Building IoT Gateway

EG71

Administrator Guide

14 rue Edouard Petit
42000 St-Etienne

Tel : +33 477 92 03 56
Email : contact@rg2i.com

www.rg2i.com

Contents

Chapter 1. About This Guide 4

Chapter 2. Product Introduction 6

Chapter 3. Getting Started 7

Chapter 4. Status 13

Chapter 5. Data Service 22

Data Acquisition 22

Device 22

IO Device 36

Device Access Network 41

LoRaWAN 47

Data Forwarding 56

Device Library 67

Data Stream 76

Chapter 6. Network 78

Interface 78

Ethernet 78

Cellular 84

WLAN 88

LoRa 92

RS485 96

Loopback 97

Firewall 98

DDNS 104

Link Failover 105

VPN 108

Chapter 7. Platform Management 124

Chapter 8. System 125

General....125
User....127
Service....129
Maintenance....133
Log....138
SNMP....140
Event....145
Chapter 9. APP....147
Python....147
Node-RED....149
Docker....152
Chapter 10. Services....154

Chapter 1. About This Guide

This guide describes the steps and details for configuring and operating the gateway's web GUI.

Readers

This guide is for administrators who need to prepare for, configure, and operate the building management system. We begin by assuming that you are familiar with networking and other IT disciplines.

Copyright Statement

This guide may not be reproduced in any form or by any means to create any derivative such as translation, transformation, or adaptation without the prior written permission of Xiamen Milesight IoT Co., Ltd (Hereinafter referred to as Milesight).

Milesight reserves the right to change this guide and the specifications without prior notice. The latest specifications and user documentation for all Milesight products are available on our official website http://www.milesight.com

Safety Instruction

These instructions are intended to ensure that users can use the product correctly to avoid danger or property loss. Milesight will not take responsibility for any loss or damage resulting from failure to follow the instructions in this operating guide.

Warning:
Serious injury or death may be caused if any of these warnings is neglected.

- This installation must be conducted by a qualified service person and should strictly comply with the electrical safety regulations of the local region.
- To avoid the risk of fire and electric shock, keep the product away from rain and moisture before installation.
- The bottom of the device becomes extremely hot during operation. Do not touch it !
- Do not power the device or connect it to other electrical devices during installation.
- Do not connect or power the device using damaged cables.
- Make sure the plug is firmly inserted into the power socket.
- Make sure the device is firmly fixed when installing.

CAUTION:

Injury or equipment damage may be caused if any of these cautions are neglected.

- The device is intended only for indoor use.
- The device must not be disassembled or remodeled in any way.
- Do not place the device close to objects with naked flames.
- Do not place the device where the temperature is below/above the operating range.
- Do not drop the device or subject it to physical shock.
- To prevent heat accumulation, do not block air circulation around the device.

Revision History

Release Date	Version	Description
Jan. 16, 2026	V1.0	Initial version
March 31, 2026	V1.1	1. Adjust the layouts and names for LoRaWAN features under Data Acquisition and tabs under Interface menus. 2. The minimum collection interval for Modbus and BACnet objects is adjusted to 1s. 3. Merge global objects into Metadata of HTTP/MQTT data forwarding rules, and remove the Device page from Object configuration page. 4. Update layout for MQTT forwarding configuration page. 5. Add wildcards for MQTT Uplink Data topics. 6. HTTPS access is enabled by default, and HTTP access is disabled. 7. The password change prompt will pop up when login the web GUI for the first time. 8. Web password must contain at least one letter and one number. 9. Add Force HTTPS Redirection option. 10. Equips with docker.

Chapter 2. Product Introduction

EG71 is an intelligent and powerful edge IoT gateway designed for smart building applications. Supporting both wired and wireless connectivity, the EG71 enables seamless data aggregation from various field devices and ensures fast, plug-and-play BMS deployment. It bridges field-level sensors and actuators with cloud platforms or BMS systems, delivering reliable data processing, local automation, and remote management in a compact form factor.

It is ideal for building automation, energy management, HVAC control, and other IoT applications in commercial buildings, campuses, hotels, and industrial facilities.

The gateway has the following features:

- A quad-core industrial-grade processor with large memory ensures stable performance for large-scale device connectivity and edge processing
- Comprehensive I/O interfaces with native support for RS485, KNX, M-BUS (UnderDevelopment), LoRaWAN®, Wi-Fi, and Ethernet devices
- Equipped with NFC for quick addition for add Milesight devices
- Multiple backhaul options including Ethernet, cellular (4G) and Wi-Fi for reliable network redundancy
- Supports mainstream protocols such as Modbus, BACnet, MQTT, and HTTP for seamless integration with third-party hardware or software
- Provides secondary development capabilities (Python SDK, Node-RED and docker) to build customized BMS systems
- Enables security communication with multiple VPN tunnels and firewall rules
- Enables centralized and simplified remote device management via Milesight Development Platform

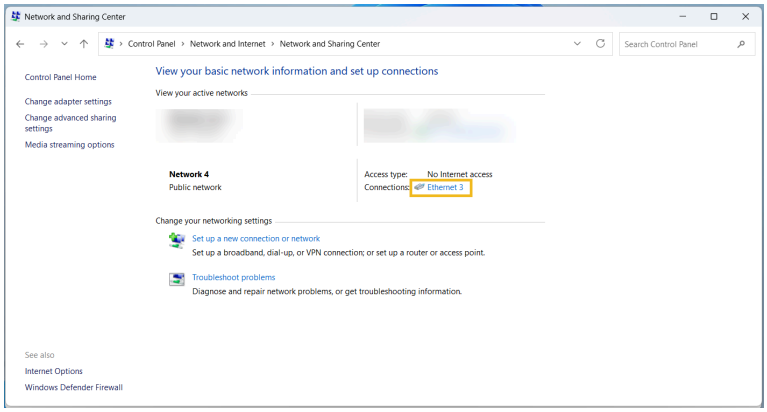
Chapter 3. Getting Started

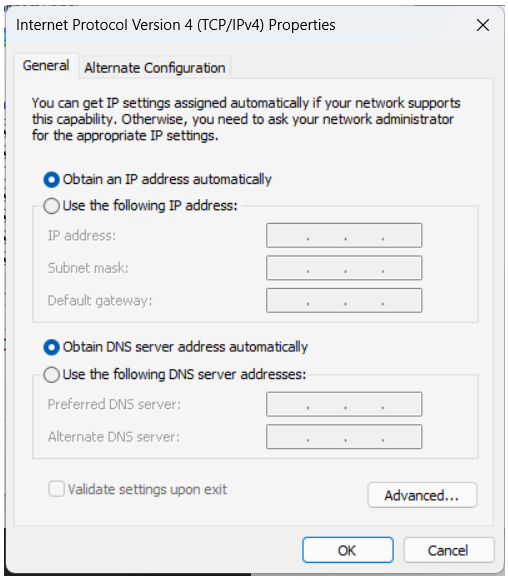
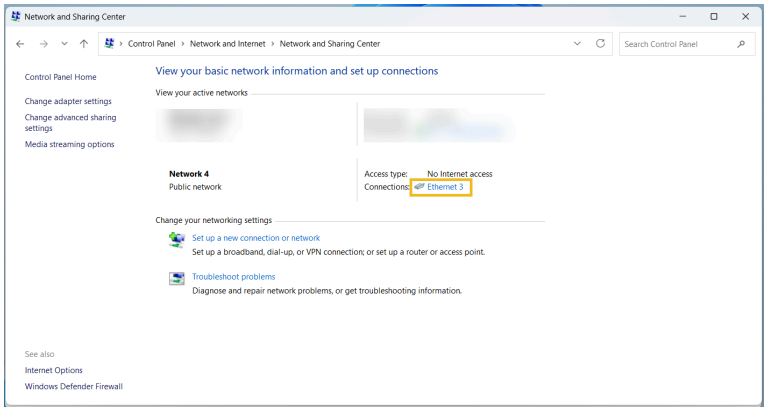
This chapter introduces the basic configuration steps for quickly using this gateway.

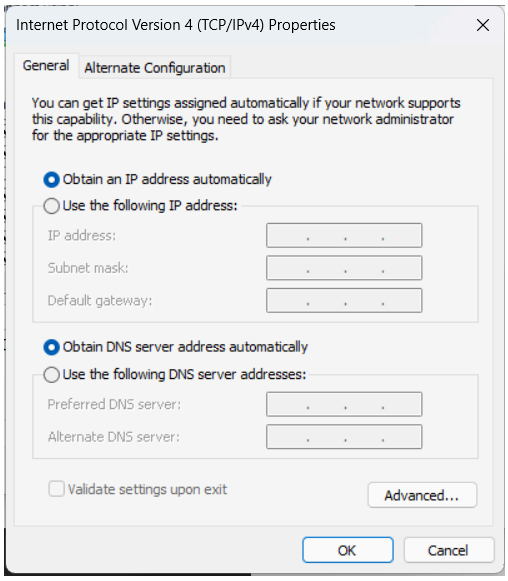
Step 1. Log in to Gateway Web GUI

The gateway can be accessed via wireless (Wi-Fi) or wired (Ethernet Port).

1. Select one of the following methods to connect to the gateway and access the web GUI.

Method	Step
Access via Wi-Fi	a. Enable the Wireless Network Connection on your computer, search for the corresponding for Wi-Fi SSID, and connect to it. Default Wi-Fi credentials: SSID: **Gateway_XXXXXX** (last 6 digits of the Wi-Fi MAC address) Password: **iotpassword** b. Open a web browser (Chrome is recommended) and type in **https://192.168.2.1** to access the web GUI.
Access via a LAN Port	a. Connect the **ETH2** port of the device to your computer using a network cable. b. Configure the computer's IP address either manually or automatically. Take Windows 10 as an example: i. Navigate to **Control Panel > Network and Internet > Network and Sharing Center** and select “Ethernet” (It may have a different name).  ii. Navigate to **Properties > Internet Protocol Version 4 (TCP/IPv4) Properties**, then select either **Obtain an IP address automatical-**

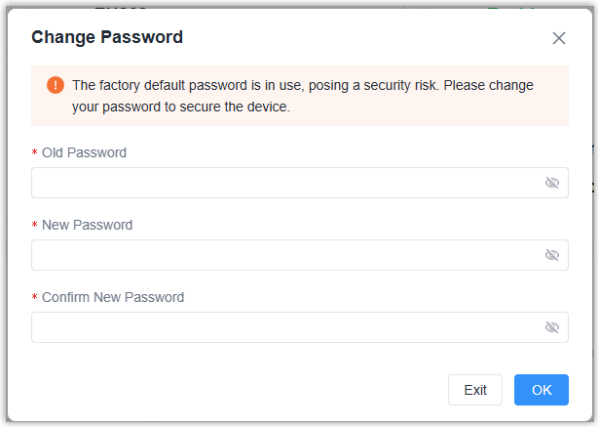
Method	Step
	ly or **Use the following IP address** to manually assign a static IP address within the same subnet as the gateway.  c. Open a web browser (Chrome is recommended) and type in **https://192.168.1.1** to access the web GUI.
Access via a WAN Port	a. Connect the **ETH1** port of the device and your computer to the same network router or switch with DHCP server enabled. b. Configure the computer's IP address automatically. Take Windows 10 as an example: i. Navigate to **Control Panel > Network and Internet > Network and Sharing Center** and select “Ethernet” (It may have a different name). 

Method	Step
	ii. Navigate to **Properties > Internet Protocol Version 4 (TCP/IPv4) Properties**, then select either **Obtain an IP address automatically**.  c. Check the device IP address received from the screen. i. Press any screen button to activate the device screen. ii. Press button to navigate to the Interface Status Menu. iii. Press ▶ button several times to navigate to the Ethernet Status page to obtain the ETH1 IP address (in the format of **xx.xx.xx.xx**). d. Open a web browser (Chrome is recommended) and type in **https://xx.xx.xx.xx** to access the web GUI.

2. Log in to the web GUI using the default credentials:

   Username: **admin**
   Password: **password**

3. After logging the web GUI for the first time, it is necessary to change the default password.

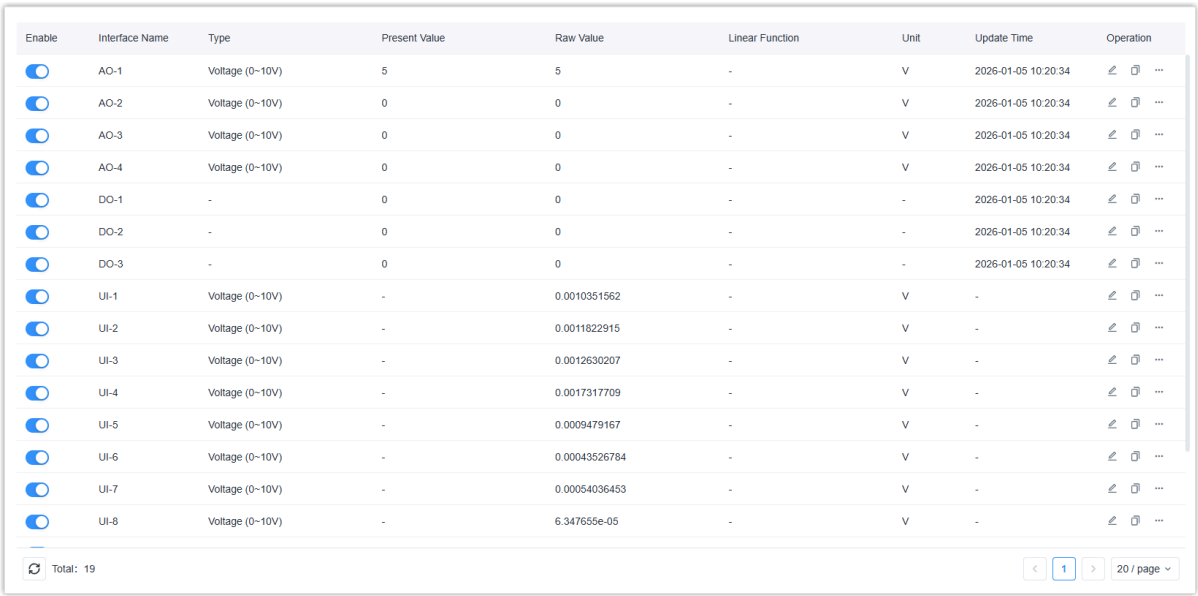


a. Enter the **Old Password**.
b. Enter a **New Password**. The password must contain at least one letter and one number, and be 5 to 31 characters long.
c. Enter **Confirm New Password**.
d. Click **OK**.
e. Log in to the web GUI using the new credentials.

Step 2. Add a Device

The gateway supports enabling IO interfaces or adding devices.

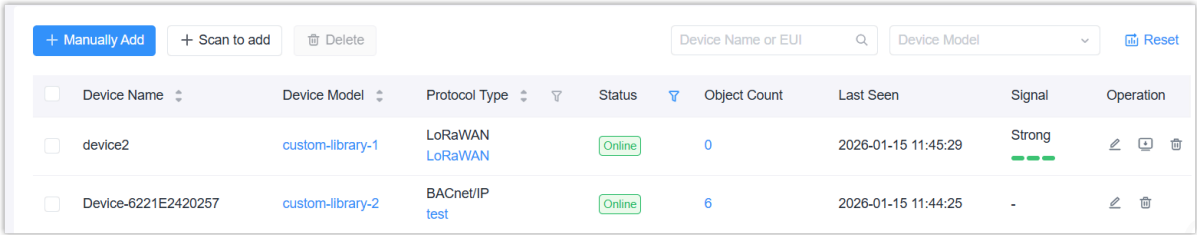
Enable IO Interface: Navigate to **Data Service > Data Acquisition > IO Device** page to enable the IO interfaces, then click to configure the IO interface parameters based on different interface types. For more details, refer to IO Device.



Enable	Interface Name	Type	Present Value	Raw Value	Linear Function	Unit	Update Time	Operation
	AO-1	Voltage (0~10V)	5	5	-	V	2026-01-05 10:20:34	
	AO-2	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-3	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-4	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	DO-1	-	0	0	-	-	2026-01-05 10:20:34	
	DO-2	-	0	0	-	-	2026-01-05 10:20:34	
	DO-3	-	0	0	-	-	2026-01-05 10:20:34	
	UI-1	Voltage (0~10V)	-	0.0010351562	-	V	-	
	UI-2	Voltage (0~10V)	-	0.0011822915	-	V	-	
	UI-3	Voltage (0~10V)	-	0.0012630207	-	V	-	
	UI-4	Voltage (0~10V)	-	0.0017317709	-	V	-	
	UI-5	Voltage (0~10V)	-	0.0009479167	-	V	-	
	UI-6	Voltage (0~10V)	-	0.00043526784	-	V	-	
	UI-7	Voltage (0~10V)	-	0.00054036453	-	V	-	
	UI-8	Voltage (0~10V)	-	6.347655e-05	-	V	-	

Total: 19 1 20 / page

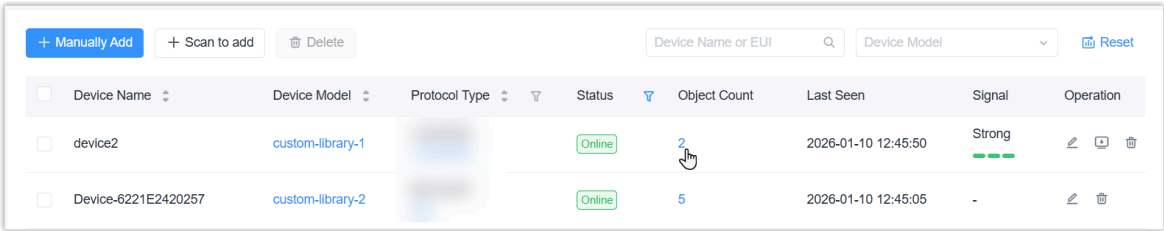
Add a Device: Navigate to **Data Service > Data Acquisition > Device** page to add devices based on different protocol types. For more details, refer to Add Devices.



Step 3. Add Device Objects

It is necessary to add device objects for read or write operations.

1. Navigate to **Data Service > Data Acquisition > Device** page, then click the object count value to go to Object List page.

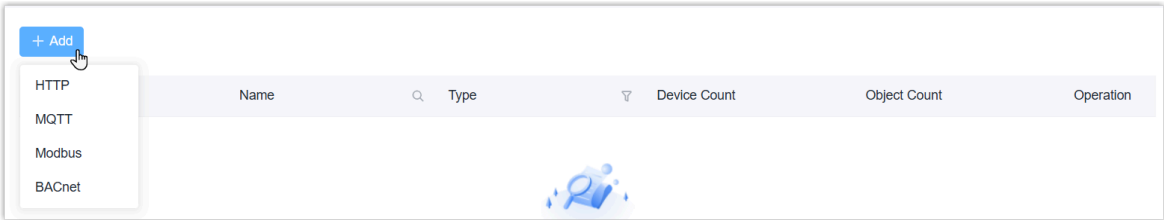


2. Add device objects and enable the desired objects. For more details, refer to Add Device Objects and Enable Device Objects.

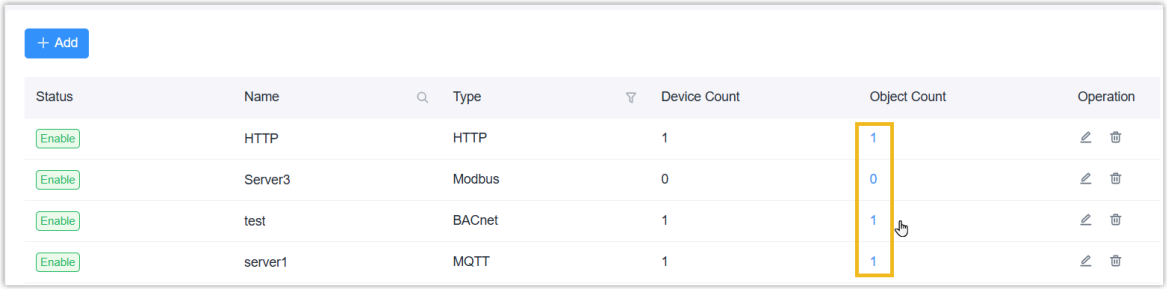
Step 4. Add Data Forwarding Destination

If you need to forward data or implement remote control, it is necessary to add data forwarding rules.

1. Navigate to **Data Service > Data Forwarding** page to add a data forwarding rule. For more details, refer to Add Data Forwarding Rule.



2. Navigate to **Data Service > Data Forwarding** page, then click the object count value to go to Object List page to add forwarding contents. For more details, refer to Add Data Forwarding Objects.

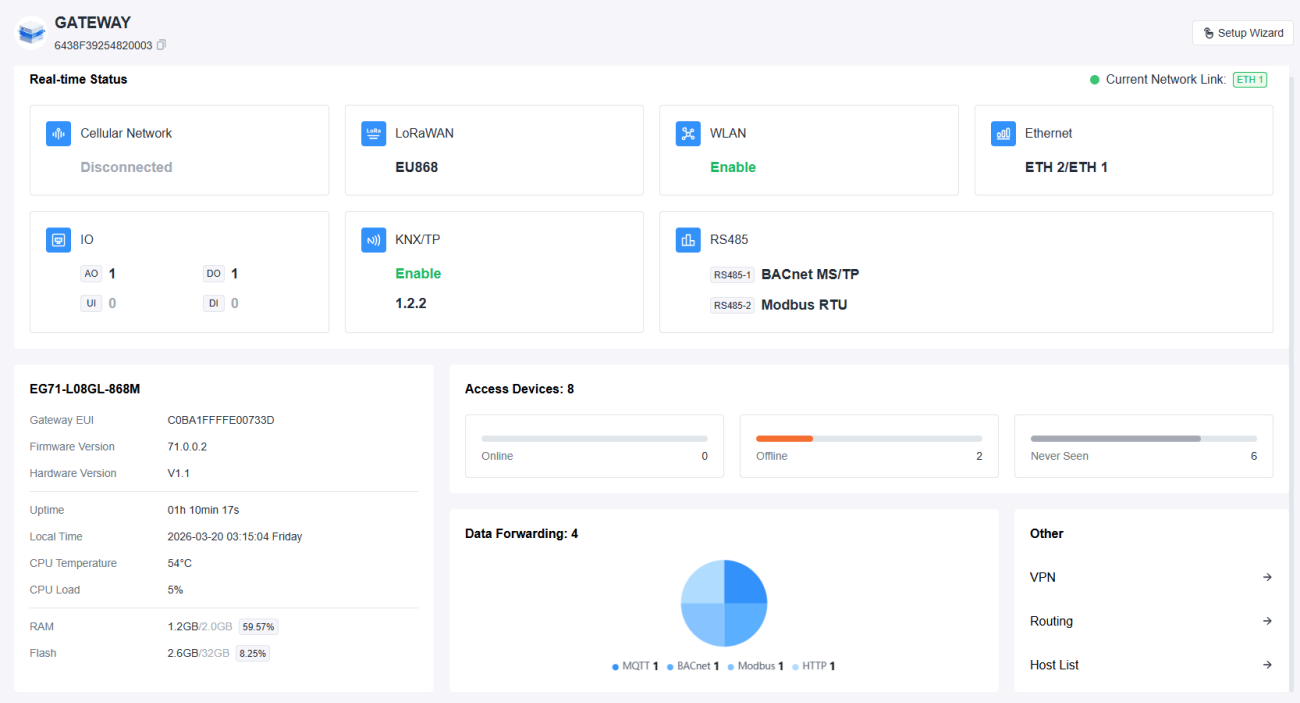


Chapter 4. Status

The Status page displays the device's basic information and operational status.

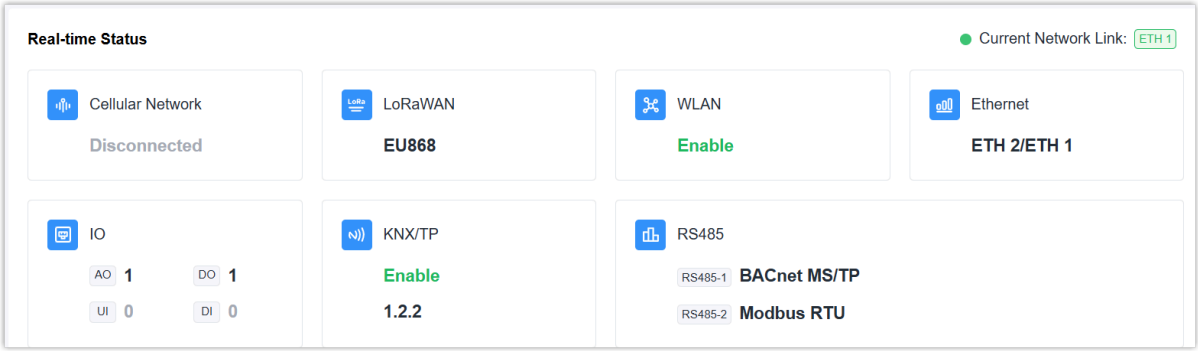
Overview

The top of the page displays the hostname, serial number, and wizard portal. Click the widgets in the figure to learn more.



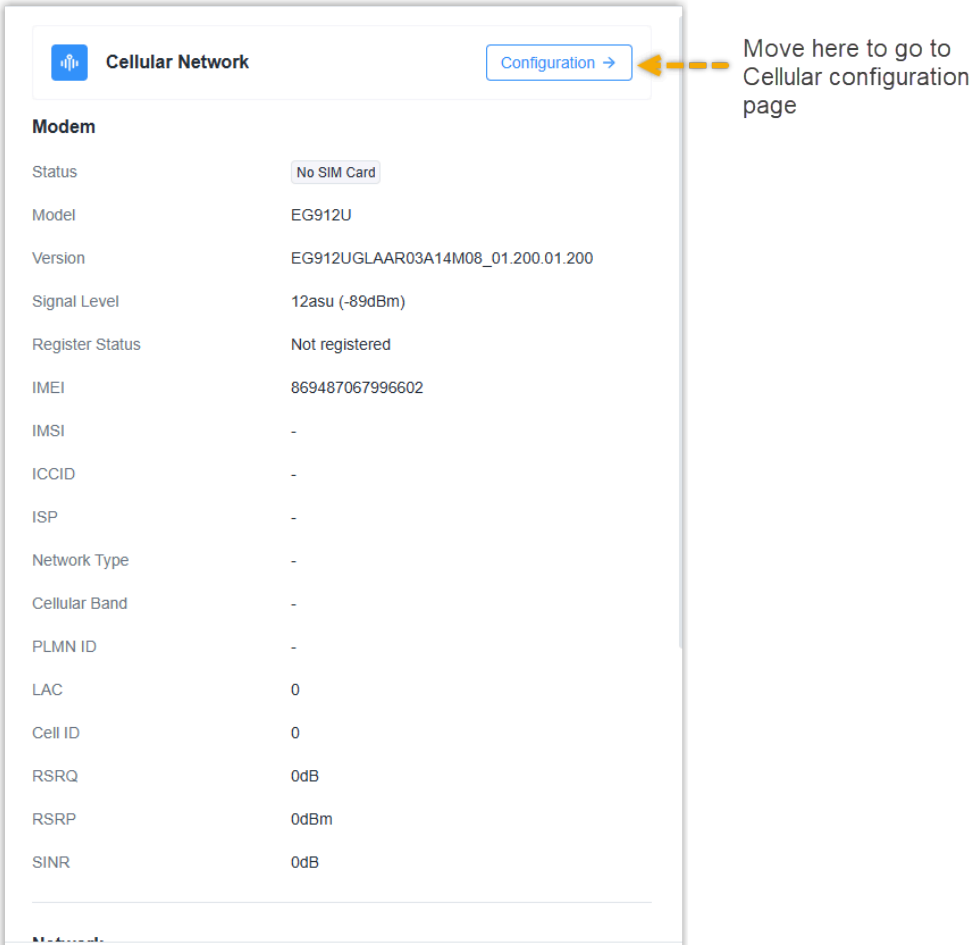
1. Real-time Status
2. Basic Information
3. Access Devices
4. Data Forwarding
5. Other

Real-time Status



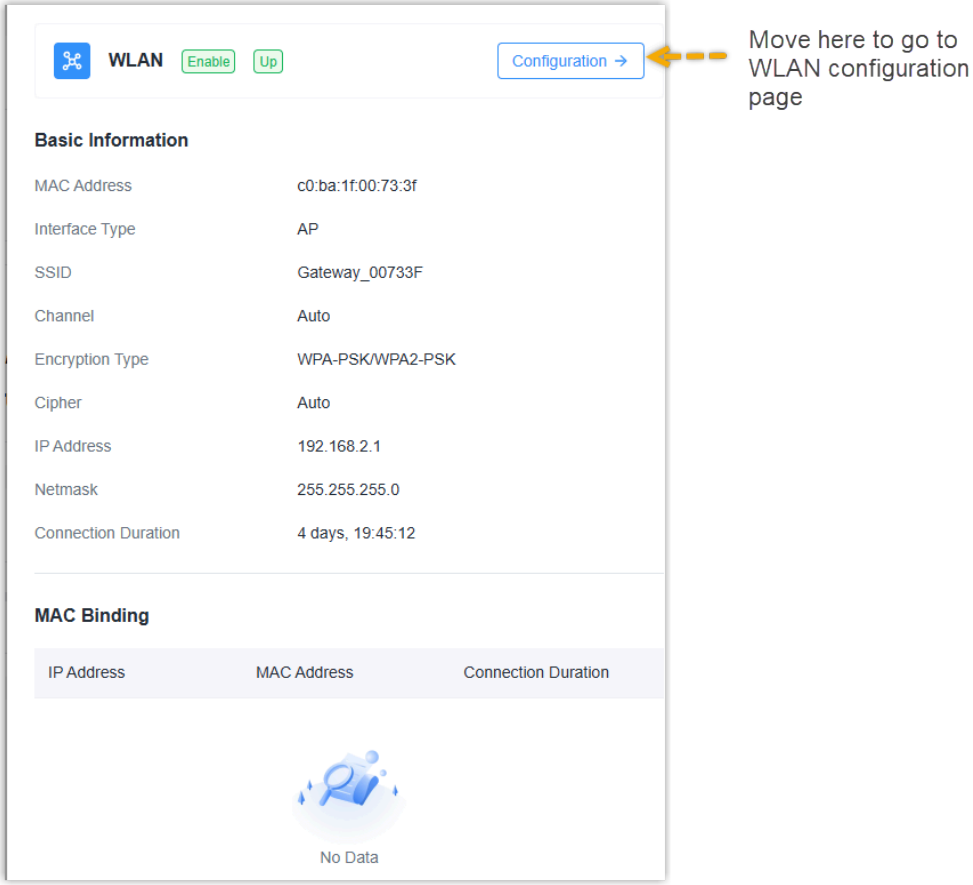
This widget displays the current network link, and includes seven small widgets to display the status of each interface. You can click every widget to check status details.

Cellular Network: Displays the cellular module status, network registration status, and monthly cellular data usage.

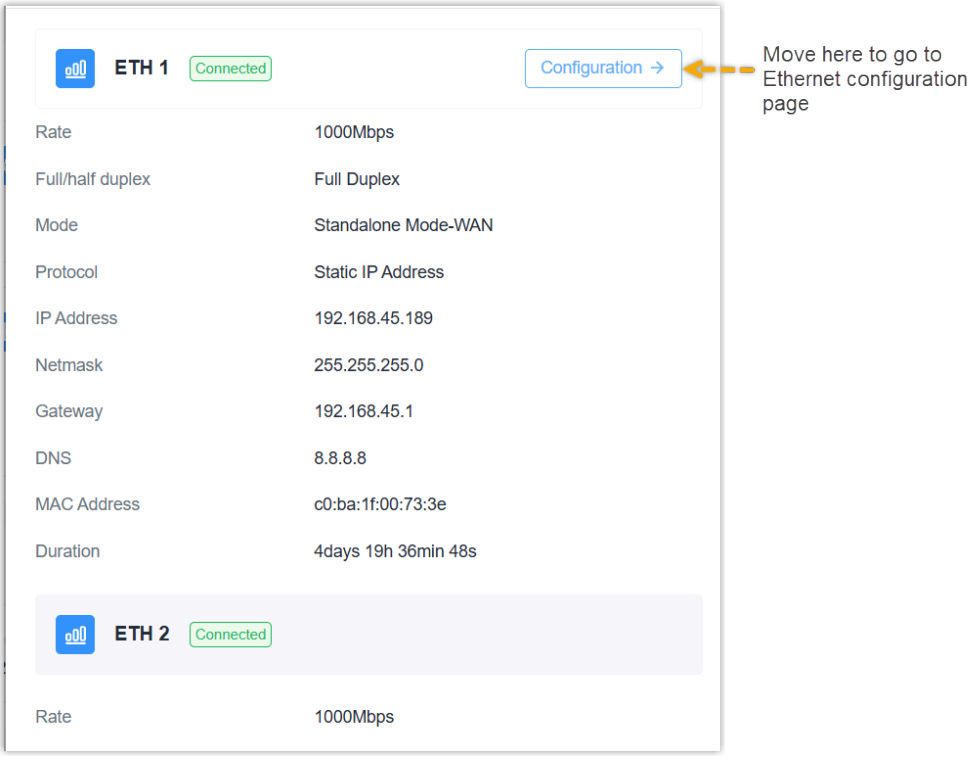


LoRaWAN: Displays the channel plan, frequencies, and the number of added LoRaWAN® devices.

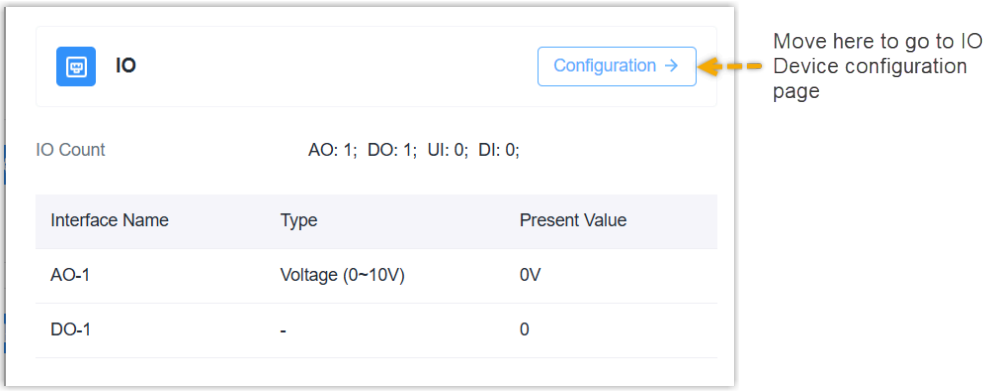
WLAN: Displays the WLAN enable status, up/down status, and information for different modes.



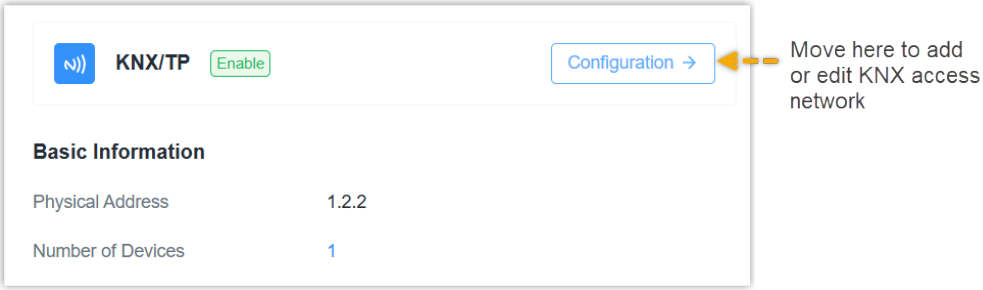
Ethernet: Displays the connection status and information of each Ethernet port.



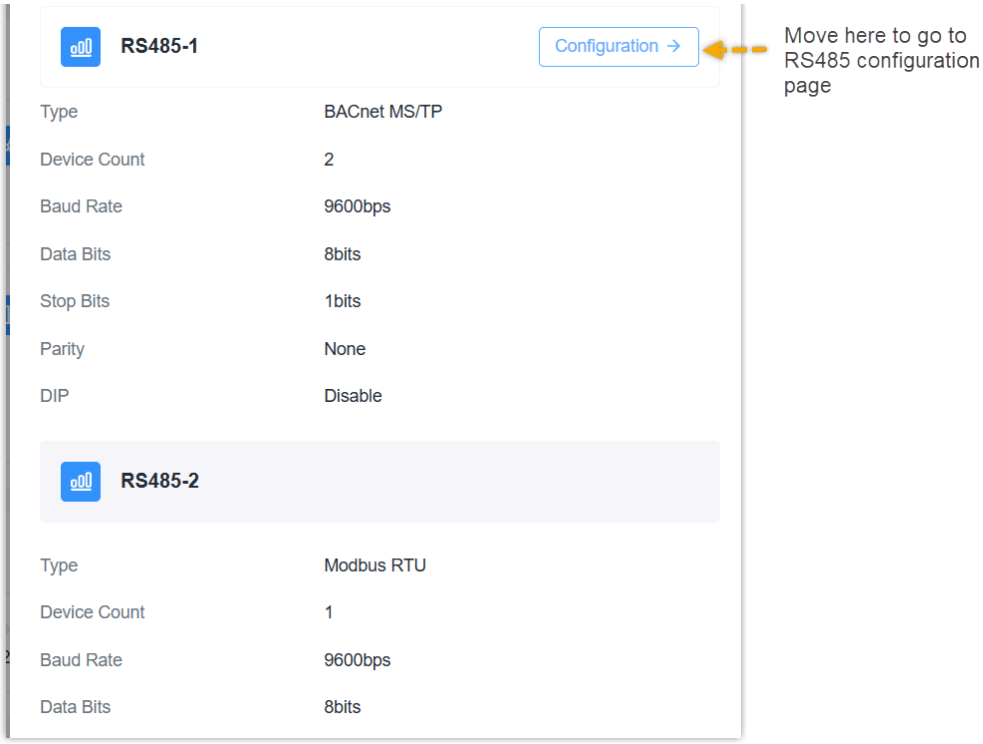
IO: Displays the number of enabled IO interfaces, their types, and present values.



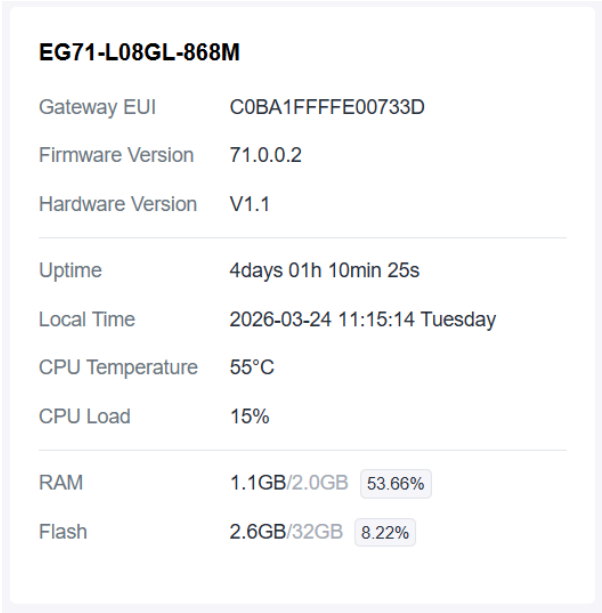
KNX/TP: Displays the physical address of this interface, and the number of added KNX/TP devices.



