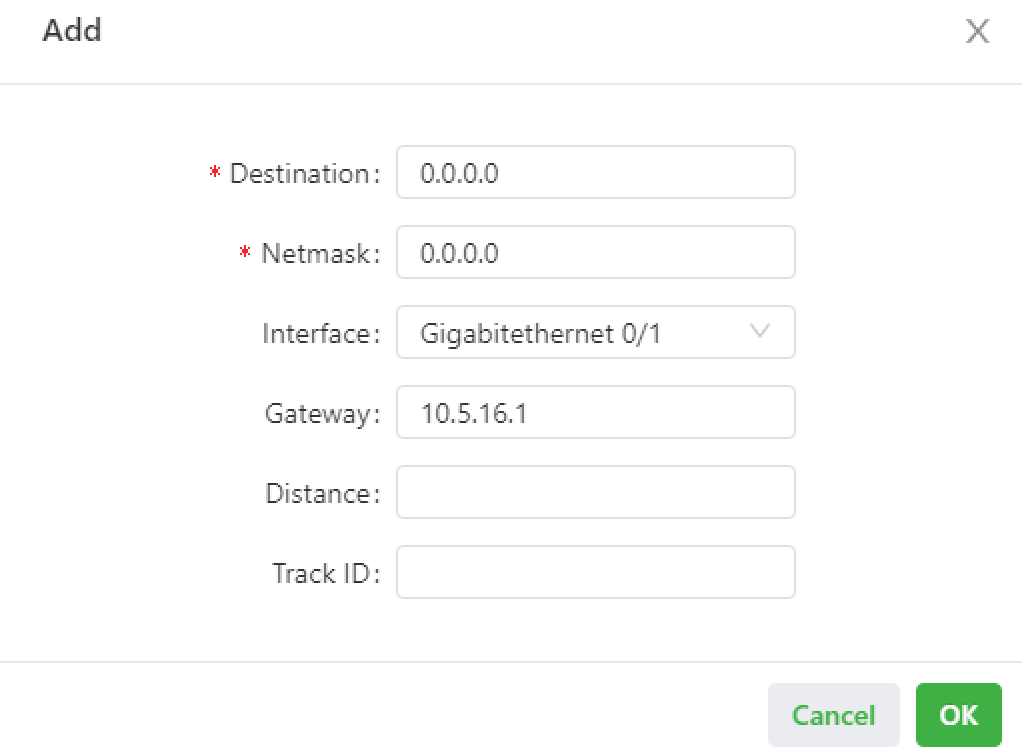
4.5.3.2. Static Routing

You can configure static routes on the **Static Routing** page. Then, packets sent to a specific destination are forwarded through the specified route. (Generally, you do not need to configure static routes.) Follow these steps to configure a static route:

1. Choose **Network** > **Routing** > **Static Routing** to display the **Static Routing** page.

2. Click the **Add** icon to add a static route.
3. Set the parameters. For details about these parameters, see static routing parameter description.
4. Click **OK** to save the configuration, and then click **Submit** to apply the configuration.

The following figure shows the configuration of a static route.



Add

* Destination: 0.0.0.0

* Netmask: 0.0.0.0

Interface: Gigabitethernet 0/1

Gateway: 10.5.16.1

Distance:

Track ID:

Parameters of a static route are described as follows:

- Destination: specifies the destination IP address to which packets are sent.
- Netmask: specifies the subnet mask of the destination IP address.

- Interface: specifies the interface through which data packets are forwarded to the destination network.
- Gateway: specifies the IP address of the next router that data packets pass through before reaching the destination IP address.
- Distance: specifies the priority of the route. A smaller value indicates a higher priority.
- Track ID: specifies the track index or ID.

4.5.4. Firewall

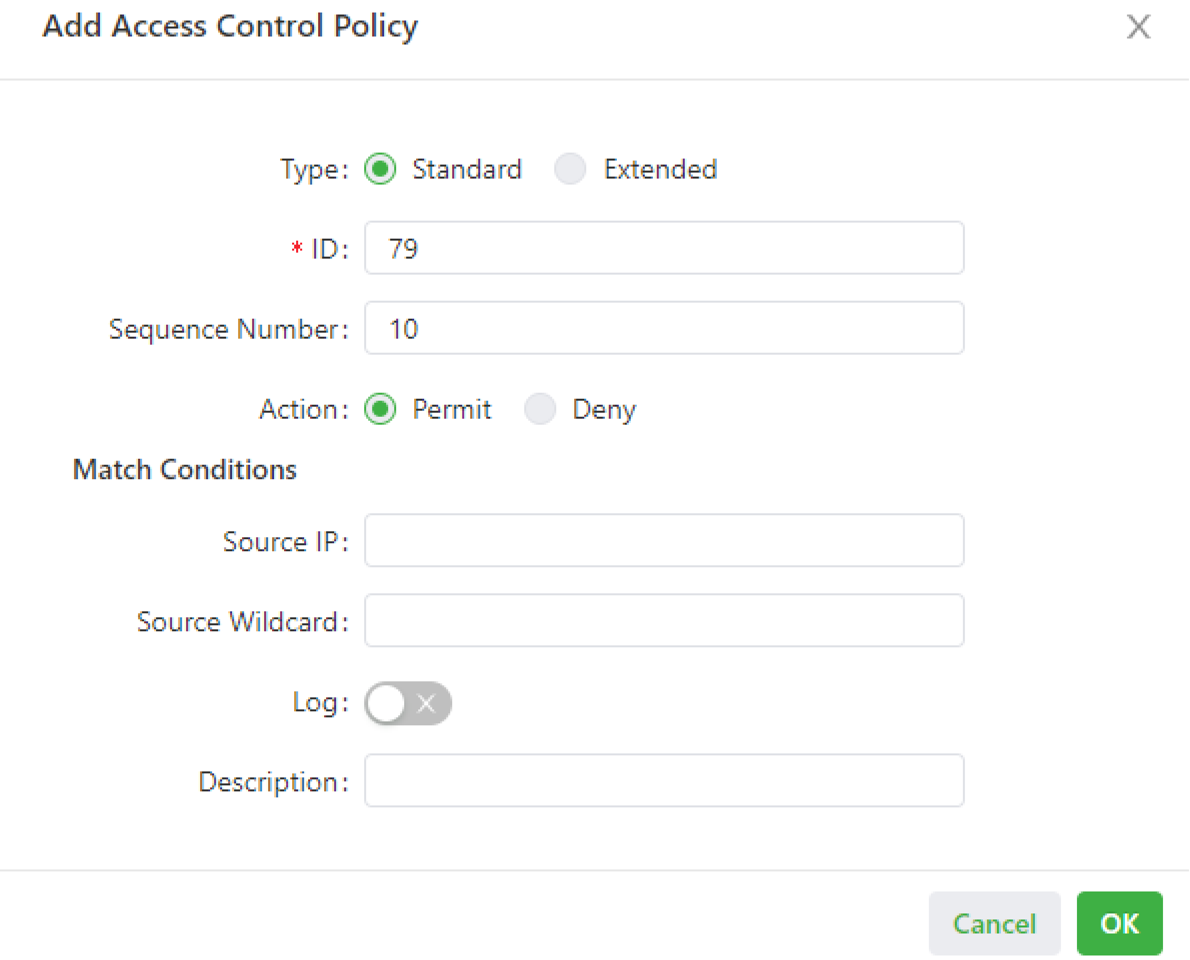
4.5.4.1. ACL

An access control list (ACL) permits or denies specified data flows (such as the data flow from a specified source IP address or account) based on a series of matching rules to filter the data reaching a network interface. You can configure a data filtering policy for a network interface on the **ACL** page. The configuration procedure is as follows:

1. Choose **Network > Firewall > ACL** to display the **ACL** page.
2. Click the Add icon under **Access Control Policy** to add an access control policy.

3. Set the parameters. For details about these parameters, see access control policy parameter description.
4. Click the Add or Edit icon under **ACL** to add an access control list on a specified interface.
5. Set the parameters. For details about these parameters, see access control list parameter description.
6. Click **OK** to save the configuration, and then click **Submit** to apply the configuration.

The following figure shows the configuration of a standard access control policy.



Add Access Control Policy

Type: ● Standard ○ Extended

* ID: 79

Sequence Number: 10

Action: ● Permit ○ Deny

Match Conditions

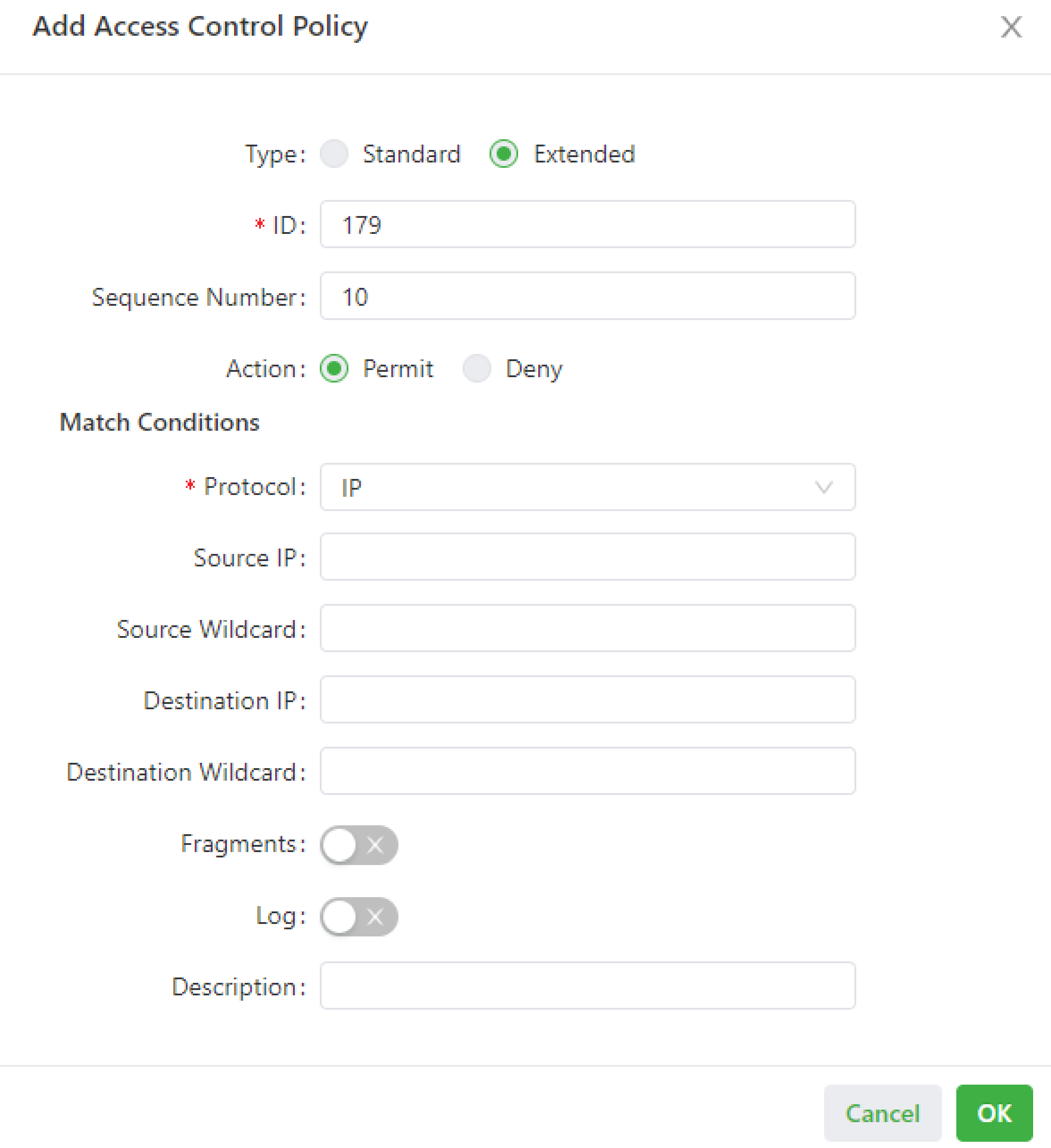
Source IP:

Source Wildcard:

Log: Off

Description:

The following figure shows the configuration of an extended access control policy.



Add Access Control Policy

Type: ○ Standard ● Extended

* ID: 179

Sequence Number: 10

Action: ● Permit ○ Deny

Match Conditions

* Protocol: IP

Source IP:

Source Wildcard:

Destination IP:

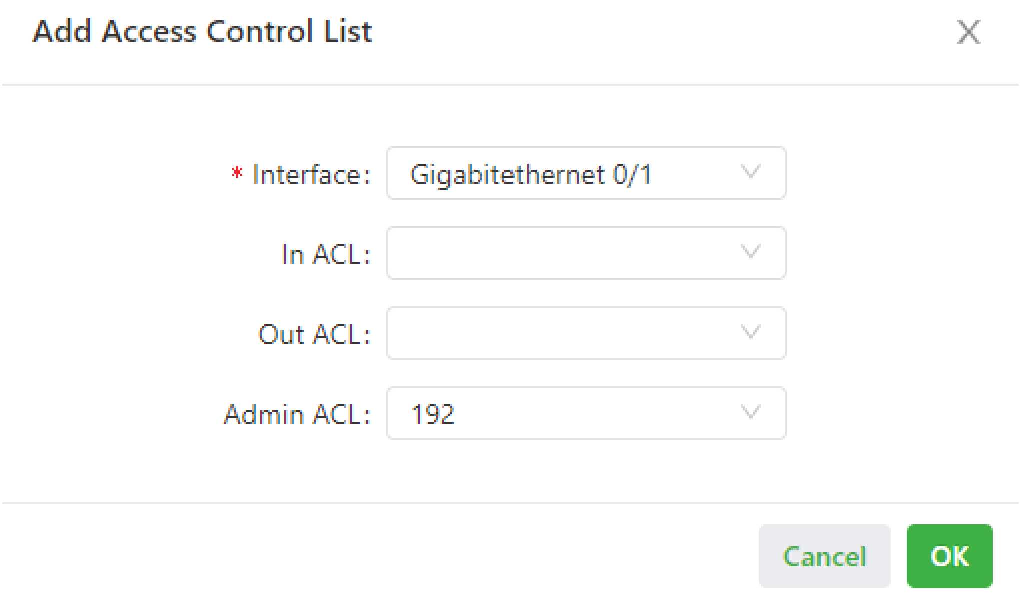
Destination Wildcard:

Fragments: off

Log: off

Description:

The following figure shows the configuration of an access control list.



Add Access Control List

* Interface: Gigabitethernet 0/1

In ACL:

Out ACL:

Admin ACL: 192

- Parameters of a standard access control policy are described as follows:
    - ID: specifies the ID of an ACL rule, in the range of 1-99. A smaller value indicates a higher priority of the rule.
    - Sequence Number: specifies the sequence number of the ACL rule. A smaller value indicates a higher priority of the rule.
    - Action: permits or denies forwarding of matching packets.
    - Source IP: specifies the source IP address of packets in the ACL rule. If this field is kept blank, the rule matches packets from all networks.
    - Source Wildcard: specifies the wildcard mask of the source IP address in the ACL rule.
    - Log: enables or disables recording of access control logs.
    - Description: records meanings of access control parameters.

- Parameters of an extended access control policy are described as follows:
    - ID: specifies the ID of an ACL rule, in the range of 100-199. A smaller value indicates a higher priority of the rule.
    - Sequence Number: specifies the sequence number of the ACL rule. A smaller value indicates a higher priority of the rule.
    - Action: permits or denies forwarding of matching packets.
    - Protocol: specifies the access control protocol.
    - Source IP: specifies the source IP address of packets in the ACL rule. If this field is kept blank, the rule matches packets from all networks.
    - Source Wildcard: specifies the wildcard mask of the source IP address in the ACL rule.
    - Source Port: specifies the source port number of packets. The value **any** indicates that TCP/UDP packets with any source ports match the rule. This parameter is available only when the TCP or UDP protocol is selected.
    - Destination IP: specifies the destination IP address of packets in the ACL rule. If this field is kept blank, the rule matches packets destined for all networks.
    - Destination Wildcard: specifies the wildcard mask of the destination IP address in the ACL rule.

    - Destination Port: specifies the destination port number of packets. The value **any** indicates that TCP/UDP packets with any destination ports match the rule. This parameter is available only when the TCP or UDP protocol is selected.
    - Established Connection: specifies the range of TCP packets controlled. If this option is selected, the system controls TCP packets on established connections and does not control those on unestablished connections. If this option is deselected, the system controls TCP packets on both established and unestablished connections. This parameter is available only when the TCP protocol is selected.
    - Fragments: enables or disables control of fragmented data packets sent from the interface.
    - Log: enables or disables recording of access control logs.
    - Description: records meanings of access control parameters.

