Product Name	GAOTek Dual Mode Long Range Wireless Getaway
Product SKU	GAOTek-IIT-163
Product URL	https://gaotek.com/product/gaotek-dual-mode-long-range-wireless-gataway/

Contact us: sales@gaotek.com

Contents

GAOTek Dual Mode Long Range Wireless Getaway

1 General Description

1.1 Product Description

The product is based on protocol, which is embedded with SimTech's high performance multi-channel transceiver SX130X/SX125X and MTK platform. It is forindoor use and easy for installation.

includes 2 modes: AP and STA as router, offers 2.4Ghz Wi-Fi and wired Ethernet for connecting internet. The gateway built-in Open WRT operating system, users can flexibly configure network parameters and protocol parameters through the Web management platform. The Gateway can be connected to terminals in various application nodes, collects useful information and sends the data to cloud server. And it supports POE, DC, Micro USBto provide power supply.

1.2 Product Features

- Support SimTech UDP Packet Forward and Basics Station protocols. Can integrate with both private and public (TTN, Senet, LORIOT, AWS, Chirp stack…. etc.) NetworkServers
- AS923-1/2/3/4 Frequency band supported
- Support Wi-Fi 2.4GHz, compatible with WLAN 802.11b/g/n
- 100Mbase-T Ethernet with POE
- AP and STA mode as router
- Configurable via WIFI
- WEB interface for related configuration and status view
- Support one key reset
- Support download log
- Support upgrade firmware by OTA or USB
- 1x Antenna, 1xWIFI Antenna

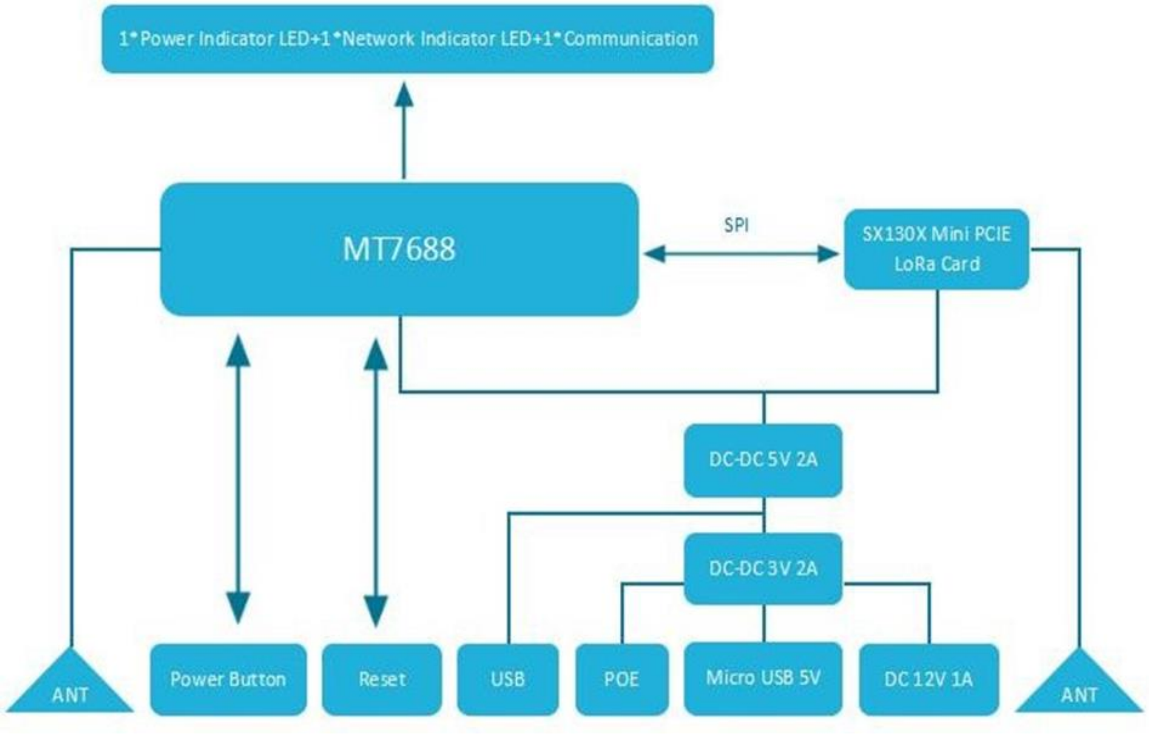
- Indoor operation temperature

1.3 Application

- Smart home, Smart hotel, Smart building and Smart city
- Wireless sensor network
- Wireless remote meter reading
- Indoor smart parking solution
- Environment monitor

2 Specifications

2.1 Block Diagram



2.2 Main Specifications

Category	Feature	Specification
Chipset	LoRa®	SimTech SX130X/125X
	Wi-Fi	128M DDR and 32M flash
Wireless Characteristics	Wi-Fi Frequencies	2.4GHz
	Regions	EU868/US915/AU915/AS923-1/AS923-2/AS923-3/AS923-4/RU864/IN865/KR920
Interfaces	Wired	Ethernet - RJ45 Connector
	Wireless	Wi-Fi 2.4 GHz
Software	Operating System	Embedded Linux, 3.10 Kernel version
		SimTech UDP Packet forwarder/ SimTech Basics Station
	Configuration	Web-based interface via Wi-Fi
Wireless coverage	WIFI	130M (Open Space)
		Up to 4 km (in urban open space)

Power Supply	DC Jack	DC 12V-1A
	POE	POE (IEEE 802.3af), 42~57VDC
	Micro USB	5V/2A
Electrical Specification	Stand By Power Consumption	Stand By Average Current ≤ 200mA@12V
	CommunicationPower Consumption	Communication Transmitting current≤220mA@12V Receiving current≤250mA@12V
	2.4G WIFI TransmissionPower	Max 20dBm
	2.4G WIFI Sensitivity	270Mbps: -61dBm@10%PER 135Mbps: -65dBm@10%PER 108Mbps: -68dBm@8%PER 54Mbps: -68dBm@10%PER 11Mbps: -85dBm@8%PER 6Mbps: -88dBm@10%PER 1Mbps: -90dBm@8%PER
	Output Power	Max 23dBm
	Sensitivity	-141dBm@SF12, BW=125kHz
LED	Power LED	1.System operating normally: Solid green 2. System operating abnormally: Solid red 3. System upgrade: Blink blue
	Network LED	1.No network: Solid yellow 2.ETH connection: Solid blue 3. WIFI connection: Solid green

	Communication LED	1.LoRa COMM √, Server COMM ×: Solid blue 2.LoRa COMM x, Server COMM √: Solid yellow3. LoRa COMM √, Server COMM √: Solid green COMM x, Server COMM x: Solid red
Antenna	WIFI antenna	1.1dBi External antenna
	antenna	1.6dBi External antenna
Environmental	Operating Temp.	(-20 to 55℃) 32 F to 131 F
	Storage Temp.	(-40 to +85℃) 104 F to 185 F
Regulatory	Approvals	FCC/CE Under Approval
Dimensions Installation	Dimensions	(166 mm x 05 mm x 28.4 mm) 6.5 in x 0.19 in x 1.11 in
	Weight	(0.15 kg) 0.33 lb.
	Installation	On the desktop or Fixed on the wall
Enclosure	Standard	Molded plastic housing
Warranty	1-Year warranty	

2.3 Electrical Specifications

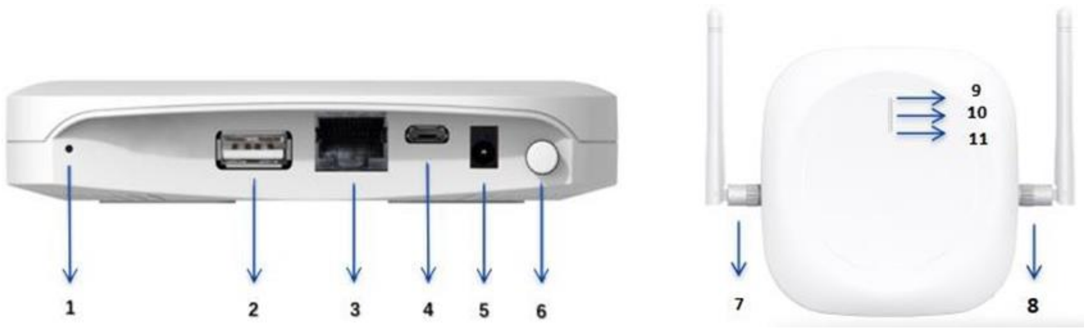
2.4 Power Supply

Item	**Description**
DC Jack	DC 12V-1A
POE	POE (IEEE 802.3af)
Micro USB	5V/2A

2.5 Consumption

Item	Description
Stand by Power Consumption	Average Current ≤200mA@12V
Communication Power Consumption	Communication Transmitting current ≤220mA@12V Receiving current ≤250mA@12V

2.6 Hardware Interfaces

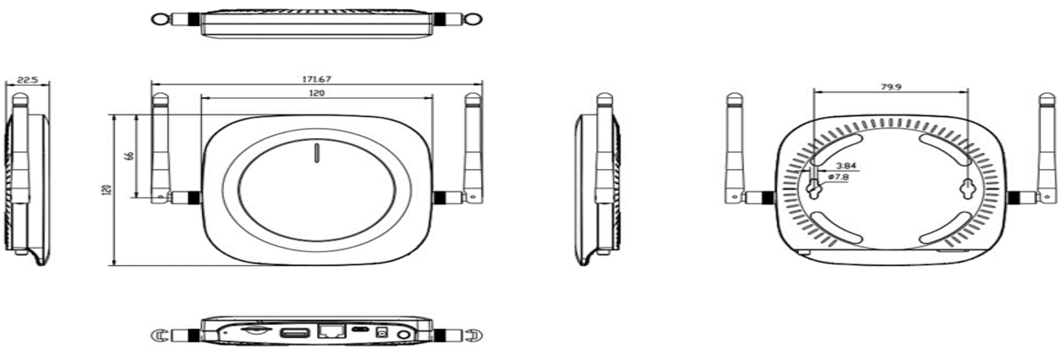


No.	Type	Function	Remark
1	Reset button	1.Reset to factory setting 2.Firmware upgrade	1.Reset: Insert and press the button then keep5s 2.Update: Before firmware upgrade, insert USB Flash Drive and short press the button
2	USB Port	Plug a USB flash drive with upgrade file for	The name of upgrade file is required to be: P grade. bin
		firmware upgrade	
3	POE Port	1.POE power supply 2.Ethernet Access	POE (IEEE 802.3af), 42 to 57VDC

4	Micro USB	USB power supply	5V/2A
5	DC Power Port	DC power supply	12V/1A
6	Power Button	ON/OFF	
7	Wi-Fi Antenna	Wi-Fi Antenna	1.1dBi External antenna
8	Antenna	Antenna	1.6dBi External antenna
9	Power LED	Indicate device operating status	1.System operating normally: Solid green 2. System operating abnormally: Solid red 3. System upgrade: Blink green
10	Network LED	Indicate network status	1.No network: Solid yellow 2.ETH connection: Solid blue 3. WIFI connection: Solid green
11	Communication LED	Indicate and server communicate status	1. COMM √, Server COMM ×: Solid blue COMM x, Server COMM √: Solid yellow 3.COMM √, Server COMM √: Solid green 4.COMM x, Server COMM x: Solid red

3 Mechanical Size and Package Information

3.1 Mechanical Size

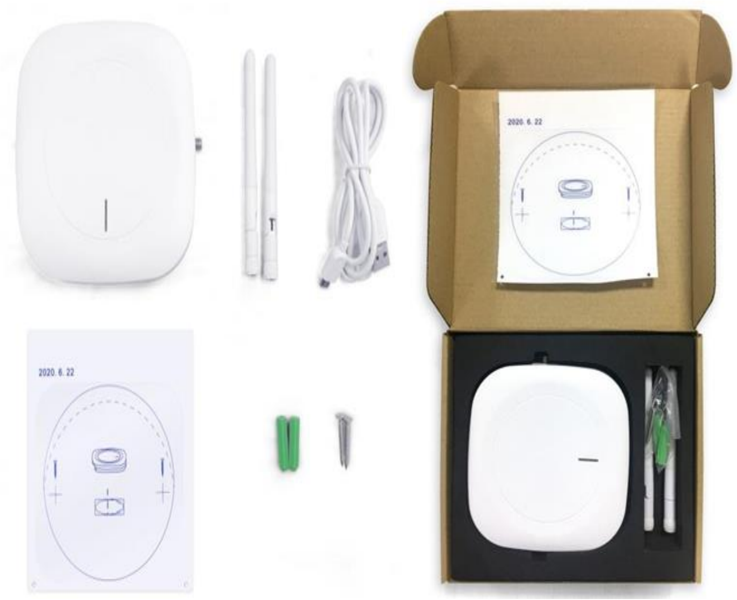


3.2 Package Information

3.2.1Package List

Item	Qty	Remark
	1	Gateway
Wi-Fi Antenna	1	
Antenna	1	
Micro USB cable	1	
Positioning screws	2	Used for fixing on the wall
Expansion rubber plug	2	Used for fixing on the wall
PET localizer	1	

3.2.2 Package Information



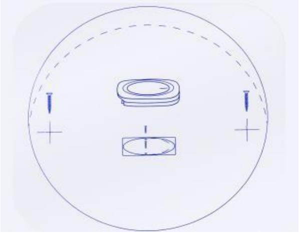
4 User Instruction

You can login to the WEB Management page to overview the status of your gatewayand configure your gateway.

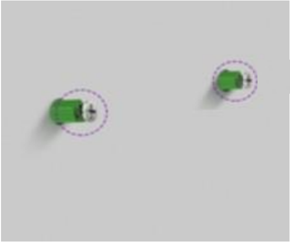
For more information about the WEB Management platform and the configuration guideof the gateway, please refer to this document:

5 Installation

Step 1: Use 5mm drill head, drill 2 holes on the wall according to the PET localizerfollowing picture and then plug the screw anchors in the wall.



Step 2: Install the screw into the wall and keep about 3 mm of clearance.

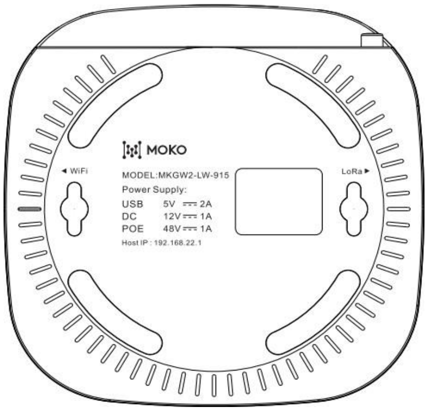


Step 3: Insert the screw head into the hanging hole behind the equipment, then gently pull down to complete the installation.

6 Connecting the Hardware

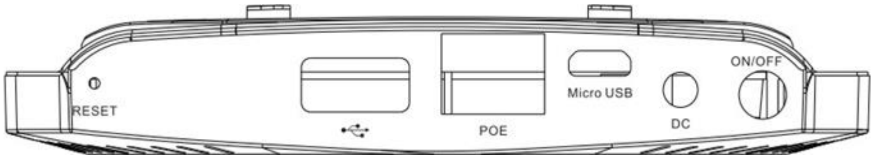
6.1 Connect the Gateway

1. Follow the silk screen on the enclosure and connect Wi-Fif and antennas. Refer to Antenna Configuration for additional information.



2. Connect the power supply (Refer to Chapter 4.2 Power up and Turn ON/OFF for additionalinformation.).

6.2 Power Up and Turn ON/OFF



- Power Up: follow the silk on the enclosure you can select different power solution.
  1. Micro USB:5V/2A
  2. DC Power Port:12V/1A
  3. POE Port: POE (IEEE 802.3af)
- Turn ON/OFF: After power up the gateway, it needs to push-down the power ON/OFF button tostart the gateway system.

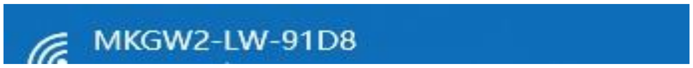
7 Access to Gateway Web GUI

7.1 Access to Web GUI via Wi-Fi

You need to prepare a computer or smartphone which has the IEEE 802.11b/g/n wireless capabilityand is configured to obtain an IP address automatically. Follow the steps below to connect to the gateway and access the Web GUI.

Step 1: Turn on the gateway and waiting for about 60s.

Step 2: Using your PC or phone connect the SSID of the gateway. The default SSID format is such as "91D8" is the last two bytes of the gateway MACaddress. verify and connect to the gateway.



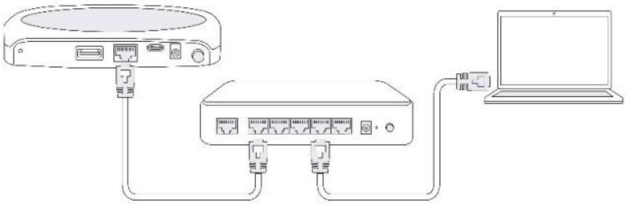
MKGW2-LW-91D8

Step 3: The default password. For security reasons, it is recommended to modify theWi-Fi password or turn off the AP function of the gateway after your configurations.

Step 4: Open the Web browser (we suggest the Web browser such as Microsoft Edge, Firefox, Safarior Google Chrome) and type the gateway's address 192.168.22.1 (by default). Then the Web GUI will be loaded.

7.2 Access to Web GUI via Ethernet Cable

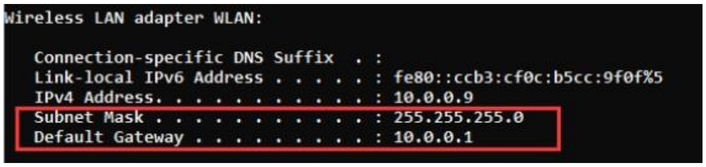
Use an Ethernet cable to connect the PoE port of the gateway with a router or switch and then makeyour computer in the same Local Area Network (LAN) with the gateway as the following picture. Andthen you can access the Web GUI by using the computer to visit the WAN IP of the gateway.



Follow the steps bellow to find the IP address of the gateway (the following steps are operated onWindows OS):

Step 1: Open the CMD window in the path where the “ARP-SCAN.exe” file is stored.

Step 2: Type “ipconfig” and press the Enter key to obtain the upstream network device’s parameters. Note down the Subnet Mask and the Default Gateway IP address. In the example figure below,the Subnet Mask is 255.255.255.0 and the Default Gateway IP address is 10.0.0.1.

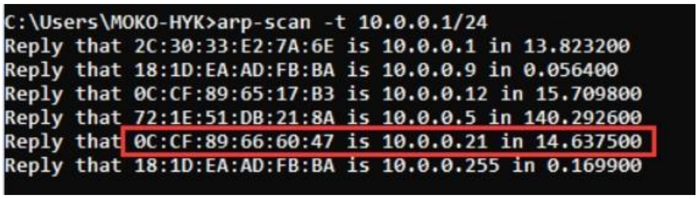


```
Wireless LAN adapter WLAN:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ccb3:cf0c:b5cc:9f0f%5
   IPv4 Address. . . . . . . . . . . : 10.0.0.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

Step 3: Type the command “Arp-scan -t -10.0.0.1/24” and note down the IP address which is corresponding to the gateway’s MAC address (Plus 1 on original MAC Address) on the IP address lists. In the figure below, the MAC address is 0C:CF:89:66:60:47 and the IP addressis 10.0.0.21.

The command “Arp-scan -t -10.0.0.1/24” - “10.0.0.1” refers to the default gateway IP address andthe “24” refers to the CIDR (Classless Inter-Domain Routing) number of the subnet mask.