RS485: Displays the settings and protocol type used of each RS485 interface.

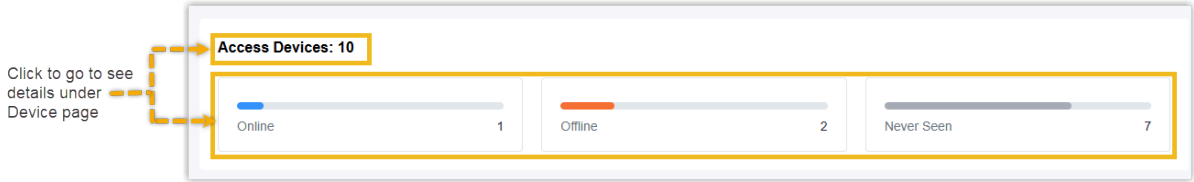


Basic Information



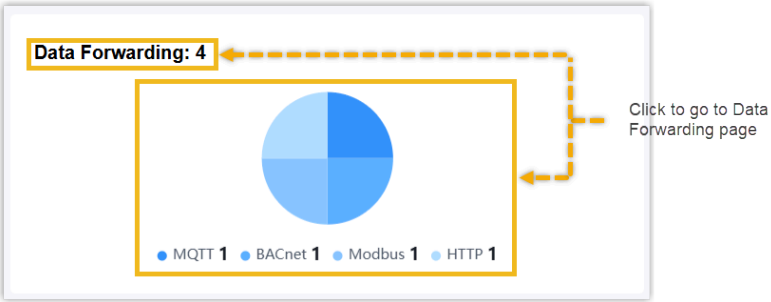
This widget displays the basic information, operational status, and storage status.

Access Devices



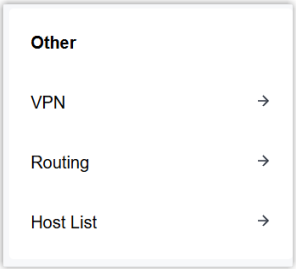
This widget displays the total number of added devices, as well as the number and proportion of devices in different statuses.

Data Forwarding



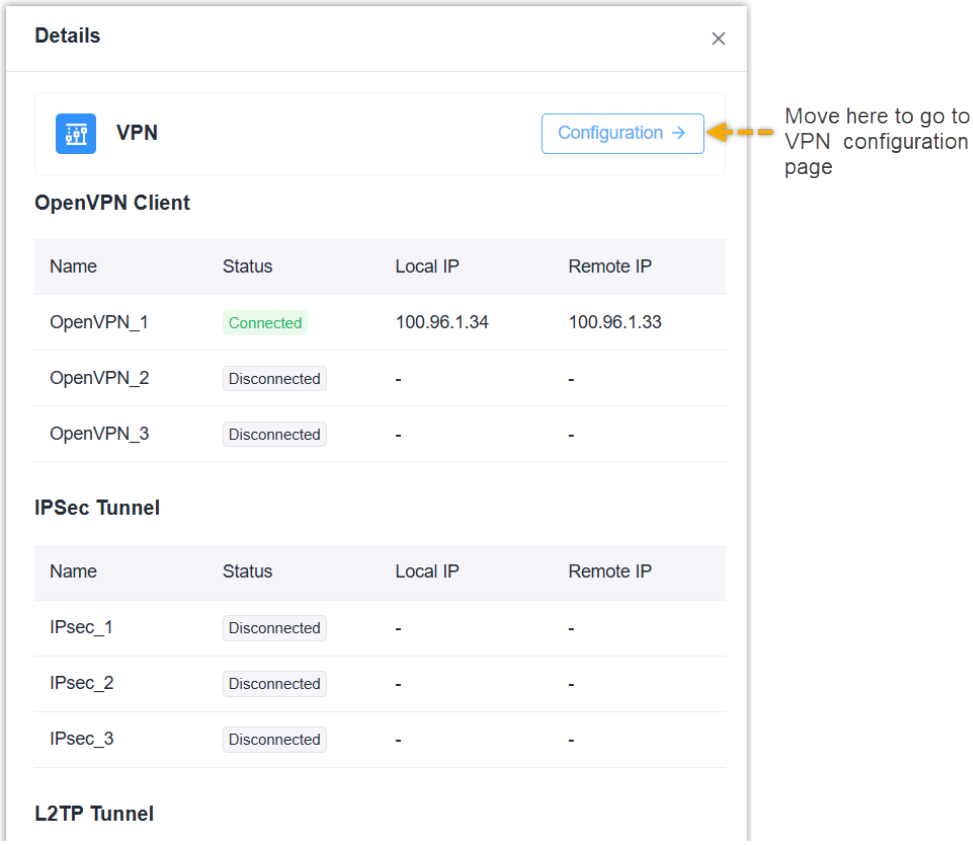
This widget displays the total number of added data forwarding rules, as well as the number and proportion of rules for different protocol types.

Other

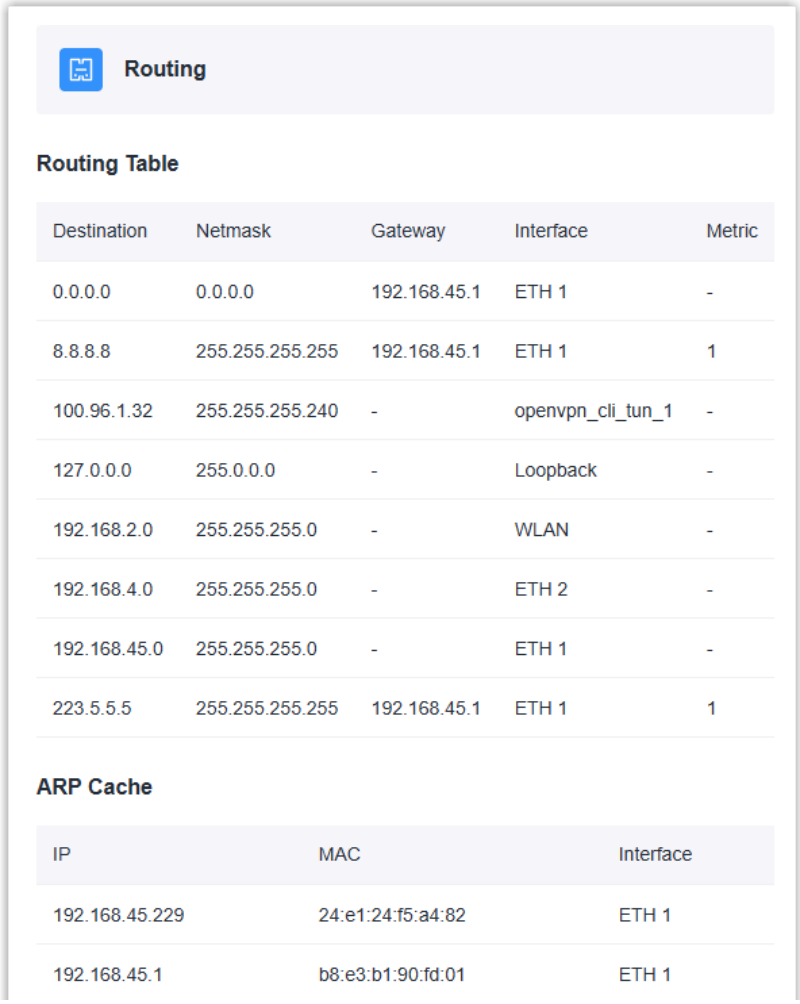


The widget displays the three menus:

VPN: Displays the connection status of OpenVPN clients, IPsec tunnels, L2TP tunnels, and PPTP tunnels.



Routing: Displays the routing table and ARP cache.



Routing

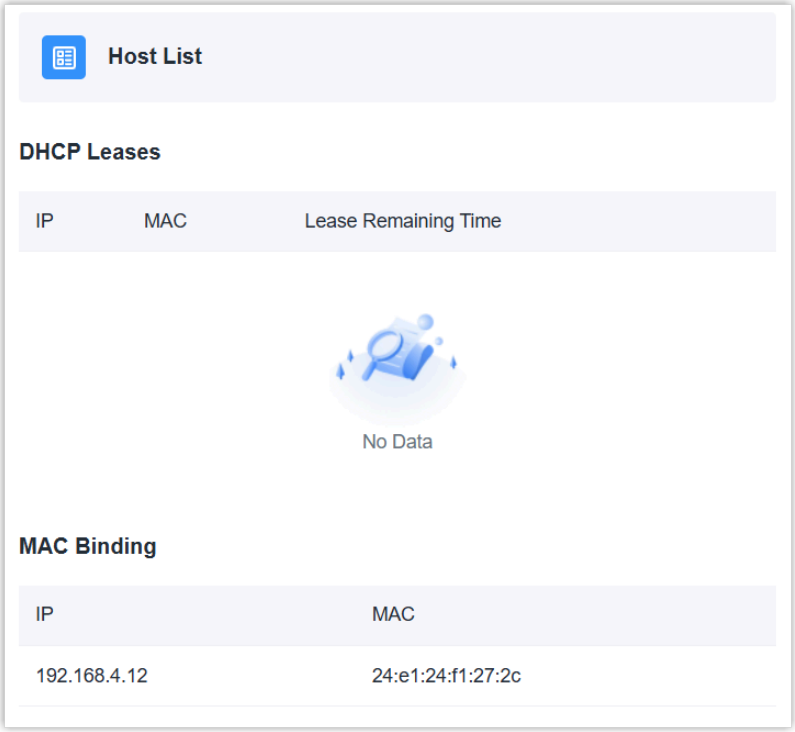
Routing Table

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.45.1	ETH 1	-
8.8.8.8	255.255.255.255	192.168.45.1	ETH 1	1
100.96.1.32	255.255.255.240	-	openvpn_cli_tun_1	-
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.2.0	255.255.255.0	-	WLAN	-
192.168.4.0	255.255.255.0	-	ETH 2	-
192.168.45.0	255.255.255.0	-	ETH 1	-
223.5.5.5	255.255.255.255	192.168.45.1	ETH 1	1

ARP Cache

IP	MAC	Interface
192.168.45.229	24:e1:24:f5:a4:82	ETH 1
192.168.45.1	b8:e3:b1:90:fd:01	ETH 1

Host Leases: Displays the DHCP lease list and MAC binding list for the DHCP server.


Host List
DHCP Leases
IP
MAC
Lease Remaining Time
No Data
MAC Binding
IP
MAC
192.168.4.12
24:e1:24:f1:27:2c

Chapter 5. Data Service

Data Acquisition

Device

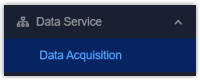
This chapter describes how to add and manage devices.

Add Devices

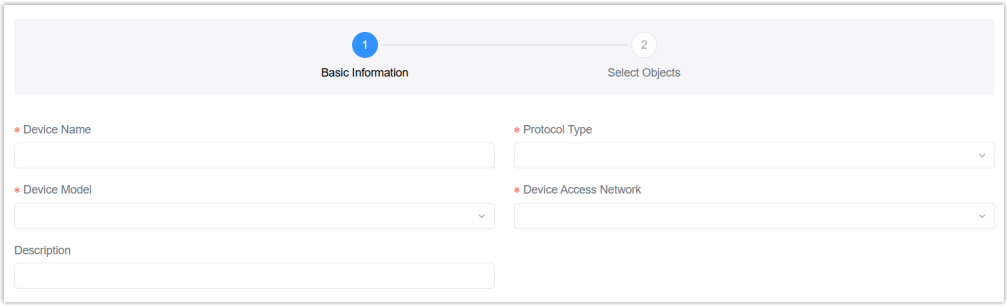
The gateway supports adding up to 2000 devices using various methods. Please select one to add devices.

Add Devices Manually

1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device** tab.
3. Click **+Manually Add** to add a new device.
4. Configure the basic information of the device.



Parameter	Description
Device Name	Define a unique name for the device.
Protocol Type	Select the protocol type according to the terminal devices: LoRaWAN, BACnet/IP, BACnet MS/TP, Modbus RTU, Modbus TCP, Modbus RTU over TCP, KNX/TP.
Device Model	Select a device model from Device Library. If the device does not have a compatible model or requires custom configurations, select **None**.

Parameter	Description
	Tip: Only when a device model is selected can the device select objects in the next step.
Device Access Network	Select the device access network added from Device Access Network.
Description	For noting this device.
Protocol Type is LoRaWAN	
Device EUI	The unique 16-digit hexadecimal EUI of the device.
Device-Profile	Select the device profile added from Device Profiles. **Note:** If the device type is Class B, ensure Class B Setting is enabled.
fPort	FPort (Frame Port) is a single-byte field in the MAC payload that identifies the type or destination of the data, functioning like a port number for different services or applications on an end device.
Modbus RTU Data Transmission	Choose from: Disable, Modbus RTU to TCP, Modbus RTU over TCP. This is only applicable to Milesight LoRaWAN® controllers. (UC501/UC300, etc.) **Modbus RTU to TCP:** The TCP client can send Modbus TCP commands to request Modbus data from the controller. **Modbus RTU over TCP:** The TCP client can send Modbus RTU commands to request Modbus data from the controller.
Application Key	When join type is OTAA. set the 32-digit hexadecimal AppKey value. For Milesight devices, users can select Default to use Milesight default AppKey or Custom to customize the AppKey.

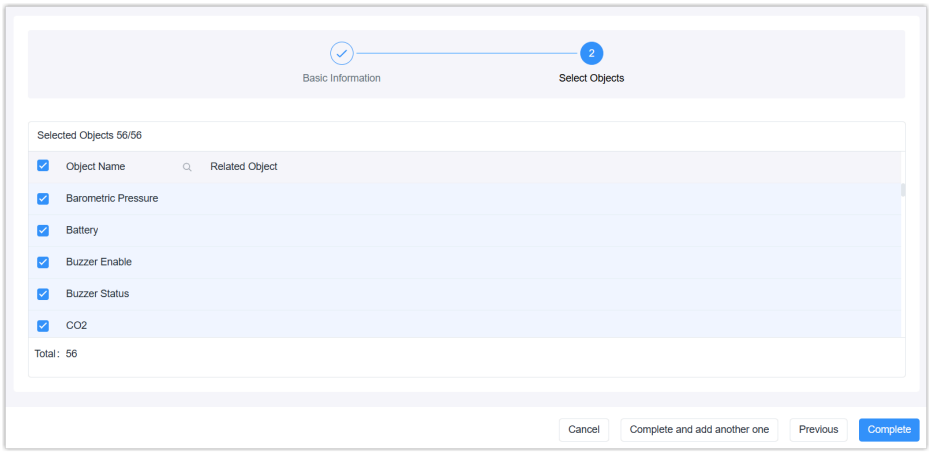
Parameter	Description
Device Address	When the join type is ABP, set the 8-digit hexadecimal DevAddr.
Application Session Key	When the join type is ABP, set the 32-digit hexadecimal NwkSKey value.
Network Session Key	When the join type is ABP, set the 32-digit alphanumeric AppSKey value.
Uplink Frame-counter	When the join type is ABP, set the uplink frame-counter.
Downlink Frame-counter	When the join type is ABP, set the downlink frame-counter.
Timeout	The time to judge the device's online/offline status. Range: 1-4320 mins
Frame-counter Validation	Enable this feature to prevent replay attacks.
Protocol Type is BACnet/IP or BACnet MS/TP	
Device Instance Nr	Set the unique identifier of the device within the BACnet network.
Protocol Type is Modbus TCP or Modbus RTU over TCP	
IP Address	Set the IP address of the Modbus server (slave) device.
Server ID	Set the unique server ID (slave ID) provided by Modbus device vendor.
Port	Set the port of the Modbus server (slave) device.
Protocol Type is Modbus RTU	
Server ID	Set the unique server ID (slave ID) provided by Modbus RTU device vendor.
Protocol Type is KNX/TP	
Physical Address	Set the unique physical address of the device within the KNX bus network.

5. Click **Next Step** to select objects for this device.

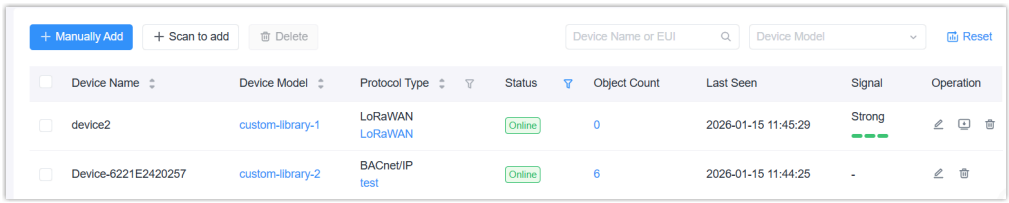
If no device model is selected, there will be no object to select, and the device will be created automatically.

If the device model is selected in previous step,

a. Select the required objects to add to the device.
b. Click **Complete** to finish adding the device, or click **Complete and add another one** to add a new device.



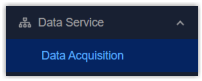
6. After adding, check the device status in the device list.



If the device is still not online, navigate to **Data Service > Data Stream** page to check for communication between the device and the gateway.

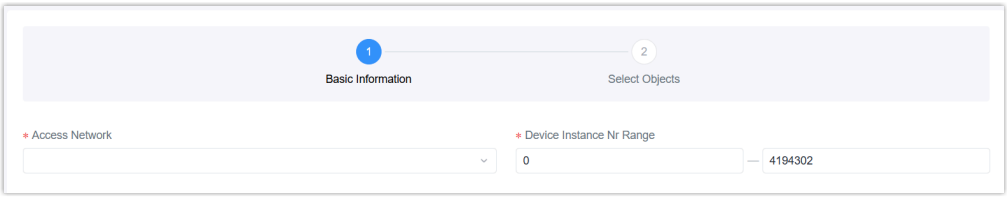
Add BACnet Devices by Scanning

1. On the left bar, select **Data Service > Data Acquisition** page.

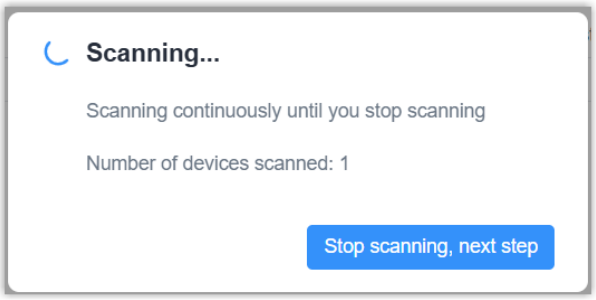


2. On the top bar, select **Device** tab.
3. Click **+Scan to Add** to add a new device, select **Scan BACnet/IP** or **Scan BACnet MS/TP**.
4. Select the access network, and configure the device instance number range to scan.

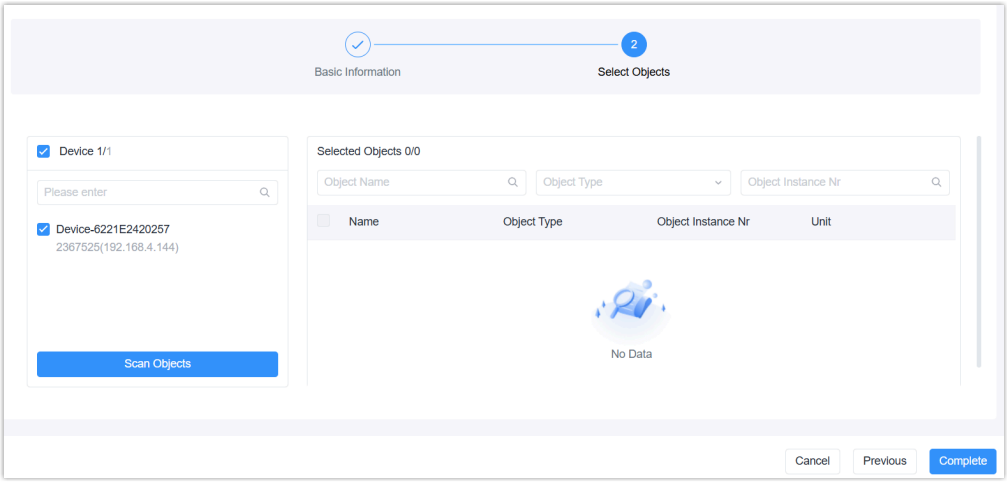
Note:
Ensure the physical or network interface of this access network can reach your BACnet devices.



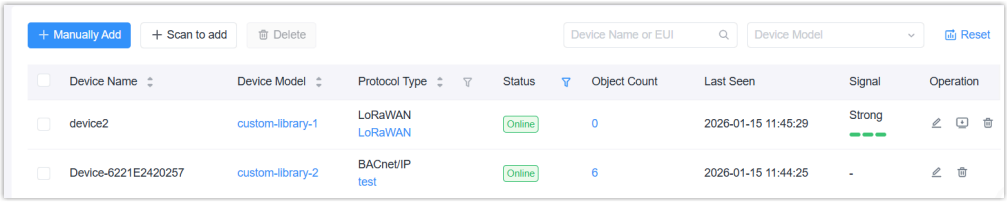
5. Click **Next Step** to start scanning the reachable BACnet devices in the network.
6. If there is any device can be scanned, click **Stop scanning, next step**.



7. Select the device from the device list, click **Complete** to finish adding it, or click **Scan Objects** to search for and add the objects for the device.



8. After adding, check the device status in the device list.



If the device is still not online, navigate to **Data Service > Data Stream** page to check for communication between the device and the gateway.

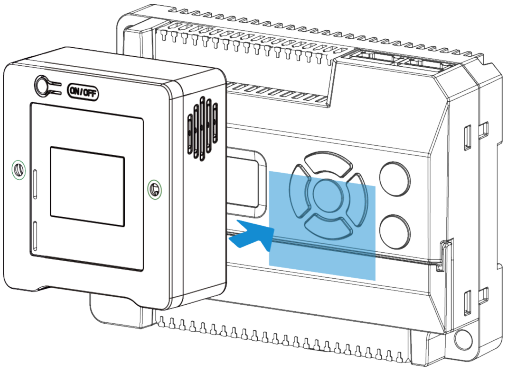
Add Milesight LoRaWAN® Devices by NFC

Prerequisites:

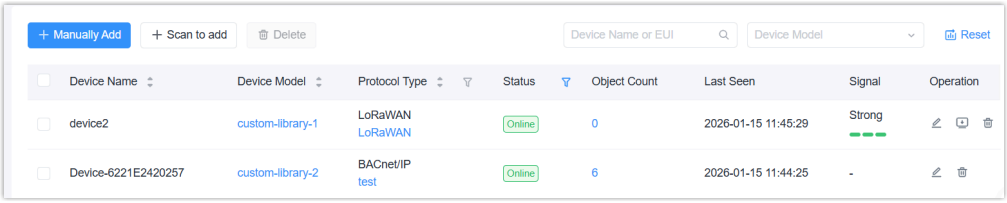
- The end device supports NFC configuration.
- The end device and the gateway support the same LoRaWAN® channel plan.

Steps:

1. Power on the end device.
2. Press any screen button on the gateway to activate the gateway screen.
3. Attach the NFC area of the end device to the gateway for a few seconds. The screen will display the adding status. If added successfully, the device will display in the device list.



4. Click of the added device to select the device model.
5. After adding, check the device status in the device list.



If the device is still not online, navigate to **Data Service > Data Stream** page to check for communication between the device and the gateway.

Add Device Objects

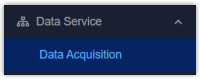
Each device supports adding objects for read or write operations. Typically, you can add the objects when adding a device. If you skip this step, please refer to the steps below to add objects for the device.

Add Objects from Device Library

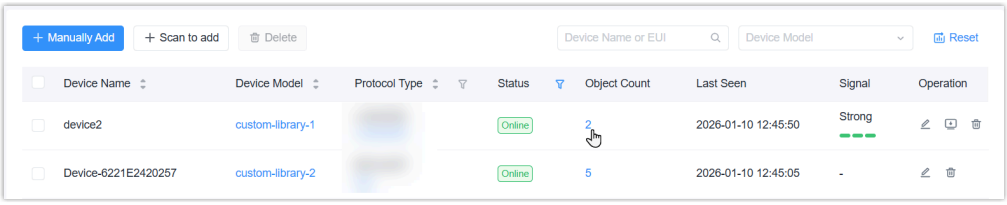
Prerequisites: A device model has been selected for he device.

Steps:

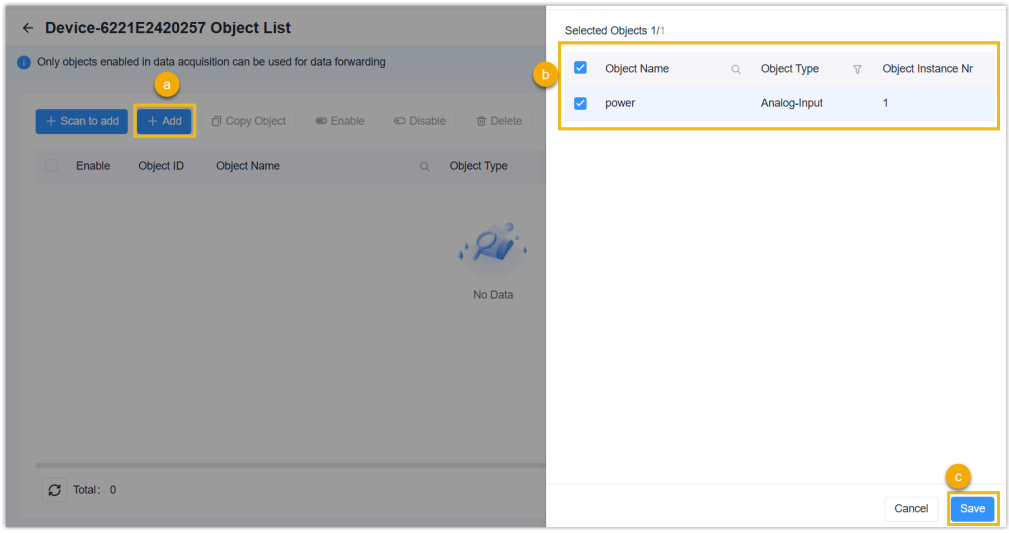
1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device** tab.
3. Select the desired device, then click the object count value to navigate to the Object List page.



4. Click **+Add** and select **Device Library**.
5. Select the objects from the pop-up list, click **Save**.



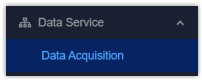
6. Click edit in the Object List to configure the object parameters (collection interval, linear function, etc.) as required.

Add Objects Manually

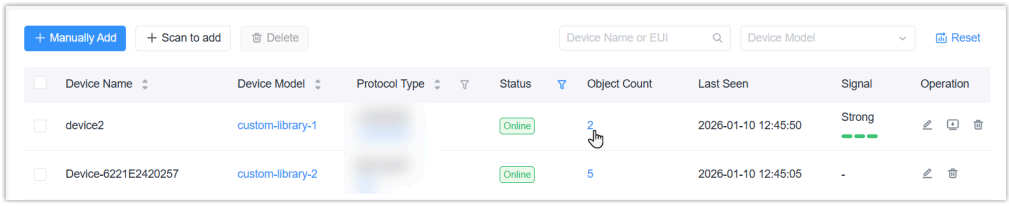
If you need to add custom objects, please follow the steps below.

> **Note:**
> LoRaWAN® devices do not support this feature.

1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device** tab.
3. Select the desired device, then click the object count value to navigate to the Object List page.



4. Click **+Add** and select **Custom Objects**.
5. Configure the object information according to the protocol type.

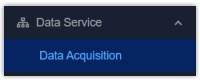
Parameter	Description
Object Name	Define a unique name for this object.
Object Description	For noting this object.
BACnet/IP or BACnet MS/TP	
Object Type	Select BACnet object type.
Object Instance Nr	Set a unique object instance number.
Collection Interval	The interval to collect the object data. Range: 1-86400s.
Unit	Select the value unit when object type is Analog type.
Linear Function	When enabled, the collected value will be substituted into the function formula before being display. The formula: `y=a*x+b` (y: present value, x: raw value/real collected value)
COV Subscription	When enabled, the gateway will send a notification when analog-type value changes.
Modbus RTU/TCP or Modbus RTU over TCP	
Register Type	Select the Modbus register type. **Discrete Input:** Reads on/off values **Coil:** Reads/Writes on/off values **Input Register:** Reads measurements and statuses **Holding Register:** Reads/Writes configuration values
Data Format	Select the data type when register type is Input Register or Holding Register.
Register Address	Set the start address for reading/writing this object's value in the register.
Register Quantity	Displays the quantity based on the data format.

Parameter	Description
Collection Interval	The interval to collect the object data. Range: 1-86400s.
Unit	Select the unit of this value when register type is Input Register or Holding Register.
Linear Function	When enabled, the collected value will be substituted into the function formula before being display. The formula: `y=a*x+b` (y: present value, x: raw value/real collected value)
KNX	
Group Address	Define the group address of this object.
Datapoint Type	Select the KNX Data Point Type (DPT) to define the value. If the type is Custom, you need to define the data length.
Access Mode	Select the access mode for this object.
Collection Interval	The interval to collect the object data. Range: 300-86400s.
Unit	Displays the data unit after selecting the datapoint type.

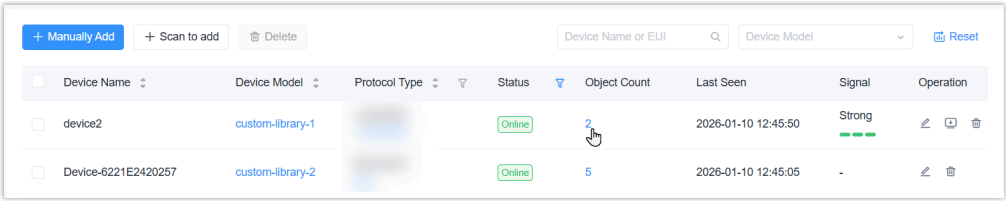
6. Click **Save** to save the settings.

Add BACnet Objects by Scanning

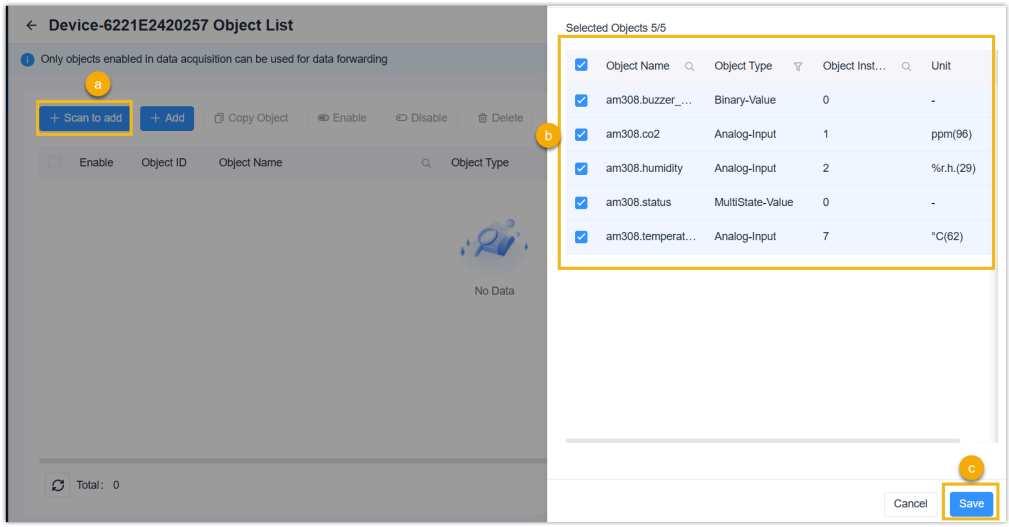
1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device** tab.
3. Select the desired device, then click the object count value to navigate to the Object List page.



4. Click **+Scan to add** to scan for objects of this BACnet device.
5. Select the desired objects from pop-up list, then click **Save**.

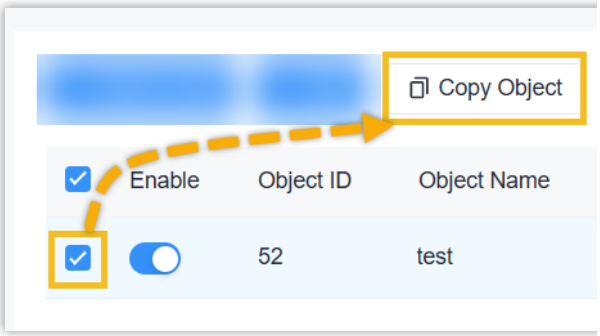


Add Objects by Copy

If you add multiple devices of the same model, follow the steps below to add objects by copying.

> **Note:**
> KNX devices do not support this feature.

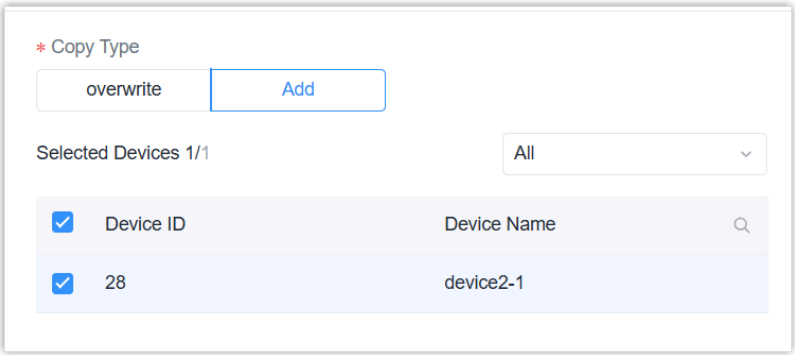
1. Follow the steps above to add objects to one of the devices.
2. Select the device with the added objects in the device list, click the object count value to go to Object List page.
3. Select the checkboxes of the desired objects, then click **Copy Object**.



4. In the pop-up window, select the copy type, and the devices.

Overwrite: The objects of the selected devices will be overwritten.

Add: The objects of the selected devices will not be overwritten.

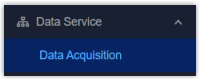


5. Click **Save** to copy the objects to the selected devices.

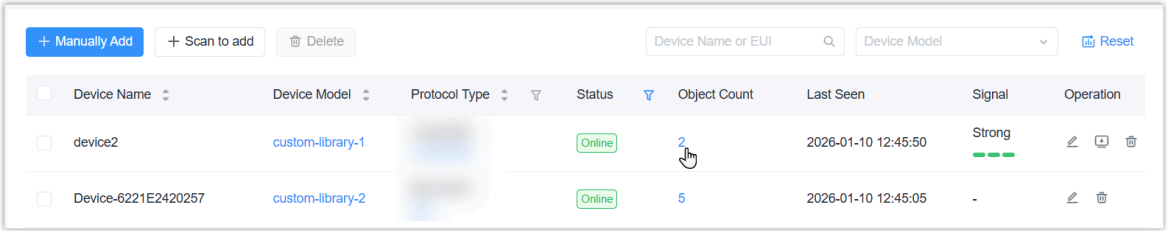
Enable or Disable Objects

After adding objects to devices, you can enable or disable the objects as needed.

1. On the left bar, select **Data Service > Data Acquisition** page.

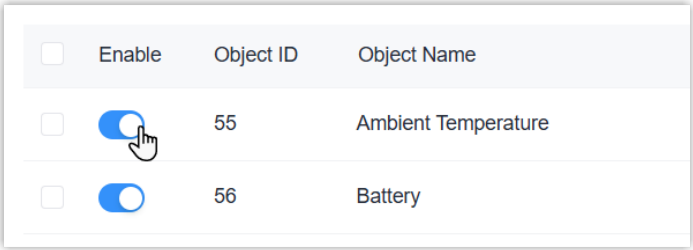


2. On the top bar, select **Device** tab.
3. Select the desired device, then click the object count value to navigate to the Object List page.

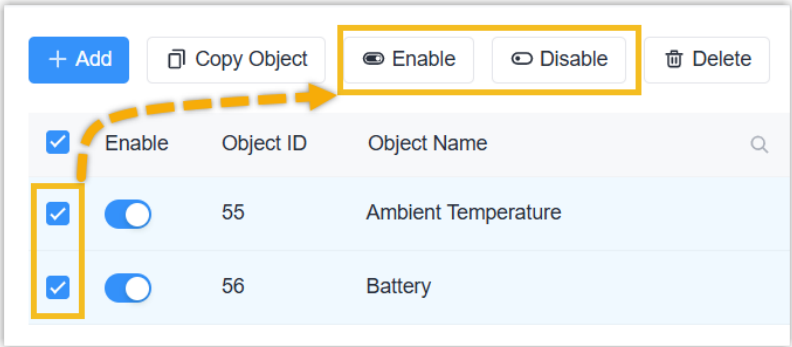


4. Enable or disable the objects. After enabled, the objects can be used for data forwarding and read/write operations.

   Enable or disable single object: Tap the **Enable** button for the desired object.



Enable or disable objects in bulk: Select the checkboxes of the desired objects, then click **Enable** or **Disable** button.



Read/Write Devices

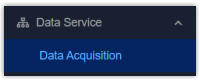
The gateway supports reading device data or send commands to devices directly.

Prerequisites:

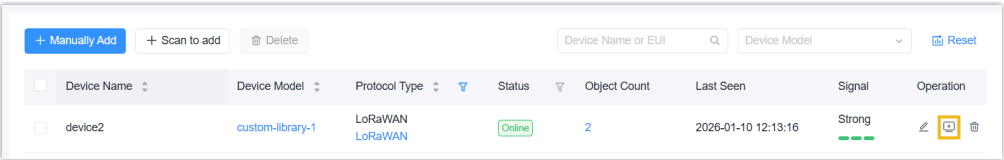
- The device is online.
- The desired device object is writable.
- If the LoRaWAN® device is of Class B type, ensure Class B Setting is enabled.