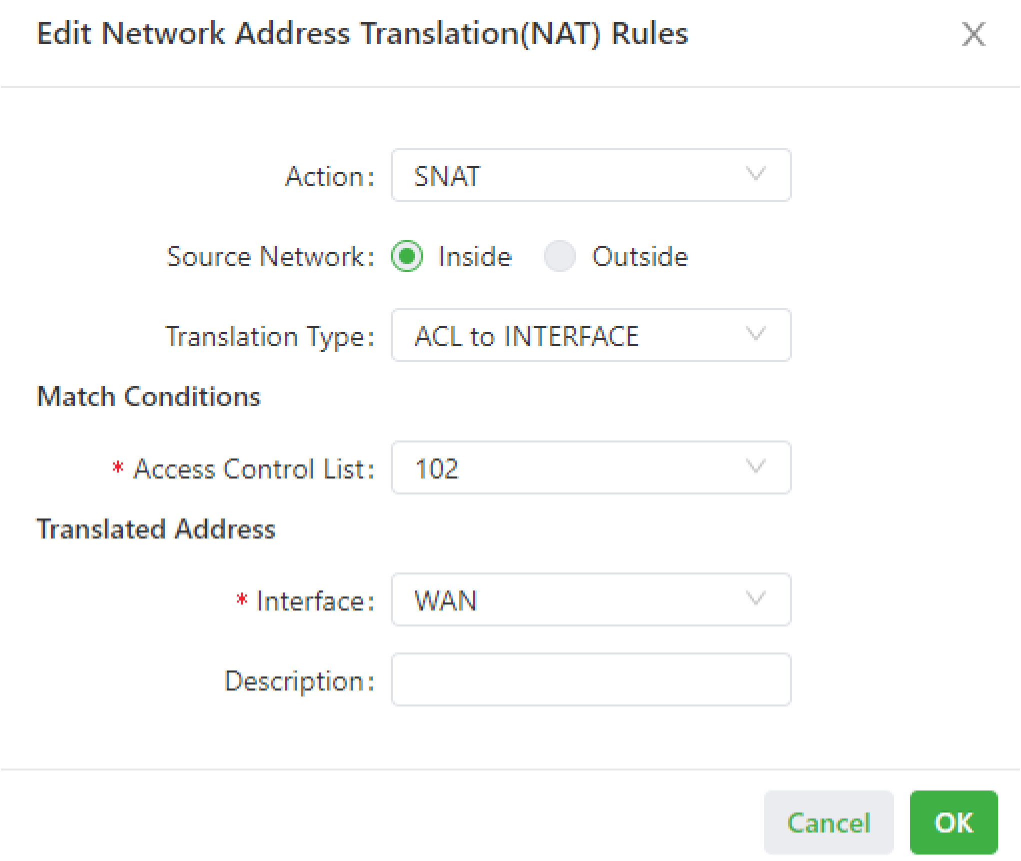
- Parameters of an access control list are described as follows:
    - Interface: specifies the name of the interface on which the access control policy is configured.
    - Rule: specifies the inbound, outbound, and administrative rules.

4.5.4.2. NAT

Network address translation (NAT) allows multiple hosts in a LAN to connect to the Internet by using one or multiple public IP addresses. This feature maps a few public IP addresses to many private IP addresses to conserve public IP addresses. You can view and configure NAT rules on the **NAT** page. The configuration procedure is as follows:

1. Choose **Network > Firewall > NAT** to display the **NAT** page.
2. Select an interface from the **Interface** drop-down list.
3. Click the Add icon under **Network Address Translation (NAT) Rules** to add an NAT rule and set parameters for the rule. For details about these parameters, see NAT rule parameter description.
4. Click **OK** to save the configuration, and then click **Submit** to apply the configuration.

As shown in the following figure, the NAT rule allows hosts connected to the IG502 to connect to the Internet by using the IP address of interface WAN.



Edit Network Address Translation(NAT) Rules

Action: SNAT

Source Network: ● Inside ○ Outside

Translation Type: ACL to INTERFACE

Match Conditions

* Access Control List: 102

Translated Address

* Interface: WAN

Description:

Parameters of the NAT rule are described as follows:

- Action
  - SNAT: uses the source network address translation feature that translates source IP addresses of data packets into another IP address. Generally, this feature is used for data packets sent to the Internet through the router.
  - DNAT: uses the destination network address translation feature that translates destination IP addresses of data packets into another IP

    address. Generally, this feature is used for data packets sent to the private network through the router.
    - 1:1NAT: uses one-to-one IP address translation.

- Source Network (available when the action is set to SNAT or DNAT):
    - Inside: translates private IP addresses.
    - Outside: translates public IP addresses.
- Translation Type, which can be:
    - IP to IP
    - IP to INTERFACE
    - IP PORT to IP PORT
    - ACL to INTERFACE
    - ACL to IP
- Access Control List (unavailable for 1:1 NAT): specifies the ACL rule used to match the packets of which the IP addresses are translated.
- Translated Address (unavailable for 1:1 NAT): specifies the IP address or interface translated from the source address.
- Description: specifies the description of the NAT rule.

4.6. Edge Computing

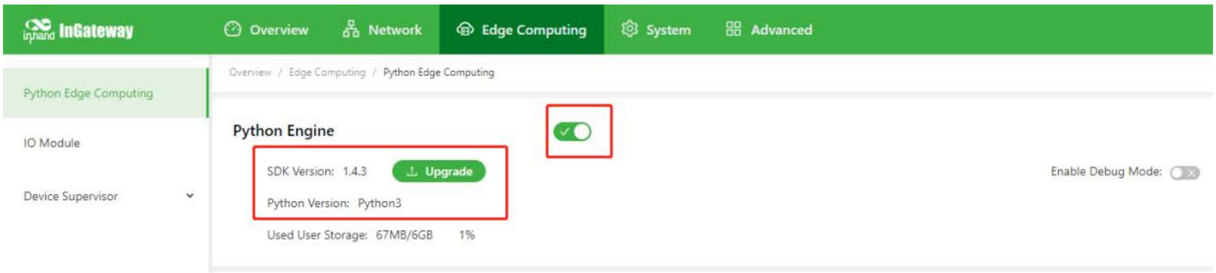
4.6.1. Python Edge Computing

4.6.1.1. Install and run Python App

To install and run Python App (App for short) in IG502, please refer to the following process, this document takes Device Supervisor as an example:

- Step 1: Install the App

  Before installing the App, you need to ensure that the Python Edge Computing Engine is enabled and the Python SDK is installed, as shown in the following figure:



Python Engine

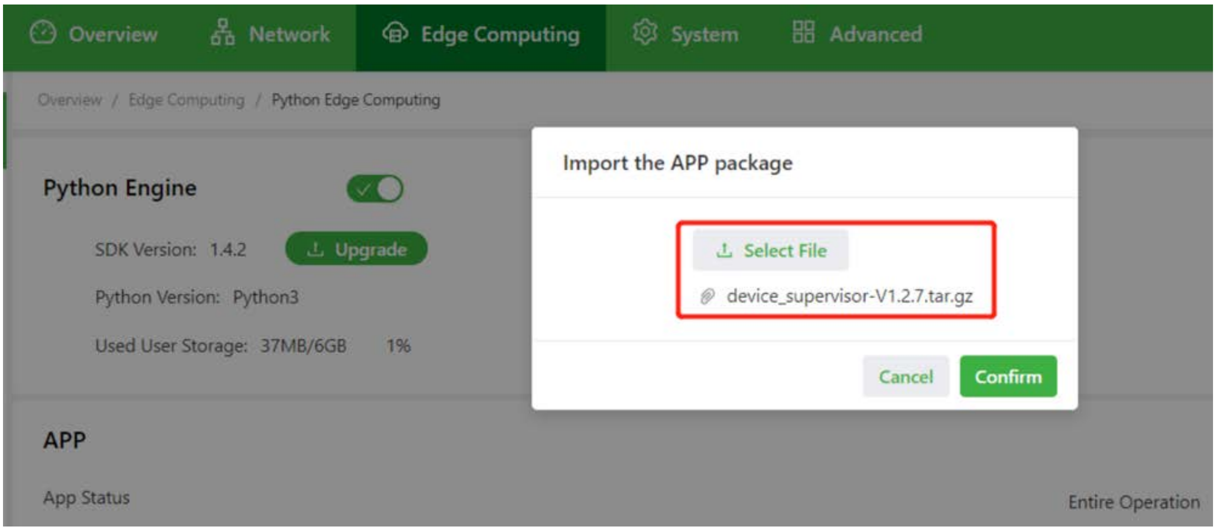
SDK Version: 1.4.3

Python Version: Python3

Used User Storage: 67MB/6GB 1%

Enable Debug Mode:

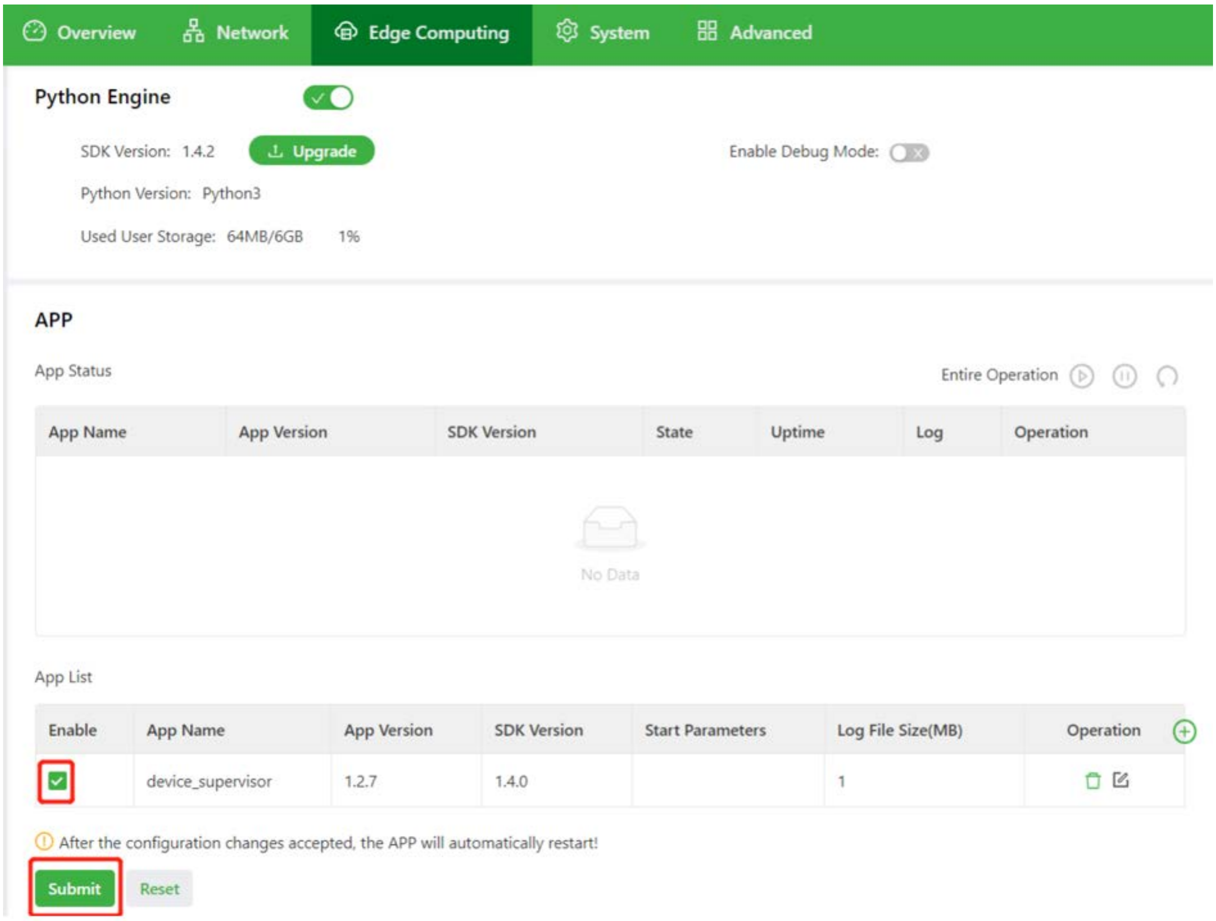
Choose Edge Computing > Python Edge Computing. click the Add button and select the App package file to be installed, then click Confirm



After importing, you can view the imported Apps, as shown in the following figure:

- Step 2: Run the App

Select enable App and click Submit.



Python Engine

SDK Version: 1.4.2

Enable Debug Mode:

Python Version: Python3

Used User Storage: 64MB/6GB 1%

APP

App Status

App Name	App Version	SDK Version	State	Uptime	Log	Operation

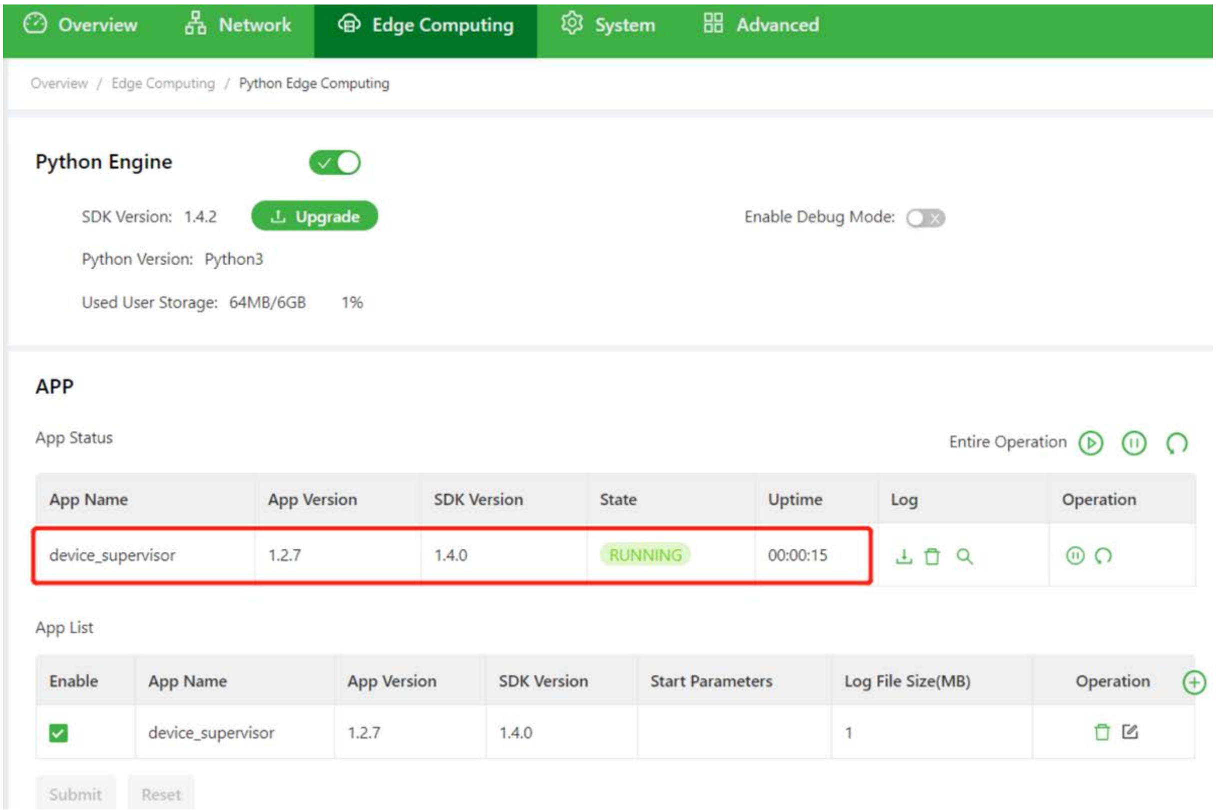
No Data

App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.7	1.4.0		1	

After the configuration changes accepted, the APP will automatically restart!

Once enabled, the App automatically runs and will run every time the IG502 is started.



Python Engine

SDK Version: 1.4.2

Enable Debug Mode:

Python Version: Python3

Used User Storage: 64MB/6GB 1%

APP

App Status

App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.7	1.4.0	RUNNING	00:00:15		

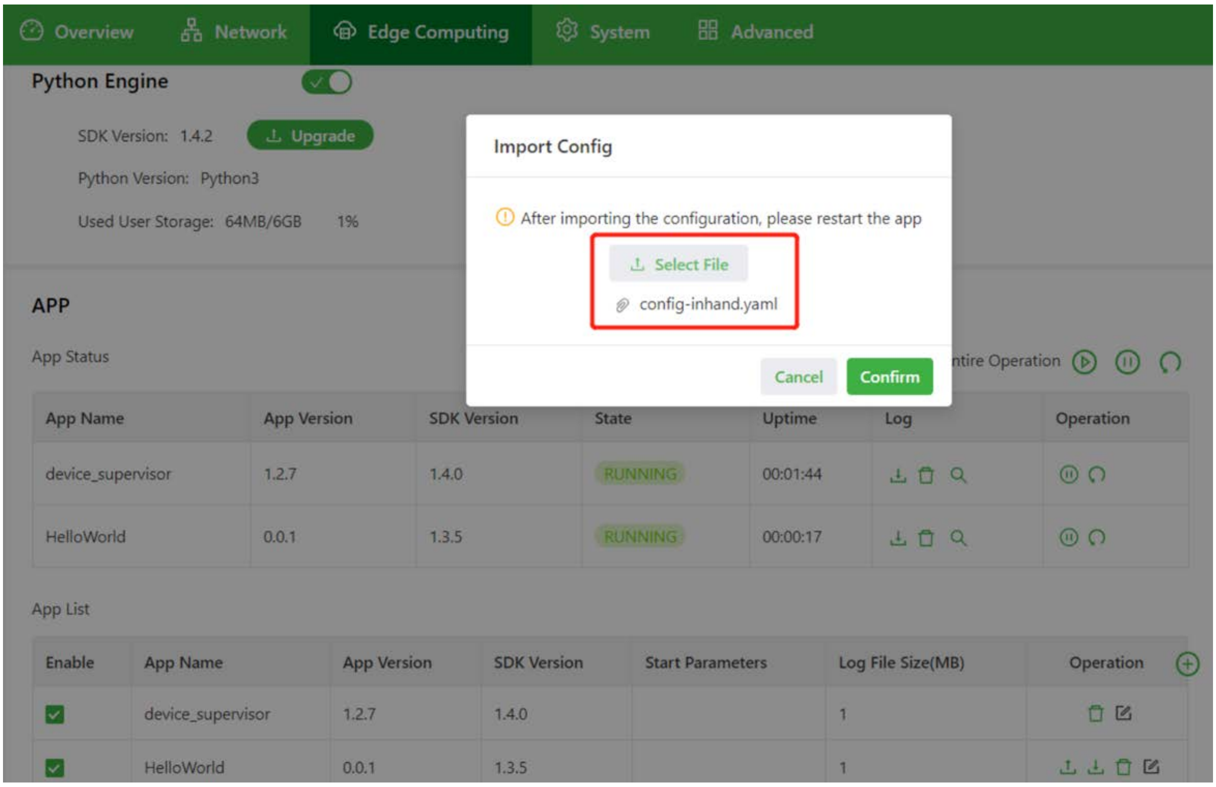
App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.7	1.4.0		1	

4.6.1.2. Update Configuration File for App

If the installed App supports importing configuration files to modify the running mode, you can update the App running configuration by referring to the following process:

- Step 1: Choose Edge Computing > Python Edge Computing, click the Import Configuration button and select the configuration file to be imported, then click Confirm.