```
C:\Users\MOKO-HYK>arp-scan -t 10.0.0.1/24
Reply that 2C:30:33:E2:7A:6E is 10.0.0.1 in 13.823200
Reply that 18:1D:EA:AD:FB:BA is 10.0.0.9 in 0.056400
Reply that 0C:CF:89:65:17:B3 is 10.0.0.12 in 15.709800
Reply that 72:1E:51:DB:21:8A is 10.0.0.5 in 140.292600
Reply that 0C:CF:89:66:60:47 is 10.0.0.21 in 14.637500
Reply that 18:1D:EA:AD:FB:BA is 10.0.0.255 in 0.169900
```

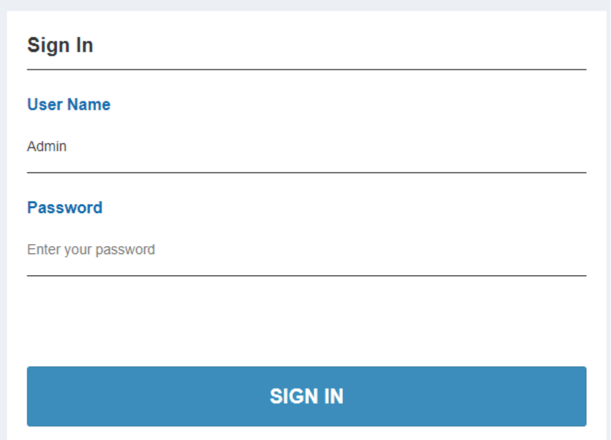
The CIDR number comes from the number of ones in the subnet mask when converted to binary.

The common subnet mask 255.255.255.0 is 11111111.11111111.11111111.00000000 in binary. This adds up to 24 ones, hence /24. A subnet mask of 255.255.255.192 is 11111111.11111111. 11111111.11000000 in binary, adds to 26 ones, hence /26.

Step 4: Open the Web browser and type the gateway's IP address 10.0.0.21 (the example above), and then the Web GUI will be loaded.

7.3 Login the Web GUI

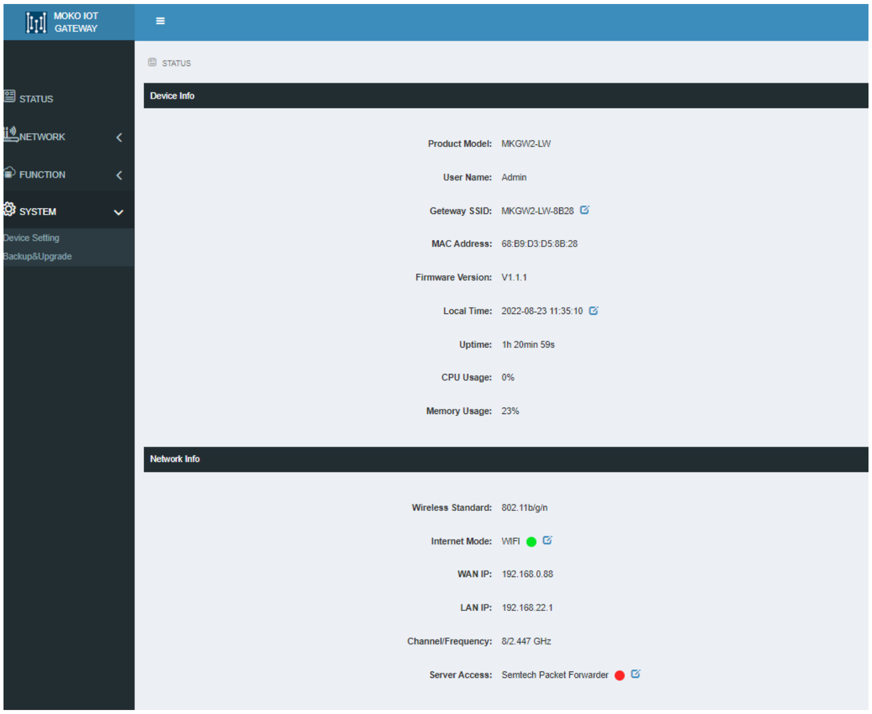
You can log in to the Web GUI by using the default user name: Admin and password: admin. For security reasons, it is recommended to modify the password after your configurations. If there is noany operation within 1 hour, the gateway will automatically sign out of the Web GUI.



User Name: Admin

7.4 Home Page of the Web GUI

After login, the gateway comes with an intuitive Web GUI that allows you to easily setup and checkall parameters. The home page of the Web GUI displays the information of the gateway. The following figure shows the home page, which contains two sections: Device Info and Network Info. Contents on this pagewill be refreshed when some of your configurations take effect.



Device Info

Product Model: MKGW2-LW

User Name: Admin

Geteway SSID: MKGW2-LW-8B28

MAC Address: 68:B9:D3:D5:8B:28

Firmware Version: V1.1.1

Local Time: 2022-08-23 11:35:10

Uptime: 1h 20min 59s

CPU Usage: 0%

Memory Usage: 23%

Network Info

Wireless Standard: 802.11b/g/n

Internet Mode: WIFI ●

WAN IP: 192.168.0.88

LAN IP: 192.168.22.1

Channel/Frequency: 8/2.447 GHz

Server Access: Semtech Packet Forwarder ●

8 Network Connection Setting

It is able to configure the network connection function on the *Network* page of the Web GUI.

8.1 Internet Setting

The gateway can access the Internet through Ethernet (ETH) or Wi-Fi, and can access the networkby Automatic IP or Static IP. Static IP requires, subnet mask, gateway IP, DNS, etc. After the network configuration is completed, wait for the gateway to access the network. You cancheck the network status in gateway STATUS web page and also can check the network LED indicator.

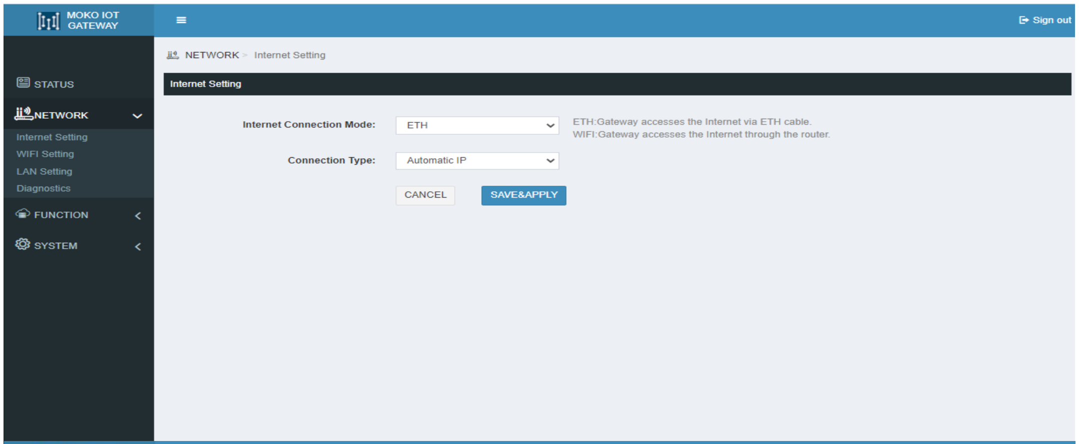
- No network: Solid yellow
- ETH connection: Solid blue

- ➢ WIFI connection: Solid green

It is able to configure the Internet connection function on the *Network – Internet Setting* page ofthe Web GUI.

8.1.1 Ethernet to Internet

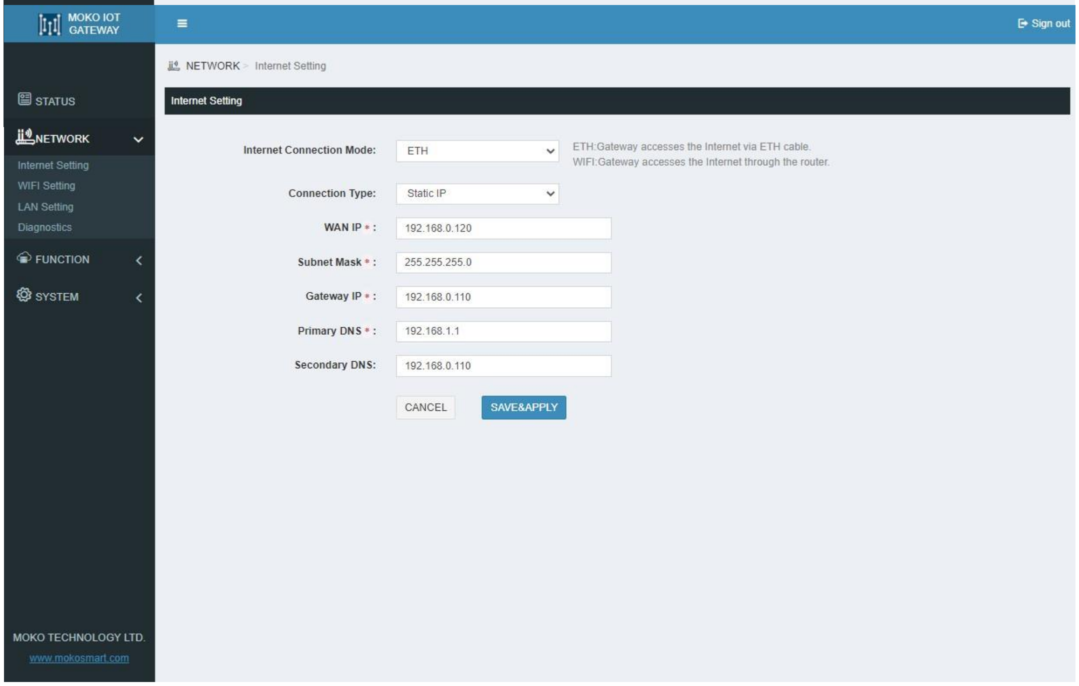
Use a network cable to connect to the PoE port of the gateway and connect the gateway to a Network Switch that is connected to the Internet.



Internet Connection Mode: ETH

ETH:Gateway accesses the Internet via ETH cable.
WIFI:Gateway accesses the Internet through the router.

Connection Type: Automatic IP



Internet Connection Mode: ETH

ETH:Gateway accesses the Internet via ETH cable.
WIFI:Gateway accesses the Internet through the router.

Connection Type: Static IP

WAN IP * : 192.168.0.120

Subnet Mask * : 255.255.255.0

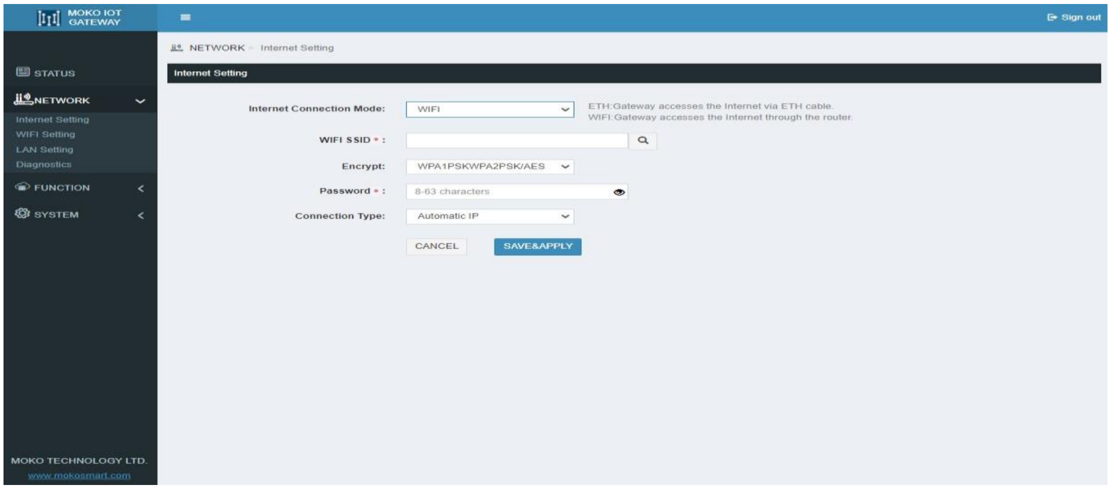
Gateway IP * : 192.168.0.110

Primary DNS * : 192.168.1.1

Secondary DNS: 192.168.0.110

8.1.2 Wi-Fi to Internet

Connect to a Wireless Router via to access the Internet. Select a wireless router and connectto it. After the configuration is complete, the gateway will restart. Then the network status can be check in the STATUS page.



Internet Setting

Internet Connection Mode: WIFI

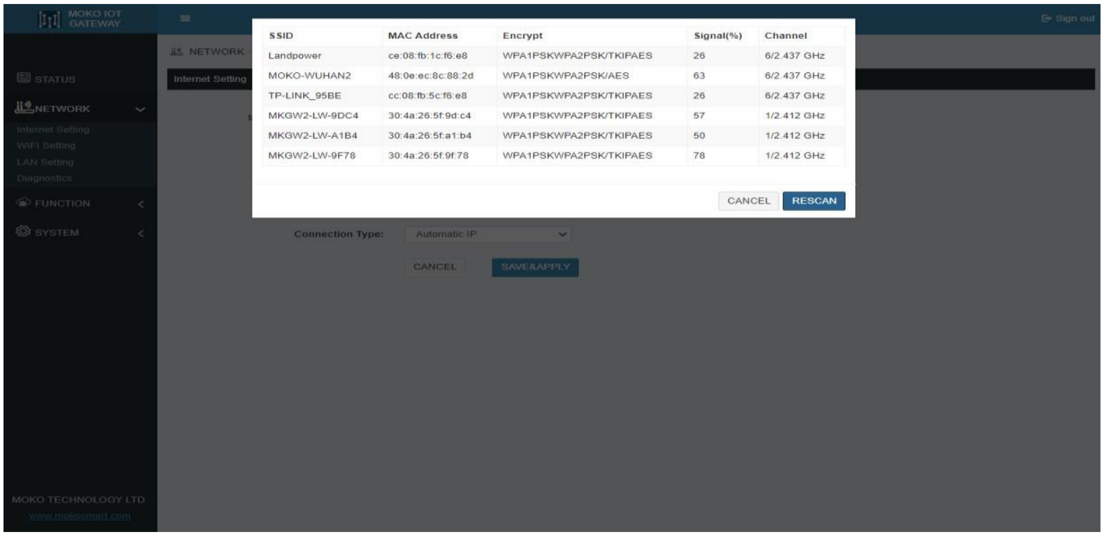
ETH:Gateway accesses the Internet via ETH cable.
WIFI:Gateway accesses the Internet through the router.

WIFI SSID * :

Encrypt: WPA1PSKWPA2PSK/AES

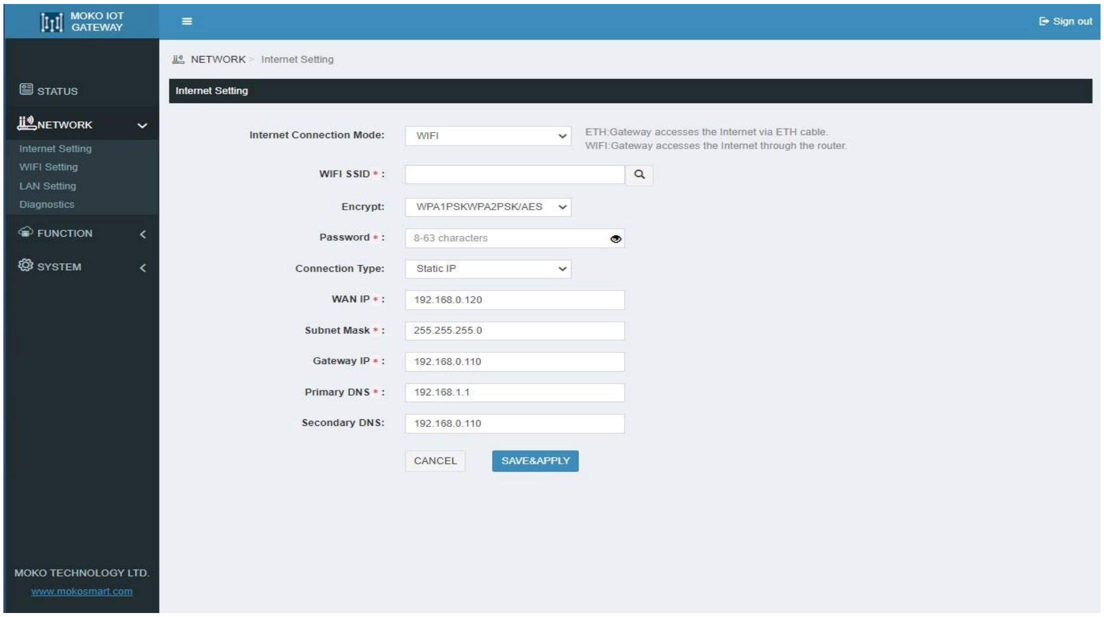
Password * : 8-63 characters

Connection Type: Automatic IP



SSID	MAC Address	Encrypt	Signal(%)	Channel
Landpower	ce:08:fb:1c:f6:e8	WPA1PSKWPA2PSK/TKIPAES	26	6/2.437 GHz
MOKO-WUHAN2	48:0e:ec:8c:88:2d	WPA1PSKWPA2PSK/AES	63	6/2.437 GHz
TP-LINK_95BE	cc:08:fb:5c:f6:e8	WPA1PSKWPA2PSK/TKIPAES	26	6/2.437 GHz
MKGW2-LW-9DC4	30:4a:26:5f:9d:c4	WPA1PSKWPA2PSK/TKIPAES	57	1/2.412 GHz
MKGW2-LW-A1B4	30:4a:26:5f:a1:b4	WPA1PSKWPA2PSK/TKIPAES	50	1/2.412 GHz
MKGW2-LW-9F78	30:4a:26:5f:9f:78	WPA1PSKWPA2PSK/TKIPAES	78	1/2.412 GHz

Connection Type: Automatic IP



Internet Setting

Internet Connection Mode: WIFI

ETH:Gateway accesses the Internet via ETH cable.
WIFI:Gateway accesses the Internet through the router.

WIFI SSID * :

Encrypt: WPA1PSKWPA2PSK/AES

Password * : 8-63 characters

Connection Type: Static IP

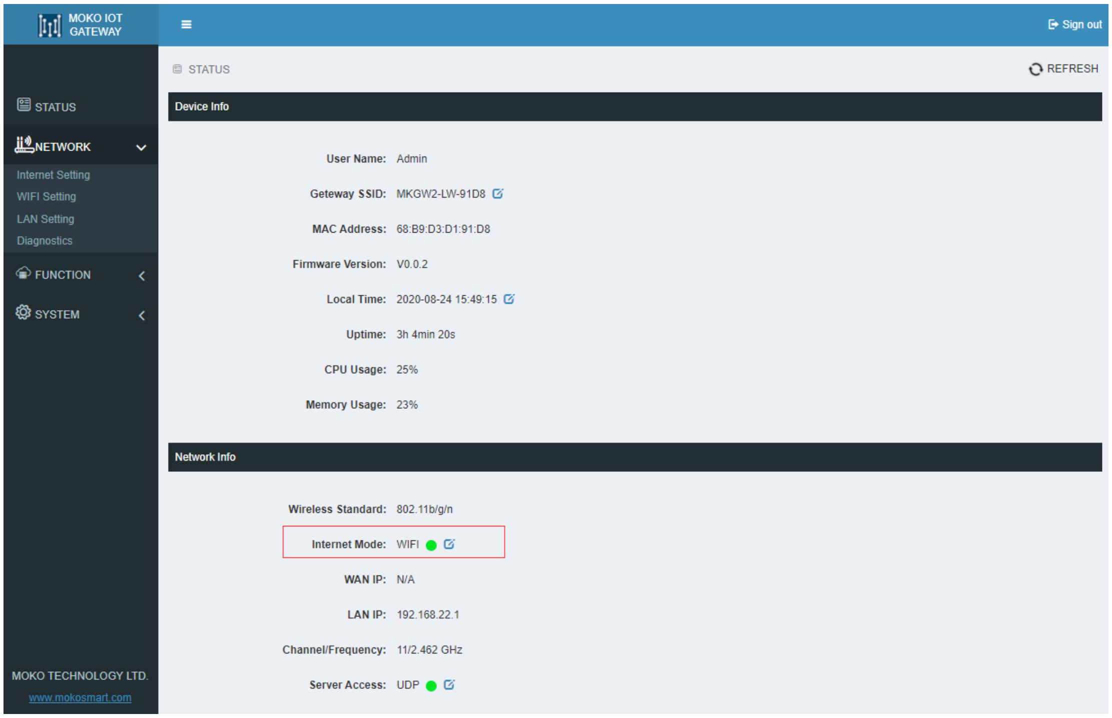
WAN IP * : 192.168.0.120

Subnet Mask * : 255.255.255.0

Gateway IP * : 192.168.0.110

Primary DNS * : 192.168.1.1

Secondary DNS: 192.168.0.110



Device Info

User Name: Admin

Geteway SSID: MKGW2-LW-91D8

MAC Address: 68:B9:D3:D1:91:D8

Firmware Version: V0.0.2

Local Time: 2020-08-24 15:49:15

Uptime: 3h 4min 20s

CPU Usage: 25%

Memory Usage: 23%

Network Info

Wireless Standard: 802.11b/g/n

Internet Mode: WIFI ●

WAN IP: N/A

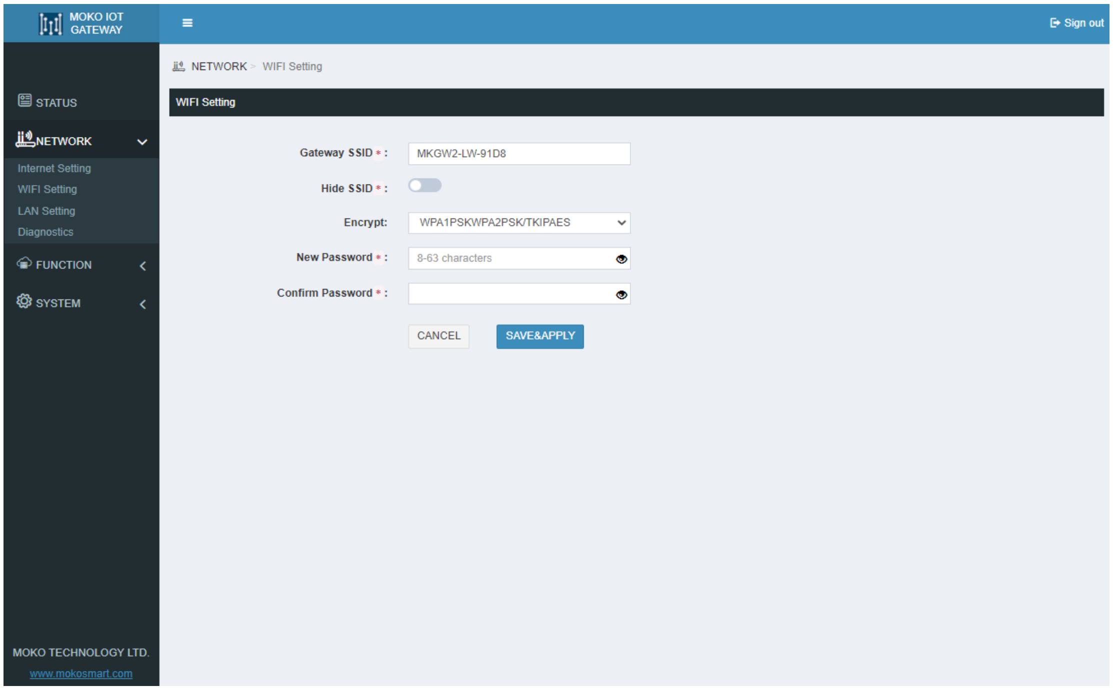
LAN IP: 192.168.22.1

Channel/Frequency: 11/2.462 GHz

Server Access: UDP ●

8.2 Wi-Fi Setting

You can modify the SSID of the gateway, whether to hide the SSID, encryption mode, and password. After the configuration is complete, the gateway will be restarted for the configurationto take effect.



WIFI Setting

Gateway SSID * : MKGW2-LW-91D8

Hide SSID * :

Encrypt: WPA1PSKWPA2PSK/TKIPAES

New Password * : 8-63 characters

Confirm Password * :

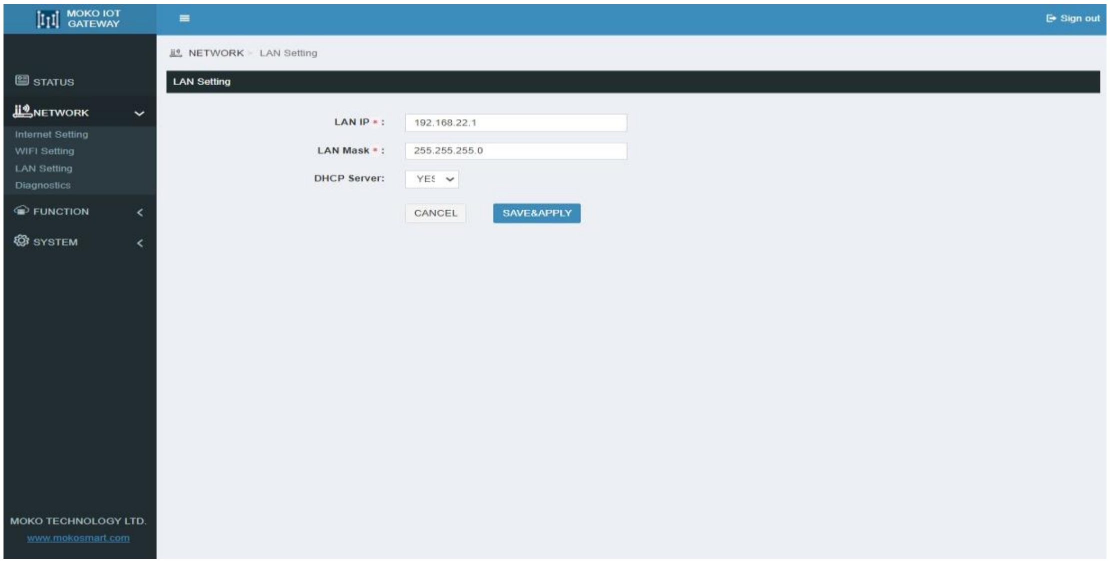
Supported encryption methods:

- WPA1PSKWPA2PSK/TKIPAES（Default）
- WPA1PSKWPA2PSK/AES
- WPA2PSK/TKIPAES
- WPA2PSK/AES
- WPA2PSK/TKIP
- WPAPSK/TKIPAES
- WPAPSK/AES
- WPAPSK/TKIP
- WEP

- None (No encryption)

8.3 LAN Setting

You can modify the gateway and subnet mask. After the configuration is complete, thegateway will be restarted for the configuration to take effect.



LAN Setting

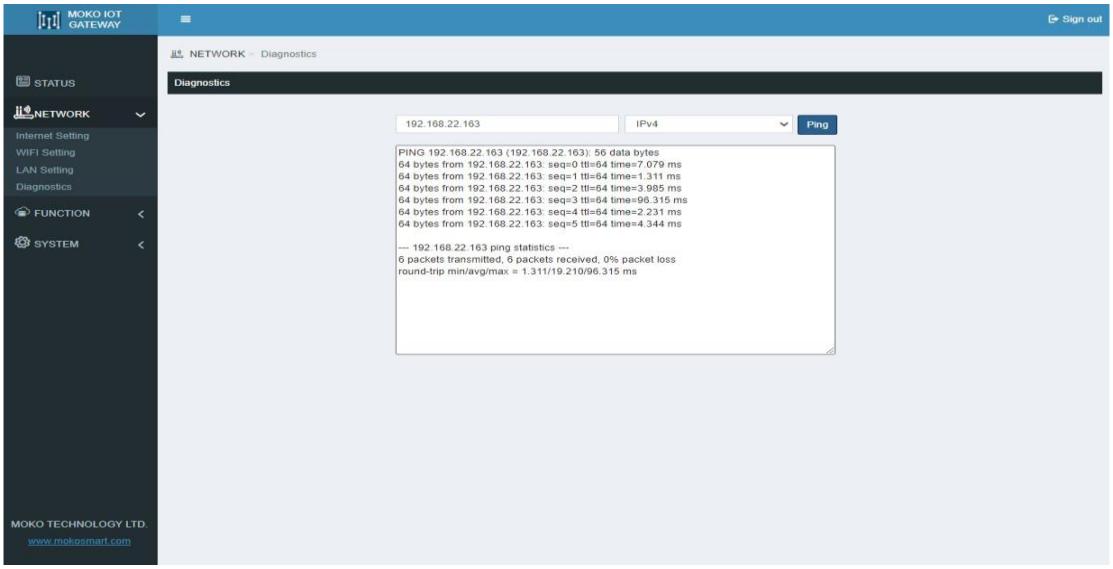
LAN IP * : 192.168.22.1

LAN Mask * : 255.255.255.0

DHCP Server: YES

8.4 Diagnostics

You can check the current network connection through the Diagnostics. Fill in the IP address andselect the network type, and use ping to check the network, it will display ping result.



192.168.22.163 | IPv4

```
PING 192.168.22.163 (192.168.22.163): 56 data bytes
64 bytes from 192.168.22.163: seq=0 ttl=64 time=7.079 ms
64 bytes from 192.168.22.163: seq=1 ttl=64 time=1.311 ms
64 bytes from 192.168.22.163: seq=2 ttl=64 time=3.985 ms
64 bytes from 192.168.22.163: seq=3 ttl=64 time=96.315 ms
64 bytes from 192.168.22.163: seq=4 ttl=64 time=2.231 ms
64 bytes from 192.168.22.163: seq=5 ttl=64 time=4.344 ms