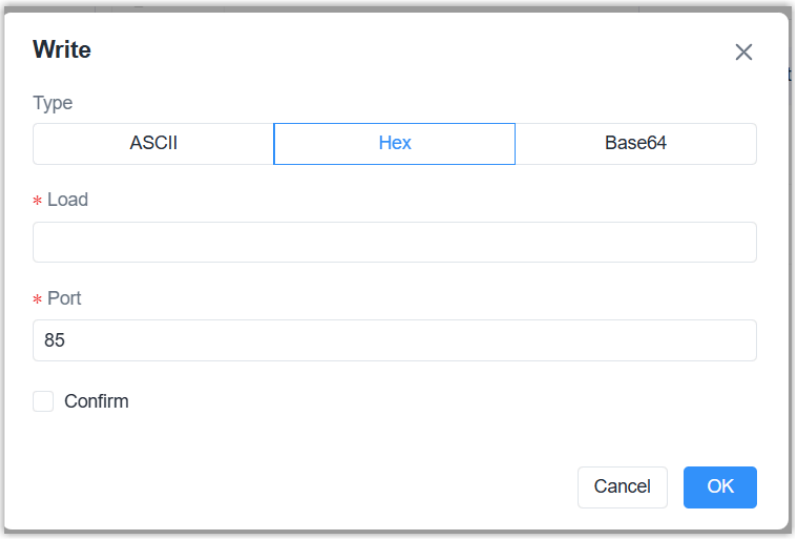
Send Command to a LoRaWAN® Device

1. On the left bar, select **Data Service > Data Acquisition** page.



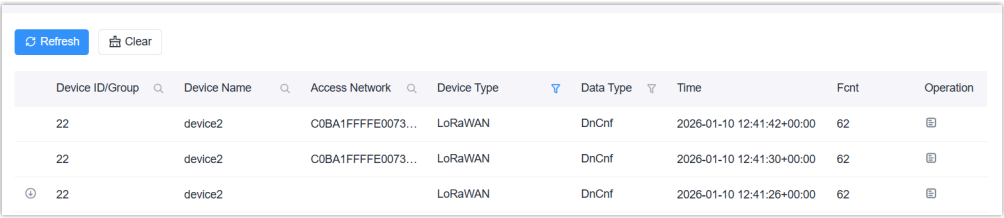
2. On the top bar, select **Device** tab.
3. Select the desired device, click to configure a downlink payload.





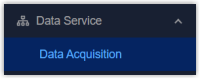
Parameter	Description
Type	Select the downlink payload type.
Load	Define the downlink payload based on the corresponding type.
Port	Define the application port for this device.
Confirm	Enable or disable the device to respond after receiving this downlink payload.

4. Click **OK** to send the downlink payload.
5. Navigate to **Data Service > Data Stream** to check the downlink sending status.

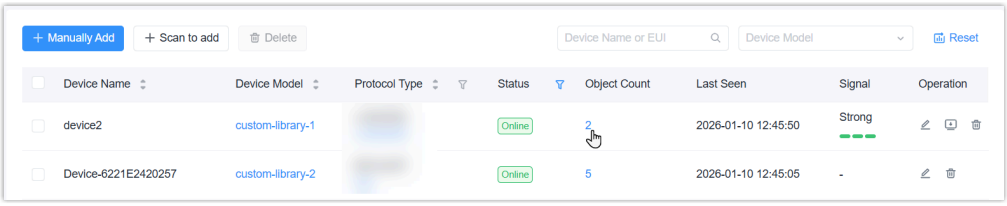


Read/Write Other Devices

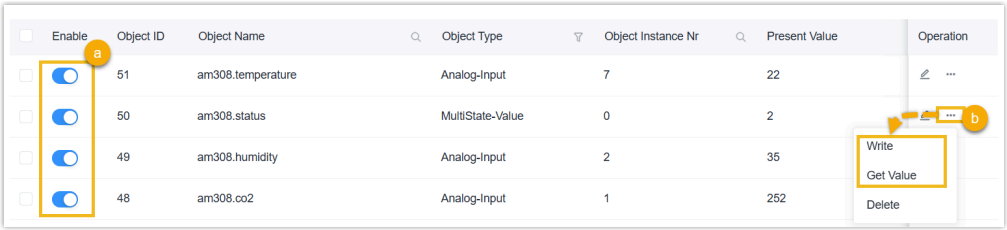
1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device** tab.
3. Select the desired device, then click the object count value to navigate to the Object List page.



4. Follow the above steps to add and enable objects.
5. Click ••• of the desired object in the Operation column.
6. Select **Get Value** to read latest value, or click **Write** to write this value. The read/write permission depends on the data type or access mode.



IO Device

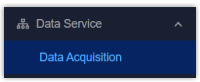
This chapter describes how to configure the IO interfaces for terminal device connection.

Prerequisites

- Refer to Wiring Diagrams to confirm that the IO devices are compatible with the gateway.
- Follow Terminal Device Wirings instructions to connect IO devices to the correct interfaces.

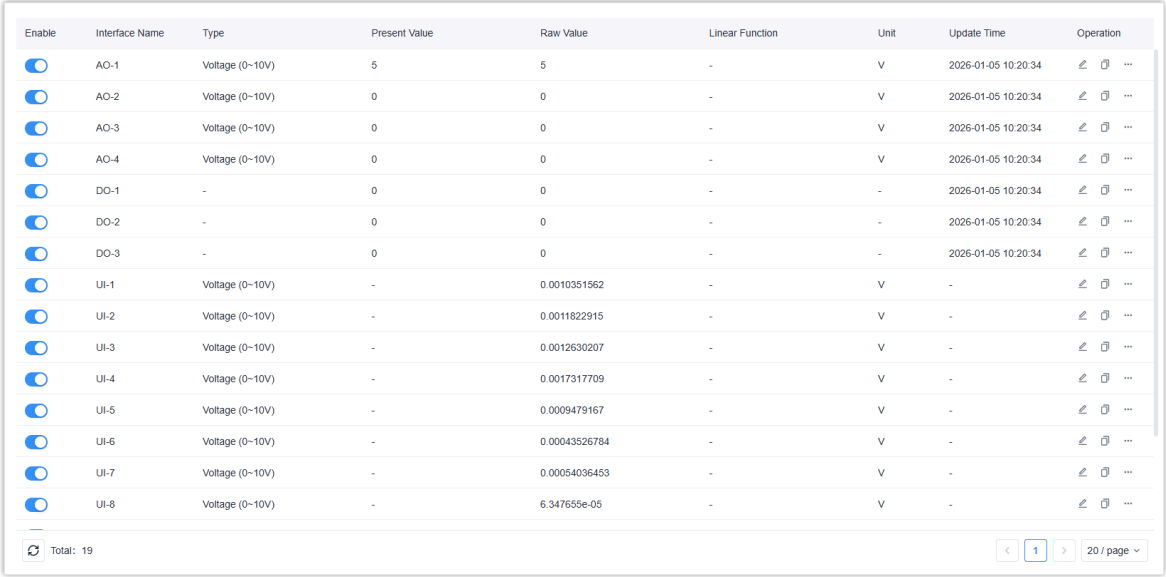
Steps

1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **IO Device** tab.

3. Enable the required IO interface and check their information.



Enable	Interface Name	Type	Present Value	Raw Value	Linear Function	Unit	Update Time	Operation
	AO-1	Voltage (0~10V)	5	5	-	V	2026-01-05 10:20:34	
	AO-2	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-3	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-4	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	DO-1	-	0	0	-	-	2026-01-05 10:20:34	
	DO-2	-	0	0	-	-	2026-01-05 10:20:34	
	DO-3	-	0	0	-	-	2026-01-05 10:20:34	
	UI-1	Voltage (0~10V)	-	0.0010351562	-	V	-	
	UI-2	Voltage (0~10V)	-	0.0011822915	-	V	-	
	UI-3	Voltage (0~10V)	-	0.0012630207	-	V	-	
	UI-4	Voltage (0~10V)	-	0.0017317709	-	V	-	
	UI-5	Voltage (0~10V)	-	0.0009479167	-	V	-	
	UI-6	Voltage (0~10V)	-	0.00043526784	-	V	-	
	UI-7	Voltage (0~10V)	-	0.00054036453	-	V	-	
	UI-8	Voltage (0~10V)	-	6.347655e-05	-	V	-	

Parameter	Description
Enable	Enable or disable the interface.
Interface Name	Display the interface type.
Type	Display the configured type of the interface.
Present Value	For input types, it displays the value after processing via Linear Function or Polarity Inversion; for output types, it displays the value sent by the user.
Raw Value	For input types, it displays the raw collected value; for output types, it displays the value after processing via Linear Function or Polarity Inversion.
Linear Function	When the type is not DI, Counter or DO, it displays the linear function formula.
Unit	When the type is not DI, Counter or DO, it displays the unit of the value.
Update Time	Displays the latest time the value was output or the input value was obtained.
Operation	: Click to configure the IO interface parameters. : Copy the parameters of the current interface to other interfaces of the same type.

Parameter	Description
	••• : Click to perform test actions based on different interface types.

4. Click to configure the IO interface parameters according to different interface types.

For Analog Output (AO)

Parameter	Description
Enable	Enable or disable this interface.
Output Type	Select the output type between Current (4-20mA) and Voltage (0-10V). **CAUTION:** Ensure the type matches the connected device; otherwise, it may damage the gateway or the connected device.
Unit	Select the output value unit.
Output After Reboot	Select the output value for after reboot. **Keep Last Raw Value**: Output the last raw value after reboot. **Custom Raw Value**: Define a custom raw value to output.
Description	For noting this interface.
Linear Function	After enabled, the configured output value will be substituted into the function formula before being output. The formula: `y=a*x+b` (y: present value/configured value, x: raw value/real output value)

For Digital Output (DO)

Parameter	Description
Enable	Enable or disable this interface.

Parameter	Description
Polarity Inversion	Select the polarity inversion status. **Normal**: Open = 0, Close = 1 **Reverse**: Close = 0, Open = 1
Output After Reboot	Select the output value after reboot. **Keep Last Value**: Output the last value before reboot. **Closed/Open**: Select the desired value to output.
Description	For noting this interface.

For Digital Input (DI)

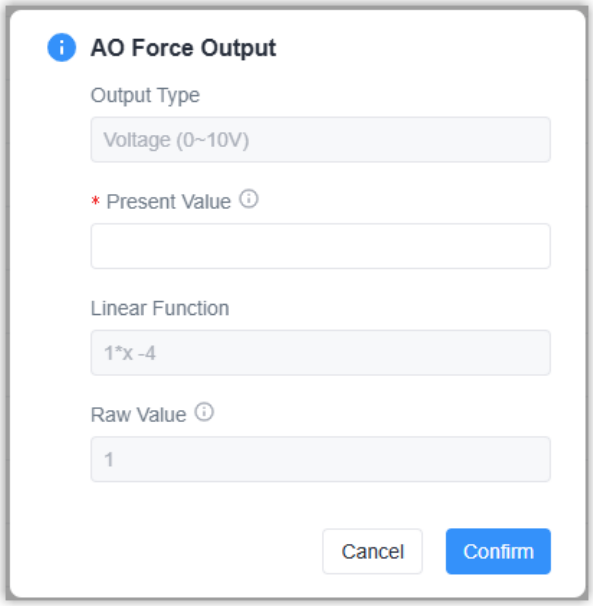
Parameter	Description
Enable	Enable or disable this interface.
Input Type	Select the input type from Level Status or Counter.
Description	For noting this interface.
Input Type is Level Status	
Filter Time	The present value will update only when the changed level status persists for longer than this time.
Polarity Inversion	Select the polarity inversion status. **Normal**: Low Level = 0, High Level = 1 **Reverse**: High Level = 0, Low Level = 1
Input Type is Counter	
Trigger Condition	Select the triggering condition for incrementing he count value.
Filter Time	The count value will increment by 1 only when the changed level status persists for longer than this time.
Trigger Count	When the count value reaches this value, a packet will be reported to the MQTT broker.

For Universal Input (UI)

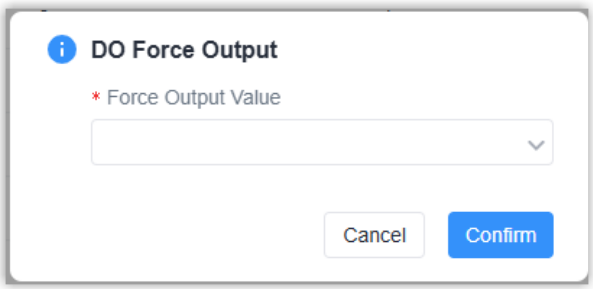
Parameter	Description
Enable	Enable or disable this interface.
Input Type	Select the input type among these options: Voltage (0-10V), Current (4-20mA), Resistance 1000Ω, Resistance 2000Ω, NTC 10K Type2, NTC 10K Type3, NTC 20K, Pt1000, Ni1000, DI. **CAUTION:** Ensure the type matches the connected device; otherwise, it may damage the gateway.
Collection Interval	Define the interval to collect data from the terminal device. Range: 1-86400 s.
Description	For noting this interface.
Input Type is DI	
High-Level Threshold	When the external voltage exceeds this threshold, the DI is determined to be at a high level. Range: 2-24V.
Low-Level Threshold	When the external voltage is below this threshold, the DI is determined to be at a low level. Range: 0-2V.
Polarity Inversion	Select the polarity inversion status. **Normal**: Low Level = 0, High Level = 1 **Reverse**: High Level = 0, Low Level = 1
Input Type is not DI	
Unit	Select the input value unit.
Linear Function	After enabled, the collected value will be substituted into the function formula before display. The formula: `y=a*x+b` (y: present value, x: raw value/real collected value)
Single Lead Resistance	For Pt1000 or Ni1000 sensors, enter the lead resistance value to prevent the leads from affecting accuracy.

5. Click **Save** to save above settings.

6. Click ••• to take some actions to test the IO interfaces.
   - For AO type, click **Force Output** to define a value to output.



   - For DO type, click **Force Output** to set the output status to Closed or Open.



   - For UI type, click **Get Value** to read the value immediately.
   - For DI-Count type, click **Reset** to reset the count value.

Device Access Network

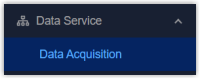
This chapter describes how to configure the network for collecting data from terminal devices.

Configure LoRaWAN® Network

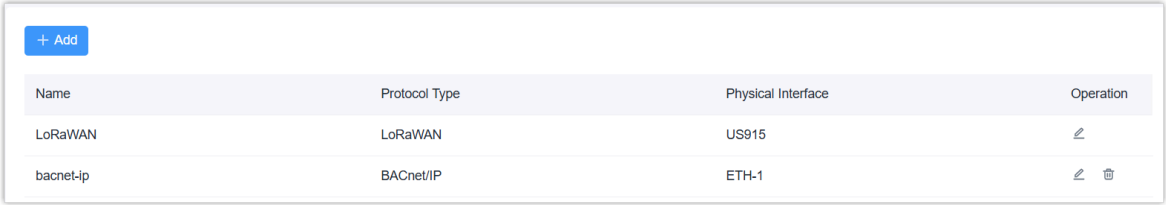
The LoRaWAN® Network is preloaded by default and cannot be deleted.

Steps:

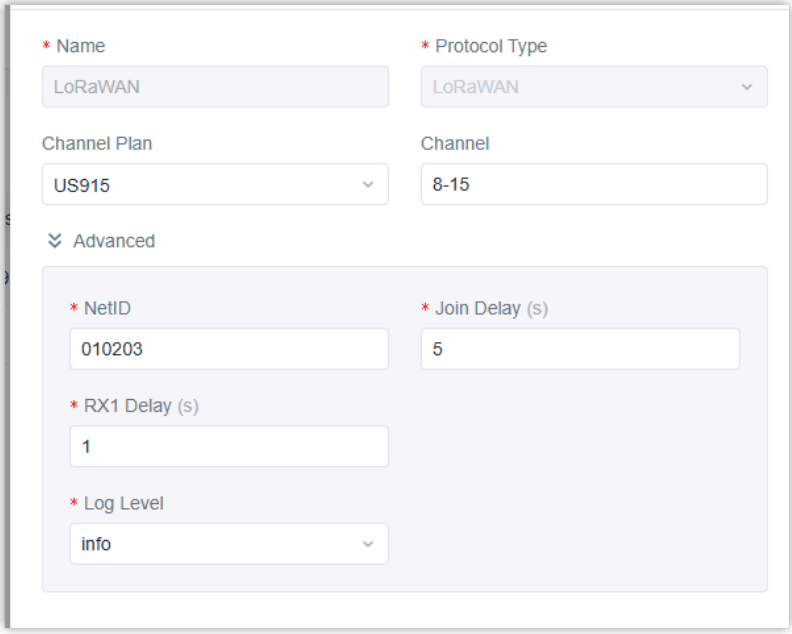
1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device Access Network** tab.



3. Click to select the channel plan. Other parameters can retain their default values or be customized as needed.



Parameter	Description
Channel Plan	Select the channel plan of the network. The options vary by model: -868M: EU868, IN865, RU864 -915M: AU915, US915, KR920, AS923-1/2/3/4 -470M: CN470
Channel	Allow end devices to communicate via specific frequency channels by entering the channel indexes. Examples:

Parameter	Description
	1,40: Enable Channel 1 and 40 1-40: Enable Channel 1-40 1-40, 60: Enable Channel 1-40 and 60 Null: Enable all channels
Additional Channels	Click **Add** to add channels not defined by the LoRaWAN® Regional Parameters. This feature only works with channel plans other than US915/AU915/CN470.
Advanced	
NetID	The unique identifier used by end devices to identify the network server.
Join Delay	Define the interval during which the end device waits for the Join Accept message after sending the Join Request.
RX1 Delay	Define the delay time after which the end device waits for the first receive window (RX1) to open.
Log Level	Select the level for recording logs.

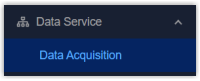
4. Click **Save** to save the settings.

Add Device Access Network

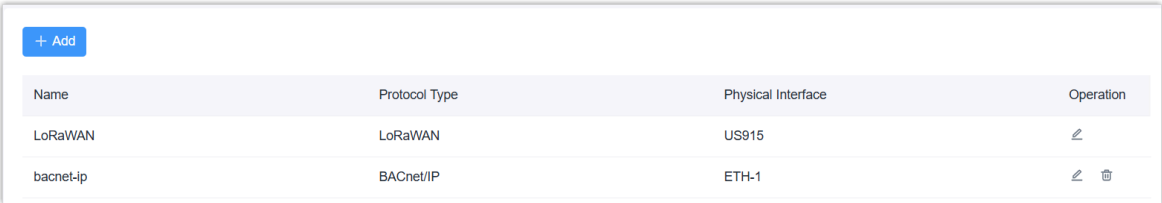
The device supports adding various types of network.

Steps:

1. On the left bar, select **Data Service > Data Acquisition** page.



2. On the top bar, select **Device Access Network** tab.



3. Click **+Add** to add a new network and configure the basic parameters.

Parameter	Description
Name	Define a unique name for the network.
Protocol Type	Select the protocol type based on the terminal devices: BACnet/IP, BACnet MS/TP, Modbus RTU, Modbus TCP, Modbus RTU over TCP, KNX/TP.

4. Configure the network parameters according to the protocol type.

BACnet/IP

Parameter	Description
Network Interface	Select network interface for communicating with other BACnet/IP terminal devices.
Advanced	
Device Instance Nr	Define the unique identifier of the gateway in the BACnet/IP network.
UDP Port	Set the communication port.
Timeout	Define the time to wait for terminal devices to respond after sending commands each time.
Retry times	Define the number of retries for send commands to terminal devices if there is no response.
Keep Alive Interval	Define the interval for sending heartbeat packets to terminal devices to check their online/offline status. If there is no response after 3 attempts, the terminal device will be considered Offline.

BACnet MS/TP

Parameter	Description
Physical Interface	Select the RS485 interface for connecting to BACnet MS/TP terminal devices.
Baud Rate	Select the serial data transmission rate.
Data Bits	The number of data bits for each character. It is fixed at 8.
Stop Bits	Indicates the end of each data frame, enabling the receiver to determine if a frame is complete. Options: 1, 2

Parameter	Description
Parity	This is used to detect errors during transmission. Options: None, Odd, Even.
DIP	Enable or disable to add a 120Ω termination resistor across terminals A and B, eliminating signal reflections from the cable ends.
Advanced	
Device Instance Nr	Define the unique identifier of the gateway within the BACnet MS/TP network.
MAC Address	Define the unique MAC address of the gateway within the BACnet MS/TP network. Range: 0-127
Max Master	Define the highest MAC address that a device will search for when looking for other masters on the network.
Max Info Frames	Define the maximum number of data frames a device can send before passing the token another device on the network.
Timeout	Define the time to wait for terminal devices to respond after sending commands each time.
Retry times	Define the number of retries for send commands to terminal devices if there is no response.
Keep Alive Interval	Define the interval for sending heartbeat packets to terminal devices to check their online/offline status. If there is no response after 3 attempts, the terminal device will be considered Offline.

Modbus TCP or Modbus RTU over TCP

Parameter	Description
Timeout	Define the time to wait for terminal devices to respond after sending commands each time.
Retry times	Define the number of retries for send commands to terminal devices if there is no response.

Parameter	Description
Keep Alive Interval	Define the interval for sending heartbeat packets to terminal devices to check their online/offline status. If there is no response after 3 attempts, the terminal device will be considered Offline.

Modbus RTU

Parameter	Description
Physical Interface	Select the RS485 interface for connecting to Modbus server (slave) devices.
Baud Rate	Select the serial data transmission rate.
Data Bits	The number of data bits for each character. It is fixed at 8.
Stop Bits	Indicates the end of each data frame, enabling the receiver to determine if a frame is complete. Options: 1, 2
Parity	This is used to detect errors during transmission. Options: None, Odd, Even.
DIP	Enable or disable to add a 120Ω termination resistor across terminals A and B, eliminating signal reflections from the cable ends.
Advanced	
Timeout	Define the time to wait for terminal devices to respond after sending commands each time.
Retry times	Define the number of retries for send commands to terminal devices if there is no response.
Keep Alive Interval	Define the interval for sending heartbeat packets to terminal devices to check their online/offline status. If there is no response after 3 attempts, the terminal device will be considered Offline.
Interframe Delay	Define the delay time between two consecutive Modbus RTU commands.

KNX/TP

Parameter	Description
Physical Address	Define the unique physical address of the gateway within the KNX bus network.
Advanced	
Timeout	Define the time to wait for terminal devices to respond after sending commands each time.
Retry times	Define the number of retries for send commands to terminal devices if there is no response.
Keep Alive Interval	Define the interval for sending heartbeat packets to terminal devices to check their online/offline status. If there is no response after 3 attempts, the terminal device will be considered Offline.

5. Click **Save** to save the settings.
6. Click to edit the network parameters, or click to delete the network if needed.

LoRaWAN

Gateway Fleet

This chapter describes how to add agent gateways to this device.

Overview

Milesight LoRaWAN® gateways can form a multi-gateway architecture using the Gateway Fleet function, enabling different gateways to provide failover for each other, extend signal coverage, and allow a single sensor to roam across multiple gateways. One gateway (referred to as the Controller Gateway) can act as the network server, while other gateways (referred to as Agent Gateways) function solely as packet forwarders and transmit all data packets to the Controller Gateway.

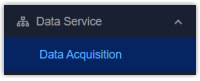
The EG71 can act as a Controller Gateway to receive data from other Milesight LoRaWAN® gateways.

Prerequisites

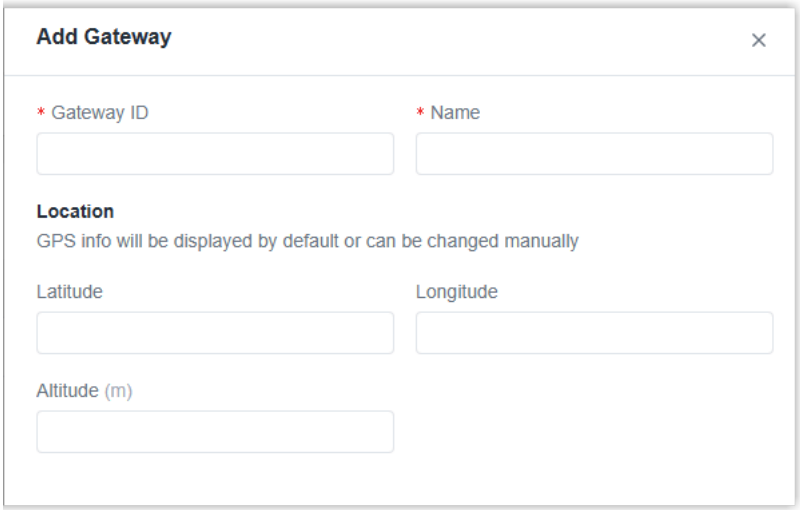
- Agent Gateway: Any other Milesight LoRaWAN® gateways other than the EG71
- The EG71 gateway has a public IP address or is reachable by other gateways.

Add Agent Gateway

1. On the left bar, select **Data Service > Data Acquisition** page.

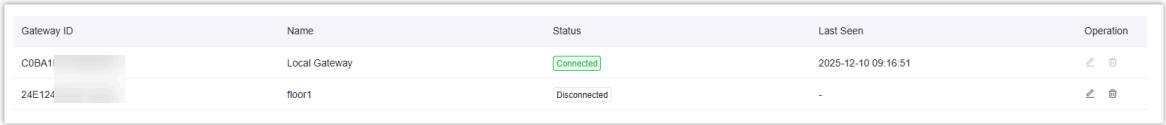


2. On the top bar, select **LoRaWAN** tab, then select **Gateway Fleet** tab.
3. Click **+Add** to add an agent gateway.
4. Configure the agent gateway parameters, click **Save**.



Parameter	Description
Gateway ID	This can be found on the Packet Forward configuration page of agent gateway.
Name	Define a recognizable name for the agent gateway.
Location	Enter the gateway's latitude, longitude, and altitude. If the agent gateway supports GPS, the location information will be updated automatically here.

5. Select the packet forward type of the agent gateway to **Remote Embedded NS** and configure the server address as the EG71 gateway's address. For details, please refer to the corresponding gateway user guides.
6. Check connection status of the agent gateway.



Gateway ID	Name	Status	Last Seen	Operation
C0BA1	Local Gateway	Connected	2025-12-10 09:16:51	
24E124	floor1	Disconnected	-	

7. Click to edit the gateway info or click to delete the gateway as required.

Device Profiles

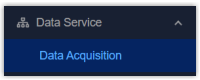
Device profiles define the capabilities of LoRaWAN® end devices and network joining parameters. The gateway provides eight types of profiles for most devices. If these profiles are not compatible with your devices, refer to this chapter to add and manage custom device profiles.

Prerequisites

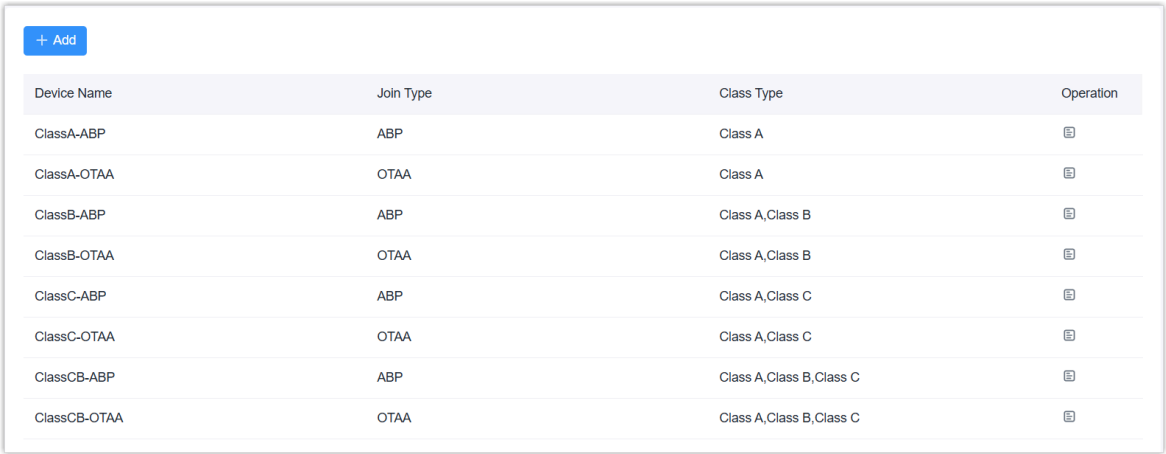
Obtain profile parameters from end device vendors.

Steps

1. On the left bar, select **Data Service > Data Acquisition** page.



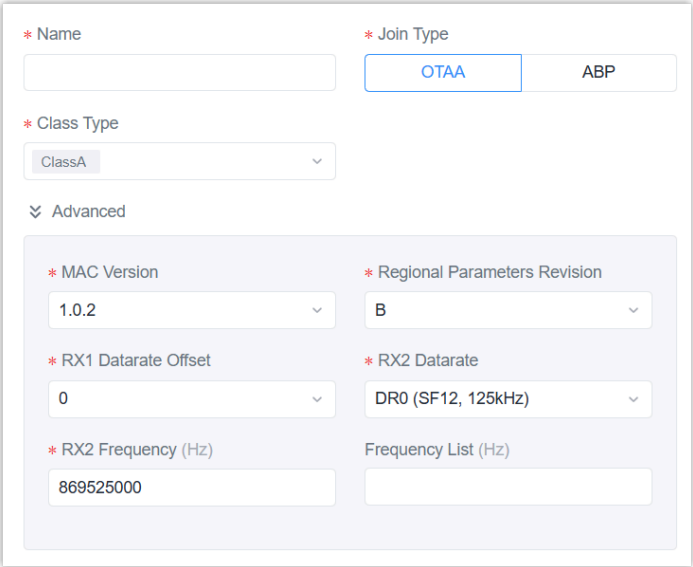
2. On the top bar, select **LoRaWAN** tab, then select **Device Profiles** tab.
3. Click to check the details of default profiles.



+ Add

Device Name	Join Type	Class Type	Operation
ClassA-ABP	ABP	Class A	
ClassA-OTAA	OTAA	Class A	
ClassB-ABP	ABP	Class A,Class B	
ClassB-OTAA	OTAA	Class A,Class B	
ClassC-ABP	ABP	Class A,Class C	
ClassC-OTAA	OTAA	Class A,Class C	
ClassCB-ABP	ABP	Class A,Class B,Class C	
ClassCB-OTAA	OTAA	Class A,Class B,Class C	

If all not matching your devices, click **+Add** to add a new profile and configure the parameters.



Parameter	Description
Name	Define a unique device profile name.
Join Type	Select OTAA or ABP.
Class Type	Select Class B or Class C. Class A is permanently enabled.
Advanced	
MAC Version	Select the MAC Version of the end devices.
Regional Parameters Revision	Select the regional parameters version identifier for this profile..
RX1 Datarate Offset	The offset used to calculate the RX1 data rate based on the uplink data rate.
RX2 Datarate	The data rate of RX2 window.
RX2 Frequency	The frequency of RX2 window.
Frequency List	Enter the factory-preset frequency values provided by the device vendor as a comma-separated list.
Device Channel	Allow end devices to communicate via specific frequency channels by entering the channel indexes. This feature only works with CN470/US915/AU915 channel plans. Examples: 1,40: Enable Channel 1 and 40 1-40: Enable Channel 1-40

Parameter	Description
	1-40, 60: Enable Channel 1-40 and 60 Null: Enable all channels **Tip:** Set this value to 8-15 when using the default settings for Milesight end devices.
Ping Slot Periodicity	The period during which Class B end devices open the ping slot to receive messages.
Ping Slot Data Rate	The data rate to receive downlinks for class B devices.
Ping Slot Frequency	The frequency to receive downlinks for class B devices.
Class B ACK Timeout	The time to wait for a downlink response from class B devices. If no response is received within this time, the gateway will retransmit the downlink command.
Class C ACK Timeout	The time to wait for a downlink response from class C devices. If no response is received within this time, the gateway will retransmit the downlink command.

4. Click **Save** to save the profile.
5. Click to edit the custom profile, or click to delete the custom profile.

Multicast

By creating a multicast group, you can send a single downlink payload to a group of devices sharing the same multicast address, session-keys and frame-counter. This chapter describes how to add and use the multicast groups.

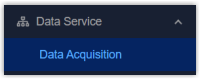
Prerequisites

Ensure all LoRaWAN® end devices in the same group meet the following conditions:

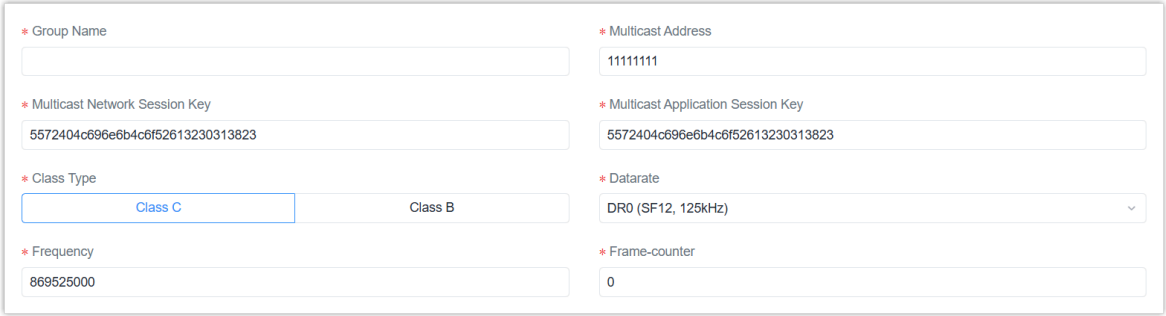
- Support the Multicast feature.
- Be configured with the same parameters: Class Type (Class B or Class C), Multicast Address, Multicast McNetSkey, Multicast McAppSkey, RX2 Datarate, RX2 Frequency, and application port.
- Have been added to this gateway.

Steps

1. On the left bar, select **Data Service > Data Acquisition** page.

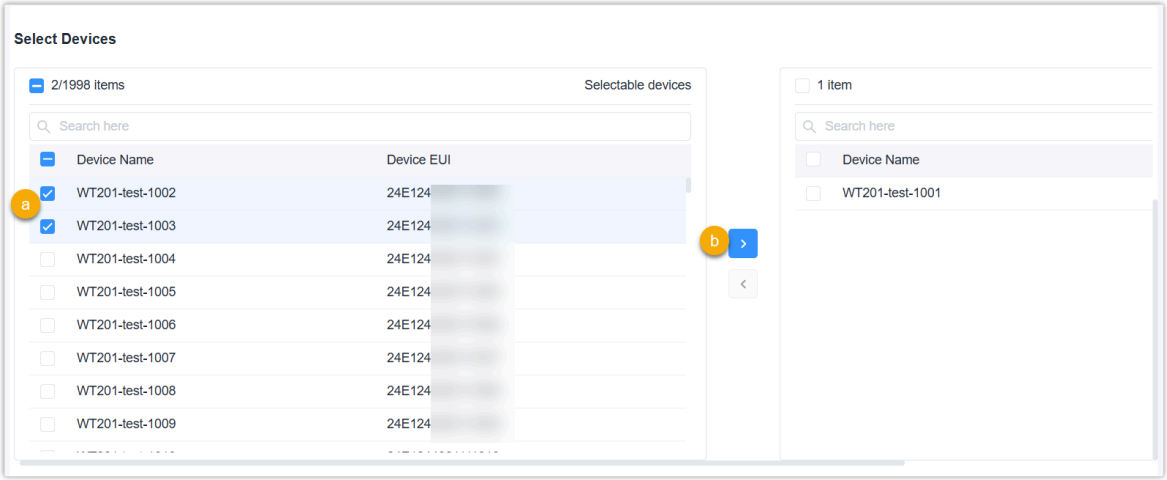


2. On the top bar, select **LoRaWAN** tab, then select **Multicast** tab.
3. Click **+Add** to add a group and configure the related parameters.

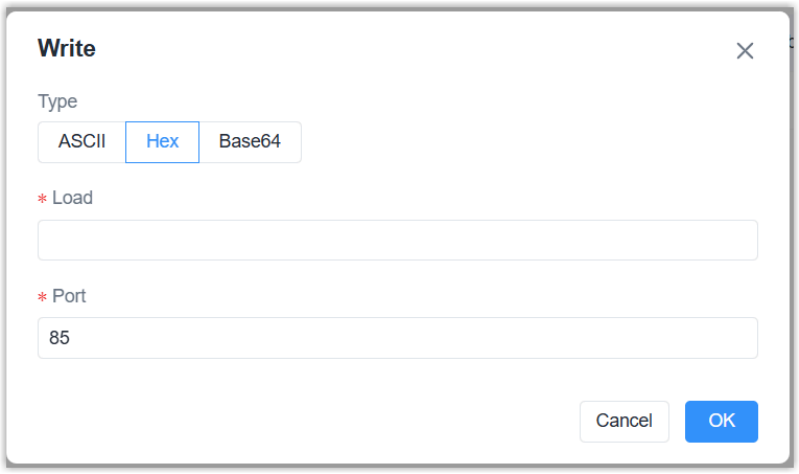


Parameter	Description
Group Name	Define a unique name for the multicast group.
Multicast Address	Define a unique 8-digit address used to distinguish between different multicast groups.
Multicast Network Session Key	The network session key (Netwks Key) for all devices in this group.
Multicast Application Session Key	The application session key (AppSKey) for all devices in this group.
Class Type	Class B or Class C is optional.
Datarate	The RX2 datarate used by end devices to receive downlink payloads.
Frequency	The RX2 frequency used by end devices to receive downlink payloads.
Frame-Counter	The number of data frames received via downlink packets. It is incremented automatically by the gateway.
Ping Slot Periodicity	The period for end devices to open the ping slot to receive messages for class B devices.

4. Select the devices to add to this multicast group. Typically, select devices of the same model.



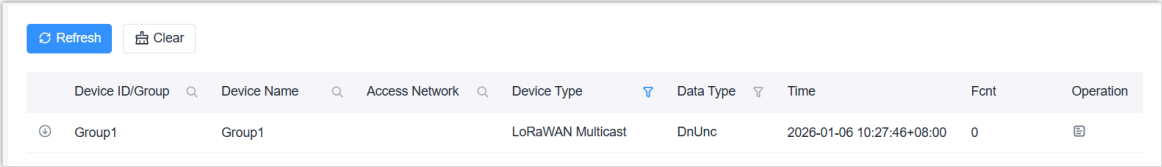
5. Click **Apply** to save the settings.
6. Select a group from the group list, click to configure a downlink payload.



Parameter	Description
Type	Select the downlink payload type.
Load	Define the downlink payload based on the corresponding type.
Port	Define the application port for the end devices.

7. Click **OK** to send the downlink payload.

8. Navigate to **Data Service > Data Stream** to check downlink sending status.



FUOTA

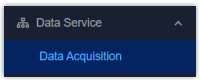
Firmware Update Over the Air (FUOTA) is a standard for distributing firmware updates to LoRaWAN® end devices using unicast or multicast. This chapter describes how to upgrade the end devices.

Prerequisites

- The end device supports the standard FUOTA protocol or has been updated to support FUOTA.
- The end devices has been added to the gateway.

Steps

1. On the left bar, select **Data Service > Data Acquisition** page.

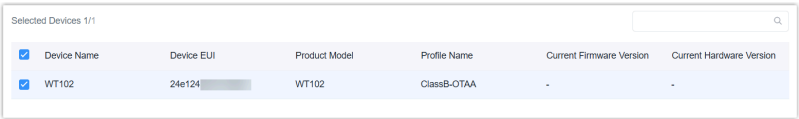


2. On the top bar, select **LoRaWAN** tab, then select **FUOTA** tab.
3. Click **+Add** to add a FUOTA task and configure the related parameters.