Python Engine

SDK Version: 1.4.2

Python Version: Python3

Used User Storage: 64MB/6GB 1%

Import Config

After importing the configuration, please restart the app

config-inhand.yaml

APP

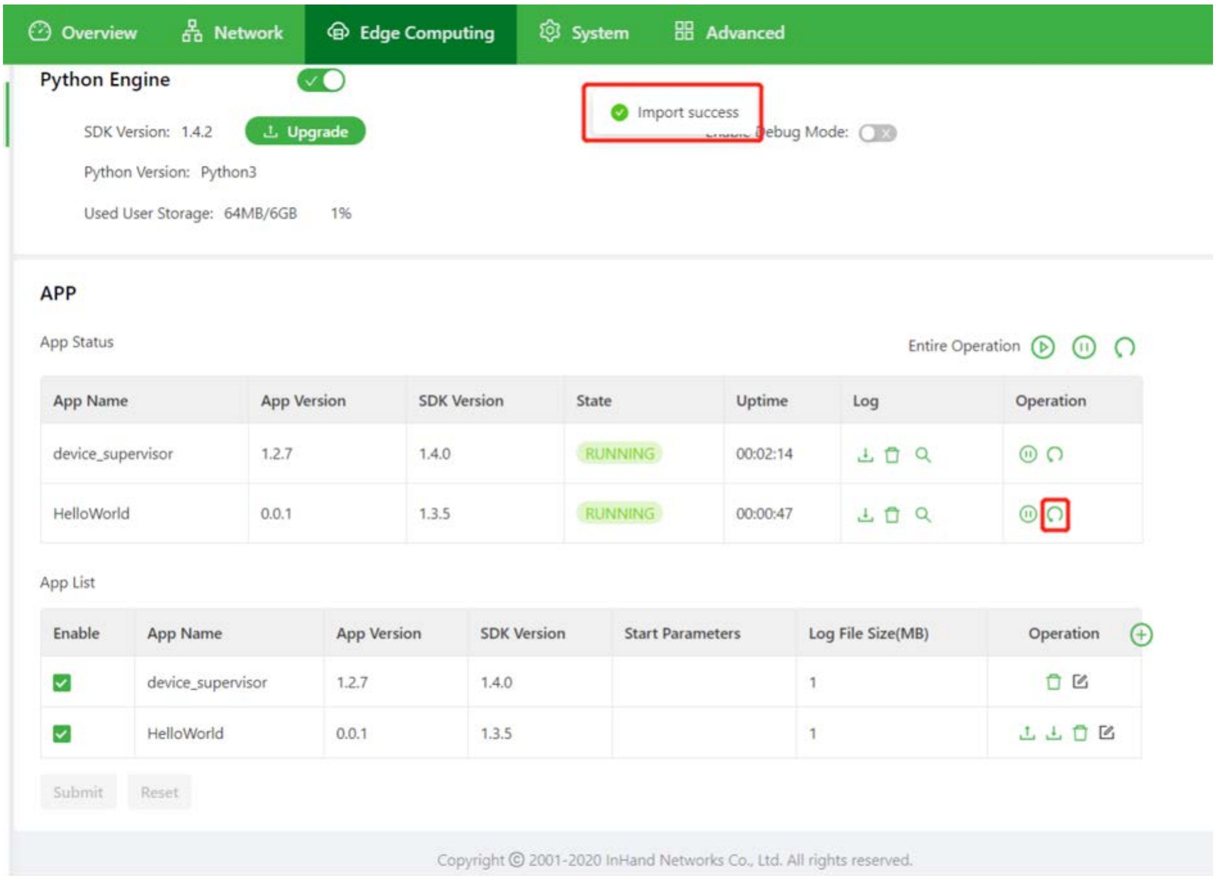
App Status

App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.7	1.4.0	RUNNING	00:01:44		
HelloWorld	0.0.1	1.3.5	RUNNING	00:00:17		

App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.7	1.4.0		1	
☑	HelloWorld	0.0.1	1.3.5		1	

- Step 2: Restart the App after the import is successful. After the App restarts, it will runing according to the imported configuration file.



Python Engine

SDK Version: 1.4.2

Python Version: Python3

Used User Storage: 64MB/6GB 1%

Debug Mode:

APP

App Status

App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.7	1.4.0	RUNNING	00:02:14		
HelloWorld	0.0.1	1.3.5	RUNNING	00:00:47		

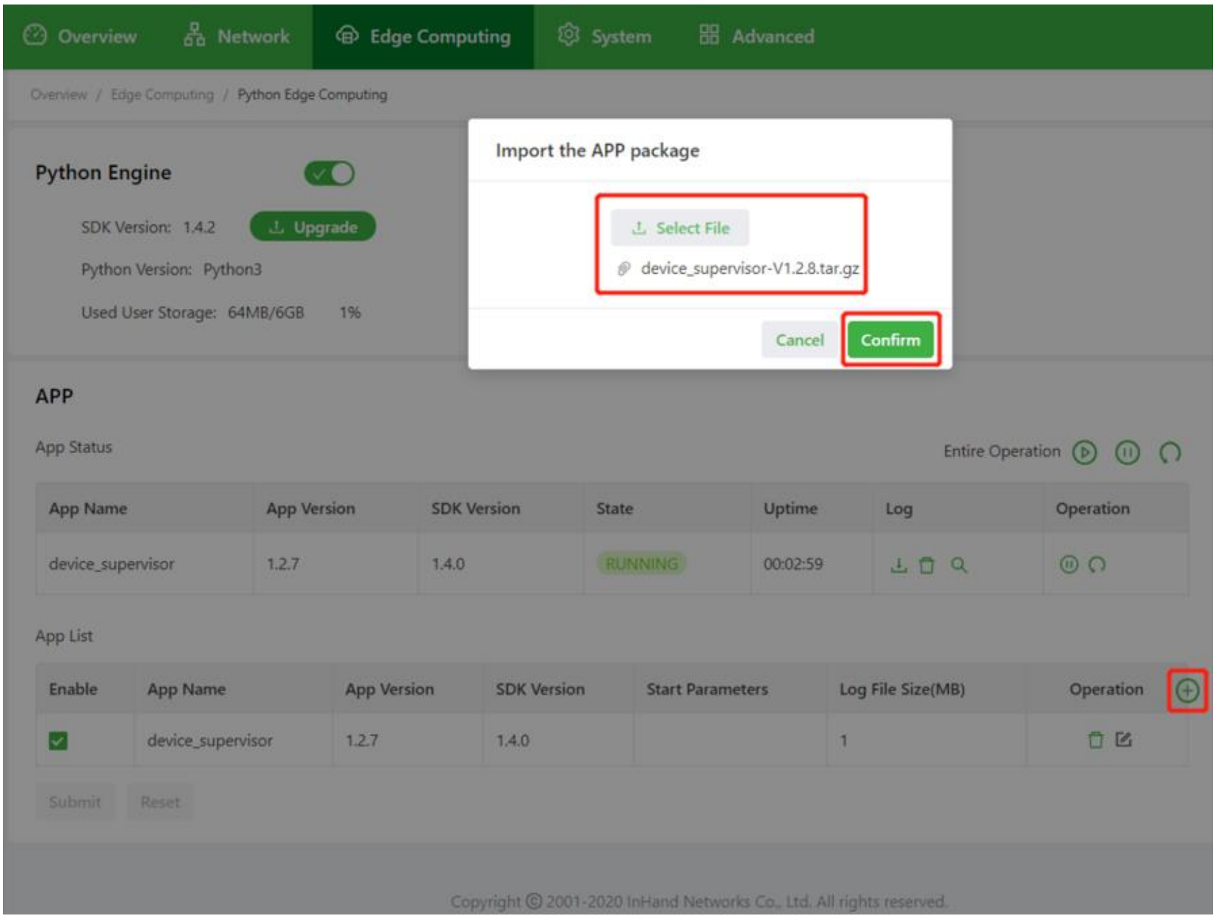
App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.7	1.4.0		1	
☑	HelloWorld	0.0.1	1.3.5		1	

Copyright © 2001-2020 InHand Networks Co., Ltd. All rights reserved.

4.6.1.3. Update Python App version

Generally, if you need to update the Python App version, you only need to import the new version of the App on the Edge Computing > Python Edge Computing page.



Import the APP package

device_supervisor-V1.2.8.tar.gz

Python Engine

SDK Version: 1.4.2

Python Version: Python3

Used User Storage: 64MB/6GB 1%

APP

App Status

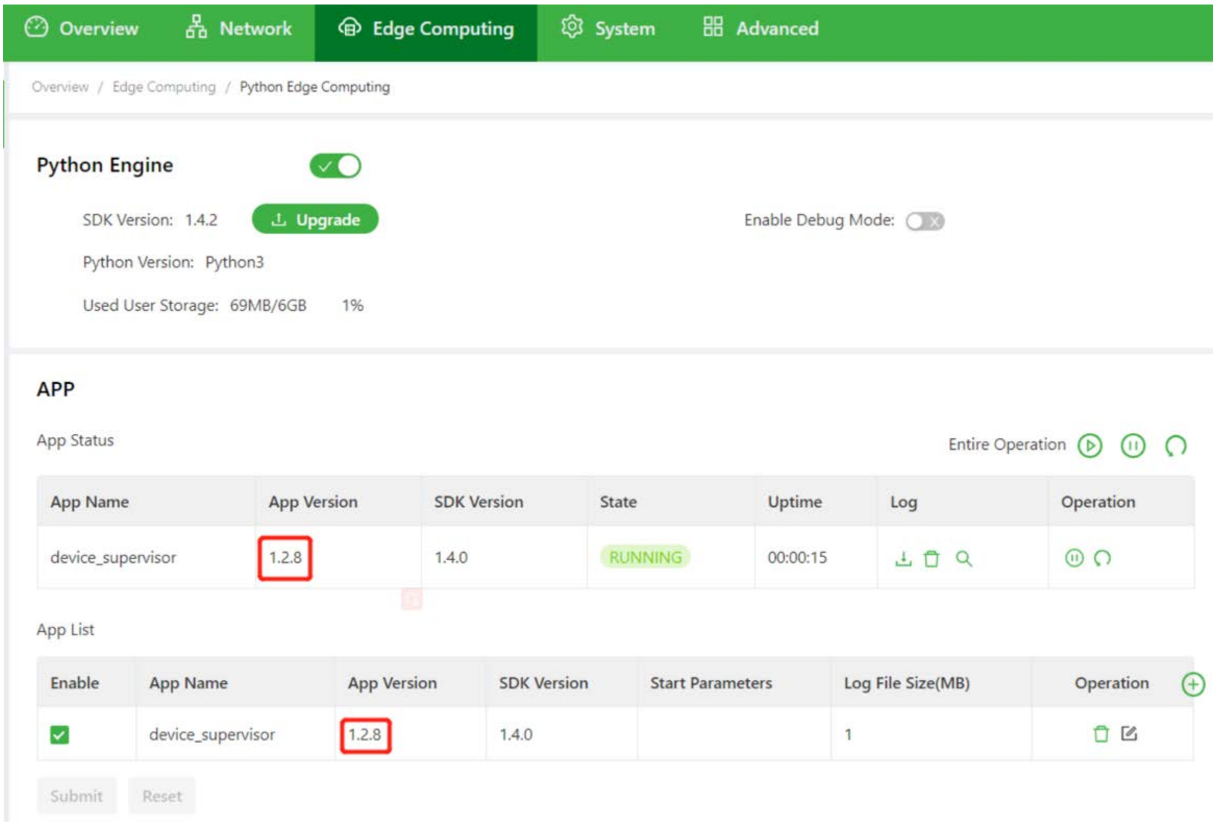
App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.7	1.4.0	RUNNING	00:02:59		

App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.7	1.4.0		1	

Copyright © 2001-2020 InHand Networks Co., Ltd. All rights reserved.

After the update is completed, as shown below：



Python Engine

SDK Version: 1.4.2

Enable Debug Mode:

Python Version: Python3

Used User Storage: 69MB/6GB 1%

APP

App Status

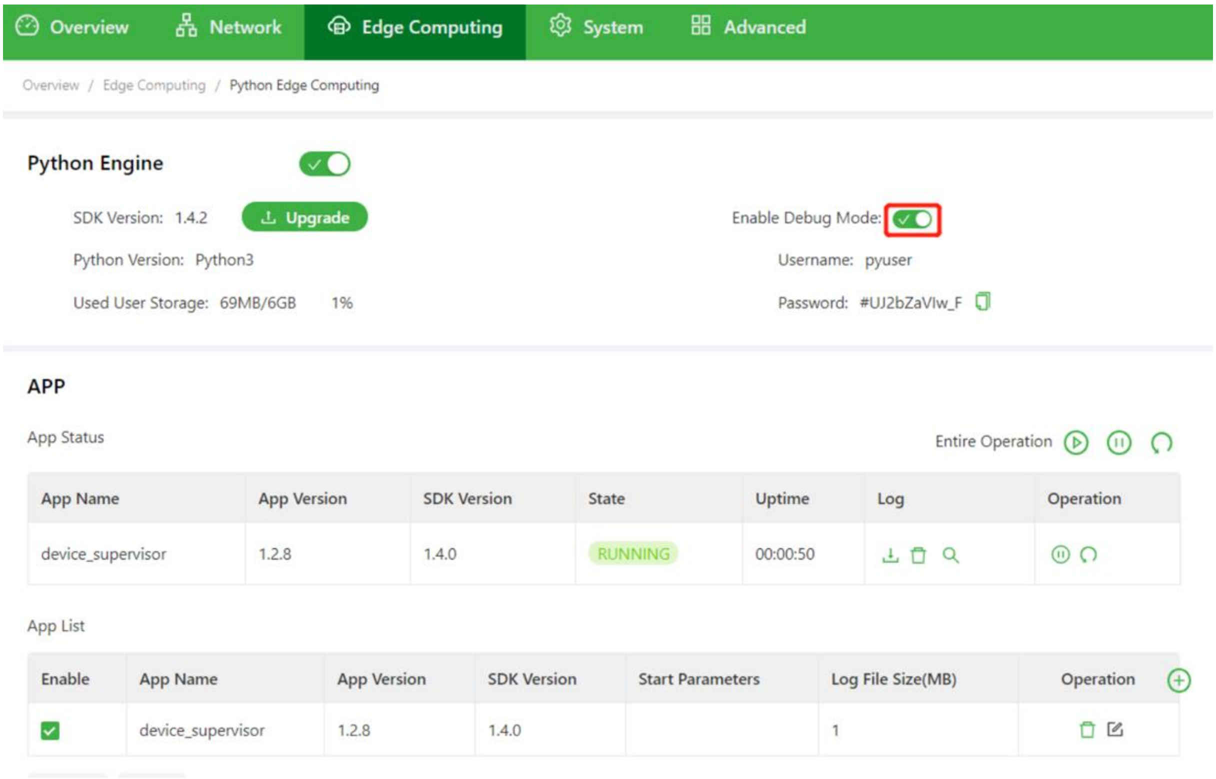
App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.8	1.4.0	RUNNING	00:00:15		

App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.8	1.4.0		1	

4.6.1.4. Enable the Debug Mode

To run and debug Python code on IG502, you need to enable IG502's debug mode. Choose Edge Computing > Python Edge Computing, select Enable Debug Mode. After enabling, you can develop IG502 through VS Code. How to use VS Code for Python development of IG502, please refer to Quick Start for MobiusPi Python Development.



Python Engine

SDK Version: 1.4.2

Python Version: Python3

Used User Storage: 69MB/6GB 1%

Enable Debug Mode: ✓

Username: pyuser

Password: #UJ2bZaVIw_F

APP

App Status

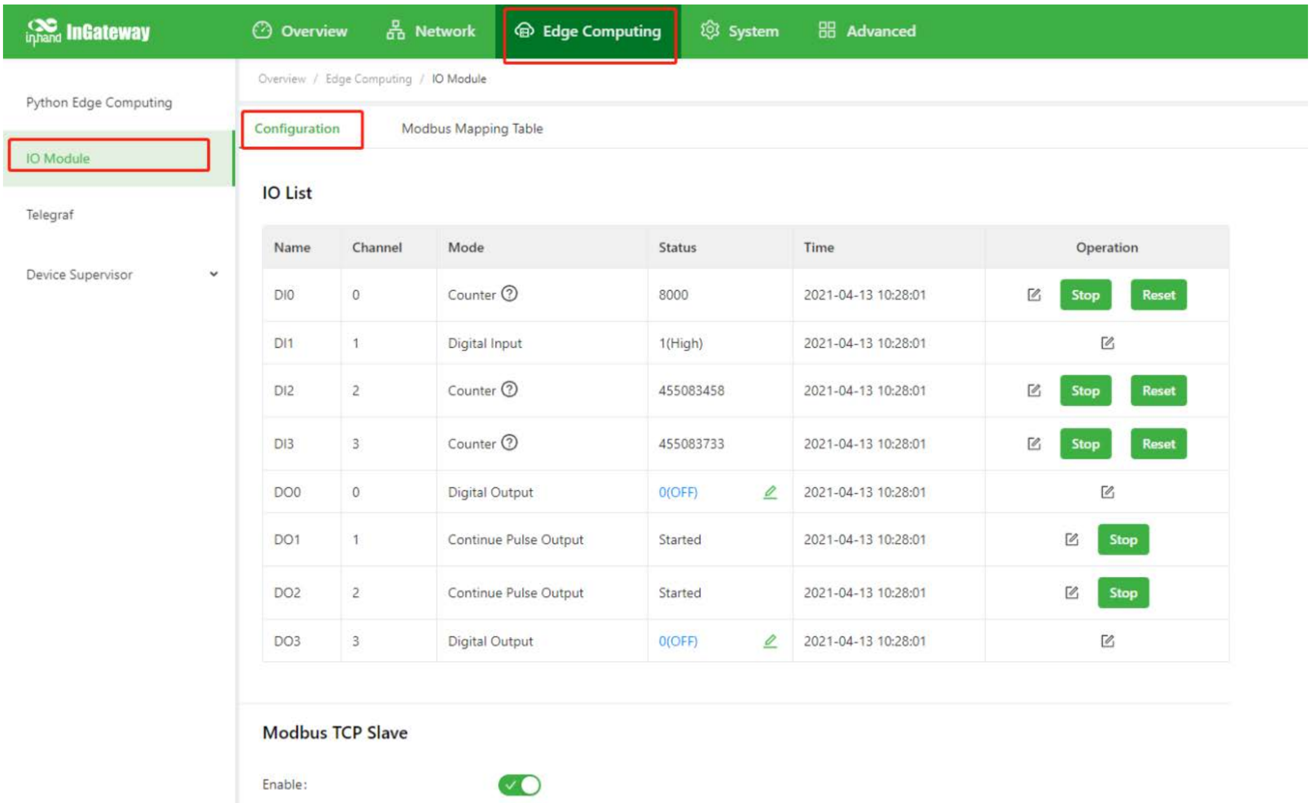
App Name	App Version	SDK Version	State	Uptime	Log	Operation
device_supervisor	1.2.8	1.4.0	RUNNING	00:00:50		

App List

Enable	App Name	App Version	SDK Version	Start Parameters	Log File Size(MB)	Operation
☑	device_supervisor	1.2.8	1.4.0		1	

After the debugging mode is enabled, IG502 will start an SSH server to listen on port 22 of LAN (default IP address being 192.168.2.1). The user name and password of the SSH server are displayed on the previous web page. A random password is generated every time the debugging mode is enabled or the IG502 is restarted to ensure security.