--- 192.168.22.163 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 1.311/19.210/96.315 ms
```

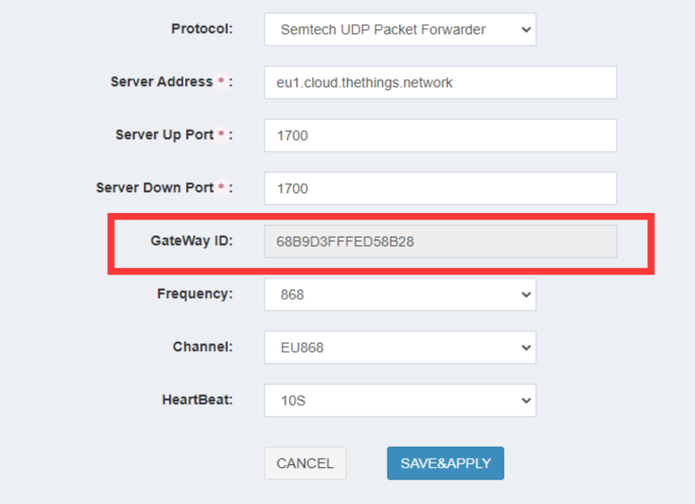
8.5 UDP Packet Forwarder

The gateway’s server access protocol is UDP Packet Forwarder in default.

Step 1: Fill in the correct Server address, it can be found on network server interface.

Step 2: Fill in the correct Sever Up Port and Server Down Port, it can be found on network server interface.

Step 3: Fill in the Gateway ID on network server and register the gateway on network server.



Protocol: Semtech UDP Packet Forwarder

Server Address * : eu1.cloud.thethings.network

Server Up Port * : 1700

Server Down Port * : 1700

GateWay ID: 68B9D3FFFED58B28

Frequency: 868

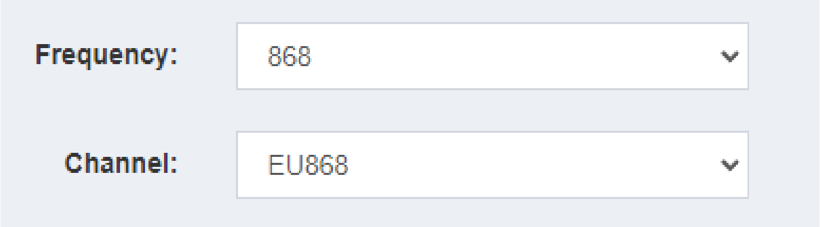
Channel: EU868

HeartBeat: 10S

Step 4: Select the Frequency and Channel, should be same to the register information on network server.

If the current used frequency band is US915/AU915/AS923/AS923-1/AS923-2/AS923-3/AS923-4/KR920, pls select 915 in Frequency.

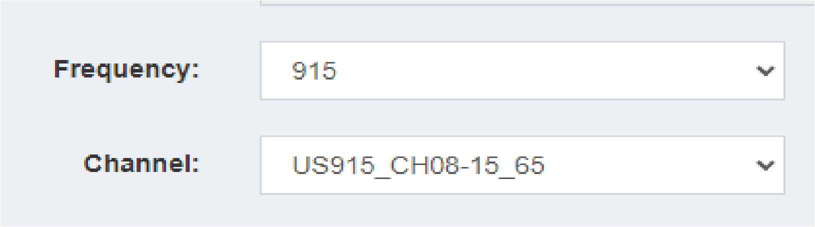
If the current used frequency band is EU868/IN865/RU864, pls select 868 in Frequency.
Example 1: If you use EU868, pls select 868 in Frequency, then select EU868 in Channel.



Frequency: 868

Channel: EU868

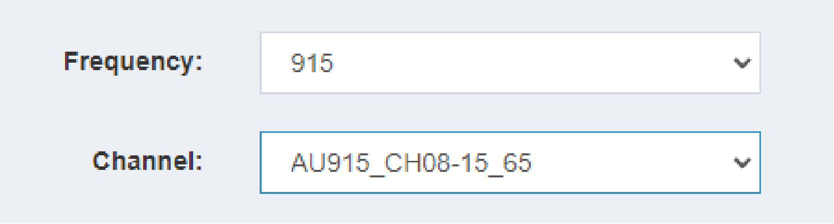
Example 2: If you use US915, pls select 915 in Frequency, then select US915_CH08-15_65 (CH08_15 means FSB2, if you use other FSB, pls select the corresponding channel).



Frequency: 915

Channel: US915_CH08-15_65

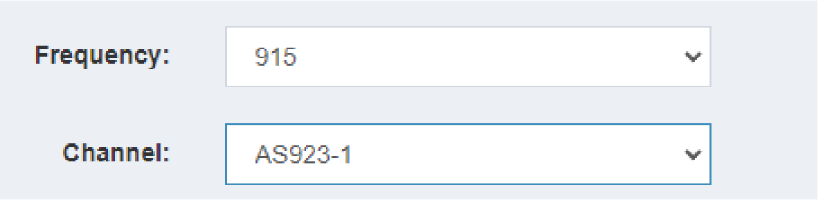
Example 3: If you use AU915, pls select 915 in Frequency, then select AU915_CH08-15_65 (CH08_15 means FSB2, if you use other FSB, pls select the corresponding channel).



Frequency: 915

Channel: AU915_CH08-15_65

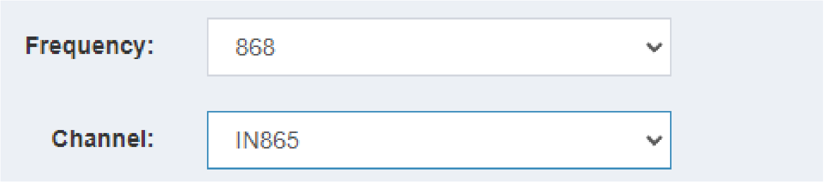
Example 4: If you use AS923-1, pls select 915 in Frequency, then select AS923-1.



Frequency: 915

Channel: AS923-1

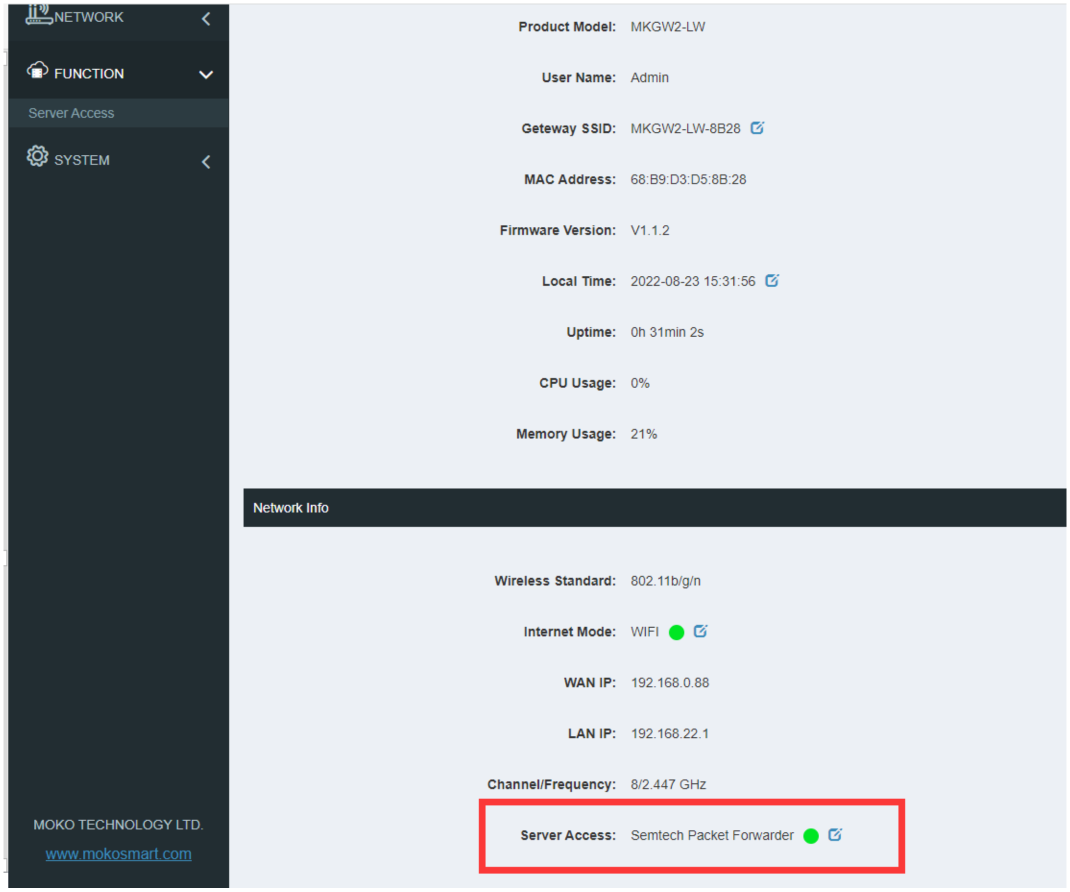
Example 5: If you use IN865, pls select 868 in Frequency, then select IN865



Frequency: 868

Channel: IN865

Step 5: Click “Save & Apply”, you can check the server access status in gateway STATUS web pageand also can check the LoRa server communication LED indicator that should be solid green.



Product Model: MKGW2-LW

User Name: Admin

Geteway SSID: MKGW2-LW-8B28

MAC Address: 68:B9:D3:D5:8B:28

Firmware Version: V1.1.2

Local Time: 2022-08-23 15:31:56

Uptime: 0h 31min 2s

CPU Usage: 0%

Memory Usage: 21%

Network Info

Wireless Standard: 802.11b/g/n

Internet Mode: WIFI ●

WAN IP: 192.168.0.88

LAN IP: 192.168.22.1

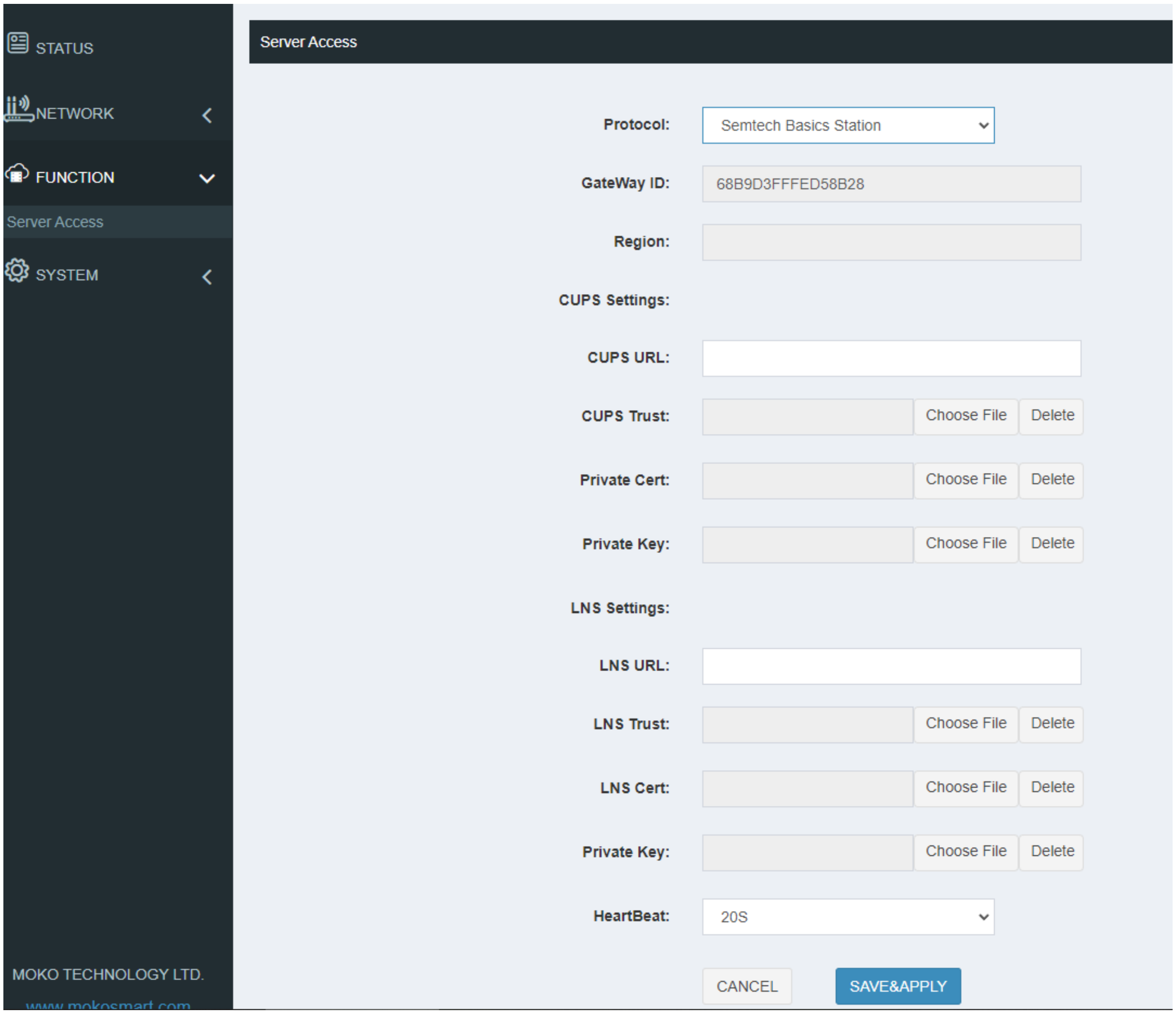
Channel/Frequency: 8/2.447 GHz

Server Access: Semtech Packet Forwarder ●

8.6 Basics Station

Select SimTech Basics Station protocol at firstly.

GAOTEK-IIT-163 supports both of CUPS and LNS of Basics Station protocol, and can be integrated withboth private and public (TTN, Senet, LORIOT, AWS, Chirp stack…. etc.) Network Servers.



Server Access

Protocol: Semtech Basics Station

GateWay ID: 68B9D3FFFED58B28

Region:

CUPS Settings:

CUPS URL:

CUPS Trust:

Private Cert:

Private Key:

LNS Settings:

LNS URL:

LNS Trust:

LNS Cert:

Private Key:

HeartBeat: 20S

Different servers have different settings for basics station, the required files (CUPS Trust, Private Cert, Private Key, LNS Trust, LNS Cert) and URL of this interface should be obtained from the server.

In general, the supports Basics Station protocol will provide an LNS URL at least, such asTTN platform.

For instructions on setting up the Basics Station, you can refer to the NetworkServer vendor's documentation.

9 System setting

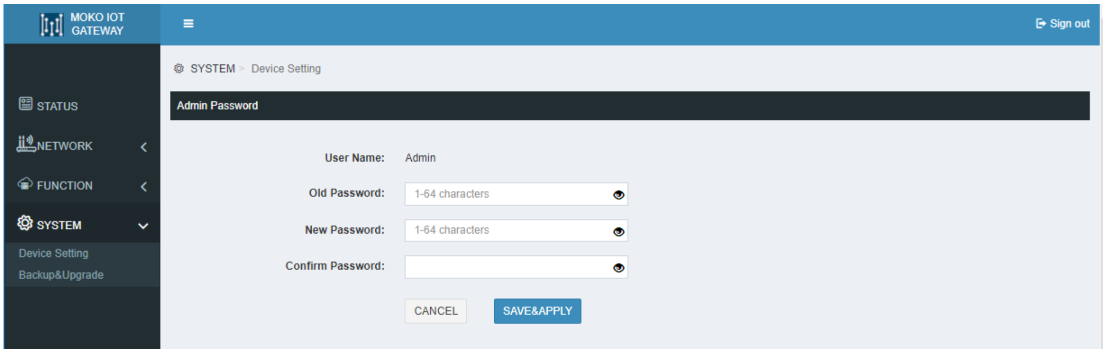
It is able to configure the system parameters on the *System* page of the Web GUI.

9.1 Device setting

9.1.1 Modify Login Password

User can modify the password for logging in configuration web GUI.The login user name is "Admin" in default (unmodifiable).

The length of password is 1-64 characters and needs to be verified with the old password.



Admin Password

User Name: Admin

Old Password: 1-64 characters

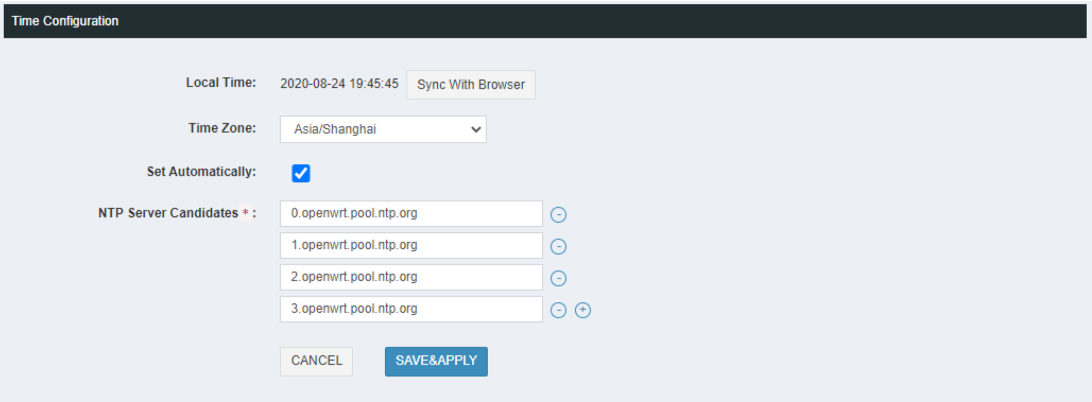
New Password: 1-64 characters

Confirm Password:

9.1.2 Time Configuration

User selects the time zone, and then checks "Set Automatically".

The NTP server follows the default settings and automatically updates to the current time in the time zone. If the user needs to set the time to match the local browser time, please uncheck "Set Automatically" and click "Sync with Browser" to update to the current browser time.



Time Configuration

Local Time: 2020-08-24 19:45:45 Sync With Browser

Time Zone: Asia/Shanghai

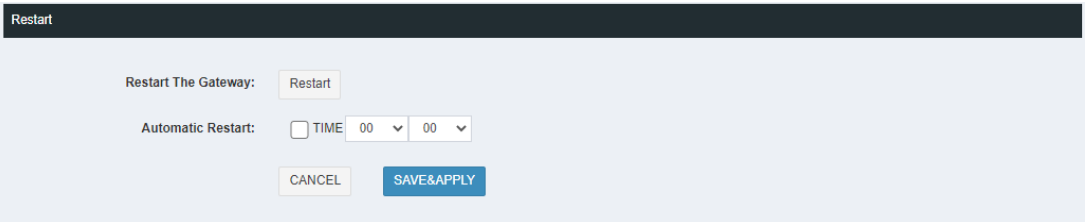
Set Automatically: ☑

NTP Server Candidates * :
- 0.openwrt.pool.ntp.org
- 1.openwrt.pool.ntp.org
- 2.openwrt.pool.ntp.org
- 3.openwrt.pool.ntp.org

9.1.3 Restart

Click “Restart” and the gateway will restart immediately.

The user can turn on the “Automatic Restart” function (Disable by default) and set the time for thegateway to automatically restart each day. This operation can free up system RAM and ensures that the system runs smoothly and steadily.



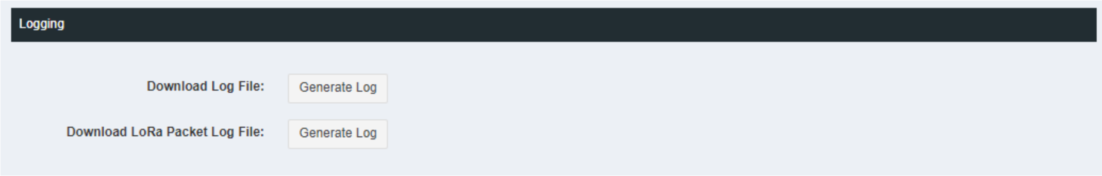
Restart

Restart The Gateway: Restart

Automatic Restart: □ TIME 00 00

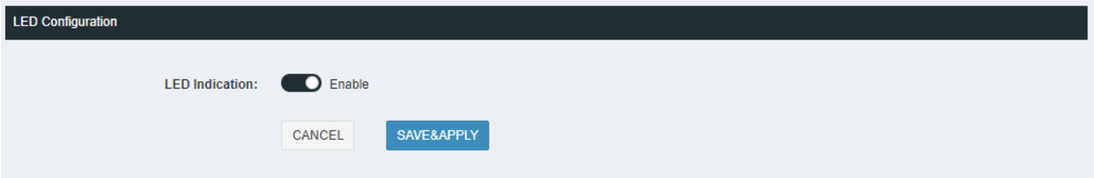
9.1.4 Log

Once the user finds the device abnormal during use, the system Log File and LoRa Packet Log file can be downloaded to the local. Please send the log file to check the system error



9.1.5 LED Configuration

User can turn off the device LED. After saving, the operation takes effect immediately. In the state of turning off the LED, if the system is abnormal or the system is upgraded, the LED will still be enabled.

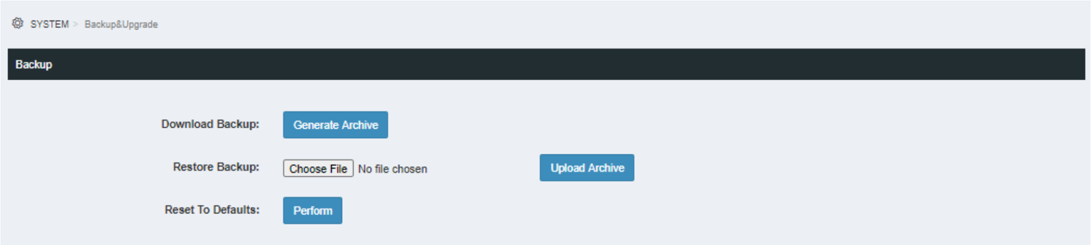


LED Indication: Enable

9.2 Backup & Upgrade

9.2.1 Backup

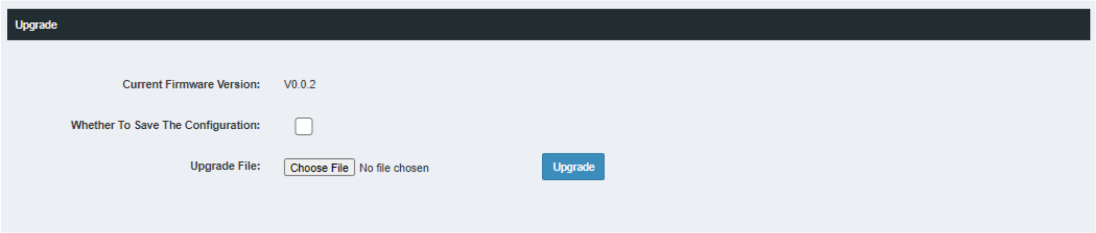
User can download the configured parameter file of the gateway to the local.
User can directly import the configured file into the current system. After the device is restarted, the configuration will take effect.



Restore Backup: No file chosen

9.2.2 Upgrade

User can upgrade the system by uploading Upgrade File in WEB. You can check “Whether to save the configuration” to ensure that the upgraded system parameters are consistent with the currentsystem configuration parameters.



Upgrade

Current Firmware Version: V0.0.2

Whether To Save The Configuration: □

Upgrade File: Choose File No file chosen

USB upgrade method：

Step 1: Copy the upgrade file named to the USB flash drive.

Step 2: Insert the USB flash drive into the gateway USB Port, short press the RESET button, and power LED will blink green that indicate the device upgrading now. With USB upgrade, the gatewaywill automatically save the current system configuration parameters.

10 Restore Factory Settings

Press the reset button and hold on 5 seconds, then release, you can see the gateway restart again and all LED turn to yellow.

Then, the gateway will restore factory setting and all gateway information need to be configured again.

11 Maintenance Instruction

- Do not use or store the device in dusty or dirty areas.
- Do not use or store the device in extremely hot temperatures. High temperatures may damagethe device.
- Do not use or store the device in extremely cold temperature. When the device warms to itsnormal temperature, moisture can form inside the device and damage the device.
- Do not drop, knock, or shake the device. Rough handing would break it.
- Do not use strong chemicals or washing to clean the device.
- Do not paint the device, paint would cause improper operation

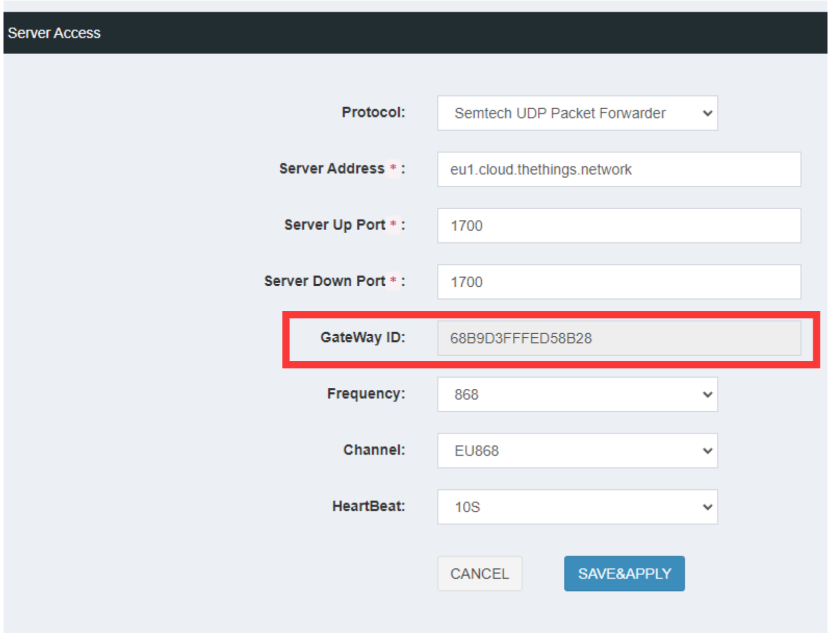
- Do not disassemble the device casually or use the tools for maintenance without permission
- Handle your device, and accessories with care. The suggestions above help you keepyour device operational.

12 Revision

Version	Description	Editor	Date
1.0	Initial Version	Iris	**2020/8/26**
1.1	1. Update document format; 2. Add TTN server address link; 3. Add gateway default frequency	Iris	**2020/12/10**
2.1	1. **Add support "Access to web GUI viaethernet cable".** 2. **Add support AS923-1/AS923-2/AS923-3/AS923-4 frequency band.** 3. **Add support "SimTech Basics Stationprotocol".** 4. **Other description modification** 5. **Suitable for firmware version V1.1.2**	**Allen**	**2022/8/23**

Appendix 1 UDP Packet Forwarder

Step 1: Power access to Web GUI, get the gateway ID on *FUNCTAION-ServerAccess* page of Web GUI.



Server Access

Protocol: Semtech UDP Packet Forwarder

Server Address * : eu1.cloud.thethings.network

Server Up Port * : 1700

Server Down Port * : 1700

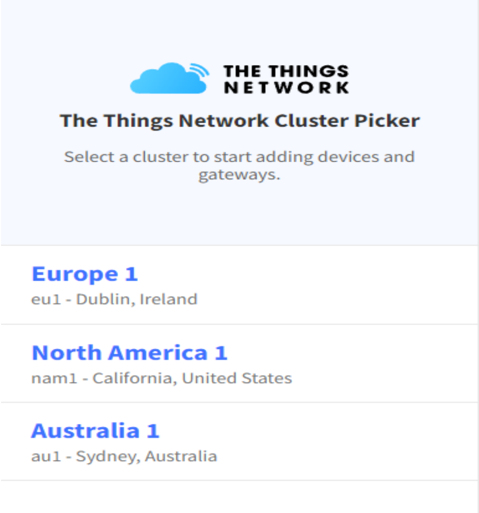
GateWay ID: 68B9D3FFFED58B28

Frequency: 868

Channel: EU868

HeartBeat: 10S

Step 2: Prepare an TTN account, then login in TTN platform and click the corresponding Cluster thatyou want to use. I will use EU868 as example, so Europe 1 cluster will be my choice.



THE THINGS NETWORK

The Things Network Cluster Picker

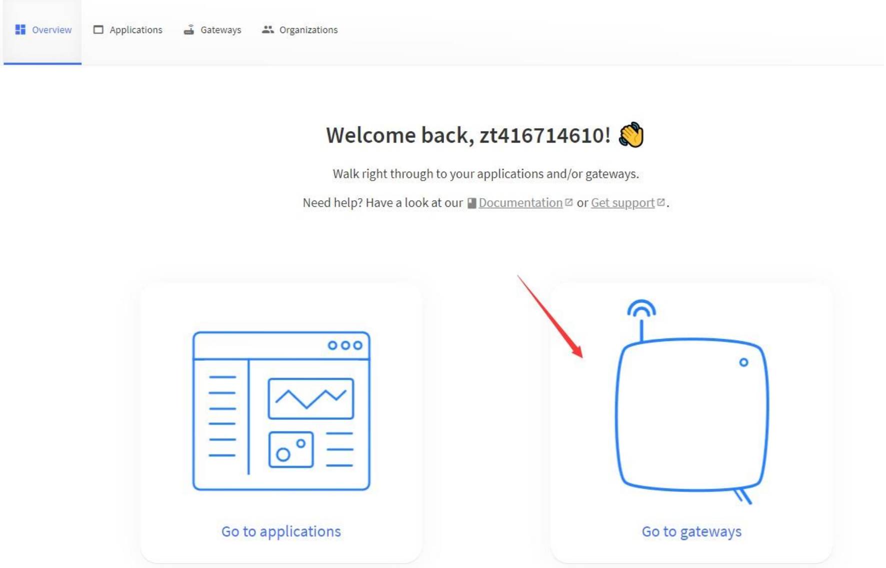
Select a cluster to start adding devices and gateways.

Europe 1
eu1 - Dublin, Ireland

North America 1
nam1 - California, United States

Australia 1
au1 - Sydney, Australia

Step 3: Go to gateway console on home page after you login in successfully.

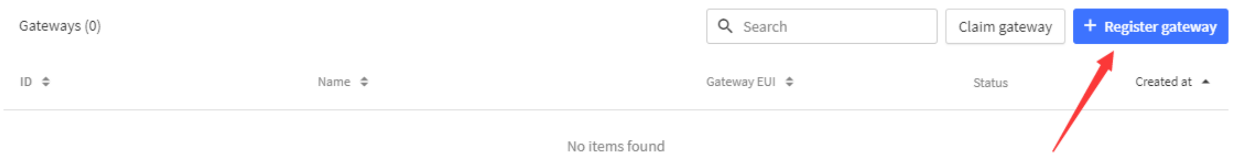


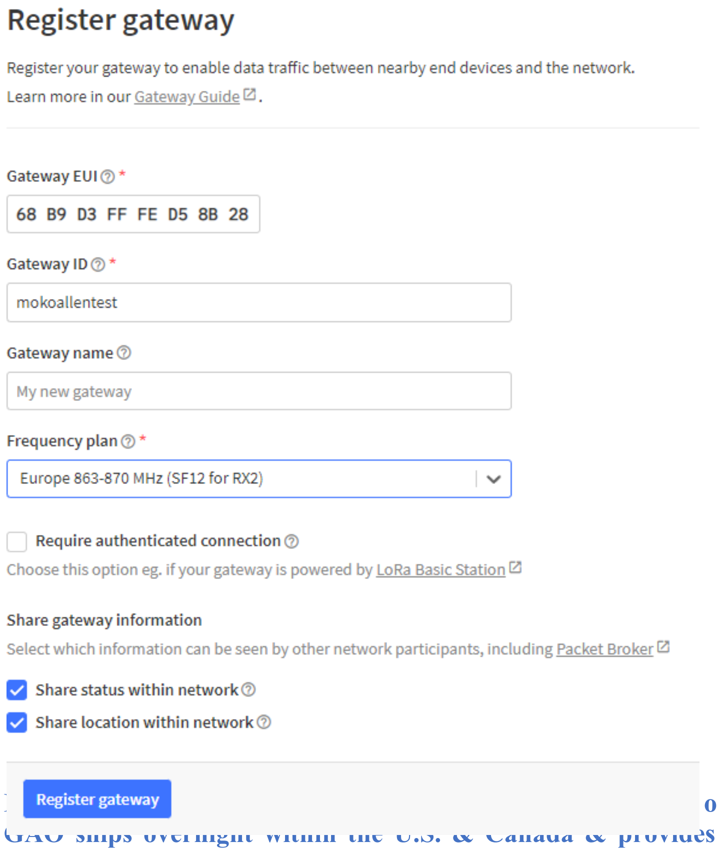
Welcome back, zt416714610! 👋

Walk right through to your applications and/or gateways.

Need help? Have a look at our Documentation or Get support.

Step 4: Register a new gateway





Register gateway

Register your gateway to enable data traffic between nearby end devices and the network. Learn more in our Gateway Guide.

Gateway EUI * 68 B9 D3 FF FE D5 8B 28

Gateway ID * mokoallentest

Gateway name My new gateway

Frequency plan * Europe 863-870 MHz (SF12 for RX2)

☐ Require authenticated connection

Choose this option eg. if your gateway is powered by LoRa Basic Station

Share gateway information

Select which information can be seen by other network participants, including Packet Broker

☑ Share status within network

☑ Share location within network

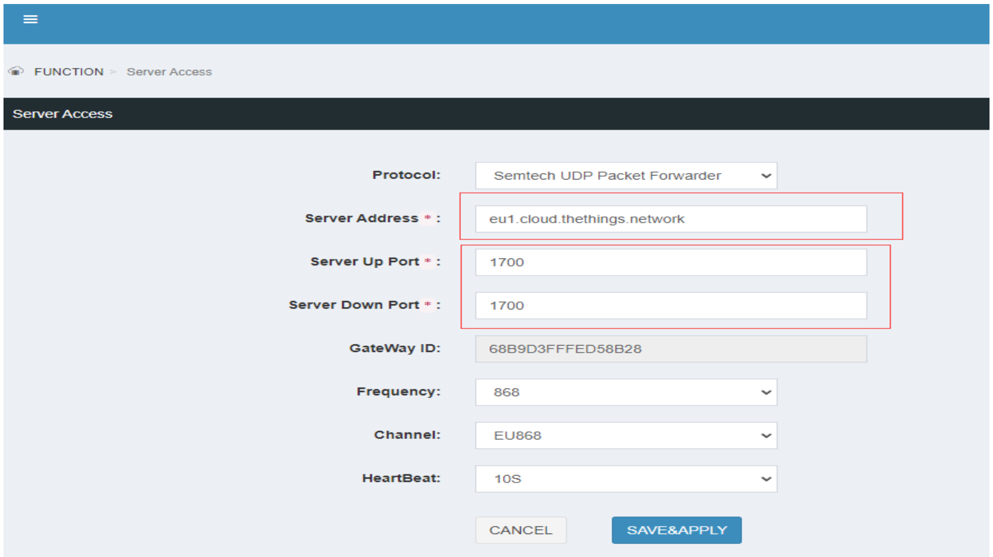
1. Fill in Gateway EUI with the mkgw2-1 w’s gateway id which have been got inStep 1.

2. Customize a TTN gateway id and fillin.

3. Select the EU868 in Frequency Plan.

4. Click “Register gateway”.

Step 5: Configure gateway's parameter on FUNCTION-Server Access page of Web GUI.



Protocol: Semtech UDP Packet Forwarder

Server Address * : eu1.cloud.thethings.network

Server Up Port * : 1700

Server Down Port * : 1700

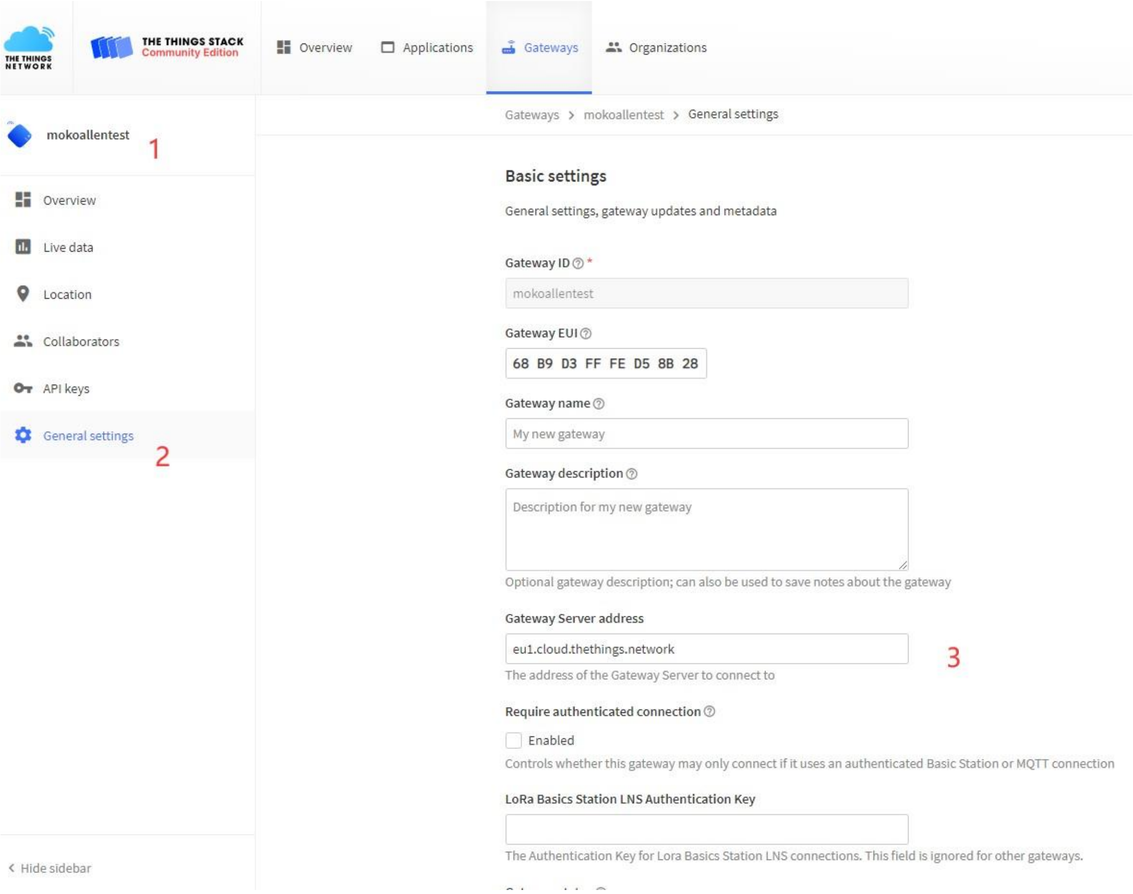
GateWay ID: 68B9D3FFFED58B28

Frequency: 868

Channel: EU868

HeartBeat: 10S

1. Fill in Server address on server access page. The server address should be same to TTN gateway information page.



Basic settings

General settings, gateway updates and metadata

Gateway ID * : mokoallentest

Gateway EUI: 68 B9 D3 FF FE D5 8B 28

Gateway name: My new gateway

Gateway description: Description for my new gateway

Optional gateway description; can also be used to save notes about the gateway

Gateway Server address: eu1.cloud.thethings.network

The address of the Gateway Server to connect to

Require authenticated connection

□ Enabled

Controls whether this gateway may only connect if it uses an authenticated Basic Station or MQTT connection

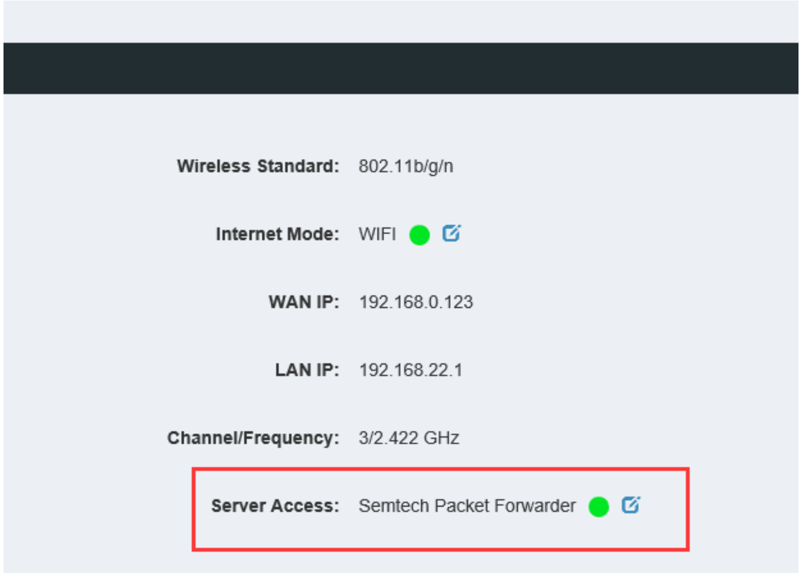
LoRa Basics Station LNS Authentication Key

The Authentication Key for Lora Basics Station LNS connections. This field is ignored for other gateways.

1. Fill in server up port and server down port, it will be 1700 when use TTN network server.
2. Select the frequency and channel. User can refer to chapter 7.2 UDP Packet Forwarder – Step 4.

Step 6: Check the gateway status.

1.Check the gateway status of home page on Web GUI, if it is green, it means that the gatewayhad been connected successfully.



Wireless Standard: 802.11b/g/n

Internet Mode: WIFI ●

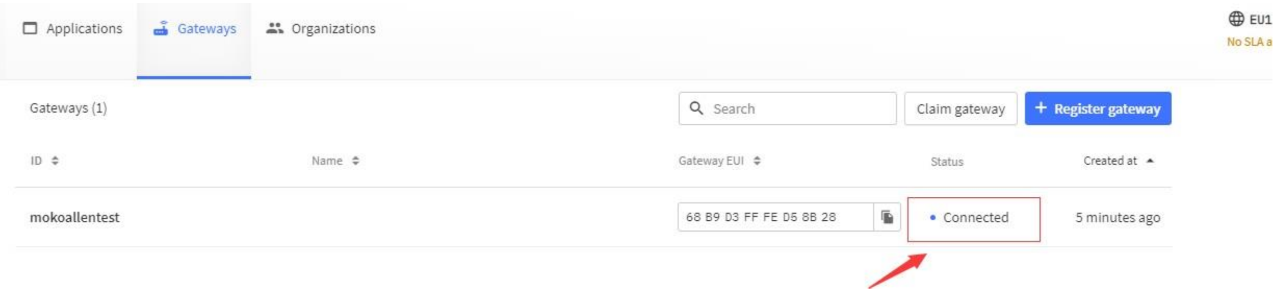
WAN IP: 192.168.0.123

LAN IP: 192.168.22.1

Channel/Frequency: 3/2.422 GHz

Server Access: Semtech Packet Forwarder ●

2. Check the gateway status on TTN platform. After registering the gateway to TTN network server at1st time, may need to wait for a few minutes before the gateway status is refreshed.

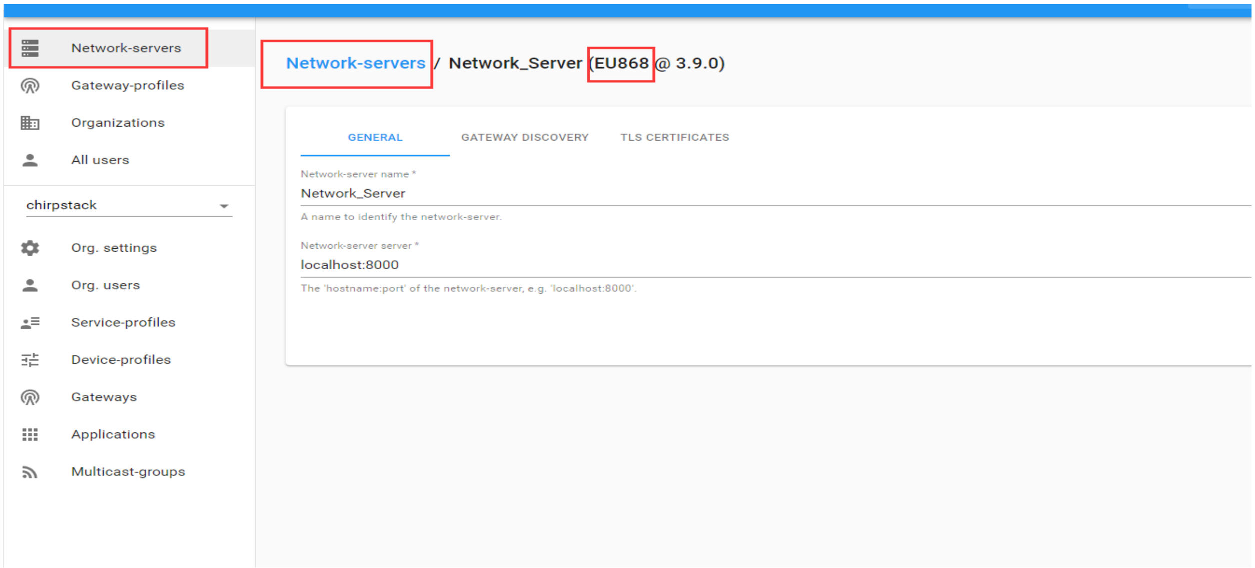


Gateways (1)

ID	Name	Gateway EUI	Status	Created at
mokoallentest		68 B9 D3 FF FE D5 8B 28	• Connected	5 minutes ago

Chirp stack platform Configuration Example

Step 1: Pls check the network-servers setting interface, there should be the region that you are usingnow.



Network-servers / Network_Server (EU868 @ 3.9.0)

Network-server name *

Network_Server

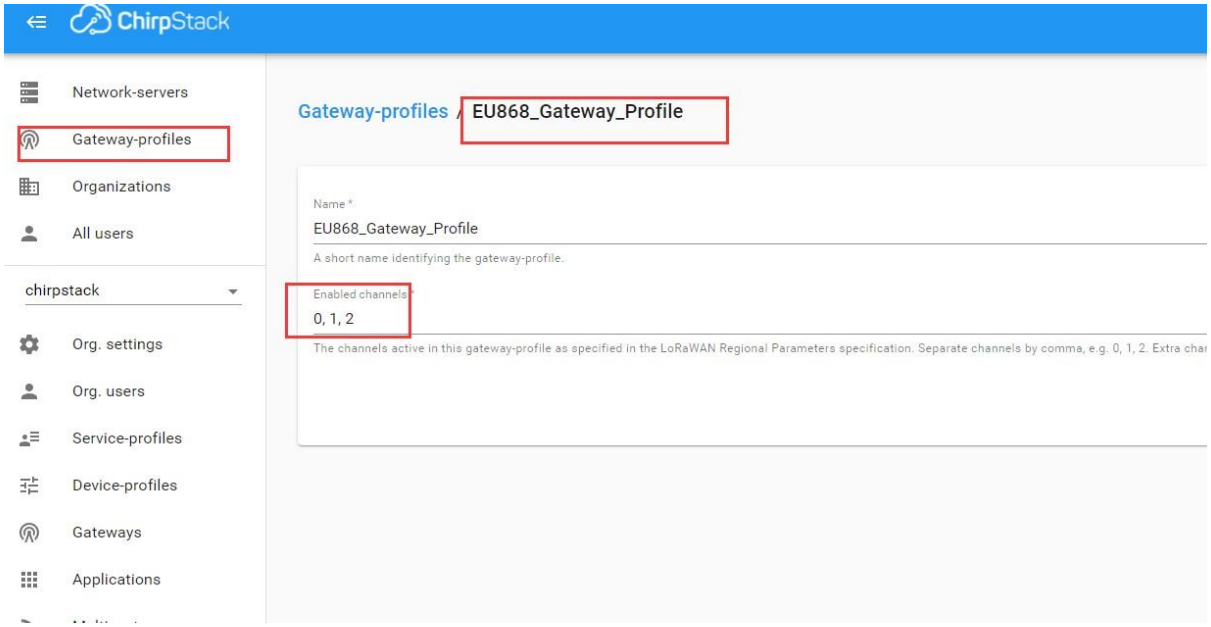
A name to identify the network-server.

Network-server server *

localhost:8000

The 'hostname:port' of the network-server, e.g. 'localhost:8000'.

Step 2: Check Gateway Profile setting Page The enabled channels should be same to CH setting of end-device that you want to use.



Gateway-profiles / EU868_Gateway_Profile

Name *

EU868_Gateway_Profile

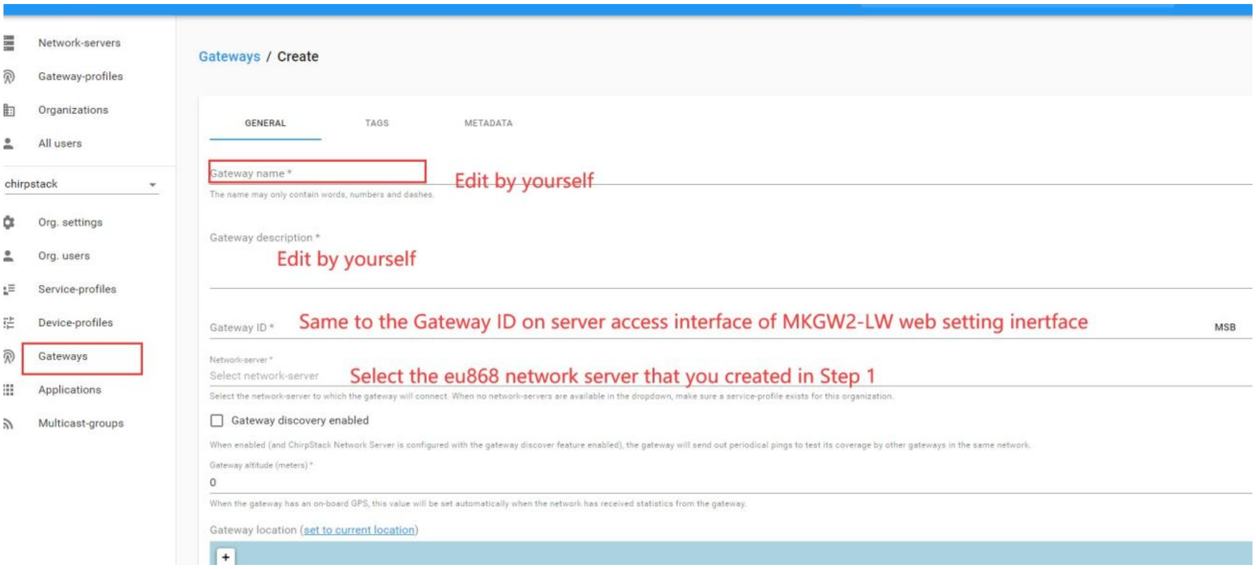
A short name identifying the gateway-profile.

Enabled channels *

0, 1, 2

The channels active in this gateway-profile as specified in the LoRaWAN Regional Parameters specification. Separate channels by comma, e.g. 0, 1, 2. Extra char