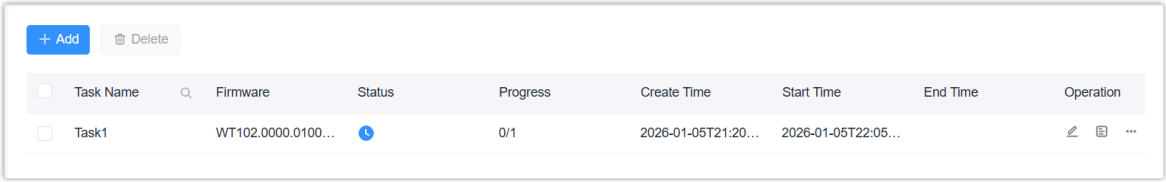
Parameter	Description
Task Settings	
Task Name	Define a unique name for the FUOTA task.
Start Time	Select the time to start this task.
Description	For noting this task.
Firmware Setting	
Firmware	Import the firmware to upgrade. **Upload:** Click to select the firmware from the local path. **Select an official firmware file:** Select the firmware to download from the official website. This requires the gateway to have Internet access.

Parameter	Description
Fragment Size	The firmware file will be split into segments of this size for distribution to devices. Typically, retain the default value. If the network environment is complex or bad, it is suggested to reduce this value to 64 or a lower value; if the network environment is good, this value can be increased to improve transmission speed.
Fragment Interval	The interval to assign firmware fragments to devices. Typically, retain the default value. If the network environment is complex or bad, it is suggested to increase this value to 7-10s or a higher value; if the network environment is good, this value can be decreased to improve transmission speed.
Redundancy Percent	The device will send 30% redundant packets for firmware packet correction. Typically, retain the default value. If the network environment is complex or bad, it is suggested to increase this value to 40%-50% or a higher value to improve transmission success; if the network environment is good, this value can be reduced.
Multicast Setting	
Datarate	Datarate to assign the firmware fragments to devices.
Frequency	Downlink frequency to assign the firmware fragments to devices.

4. Select the devices to execute this task. Please select the devices with the same model.



5. Click **Apply** to save the settings.
6. Check the task status on the list.



Parameter	Description
Task Name	Displays the task name.
Firmware	Displays the firmware to upgrade in this task.
Status	Displays the task status. **Pending:** Wait for the scheduled time to process the task. **Waiting:** Preparing to create a session for the upgrade. **Executing:** At least one device replies the upgrade result. **Finished:** All devices reply the upgrade results including success and failure.
Progress	Displays the number of devices in upgraded/planned status.
Create Time	Displays the time to create this task.
Start Time	Displays the time to start this task.
End Time	Displays the time to complete this task.
Operation	: Edit this task when task status is Pending. : Check task details, including the success and failure status of every device. : Click **Update** to retry the task for devices that failed to upgrade when task status is Finished, click **Delete** to delete this task when task status is Pending or Finished.

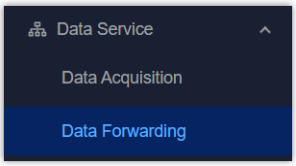
Data Forwarding

This chapter describes how to forward data to external servers (clients).

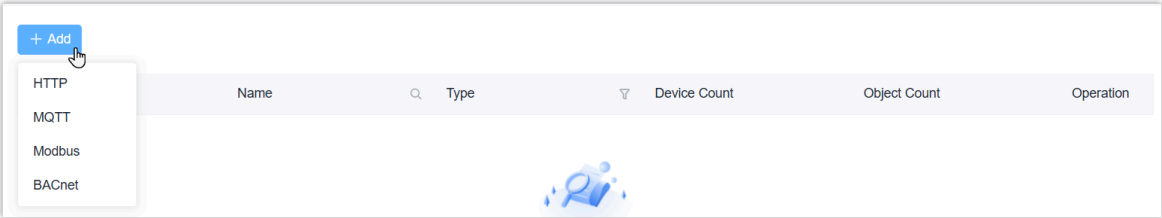
Add Data Forwarding Rules

The gateway supports connecting to HTTP/MQTT servers or working as BACnet/Modbus servers to forward the data or receive the downlink control commands.

1. On the left bar, select **Data Service > Data Forwarding** page.



2. Click **+Add** and select the protocol from HTTP, MQTT, Modbus and BACnet.



3. Configure the related parameters according to the protocol.

HTTP

Parameter	Description
Enable	Enable or disable to forward data to a HTTP(s) server.
Name	Define a unique name for this data forwarding rule.
Description	For noting this data forwarding rule.
Metadata	After enabled, the gateway will add selected items to forwarding content for Uplink Data.
HTTP Header	Click **Add** to add an HTTP header name and value.
URL	Set the URL starting with `http://` or `https://` to send different types of data. For more details, refer to MQTT&HTTP Application Guide. **Data Up:** Normal data uplinks. **ACK Notification:** ACK notification after sending confirmed downlink commands to LoRaWAN® devices. **Error Notification:** Device error notification. **Online Notification:** Device online notification. **Offline Notification:** Device offline notification.

MQTT

Parameter	Description
Enable	Enable or disable to set up the communication with a MQTT broker.
General	
Name	Define a unique name for this data forwarding rule.
Description	For noting this data forwarding rule.
Broker Address	The IP address or domain name of the MQTT broker.
Broker Port	The service port of the MQTT broker.
Client ID	The unique identifier of the gateway.
Connection Timeout	If the gateway does not get a response after the connection timeout, the connection will be considered as broken.
Keep Alive Interval	The interval to send heartbeat packets regularly to keep alive.
User Credentials	Enable or disable to authenticate with username and password. **Username:** The username for authentication. **Password:** The password for authentication.
TLS	Enable or disable TLS authentication. **SSL Security:** After enabled, the gateway will verify the certificate's validity. **Mode:** Select the certificate mode as **CA Signed Server Certificate** to use preloaded certificates, or **Self Signed Certificates** to import the custom CA certificates(.crt or .pem), client Certificates(.crt) and client key(.key) for verification.
Data Retransmission	When enabled, it supports storing up to 10,000 pieces of data when the network is disconnected and re-transmits the data after network recovery.
Data	
Data Format	Select the report format for uplink object data.

Parameter	Description
	Combined: Report all object data in a single message. **Per Object:** Report each object's data separately.
Metadata	After enabled, the gateway will add selected items to forwarding content for Uplink Data.
Topic	
Data Type	The data type to communicate with MQTT broker. For more details, refer to MQTT&HTTP Application Guide. **Uplink Data:** Receive device uplink packets. If you need to limit the received content, add wildcards "$gatewaySN", "$deviceName", "devEUI", "deveui", "objectID", "objectName" to this topic and replace them with the actual values when subscribing to this topic. **Downlink Data:** Send downlink commands to devices. If you require to send downlink command to specific device or object, add wildcards “gatewaySN”, “$devEUI”, "devui", "$deviceID" or "$objectID" to this topic and replace them with the actual values when subscribing to this topic. **Multicast Downlink Data:** Send downlink commands to LoRaWAN® multicast group. **Online Notification:** Receive device online notification. **Offline Notification:** Receive device offline notification. **ACK Notification:** Receive ACK notification after sending confirmed downlink commands to LoRaWAN® devices. **Error Notification:** Receive device error notification. **Management Request:** Send a blank packet to enquire the device and object info added to this data forwarding rule. **Management Response:** Receive the device and object info (include count, name, and ID) added to this data forwarding rule after sending request to Management Request topic.
Topic	Topic name of the data type used for publishing.
QoS	QoS0, QoS1 or QoS2 is optional.

Parameter	Description
Retain	Enable or disable to set the latest message of this topic as retain message.
Will	
Will	Enable or disable sending will message. The last will message will be sent automatically when the MQTT client is abnormally disconnected. It is typically used to send device status information or notify other devices or proxy servers of the device's offline status.
Will Topic	The topic to receive last will messages.
Will QoS	QoS0, QoS1 and QoS2 are optional.
Will Retain	Enable or disable to set last will message as retain message.
Will Message	Customize the content of the last will message.

Modbus

Parameter	Description
Enable	Enable or disable to this Modbus server (slave).
Name	Define a unique name for this data forwarding rule.
Port	The communication port of this server.
Connection Type	Select the connection type with the remote Modbus client (master). **Modbus TCP:** The Modbus client sends Modbus TCP-format commands to this Modbus server. **Modbus RTU over TCP:** The Modbus client sends Modbus-RTU format commands to this Modbus server.
Network Interface	Select the network interface for this server to communicate with Modbus clients (masters). After saving the settings, the IP address of this interface will display.
Server ID	Define a unique ID to identify this server.
Description	For noting this data forwarding rule.

Parameter	Description
Global Object	Once enabled, the selected global objects will be automatically added to the forwarding object when adding device objects.

BACnet

Parameter	Description
Enable	Enable or disable this BACnet/IP server.
Name	Define a unique name for this data forwarding rule.
UDP Port	The communication port of this server.
Network Interface	Select the network interface for this server to communicate with BACnet clients.
Device Instance Nr	Define a unique ID to identify this server within the BACnet network.
Device Name	Define a unique name to identify this server in the BACnet network.
Description	For noting this data forwarding rule.
Global Object	Once enabled, the selected global objects will be automatically added to the forwarding object when adding device objects.
BBMD	
BBMD	Enable BBMD (BACnet/IP Broadcast Management Device) if BACnet devices of different network subnets should work together.
BBMD Type	Select the BBMD type. **BBMD:** Work as the device to broadcast messages to different network subnets. **Foreign Device Registration:** Register to a BBMD to receive broadcast messages.
Broadcast Distribution Table	Click **Add** to add BBMD or foreign device information (including IP address, port, and subnet mask) to forward messages. At most 10 devices can be added.

Parameter	Description
IP Address	When BBMD type is Foreign Device Registration, set the IP address of BBMD.
IP Port	When BBMD type is Foreign Device Registration, set the UDP/IP port of BBMD.
Registration Interval	When BBMD type is Foreign Device Registration, set the registration interval.

4. Click **Apply** to save the settings.
5. (MQTT Only) In the data forwarding list, click to go to edit page of MQTT data forwarding rule, click **Connect** to set up the connection with MQTT broker.

Add Data Forwarding Objects

The gateway supports defining the forwarding contents to external servers (clients).

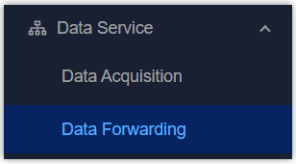
Add Device Objects

After adding the device objects, the object data supports forwarding to HTTP/MQTT servers or being read by Modbus/BACnet clients.

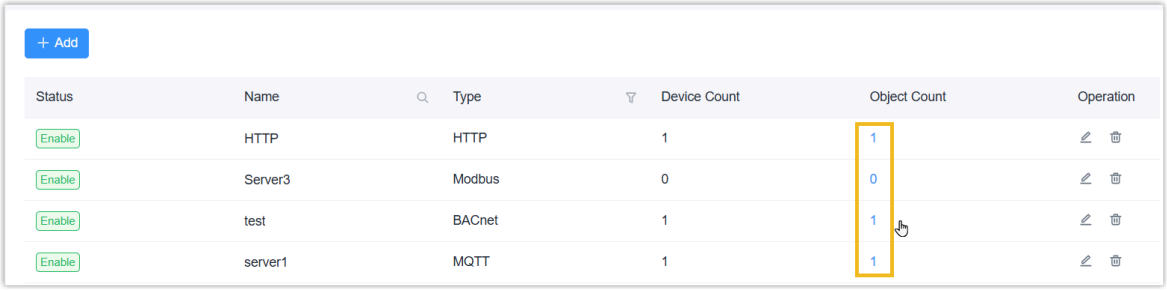
Prerequisites: Enable the IO interfaces or enable the desired device objects.

Steps:

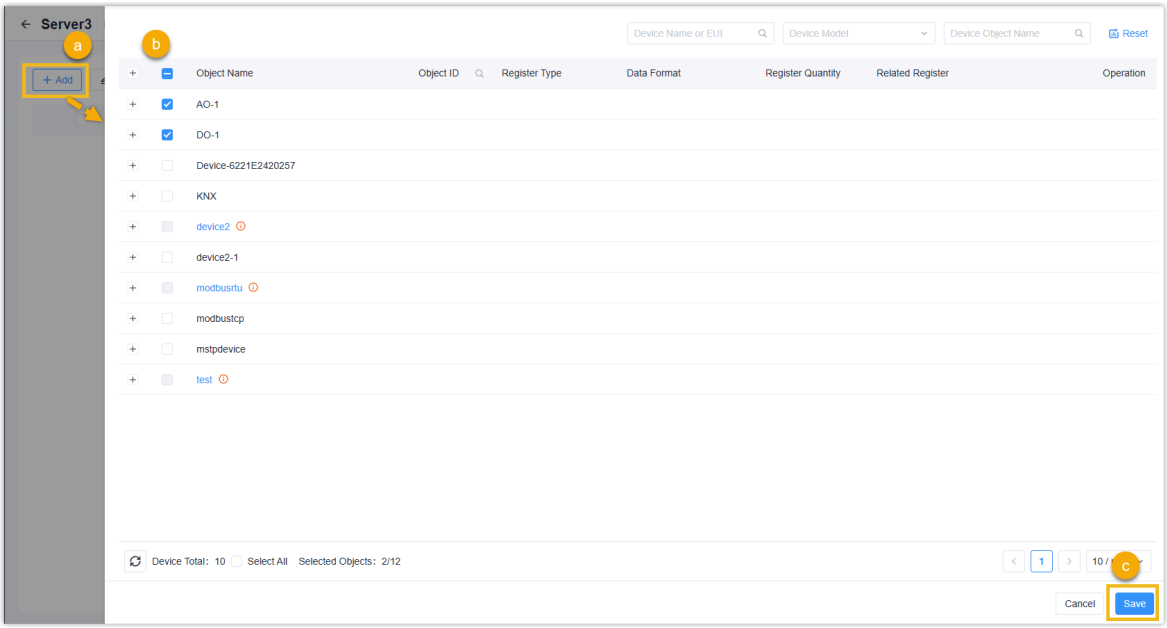
1. On the left bar, select **Data Service > Data Forwarding** page.



2. Select the desired data forwarding rule, click the object count value to go to **Device Object** page.



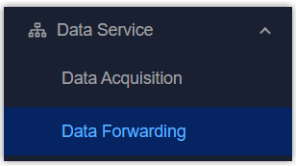
3. Click **+Add** to select the objects to add, then click **Save**. For HTTP/MQTT type, it supports selecting the LoRaWAN® device directly if the device objects are not added.



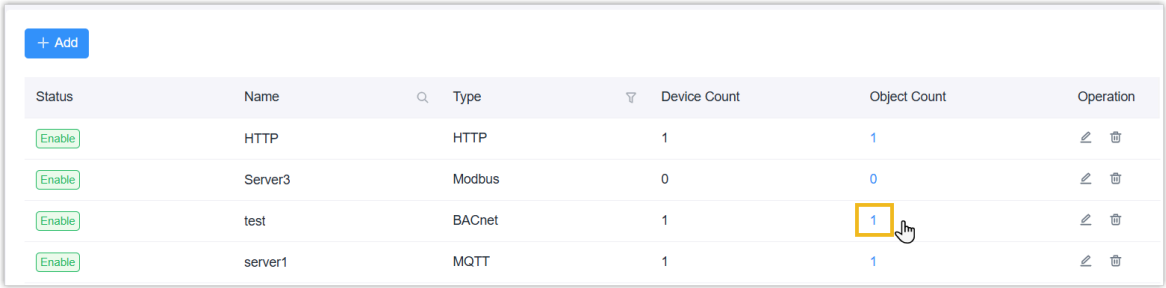
Add NC Object for BACnet Clients

The gateway supports adding notification-class objects to send alarms to BACnet clients.

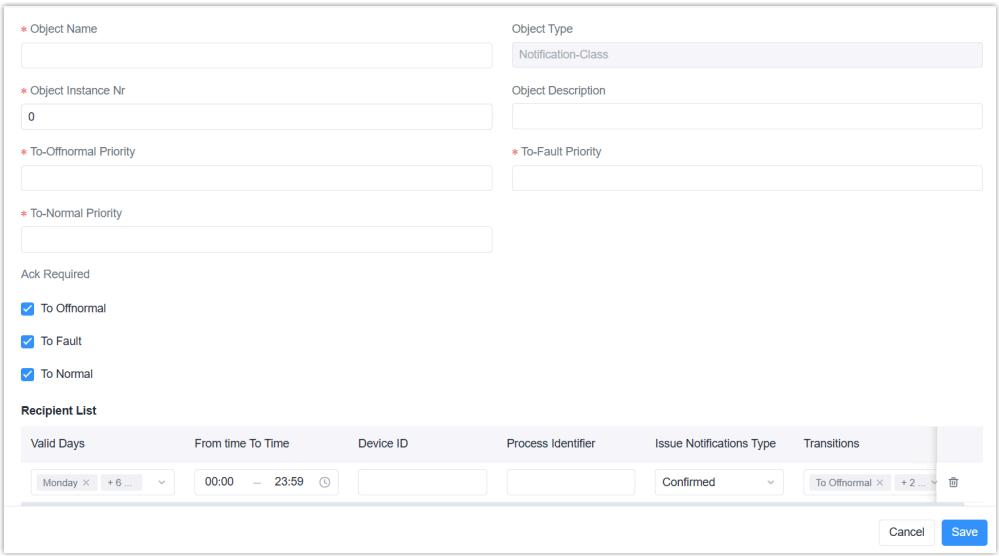
1. On the left bar, select **Data Service > Data Forwarding** page.



2. Select the desired BACnet data forwarding rule, click the object count value to go to **Device Object** page.



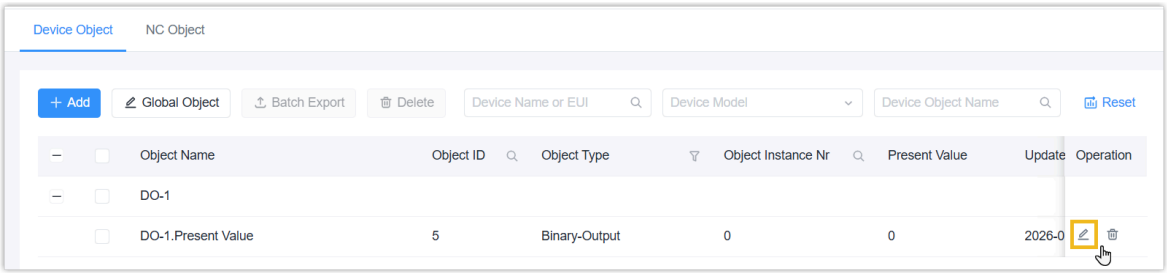
3. On the top bar, select **NC Object** page.
4. Click +Add to add a new notification class object to determine the alarm parameters.



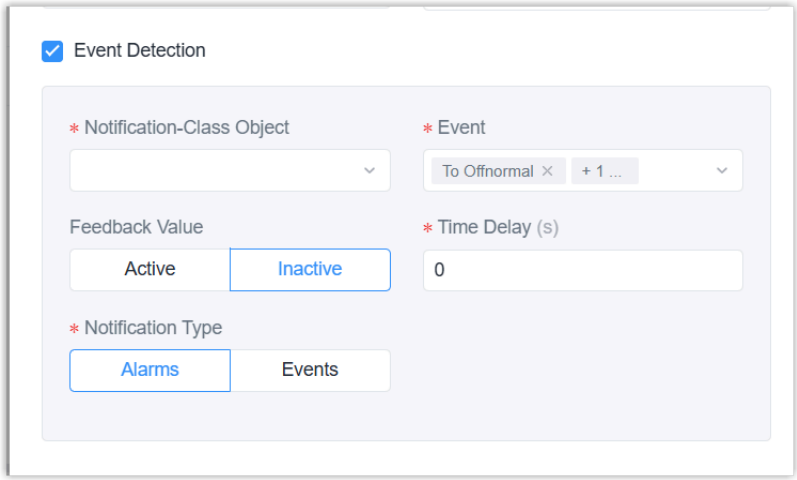
Parameter	Description
Object Name	Define a unique name for this object.
Object Type	It is fixed as Notification-Class.
Object Instance Nr	Set a unique object instance number.
Object Description	For noting this object.
To-Offnormal Priority	Set the priority number used by recipients to sort event notifications. Range: 0-255 (0 being most important, 255 least important)
To-Fault Priority	
To-Normal Priority	
Ack Required	Specify if this event requires the recipient to send the Acknowledgement Alarm message back to gateway.

Parameter	Description
Recipient List	When event is triggered, the event notification will be sent to recipients in this list. One list supports to add 10 recipients at most. **Valid Days:** Valid days to send notifications. **From time to time:** Valid time to send notifications. **Device ID:** The target recipient device ID. **Process Identifier:** An identifier indicating which process the alarm is intended for. For example, maybe process identifier 1 means maintenance alarms, 2 means critical alarms and 3 means life safety alarms, etc. **Issue Notifications Type:** Select the notification type as confirmed or unconfirmed. If the gateway does not receive a response to the Confirmed notification, it will send the notification once again. **Transitions:** select the reported event types.

5. Click **Save** to save the NC object settings.
6. On the top bar, select **Device Object** page.
7. Select the desired object, click to edit this object.



8. Enable the **Event Detection** and configure the related parameters. This feature is supported for all object types except for Character String Value.



Parameter	Description
Notification-Class Object	Select the notification class to determine the recipients and other alarm configuration.
Event	Select the event type to report.
Time Delay	Only when current value matches the threshold condition or is out of threshold for this time, the device will report the corresponding event.
Notification Type	Select the notification type as Alarms or Events.
Object Type is Analog Input/Output/Value	
Limit Event	Select if reporting the event when reaching the high limit or low limit.
High Limit	Define the high limit threshold value.
Low Limit	Define the low limit threshold value.
Deadband	Under To Offnormal status, when current value returns to (high limit - deadband) value or (low limit + deadband) lasting the delay time, the device will generate To Normal event.
Object Type is Binary Input/Output/Value	
Alarm/Feedback Value	Report To Offnormal event if the current value is equal to this value for delay time; report To Normal event if the current value is not equal to this value for delay time.
Object Type is Multi-State Input/Output/Value	

Parameter	Description
Alarm Value	For Multi-State Input/Value, report To Offnormal event if the current value is equal to alarm value for delay time; report To Normal event if the current value is not equal to alarm value for delay time.
Fault Value	For Multi-State Input/Value, report To Fault event if the current value is equal to fault value.
Feedback Value	For Multi-State Output, report To Offnormal event if the current value is equal to feedback value for delay time; report To Normal event if the current value is not equal to feedback value for delay time.

9. Click **Save** to save the object settings.

Device Library

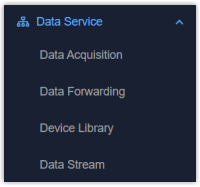
The device supports converting the terminal device data to objects for quick and easy integration. This chapter describes to how update the inbuilt device repository or custom device repository.

Update Inbuilt Device Repository

The device has built-in the repository of Milesight LoRaWAN® end devices.

Steps:

1. On the left bar, select **Data Service > Data Library** page.



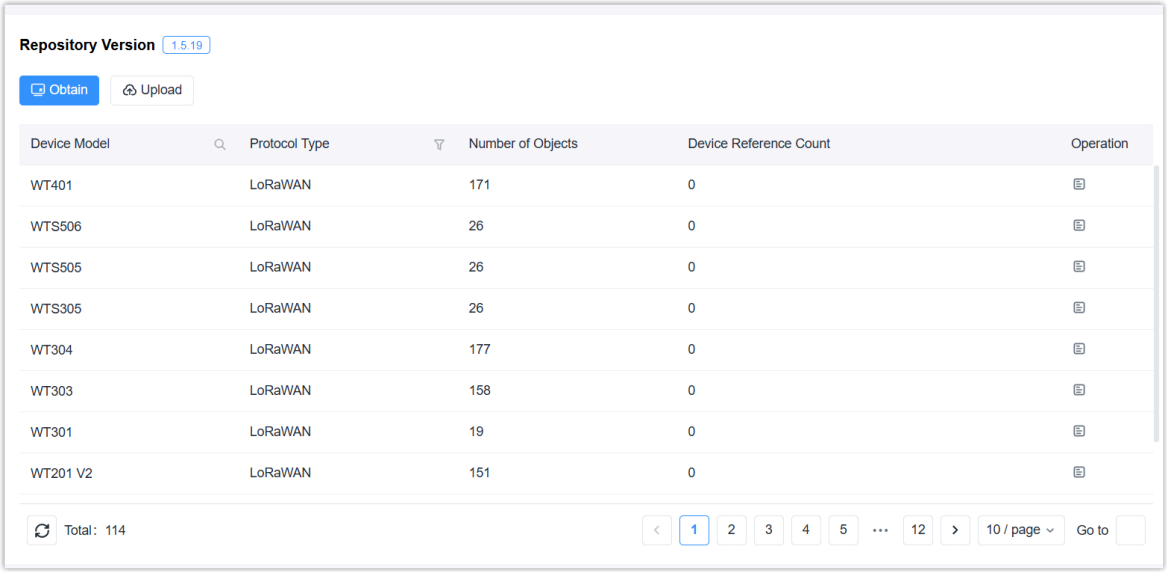
2. On the top bar, select **Inbuilt Device Repository** tab.
3. Update the device repository by the following methods:

   Update Online: Click **Obtain** to update the device repository. This requires the device to access the Internet.

   Update Locally: Click **Upload** to select the repository file from the local path. The latest repository file of Milesight products can be download here.

Note:

Only supports importing versions later than the current version.



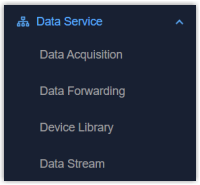
Custom Device Repository

The device can add custom device repository for third-party devices or adding customized content.

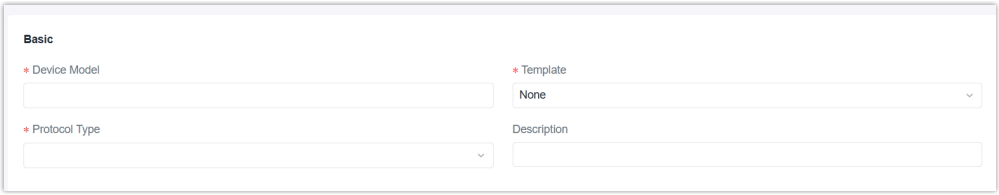
Prerequisites: Obtain the device's communication protocol or encoders/decoders from the device vendor.

Add Device Model Individually

1. On the left bar, select **Data Service > Data Library** page.



2. On the top bar, select **Custom Device Repository** tab.
3. Click **+Add** to add a device repository and configure the basic parameters.

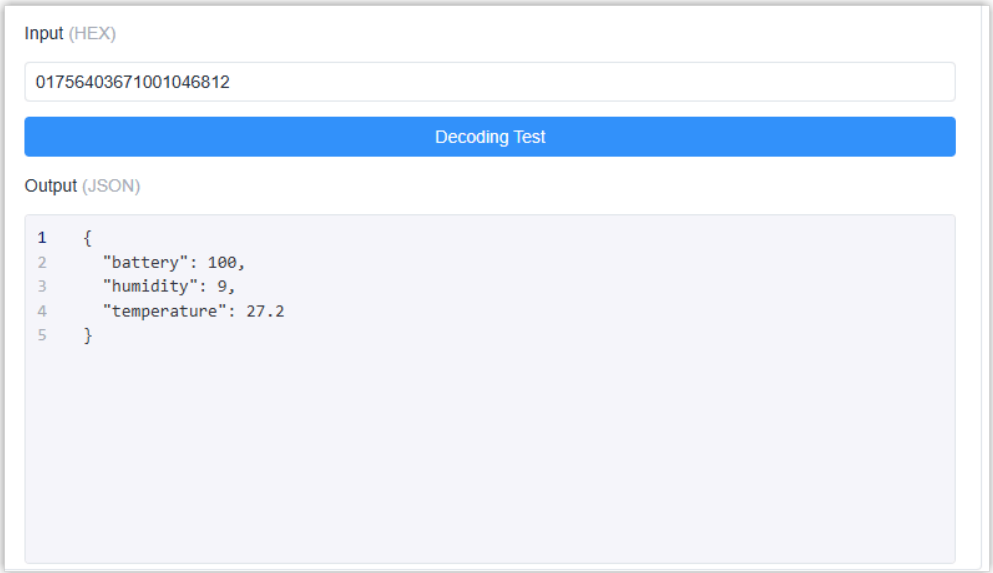


Parameter	Description
Device Model	Set the device model name.
Template	Select a template from inbuilt device repository. This is suitable for adjusting custom content to Milesight LoRaWAN® device models. For third-party devices or other protocol types, select None.
Protocol Type	Select the protocol type of the device model.
Description	For noting this device model.
Protocol type is LoRaWAN®	
DevEUI Prefix (9 chars)	Set the first 9 characters of the device EUI.
Device-Profile	Select the device profile of this model.

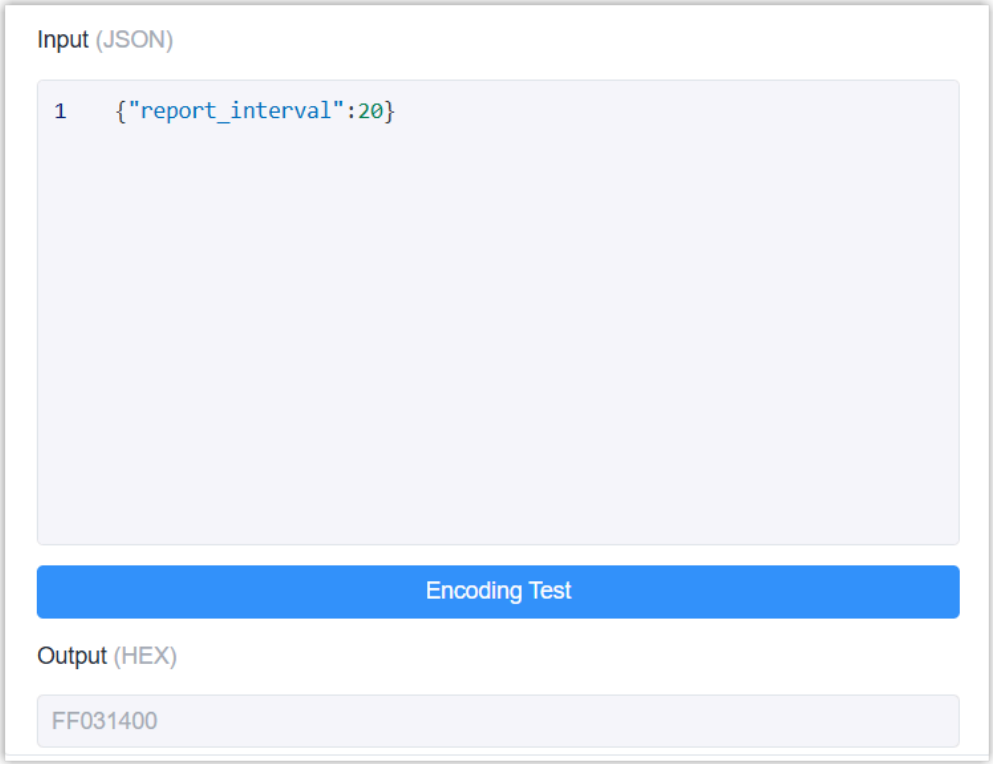
4. Add a payload decoder and encoder for LoRaWAN®-type devices. For other protocol types, skip this step.
   a. Add decoder to decode Hex format raw data to JSON format results; or add encoder to encoder JSON format command to Hex format raw commands. The supported language is JavaScript ES2020.

   > **Note:**
   > If a variable appears in both the decoder and encoder, the variable names used must be identical.

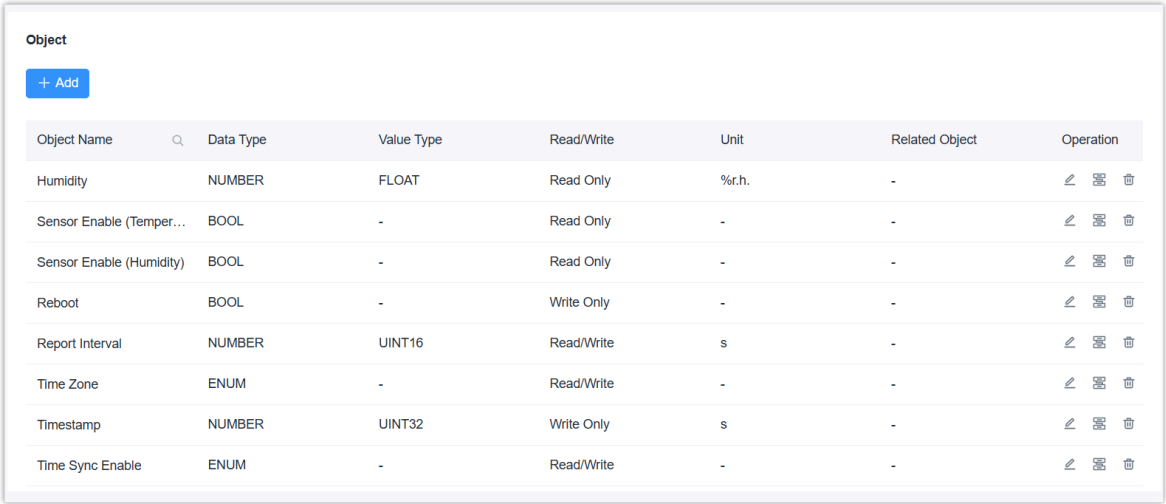
   b. Input a HEX raw data, click **Decoding Test** to check if the decoder works well.



c. Input a JSON format content, click **Encoding Test** to check if the encoder works well.



5. Click **+Add** to add objects. You can also click in the object list to adjust the object parameters in the object list.



Object

+ Add

Object Name	Data Type	Value Type	Read/Write	Unit	Related Object	Operation
Humidity	NUMBER	FLOAT	Read Only	%r.h.	-	
Sensor Enable (Temper…	BOOL	-	Read Only	-	-	
Sensor Enable (Humidity)	BOOL	-	Read Only	-	-	
Reboot	BOOL	-	Write Only	-	-	
Report Interval	NUMBER	UINT16	Read/Write	s	-	
Time Zone	ENUM	-	Read/Write	-	-	
Timestamp	NUMBER	UINT32	Write Only	s	-	
Time Sync Enable	ENUM	-	Read/Write	-	-	

6. Configure the object information according to the protocol type.

LoRaWAN

Parameter	Description
Object Name	Define a unique name for this object.
Object Description	For noting this object.
Data Type	Select the data type of this object and configure the related parameters. **BOOL:** Set the values for the 0 or 1 state. **ENUM:** Set the enumeration count and each enumeration value. **NUMBER:** Select the data value type. **TEXT:** Set the maximum length of the string.
Read/Write	Select the access mode of this object.
BACnet Forward	
BACnet Forward	Enable or disable to convert this object to BACnet object.
Object Type	Select BACnet object type. After selecting the Data Type and Read/Write options, the device matches the object type and parts of BACnet parameters automatically.
Polarity	Select the binary input/output/value status as Normal or Reverse.

Parameter	Description
Active Text	Add the text to indicate the active status for Binary Input/Output/Value types. It is the same as Value 1.
Inactive Text	Add the text to indicate the active status for Binary Input/Output/Value types. It is the same as Value 0.
Number of States	Set the number of status when object type is MultiState type. It is the same as Enumeration Number. **State Text:** Add the text to indicate every status. It is the same as Enumeration Value.
Relinquish Default	Set the default output value for Analog Output, Binary Output, or MultiState Output types.
Modbus Forward	
Modbus Forward	Enable or disable to convert this object to Modbus object.
Register Type	Select the Modbus register type according to the Data Type and Read/Write options. **Discrete Input:** Select for BOOL type and Read-Only access **Coil:** Select for BOOL type **Input Register:** Select for ENUM, NUMBER or TEXT type and Read-Only **Holding Register:** Select for ENUM, NUMBER or TEXT type
Data Format	Select the data type when register type is Input Register or Holding Register.
Register Quantity	Displays the quantity based on the data format.

BACnet/IP or BACnet MS/TP

Parameter	Description
Object Name	Define a unique name for this object.
Object Description	For noting this object.

Parameter	Description
Data Type	Select the object type.
Object Instance Nr	Set a unique object instance number.

Modbus TCP/RTU or Modbus RTU over TCP

Parameter	Description
Object Name	Define a unique name for this object.
Register Type	Select the Modbus register type. **Discrete Input:** Reads on/off values **Coil:** Reads/Writes on/off values **Input Register:** Reads measurements and statuses **Holding Register:** Reads/Writes configuration values
Data Format	Select the data type when register type is Input Register or Holding Register.
Register Quantity	Displays the quantity based on the data format.
Register Address	Set the start address for reading/writing this object's value in the register.
Unit	Select the unit of this value when register type is Input Register or Holding Register.
Object Description	For noting this object.
BACnet Forward	
BACnet Forward	Enable or disable to convert this object to BACnet object.
Object Type	Select BACnet object type. After selecting the Register Type, the device matches the object type automatically.
Polarity	Select the binary input/output/value status as Normal or Reverse.
Active Text	Add the text to indicate the active status for Binary Input/Output/Value types.

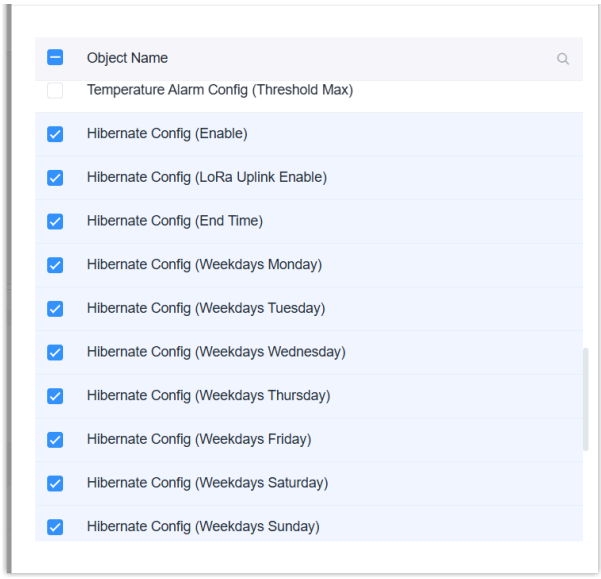
Parameter	Description
Inactive Text	Add the text to indicate the inactive status for Binary Input/Output/Value types.
Number of States	Set the number of status when object type is MultiState type.
State Text	Add the text to indicate every status when object type is MultiState type.
Relinquish Default	Set the default output value for Analog Output, Binary Output, or MultiState Output types.