4.6.2. IO Module



IO List

Name	Channel	Mode	Status	Time	Operation
DI0	0	Counter ⓘ	8000	2021-04-13 10:28:01	✎ Stop Reset
DI1	1	Digital Input	1(High)	2021-04-13 10:28:01	✎
DI2	2	Counter ⓘ	455083458	2021-04-13 10:28:01	✎ Stop Reset
DI3	3	Counter ⓘ	455083733	2021-04-13 10:28:01	✎ Stop Reset
DO0	0	Digital Output	0(OFF) ✎	2021-04-13 10:28:01	✎
DO1	1	Continue Pulse Output	Started	2021-04-13 10:28:01	✎ Stop
DO2	2	Continue Pulse Output	Started	2021-04-13 10:28:01	✎ Stop
DO3	3	Digital Output	0(OFF) ✎	2021-04-13 10:28:01	✎

Modbus TCP Slave

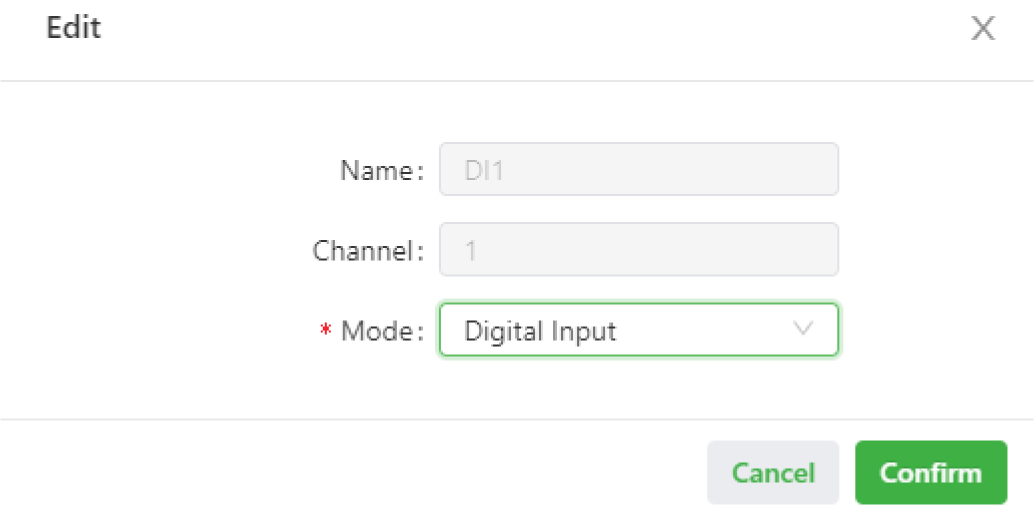
Enable: ✓

The procedure for configuring I/O and obtaining I/O status data is as follows:

Step 1: configure the I/O functions

Choose **"Edge Computing** > **IO Module** > **Configuration"** and configure the I/O functions based on the site requirements. The following figures show a configuration example.

Digital input



Edit

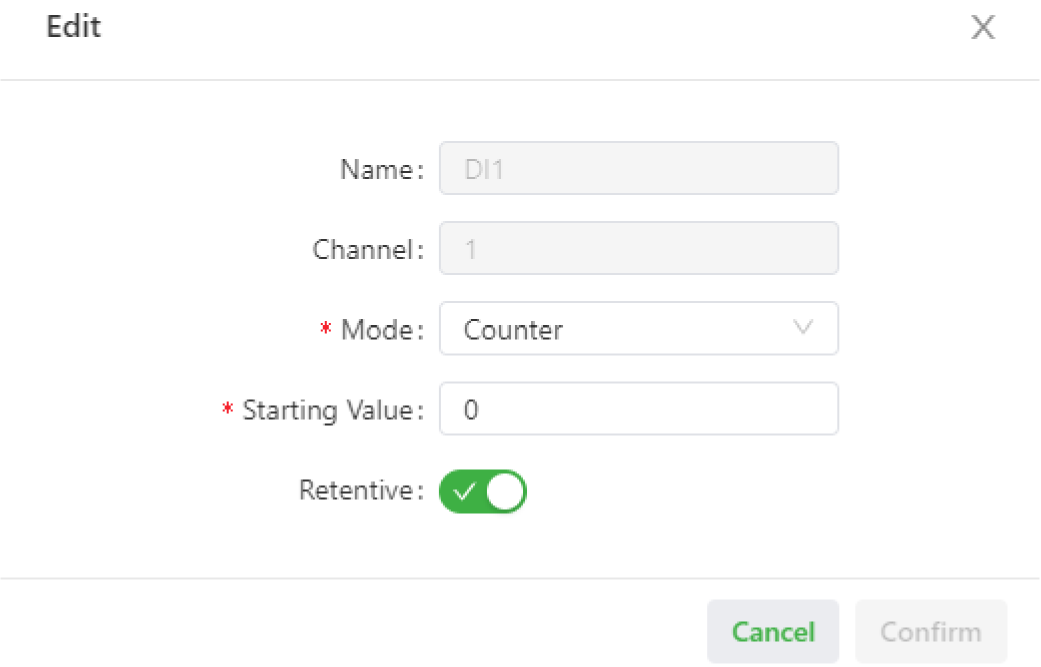
Name: DI1

Channel: 1

* Mode: Digital Input

Pulse counting

The starting value is 0. After power down, the value counted by the power down is retained.



Edit

Name: DI1

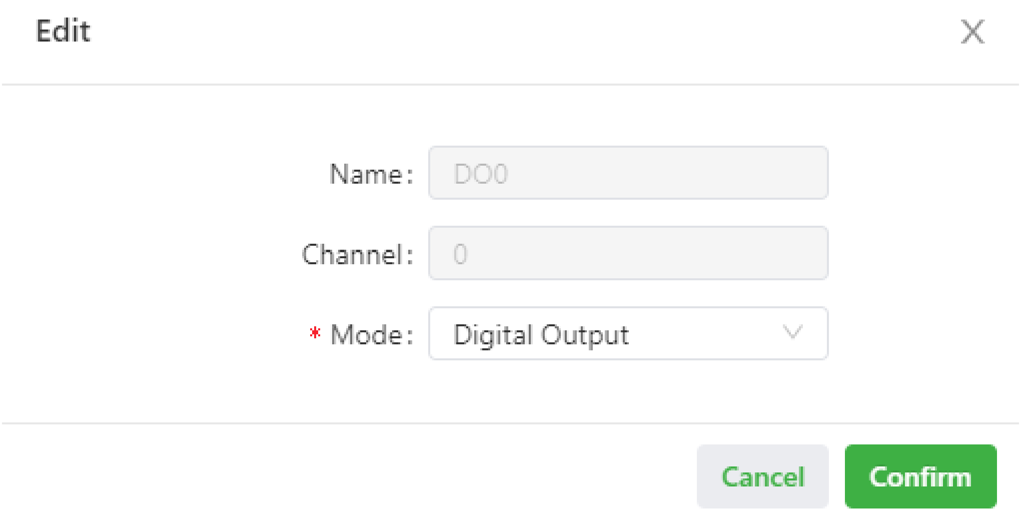
Channel: 1

* Mode: Counter

* Starting Value: 0

Retentive: ✓

Digital output



Edit

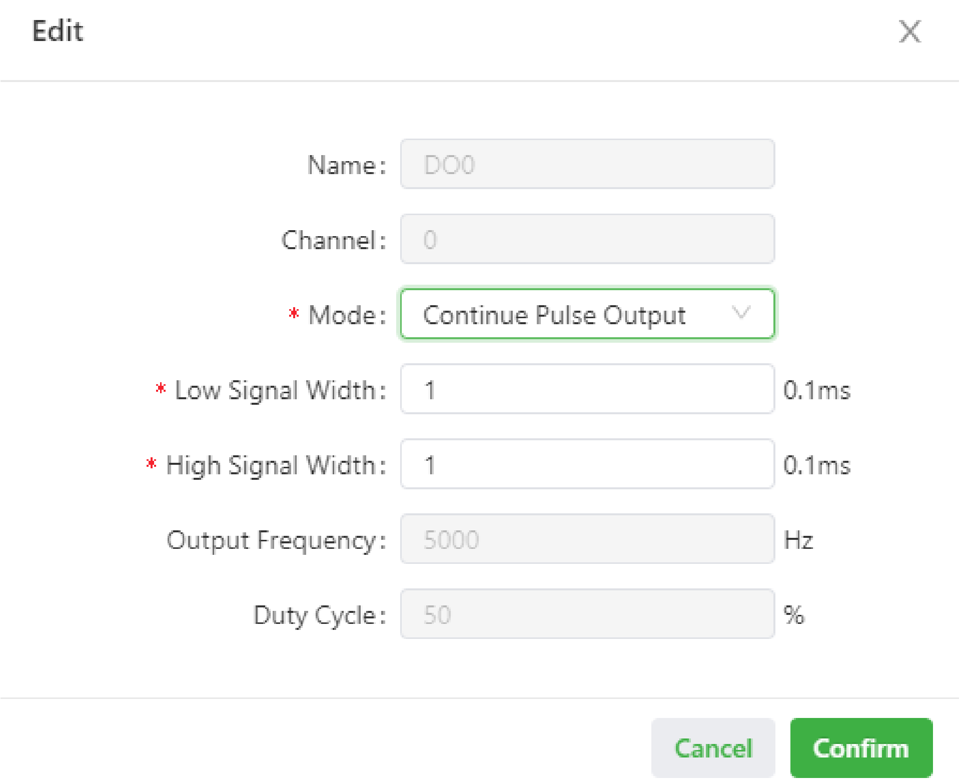
Name: DO0

Channel: 0

* Mode: Digital Output

Pulse output

According to the frequency of 5000 Hz, the duty cycle is 50% for the pulse output.



Edit

Name: DO0

Channel: 0

* Mode: Continue Pulse Output

* Low Signal Width: 1 0.1ms

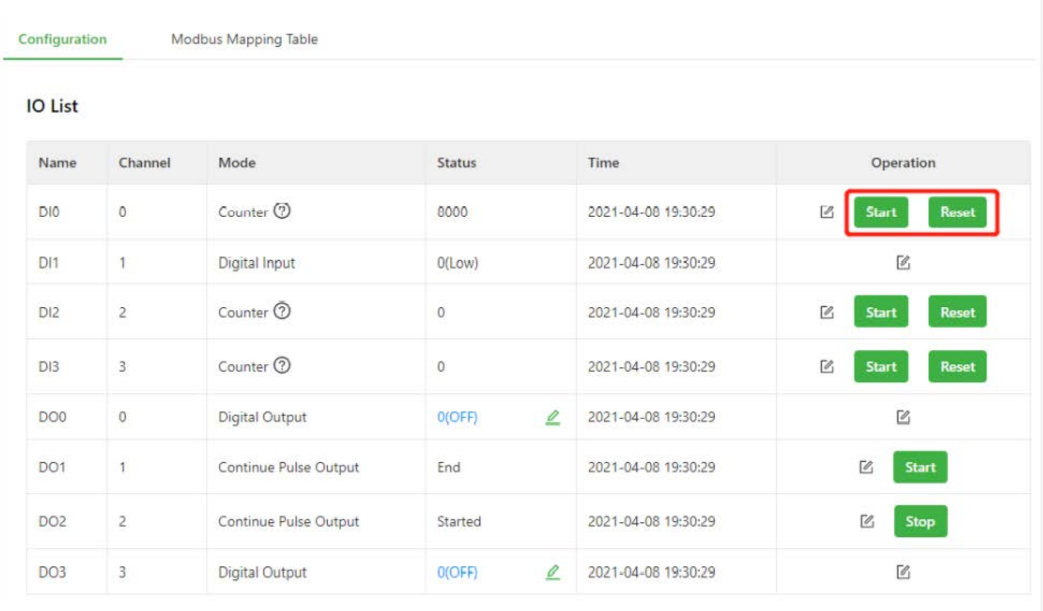
* High Signal Width: 1 0.1ms

Output Frequency: 5000 Hz

Duty Cycle: 50 %

Step 2 (optional): Set the pulse counting and pulse output.

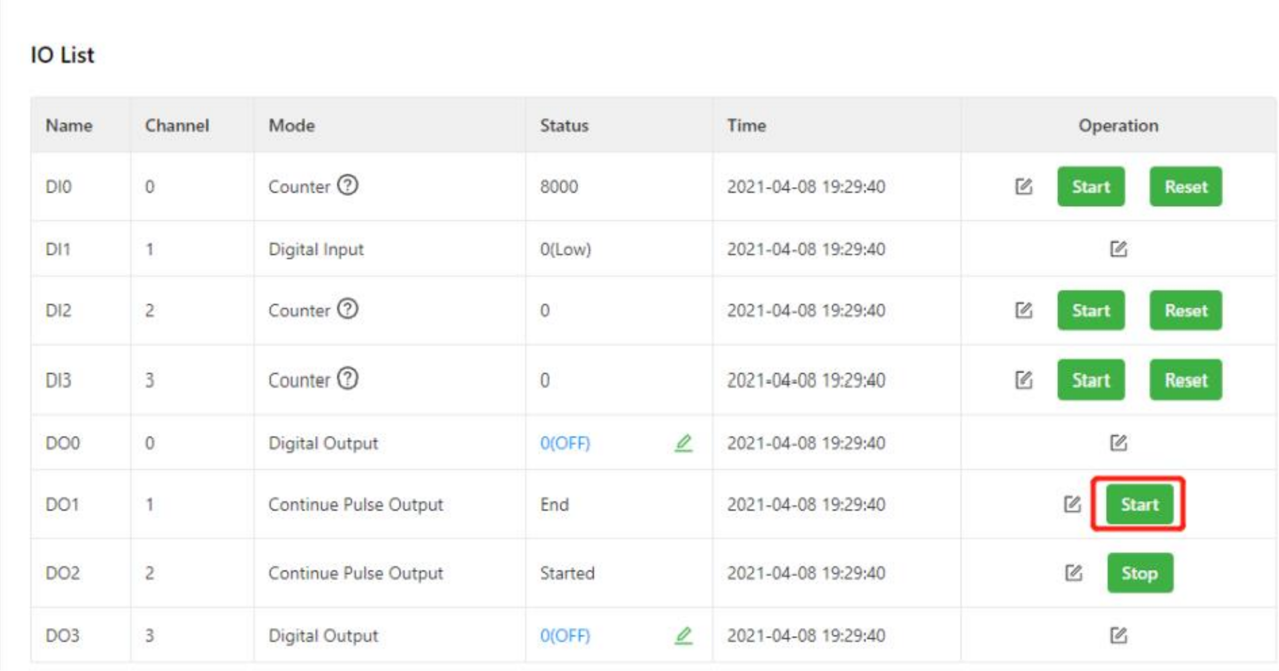
After setting DI to the pulse counting, click **Start** to count the pulses received by the DI. Otherwise, do not count it. Click **Reset** to reset the count value to the starting value.



IO List

Name	Channel	Mode	Status	Time	Operation
DI0	0	Counter ⓘ	8000	2021-04-08 19:30:29	✎ Start Reset
DI1	1	Digital Input	0(Low)	2021-04-08 19:30:29	✎
DI2	2	Counter ⓘ	0	2021-04-08 19:30:29	✎ Start Reset
DI3	3	Counter ⓘ	0	2021-04-08 19:30:29	✎ Start Reset
DO0	0	Digital Output	0(OFF) ✎	2021-04-08 19:30:29	✎
DO1	1	Continue Pulse Output	End	2021-04-08 19:30:29	✎ Start
DO2	2	Continue Pulse Output	Started	2021-04-08 19:30:29	✎ Stop
DO3	3	Digital Output	0(OFF) ✎	2021-04-08 19:30:29	✎

After setting DO to the pulse counting, click **Start** to output pulses based on the specified output frequency. Otherwise, do not output pulses.