Step 3: Register Gateway on chirp stack.



Gateway name * — Edit by yourself

The name may only contain words, numbers and dashes.

Gateway description * — Edit by yourself

Gateway ID * — Same to the Gateway ID on server access interface of MKGW2-LW web setting inertface — MSB

Network-server *
Select network-server — Select the eu868 network server that you created in Step 1

Select the network-server to which the gateway will connect. When no network-servers are available in the dropdown, make sure a service-profile exists for this organization.

□ Gateway discovery enabled

When enabled (and ChirpStack Network Server is configured with the gateway discover feature enabled), the gateway will send out periodical pings to test its coverage by other gateways in the same network.

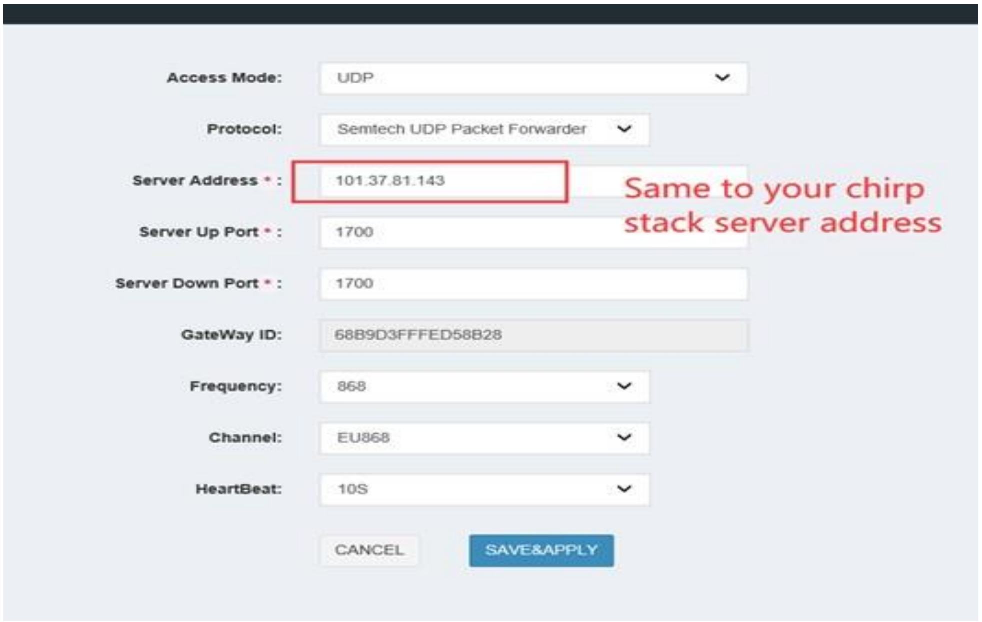
Gateway altitude (meters) *
0

When the gateway has an on-board GPS, this value will be set automatically when the network has received statistics from the gateway.

Gateway location (set to current location)

Step 4: Configure gateway's parameter on FUNCTION-Server *Access* page of Web GUI.

1. Fill in Server address on server access page. The server address should be same to Chirp

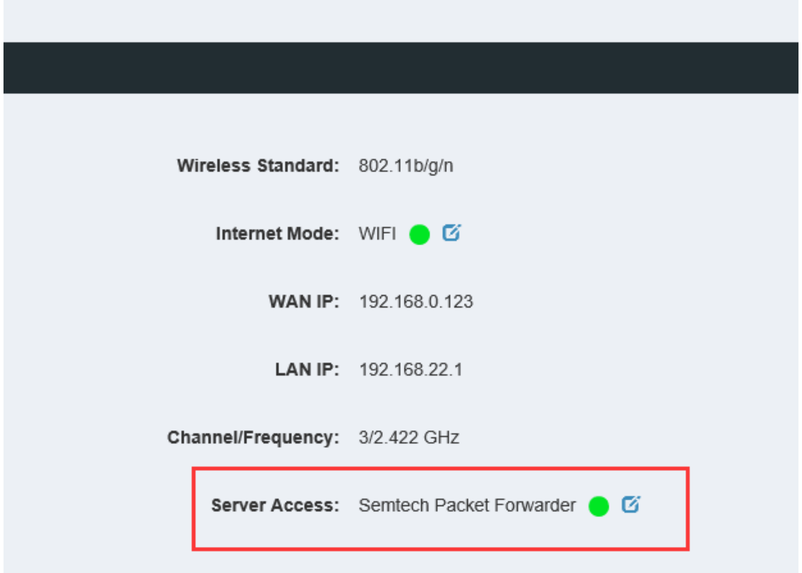


Access Mode:	UDP
Protocol:	Semtech UDP Packet Forwarder
Server Address * :	101.37.81.143
Server Up Port * :	1700
Server Down Port * :	1700
GateWay ID:	68B9D3FFFED58B28
Frequency:	868
Channel:	EU868
HeartBeat:	10S

Same to your chirp stack server address

stack gateway information page.
2. Fill in server up port and server down port, it will be 1700 when use Chirp stack network server.
3. Select the frequency and channel, it should be matched to CH setting of *Step 2*.
About setting example, user can refer to *chapter 7.2 UDP Packet Forwarder - Step 4*.

Step 5: Check the gateway status of home page on Web GUI.
Check the network led indicator of gateway, if it is green, it means that the gateway had been connected successfully.



Wireless Standard: 802.11b/g/n
Internet Mode: WIFI ●
WAN IP: 192.168.0.123
LAN IP: 192.168.22.1
Channel/Frequency: 3/2.422 GHz
Server Access: Semtech Packet Forwarder ●

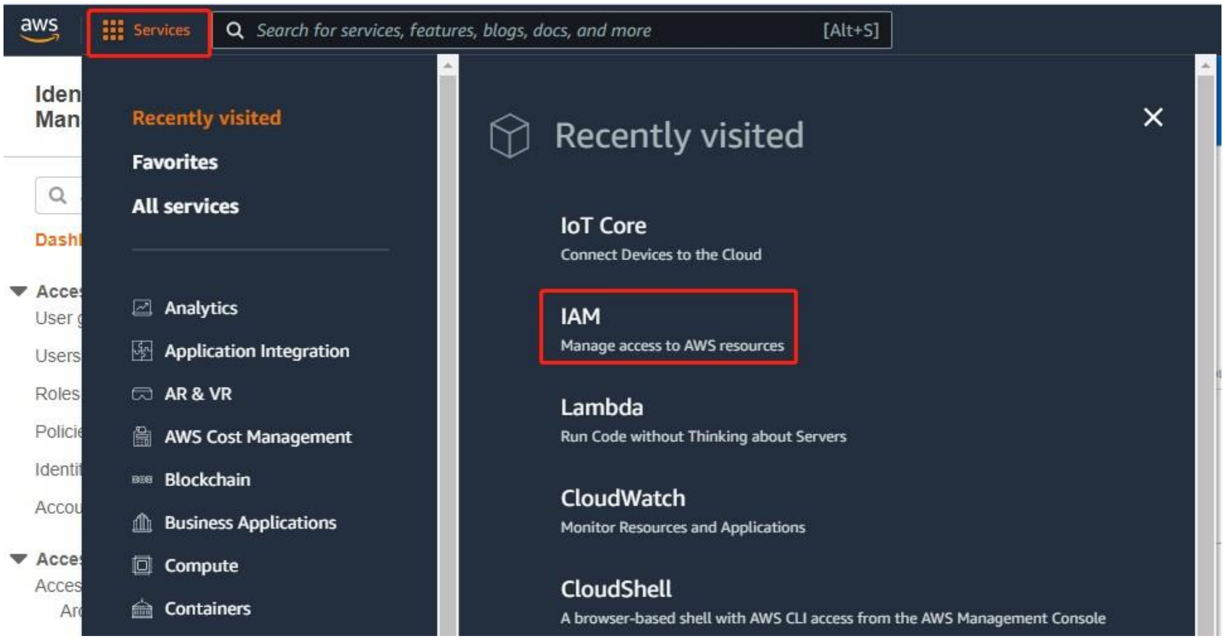
Appendix 2 SimTech Basics Station

AWS platform Configuration Example

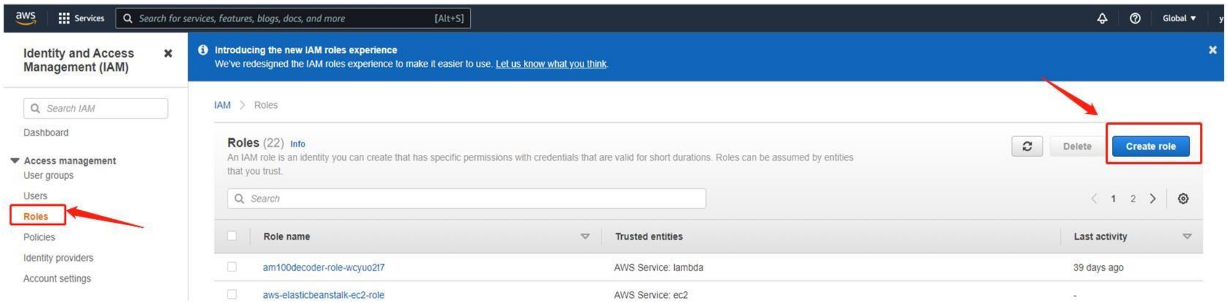
If you are familiar with AWS, you may refer directly to the AWS developer guide:
https://docs.aws.amazon.com/iot/latest/developerguide/connect-iot-lorawan.html

Part 1: Set up Policies and Roles in IAM

Step 1: Login in your AWS account, then go to IAM console.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Recently visited
Favorites
All services
Analytics
Application Integration
AR & VR
AWS Cost Management
Blockchain
Business Applications
Compute
Containers
Recently visited
IoT Core
Connect Devices to the Cloud
IAM
Manage access to AWS resources
Lambda
Run Code without Thinking about Servers
CloudWatch
Monitor Resources and Applications
CloudShell
A browser-based shell with AWS CLI access from the AWS Management Console

Step 2: Go to Roles page, then click "Create role".



Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

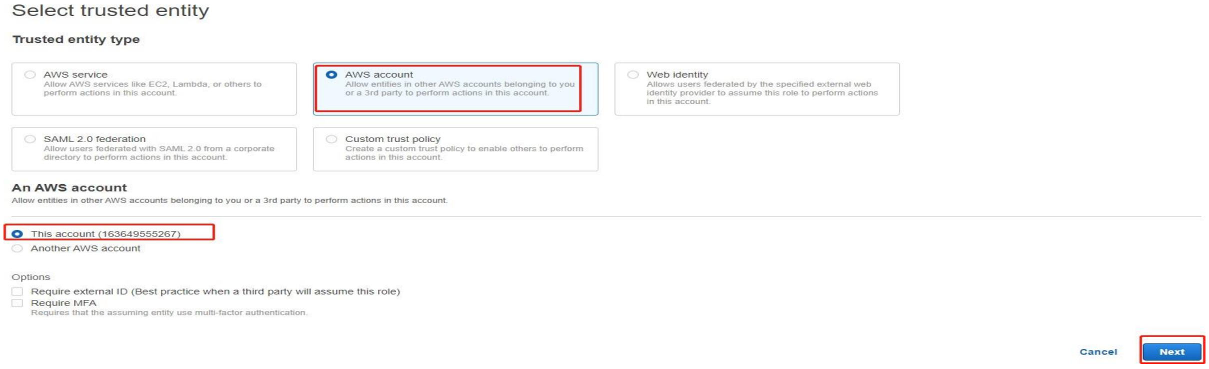
Roles (22) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
am100decoder-role-wcyuo2t7	AWS Service: lambda	39 days ago
aws-elasticbeanstalk-ec2-role	AWS Service: ec2	-

Step 3: Then select "AWS account" and "This account", then click "Next".

Step 4: Enter “Wireless Gateway Cert Manager” on the search box and search it.



Select trusted entity

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

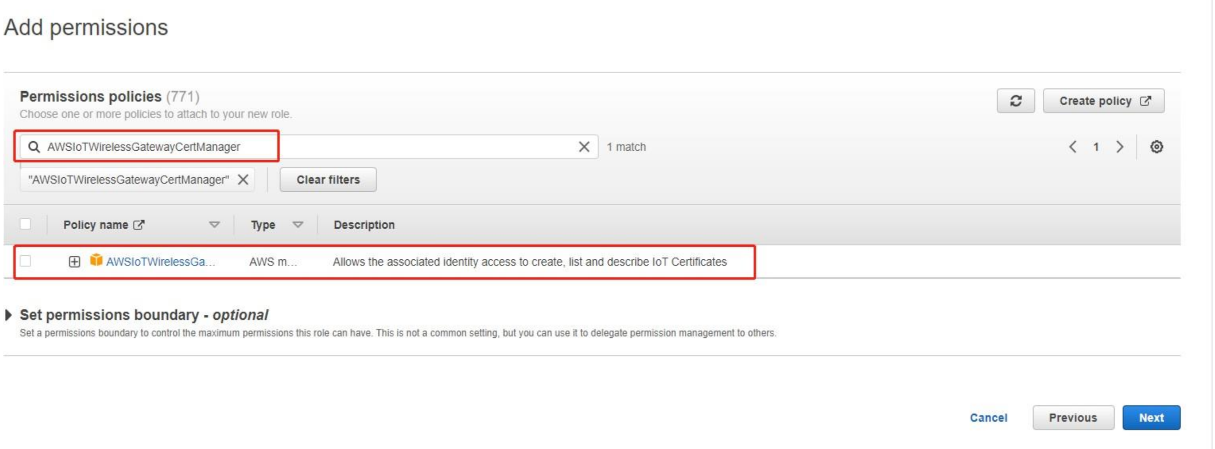
○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

● This account (163649555267)
○ Another AWS account

Options
□ Require external ID (Best practice when a third party will assume this role)
□ Require MFA
Requires that the assuming entity use multi-factor authentication.



Add permissions

Permissions policies (771)
Choose one or more policies to attach to your new role.

AWSIoTWirelessGatewayCertManager   1 match

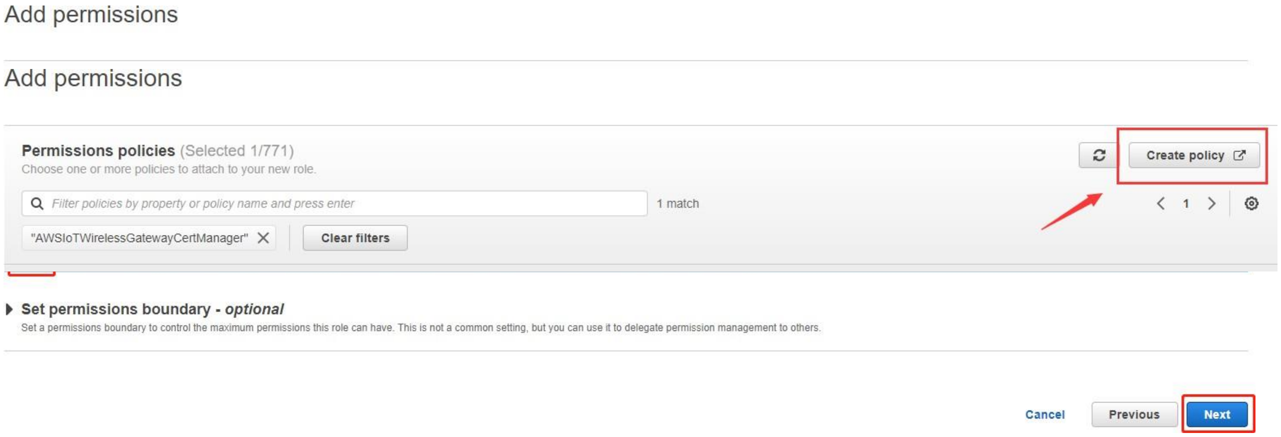
"AWSIoTWirelessGatewayCertManager"

□	Policy name	Type	Description
□	⊞ AWSIoTWirelessGa...	AWS m...	Allows the associated identity access to create, list and describe IoT Certificates

▸ Set permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Step 5: If there is related policy in search result, select it on the check box, and then click “Next”.

Then, turn to *Step 9*.



Add permissions

Add permissions

Permissions policies (Selected 1/771)
Choose one or more policies to attach to your new role.

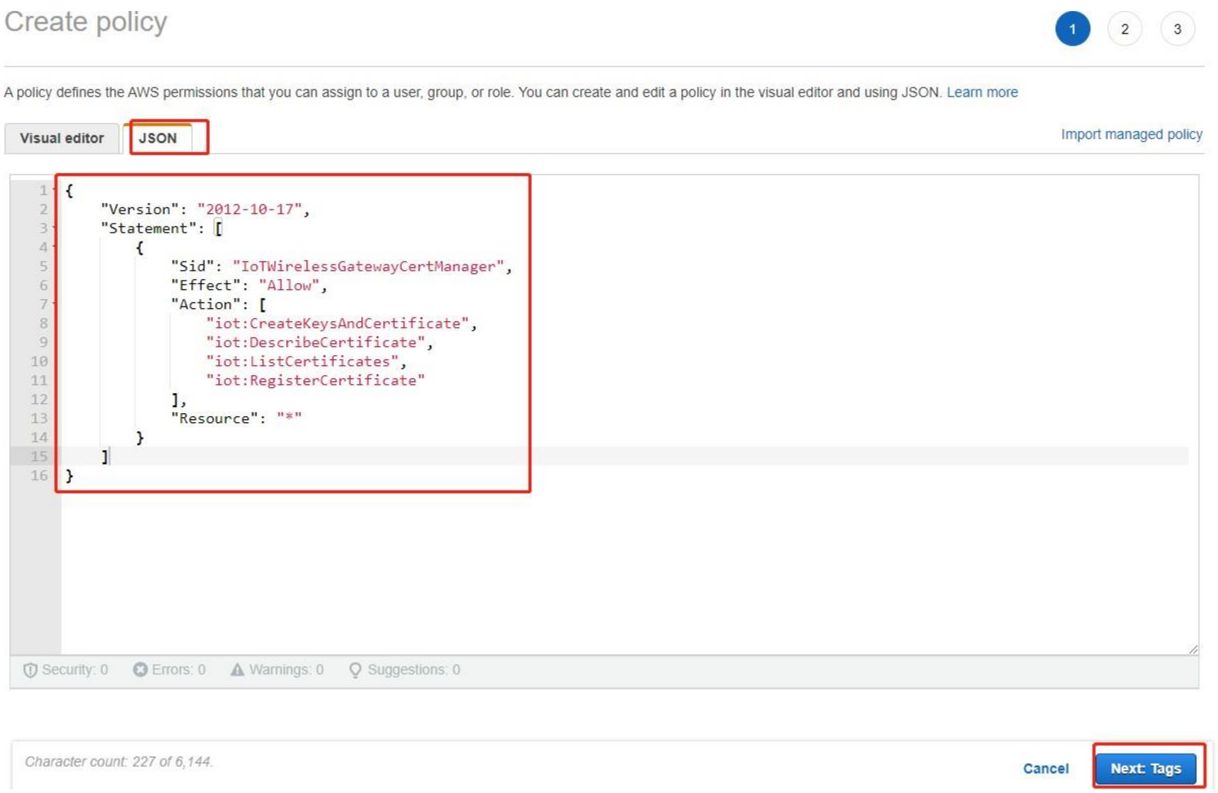
Filter policies by property or policy name and press enter — 1 match

"AWSIoTWirelessGatewayCertManager" ✕ | Clear filters

▸ **Set permissions boundary -** ***optional***
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Step 6: If there isn’t related policy in search result, click “Create policy”.
Modify the content of Json file. The content should be same to the following picture.

Then click “Next Tags”.



Create policy

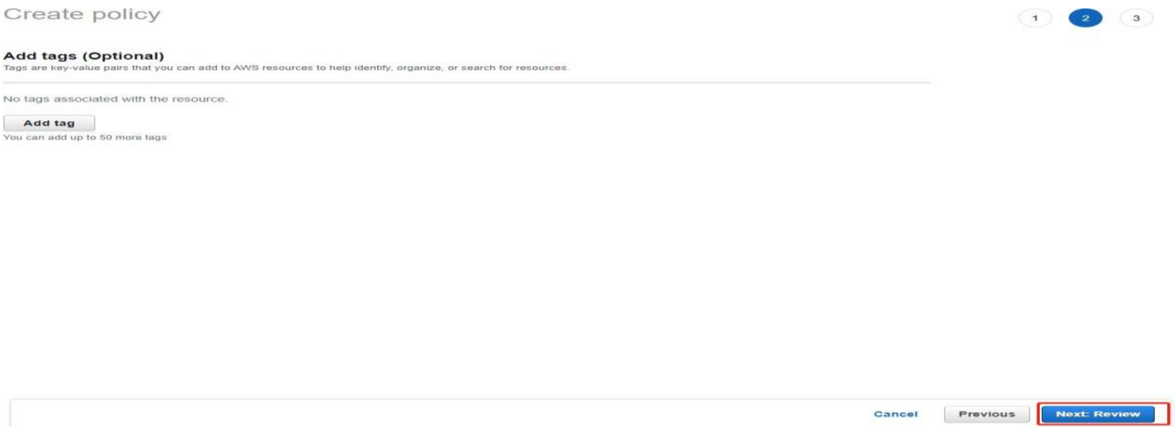
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IoTWirelessGatewayCertManager",
            "Effect": "Allow",
            "Action": [
                "iot:CreateKeysAndCertificate",
                "iot:DescribeCertificate",
                "iot:ListCertificates",
                "iot:RegisterCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Character count: 227 of 6,144.

Then click “Next: Reviews”.



Create policy

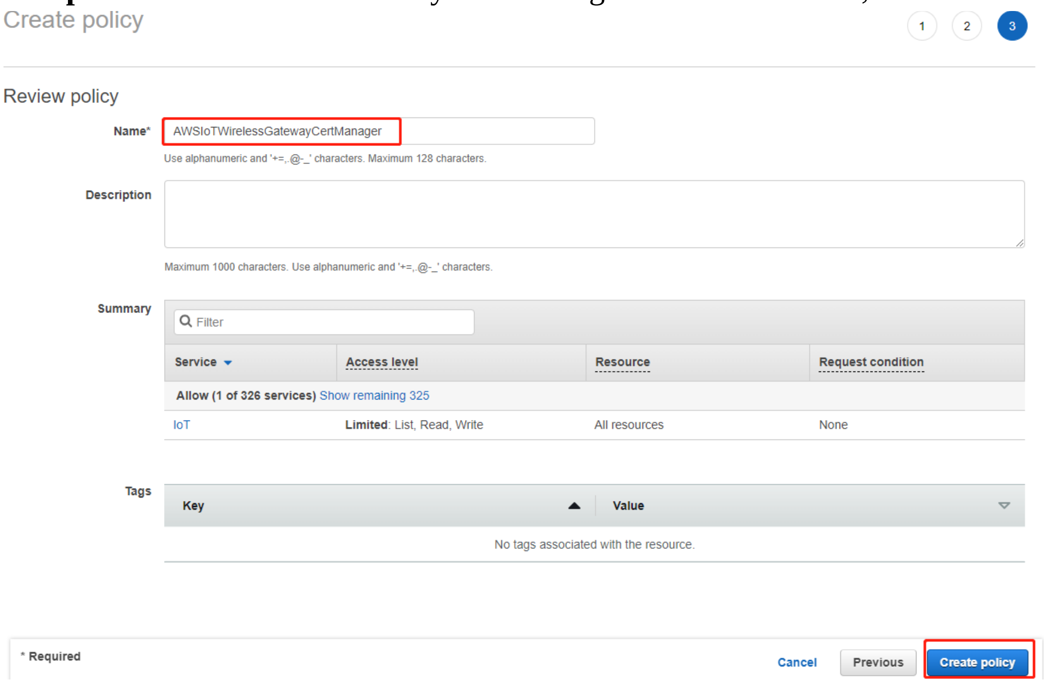
Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags

Step 7: Enter “Wireless Gateway Cert Manager” on the name box, then choose create policy.



Create policy

Review policy

Name* AWSIoTWirelessGatewayCertManager

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

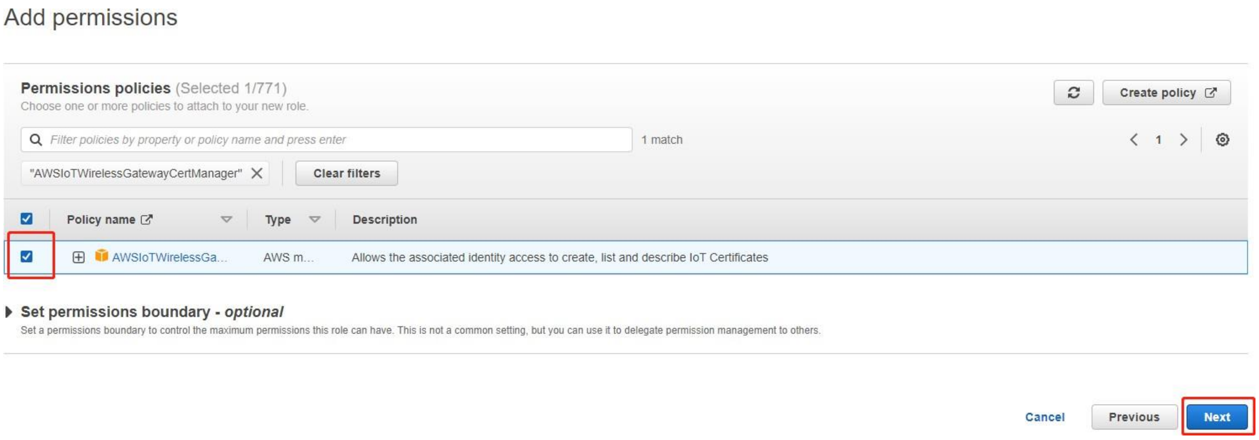
Service	Access level	Resource	Request condition
Allow (1 of 326 services) Show remaining 325			
IoT	**Limited**: List, Read, Write	All resources	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Step 8: select it on the check box, and then click "Next".



Add permissions

Permissions policies (Selected 1/771)

Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter — 1 match

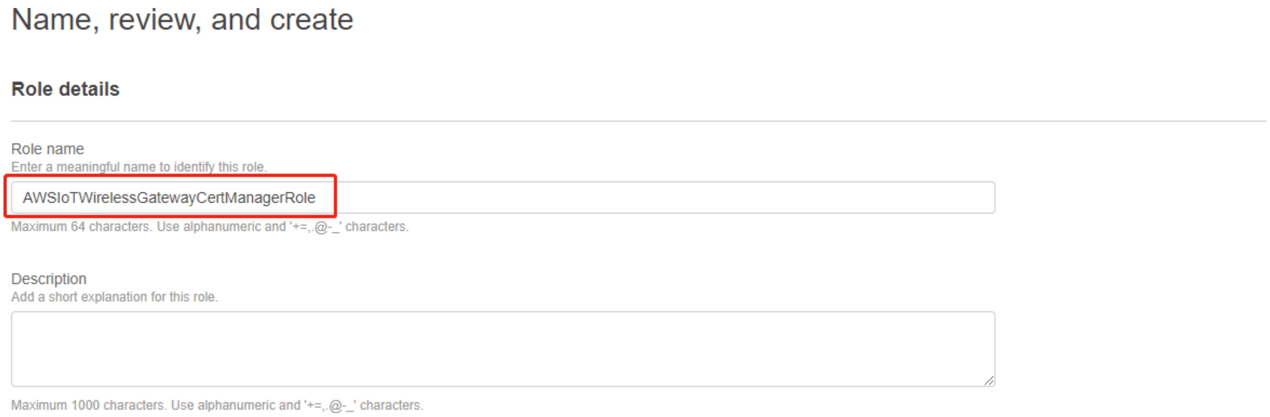
"AWSIoTWirelessGatewayCertManager" ✕ — Clear filters

☑	Policy name	Type	Description
☑	⊞ AWSIoTWirelessGa...	AWS m...	Allows the associated identity access to create, list and describe IoT Certificates

▸ **Set permissions boundary - *optional***

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Step 9: After set up policies in IAM, enter "Wireless Gateway Cert Manager Role" on Role name box, then click "Create role".



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

AWSIoTWirelessGatewayCertManagerRole

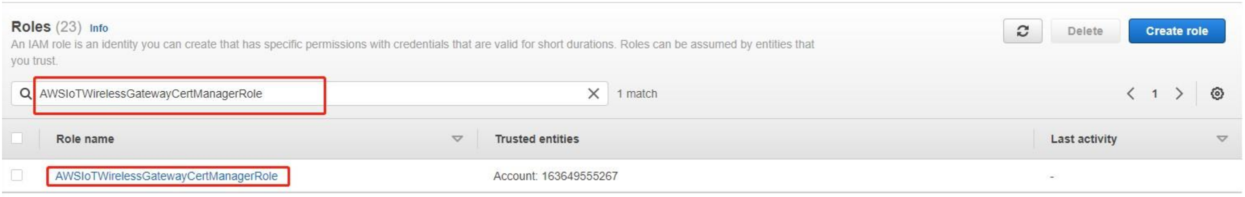
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 10: Search "Wireless Gateway Cert Manager Role", then click the Wireless Gateway Cert Manager Role" on role name result.



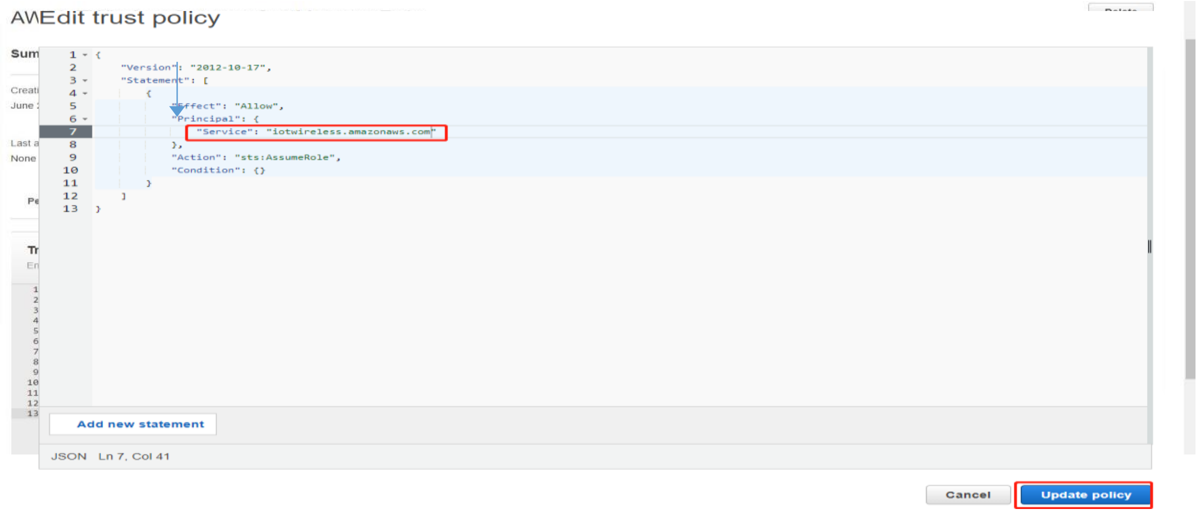
Roles (23) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

AWSIoTWirelessGatewayCertManagerRole ✕ — 1 match

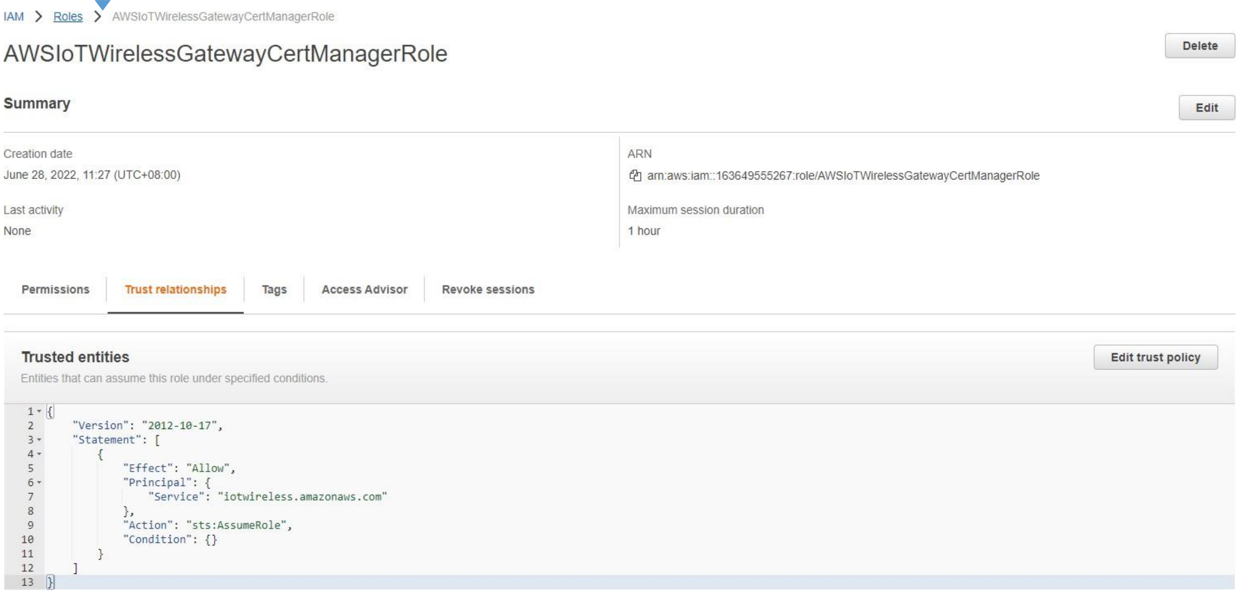
□	Role name	Trusted entities	Last activity
□	AWSIoTWirelessGatewayCertManagerRole	Account: 163649555267	-

Step 11: Click” Trust relationships”, then click “Edit trust policy”, and update the “Principal” contentto "Principal": {"Service": "iotwireless.amazonaws.com"}



AWEdit trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotwireless.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```



AWSIoTWirelessGatewayCertManagerRole

Summary

Creation date
June 28, 2022, 11:27 (UTC+08:00)

Last activity
None

ARN
arn:aws:iam::163649555267:role/AWSIoTWirelessGatewayCertManagerRole

Maximum session duration
1 hour

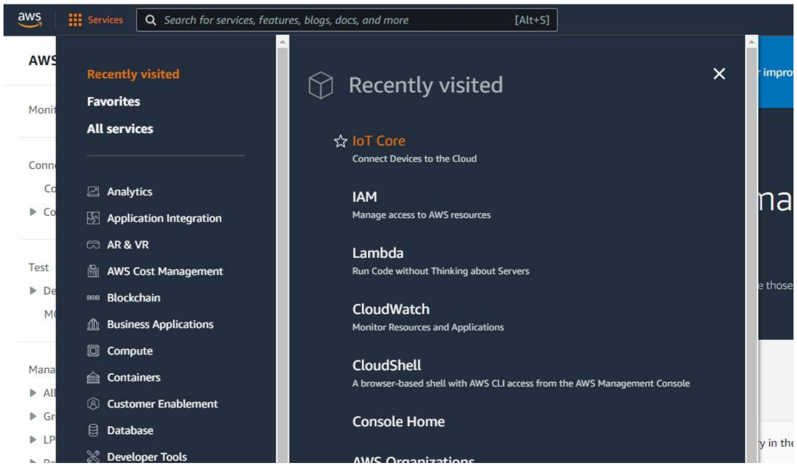
Trusted entities

Entities that can assume this role under specified conditions.

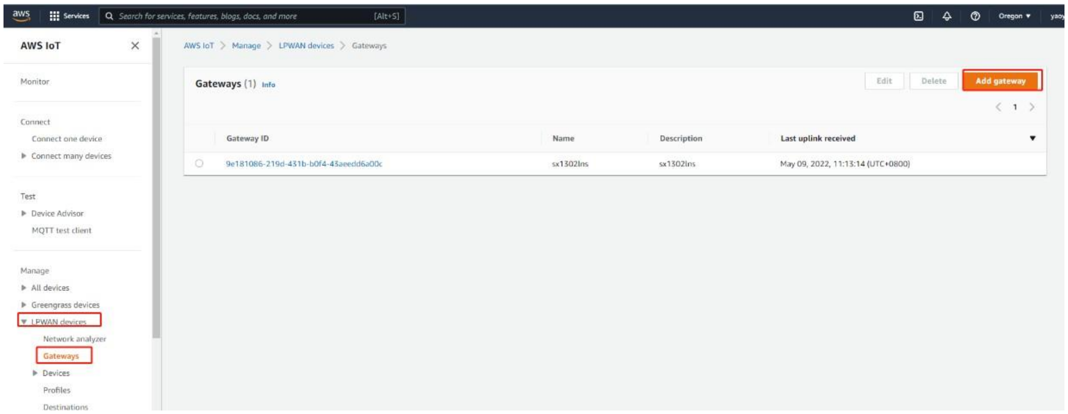
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotwireless.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Part 2: Add the Gateway to AWS

Step 1: Select Service - IOT Core on AWS console.



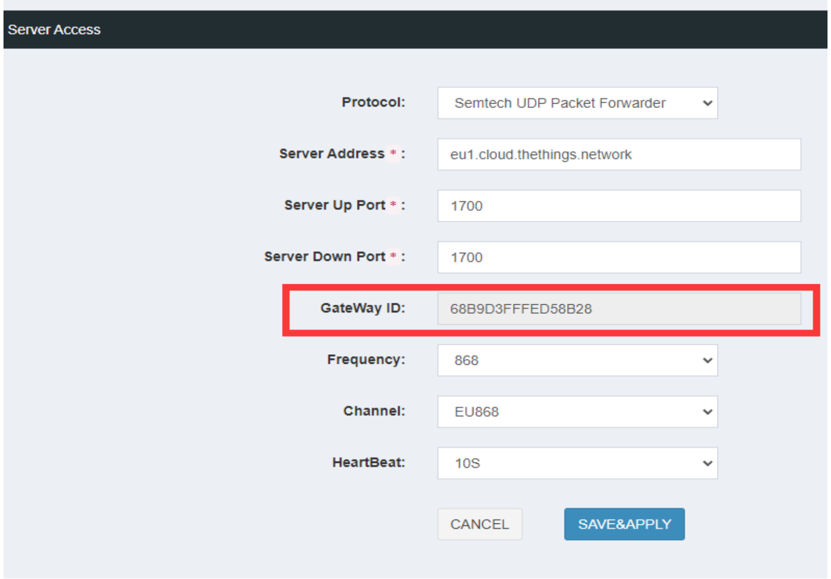
Step 2: Select LPWAN devices – Gateways.



Gateways (1) Info

	Gateway ID	Name	Description	Last uplink received
○	9e181086-219d-431b-b0f4-43aeedd6a00c	sx1302lns	sx1302lns	May 09, 2022, 11:13:14 (UTC+0800)

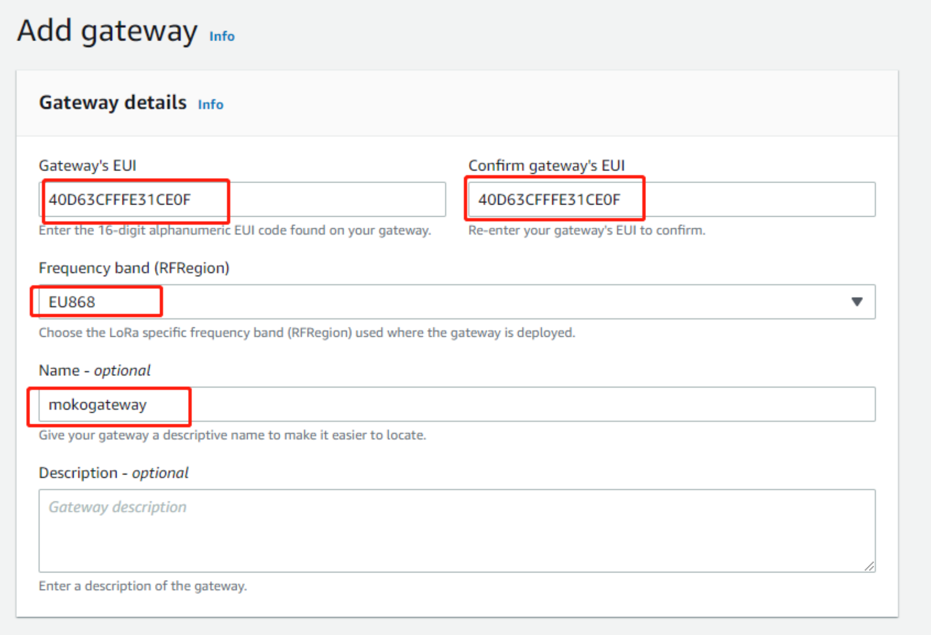
Step 3: Power access to Web GUI, get the gateway ID on *FUNCTAION-ServerAccess* page of Web GUI.



Server Access

Protocol:	Semtech UDP Packet Forwarder
Server Address * :	eu1.cloud.thethings.network
Server Up Port * :	1700
Server Down Port * :	1700
GateWay ID:	68B9D3FFFED58B28
Frequency:	868
Channel:	EU868
HeartBeat:	10S

Step 4: Enter the gateway register information, then click “add gateway”.



Add gateway Info

Gateway details Info

Gateway's EUI: 40D63CFFFE31CE0F
Enter the 16-digit alphanumeric EUI code found on your gateway.

Confirm gateway's EUI: 40D63CFFFE31CE0F
Re-enter your gateway's EUI to confirm.

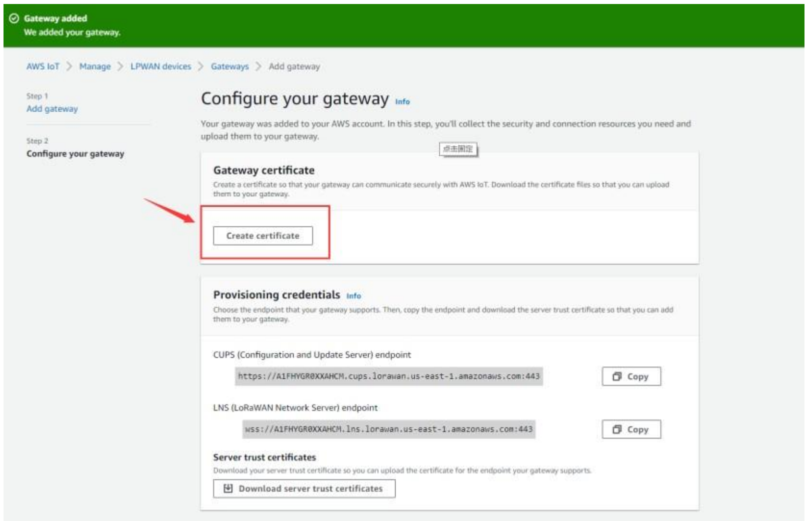
Frequency band (RFRegion): EU868
Choose the LoRa specific frequency band (RFRegion) used where the gateway is deployed.

Name - *optional*: mokogateway
Give your gateway a descriptive name to make it easier to locate.

Description - *optional*: *Gateway description*
Enter a description of the gateway.

Fill in Gateway EUI with the GAOTek-IIT-163's gateway id which have been got in Step 3.Select the currently used frequency band and remember it.

Step 5: Click "Create certificate".



Gateway added
We added your gateway.

AWS IoT > Manage > LPWAN devices > Gateways > Add gateway

Step 1
Add gateway

Step 2
Configure your gateway

Configure your gateway Info

Your gateway was added to your AWS account. In this step, you'll collect the security and connection resources you need and upload them to your gateway.

点击固定

Gateway certificate

Create a certificate so that your gateway can communicate securely with AWS IoT. Download the certificate files so that you can upload them to your gateway.

Provisioning credentials Info

Choose the endpoint that your gateway supports. Then, copy the endpoint and download the server trust certificate so that you can add them to your gateway.

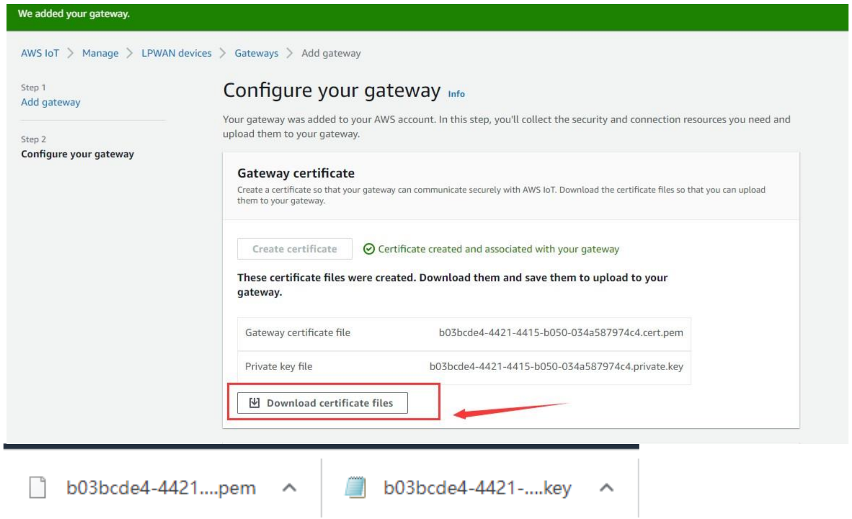
CUPS (Configuration and Update Server) endpoint: https://A1FHYGR0XXAHCM.cups.lorawan.us-east-1.amazonaws.com:443

LNS (LoRaWAN Network Server) endpoint: wss://A1FHYGR0XXAHCM.lns.lorawan.us-east-1.amazonaws.com:443

Server trust certificates

Download your server trust certificate so you can upload the certificate for the endpoint your gateway supports.

Step 6: Download certificate files



We added your gateway.

Configure your gateway Info

Your gateway was added to your AWS account. In this step, you'll collect the security and connection resources you need and upload them to your gateway.

Gateway certificate

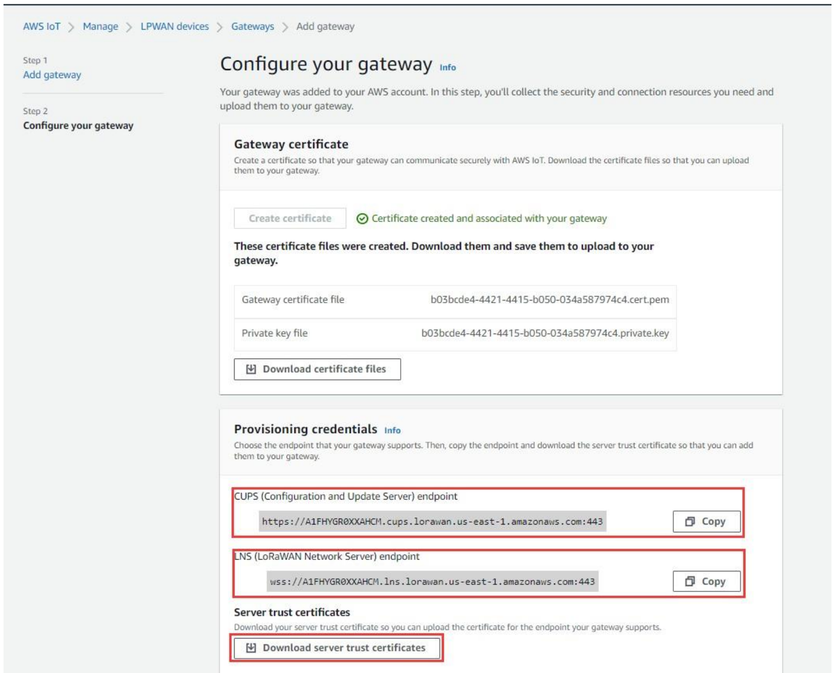
Create a certificate so that your gateway can communicate securely with AWS IoT. Download the certificate files so that you can upload them to your gateway.

Certificate created and associated with your gateway

These certificate files were created. Download them and save them to upload to your gateway.

Gateway certificate file	b03bcde4-4421-4415-b050-034a587974c4.cert.pem
Private key file	b03bcde4-4421-4415-b050-034a587974c4.private.key

Step 7: Copy CUPS URL and LNS URL, then download server trust certificates.



Configure your gateway Info

Your gateway was added to your AWS account. In this step, you'll collect the security and connection resources you need and upload them to your gateway.

Gateway certificate

Create a certificate so that your gateway can communicate securely with AWS IoT. Download the certificate files so that you can upload them to your gateway.

Certificate created and associated with your gateway

These certificate files were created. Download them and save them to upload to your gateway.

Gateway certificate file	b03bcde4-4421-4415-b050-034a587974c4.cert.pem
Private key file	b03bcde4-4421-4415-b050-034a587974c4.private.key

Provisioning credentials Info

Choose the endpoint that your gateway supports. Then, copy the endpoint and download the server trust certificate so that you can add them to your gateway.

CUPS (Configuration and Update Server) endpoint

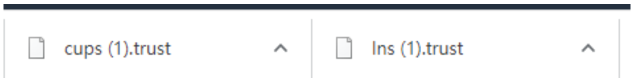
```
https://A1FHYGR0XXAHCM.cups.lorawan.us-east-1.amazonaws.com:443
```

LNS (LoRaWAN Network Server) endpoint

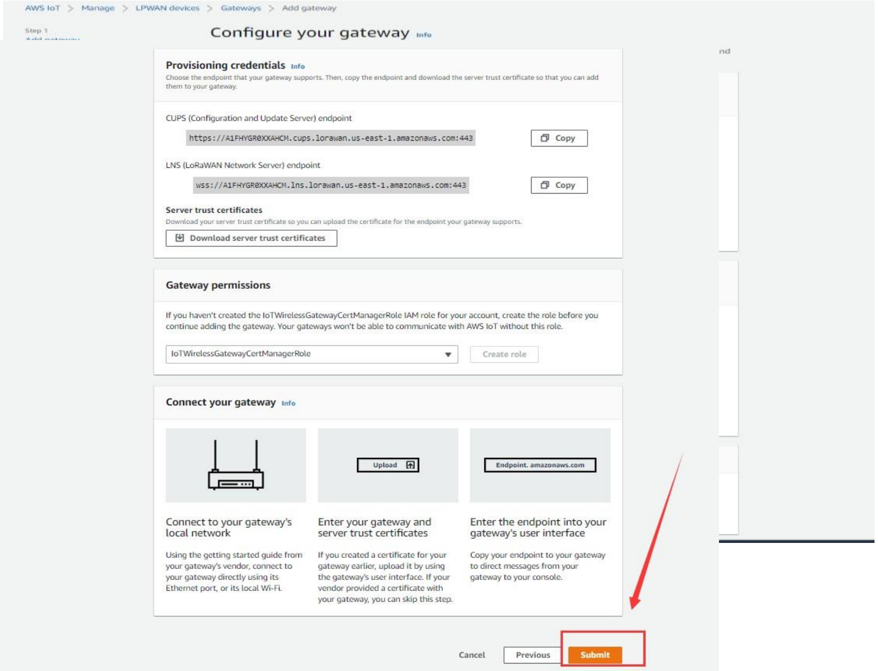
```
wss://A1FHYGR0XXAHCM.lns.lorawan.us-east-1.amazonaws.com:443
```

Server trust certificates

Download your server trust certificate so you can upload the certificate for the endpoint your gateway supports.



Step 8: Make sure that the role of gateway permissions is "IoT Wireless Gateway Cert Manager Role".


AWS IoT > Manage > LPWAN devices > Gateways > Add gateway
Step 1
Info
Info
Copy
Copy
Download server trust certificates
Create role
Info
Upload
Endpoint. amazonaws.com
Cancel
Previous
Submit

Configure your gateway

Provisioning credentials

Choose the endpoint that your gateway supports. Then, copy the endpoint and download the server trust certificate so that you can add them to your gateway.

CUPS (Configuration and Update Server) endpoint