KNX/TP

Parameter	Description
Object Name	Define a unique name for this object.
Object Description	For noting this object.
Datapoint Type	Select the KNX Data Point Type (DPT) to define the value. If the type is Custom, you need to define the data length.
Unit	Displays the data unit after selecting the datapoint type.
Access Mode	Select the access mode for this object.
BACnet Forward	
BACnet Forward	Enable or disable to convert this object to BACnet object.
Object Type	Select BACnet object type. After selecting the Datapoint Type, the device matches the object type automatically.
Polarity	Select the binary input/output/value status as Normal or Reverse.
Active Text	Add the text to indicate the active status for Binary Input/Output/Value types.
Inactive Text	Add the text to indicate the inactive status for Binary Input/Output/Value types.
Number of States	Set the number of status when object type is MultiState type.

Parameter	Description
State Text	Add the text to indicate every status when object type is Multi-State type.
Relinquish Default	Set the default output value for Analog Output, Binary Output, or MultiState Output types.
Modbus Forward	
Modbus Forward	Enable or disable to convert this object to Modbus object.
Register Type	Select the Modbus register type. After selecting the Datapoint Type, the device matches the register type automatically.
Data Format	Select the data type when register type is Input Register or Holding Register.
Register Quantity	Displays the quantity based on the data format.

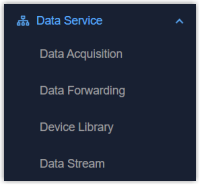
7. Click **Save** to save this object.
8. If an object must be written at the same time as other objects, click in the object list to add related objects.



9. Click **Apply** to save this custom device model.

Add Device Models in Bulk

1. On the left bar, select **Data Service > Data Library** page.



2. On the top bar, select **Custom Device Repository** tab.
3. If there is already at least one custom device repository, select all and click **Batch Export** to export the .ZIP file.

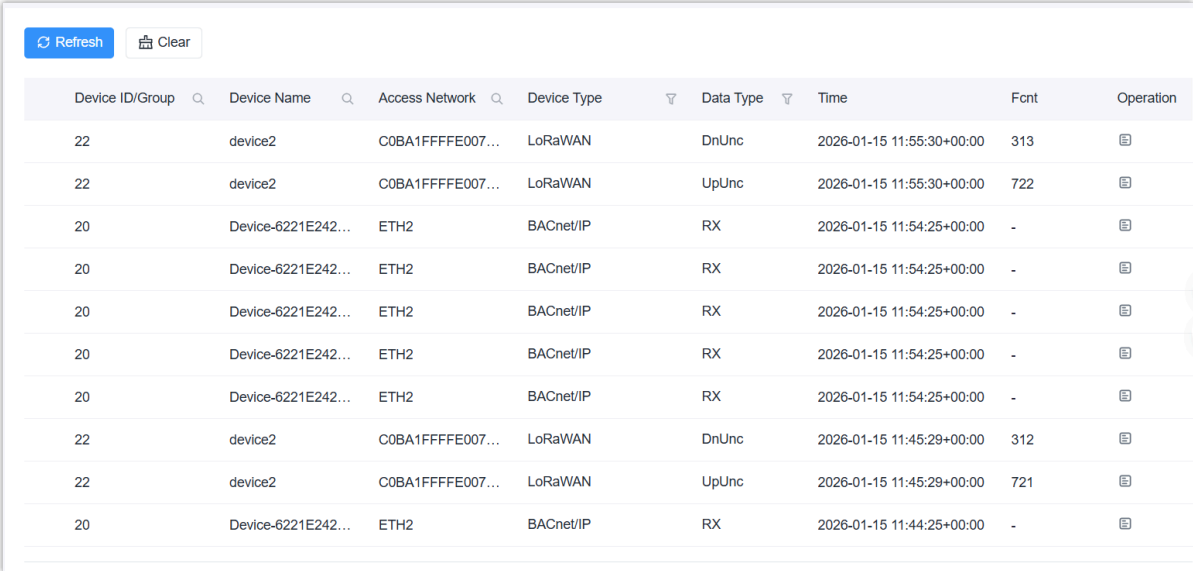
> **Tip:**
> It is recommended to add one or more devices manually, then export the files to check the format.

4. Modify the exported files to add the new device models.
5. Click **Import** to select the device repository .ZIP file from local path. After importing, the device will pop up the import result.

> **Note:**
> When importing the files, the device will overwrite the repository instead of appending to it.

Data Stream

This page is used to view communication packets between the connected devices and the gateway.



Refresh Clear

Device ID/Group	Device Name	Access Network	Device Type	Data Type	Time	Fcnt	Operation
22	device2	C0BA1FFFFE007...	LoRaWAN	DnUnc	2026-01-15 11:55:30+00:00	313	
22	device2	C0BA1FFFFE007...	LoRaWAN	UpUnc	2026-01-15 11:55:30+00:00	722	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:54:25+00:00	-	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:54:25+00:00	-	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:54:25+00:00	-	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:54:25+00:00	-	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:54:25+00:00	-	
22	device2	C0BA1FFFFE007...	LoRaWAN	DnUnc	2026-01-15 11:45:29+00:00	312	
22	device2	C0BA1FFFFE007...	LoRaWAN	UpUnc	2026-01-15 11:45:29+00:00	721	
20	Device-6221E242...	ETH2	BACnet/IP	RX	2026-01-15 11:44:25+00:00	-	

Parameter	Description
Refresh	Click to update the latest data stream records.
Clear	Click to clear all data stream records.
Device ID/Group	Display the device ID or multicast group name.
Device Name	Display the device name or multicast group name.
Access Network	Display the LoRaWAN® device EUI or the used interface name.
Device Type	Display the device protocol type.
Data Type	Display the data type. LoRaWAN® devices display JnAcc (Join Accept), JnReq (Join Request), UpUnc (Uplink Unconfirmed), UpCnf (Uplink Confirmed), DnUnc (Downlink Unconfirmed), or DnCnf (Downlink Confirmed), while other devices display TX or RX.
Time	Display the time to receive or send this data packet.
Fcnt	Display the Fcnt of the LoRaWAN® packet.
Operation	Click to check packet details including the data content.

Chapter 6. Network

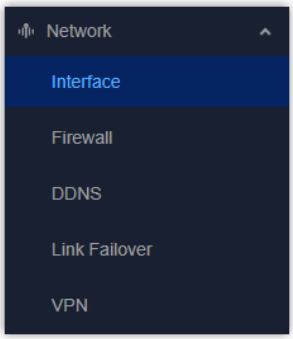
Interface

Ethernet

The device has two Ethernet ports. This chapter describes how to configure these Ethernet ports.

Steps

1. On the left bar, select **Network > Interface** page.



2. On the top bar, select **Ethernet** tab.
3. Select the port mode as Standalone mode or Bridge Mode.

   Standalone Mode: Each Ethernet port can work as either WAN port or LAN port.
   Bridge Mode: The two Ethernet ports are bridged together for transparent forwarding.

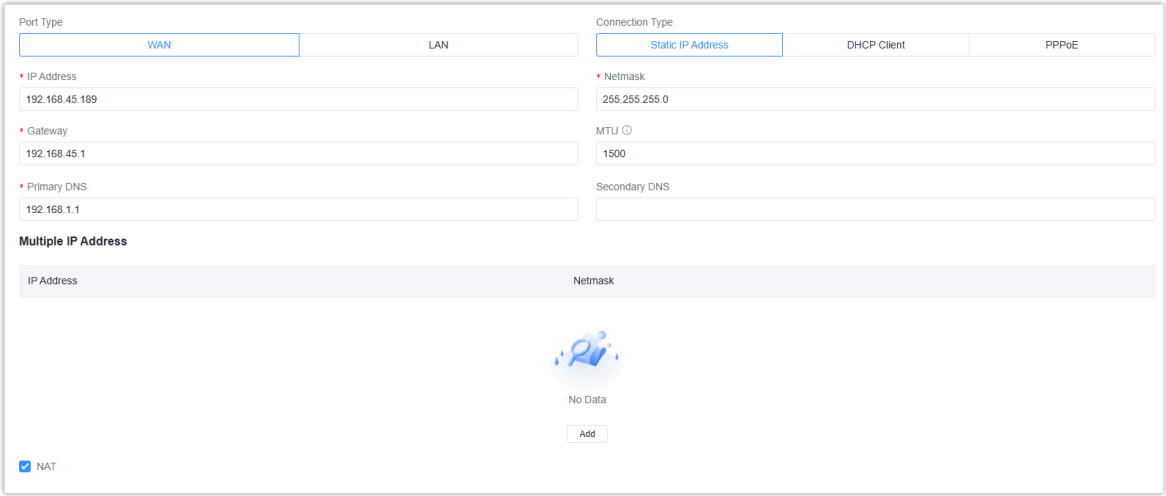
4. Configure the Ethernet parameters according to the port mode.
   - Standalone-WAN Settings
   - Standalone-LAN Settings
   - Bridge Mode Settings
5. Enable or disable Ethernet ports in Interface Settings.
6. Click **Apply** to save the settings.
7. After connecting the Ethernet ports to devices, check the screen or go to **Status** page to check connection status of Ethernet ports.
8. Configure Link Failover settings to enable ETH interface or bridge interface as network link.

Standalone Mode - WAN Settings

When the Ethernet port works as WAN port to connects to the external network (Internet). It supports 3 connection types:

1. Static IP Address

Assign a static IP address to this WAN port manually.



Parameter	Description
IP Address	The IPv4 address of this interface. The address must be in the same subnet as the gateway address.
Netmask	The IPv4 netmask of this interface.
Gateway	The IPv4 gateway address of this WAN port.
MTU	The maximum transmission unit of the packets passing this interface.
Primary DNS	The primary DNS server address.
Secondary DNS	The secondary DNS server address if the primary DNS server does not work.
Multiple IP Address	Click **Add** to add extra IP address and netmask for this interface.
NAT	Enable or disable NAT for this interface.

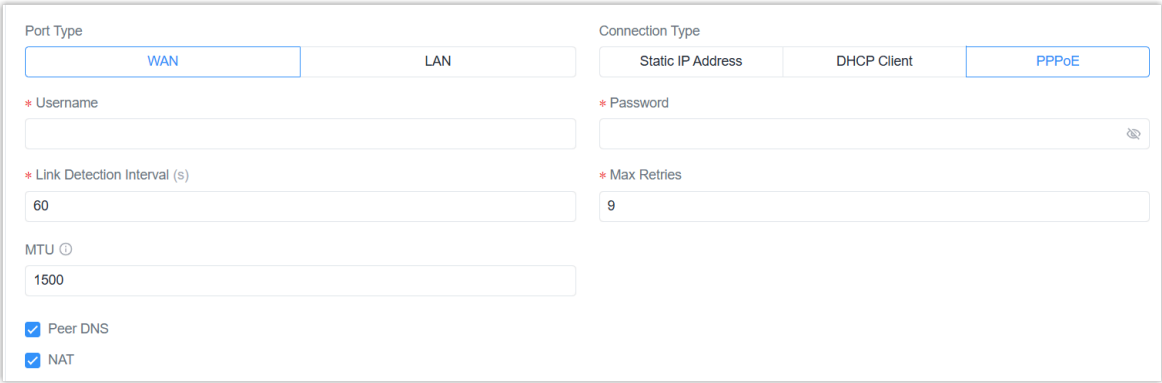
2. DHCP Client

Obtain IPv4 address automatically from DHCP server.

Parameter	Description
MTU	The maximum transmission unit of the packets passing this interface.
Peer DNS	Use the DNS server address of the peer. If disabled, it is necessary to configure the primary DNS server and secondary DNS sever manually.
NAT	Enable or disable NAT for this interface.

3. PPPoE

Set up a PPP (Point-to-Point Protocol) connection over the Ethernet port to receive the IP address.

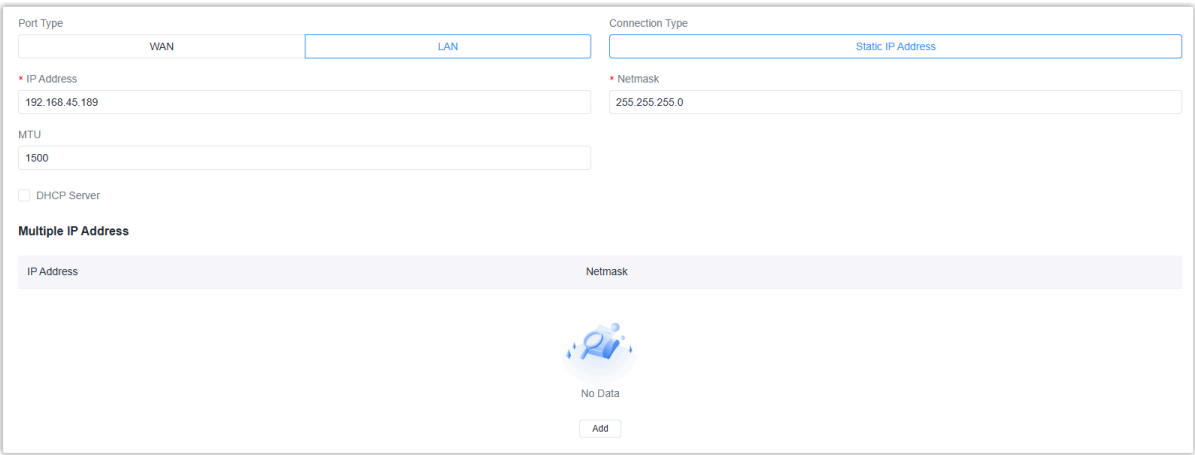


Parameter	Description
Username	The username for PAP/CHAP authentication.
Password	The password for PAP/CHAP authentication.
Link Detec-tion Interval	The interval to send heartbeat packets to detect the link status.
Max Retries	The maximum retry times if the dialing is failed.
MTU	The maximum transmission unit of the packets passing this interface. The actual MTU value is the configured value minus 8.

Parameter	Description
Peer DNS	Use the DNS server address of the peer. If disabled, it is necessary to configure the primary DNS server and secondary DNS sever manually.
NAT	Enable or disable NAT for this interface.

Standalone Mode - LAN Settings

When the Ethernet port works as LAN port to connect internal devices for local interconnection and data sharing.



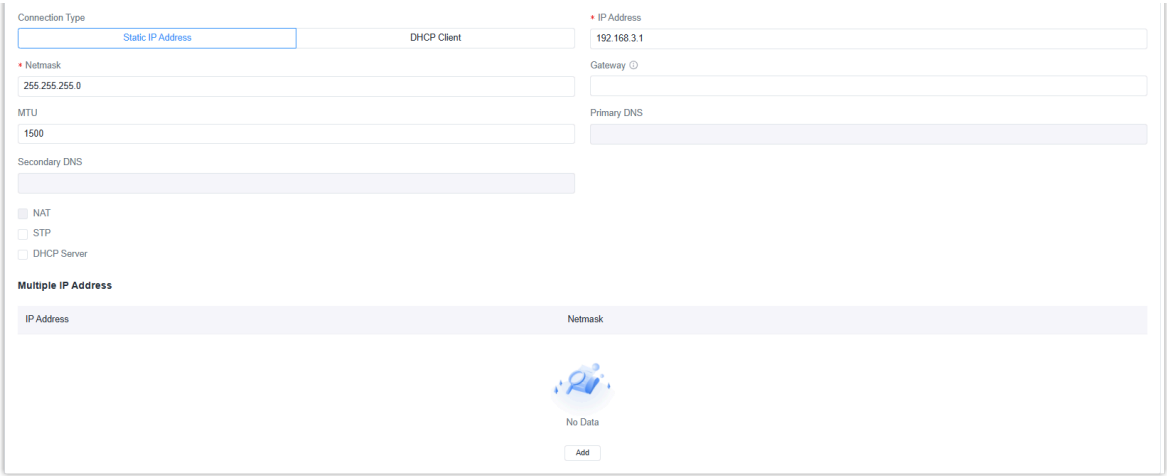
Parameter	Description
IP Address	The IPv4 address of this interface.
Netmask	The IPv4 netmask of this interface.
MTU	The maximum transmission unit of the packets passing this interface.
Multiple IP Address	Click **Add** to add extra IP address and netmask for this interface.
DHCP Server	
DHCP Server	Enable the DHCP server to assign IP address to connected client devices automatically. If disabled, the client devices are required to configure their own IP addresses.
Start Address	Set the start IP address of the IP range to assign IP addresses.
End Address	Set the end IP address of the IP range to assign IP addresses.
Lease Time	Set the lease time during which the client can use the IP address from the DHCP server. After this time, the client has to request a new lease.

Parameter	Description
Primary DNS	The primary DNS server address.
Secondary DNS	The secondary DNS server address if the primary DNS server does not work.
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from the DHCP server. Generally, you can leave it blank.
MAC Binding	Click **Add** to bind the specific IP addresses to specific clients by client MAC addresses.

Bridge Mode Settings

Both Ethernet ports share the same configuration and support 2 connection types:

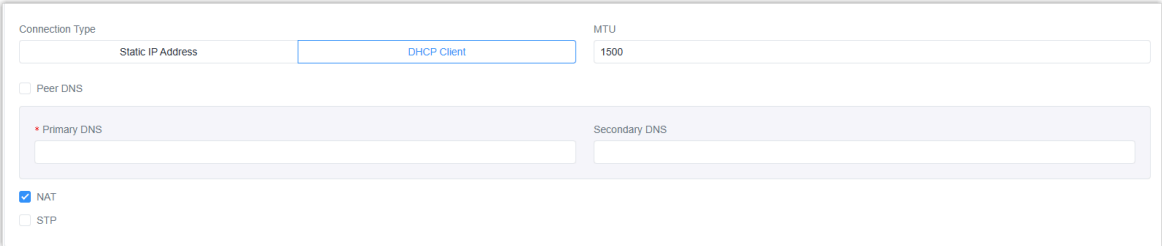
1. Static IP Address



Parameter	Description
IP Address	The IPv4 address of this interface. The address must be in the same subnet as the gateway address when it needs to connect to the external network.
Netmask	The IPv4 netmask of this interface.
Gateway	Enter the IPv4 gateway address of this interface when it needs to connect to the external network.
MTU	The maximum transmission unit of the packets passing this interface.
Primary DNS	When gateway address is typed, set the primary DNS server address.
Secondary DNS	When gateway address is typed, set he secondary DNS server address.

Parameter	Description
NAT	When gateway address is typed, enable or disable NAT for this interface.
STP	Disable or enable STP for this interface.
Multiple IP Address	Click **Add** to add extra IP address and netmask for this interface.
DHCP Server	
DHCP Server	Enable the DHCP server to assign IP address to connected client devices automatically. If disabled, the client devices are required to configure their own IP addresses.
Start Address	Set the start IP address of the IP range to assign IP addresses.
End Address	Set the end IP address of the IP range to assign IP addresses.
Lease Time	Set the lease time during which the client can use the IP address from the DHCP server. After this time, the client has to request a new lease.
Primary DNS	The primary DNS server address.
Secondary DNS	The secondary DNS server address if the primary DNS server does not work.
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from the DHCP server. Generally, you can leave it blank.
MAC Binding	Click **Add** to bind the specific IP addresses to specific clients by client MAC addresses.

2. DHCP Client

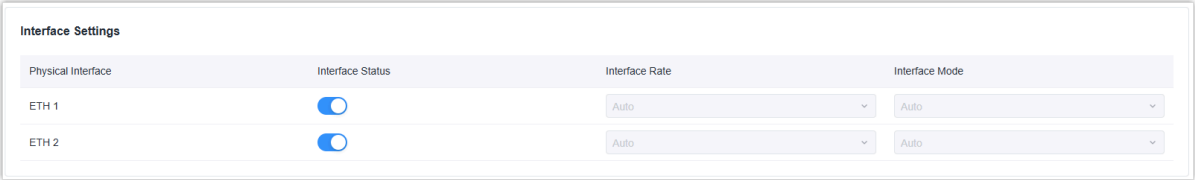


Parameter	Description
MTU	The maximum transmission unit of the packets passing this interface.
Peer DNS	Use the DNS server address of the peer. If disabled, it is necessary to configure the primary DNS server and secondary DNS sever manually.

Parameter	Description
NAT	Enable or disable NAT for this interface.
STP	Disable or enable STP for this interface.

Interface Settings

Enable or disable the ETH interfaces as required.



Cellular

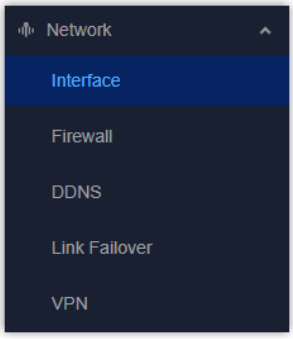
This chapter describes how to configure the settings to register to cellular network.

Prerequisites

- The supported frequencies of the SIM card matches the device model.
- Ensure the SIM card has sufficient balance and works properly in other devices.
- Ensure the device has installed the SIM card and the cellular antenna.
- Gather SIM information from the cellular operator.

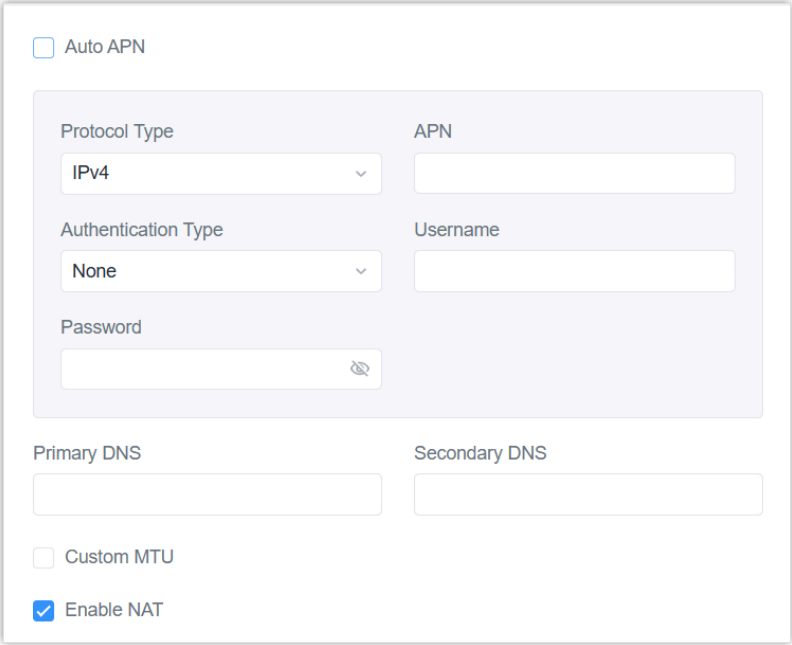
Steps

1. On the left bar, select **Network > Interface** page.



2. On the top bar, select **Cellular** tab.
3. Enable the cellular interface.

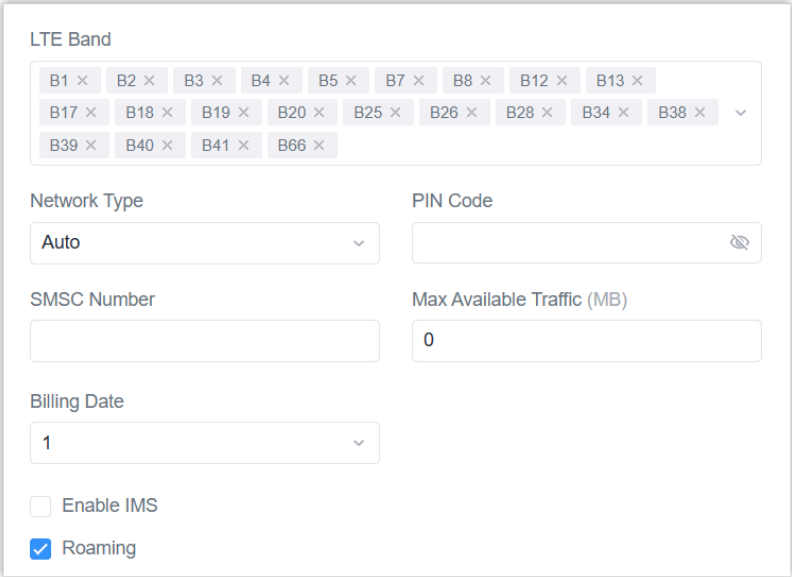
4. Click to configure the settings of this SIM card. Skip this step if not required.



Parameter	Description
Auto APN	After enabled, the device will scan an internal APN database and selects an APN based on the SIM card's operator and country. If the first chosen automatically APN doesn't work, it attempts to use the next existing APN from the internal database. If disabled, set below parameters to custom APN info: **Protocol Type**: Set the type as IPv4 or IPv4/IPv6. **APN**: Set the Access Point Name for cellular registration and defining which external network to connect. Only letters, digits, "-" and "." are allowed, and the first character must not be "_" or ".". The maximum length is 63 characters. **Authentication Type**: Set the method to authenticate new connections on the carrier's network.

Parameter	Description
	Username: Set the username for cellular registration. **Password**: Set the password for cellular registration.
Primary DNS	Customize the cellular primary DNS server. If left blank, the device will use operator's settings.
Secondary DNS	Customize the cellular secondary DNS server. If left blank, the device will use operator's settings.
Custom MTU	Enable or disable to customize the maximum transmission unit. If disabled, the device will use operator's MTU settings.
Enable NAT	Enable or disable NAT.

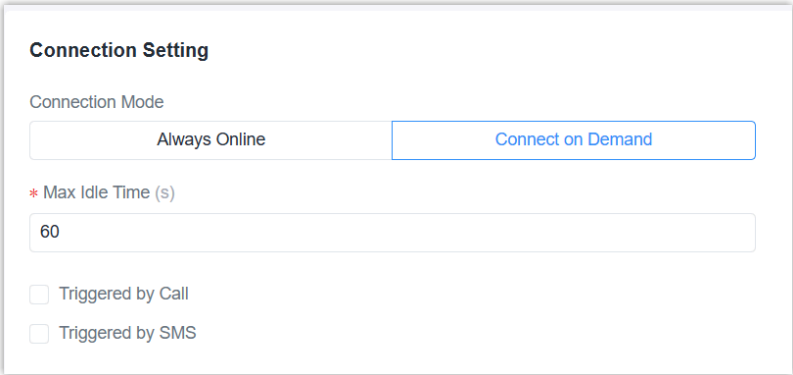
5. Click **SIM Setting** to configure the SIM parameters of all interfaces. Skip this step if not required.



Parameter	Description
LTE Band	Select the cellular bands used to register the cellular network. It can be used to optimize cellular speeds by selecting specific bands.
Network Type	Select from Auto, 4G Only, etc. (The options differ according the model).
PIN Code	Set a 4-8 characters PIN code to unlock the SIM.
SMSC Number	Set a hub number to store, route or deliver SMS messages. This feature is only available for -L08GL model.

Parameter	Description
Max Available Traffic	After reaching this limit, the SIM card is not allowed to use until the billing day. 0 means no limit.
Billing Date	Select the month's date to reset the available traffic data.
IPv4 Subnet Mask	Customize the cellular subnet mask. If left blank, the device will use operator's settings. This feature is only available for -L09NA model.
Enable IMS	Enable or disable IMS feature. This feature is only available for -L08GL model.
Roaming	Enable or disable roaming.

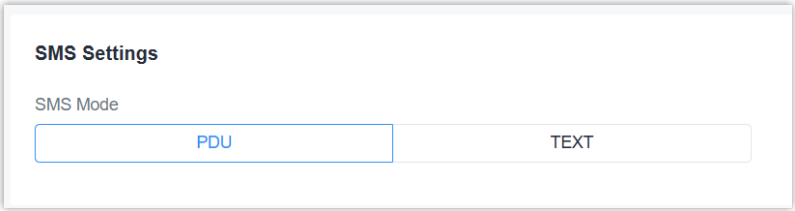
6. Select the connection mode as required. This feature is only available for -L08GL model.



If **Connect on Demand** is selected, configure the following parameters:

Parameter	Description
Max Idle Time	If there is no cellular data transmission during this time, drop the cellular connection.
Triggered by Call	After enabled, the device will try to register to cellular network after receiving a call from any number of the selected call group.
Triggered by SMS	After enabled, the device will try to register to cellular network after receiving a specific SMS message from any number of the selected SMS group.

7. Select the SMS mode as PDU or TEXT as required. This feature is only available for -L08GL model.



8. Click **Apply** to save the settings.
9. Check if the cellular status is Connected.
10. Configure Link Failover settings to enable cellular interface as network link.

Related information

Status

Link Failover

Service

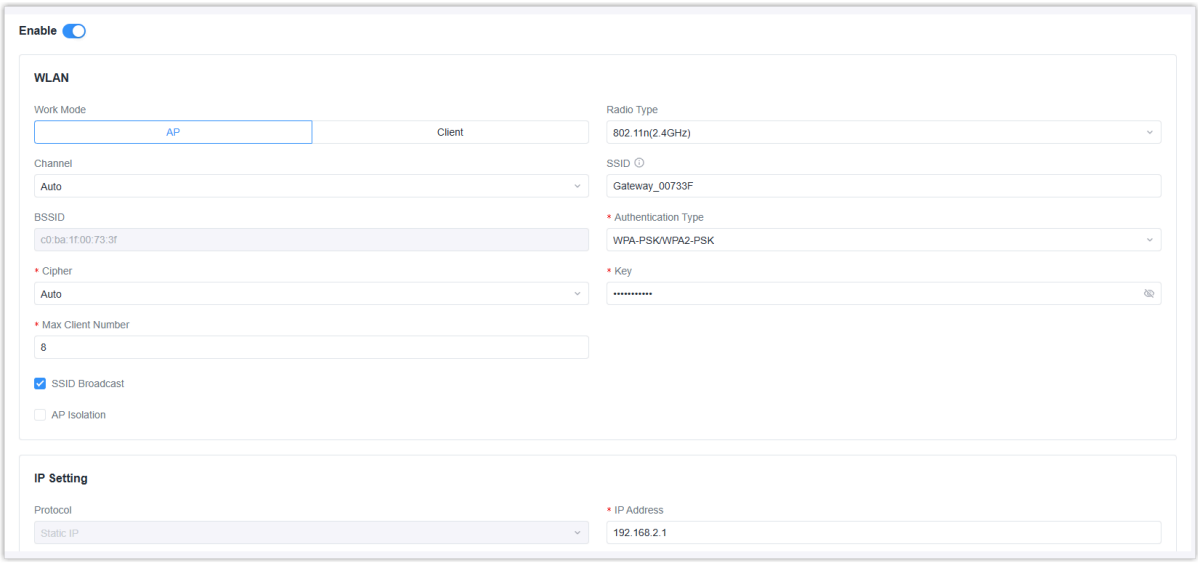
Tools

WLAN

This chapter describes how to configure Wi-Fi settings.

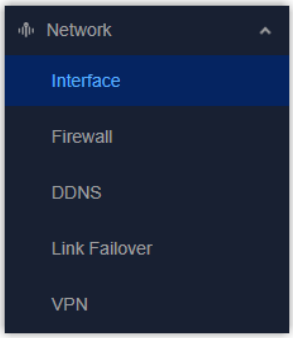
AP Mode Settings

The device can work as a Access Point for device web access or Wi-Fi sensors connection.



Steps:

1. On the left bar, select **Network > Interface** page.



2. On the top bar, select **WLAN** tab.
3. Enable WLAN feature.
4. Select the work mode as AP and configure the related parameters.

Parameter	Description
Radio Type	Select the radio type from 802.11b(2.4GHz), 802.11g(2.4GHz), 802.11n(2-.4GHz).
Channel	Select the frequency channel to transmit data. **Tip:** It is recommended to use a Wi-Fi analyzer tool to check channel occupancy at the target installation location. Select the least crowded channel to avoid interference, improve network speed, and enhance stability.
SSID	Set the Service Set Identifier (SSID) to identify this access point. The default value is **Gateway_XXXXXX** (=last 6 digits of WLAN MAC address).
BSSID	Display the MAC address of WLAN interface.
Authentication Type	Select the authentication type for connection. Options: No Encryption, WEP, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK. **Cipher:** Select the encryption cipher when the encryption mode is not No Encryption. **Key:** Set the key to connect to this access point. Only ASCII characters without spaces are allowed. The default value is **iotpassword**.

Parameter	Description
Max. Client Number	Set the maximum allowed clients to connect to this access point. Range: 1-8.
SSID Broadcast	After disabled, the SSID can not be searched directly. Users have to enter the SSID manually to connect to the access point.
AP Isolation	After enabled, all connected clients can not communicate with each other.

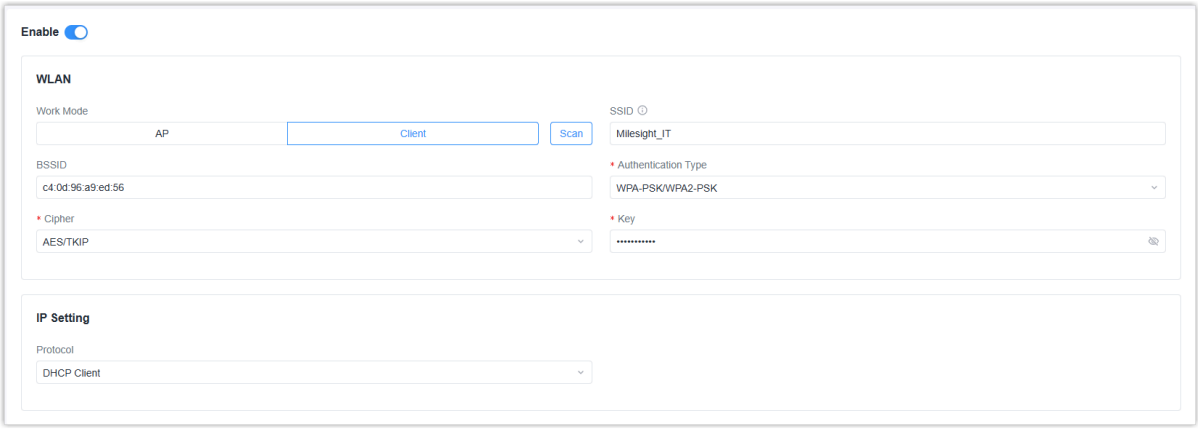
5. Configure the IP settings for client devices as required.

Parameter	Description
Protocol	It's fixed as Static IP.
IP Address	Set the IP address of this WLAN interface. The default value is **192.168.2.1**.
Subnet Mask	Set the subnet mask of this WLAN interface.
DHCP Server	
DHCP Server	Enable the DHCP server to assign IP address to connected client devices automatically. If disabled, the client devices are required to configure their own IP addresses.
Start Address	Set the start IP address of the IP range to assign IP addresses.
End Address	Set the end IP address of the IP range to assign IP addresses.
Netmask	Set the netmask of the IP range to assign IP addresses.
Lease Time	Set the lease time during which the client can use the IP address from the DHCP server. After this time, the client has to request a new lease.
Primary DNS Server	Set the primary DNS server address.
Secondary DNS Server	Set the secondary DNS server address if the primary DNS server does not work.
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from the DHCP server. Generally, you can leave it blank.
MAC Binding	Click **Add** to bind the specific IP addresses to specific clients by client MAC addresses.

6. Click **Apply** to save the settings.
7. Connect a smart phone or a Wi-Fi client device to the access point. This requires the parameters the same as the access point.
8. After connected, go to **Status** page to check if there is any client information.

Client Mode Settings

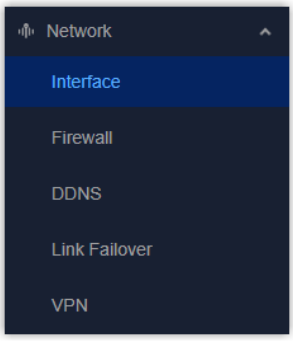
The device can work as a Client to connect to another Access Point for Internet access or Wi-Fi sensors connection.



Note:
Do not access the web GUI via wireless method if you need to configure the WLAN interface as client mode!

Steps:

1. On the left bar, select **Network > Interface** page.



2. On the top bar, select **WLAN** tab.
3. Enable WLAN feature.
4. Select the work mode as Client, click **Scan** to search the access points around the device.

5. Select an available access point, click **Join Network**.
6. After selected, the basic information of the access point will be typed automatically. For some access points, it requires typing the key (Wi-Fi password).
7. Configure the IP settings for client devices as required.

Parameter	Description
Protocol	Select the mode to receive the WLAN IP address. **DHCP Client**: Receive IP address from the access point. **Static IP:** Assign the IP address manually.
Static IP Setting	
IP Address	Set the WLAN interface IP address with the same subnet as the access point.
Subnet Mask	Set the subnet mask of the WLAN interface IP address.
Gateway	Set the IP address of the connected gateway.
Primary DNS Server	Set the primary DNS server address.
Secondary DNS Server	Set the secondary DNS server address if the primary DNS server does not work.

8. Click **Apply** to save the settings.
9. After connected, go to **Status** page to check if the status is Connected.
10. Configure Link Failover settings to enable WLAN interface as network link.

Related information

Link Failover

LoRa

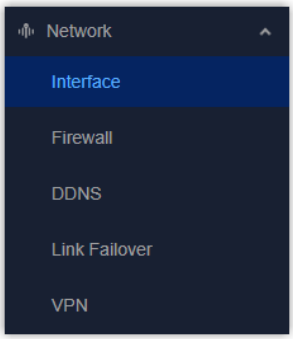
This chapter describes the frequency settings for LoRaWAN® communication.

Basic Settings

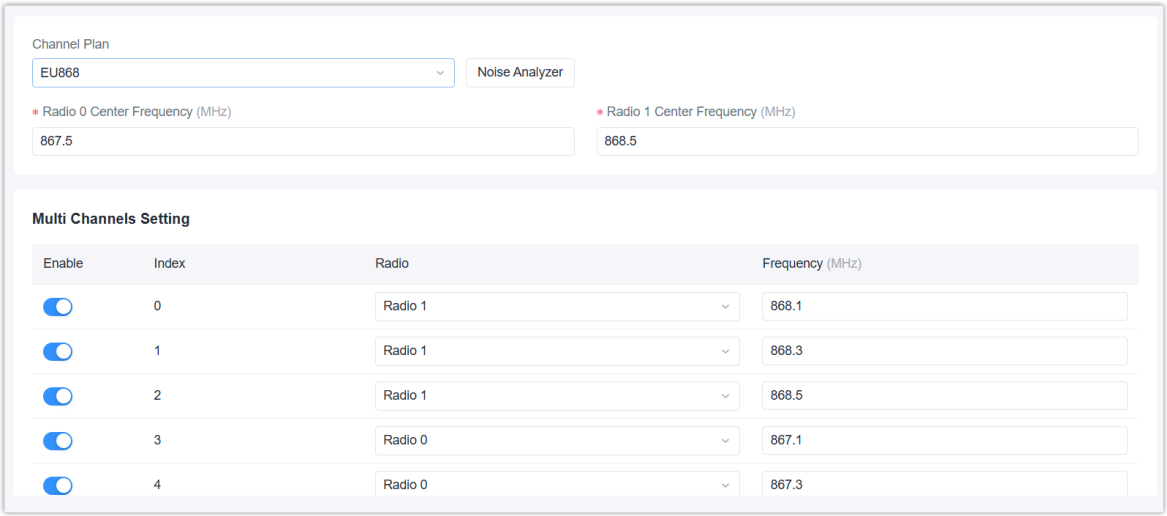
This section is used for most of LoRaWAN® device communication.