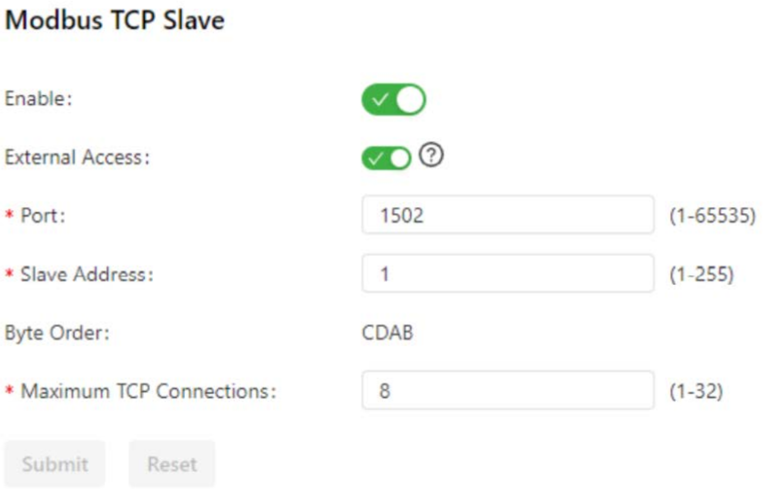


IO List

Name	Channel	Mode	Status	Time	Operation
DI0	0	Counter ?	8000	2021-04-08 19:29:40	Start Reset
DI1	1	Digital Input	0(Low)	2021-04-08 19:29:40	
DI2	2	Counter ?	0	2021-04-08 19:29:40	Start Reset
DI3	3	Counter ?	0	2021-04-08 19:29:40	Start Reset
DO0	0	Digital Output	0(OFF)	2021-04-08 19:29:40	
DO1	1	Continue Pulse Output	End	2021-04-08 19:29:40	Start
DO2	2	Continue Pulse Output	Started	2021-04-08 19:29:40	Stop
DO3	3	Digital Output	0(OFF)	2021-04-08 19:29:40	

Step 3: **Set Modbus TCP Slave.**

Turn on the **Enable** switch to enable the Modbus TCP Slave function. This function allows Modbus TCP Master to read the I/O status of IG502. After you turn on the **External Access** switch, Modbus TCP Master outside the gateway can read the I/O status of IG502, such as the SCADA software. Set other parameters based on the site requirements. The following figure shows a configuration example.

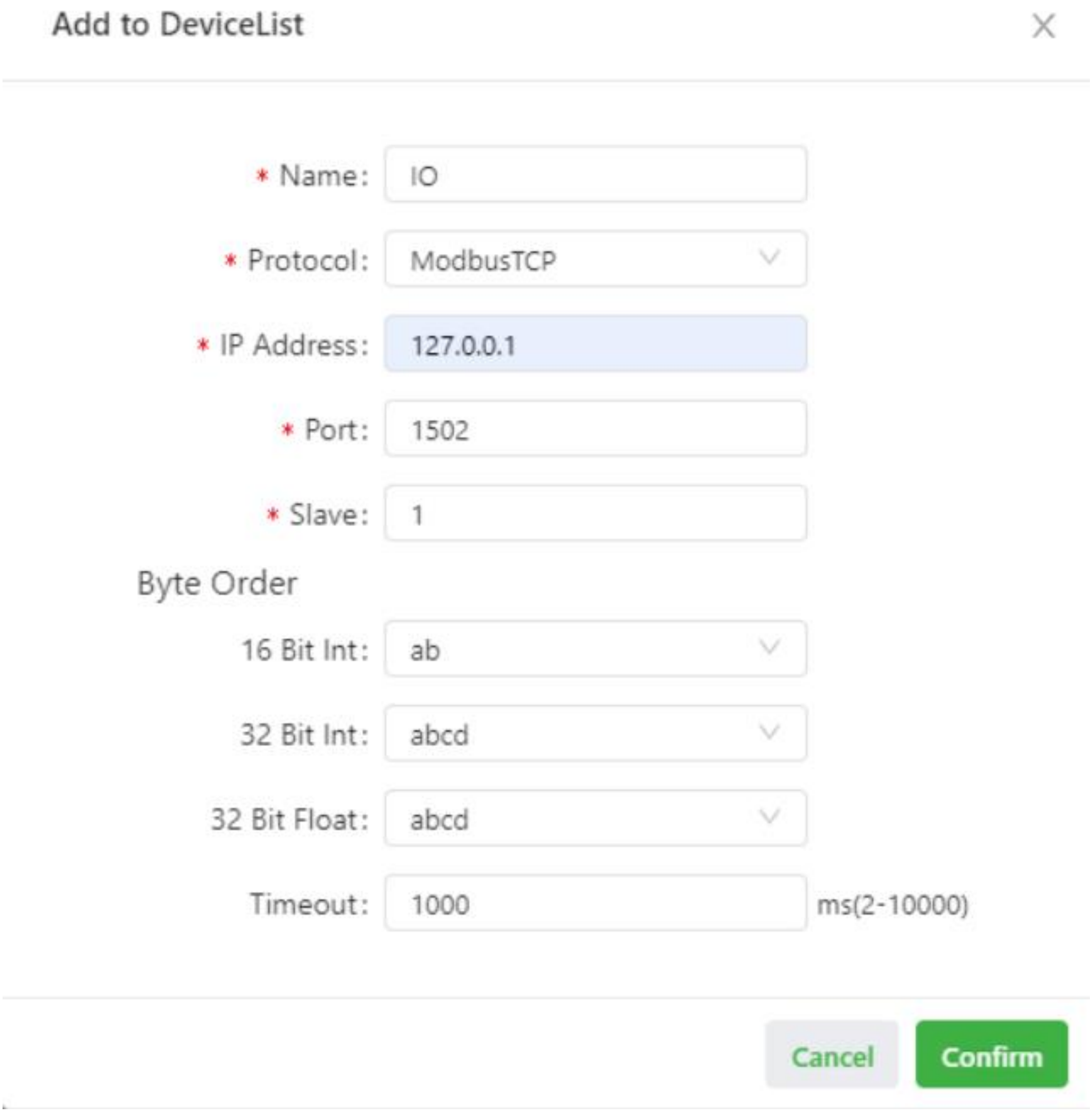


Modbus TCP Slave

Enable:	✓	
External Access:	✓ ?	
* Port:	1502	(1-65535)
* Slave Address:	1	(1-255)
Byte Order:	CDAB	
* Maximum TCP Connections:	8	(1-32)

Step 4: Read the I/O status through Modbus TCP.

Use Device Supervisor to read the I/O status of IG502 in Step 3 as an example. First, add a Modbus TCP controller and set the controller communication parameters based on Modbus TCP Slave.



Add to DeviceList

* Name: IO

* Protocol: ModbusTCP

* IP Address: 127.0.0.1

* Port: 1502

* Slave: 1

Byte Order

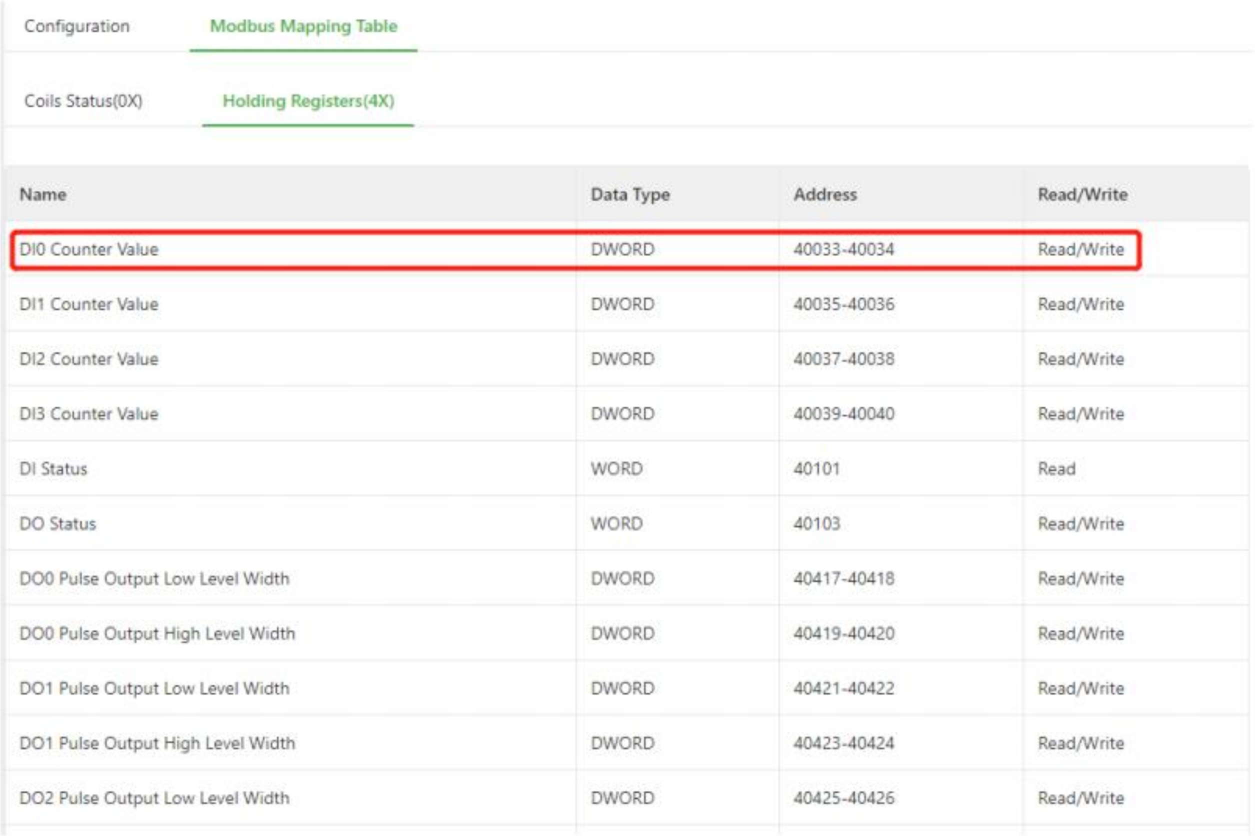
16 Bit Int: ab

32 Bit Int: abcd

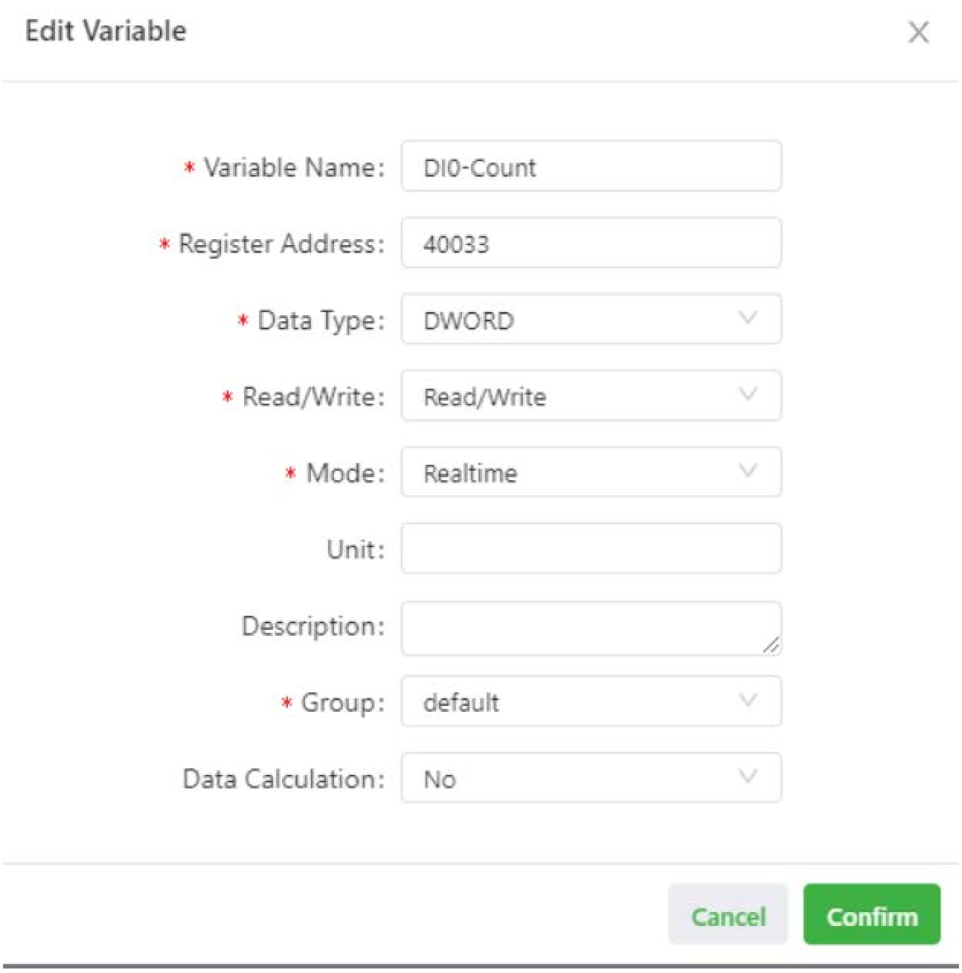
32 Bit Float: abcd

Timeout: 1000 ms(2-10000)

Then, configure the data to be collected according to the Modbus mapping table. For example, read **DI0 Counter Value** as an example.



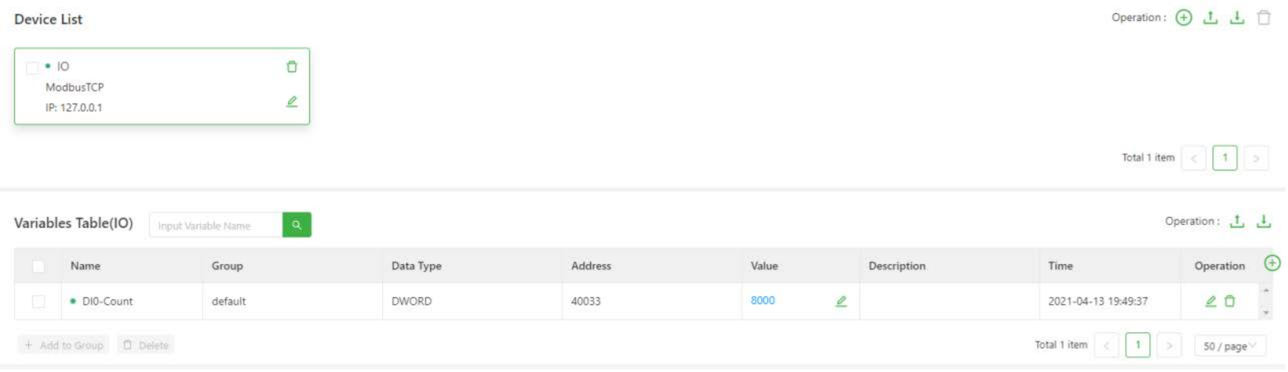
Name	Data Type	Address	Read/Write
DI0 Counter Value	DWORD	40033-40034	Read/Write
DI1 Counter Value	DWORD	40035-40036	Read/Write
DI2 Counter Value	DWORD	40037-40038	Read/Write
DI3 Counter Value	DWORD	40039-40040	Read/Write
DI Status	WORD	40101	Read
DO Status	WORD	40103	Read/Write
DO0 Pulse Output Low Level Width	DWORD	40417-40418	Read/Write
DO0 Pulse Output High Level Width	DWORD	40419-40420	Read/Write
DO1 Pulse Output Low Level Width	DWORD	40421-40422	Read/Write
DO1 Pulse Output High Level Width	DWORD	40423-40424	Read/Write
DO2 Pulse Output Low Level Width	DWORD	40425-40426	Read/Write



Edit Variable

* Variable Name: DI0-Count
* Register Address: 40033
* Data Type: DWORD
* Read/Write: Read/Write
* Mode: Realtime
Unit:
Description:
* Group: default
Data Calculation: No

After the configuration is completed, you can obtain **DI0 Counter Value**.



Device List

IO
ModbusTCP
IP: 127.0.0.1

Total 1 item

Variables Table(IO)

Name	Group	Data Type	Address	Value	Description	Time	Operation
DI0-Count	default	DWORD	40033	8000		2021-04-13 19:49:37	

Total 1 item

4.7. System

4.7.1. System Time

To enable the IG502 to cooperate with other devices properly, you may need to set an accurate system time for it. For this purpose, set the system time on the **System Time** page and enable the NTP protocol to implement clock synchronization among all clock-supporting devices on the network. In this way, all devices maintain the same clock to provide applications based on the consistent time. Follow these steps to set the system time:

Method 1: Select a time zone.

1. Choose **System** > **System Time** to display the **System Time** page.
2. Select the time zone where the IG502 is located from the **Time Zone** drop-down list.
3. Click **Apply**.

Method 2: Set the system time manually.

1. Choose **System > System Time** to display the **System Time** page.
2. Set a specific time in the Set Time field.
3. Click **Apply**.

Method 3: Use the local time of the PC.

1. Choose **System > System Time** to display the **System Time** page.
2. The IG502 can obtain the time of the PC as its local time.
3. Click Sync next to the Device Time field.

Method 4: Enable SNTP clients.

1. Choose System > System Time to display the System Time page.
2. Select Enable SNTP Clients.
3. Set the parameters. For details about these parameters, see SNTP client parameter description.
4. Click Submit to apply the configuration.

4.7.2. System Logs

Choose **System > Log** to display the **Log** page. This page displays a large amount of information about the network and IG502, such as its running status and changes of configuration. On the **Configure** page, you can set a remote log server. Then, the IG502 will synchronize all system logs to the remote log server. The host used as the remote log server must run a remote log program (for xample, Kiwi Syslog Daemon).

4.7.3. Configuration Management

Choose **System > Configuration Management** to display the **Configuration Management** page. On this page, you can back up configuration parameters, import parameter settings, and restore factory settings of the IG502. These functions are described as follows:

- Configuration Management
    - Auto Save: enables or disables automatic saving of modified configuration in the startup configuration file.
    - Encrypted: enables or disables password encryption. After this option is selected, all passwords configured on the IG502 web system are displayed in encrypted text. This feature improves the security of passwords.
- Configuration Files Operations
    - Import Startup Config: allows you to import a configuration file as the startup configuration of the IG502. The IG502 will load the imported configuration file upon a reboot. Ensure the validity and correct order of commands in the imported configuration file. The IG502 filters out invalid commands in the imported configuration file, and then saves the valid commands as the startup configuration. The system will execute these commands sequentially

after a reboot. If commands in the imported configuration file are not listed in a valid order, the system cannot enter the expected state after a reboot.