```
https://A1FHYGR0XXAHCM.cups.lorawan.us-east-1.amazonaws.com:443
```

LNS (LoRaWAN Network Server) endpoint

```
wss://A1FHYGR0XXAHCM.lns.lorawan.us-east-1.amazonaws.com:443
```

Server trust certificates

Download your server trust certificate so you can upload the certificate for the endpoint your gateway supports.

Gateway permissions

If you haven't created the IoTWirelessGatewayCertManagerRole IAM role for your account, create the role before you continue adding the gateway. Your gateways won't be able to communicate with AWS IoT without this role.

IoTWirelessGatewayCertManagerRole

Connect your gateway

Connect to your gateway's local network

Using the getting started guide from your gateway's vendor, connect to your gateway directly using its Ethernet port, or its local Wi-Fi.

Enter your gateway and server trust certificates

If you created a certificate for your gateway earlier, upload it by using the gateway's user interface. If your vendor provided a certificate with your gateway, you can skip this step.

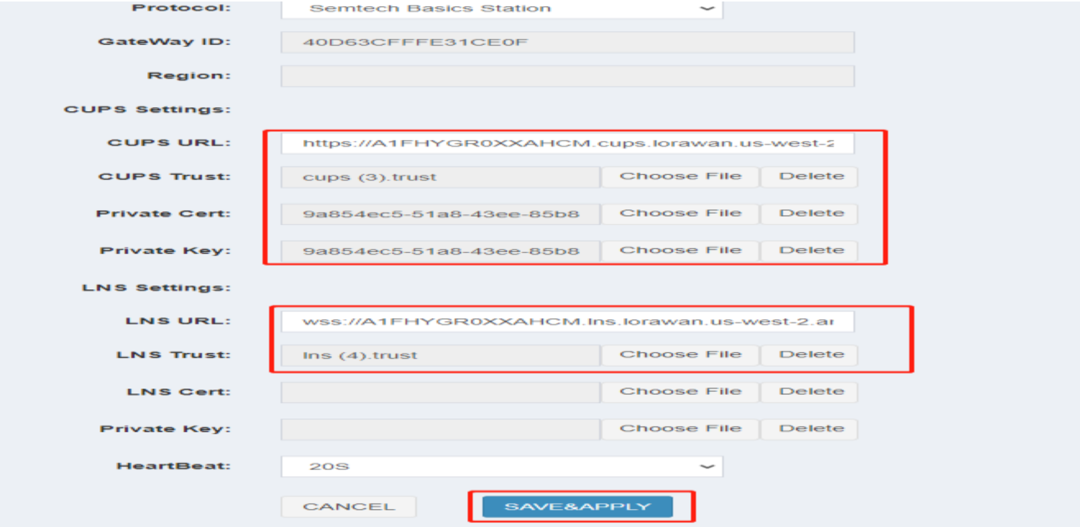
Enter the endpoint into your gateway's user interface

Copy your endpoint to your gateway to direct messages from your gateway to your console.

Step 9: Click "Submit" on the bottom of page.

Part 3: Configure GAOTek-IIT-163 on Web GUI

Step 1: Power on GAOTek-IIT-163, then access to Web GUI, configure gateway's parameter on *FUNCTION - Server Access* page of Web GUI.



Protocol: Semtech Basics Station

GateWay ID: 40D63CFFFE31CE0F

Region:

CUPS Settings:

CUPS URL: https://A1FHYGR0XXAHCM.cups.lorawan.us-west-2

CUPS Trust: cups (3).trust

Private Cert: 9a854ec5-51a8-43ee-85b8

Private Key: 9a854ec5-51a8-43ee-85b8

LNS Settings:

LNS URL: wss://A1FHYGR0XXAHCM.lns.lorawan.us-west-2.ar

LNS Trust: lns (4).trust

LNS Cert:

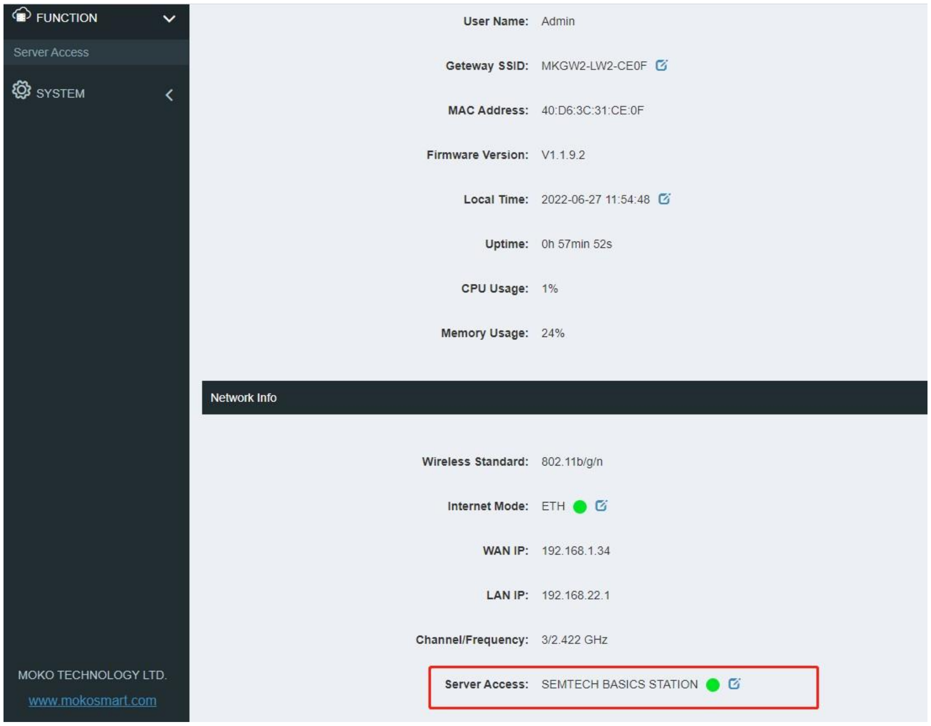
Private Key:

HeartBeat: 20S

Enter the LNS URL and CUPS URL that copied from Part 2 – Step 6 & Step 7.Load “cups. trust” file on CUPS Trust item.
Load “ins. trust” file on LNS Trust item.
Load “xxxxxxx.” file on Private Cert item.
Load “xxxxxxx. key” file on Private Key item. Then, click “SAVE&APPLY”.

Step 2: Check the Server Access status.

If the indicator is green, it means that the gateway had been connected successfully.



User Name: Admin

Geteway SSID: MKGW2-LW2-CE0F

MAC Address: 40:D6:3C:31:CE:0F

Firmware Version: V1.1.9.2

Local Time: 2022-06-27 11:54:48

Uptime: 0h 57min 52s

CPU Usage: 1%

Memory Usage: 24%

Network Info

Wireless Standard: 802.11b/g/n

Internet Mode: ETH ●

WAN IP: 192.168.1.34

LAN IP: 192.168.22.1

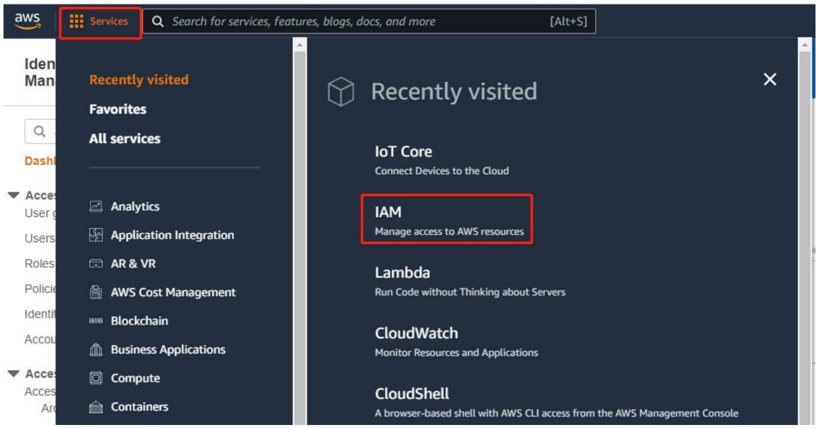
Channel/Frequency: 3/2.422 GHz

Server Access: SEMTECH BASICS STATION ●

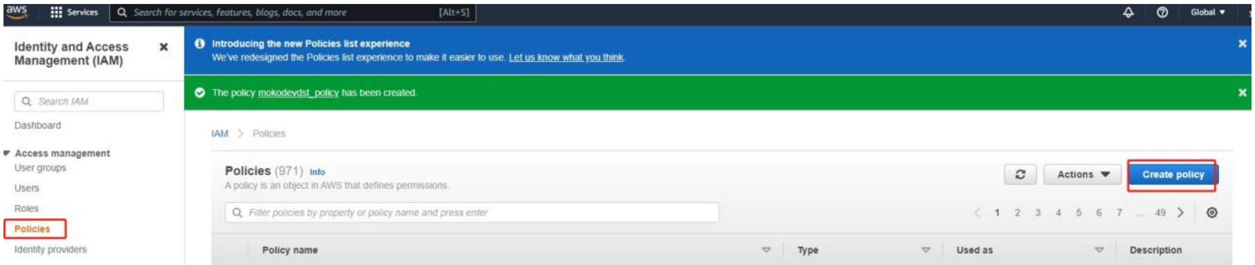
Part 4: Add IAM Role for Destination (Optional)

Note: The destination is created to make it easier for customers to view data on AWS. Ifyou are familiar with AWS server, don’t need to follow this part.

Step 1: Select IAM on AWS console.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Recently visited
Favorites
All services
Analytics
Application Integration
AR & VR
AWS Cost Management
Blockchain
Business Applications
Compute
Containers
Recently visited
IoT Core
Connect Devices to the Cloud
IAM
Manage access to AWS resources
Lambda
Run Code without Thinking about Servers
CloudWatch
Monitor Resources and Applications
CloudShell
A browser-based shell with AWS CLI access from the AWS Management Console

After turn to policy page, click "Create Policy", and then edit JSON content, then click "Next Tags".The JSON content should be same to the following picture.



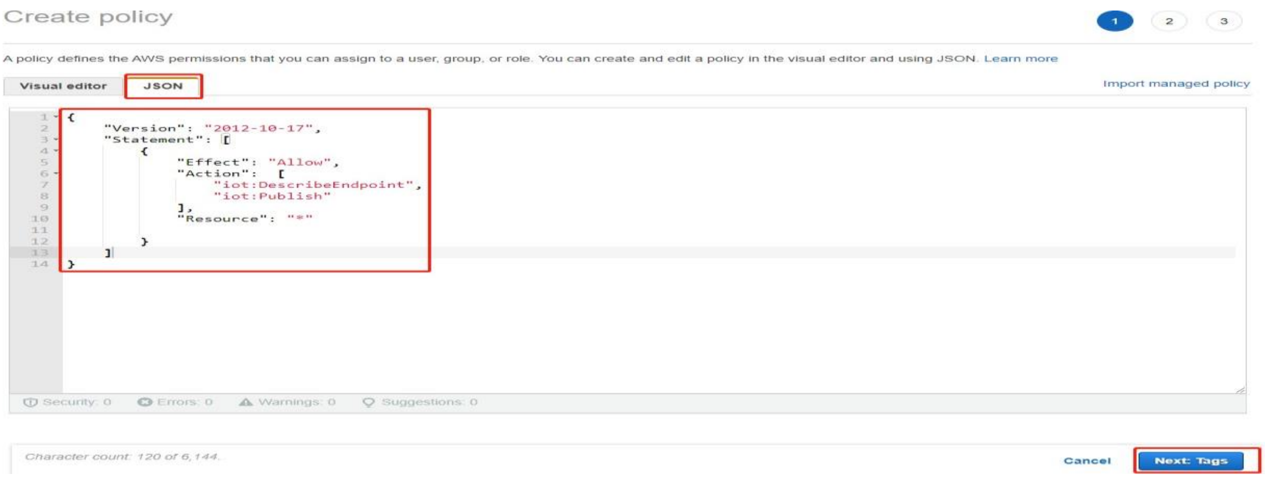
Introducing the new Policies list experience

We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy mokodevdst_policy has been created.

Policies (971) Info

A policy is an object in AWS that defines permissions.

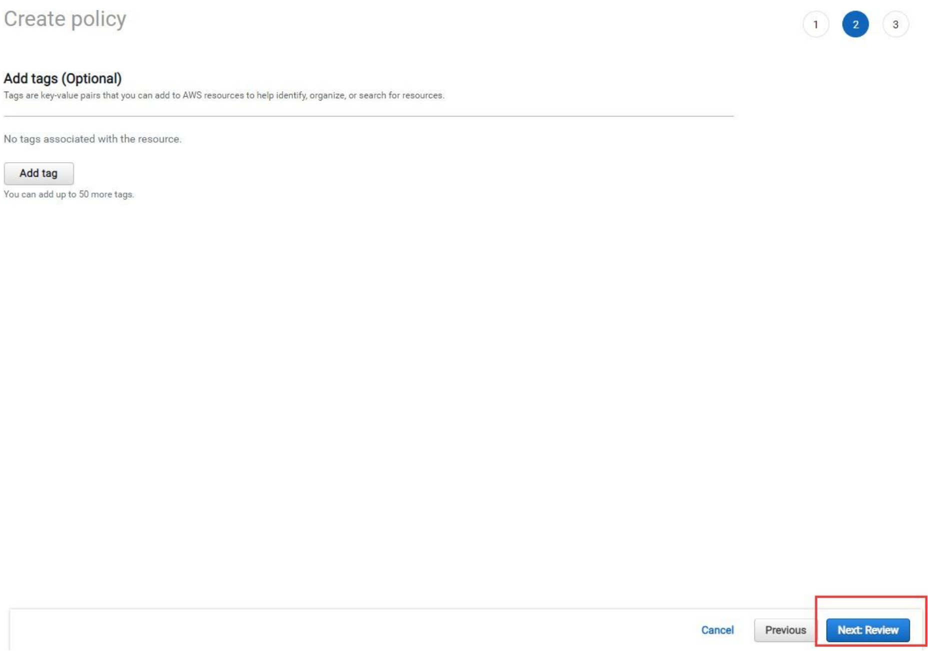


A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeEndpoint",
                "iot:Publish"
            ],
            "Resource": "*"
        }
    ]
}
```