Steps:

1. On the left bar, select **Network > Interface** page.



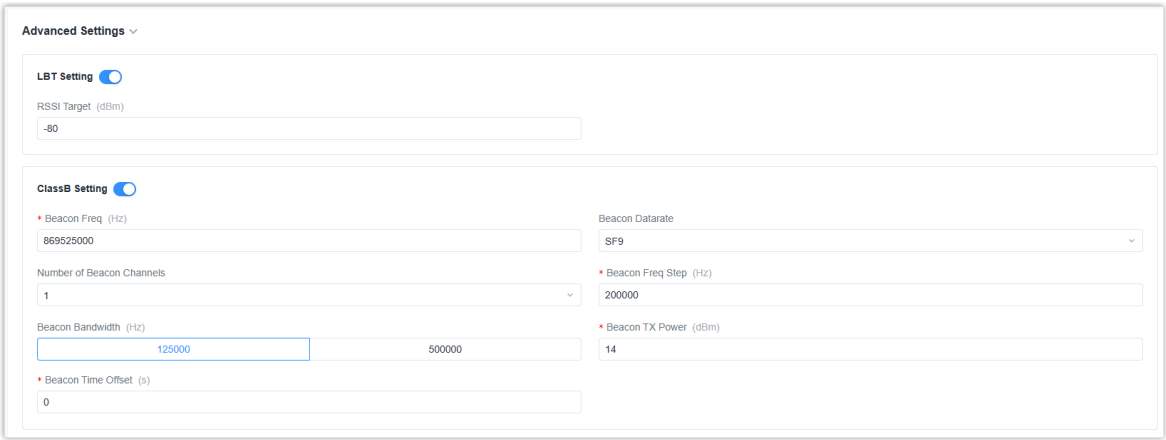
2. On the top bar, select **LoRa** tab.
3. Select the channel plan the same as the LoRaWAN® end devices.
4. Configure the frequency parameters as required. You can also keep these settings by default.



Parameter	Description
Channel Plan	Select the channel plan of the network. The options vary by model: -868M: EU868, IN865, RU864 -915M: AU915, US915, KR920, AS923-1/2/3/4 -470M: CN470
Noise Analyzer	Click here to see details.

Parameter	Description
Center Frequency	Set the center frequencies of different modules.
Multi Channels Setting	
Enable	Enable or disable the channel to transmit packets.
Radio	Select Radio 0 or Radio 1 as center frequency.
Frequency	Set the frequency point of every channel.
LoRa/FSK Channel Setting	
Enable	Enable or disable the LoRa/FSK channel.
Radio	Select Radio 0 or Radio 1 as center frequency.
Frequency	Set the frequency of the LoRa/FSK channel.
Bandwidth	Set the bandwidth of the LoRa/FSK channel.
Data Rate	Set the data rate of the LoRa/FSK channel.

5. Configure the advanced settings as required.



Parameter	Description
LBT Setting	Enable or disable LBT feature. Listen before talk (LBT) is used to detect whether the downlink channel is idle and avoid channel access conflicts. **Note:** AU915 and US915 do not support this feature.

Parameter	Description
	RSSI Target: Enter the criteria of an idle channel. If the actual RSSI of a channel is less than the criteria/target, the channel is considered as idle.
Class B Setting	Enable or disable to send beacons to communicate with class B end devices. **Beacon Freq:** The frequency to transmit the beacons. **Beacon Datarate:** The datarate to transmit the beacons. **Number of Beacon Channels:** The number of used beacon channels. **Beacon Freq Step:** The frequency step to transmit the beacons. **Beacon Bandwidth:** The bandwidth of the beacons. **Beacon Tx Power:** The Tx power of the beacons. **Beacon Time Offset:** Add this offset to the system time and assign the time result to class B devices. This can avoid the interference when multiple class B devices are close.

6. Click **Apply** to save the settings.

Noise Analyzer

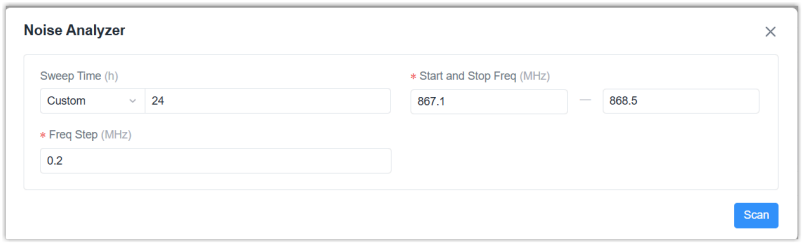
Noise analyzer is used for sweeping the noise of every frequency channel and giving a diagram for users to analyze the environmental interference condition and select the best deployment.

Prerequisites

- The device is placed to the target location. If the installation location is changed, please reproduce the noise analyzer.
- This feature will impact LoRaWAN® downlink transmission, so do not send downlink commands to devices during sweeping.

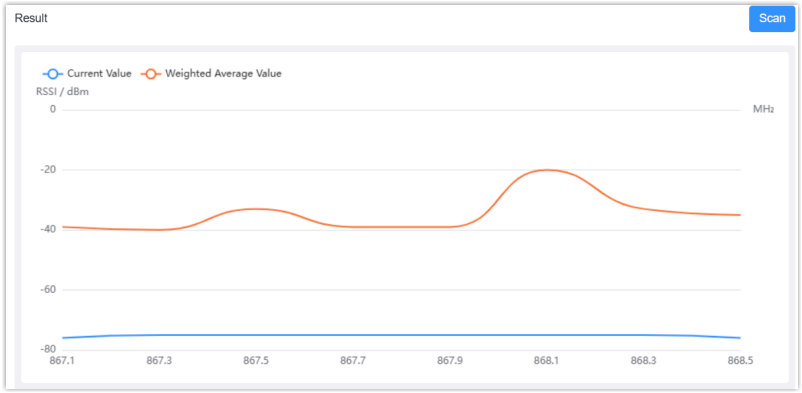
Steps:

1. Click **Noise Analyzer**.
2. In the pop-up window, configure the frequency range and the time.



Parameter	Description
Sweep Time	Set the time to sweep the frequency range. **Continuous:**Sweep the frequencies continuously. **Custom:** Custom the time to sweep the frequencies. **Tip:** To ensure the accurate result, it is recommended to set the sweep time as 24h.
Start and Stop Freq	Configure the frequency range to scan.
Freq Step	Configure the step for each frequency channel to be scanned.

3. Click **Scan** to start sweeping the frequencies.
4. The device will stop sweeping after the custom time, or click **Stop Scanning**.
5. Check the analysis results. The lower the RSSI value, the better the signal.



6. Adjust the frequencies in Multi Channels Setting as required.

RS485

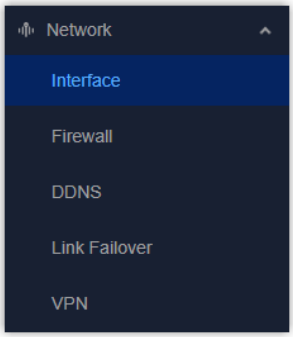
This chapter describes how to configure RS485 basic parameters.

Prerequisites

Gather the RS485 basic parameters from terminal devices' user guides or manufacturers.

Steps

1. On the left bar, select **Network > Interface** page.



2. On the top bar, select **RS485** tab.
3. Configure the basic parameters of the corresponding RS485 interface. **Usually, these should be the same as the terminal devices.**

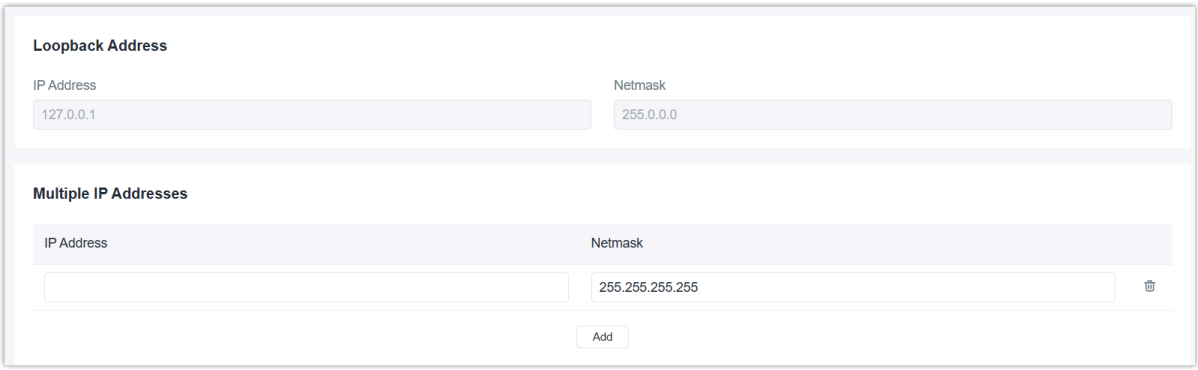
Parameter	Description
Baud Rate	Select the serial data transmission rate.
Data Bits	The number of data bits for each character. It is fixed at 8.
Stop Bits	Indicates the end of each data frame, enabling the receiver to determine if a frame is complete. Options: 1, 2
Parity	This is used to detect errors during transmission. Options: None, Odd, Even.
DIP	Enable or disable to add a 120Ω termination resistor across terminals A and B, eliminating signal reflections from the cable ends.

4. Click **Apply** to save the settings.

Loopback

A loopback address is a special reserved IP address that allows the device to send data to itself, bypassing the physical network for internal testing, development, and troubleshooting. It's also known as localhost, creating a virtual interface for applications to communicate internally, confirming network software works without impacting live traffic.

This page displays the default loopback address and supports adding extra loopback addresses as required.

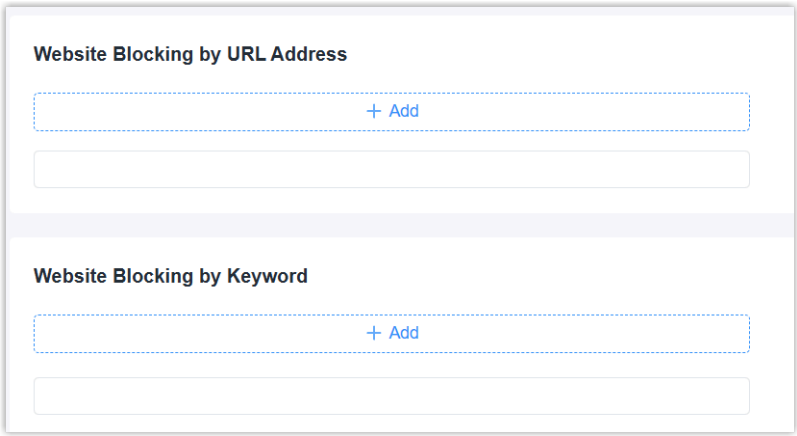


Firewall

This chapter describes the firewall settings for the device security.

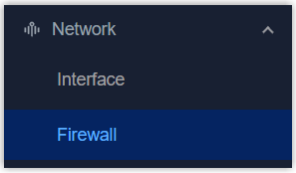
Security

This page is used to add the URL address or keyword to block the devices under LAN ports to access specific websites.



Steps:

1. On the left bar, select **Network > Firewall** page.

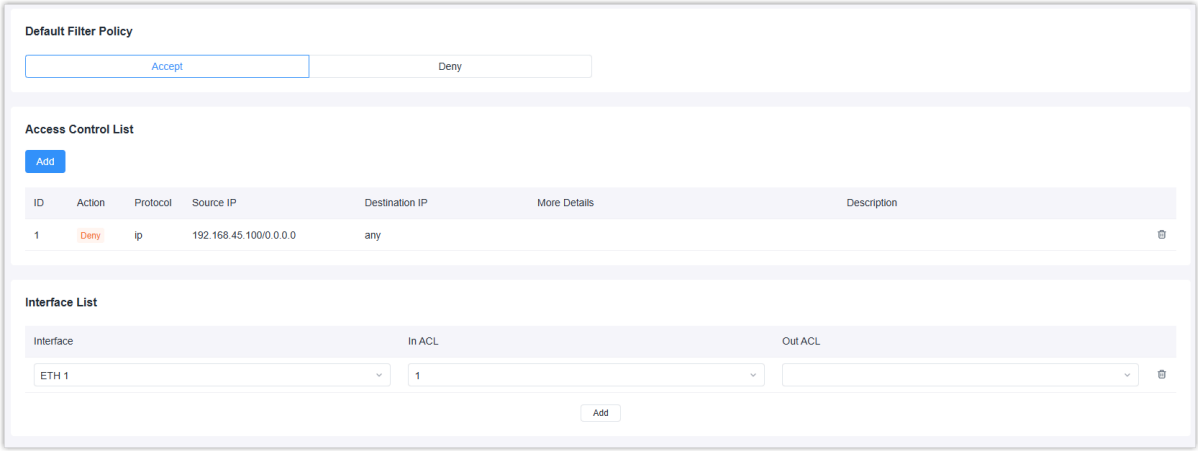


2. On the top bar, select **Security** tab.

3. Click **+Add** to add URL addresses or keywords to block.
4. Click **Apply** to save the settings.

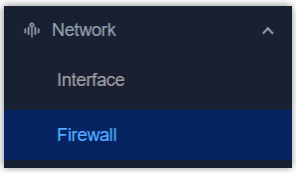
ACL

This page is used to add and manage ACL rules.

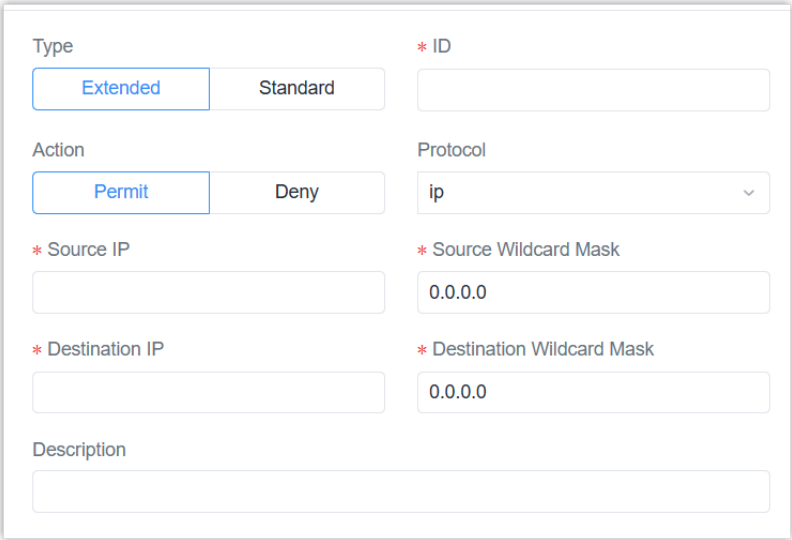


Steps:

1. On the left bar, select **Network > Firewall** page.



2. On the top bar, select **Security** tab.
3. Select the default filter policy as Accept or Deny. The packets that are not included in the ACL rule will be processed by this policy.
4. Click **Add** to add an ACL rule and configure the related parameters.



Parameter	Description
Type	Select the ACL type. **Standard:**Filter traffic based only on the source IP address. **Extended:** Filter traffic by source IP, destination IP, protocol, and port numbers for precise control.
ID	Define a unique ID for this rule.
Action	Select the action to be taken when a packet matches this rule.
Source IP	The source IPv4 address of the packet to filter.
Source Wildcard Mask	Wildcard mask of the source IP address.
Description	For noting this ACL rule.
Extended Type ACL	
Protocol	Select the protocol type of the packet to filter.
Destination IP	The destination IPv4 address of the packet to filter.
Destination Wildcard Mask	Wildcard mask of the destination IP address.
ICMP Type	When protocol is ICMP, set the ICMP message type ID to filter.
ICMP Code	When protocol is ICMP, set the ICMP message code ID to filter.
Source Port Type	When protocol is UDP or TCP, set the source port condition.

Parameter	Description
	Source Port: If the type is not any, set the specific source port number or port range to filter.
Destination Port Type	When protocol is UDP or TCP, set the destination port condition. **Destination Port:** If the type is not any, set the specific destination port number or port range to filter.

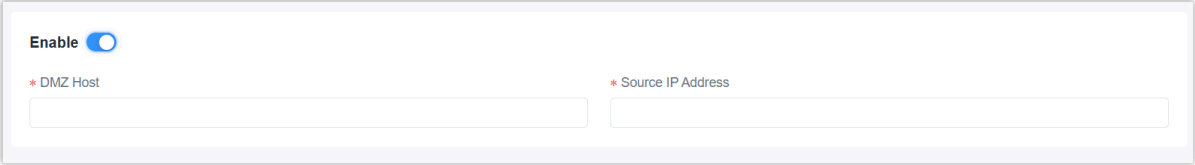
5. Select the interface and the direction to execute the ACL rule.

   In ACL: Filter the packets incoming to this interface.
   Out ACL: Filter the packets outgoing from this interface.

6. Click **Apply** to save the settings.

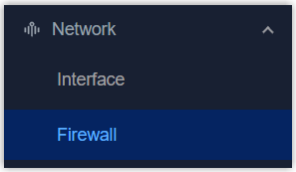
DMZ

This page is used to configure DMZ settings. DMZ (demilitarized zone) allows external network users to access the internal network server when a firewall has been setup. When DMZ is enabled, users can access the DMZ host (e.g., your computer) directly from the Internet.



Steps:

1. On the left bar, select **Network > Firewall** page.



2. On the top bar, select **DMZ** tab.
3. Enable DMZ and configure the related parameters.

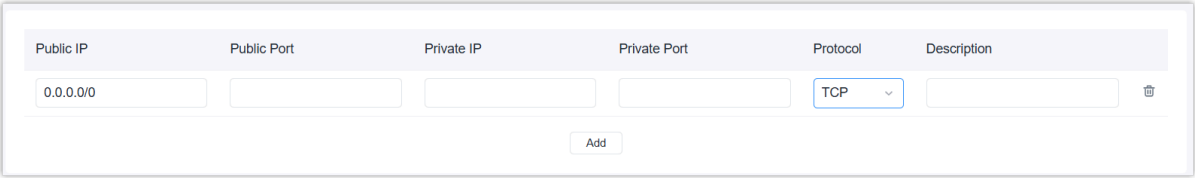
Parameter	Description
Enable	Enable or disable DMZ feature.

Parameter	Description
DMZ Host	The IP address of the internal host.
Source IP Address	The IP address or IP address/mask which can access the DMZ host. 0.0.0.0/0 means all.

4. Click **Apply** to save the settings.

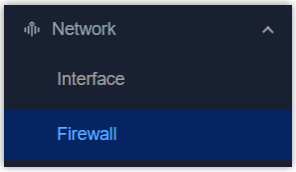
Port Mapping (DNAT)

This page is used to add port mapping rules. Port Mapping (also known as Port Forwarding or DNAT) is a network technique that changes the destination IP address of incoming packets to make internal network services accessible from the public or outside network.



Steps:

1. On the left bar, select **Network > Firewall** page.



2. On the top bar, select **Port Mapping** tab.
3. Click **Add** to add a port mapping rule and configure the related parameters.

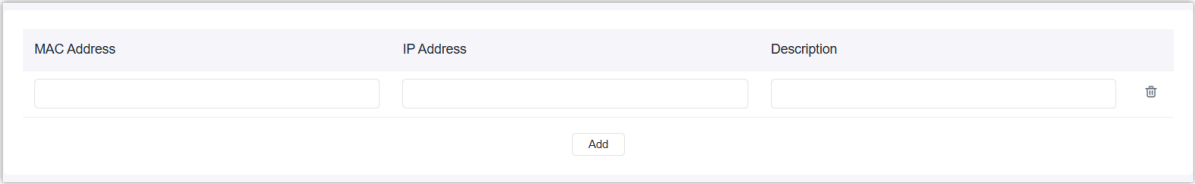
Parameter	Description
Public IP	The IP address/mask which can access the internal service. 0.0.0.0/0 means all.
Public Port	The port number or port range which
Private IP	The IP address or IP address/mask which the incoming packets will be redirected.
Private Port	The port number or port range which the incoming packets will be redirected.
Protocol	Select the apply protocol from TCP, UDP and Both.

Parameter	Description
Description	For noting this port mapping rule.
	Delete this port mapping rule.

4. Click **Apply** to save the settings.

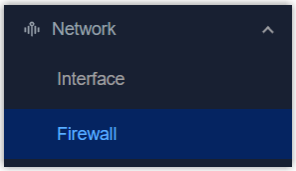
MAC Binding

This page is used to configure MAC binding settings. If any MAC binding rule is added, only devices in this list can access the external network.



Steps:

1. On the left bar, select **Network > Firewall** page.



2. On the top bar, select **MAC Binding** tab.
3. Click **Add** to add a MAC binding rule and configure the related parameters.

Parameter	Description
MAC Address	The MAC address of the hosts.
IP Address	The IPv4 address of the hosts.
Description	For noting this MAC binding rule.
	Delete this MAC binding rule.

4. Click **Apply** to save the settings.

DDNS

This chapter introduces the DDNS settings.

Overview

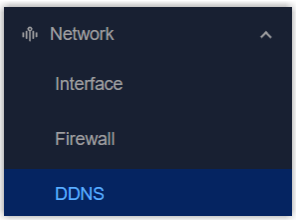
Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows users to alias a dynamic IP address to a static domain name. DDNS serves as a client tool and needs to coordinate with the DDNS server.

Prerequisites

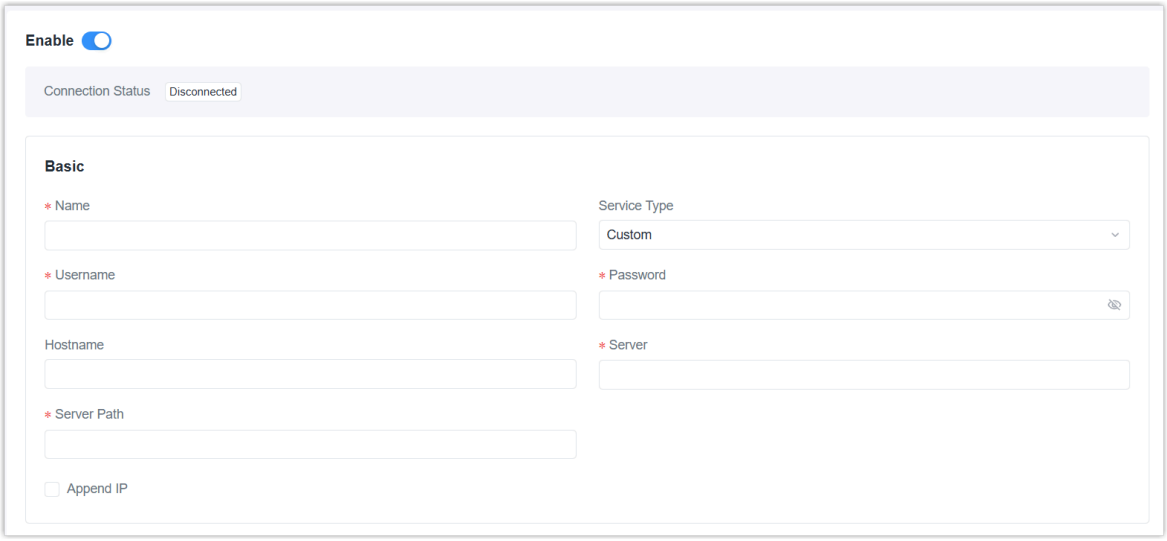
- Register on a proper DNS service provider's website and apply for a domain name.
- Enable device remote access service as required.

Steps

1. On the left bar, select **Network > DDNS** page.



2. Enable DDNS service and configure the basic settings.



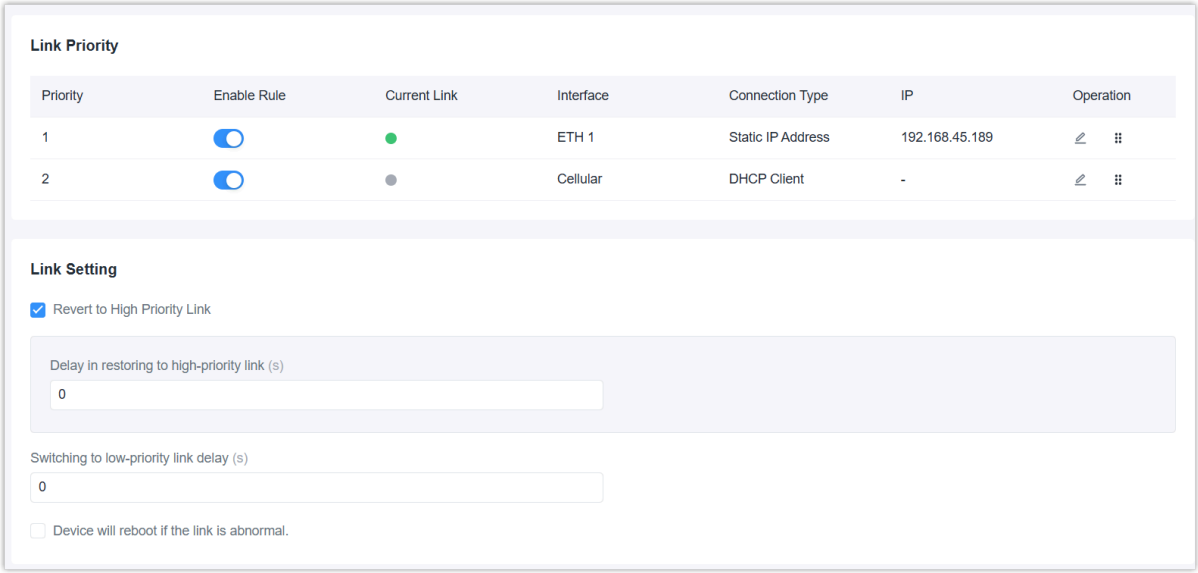
Parameter	Description
Name	Define a name for this DDNS service.
Service Type	Select the DNS service provider. If it does not exist in these options, select Custom.
Username	The username to login to the DNS service provider account and make updates.
User ID	Some DNS service providers require this ID to categorize something.
Password	The password to login to the DNS service provider account and make updates.
Hostname	The domain name to be linked with this device IP address.
If service type is Custom	
Server	The server address of the custom DNS service provider.
Server Path	The URL for sending IP update requests to the DNS service provider.
Append IP	Enable or disable appending the current device IP to the server path.

3. Click **Apply** to save the settings.
4. Check if the connection status is Connected.
5. Use the domain name to access the device to check if the DDNS settings take effect.

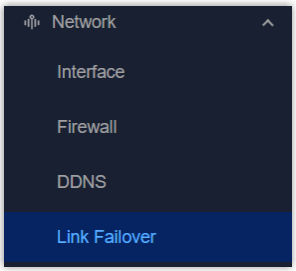
Link Failover

This chapter describes how to configure the link failover settings.

Steps



1. On the left bar, select **Network > Failover** page.



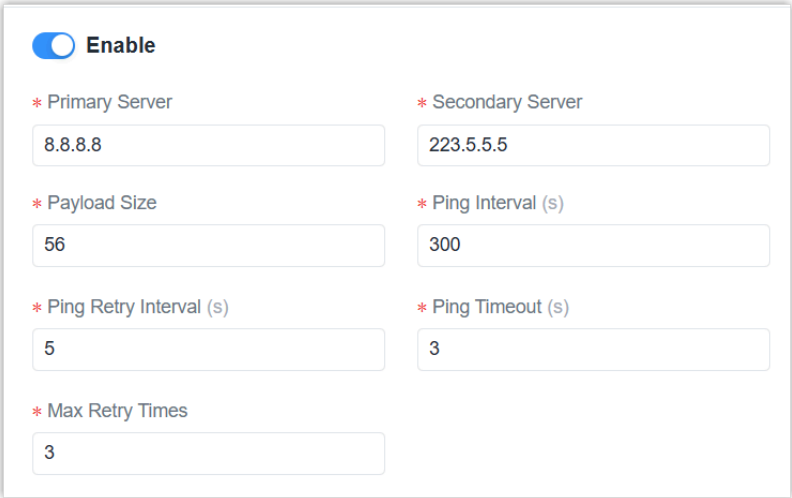
2. Tap **Enable Rule** buttons to enable the interfaces as network links of this device, then drag ⠿ to adjust the priorities of these network links.

Parameter	Description
Priority	Display the priority of this link. 1 means the highest priority.
Enable Rule	Enable or disable to use this interface as network link.
Current Link	Mark the current network link as green.
Interface	Display the available interfaces to work as the network links.
Connection Type	Display the connection type of this interface. For cellular interface, it's fixed as DHCP client.
IP	Display the IP address of this interface.

Parameter	Description
Operation	: Click to edit ping detection settings. : Drag to adjust the link priorities.

3. Click to enable the ping detection of selected link as required, and configure the related parameters.

Note:
If the device registers to a private network, it is recommended to disable the ping detection or configure the server addresses as private network reachable addresses.



Parameter	Description
Enable	After enabled, the device will periodically detect the connection status of the link by sending ICMP packets.
Primary Server	The primary server address to send the ICMP packet.
Secondary Server	The secondary server address to send the ICMP packet if the device does not receive the replies from the primary server.
Payload Size	The payload size of the ICMP packet.
Ping Interval	The interval between two Ping detections.

Parameter	Description
Ping Retry Interval	The interval to retry the ping if the previous ping reaches the timeout and does not reach the max retry times.
Ping Timeout	The maximum amount of time the device will wait for a response to a ping request. If it does not receive a response within the amount of time predefined in this field, the ping request will be considered a failure.
Max Retry Times	The retry times of the device sending ping request until determining that the connection has failed.

4. Configure the Link Setting parameters as required.

Parameter	Description
Revert to High Priority Link	After enabled, switch back to high priority link if it recovers. **Delay in restoring to high-priority link:** The delay time to switch back to high priority link. 0 means immediately.
Switch to low-priority link delay	The delay time to switch to low priority link. 0 means immediately.
Device will reboot if the link is abnormal	If all links are unavailable, reboot this device. If the links still fail to recover after three reboots, no further reboots will be performed.

5. Click **Apply** to save the settings.

Related information

Cellular

WLAN

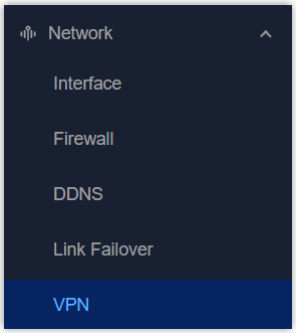
VPN

This chapter introduces the VPN feature to ensure secure communication.

Overview

Virtual Private Network (VPN) is a feature to set up encrypted tunnels to ensure data secure transmission, and allow the access between two private networks. Here are the basic steps:

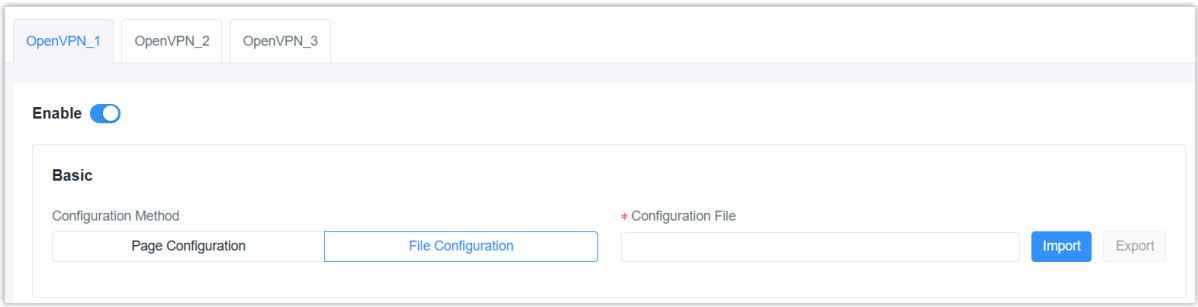
1. On the left bar, select **Network > VPN** page.



2. On the top bar, select the corresponding VPN page and configure the VPN parameters. The parameters must match the peer side.
    - OpenVPN Client Settings
    - OpenVPN Server Settings
    - IPsec Settings
    - WireGuard Settings
    - L2TP Client Settings
    - PPTP Client Settings
3. Click **Apply** to save the settings.
4. Navigate to **Status** page, select **VPN** from Other module to check VPN connection status.

OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

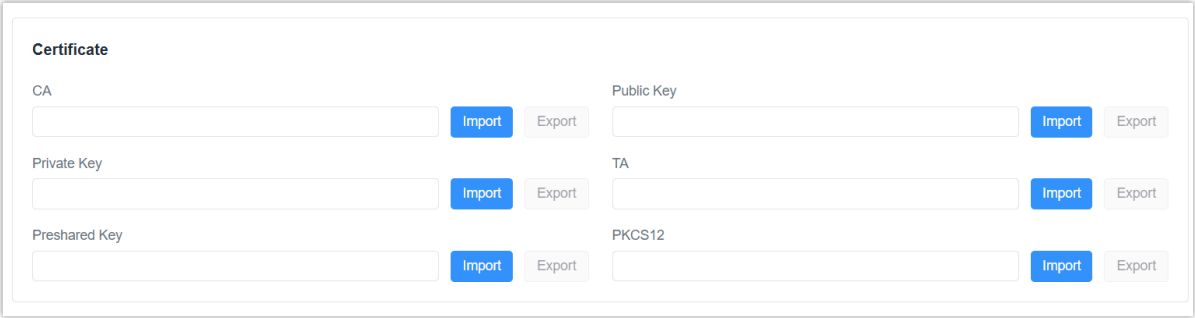


Parameter	Description
Enable	Enable or disable this OpenVPN client. The gateway supports running at most 3 clients.
Configuration Method	Select the configuration method.

Parameter	Description
	Page Configuration: Configure via webpage. **File Configuration:** Configure by importing configuration file including the parameters and certificate contents.
File Configuration	
Configuration File	Click **Import** to upload the `.ovpn` configuration file. Please refer to the client configuration file according to sample: client.conf
Page Configuration	
Protocol	Select the protocol from UDP and TCP to communicate with remote server.
Remote IP Address	The IP address or domain name of the OpenVPN server.
Port	The port number of the OpenVPN service. Make sure this port is open in the firewall.
Interface	Select the virtual interface type from Tap and Tun. Tun devices encapsulate IPv4 or IPv6 (OSI Layer 3) while Tap devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication	Select the method to authenticate the VPN network. **None:** No need any authentication. **Pre-shared:** Use the static key file. **Username/Password:** Use username/password which is preset in server side. **X.509 cert:** Use certificates. **X.509 cert + user:** Use both username/password and certificates.
Local IP	When authentication type is None or Pre-shared, set the local virtual IP address.
Remote IP	When authentication type is None or Pre-shared and Interface is Tun, set the remote side virtual IP address.
Local Subnet Mask	When authentication type is None or Pre-shared and Interface is Tap, set the local subnet mask.
Global Traffic Forwarding	When authentication type includes X.509 cert, all data traffic will be sent out via this OpenVPN tunnel after enabled.
TLS Authentication	When authentication type includes X.509 cert, disable or enable TLS authentication. After enabled, it is necessary to import TA key file.

Parameter	Description
	Note: This option only supports `tls-auth`. For `tls-crypt`, please add option strings to export option like this: `tls-crypt /etc/openvpn/openvpn_1-ta.key`
NAT	Enable or disable NAT for this interface.
Compression	Enable or disable LZO compression algorithm.
Ping Interval	The interval to send heartbeat packet to check if the connection is alive. If this value is set on both server and client, the value pushed from the server will override the client value.
Ping Retry	If no packets are received from the server within this time, the gateway will restart the connection. If this value is set on both server and client, the value pushed from the server will override the client value.
Cipher	Select the cipher to encrypt data packets from None, AES-128-CBC, AES-192-CBC, and AES-256-CBC.
MTU	The maximum transmission unit of the packets passing this Tun/Tap virtual interface.
Max Frame Size	If the UDP data packet is over this size, it will be fragmented.
Verbose Level	Select log output verbosity level from Error (0), Warning (4), Notice (5), and Debug (6).
Expert Options	Add configuration option strings and separate them with semicolons. The supported options can be found here. **Example:** auth SHA256; key direction 1
Local Route	Click **Add** to add the local host subnet and netmask.

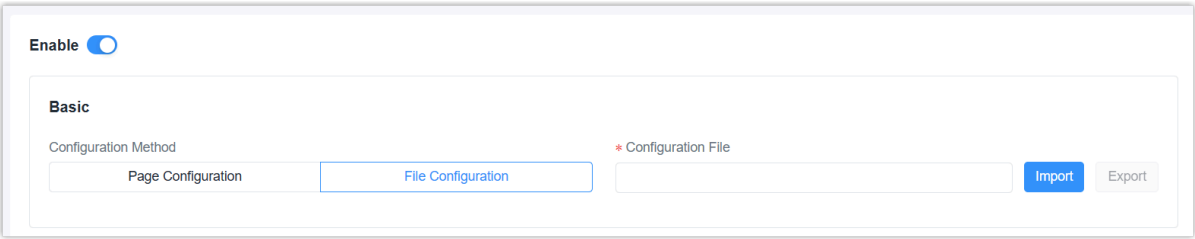
It is necessary to import certificates if using page configuration, or if the configuration file does not include certificate contents. Click here to get sample key files.



Certificate Type	Description
CA	Import root CA certificate file (.crt) when authentication type includes X.509 cert. This must match the server.
Public Key	Import client certificate file (.crt) when authentication type includes X.509 cert.
Private Key	Import local client private key file (.key) when authentication type includes X.509 cert.
TA	Import ta key file (.key) when authentication type includes X.509 cert and TLS authentication is enabled.
Preshared Key	Import static key file (.key) when authentication type is Pre-shared. This must match the server.
PKCS12	Import a PCKS (.p12) file including CA, Public Key and Private Key contents. This can simplify the file management and import process.

OpenVPN Server

The gateway supports working as OpenVPN server to allow the connections of OpenVPN clients. This requires the gateway has a reachable address for all clients.