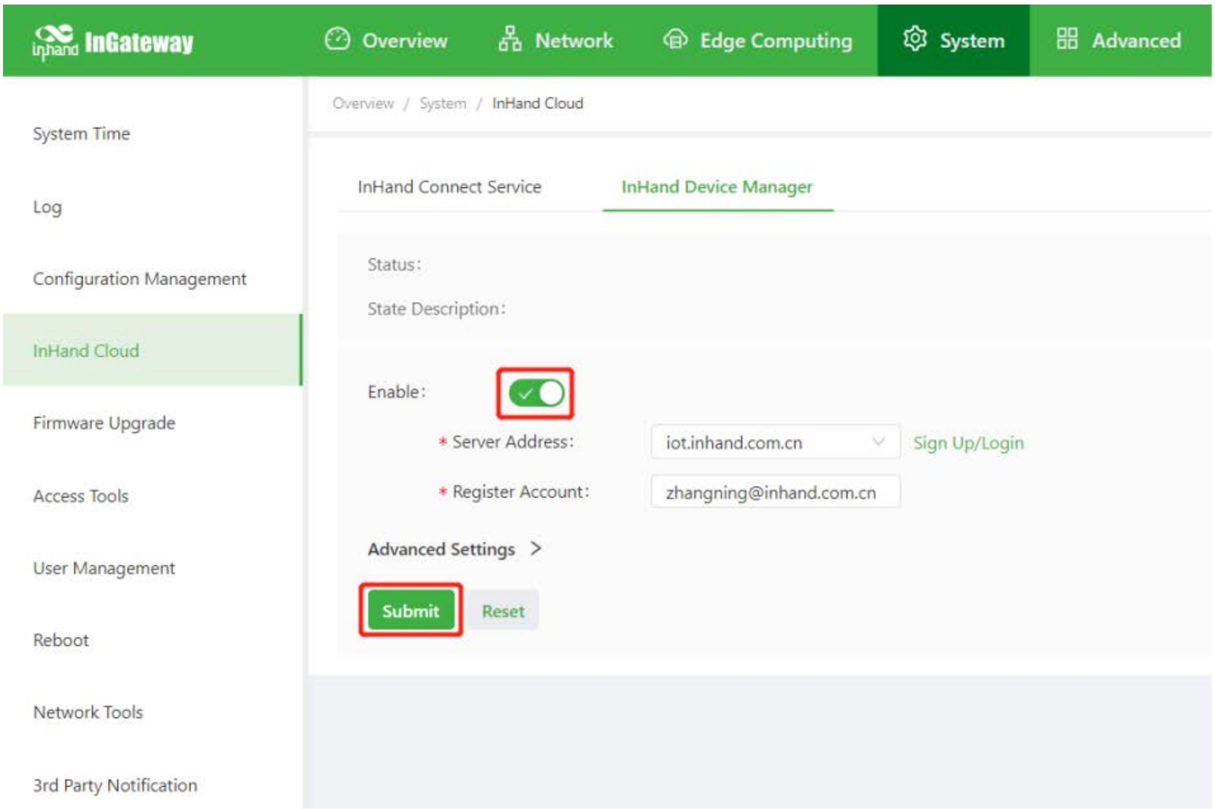
- Export Startup Config: allows you to back up the startup configuration on a host. The startup configuration is the configuration that the IG502 loads after it starts.
- Export Running Config: allows you to back up the running configuration on a host. The running configuration is the configuration that the IG502 is running.
- Restore Factory Configuration: allows you to restore the factory settings of the IG502. This operation restores all parameters on the IG502 to the default settings. The factory settings are restored after a reboot of the IG502.

4.7.4. InHand Cloud

The InHand Cloud developed by InHand supports functions such as monitoring IG502 status, remote maintenance of equipment, remote batch delivery of IG502 configuration, and IG502 batch upgrade, helping users to conveniently and efficiently manage IG502 and field devices. In order to enable the InHand Cloud to remotely manage the IG502 and field devices, the IG502 needs to be connected to the cloud platform. The connection method is as follows:

Choose System Management > InHand Cloud, tick Enable InHand Cloud and configure the corresponding server address and registered account, and click Submit after the configuration is complete. The **InHand Connect Service** platform mainly provides users with remote maintenance channels, and the **InHand Device Manager** platform mainly provides users with gateway management services (such as batch remote upgrades, etc.).

- Server address: the address of the InHand Cloud.
- Registered account: the InHand Cloud account associated with the IG502 device (if you have not registered an account, you need to register an account first)
- Advanced settings: Contains configurations such as heartbeat interval. Generally, you can use the default configuration.



Status:

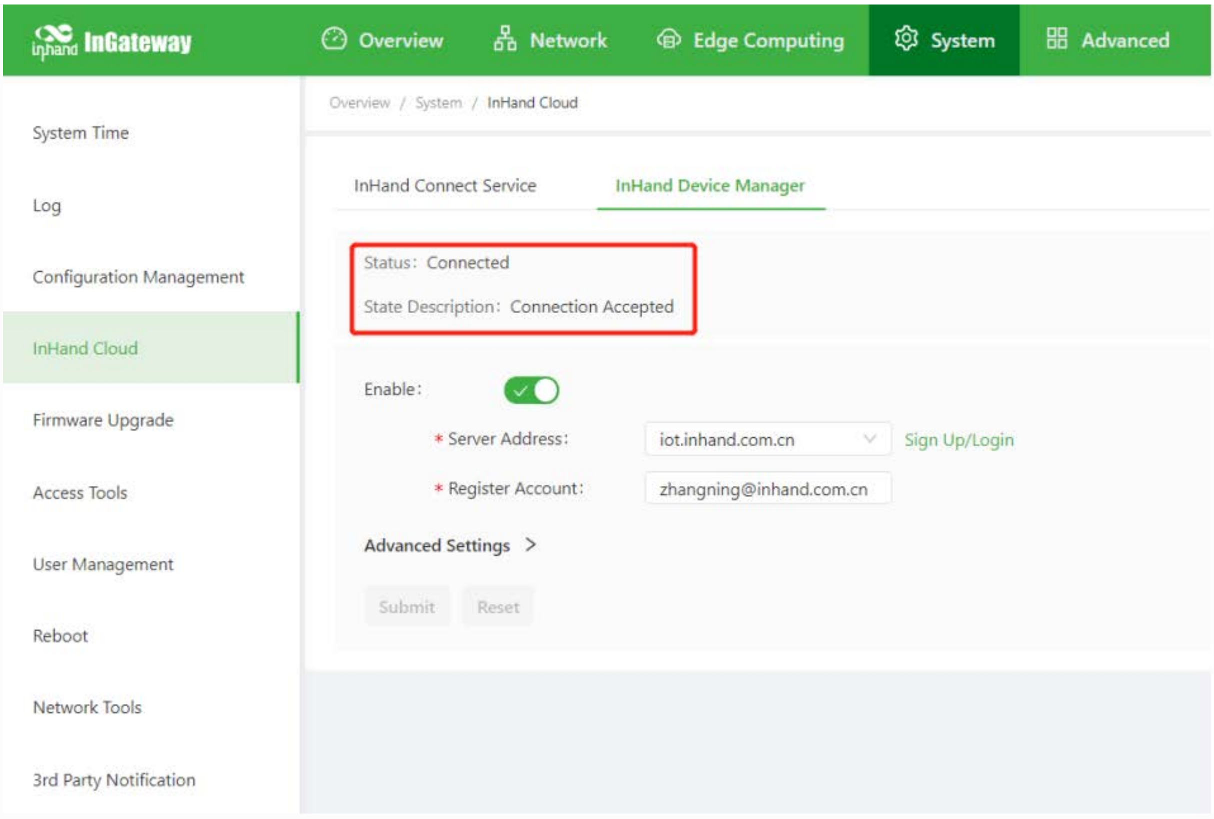
State Description:

Enable: ✓

* Server Address: iot.inhand.com.cn

* Register Account: zhangning@inhand.com.cn

After the IG502 is successfully connected to the InHand Device Manager, the status is described as Connection Accepted.



Status: Connected

State Description: Connection Accepted

Enable: ✓

* Server Address: iot.inhand.com.cn

* Register Account: zhangning@inhand.com.cn

4.7.5. Firmware Upgrade

You can upgrade the firmware version for the IG502 on the **Firmware Upgrade** page, so that the IG502 can provide new functions or better user experiences. Follow these steps to upgrade the firmware version:

1. Choose **System** > **Firmware Upgrade** to display the **Firmware Upgrade** page.
2. Click **Select File** to select a firmware file for the IG502.
3. Click **Starting Upgrade** and **OK** to start the firmware upgrade.
4. Wait until the upgrade succeeds, and then click **Reboot** to restart the IG502.

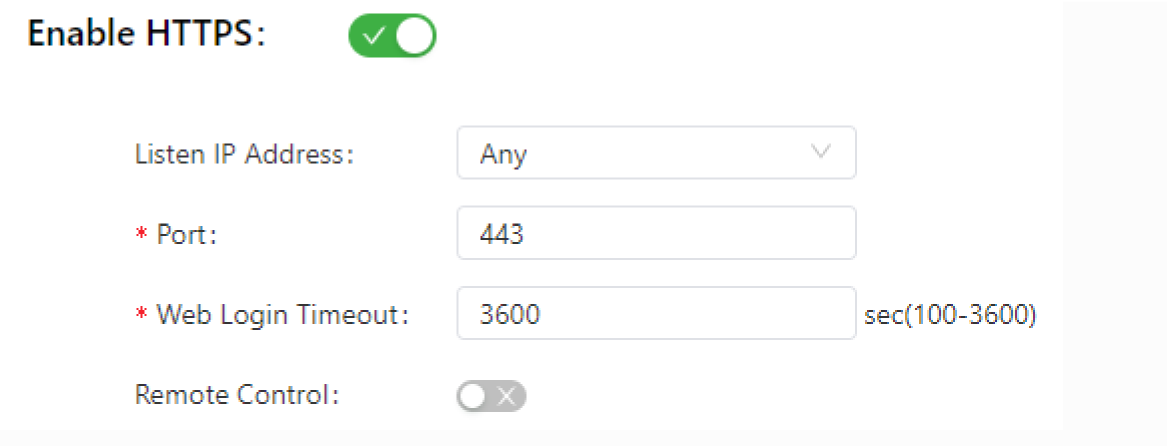
4.7.6. Access Tools

To facilitate IG502 management and configuration, you can configure the IG502 management and access methods on the **Access Tools** page. Follow these steps to complete the configuration:

- Configure HTTPS
    1. Choose **System > Access Tools** to display the **Access Tools** page.
    2. Select **Enable HTTPS** and set the parameters. For details about these parameters, see HTTPS parameter description.
    3. Click **Submit** to apply the configuration.
- Configure Telnet
    1. Choose **System > Access Tools** to display the **Access Tools** page.
    2. Select **Enable TELNET** and set the parameters. For details about these parameters, see Telnet parameter description.
    3. Click **Submit** to apply the configuration.
- Configure SSH
    1. Choose **System > Access Tools** to display the **Access Tools** page.

2. Select **Enable SSH** and set the parameters. For details about these parameters, see SSH parameter description.
3. Click **Submit** to apply the configuration.

The following figure shows the configuration of HTTPS-based management.



Enable HTTPS: ✓

Listen IP Address: Any

* Port: 443

* Web Login Timeout: 3600 sec(100-3600)

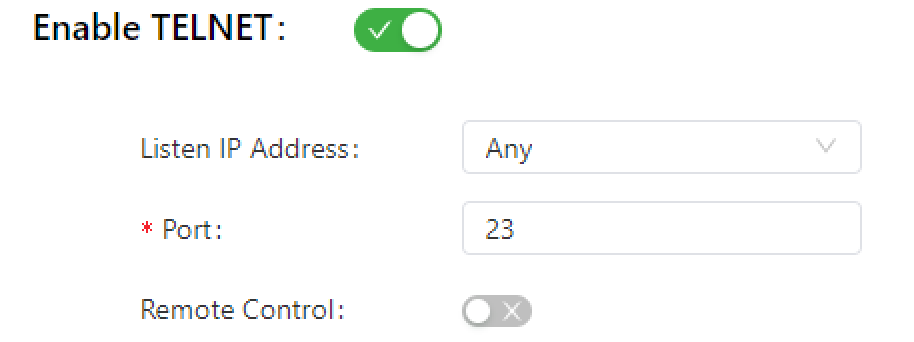
Remote Control: ✕

The HTTPS parameters are described as follows:

1. Listen IP Address: specifies the listening IP address. Options include Any, 127.0.0.1, and other IP addresses.
2. Port: specifies the listening port number of HTTPS.
3. Web Login Timeout: specifies the timeout period of web page login. The valid value range is 0-3600.

4. Remote Control: enables or disables remote access to the IG502 through HTTPS. If no remote control network is specified, the IG502 can be remotely controlled through any network.

The following figure shows the configuration of Telnet-based management.



Enable TELNET: ✓

Listen IP Address: Any

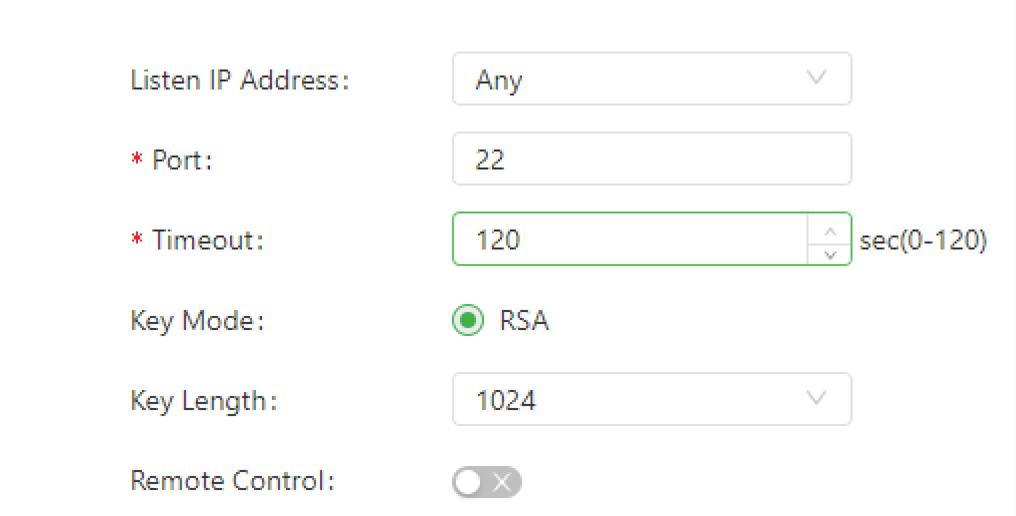
* Port: 23

Remote Control: ✗

The Telnet parameters are described as follows:

1. Listen IP Address: specifies the listening IP address. Options include Any, 127.0.0.1, and other IP addresses.
2. Port: specifies the listening port number of Telnet.
3. Remote Control: enables or disables remote access to the IG502 through Telnet. If no remote control network is specified, the IG502 can be remotely controlled through any network.

The following figure shows the configuration of SSH-based management.



Listen IP Address: Any

* Port: 22

* Timeout: 120 sec(0-120)

Key Mode: ● RSA

Key Length: 1024

Remote Control: ○

The SSH parameters are described as follows:

1. Listen IP Address: specifies the listening IP address. Options include Any, 127.0.0.1, and other IP addresses.
2. Port: specifies the listening port number of SSH.
3. Timeout: specifies the SSH timeout period. The valid value range is 0-120.
4. Key Mode: fixed as RSA.
5. Key Length: specifies the length of the key used. Options are 512, 1024, 2048, and 4096.
6. Remote Control: enables or disables remote access to the IG502 through Telnet. If no remote control network is specified, the IG502 can be remotely controlled through any network.

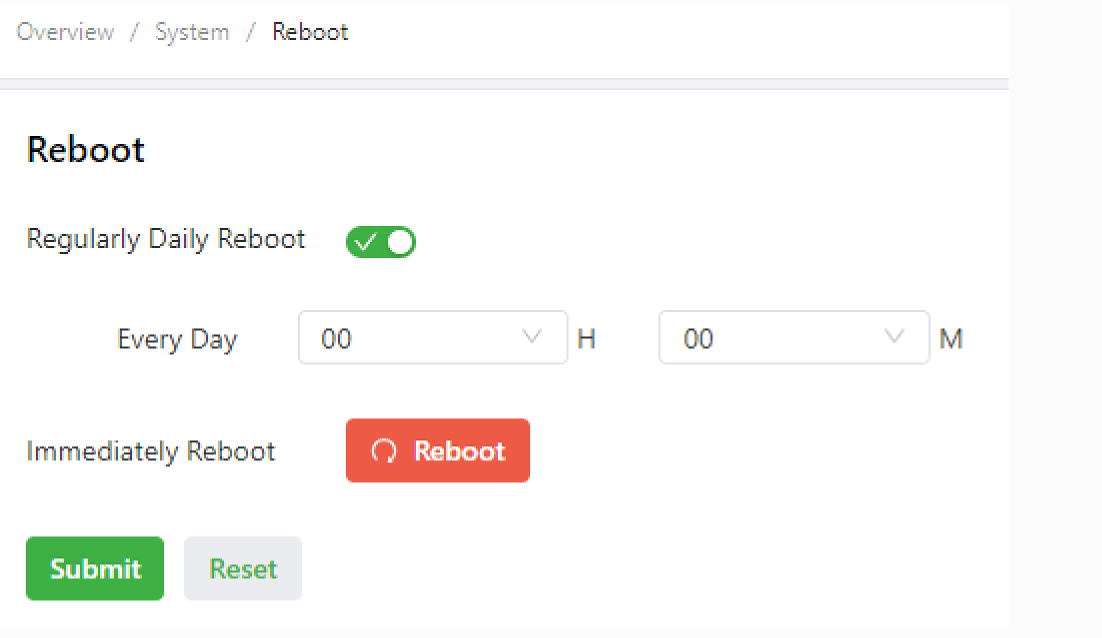
4.7.7. User Management

On the **User Management** page, you can add user accounts and manage the password and access rights of each account. These accounts allow multiple users to access and manage the IG502. Follow these steps to add a user:

1. Choose **System > User Management** to display the **User Management** page.
2. Click the **Add** icon to add a user.
3. Set the parameters.
4. Click **OK** to save the configuration.