Character count: 120 of 6,144.

Then click “Next: Review”.



Create policy

1 2 3

Add tags (Optional)

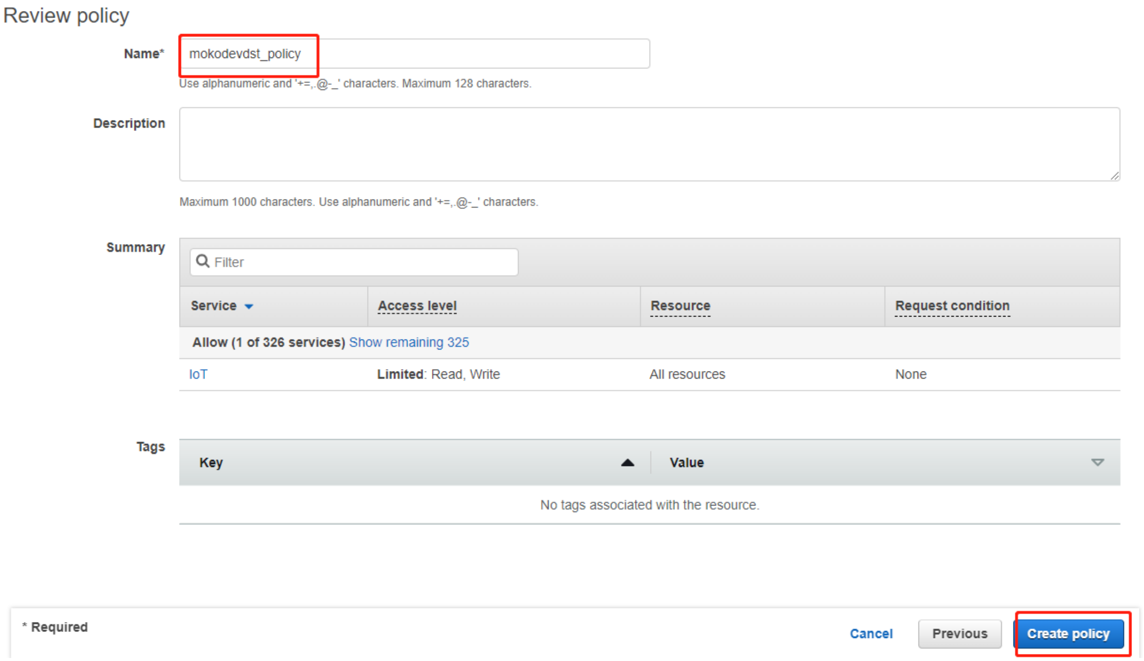
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Step 2: Enter then click “Create policy”.