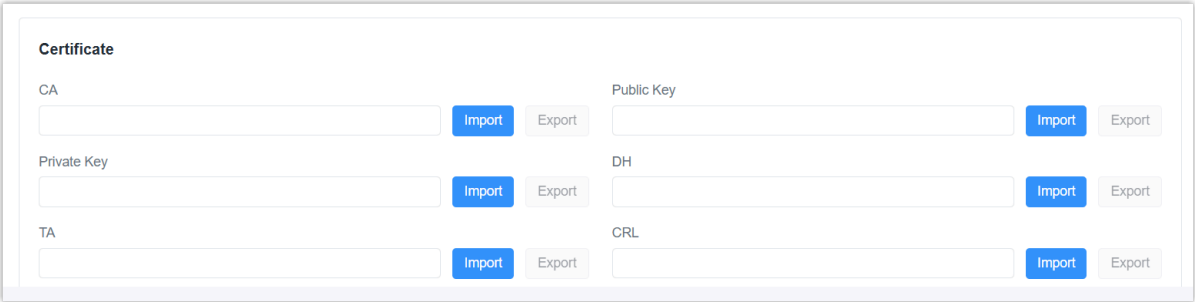
Parameter	Description
Enable	Enable or disable this OpenVPN server.
Configuration Method	Select the configuration method.

Parameter	Description
	Page Configuration: Configure via webpage. **File Configuration:** Configure by importing configuration file including the parameters and certificate contents.
File Configuration	
Configuration File	Click **Import** to upload the `.ovpn` configuration file. Please refer to the client configuration file according to sample: server.conf
Page Configuration	
Protocol	Select the protocol from UDP and TCP to communicate with remote clients.
Port	The port number of the OpenVPN service. Make sure this port is open in the firewall.
Listen IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.
Interface	Select the virtual interface type from Tap and Tun. Tun devices encapsulate IPv4 or IPv6 (OSI Layer 3) while Tap devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication	Select the method to authenticate the VPN network. **None:** No need any authentication. **Pre-shared:** Use the static key file. **Username/Password:** Use username/password. **X.509 cert:** Use certificates. **X.509 cert + user:** Use both username/password and certificates.
Local IP	When authentication type is None or Pre-shared, set the local virtual IP address.
Remote IP	When authentication type is None or Pre-shared and Interface is Tun, set the remote side virtual IP address.
Local Subnet Mask	When authentication type is None or Pre-shared and Interface is Tap, set the local subnet mask.
Client Subnet	When authentication type includes username/password or x.509 cert, define an IP address pool for openVPN clients.
Client Submask	Set the submask for the client subnet.
Renegotiation Interval	Renegotiate the data channel key after this interval. 0 means disabled.

Parameter	Description
Max Clients	The maximum number of client connections allowed. Range: 1-128
Enable TLS Authentication	When authentication type includes X.509 cert, disable or enable TLS authentication. After enabled, it is necessary to import TA key file. **Note:** This option only supports `tls-auth`. For `tls-crypt`, please add option strings to export option like this: `tls-crypt /etc/openvpn/openvpn_1-ta.key`
Enable CRL	When authentication type includes username/password or x.509 cert, enable or disable CRL verify.
Enable Client to Client	When authentication type includes username/password or x.509 cert, enable or disable clients to communicate with each other.
Enable Dup Client	When authentication type includes username/password or x.509 cert, enable or disable clients to use the same certificates or username/password to connect to this server.
NAT	Enable or disable NAT for this interface.
Compression	Enable or disable LZO compression algorithm.
Ping Interval	The interval to send heartbeat packet to check if the connection is alive. If this value is set on both server and client, the value pushed from the server will override the client value.
Ping Retry	If no packets are received from the server within this time, the gateway will restart the connection. If this value is set on both server and client, the value pushed from the server will override the client value.
Cipher	Select the cipher to encrypt data packets from None, AES-128-CBC, AES-192-CBC, and AES-256-CBC.
MTU	The maximum transmission unit of the packets passing this Tun/Tap virtual interface.
Max Frame Size	If the UDP data packet is over this size, it will be fragmented.
Verbose Level	Select log output verbosity level from Error (0), Warning (4), Notice (5), and Debug (6).
Expert Options	Add configuration option strings and separate them with semicolons. The supported options can be found here.

Parameter	Description
	Example: auth SHA256; key direction 1
Account	Click **Add** to add username/password for OpenVPN client when authentication type includes username/password.
Local Route	Click **Add** to add the local host subnet and netmask.
Client Subnet	Click **Add** to add the subnet of OpenVPN Clients. The subnet name must be OpenVPN client certificate common name.

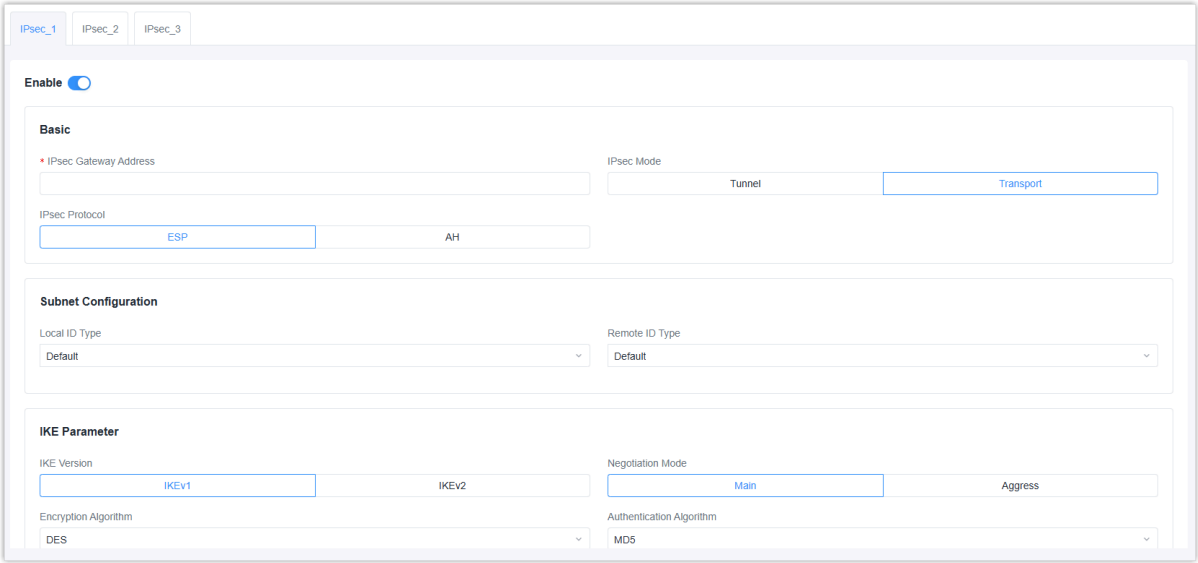
It is necessary to import certificates if using page configuration, or if the configuration file does not include certificate contents. Click here to get sample key files.



Certificate Type	Description
CA	Import root CA certificate file (.crt) when authentication type includes X.509 cert.
Public Key	Import server certificate file (.crt) when authentication type includes X.509 cert.
Private Key	Import server private key file (.key) when authentication type includes X.509 cert.
DH	Import DH group file (.pem).
TA	Import ta key file (.key) when TLS authentication is enabled.
CRL	Import CRL file (.pem) when CRL verify is enabled.
Preshared Key	Import static key file (.key) when authentication type is Pre-shared.

IPsec

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connections to private networks. The gateway supports running at most 3 clients.



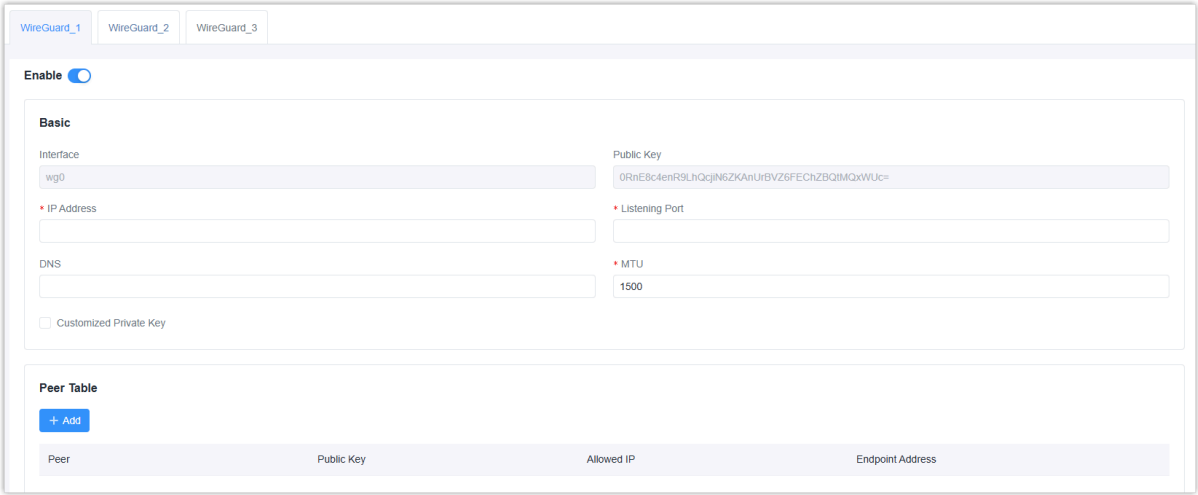
Parameter	Description
Enable	Enable or disable IPsec tunnel. A maximum of 3 IPsec tunnels is allowed.
IPsec Gateway Address	The IP address or domain name of the peer side.
IPsec Mode	Select Tunnel or Transport. **Tunnel:** It is most commonly used for configurations that need a secure connection between two different networks, separated by an intermediate untrusted network (like the Internet). **Transport:** It is commonly used when fast and secure end-to-end communications are required, such as client-server communications (workstation-to-gateway and host-to-host scenarios).
IPsec Protocol	Select ESP or AH.
Subnet Configuration	
Local ID Type	Select the identifier type to send to remote peer. **Default:** None **ID:** use local subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com
Remote ID Type	Select the identifier type that is the same as remote peer local ID.

Parameter	Description
	Default: None **ID:** use remote subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com
Local Subnet	When IPsec mode is Tunnel, set the local LAN subnet.
Local Subnet Mask	When IPsec mode is Tunnel, set the local LAN subnet mask.
Remote Subnet	When IPsec mode is Tunnel, set the remote LAN subnet.
Remote Sub-net Mask	When IPsec mode is Tunnel, set the remote LAN subnet mask.
IKE Parameter	
IKE Version	Select IKEv1 or IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select from AES128, AES192, and AES256.
Authentica-tion Algorithm	Select MD5 or SHA1.
DH Group	Select from MODP768-1, MODP1024-2 or MODP1536-5.
Local Authen-tication Type	Select PSK or CA. **PSK:** Use pre-shared key to complete the authentication. It requires entering the local secret key value the same as peer. **CA:** Use certificate to complete the authentication. After selecting, it is necessary to import CA certificate, client certificate and private key to corresponding fields.
Remote Authen-tication Type	When using IKEv2, select PSK or CA. **PSK:** Use pre-shared key to complete the authentication. It requires entering the remote secret key value. **CA:** Use certificate to complete the authentication. After selecting, it is necessary to import server certificate to corresponding field.
Lifetime	The last time before IKE re-negotiation.

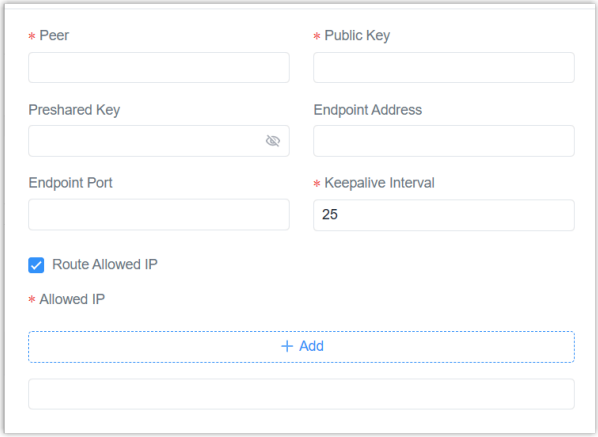
Parameter	Description
XAUTH	When using IKEv1, define XAUTH username and password to reply to an XAUTH request after XAUTH is enabled.
SA Parameter	
SA Algorithm	Select from AES128-SHA1, AES128-MD5, AES192-SHA1, AES192-MD5, AES256-SHA1, and AES256-MD5.
PFS Group	Select from NULL, MODP768-1, MODP1024-2 or MODP1536-5.
DPD Time Interval	The retry interval to send DPD requests.
DPD Timeout	When using IKEv1, set DPD timeout to detect the remote side fails.
Lifetime	The last time before SA re-negotiation.
IPsec Advanced	
VPN Over IPsec Type	Select whether to enable L2TP over IPsec. If L2TP is selected, it is necessary to select the L2TP tunnel.
Enable Compression	Enable or disable to compress the head of IP packets.
Certificate	
CA	Import root CA certificate file (.crt) when local authentication type is CA.
Client Certificate	Import client certificate file (.crt) when local authentication type is CA.
Server Certificate	Import server certificate file (.crt) when remote authentication type is CA.
Private Key	Import local client private key file (.key) when local authentication type is CA.
CRL	Import Certificate Revocation List as required.

WireGuard

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. WireGuard passes traffic over UDP protocol.

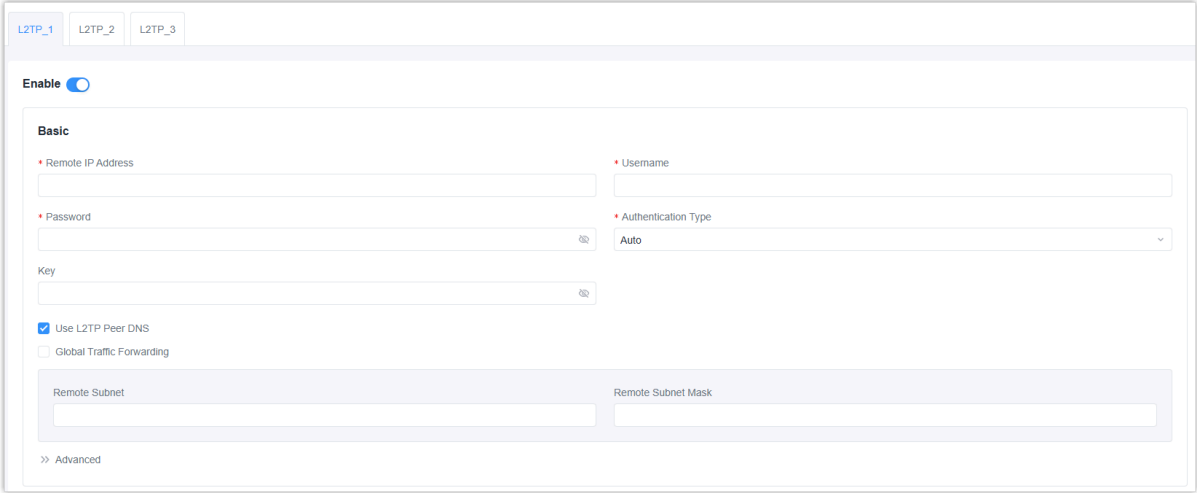


Parameter	Description
Enable	Enable or disable WireGuard interface. A maximum of 3 WireGuard interfaces is allowed.
Interface	Display the WireGuard interface name.
Public Key	Display the public key generated by the private key.
IP Address	The local virtual IP address and netmask. Example: 10.8.0.2/24
Listening Port	The port to send or receive WireGuard packets. The port numbers of different WireGuard interfaces should be different.
DNS	The DNS server address of this WireGuard interface. If left blank, the device will use DNS server address of common network interfaces (WAN, cellular, etc.).
MTU	The maximum transmission unit of this WireGuard interface.
Customized Private Key	Enable or disable to customize the private key of this WireGuard interface. If disabled, the client will use the private key generated by this device.
Peer Table	Click **+Add** to WireGuard peers of this WireGuard interface.

Parameter	Description
	 **Peer:** A unique peer name. **Public Key:** The public key of the peer. **Preshared Key:** Set the preshared key. Both this interface and the peer interface must use the same key value. **Endpoint Address:** The IP address or domain name of the peer. **Endpoint Port:** The destination port of the peer. **Keepalive Interval:** After connected, the interval to send heartbeat packets regularly to keep alive. 0 means disabled. **Route Allowed IP:** Enable or disable to add static routings of allowed IP addresses. **Allowed IP:** The real IP address and netmask of the WireGuard peer's LAN network. One WireGuard peer supports to add 8 allowed IP addresses. Example: 192.168.1.0/24

L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

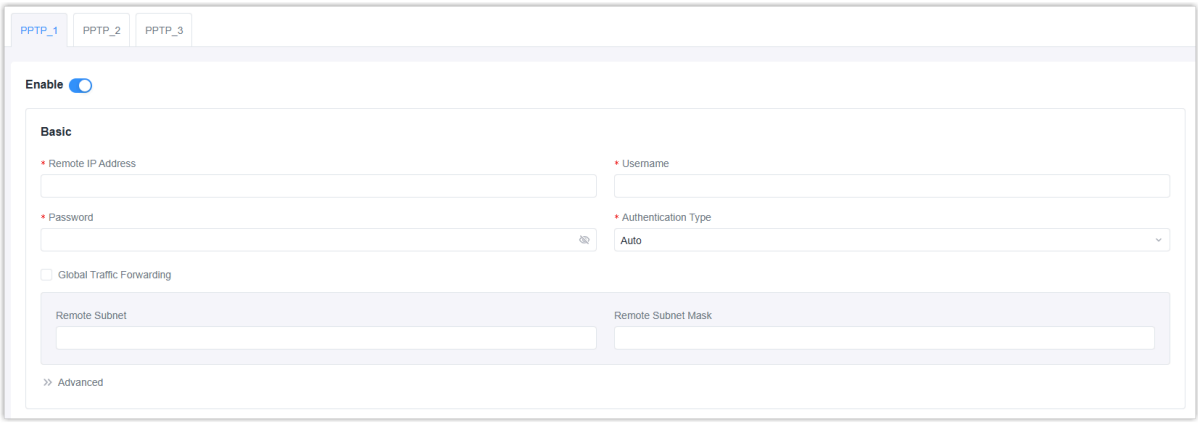


Parameter	Description
Enable	Enable or disable L2TP client. A maximum of 3 L2TP clients is allowed.
Remote IP Address	The IP address or domain name of the L2TP server.
Username	Username used for authentication to the L2TP server.
Password	Password used for authentication to the L2TP server.
Authentication Type	Select from Auto, PAP, CHAP, MS-CHAPv1, and MS-CHAPv2.
Key	The key used for L2TP tunnel authentication.
Use L2TP Peer DNS	Enable or disable to use the DNS address of peer L2TP server.
Global Traffic Forwarding	All data traffic will be sent out via this VPN tunnel after enabled. If disabled, it is necessary to set the remote subnet and mask.
Advanced	
Local IP Address	The local tunnel IP address of this client. If left blank, the client will obtain the tunnel IP address from the server.
Peer IP Address	The peer tunnel IP address.
Asyncmap Value	Define which ASCII control characters should be escaped on an asynchronous link. Range: 0-ffffffff.
MRU	The maximum receiving unit of the packets passing this L2TP interface.
MTU	The maximum transmission unit of the packets passing this L2TP interface.
Link Detection Interval	The interval to send heartbeat packet to check if the connection is alive.

Parameter	Description
Max Retries Times	If no packets are received from the server within this time, the gateway will restart the connection.
Expert Options	Add configuration option strings and separate them with semicolons.
Enable NAT	Enable or disable NAT for this interface.
Enable MPPE	Enable or disable MPPE encryption.
Address/Control Compression	Enable or disable Address and Control Field Compression (ACFC).
Protocol Field Compression	Enable or disable protocol Field Compression (PFC).

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.



Parameter	Description
Enable	Enable or disable PPTP client. A maximum of 3 **PPTP** clients is allowed.
Remote IP Address	The IP address or domain name of the PPTP server.
Username	Username used for authentication to the PPTP server.
Password	Password used for authentication to the PPTP server.
Authentication Type	Select from Auto, PAP, CHAP, MS-CHAPv1, and MS-CHAPv2.

Parameter	Description
Global Traffic Forwarding	All data traffic will be sent out via this VPN tunnel after enabled. If disabled, it is necessary to set the remote subnet and mask.
Advanced	
Local IP Address	The local tunnel IP address of this client. If left blank, the client will obtain the tunnel IP address from the server.
Peer IP Address	The peer tunnel IP address.
Asyncmap Value	Define which ASCII control characters should be escaped on an asynchronous link. Range: 0-ffffffff.
MRU	The maximum receiving unit of the packets passing this PPTP interface.
MTU	The maximum transmission unit of the packets passing this PPTP interface.
Link Detection Interval	The interval to send heartbeat packet to check if the connection is alive.
Max Retries Times	If no packets are received from the server within this time, the gateway will restart the connection.
Expert Options	Add configuration option strings and separate them with semicolons.
Enable NAT	Enable or disable NAT for this interface.
Enable MPPE	Enable or disable MPPE encryption.
Address/Control Compression	Enable or disable Address and Control Field Compression (ACFC).
Protocol Field Compression	Enable or disable protocol Field Compression (PFC).

Chapter 7. Platform Management

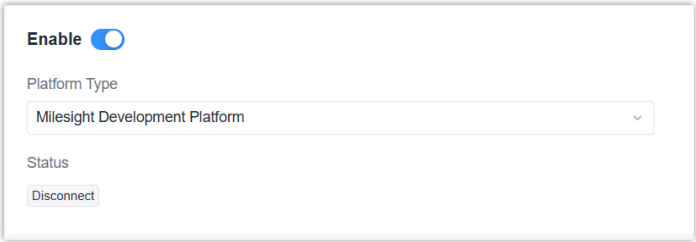
This chapter describes how to connect the device to Milesight remote management platform.

Prerequisites

- The device has accessed the Internet network.
- Milesight Development Platform account and enterprise have been created, and device addition is supported.

Steps

1. On the left bar, select **Platform Management** page.
2. Enable the device to connect to the platform.



3. Click **Apply** to save the settings.
4. Add the device to the platform. For more details, refer to Connect a Device.
5. Check if connection status changes to Connected on the platform and the device.

Chapter 8. System

General

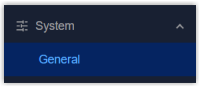
This chapter describes the general access settings and time settings.

General

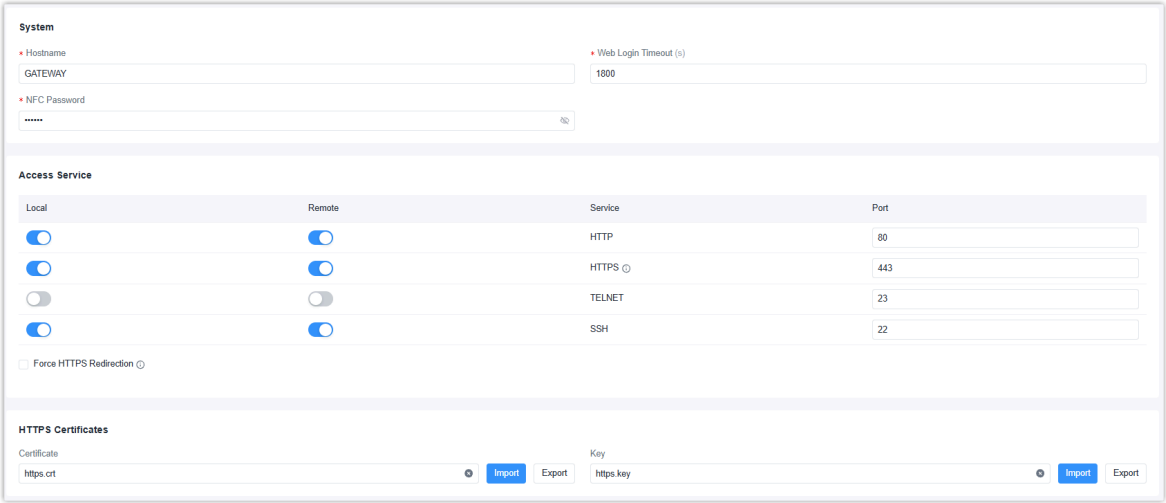
This page is used to set up some basic parameters and access parameters.

Steps:

1. On the left bar, select **System > General** page.



2. On the top bar, select **General** tab.
3. Configure the general parameters as required.



Parameter	Description
System	
Hostname	Define a unique name to identify this device.
Web Login Timeout	After this timeout, the web GUI will log out automatically. Range: 100-3600s.
NFC Password	Define the password for writing configuration to Milesight LoRaWAN® end devices.

Parameter	Description
Access Service	
Local	Enable or disable the service to access the device locally.
Remote	Enable or disable the service to access the device remotely.
Service	The device supports web access via HTTP/HTTPS or CLI access via SSH/TELNET.
Port	Set the port number of the service. Each service must use a unique port.
Force HTTPS Redirection	Once enabled, when HTTPS access service is enabled, HTTP access will automatically redirect to HTTPS.
HTTPS Certificates	
Certificate	The gateway has preloaded certificate and key files for HTTPS access. **Import**: Click to import customized files. **Export**: Click to export the files.
Key	

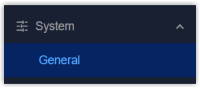
4. Click **Apply** to save the settings.

System Time

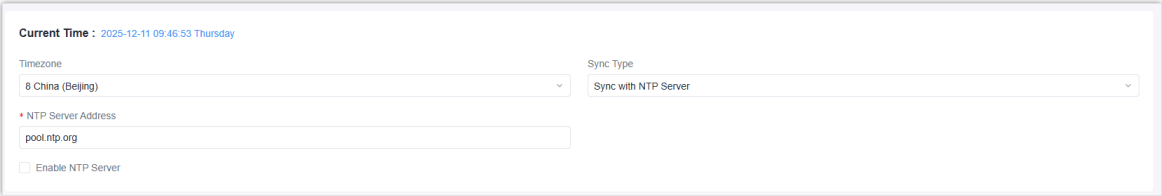
This page is used to configure the device system time parameters.

Steps:

1. On the left bar, select **System > General** page.



2. On the top bar, select **System Time** tab.
3. Configure the general parameters as required.



Parameter	Description
Current Time	Displays the current device time.
Timezone	Select the time zone of the device.
Sync Type	Select the time sync source among Sync with Browser, Sync with NTP server or Set up Manually.
Sync with NTP Server	
NTP Server Address	Set the NTP server address (domain name/IP) to synchronize the time. This requires the gateway to be able to access this server.
Enable NTP Server	After enabled, the device can work as an NTP server to provide time to other connected devices.

4. Click **Apply** to save the settings.

User

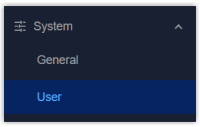
This chapter describes how to change the account info and add sub-users.

Account

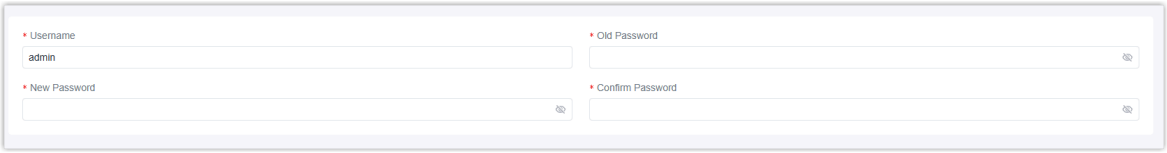
This section is used to change current account info.

Steps:

1. On the left bar, select **System > User** page.



2. On the top bar, select **Account** tab.
3. Change the info of the current account as required.



Parameter	Description
Username	Enter a new username. Only lowercase letters, digits, "-" and "_" are allowed, and the first character must be a letter or "_". Length limitation: 1-31 characters.
Old Password	Enter the old password.
New Password	Enter a new password. Only ASCII characters are allowed except spaces. The password must contain at least one letter and one number, and be 5 to 31 characters long.
Confirm Password	Enter the new password again.

4. Click **Apply** to save the settings.

User Management

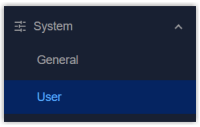
This section is used to add and manage sub-accounts of the device.

Prerequisites

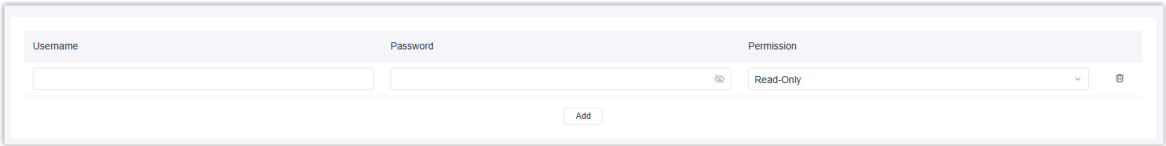
Current account is administrator account.

Steps:

1. On the left bar, select **System > User** page.



2. On the top bar, select **User Management** tab.
3. Click **Add** to add a sub-account, and configure the account info.



Parameter	Description
Username	Enter a new username. Only lowercase letters, digits, "-" and "_" are allowed, and the first character must be a letter or "_". Length limitation: 1-31.

Parameter	Description
Password	Enter a password. Only ASCII characters are allowed except spaces. The password must contain at least one letter and one number, and be 5 to 31 characters long.
Permission	Select the permission of this sub-account. **Read-Write**: Allows the users to read and write all configurations. **Read-Only**: Allows the users to read all configurations and configure below settings: ◦ User debug tools under **System > Maintenance > Tools** page. ◦ Download logs under **System > Log** page. ◦ Change current account info under **System > User** page.
	Delete this sub-account.

4. Click **Apply** to save the settings.

Service

This chapter describes how to configure email settings and phone settings.

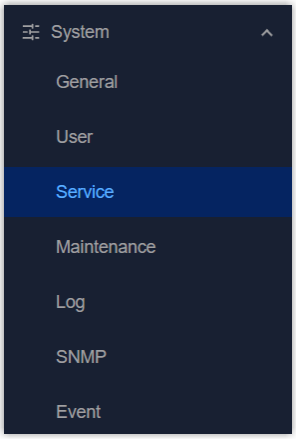
SMTP

The device supports working as a SMTP client to send or receive emails.

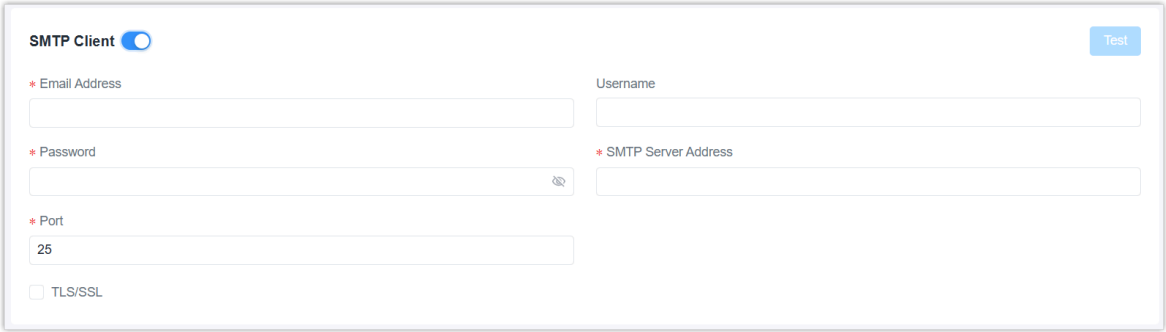
Prerequisites: A working email address information, and ensure the email address allows third-party app access.

Steps:

1. On the left bar, select **System > Service** page.



2. On the top bar, select **SMTP** tab.
3. Enable the SMTP client and configure the related parameters.



Parameter	Description
SMTP Client	Enable or disable SMTP client.
Email Address	The address used for sending emails. Format: xxx@xxx.xx
Username	Username for authentication on SMTP server.
Password	Password for authentication on SMTP server.
SMTP Server Address	The address of the email service provider's SMTP server.
Port	The port of the email service provider's SMTP server.
TLS/SSL	Enable or disable TLS/SSL authentication.

4. Click **Apply** to save the settings.
5. Click **Test** button on the right corner to check if the settings take effect.

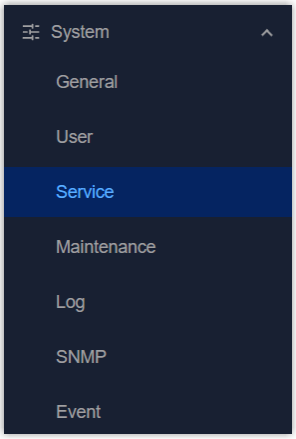
Email

This page is used to configure email groups to send Email alarms.

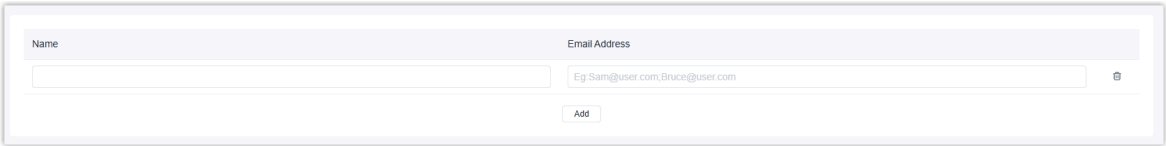
Prerequisites: The SMTP client settings take effect.

Steps:

1. On the left bar, select **System > Service** page.



2. On the top bar, select **Email** tab.
3. Click **Add** to add an email group and configure the related parameters.



Parameter	Description
Name	Set a unique name to identify this email group.
Email Address	Enter email addresses into the email group, separating each address with a semicolon.
	Delete this email group.

4. Click **Apply** to save the settings.

Phone

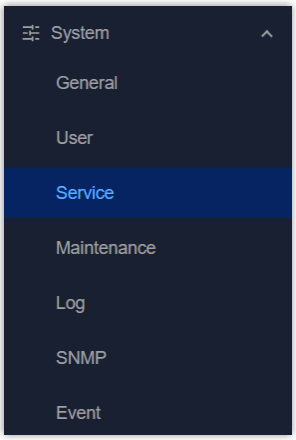
This page is used to configure phone groups to send alarms.

Prerequisites:

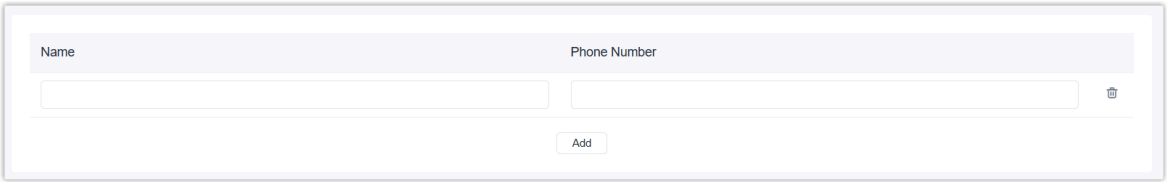
- This feature is only available for -L08GL model.
- Ensure the used SIM card supports SMS services.
- SMS Center Number is configured correctly.

Steps:

1. On the left bar, select **System > Service** page.



2. On the top bar, select **Phone** tab.
3. Click **Add** to add a phone group and configure the related parameters.



Parameter	Description
Name	Set a unique name to identify this phone group.
Phone Number	Enter phone numbers into the phone group, separating each number with a semicolon.
	Delete this phone group.

4. Click **Apply** to save the settings.

Related information

Event

Maintenance

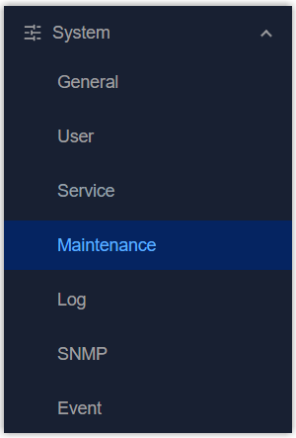
This chapter describes the maintenance tools and features.

Tools

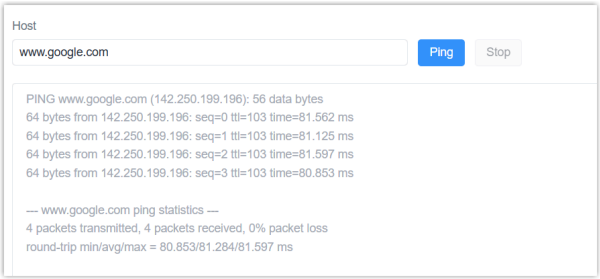
This section is used to check network connectivity via different tools.

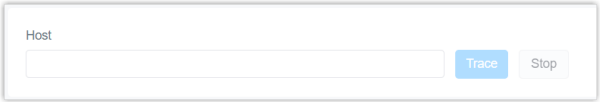
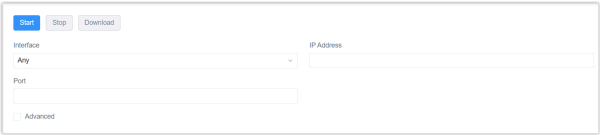
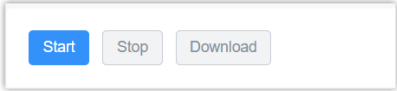
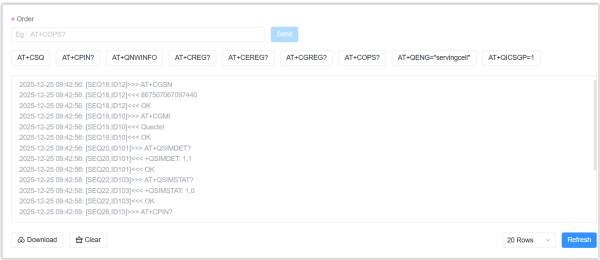
Steps:

1. On the left bar, select **System > Maintenance** page.



2. On the top bar, select **Tools** tab.
3. The device provides 5 tools for debugging. Please select according to your problems.

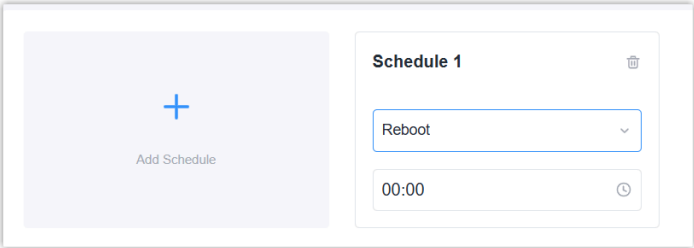
Tool	Feature	Steps
Ping	Test network connectivity and latency between the device and target hosts.	 a. Enter an IP address or a domain name. b. Click **Ping**.

Tool	Feature	Steps
Traceroute	Trace the route that packets take from the device to the target host.	 a. Enter an IP address or a domain name. b. Click **Trace**.
Packet Analyzer	Capture network packets passing through the device network interfaces via TCP-DUMP.	 a. Configure the packet capture conditions like interface, IP address or port. For more complex requirements, enable **Advanced** and enter the TCP-DUMP command. b. Click **Start** and wait for a while. c. Click **Stop** to stop capturing. d. Click **Download** to download .pcap file. e. Use a tool to analyze the file, or send it to Milesight technical support.
Qxdmlog	Collect diagnostic logs from cellular modules.	 a. Click **Start** and wait for more than 2 minutes. b. Click **Stop** to stop collecting. c. Click **Download** to download the logs and send them to Milesight technical support.
Cellular AT Debug	Send AT commands to get debug info from cellular module or configure the module.	