4.7.8. Reboot

Choose **System > Reboot** to display the **Reboot** page, and then reboot the IG502 or set a scheduled reboot plan for it.As shown in the following figure, the IG502 is configured to reboot on 0:00 every day.



Overview / System / Reboot

Reboot

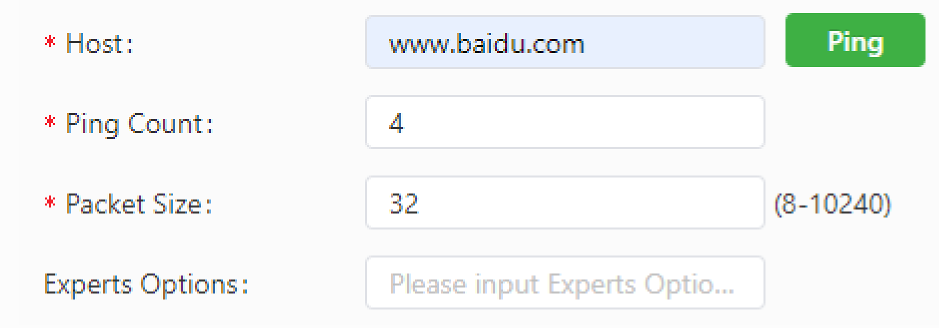
Regularly Daily Reboot: ✓ (on)

Every Day: 00 H 00 M

Immediately Reboot: Reboot

4.7.9. Network Tools

Choose **System > Network Tools** to display the **Network Tools** page. You can diagnose network problems of the IG502 on this page. You can enter some extension options in the Expert Options area. For example, expert option -t for the ping tool enables the IG502 to ping a specified host continuously until you stop the ping.The ping tool can be used to check whether a network is reachable. The following figure shows the configuration of a ping test.



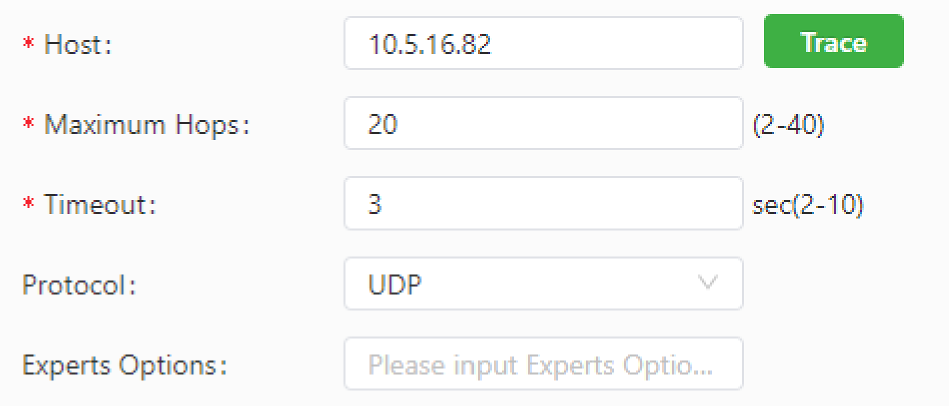
* Host: www.baidu.com

* Ping Count: 4

* Packet Size: 32 (8-10240)

Experts Options: Please input Experts Optio...

The traceroute tool can be used to determine the route used to transmit IP datagrams to a destination. The following figure shows the configuration of a traceroute test.



* Host: 10.5.16.82

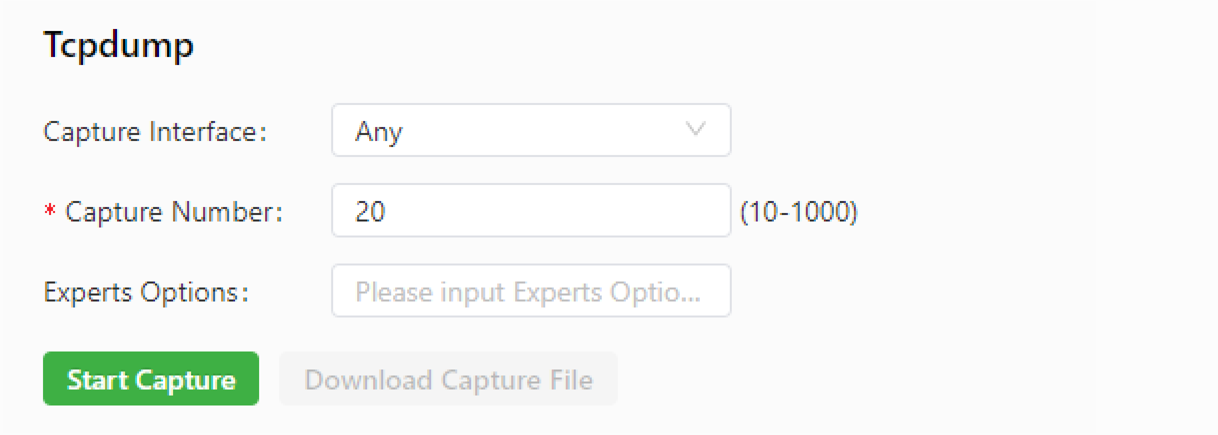
* Maximum Hops: 20 (2-40)

* Timeout: 3 sec(2-10)

Protocol: UDP

Experts Options: Please input Experts Optio...

The Tcpdump tool can be used to capture packets transmitted on a specified interface. The following figure shows the Tcpdump configuration.



Tcpdump

Capture Interface: Any

* Capture Number: 20 (10-1000)

Experts Options: Please input Experts Optio...

4.7.10. 3rd Party Notification

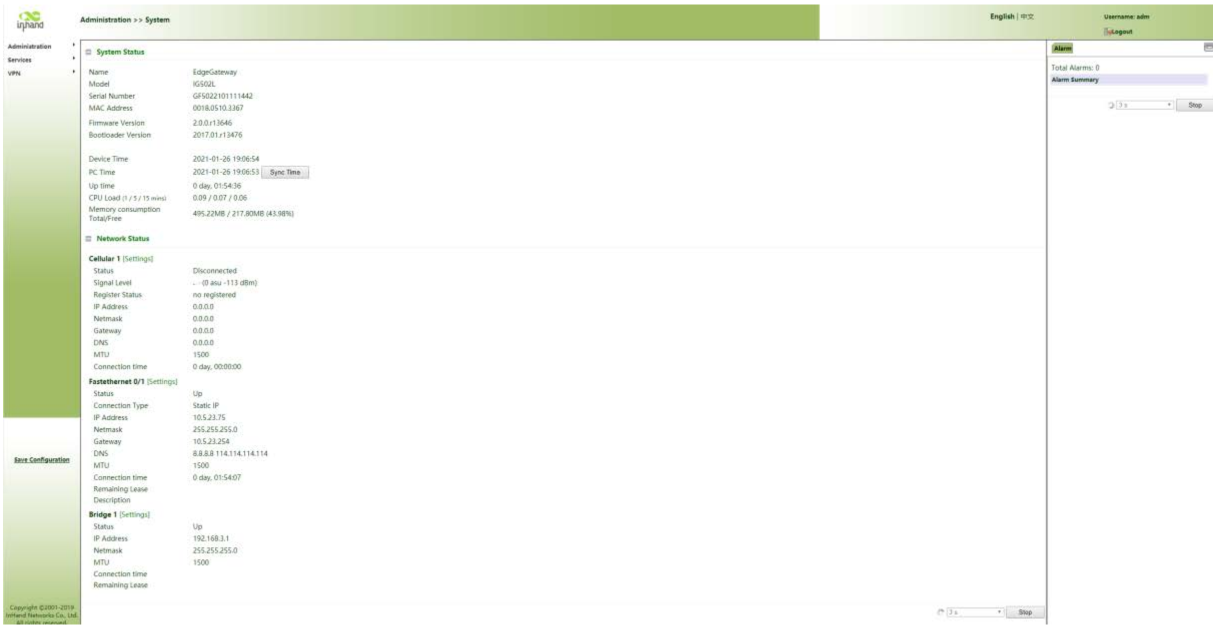
Choose **System** > **3rd Party Notification** to display the **3rd Party Notification** page. You can view the statement about the third-party software used for the IG502.

4.8. Advanced

4.8.1. Administration

4.8.1.1 System

On this page, you can view the system status and network status (including the firmware version, MAC address, system time, and start time of the gateway), specify the language of the web pages, and set a host name for the gateway.



System Status

Name EdgeGateway
Model IG502L
Serial Number GF5022101111442
MAC Address 0018.0510.3367
Firmware Version 2.0.0.r13646
Bootloader Version 2017.01.r13476
Device Time 2021-01-26 19:06:54
PC Time 2021-01-26 19:06:53
Up time 0 day, 01:54:36
CPU Load (1 / 5 / 15 mins) 0.09 / 0.07 / 0.06
Memory consumption Total/Free 495.22MB / 217.80MB (43.98%)

Network Status

Cellular 1 [Settings]
Status Disconnected
Signal Level (0 asu -113 dBm)
Register Status no registered
IP Address 0.0.0.0
Netmask 0.0.0.0
Gateway 0.0.0.0
DNS 0.0.0.0
MTU 1500
Connection time 0 day, 00:00:00

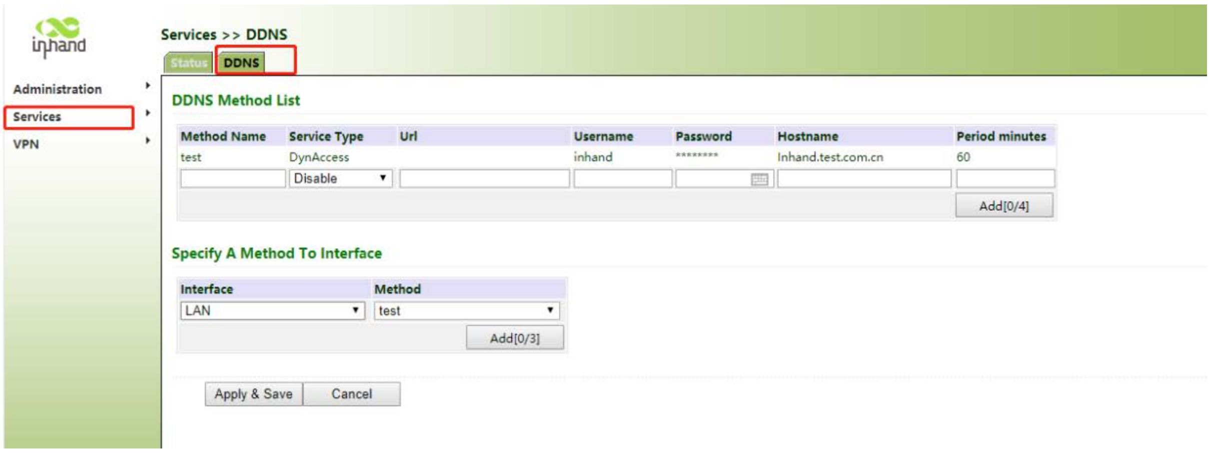
Fastethernet 0/1 [Settings]
Status Up
Connection Type Static IP
IP Address 10.5.23.75
Netmask 255.255.255.0
Gateway 10.5.23.254
DNS 8.8.8.8 114.114.114.114
MTU 1500
Connection time 0 day, 01:54:07
Remaining Lease
Description

Bridge 1 [Settings]
Status Up
IP Address 192.168.3.1
Netmask 255.255.255.0
MTU 1500
Connection time
Remaining Lease

Total Alarms: 0
3 s

4.8.2. Services

4.8.2.1. DDNS



DDNS Method List

Method Name	Service Type	Url	Username	Password	Hostname	Period minutes
test	DynAccess		inhand	********	Inhand.test.com.cn	60
	Disable					

Specify A Method To Interface

Interface	Method
LAN	test

The DDNS parameters are described as follows:

Method Name : specifies the name

Service Type: specifies the type of the software Dynamic Domain Name Service Disable

- DynAccess

- QDNS(3322)-Dynamic
- QDNS(3322)-Static
- DynDNS-Dynamic
- DynDNS-Static

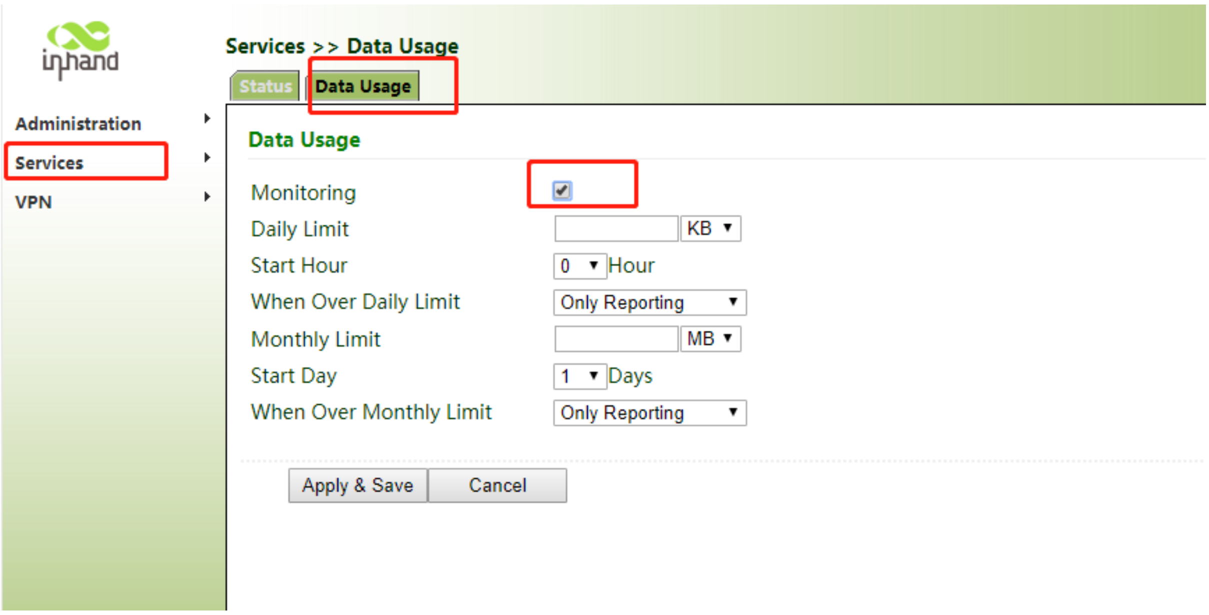
Url : the address of a web page on the world wide web

Username : Registered username for DDNS

Password : Registered password for DDNS

Hostname : Registered hostname for DDNS

4.8.2.2. Data Usage



Data Usage

Monitoring	☑
Daily Limit	KB
Start Hour	0 Hour
When Over Daily Limit	Only Reporting
Monthly Limit	MB
Start Day	1 Days
When Over Monthly Limit	Only Reporting

Monitoring: enables the monitoring usage

Daily Limit: specifies the maximum daily flow , which is expressed in KB/MB/GM.

Start Hour: 0~23

When Over Daily Limit: which can be Only Reporting or Stop Forward or Shutdown Interface

Monthly Limit: specifies the maximum monthly flow , which is expressed in MB/GM.

Start Day:1~31

When Over Monthly Limit : which can be Only Reporting or Stop Forward or Shutdown Interface

4.8.3. VPN

4.8.3.1. IPsec

IPsec is a group of open network security protocols formulated by the IETF, which provide data source authentication, data encryption, data integrity check, and anti-replay on the IP layer to ensure the security of data transmission over the Internet. IPsec lowers the risk of data leakage and interception, ensures data integrity and confidentiality, and protects security of service data transmission.

The IPsec parameters are described as follows:

- IKEv1 Policy
  - ID: specifies the ID of an IKEv1 policy.
  - Encryption: specifies the algorithm used to encrypt plain text. Options are 3DES, DES, AES128, AES192, and AES256.
  - 3DES: uses three 64-bit DES keys to encrypt plain text.
  - DES: uses a 64-bit key to encrypt a 64-bit plain-text block.
  - AES: uses a 128-bit, 192-bit, or 256-bit key to encrypt plain text.
  - Hash: specifies the hash algorithm used in the policy. Options are MD5, SHA1, SHA2-256, SHA2-384, and SHA2-512.
  - MD5: generates a 128-bit message digest for a message of any length.

- SHA1: generates a 160-bit message digest for a message of a length less than 128 bits.
- SHA2-256: generates a 256-bit message digest.
- SHA2-384: generates a 384-bit message digest.
- SHA2-512: generates a 512-bit message digest.

- Diffie-Hellman Group: specifies the Diffie-Hellman algorithm, an open key algorithm. Two parties calculate a shared key based on the data exchanged between them, without transmitting the key to each other. To encrypt data sent to each other, the two parties must have a shared key. The essence of Internet Key Exchange (IKE) is that the communication parties never transmit the key over an insecure network. Instead, they exchange a series of data to calculate a shared key. Other parties (such as hackers) cannot calculate the key even if they intercept all the data exchanged for key calculation.
- Lifetime: specifies the lifetime of the IKE security association (SA). The two parties negotiate another SA to replace the old one before the lifetime expires.

- IKEv2 Policy
  - ID: specifies the ID of an IKEv2 policy.
  - Encryption: specifies the algorithm used to encrypt plain text. Options are 3DES, DES, AES128, AES192, and AES256.
    - 3DES: uses three 64-bit DES keys to encrypt plain text.
    - DES: uses a 64-bit key to encrypt a 64-bit plain-text block.
    - AES: uses a 128-bit, 192-bit, or 256-bit key to encrypt plain text.
  - Integrity: specifies the algorithm used to check data integrity. Options are MD5, SHA1, SHA2-256, SHA2-384, and SHA2-512.
    - MD5: generates a 128-bit message digest for a message of any length.
    - SHA1: generates a 160-bit message digest for a message of a length less than 128 bits.
    - SHA2-256: generates a 256-bit message digest.
    - SHA2-384: generates a 384-bit message digest.
    - SHA2-512: generates a 512-bit message digest.
  - Diffie-Hellman Group: specifies the Diffie-Hellman algorithm, an open key algorithm. Two parties calculate a shared key based on the data exchanged between them, without transmitting the key to each other. To encrypt data sent to each other, the two parties must have a shared key. The essence of IKE is that the communication parties never transmit the key over an insecure network. Instead, they exchange a series of data to

calculate a shared key. Other parties (such as hackers) cannot calculate the key even if they intercept all the data exchanged for key calculation.