Review policy

Name* mokodevdst_policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

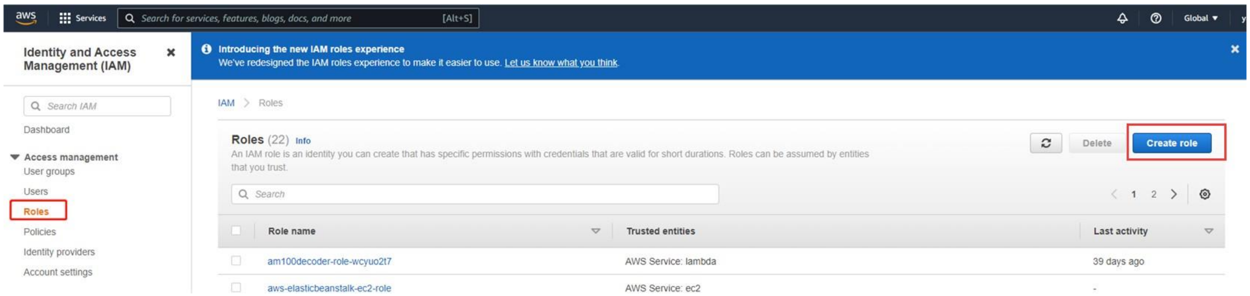
Service	Access level	Resource	Request condition
Allow (1 of 326 services) Show remaining 325			
IoT	**Limited**: Read, Write	All resources	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Step 3: Turn to Roles page, then click “Create role”.



Identity and Access Management (IAM)

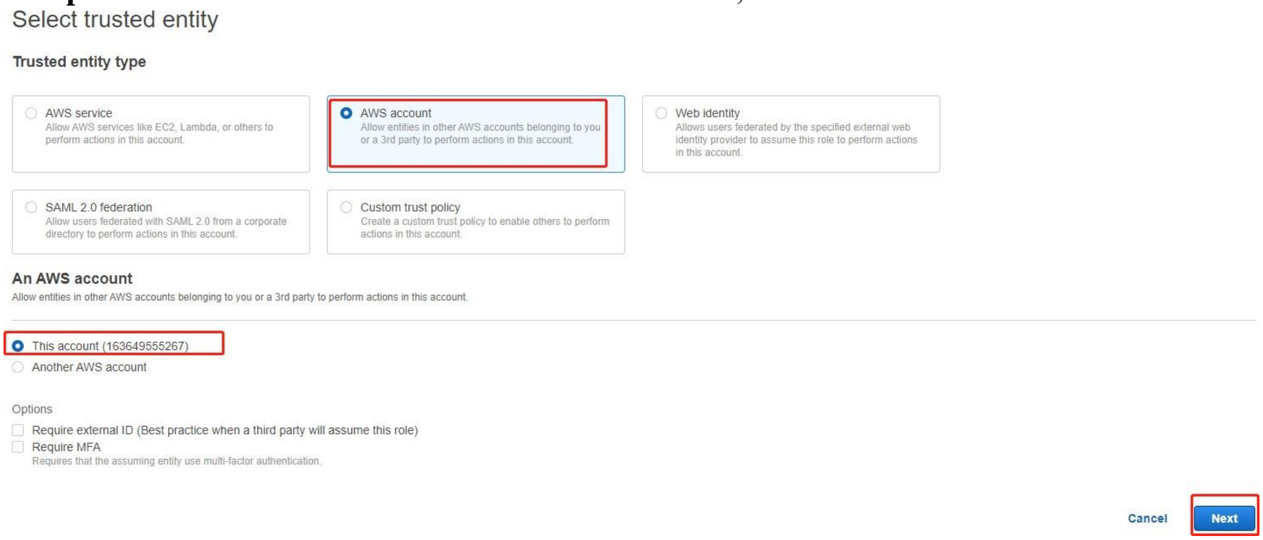
Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

IAM > Roles

Roles (22) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	am100decoder-role-wcyuo2t7	AWS Service: lambda	39 days ago
□	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	-

Step 4: Then select “AWS account” and “This account”, then click “Next”.



Select trusted entity

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

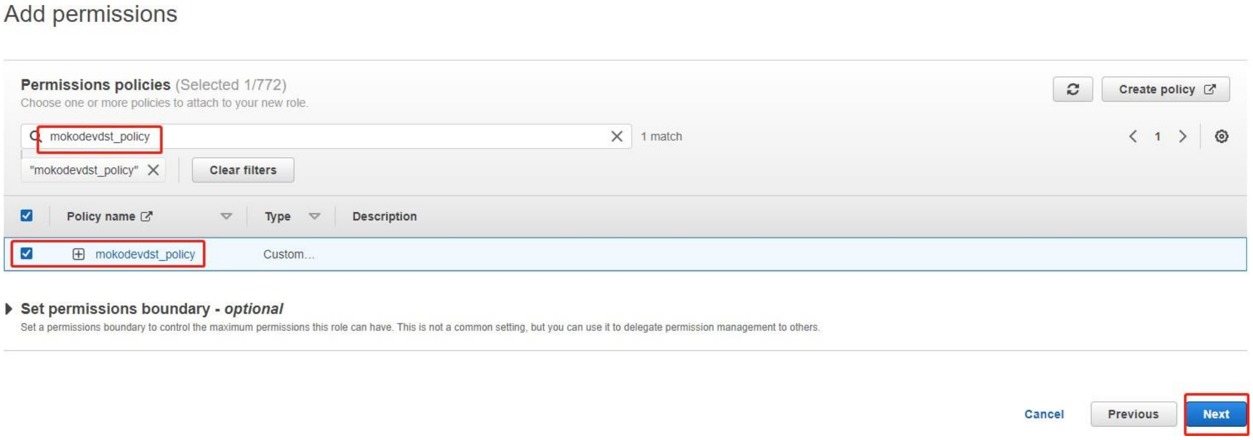
○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

● This account (163649555267)
○ Another AWS account

Options
□ Require external ID (Best practice when a third party will assume this role)
□ Require MFA
Requires that the assuming entity use multi-factor authentication.

Step 5: Search check it on the result box and click “Next”.



Add permissions

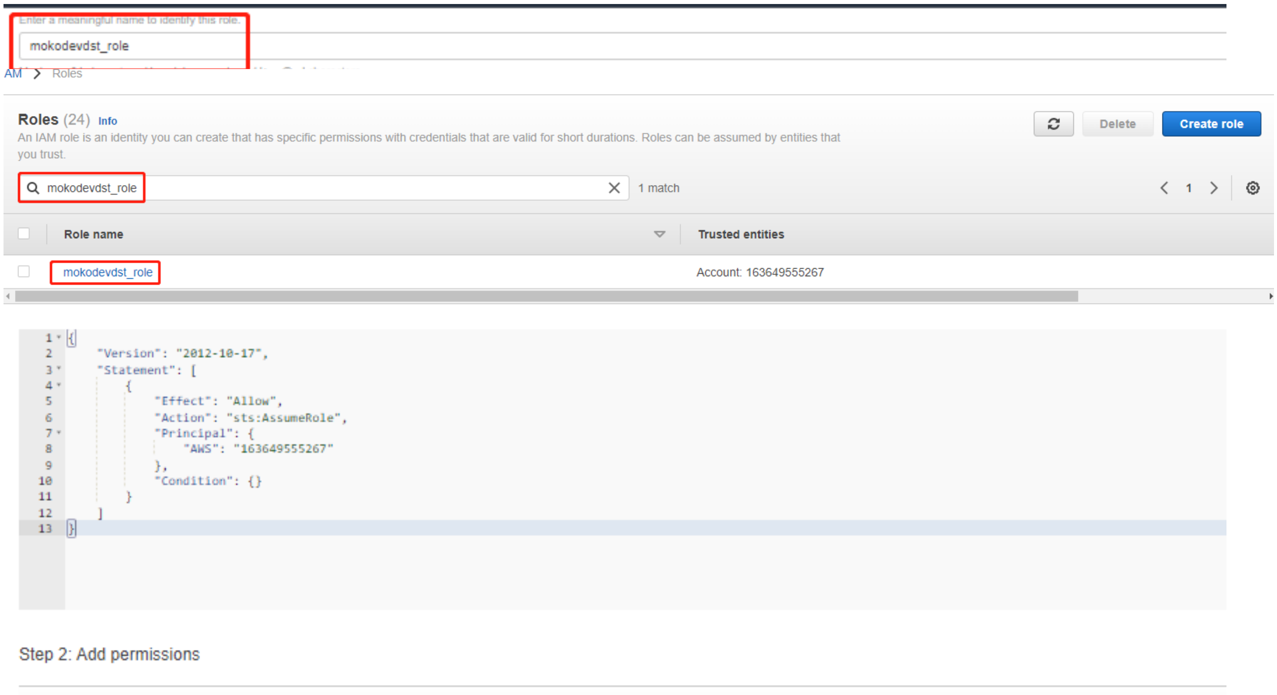
Permissions policies (Selected 1/772)
Choose one or more policies to attach to your new role.

mokodevdst_policy
1 match
"mokodevdst_policy"

☑	Policy name	Type	Description
☑	mokodevdst_policy	Custom...	

Set permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Step 6: Enter name box, then click "Create role" on the bottom of page.



Enter a meaningful name to identify this role.

mokodevdst_role

Roles (24) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

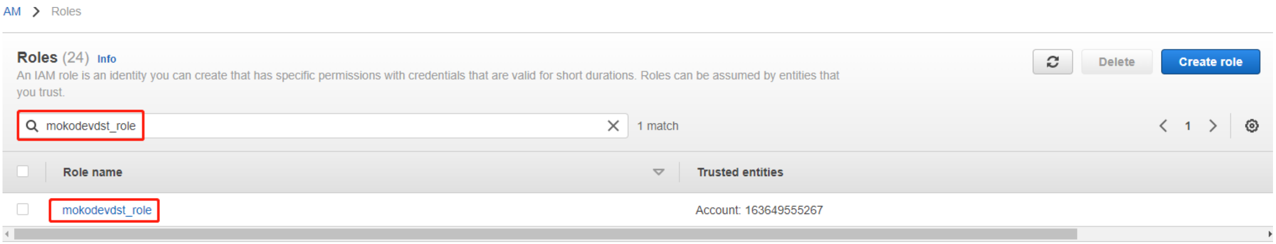
mokodevdst_role ✕ 1 match

□	Role name	Trusted entities
□	mokodevdst_role	Account: 163649555267

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": "163649555267"
            },
            "Condition": {}
        }
    ]
}
```

Step 2: Add permissions

Step 7: Search on filter box, then click it in result box, then edit trust policy.

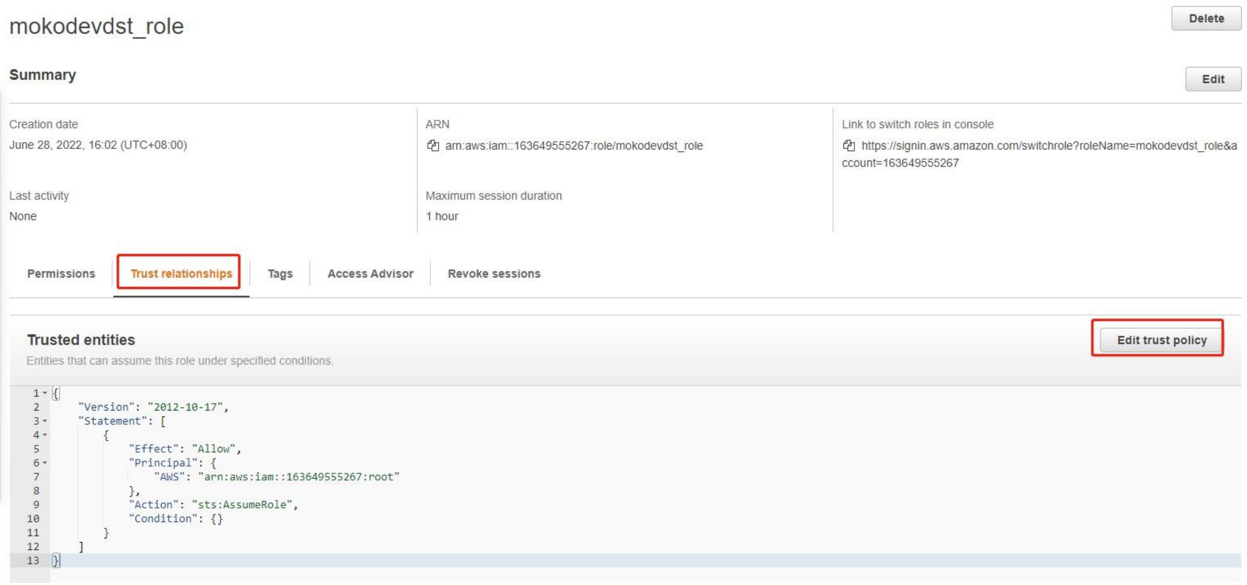


Roles (24) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

mokodevdst_role ✕ 1 match

□	Role name	Trusted entities
□	mokodevdst_role	Account: 163649555267



mokodevdst_role

Summary

Creation date
June 28, 2022, 16:02 (UTC+08:00)

ARN
arn:aws:iam::163649555267:role/mokodevdst_role

Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=mokodevdst_role&account=163649555267

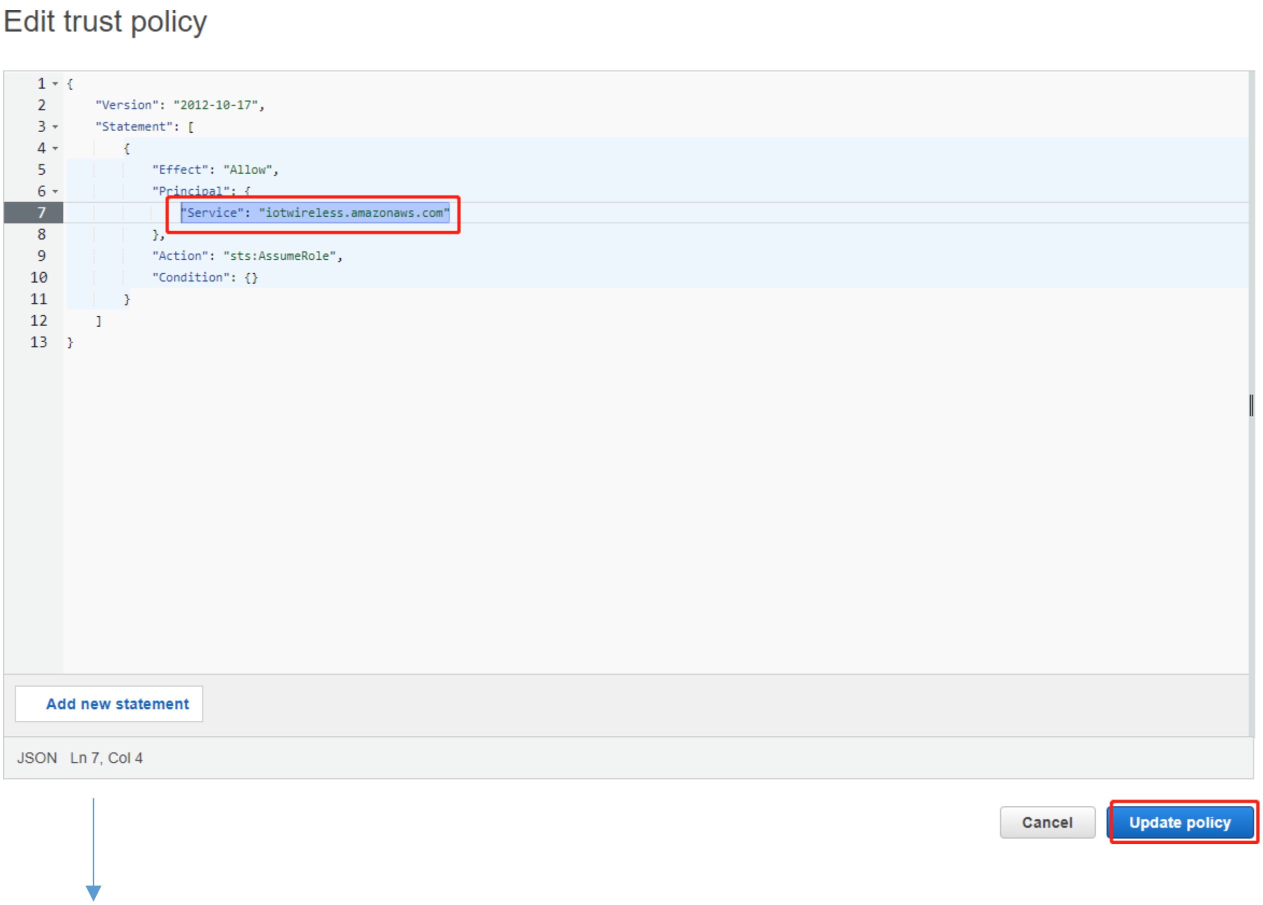
Last activity
None

Maximum session duration
1 hour

Trusted entities

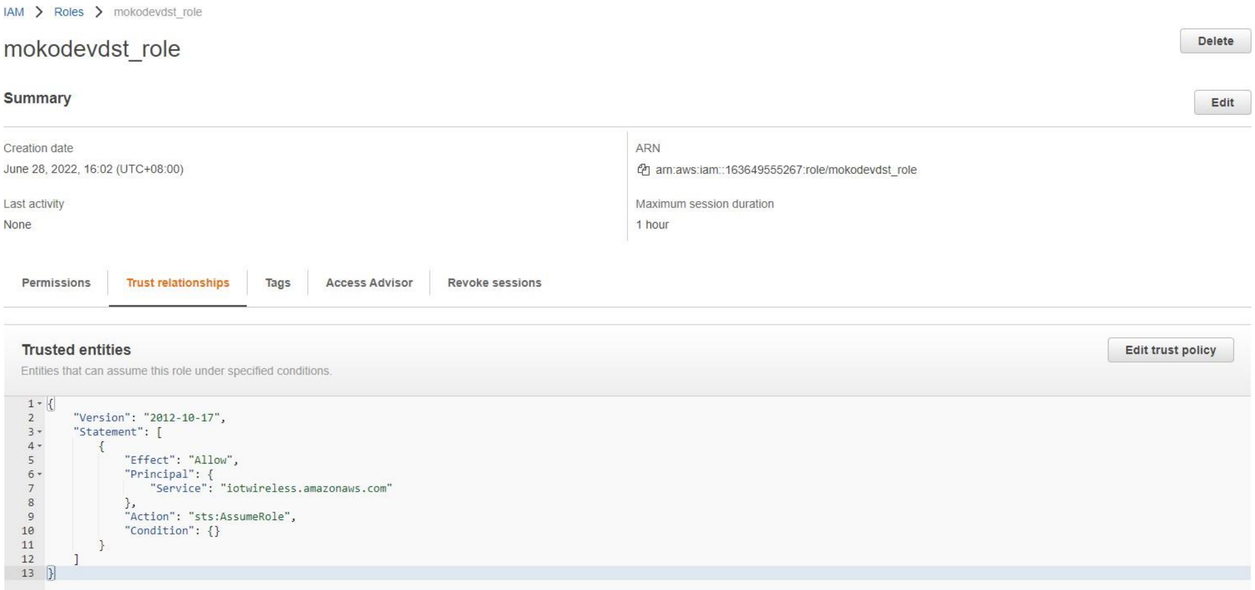
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::163649555267:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```



Edit trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotwireless.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```



IAM > Roles > mokodevdst_role

mokodevdst_role

Summary

Creation date
June 28, 2022, 16:02 (UTC+08:00)

ARN
arn:aws:iam::163649555267:role/mokodevdst_role

Last activity
None

Maximum session duration
1 hour

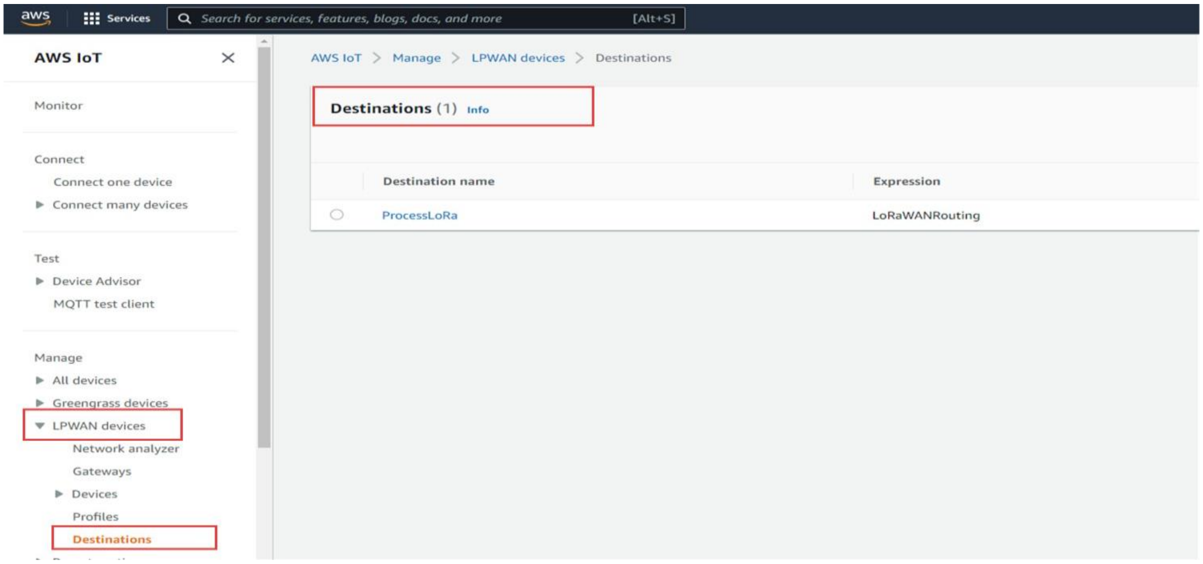
Trusted entities
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotwireless.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Part 5: Configure Destination of AWS Core (Optional)

Note: The destination is created to make it easier for customers to view data on AWS. Ifyou are familiar with AWS server, don't need to follow this part.

Step 1: Go to AWS console, and select IoT Core. Then go to Destinations page.

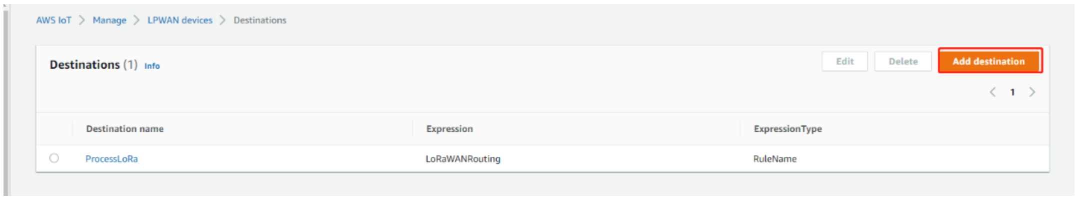


AWS IoT > Manage > LPWAN devices > Destinations

Destinations (1) Info

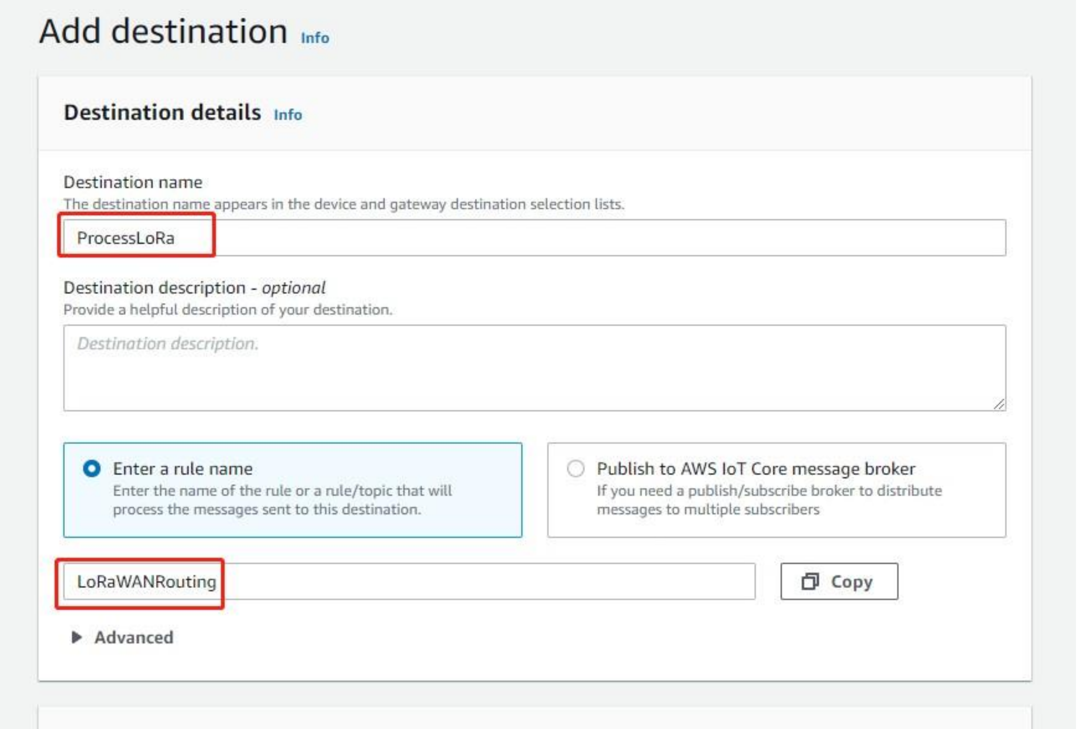
	Destination name	Expression
○	ProcessLoRa	LoRaWANRouting

Step 2: Click “Add destination”. On the next page, enter on destination name box and enter on rule name box, then select on role selectionbox, then click “Add destination” on the bottom of page.



Destinations (1) Info

	Destination name	Expression	ExpressionType
○	ProcessLoRa	LoRaWANRouting	RuleName



Add destination Info

Destination details Info

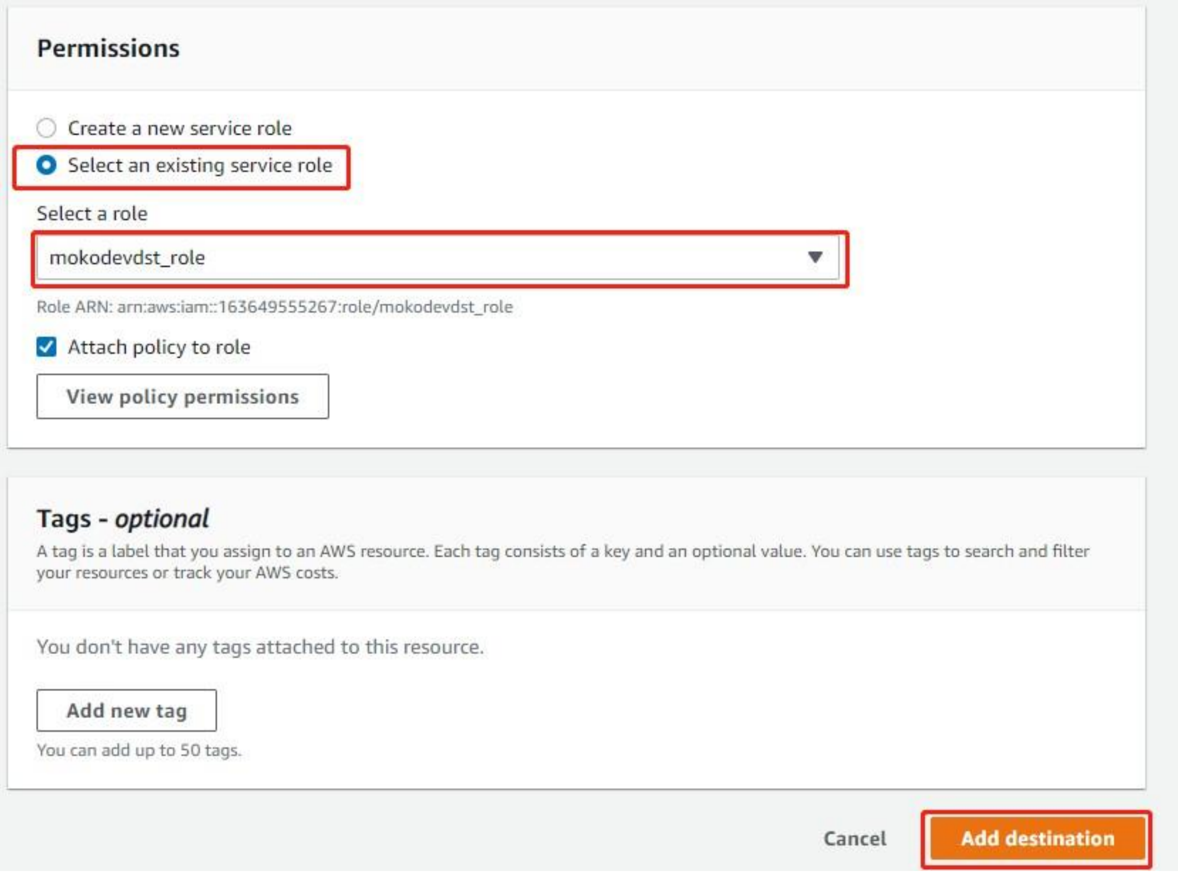
Destination name
The destination name appears in the device and gateway destination selection lists.
ProcessLoRa

Destination description - *optional*
Provide a helpful description of your destination.
Destination description.

● Enter a rule name
Enter the name of the rule or a rule/topic that will process the messages sent to this destination.

○ Publish to AWS IoT Core message broker
If you need a publish/subscribe broker to distribute messages to multiple subscribers

LoRaWANRouting



Permissions

○ Create a new service role

● Select an existing service role

Select a role

mokodevdst_role ▼

Role ARN: arn:aws:iam::163649555267:role/mokodevdst_role

☑ Attach policy to role

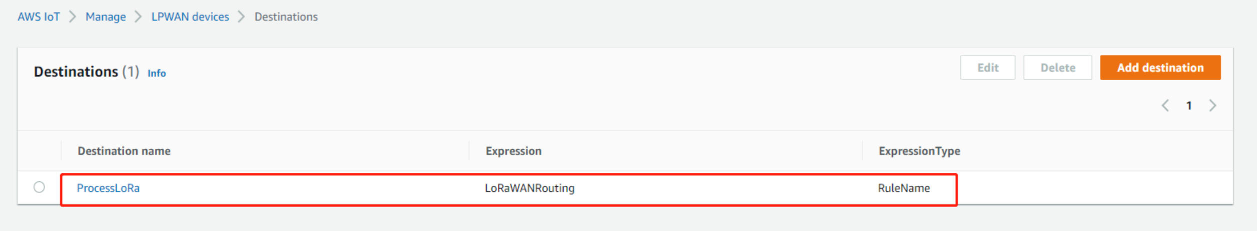
Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

You don't have any tags attached to this resource.

You can add up to 50 tags.

Step 3: Check the destination that you added on Destinations page.



AWS IoT > Manage > LPWAN devices > Destinations

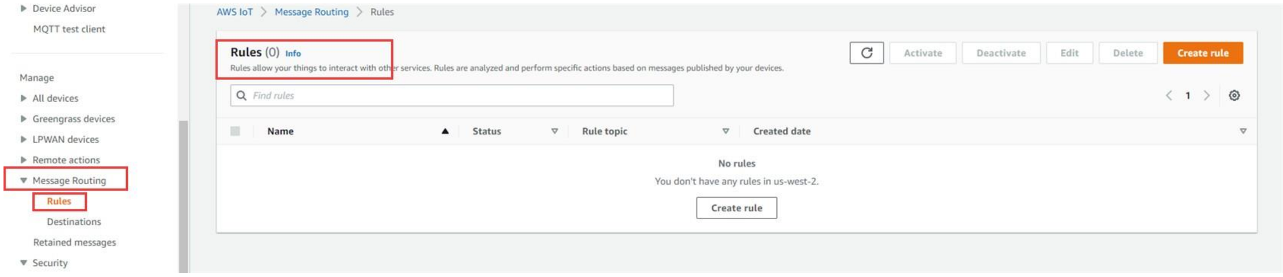
Destinations (1) Info

	Destination name	Expression	ExpressionType
○	ProcessLoRa	LoRaWANRouting	RuleName

Part 6: Configure Message Rule for Destination (Optional)

Note: The destination is created to make it easier for customers to view data on AWS. Ifyou are familiar with AWS server, don’t need to follow this part.

Step 1: Go to AWS console, and select IoT Core. Then go to Rules page.



▶ Device Advisor
MQTT test client

Manage
▶ All devices
▶ Greengrass devices
▶ LPWAN devices
▶ Remote actions
▼ Message Routing
Rules
Destinations
Retained messages
▼ Security

AWS IoT > Message Routing > Rules

Rules (0) Info
Rules allow your things to interact with other services. Rules are analyzed and perform specific actions based on messages published by your devices.

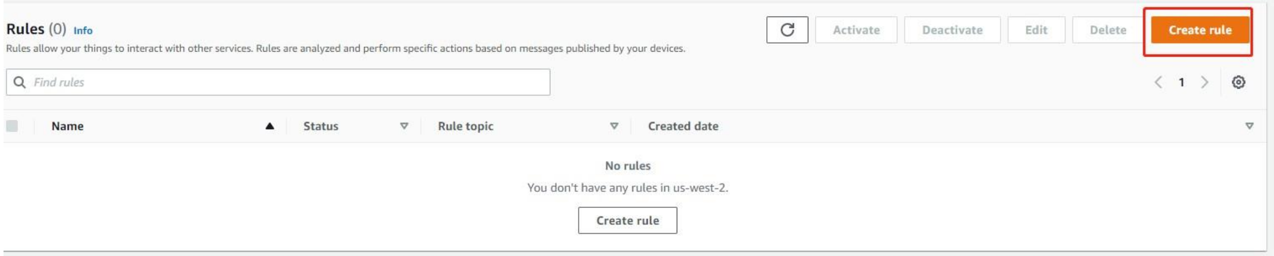
Activate | Deactivate | Edit | Delete | Create rule

Find rules

Name	Status	Rule topic	Created date

No rules
You don't have any rules in us-west-2.
Create rule

Step 2: Click "Create rule".



Rules (0) Info
Rules allow your things to interact with other services. Rules are analyzed and perform specific actions based on messages published by your devices.

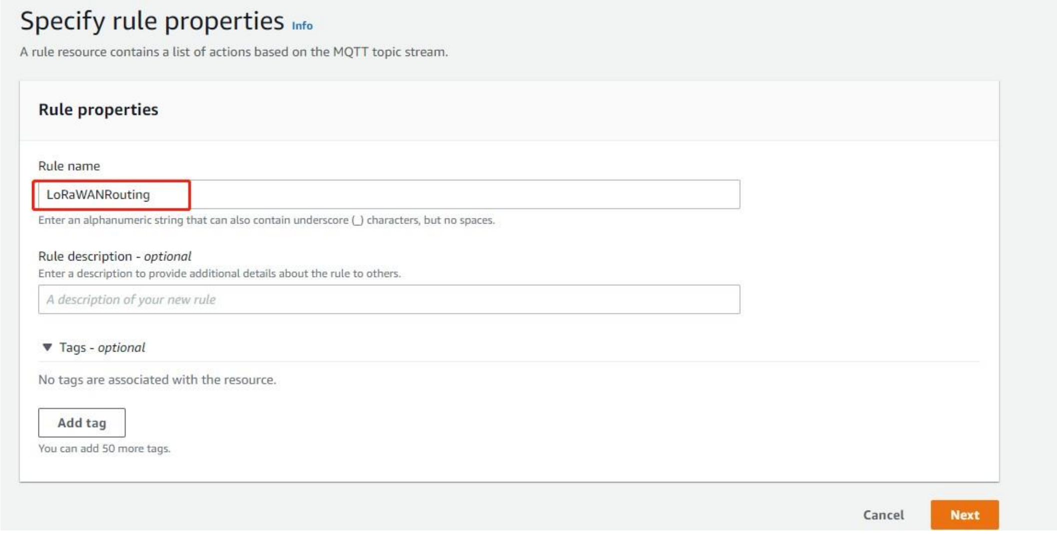
Activate | Deactivate | Edit | Delete | Create rule

Find rules

Name	Status	Rule topic	Created date

No rules
You don't have any rules in us-west-2.
Create rule

Step 3: Enter on rule name box. Then click "Next".



Specify rule properties Info
A rule resource contains a list of actions based on the MQTT topic stream.

Rule properties

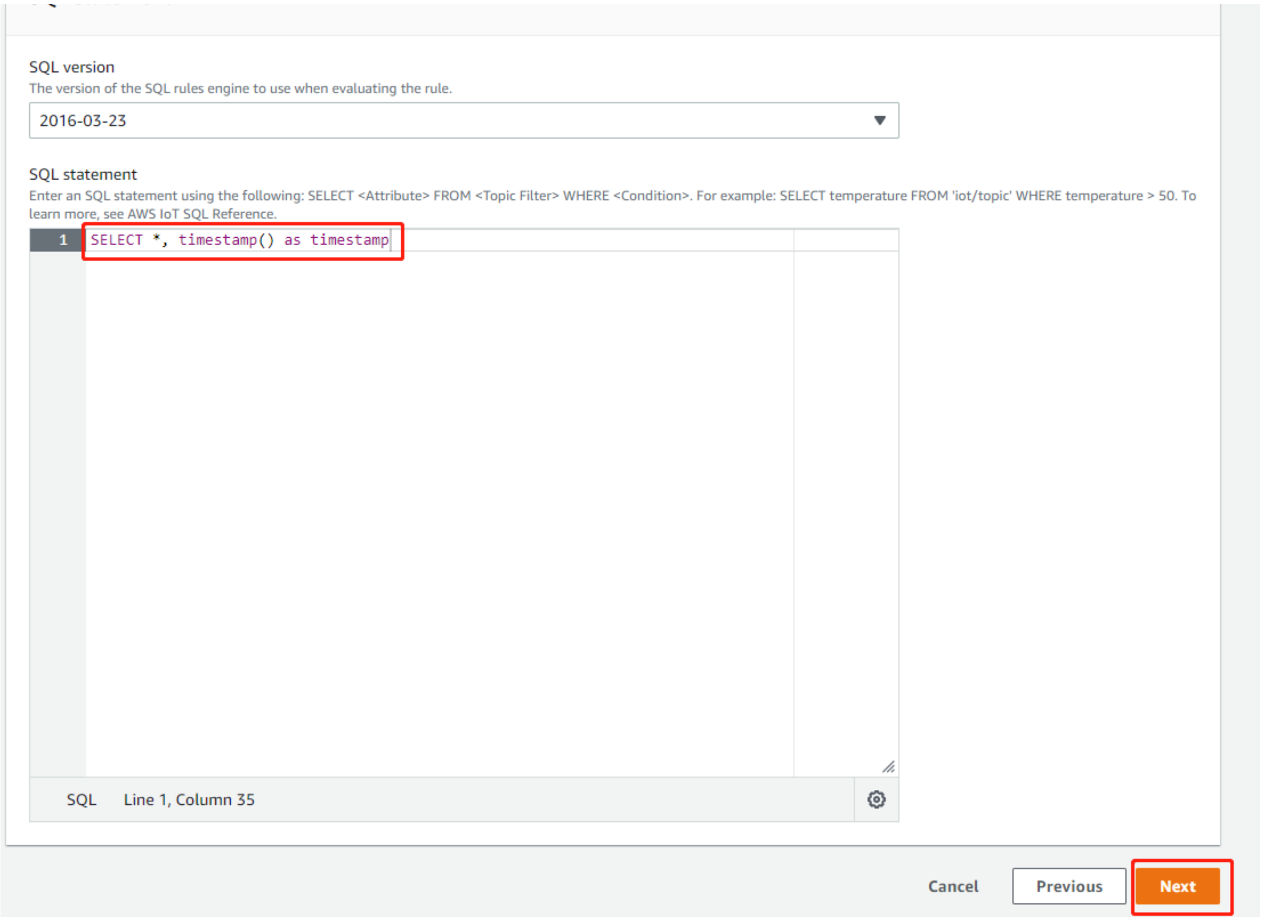
Rule name
LoRaWANRouting
Enter an alphanumeric string that can also contain underscore (_) characters, but no spaces.

Rule description - *optional*
Enter a description to provide additional details about the rule to others.
A description of your new rule

▼ Tags - *optional*
No tags are associated with the resource.
Add tag
You can add 50 more tags.

Cancel | Next

Step 4: Enter “SELECT *, timestamp () as timestamp” in SQL statement, then click “Next”.



SQL version

The version of the SQL rules engine to use when evaluating the rule.

2016-03-23

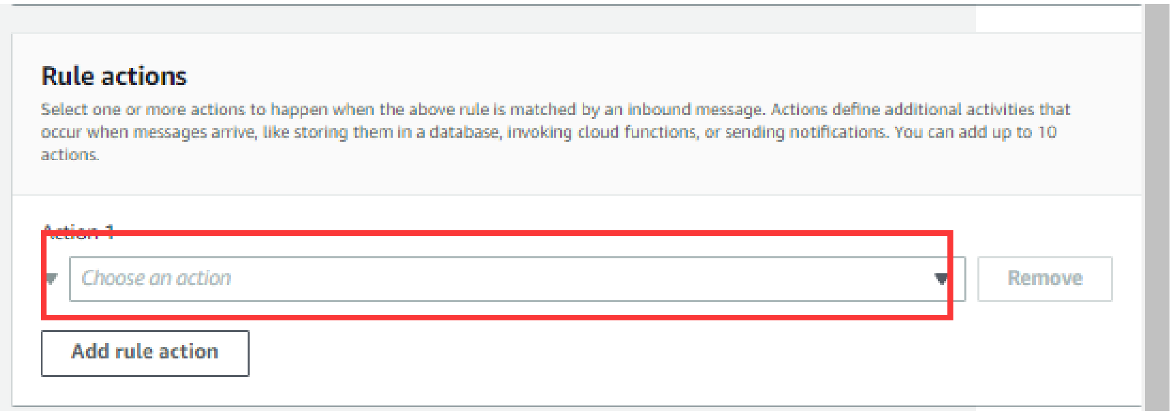
SQL statement

Enter an SQL statement using the following: SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see AWS IoT SQL Reference.