Tool	Feature	Steps
		a. Enter the AT commands, click **Send**. Or click the preset command buttons to send directly. b. Check the cellular logs on the box, and click **Download** to download the log files as required. c. Send the file to Milesight technical support.

Schedule

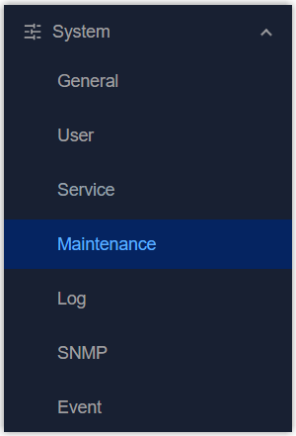
This section is used to add schedule reboot settings.



Prerequisites: Ensure the device time is correct.

Steps:

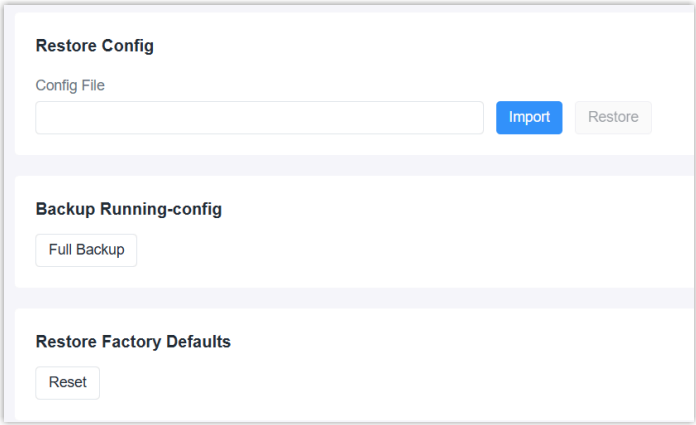
1. On the left bar, select **System > Maintenance** page.



2. On the top bar, select **Schedule** tab.
3. Click **Add Schedule** to add a new schedule.
4. Select the reboot event and select the reboot time.
5. Click **Apply** to save the settings.

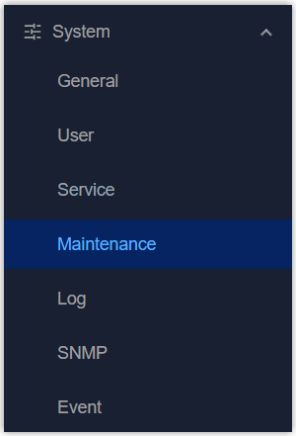
Backup and Restore

This section is used to backup and restore settings.



Backup and Restore Steps:

1. On the left bar, select **System > Maintenance** page.



2. On the top bar, select **Backup and Restore** tab.
3. Click **Full Backup** to download the configuration file of current device.
4. Open the web GUI of a new device, click **Import** to select the configuration file from the local path.
5. Click **Restore** to import the configurations to a new device.

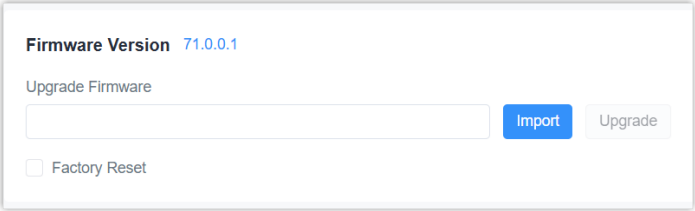
Factory Reset Steps:

1. Click **Reset** to reset factory default settings.

> **Note:**
> If it is not possible to log in to the web GUI, please use the reset button to reset the device.

Upgrade

This section is used to upgrade the device.

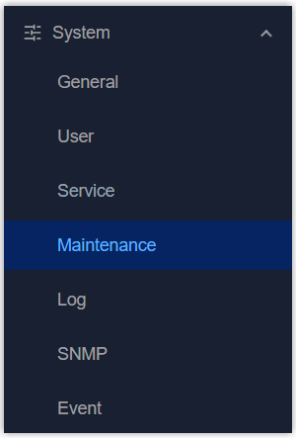


Prerequisites:

- Download the correct device firmware file from Milesight official website. It is recommended to consult technical support before upgrading to ensure a safe and successful upgrade.
- Ensure the network connection is stable enough for upgrade.

Steps:

1. On the left bar, select **System > Maintenance** page.



2. On the top bar, select **Upgrade** tab.
3. Click **Import** to select the firmware file from the local path.
4. Enable **Factory Reset** as required. After enabled, the device will reset factory default settings after upgrade.
5. Click **Upgrade** to upgrade the device.

> **CAUTION:**
> Any operation on web page is not allowed during firmware upgrade; otherwise, the upgrade will be interrupted, or the device may even become inoperable.

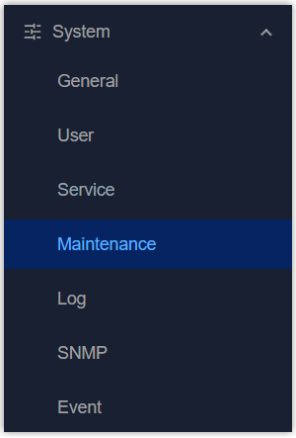
6. When the SYS LED of the device turns to static green, log in to the web GUI to verify that the upgrade was successful.

Reboot

This section is used to reboot the device.

Steps:

1. On the left bar, select **System > Maintenance** page.



2. On the top bar, select **Reboot** tab.
3. Click **Reboot** to reboot this device.

Log

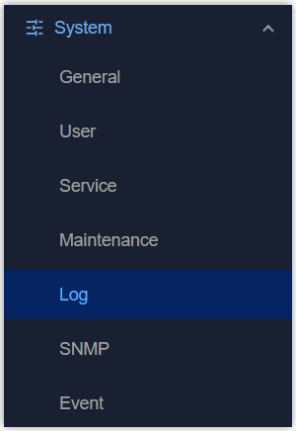
This chapter describes how to get device logs used for debug.

Prerequisites

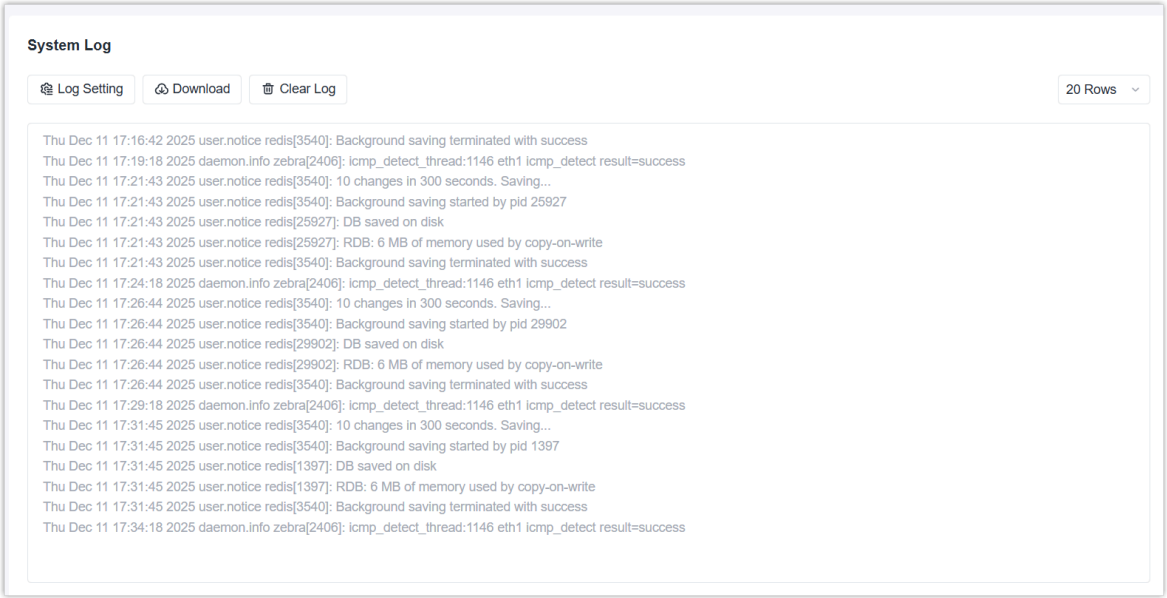
Ensure the device system time is correct.

Steps

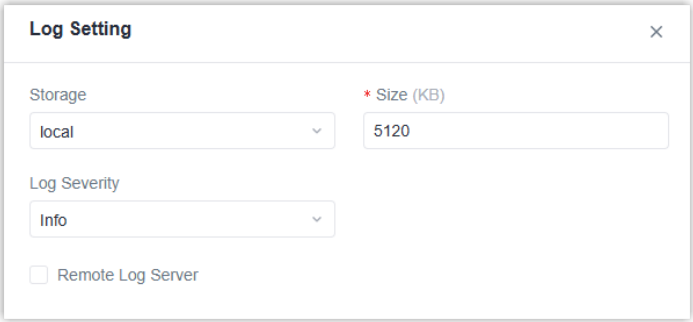
1. On the left bar, select **System > Log** page.



2. The system logs will display in the view. If you require updating the logs in the view, please switch to other pages and then return to this one.



3. Click **Log Setting** to configure related parameters, then click **Save**.



Parameter	Description
Storage	Select the log storage location.
Size	Set the log file size to store.
Log Severity	Select the severity to display the logs. To submit logs to technical support, it is recommended to set the log severity to Debug. **Note:** After changing the log severity, please replicate the issue to ensure the logs capture the details.
Remote Log Server	Enable or disable to send all log files to a remote server. **Syslog Server Address:** Set the remote log server address (IP/domain name). **Port:** Set the remote log server port.

4. Click **Download** to download all log files as required. You can unzip the log files to check directly or send them all to Milesight technical support.

SNMP

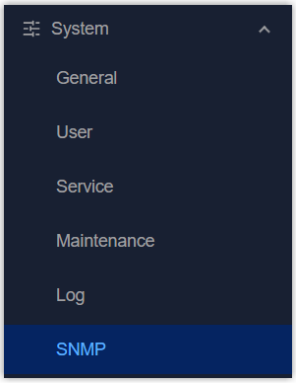
This chapter gives an overview of the SNMP feature in this device.

Overview

Simple Network Management Protocol (SNMP) is a network management protocol used for collecting information and configuring network devices.

Steps:

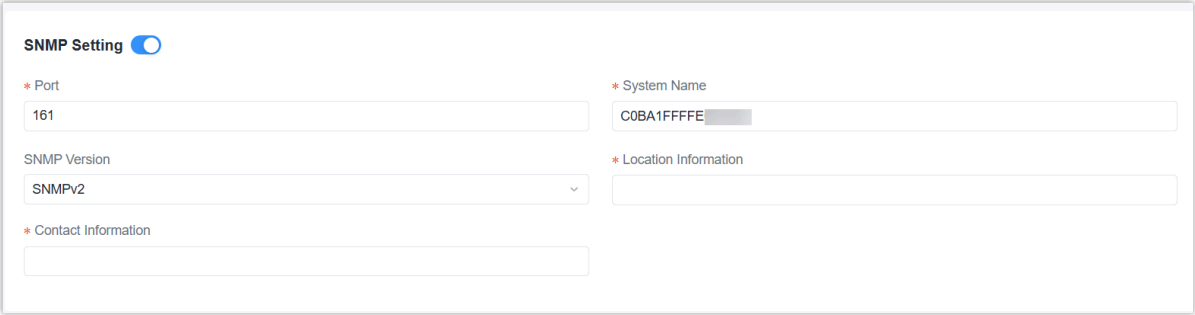
1. On the left bar, select **System > SNMP** page.



2. Select **SNMP** tab to enable SNMP feature and configure general SNMP information, then click **Apply** to save the settings.
3. (Optional) Select **MIB View** tab to add MIB views to define different access ranges, then click **Apply** to save the settings.
4. (Optional) Select **VACM** tab to add communities or users to manage the access permissions, then click **Apply** to save the settings.
5. (Optional) Select **Trap** tab to enable SNMP trap feature and configure the information to receive SNMP traps, then click **Apply** to save the settings.
6. Select **MIB** tab to download the MIB files, then import the files to any SNMP MIB browser tool to check the device status and configuration variables.

SNMP Setting

This page is used to configure general SNMP information.

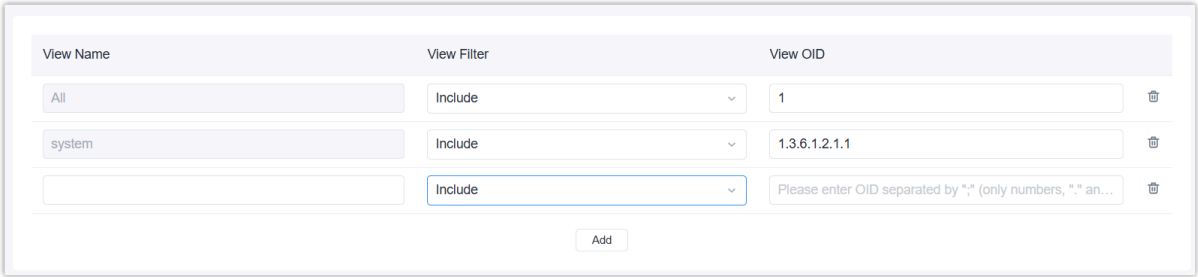


Parameter	Description
SNMP Setting	Enable or disable the device to work as an SNMP agent.
Port	The port of SNMP service.

Parameter	Description
System Name	The name to represent this device system.
SNMP Version	Select the version from SNMPv1, SNMPv2 and SNMPv3.
Location Information	The location of the system.
Contact Information	The contact information of the system.

MIB View

This page is used to add and manage MIB views to define the access ranges.

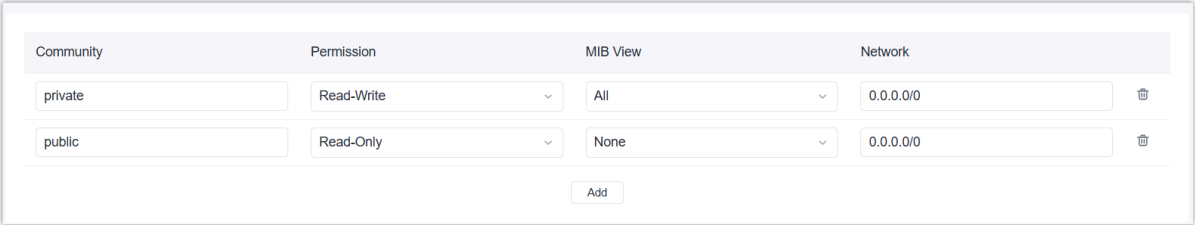


Parameter	Description
Add	Add a MIB view.
View Name	Define a unique MIB view name.
View Filter	Select the filter option to define the OID range of this MIB view. **Include:** Only support the access of listed OIDs in the MIB. **Excluded:** Only support the access of the MIB except the listed OIDs.
View OID	Enter the included or excluded access OIDs separated by semicolons.
	Delete this MIB view.

VACM

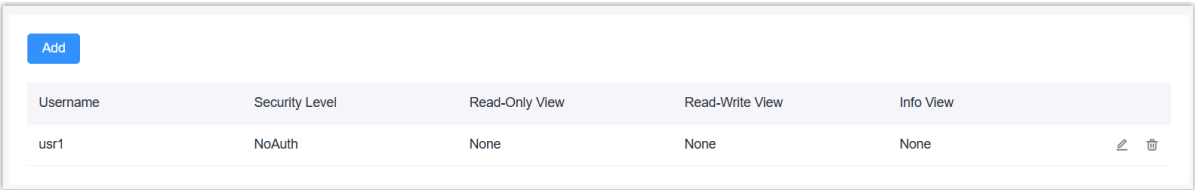
This page is used to add and manage the access permissions of communities/users.

If SNMP Version is SNMPv1/SNMPv2



Parameter	Description
Add	Add a community.
Community	Define a unique community name.
Permission	Select the access permission of this community.
MIB View	Select the accessible MIB view of this community.
Network	Enter the external IP address/subnet to allow to access this MIB view. 0.0.0.0/0 means all allows.
	Delete this community.

If SNMP version is SNMPv3

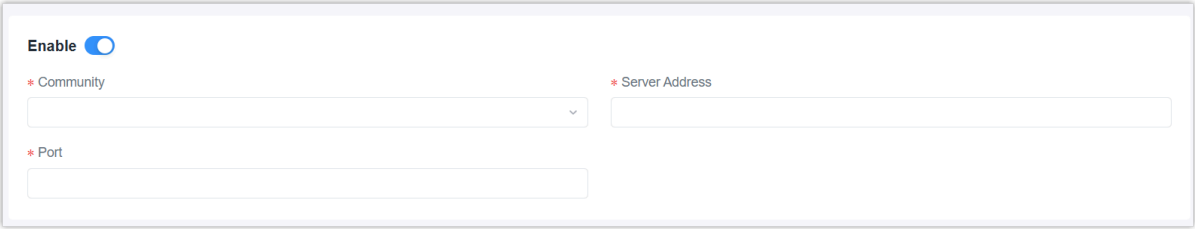


Parameter	Description
Add	Add a SNMPv3 user.
Username	Define a unique username.
Security Level	Select the authentication strategy for this user. **NoAuth:** No authentication, no privacy. **Auth/NoPriv:** Authentication, no privacy. **Auth/Priv:** Authentication, privacy. If Auth/NoPriv or Auth/Priv is selected, it needs to configure the authentication algorithm and password; if Auth/Priv is enabled, it needs to configure the encryption algorithm and password.

Parameter	Description
Read-Only View	Select the MIB view to assign this permission.
Read-Write View	
Notify View	
	Edit this user.
	Delete this user.

Trap

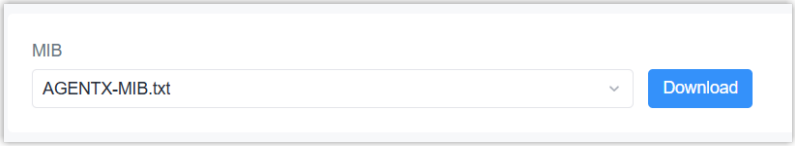
This page is used to configure SNMP trap settings. SNMP Traps are used to send real-time and unsolicited alert messages to SNMP managers when an important event happens. This allows for immediate notification rather than waiting for the manager to poll for update.



Parameter	Description
Enable	Enable or disable SNMP trap feature.
Community/User	Select the community/user to send SNMP traps.
Server Address	The IP address or domain name to send SNMP traps.
Port	The server port to send SNMP traps.

MIB

This page is used to download MIB files. These files can be imported to MIB browsers to access the status and configuration variables of this device.



Event

This chapter describes the event settings to record device related events.

Event List

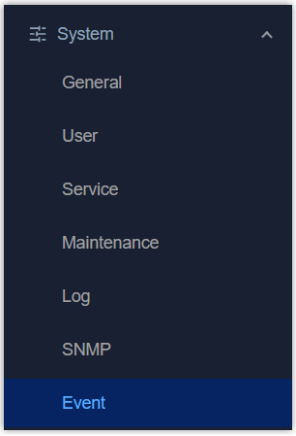
This section list events related to the device.

Time	Type	Message
2025-12-11 13:49:07	Power On	Power On
2025-12-11 13:49:02	Ethernet up	ETH1 WAN up
2025-12-11 11:59:01	Ethernet up	ETH1 WAN up
2025-12-11 11:58:58	Ethernet down	ETH1 WAN down
2025-12-11 11:49:37	Power On	Power On
2025-12-11 11:49:32	Ethernet up	ETH1 WAN up
2025-12-11 09:05:49	Power On	Power On
2025-12-10 01:00:58	Power On	Power On
2025-12-09 02:55:58	Power On	Power On
2025-11-28 01:03:41	Power On	Power On

Prerequisites: The device system time is correct.

Steps:

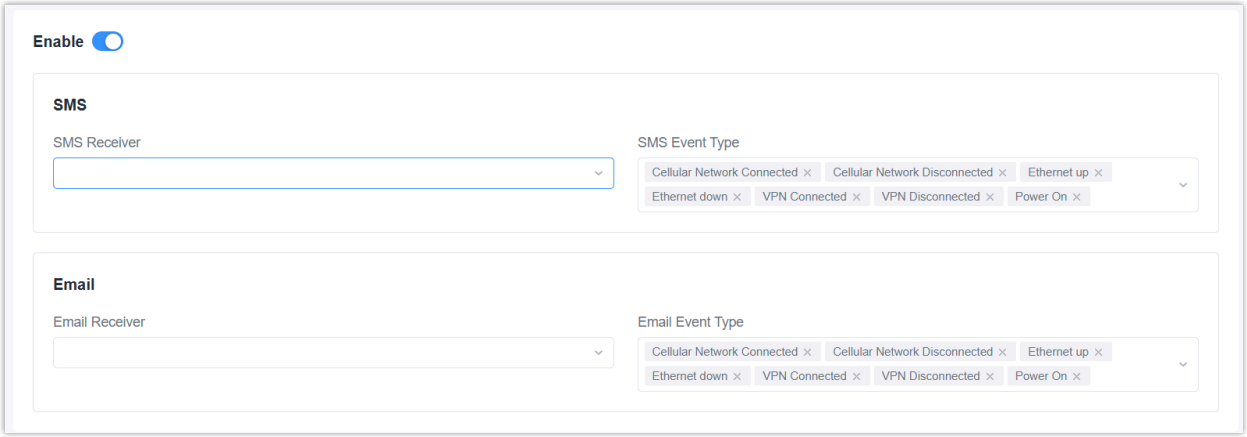
1. On the left bar, select **System > Event** page.



2. On the top bar, select **Event List** tab. The list will display device related events.

Event Notification

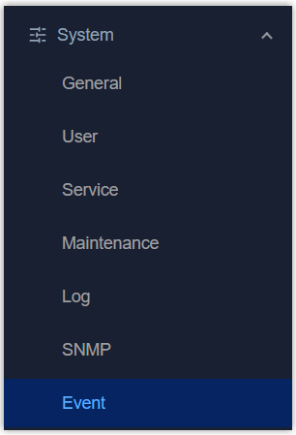
This section is used to configure the email or phone receivers to receive event alarms.



Prerequisites: The email group or phone group is added.

Steps:

1. On the left bar, select **System > Event** page.



2. On the top bar, select **Event Notification** tab.
3. Enable the event notification.
4. Select the email group and event types to send the event emails as required.
5. Select the phone group and event types to send the event SMS as required.
6. Click **Apply** to save the settings.

Chapter 9. APP

Python

This chapter describes the steps to run Python Apps to the device.

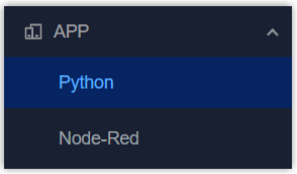
Prerequisites

- Make sure there is enough device space to import the Python Apps.
- Download Python SDK from Milesight official website.
- Develop the Python Apps and package them into ZIP files.

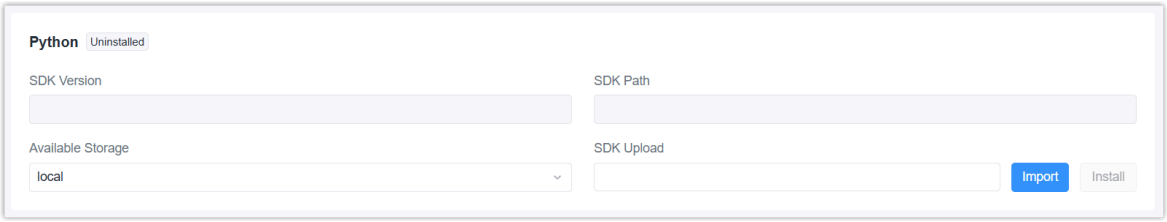
Step

Install Python SDK

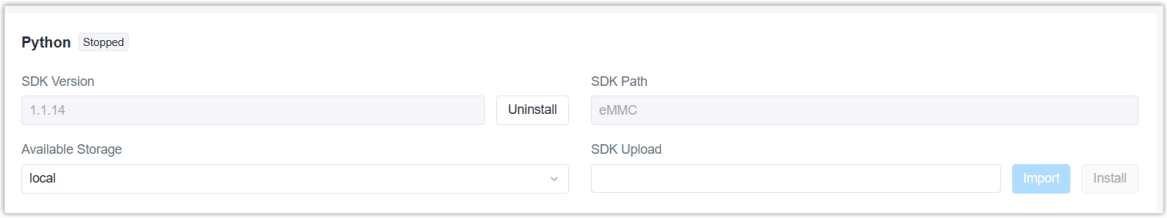
1. On the left bar, select **APP > Python** page.



2. On the top bar, select **Python** tab.
3. Click **Import** to select the Python SDK file from local path.

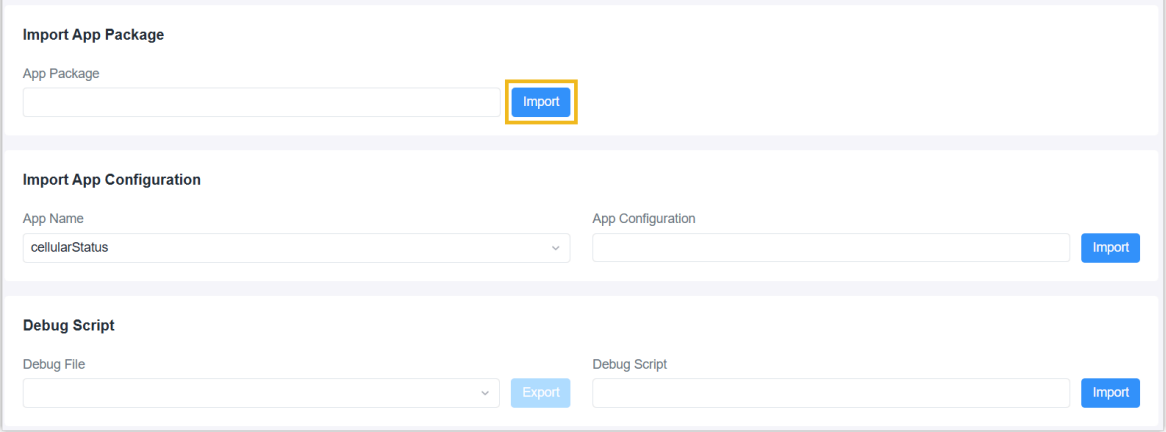


4. Click **Install** to install the Python SDK. After installing, the SDK version and path will display.

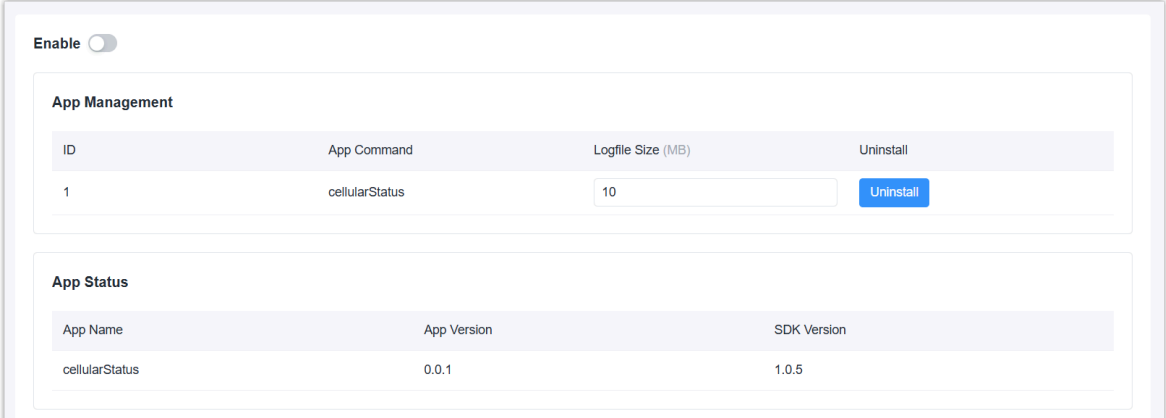


Install and Uninstall Python App

1. On the top bar, select **Python APP** tab.
2. Click **Import** to select the App file from local path and import the APP.

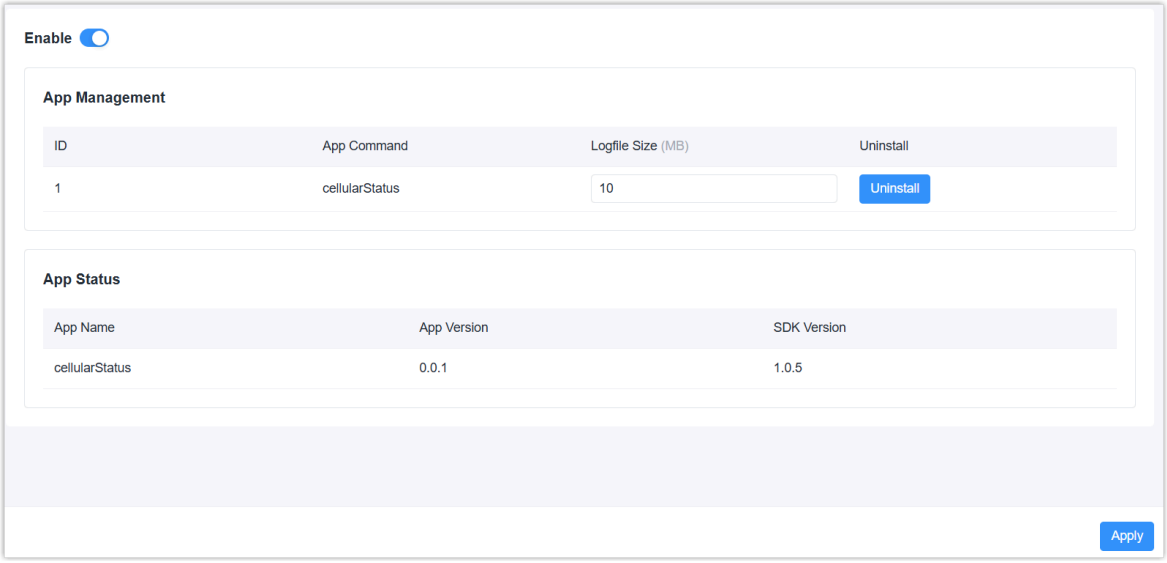


If the App is imported well, it will display on the **AppManager Configuration** page. You can click **Uninstall** as required.

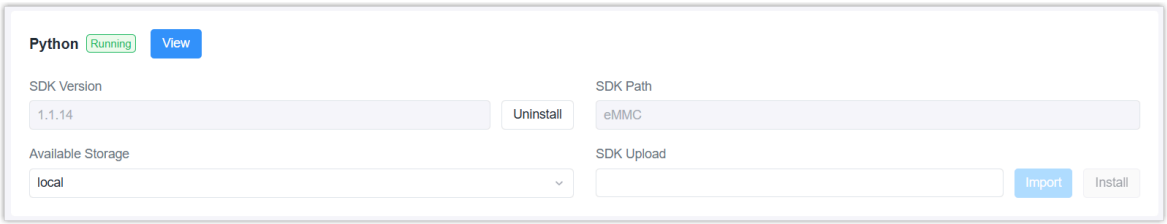


Run Python App

1. On the top bar, select **AppManager Configuration** tab.
2. Enable App Management feature, then click **Apply** to save the setting.



3. On the top bar, select **Python** tab.
4. The Python status will display as **Running**. Click **View** to check the running status and logs of the App.



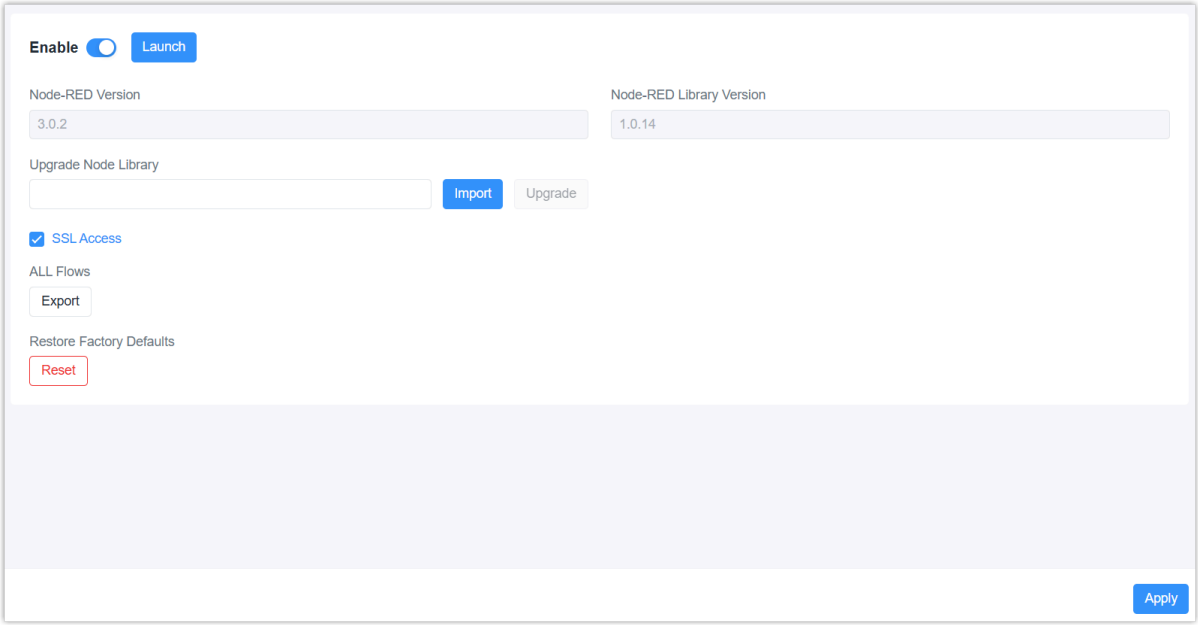
Node-RED

The gateway has built-in the Node-RED tool. This chapter introduces the Node-RED software in this gateway.

Overview

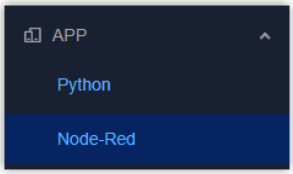
Node-RED is a flow-based development tool for visual programming and wiring together hardware devices, APIs, and online services as part of the Internet of Things. Node-RED provides a web-browser-based flow editor, which can easily wire together flows using the wide range of nodes in the palette. For more details please refer to Node-RED official website.

Start the Node-RED



Steps:

1. On the left bar, select **APP > Node-Red** page.



2. Enable the Node-RED.
3. If you require Node-RED web access via HTTPS, enable **SSL Access** option; if you require Node-RED web access via HTTP, disable **SSL Access** option.
4. Click **Apply** to save the settings and start the Node-RED.
5. Click **Launch** to open the Node-RED web GUI.
6. Log into the Node-RED web GUI using the credentials the same as gateway web GUI.

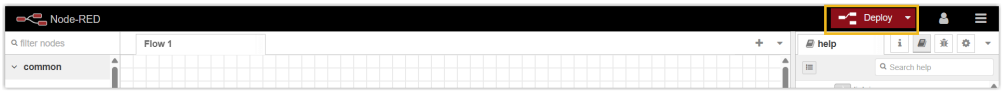
Create a New Node-RED Flow

Here are the basic steps to create a Node-RED flow, for more details please refer to Node-RED User Guide.

Steps:

1. Click "+" to add a new flow.
2. Drag and drop any nodes onto the workspace.

3. Configure the parameters of some nodes as required.
4. Connect the nodes together to make a flow.
5. Click **Deploy** in the upper right corner to save the settings.



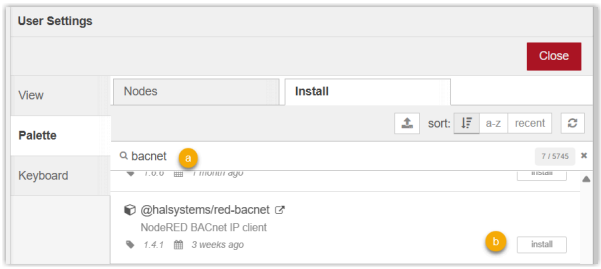
6. Trigger the flow and check the results.

Node-RED Library Update

Nodes are the basic building blocks for creating a flow. The device has preloaded the basic nodes from Node-RED official library and custom nodes from Milesight.

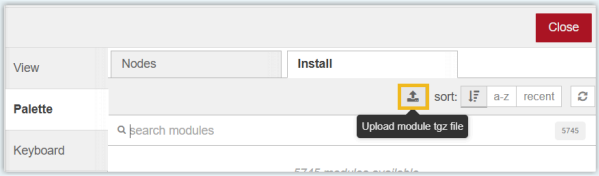
Install Node-RED Official Library Module

1. Click **Launch** to open and log in to the Node-RED web GUI.
2. Click in the upper right corner, select **Manage palette**.
3. Select **Install** tab, search for the module name and select the target one to install. This requires the device access the Internet network.



Note:

If the device cannot connect to the Internet, please search and download the node-red module package from Node-RED official library, then upload the file to the device.



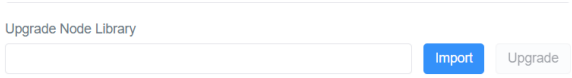
Update Custom Node-RED Library

The device has preloaded custom nodes related to the device's programs and applications:

Node	Description
LoRa Input	Input all received LoRaWAN® packets from the LoRaWAN® network.
LoRa Output	Send downlink command to the specific LoRaWAN® end device.
Device Filter	Filter out the input LoRaWAN® packets via device EUIs.
GW Info	Monitor events of the device. This needs to enable the Event Notification first.
Email Output	Send custom emails. If the SMTP Option is **Same as gateway**, it is necessary to configure the SMTP Client settings first.
SMS Input	Receive SMS message. This feature is only available for -L08GL model and ensure the cellular connection is active.
SMS Output	Send SMS messages. This feature is only available for -L08GL model and ensure the cellular connection is active.

To update this custom library, here are the steps:

1. Receive the custom node library package from Milesight.
2. Click **Import** to select the library package from local path, then click **Upgrade**.



Docker

The gateway has built-in the docker. This chapter introduces the docker feature in this gateway.

Prerequisites

- It is recommended to ensure that the available RAM be at least 1 GB and the available flash memory be at least 6 GB.
- SSH or TELNET access service is enabled in General settings.
- Any SSH/TELNET tool: Putty, etc.

Basic Steps

1. Open an SSH/TELNET tool, and enter the gateway's IP address to access the CLI.
2. Log in to the CLI using the username **admin**, and the same password as the web GUI.

3. Enter the commands to check docker info and operate as required. For more details, please refer to docker docs.

```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
> docker -v
Docker version 20.10.17, build 100c701
> docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
>
```

Chapter 10. Services

Milesight provides customers with timely and comprehensive technical support services. End-users can contact their local dealer to obtain technical support. Distributors and resellers can contact Milesight directly for technical support.

Technical Support Mailbox: iot.support@milesight.com

Online Support Portal: https://support.milesight-iot.com

Resource Download Center: https://www.milesight.com/iot/resources/download-center/

MILESIGHT CHINA

TEL: +86-592-5085280

FAX: +86-592-5023065

Add: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China