  - Lifetime: specifies the lifetime of the IKE SA. The two parties negotiate another SA to replace the old one before the lifetime expires.

- IPsec Policy
  - Name: specifies the name of the IPsec policy. This parameter cannot be changed after the IPsec policy is configured successfully.
  - Encapsulation: specifies the encapsulation protocol used for IP packets. The Authentication Header (AH) protocol defines an authentication method to authenticate data sources and ensure data integrity. The Encapsulating Security Payload (ESP) protocol defines encryption and authentication (optional) methods to ensure data reliability.
    - AH: provides data source authentication, data integrity check, and packet anti-replay. The sender uses a hash algorithm to calculate a digest field for an IP packet based on the fixed fields in the IP header and the IP payload. The receiver calculates the digest for the received IP packet and compares it with the digest field carried in the packet to determine whether the packet has been tampered with during transmission on the network.
    - ESP: provides all functions of the AH protocol and encrypts payload of IP packets. The ESP protocol can protect data in IP headers of IP packets.
  - Authentication: specifies the algorithm used for authentication. Options are MD5, SHA1, SHA2-256, SHA2-384, and SHA2-512.
    - MD5: generates a 128-bit message digest for a message of any length.
    - SHA1: generates a 160-bit message digest for a message of a length less than 128 bits.
    - SHA2-256: generates a 256-bit message digest.
    - SHA2-384: generates a 384-bit message digest.
    - SHA2-512: generates a 512-bit message digest.
  - IPsec Mode: specifies the IPsec encapsulation mode.
    - Tunnel Mode: adds an IPsec header (AH or ESP) outside the original IP header and adds a new IP header at the outermost layer. Then, the original IP packet is protected by IPsec as a part of payload. The tunnel mode is generally used between two security gateways. The packets encrypted by one security gateway can only be decrypted by the peer security gateway.

- Transport Mode: inserts an IPsec header (AH or ESP) between the IP header and upper-layer protocol header. This mode retains the original IP header but changes the IP protocol field to AH or ESP, and calculates a new checksum for the IP header. The transport mode is applicable to communication between two hosts or between a host and a security gateway.

- IPsec Tunnels
    - Basic Parameters
        - Destination Address: specifies the IP address or domain name of the IKE peer. (Set this parameter to 0.0.0.0 when the IG902 acts as a server.)
        - Map Interface: specifies the interface to which the IPsec policy is applied.
        - IKE Version: specifies the version of the IKE protocol. Options are IKEv1 and IKEv2.
        - IKEv1 Policy: specifies a policy ID defined in the IKEv1 policy list.
        - IKEv2 Policy: specifies a policy ID defined in the IKEv2 policy list.
        - IPsec Policy: specifies a policy ID defined in the IPsec policy list.
            - Authentication Type: specifies the authentication method used for the IPsec tunnel. Shared key authentication and digital certificate authentication are supported.
                - Shared Key: specifies the shared key used for authentication.

- Digital Certificate: specifies the digital certificate used for authentication. You need to import a valid certificate on the certificate management page.
- ▪ Negotiation Mode: specifies the mode of IKEv1 negotiation.
- Main Mode: separates key exchange information from the identity information. This mode protects identity information to enhance the security.
- Aggressive Mode: does not provide identity authentication but meets requirements of some special network environments. The aggressive mode can be used when the address of the tunnel initiator cannot be obtained in advance or keeps changing, but both parties want to establish an IKE SA by using a pre-shared key.
- ▪ Local Subnet: specifies the source network of the interested flow defined for the IPsec tunnel.
- ▪ Remote Subnet: specifies the destination network of the interested flow defined for the IPsec tunnel.

- IKE Advance (Phase 1)
  - Local ID: specifies the type of the local device’s identifier for IKE negotiation.
    - IP Address: specifies the peer IP address used to establish the IPsec interface.
    - FQDN: specifies the character string used as the identifier of the local device.
    - User FQDN: specifies the fully qualified domain name used as the identifier of the local device.
  - Remote ID: specifies the type of the peer device’s identifier for IKE negotiation.
    - IP Address: specifies the interface IP address that the local device uses to complete IKE negotiation and exchange identity information with the peer device.
    - FQDN: specifies the identifier string that the peer devices used for IKE negotiation. The value must be the same as that set on the peer device.
    - User FQDN: specifies the fully qualified domain name used as the identifier of the peer device. The value must be the same as that set on the peer device.
  - IKE Keepalive (DPD): enables or disables dead peer detection (DPD).
    - DPD Timeout: specifies the timeout period of a DPD probe. After the receiving end triggers a DPD probe by sending a DPD request to the peer, it waits for a DPD response. If no DPD response is received from the peer, it deletes the IPsec SA. The valid value range is 10-3600, and the unit is second.
    - DPD Interval: specifies the IPsec neighbor detection interval. After DPD is enabled, the receiving end can trigger a DPD probe if it does not receive any IPsec-encrypted packets from the peer within the DPD interval. In this case, the receiving end sends a DPD request to check whether the IKE peer is available. The valid value range is 10-3600, and the unit is second.
  - XAUTH: specifies the XAUTH user name and password.
- IPsec Advance (Phase 2)
  - PFS: enables or disables Perfect Forward Secrecy (PFS), a feature that ensures security of other keys when a key is encrypted, because these keys are not derived from one another. The key used in phase-2 IPsec negotiation is derived from the key generated in phase 1. If the phase -1 key for IKE negotiation is intercepted by an attacker, the attacker may collect sufficient information to derive the phase-2 key for IPsec SA negotiation. The PFS feature prevents this problem by performing an additional DH exchange, ensuring security of the phase-2 key.

- IPsec SA Lifetime: specifies the duration in which the IPsec SA is alive. When the two ends perform IPsec negotiation to establish an SA, the smaller value between the lifetime values set on the local and peer devices takes effect.
- IPsec SA Idletime: specifies the maximum idle duration of an IPsec SA. If no data is transmitted within this duration after the IPsec SA is established, the IPsec SA becomes invalid. When the current IPsec SA is about to expire, IPsec negotiation is triggered to establish a new SA, so that the new SA is ready before the old SA becomes invalid.

- Tunnel Advance
- Tunnel Start Mode: specifies how the IPsec tunnel is initiated.
- Automatically: indicates that the local device completes IKE negotiation automatically to set up an IPsec tunnel after the IPsec policy is applied. This mode is often used on a client.
- Respond Only: indicates that local device only receives IPsec requests and does not initiate a connection. This mode is often used on a server.
  - On-demand: indicates that the local device completes IKE negotiation to set up an IPsec tunnel only when detecting IPsec packets on the interface.
- Local/Remote Send Cert Mode: specifies when to send the certificate. Options are Send cert always, Send cert on request, and Not send cert.
- Send cert always: Some IPsec services do not send certificate requests but need to receive the certificate from the peer because they do not save the certificate. For these IPsec services, you must select this option on the peer to enable the IPsec tunnel to be established.
- Send cert on request: The local device sends the certificate to the peer only when receiving a request from the peer.
- Not send cert: The local device sends the certificate to the peer regardless of whether the peer sends a request.
- ICMP Detect
- ICMP Detection Server: specifies the address of the peer host to be detected.
- ICMP Detection Local IP: specifies the source address of the traffic to be protected by IPsec.
- ICMP Detection Interval: specifies the interval between ICMP probe packets sent from the local device.

- ICMP Detection Timeout: specifies the timeout period of an ICMP probe. If the local device does not receive any ICMP Reply packet within this period, it considers that the ICMP probe times out.
- ICMP Detection Max Retries: specifies the maximum number of retries after an ICMP probe failure. (The local device restarts the IPsec service when the number of retries reaches this value.)

4.8.3.2. GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets of any network-layer protocol with another network-layer protocol. GRE can be used as a Layer 3 tunneling protocol to provide a transparent transmission channel for VPN data. To put it simply, GRE is a tunneling technology that provides a channel to transmit encapsulated data packets. Data packets are encapsulated on one end of the tunnel and decapsulated on the other end.The GRE parameters are described as follows:

- Enable: enables or disables GRE.
- Index: specifies a GRE tunnel ID. The valid range is 1-100.
- Network Type: specifies the GRE network type.
- Local Virtual IP: specifies the virtual IP address of the local device.
- Peer Virtual IP: specifies the virtual IP address of the peer device. If the network type is set to subnet, enter a subnet mask in this field.
- Source Type: specifies the type of the source address. It can be an IP address or interface name.
- Local Interface: specifies the source interface of the GRE tunnel.
- Local IP: specifies the source IP address of the GRE tunnel.
- Peer IP: specifies the destination address of the GRE tunnel.
- Key: specifies the authentication key of the GRE tunnel. The same key must be set on both ends of the tunnel.
- MTU: specifies the maximum transmit unit allowed on the GRE tunnel, which is expressed in bytes.
- NHRP Enable: enables or disables the Next Hop Resolution Protocol (NHRP). This protocol is used by a source station (host or router) connected to a non-broadcast

  multiple access (NBMA) subnet to determine the next-hop IP address and NBMA subnet address toward the destination station.
    - NHS IP Address: specifies the next-hop server address.
    - Authentication Key: specifies the NHRP authentication key.
    - Hold Time: The valid value range is 1-65535.
    - Purge Forbid: disables or enables transmission of NHRP Purge messages.
- IPsec Profile: enables or disables the IPsec profile. It is used together with IPsec extensions.
- Description: specifies the description of the GRE tunnel.

: **Note**

- NHRP is applicable only to dynamic multipoint virtual private networks (DMVPNs) and does not need to be enabled for GRE.
- GRE is usually used when both ends use a fixed public IP address.

4.8.3.3. OpenVPN

In the OpenVPN architecture, when a user accesses a remote virtual address (an address of a virtual NIC, not a real address), the operating system uses the routing mechanism to send the datagrams (TUN mode) or data frames (TAP mode) to the virtual NIC. When the service program receives the data, it processes the data and sends the data to the external network through the socket. When the remote service program receives the data from the external network through its socket, it processes the data and sends the data to the virtual NIC. The application software then receives the data. At this time, a unidirectional transmission process is completed. The reverse transmission process is similar.

OpenVPN Client

The parameters of an OpenVPN client are described as follows:

- Enable: enables or disables the OpenVPN client.
- Index: specifies a tunnel ID.
- OpenVPN Server: specifies the IP address or domain name of an OpenVPN server.
- Port: specifies the port number used to establish an OpenVPN tunnel.
- Protocol Type: specifies the protocol used for data transmission. Options are UDP and TCP.
- Authentication Type: Select an authentication type and set parameters for the authentication type.
- Description: specifies the description of the OpenVPN tunnel.
- Show Advanced Options

- Source Interface: specifies the interface used to establish the OpenVPN tunnel.
- Interface Type: specifies the type of data sent from the interface.
    - Tun: mostly used for IP-based communication.
    - Tap: allows complete Ethernet frames to pass through the OpenVPN tunnel and provides support for non-IP protocols.

- Network Type: Options are net30, p2p, and subnet.
    - net30: Four IP addresses with a 30-bit mask are selected from the IP address pool. The larger one between the two intermediate IP addresses is used as the IP address of the client’ s virtual NIC, and the smaller one is used as the peer IP address.
    - p2p: An IP address is selected from the IP address pool as the IP address of the client’ s virtual NIC, and the actual IP address of the virtual NIC is used as the peer IP address.
    - subnet: An IP address is selected from the IP address pool as the IP address of the client’ s virtual NIC, and the

subnet mask of the virtual NIC is used as the peer IP address.

- Cipher: specifies the protocol used to encrypt the data transmitted over the OpenVPN tunnel. The setting must be the same on the client and server.
- HMAC: specifies the authentication method used for data transmitted over the OpenVPN tunnel. Data cannot be transmitted if the authentication fails. The setting must be the same on the client and server.
- Compression LZO: specifies the compression format of data transmitted over the OpenVPN tunnel.
- Redirect-Gateway: enables the OpenVPN interface to act as the default gateway for the client, so that all traffic of the client is forwarded through the OpenVPN interface.
- Remote Float: allows the remote device to change its IP address or port.
- Link Detection Interval: specifies the interval for sending link detection packets after an OpenVPN tunnel is established. The valid value range is 10-1800, and the unit is second.

- Link Detection Timeout: specifies the timeout period of OpenVPN link detection. After the number of link detection failures reaches the maximum value, the local device initiates a new L2TP connection. The valid value range is 60-3600.
- MTU: specifies the maximum transmit unit on the OpenVPN interface, which is expressed in bytes.
- Enable Debug: enables or disables debugging logs.
- Expert Configuration: specifies OpenVPN extension parameters.
- Import Configuration: Select the OpenVPN configuration file you want to import.

OpenVPN Server

The parameters of an OpenVPN server are described as follows:

- Enable: enables or disables the OpenVPN server.
- Config Mode: specifies whether to complete the configuration manually or import a configuration file.
  - Manual Config
    - Authentication Type: specifies the authentication method used.

  - ◆ Local IP Address: specifies the virtual IP address of the OpenVPN server interface.
  - ◆ Remote IP Address: specifies the virtual IP address of the OpenVPN client.
  - ◆ Description: specifies the description of the OpenVPN tunnel.

Show Advanced Options: enables or disables display of advanced options.

- Source Interface: specifies the interface used to establish the OpenVPN tunnel.
- Interface Type: specifies the type of data sent from the interface.
  - ✓ Tun: mostly used for IP-based communication.
  - ✓ Tap: allows complete Ethernet frames to pass through the OpenVPN tunnel and provides support for non-IP protocols.
- Network Type: Options are net30, p2p, and subnet.
- Protocol Type: specifies the communication protocol used between the client and server. The setting must be the same on the client and server.
- Port: specifies the port number of the OpenVPN service.

- Cipher: specifies the protocol used to encrypt the data transmitted over the OpenVPN tunnel. The setting must be the same on the client and server.
- HMAC: specifies the authentication method used for data transmitted over the OpenVPN tunnel. Data cannot be transmitted if the authentication fails. The setting must be the same on the client and server.

- Compression LZO: specifies the compression format of data transmitted over the OpenVPN tunnel. The setting must be the same as that on the client.
- Link Detection Interval: specifies the interval for sending link detection packets after an OpenVPN tunnel is established. The valid value range is 10-1800, and the unit is second.
- Link Detection Timeout: specifies the timeout period of OpenVPN link detection. If the local device does not receive a response to the link detection packet within this period, link detection fails. The valid value range is 60-3600.
- MTU: specifies the maximum transmit unit on the OpenVPN interface, which is expressed in bytes.

- Enable Debug: enables or disables debugging logs.
- Expert Configuration: specifies OpenVPN extension parameters.
- Username/Password: specifies the user name and password used for server access when password authentication is used.

4.8.3.4. Certificate Management

The Simple Certificate Enrollment Protocol (SCEP) is a certificate management protocol formulated jointly by Cisco and Verisign. This protocol combines PKCS#7 and PKCS#10 standards, and supports extensive clients and certification authorities (CAs).The certification management parameters are described as follows:

- Enable SCEP: enables or disables the Simple Certificate Enrollment Protocol.
- Force to re-enroll: restarts the certificate enrollment service every time without checking the status of the current certificate.
- Status: displays the current certificate enrollment status on the device, which can be Initiation, Enrolling, Re-Enrolling, or Complete.
- Protect Key: specifies the key set during certificate enrollment for encryption of the digital certificate. You can import or export a certificate only after entering the protection key set during certificate enrollment.

- Protect Key Confirm: Enter the protection key again to confirm the key.
- Strict CA: sets the ID of a trusted CA. The certificate of a device is enrolled and issued by a trusted CA. Therefore, you must specify the ID of a trusted CA to bind the device to the CA. Then, the device completes certificate application, acquisition, revocation, and query through this CA.
- Server URL: specifies the URL of the CA server. You must specify a CA server URL beforehand, so that the device can apply to this server for a certificate through SCEP, for example, http://100.17.145.158:8080/certsrv/mscep/mscep.dll.
- Common Name: specifies the general name of the certificate required.
- FQDN: specifies the fully qualified domain name (FQDN) of the certificate. FQDN is the unique identifier of an entity on a network and is composed of a host name and a domain name. It can be resolved into an IP address. For example, host name www and domain name whatever.com form an FQDN www.whatever.com.
- Unit 1: specifies the name of the first organization of the certificate.
- Unit 2: specifies the name of the second organization of the certificate.
- Domain: specifies the qualified domain name of the certificate.
- Serial Number: specifies the serial number of the certificate.

- Challenge: specifies the challenge code of the certificate, which is required for certificate revocation (optional).
- Challenge Confirm: Enter the challenge code again to confirm the setting.
- Unstructured address: specifies the IP address of the certificate.
- RSA Key Length: specifies the length of the RSA key. The valid value range is 128-2048, and the unit is bit.
- Poll Interval: specifies the interval at which the device queries the current certificate status from the server. The valid value range is 30-3600, and the unit is second.
- Poll Timeout: specifies the maximum duration for querying the certificate status. The device considers the certificate application fails when the timeout period expires. The valid value range is 30-86400, and the unit is second.
- Revocation: enables or disables certificate revocation.
    - CRL URL: specifies the URL of the certificate revocation list (CRL) distribution point.
    - OCSP URL: specifies the URL of the Online Certificate Status Protocol (OCSP) server. Generally, it is the same as the URL of the CA server.

Note: When using a certificate, ensure that the system time is consistent with the actual time.

5. FAQ

How Do I Restore Factory Settings Through Hardware?

Follow these steps:

1. Find the RESET button on the operation panel.
2. Hold down the RESET button within 10s after the device is powered on.
3. When the ERR indicator turns red, release the RESET button.
4. After a few seconds, when the ERR indicator turns off, hold down the RESET button again.
5. When you see the ERR indicator blink, release the RESET button. After a while, the ERR indicator turns off, the factory settings of the device have been restored.