```
SELECT *, timestamp() as timestamp
```

SQL Line 1, Column 35

Step 5: Select “Republish to AWS IoT topic” on action box.



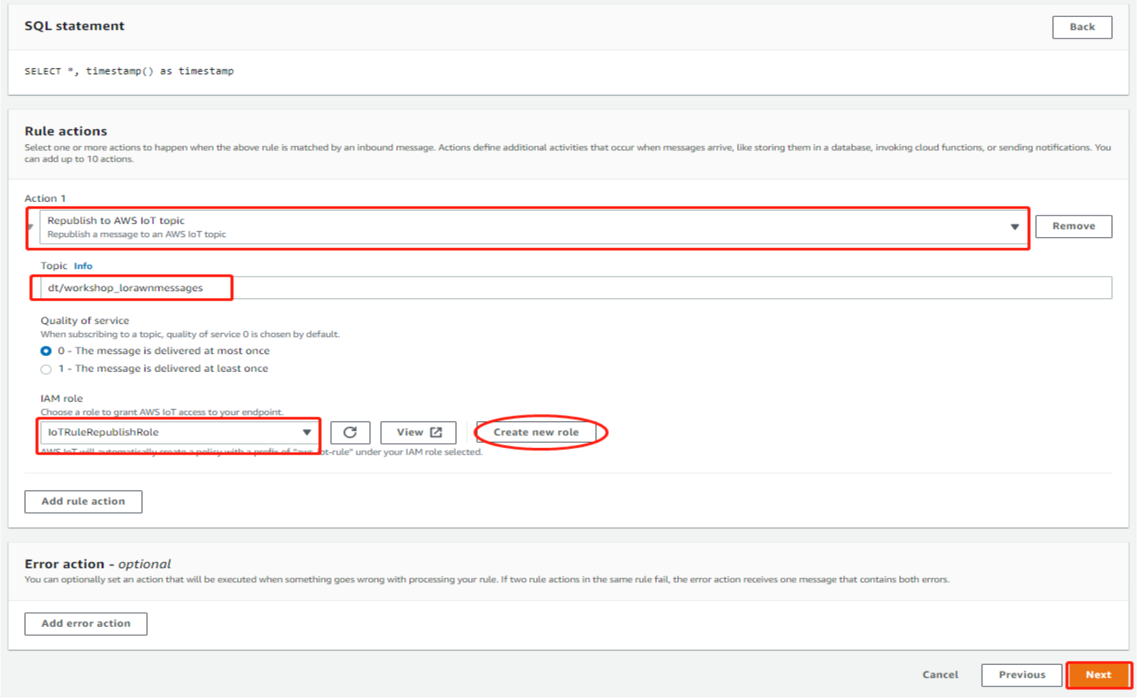
Rule actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. You can add up to 10 actions.

Action 1

Step 6: Enter in topic box.
Select “IoT Rule Republish Role” on IMA role choose item, then click “Next”.

If there isn’t “IoT Rule Republish Role” on IMA role choose item, please turn to Step 6.



SQL statement

```
SELECT *, timestamp() as timestamp
```

Rule actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. You can add up to 10 actions.

Action 1: Republish to AWS IoT topic — Republish a message to an AWS IoT topic

Topic: dt/workshop_lorawnmessages

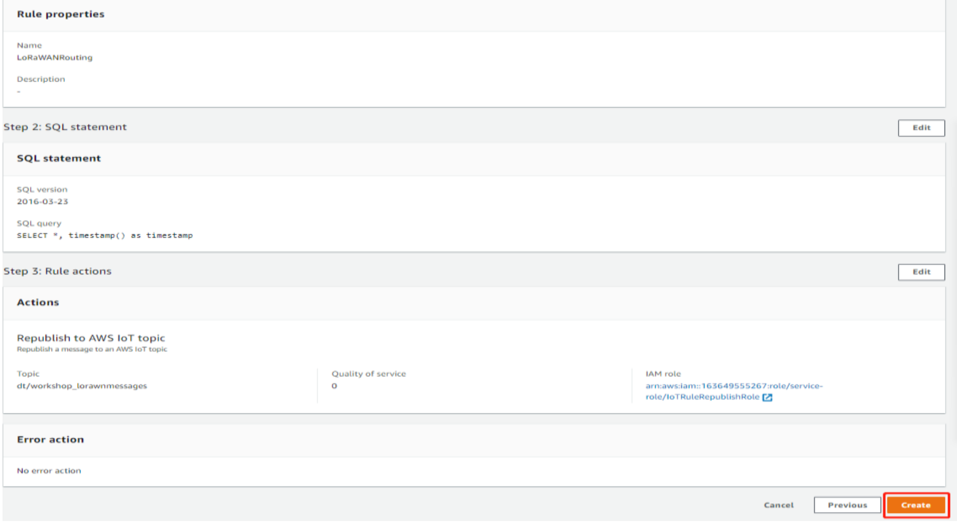
Quality of service
When subscribing to a topic, quality of service 0 is chosen by default.
● 0 - The message is delivered at most once
○ 1 - The message is delivered at least once

IAM role
Choose a role to grant AWS IoT access to your endpoint.
IoTRuleRepublishRole
AWS IoT will automatically create a policy with a prefix of "aws-iot-rule" under your IAM role selected.

Error action - *optional*

You can optionally set an action that will be executed when something goes wrong with processing your rule. If two rule actions in the same rule fail, the error action receives one message that contains both errors.

Then, click “Create” and finished.



Rule properties

Name
LoRaWANRouting

Description
-

Step 2: SQL statement

SQL statement

SQL version
2016-03-23

SQL query
```
SELECT *, timestamp() as timestamp
```

Step 3: Rule actions

Actions

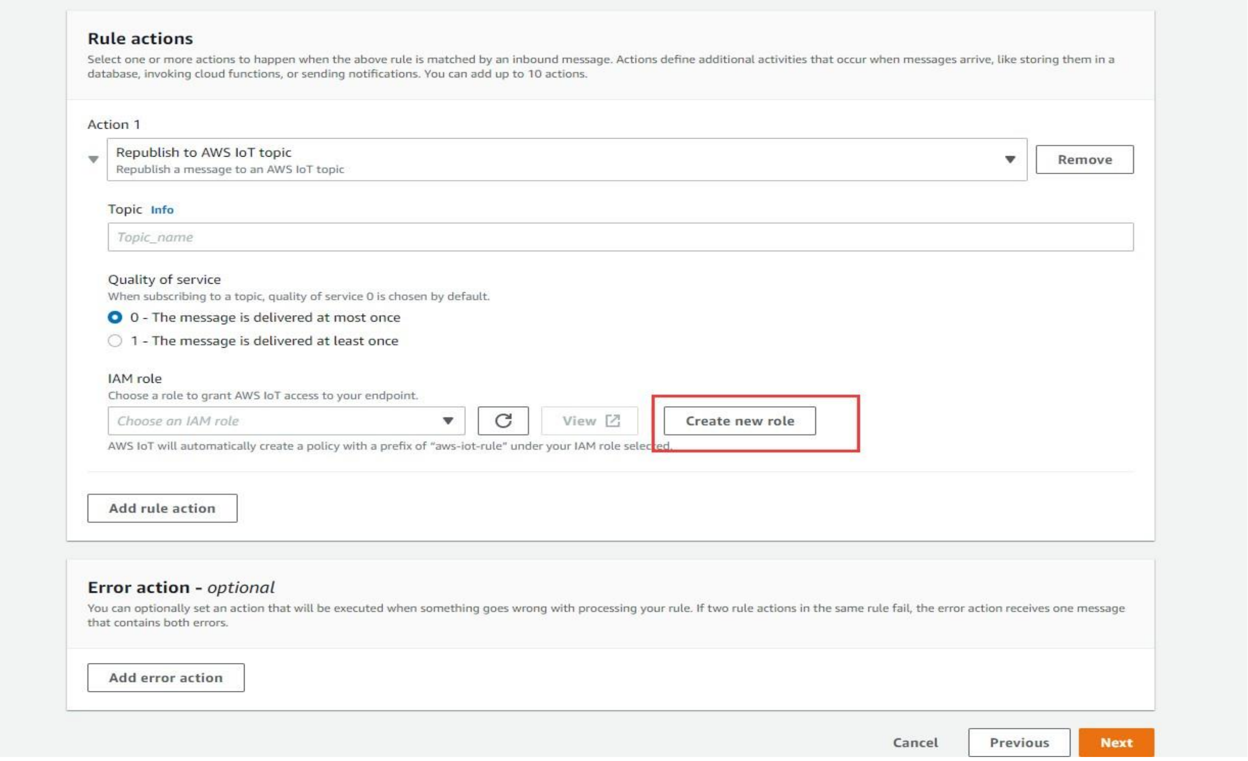
Republish to AWS IoT topic
Republish a message to an AWS IoT topic

Topic	Quality of service	IAM role
dt/workshop_lorawnmessages	0	arn:aws:iam::163649555267:role/service-role/IoTRuleRepublishRole

Error action

No error action

Step 7: Click “Create new role”,



Rule actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. You can add up to 10 actions.

Action 1

Republish to AWS IoT topic
Republish a message to an AWS IoT topic

Topic Info

Topic_name

Quality of service
When subscribing to a topic, quality of service 0 is chosen by default.

● 0 - The message is delivered at most once

○ 1 - The message is delivered at least once

IAM role
Choose a role to grant AWS IoT access to your endpoint.

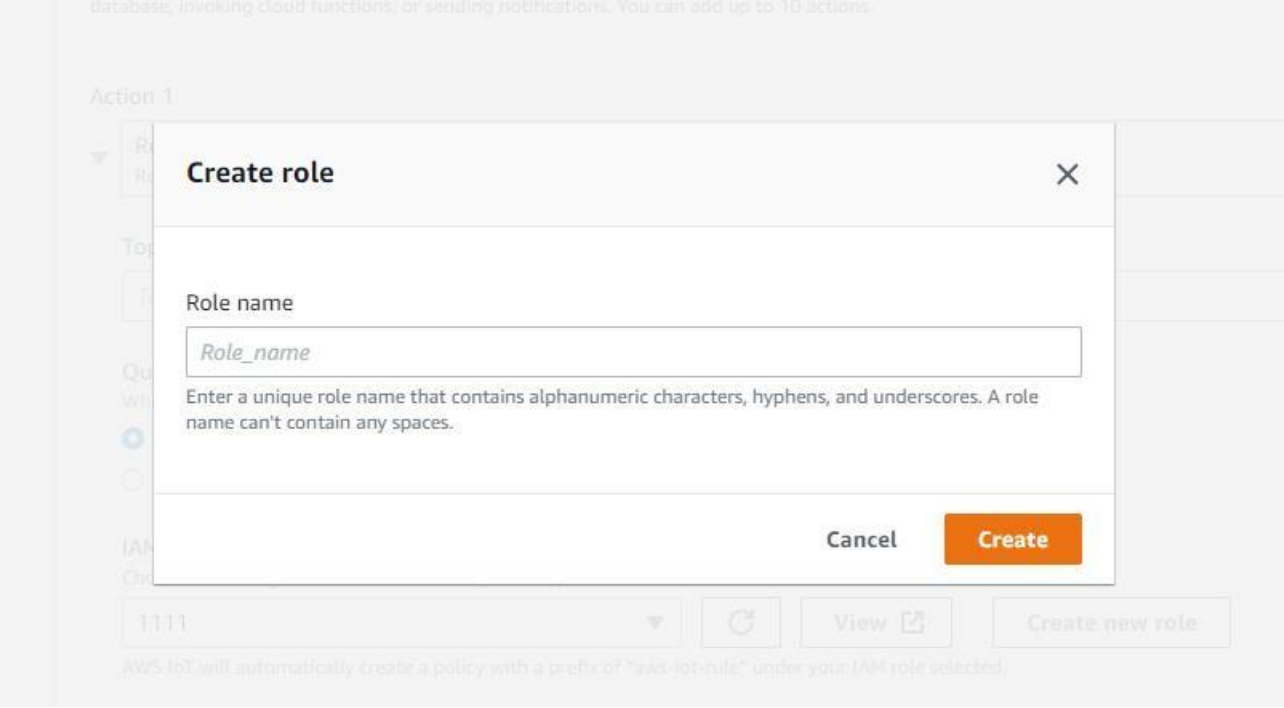
Choose an IAM role

AWS IoT will automatically create a policy with a prefix of “aws-iot-rule” under your IAM role selected.

Error action - *optional*

You can optionally set an action that will be executed when something goes wrong with processing your rule. If two rule actions in the same rule fail, the error action receives one message that contains both errors.

Then enter “IoT Rule Republish Role” in Role name box and click “Create”. Then back to Step 5.



database, invoking cloud functions, or sending notifications. You can add up to 10 actions.

Action 1

Create role

Role name

Role_name

Enter a unique role name that contains alphanumeric characters, hyphens, and underscores. A role name can't contain any spaces.

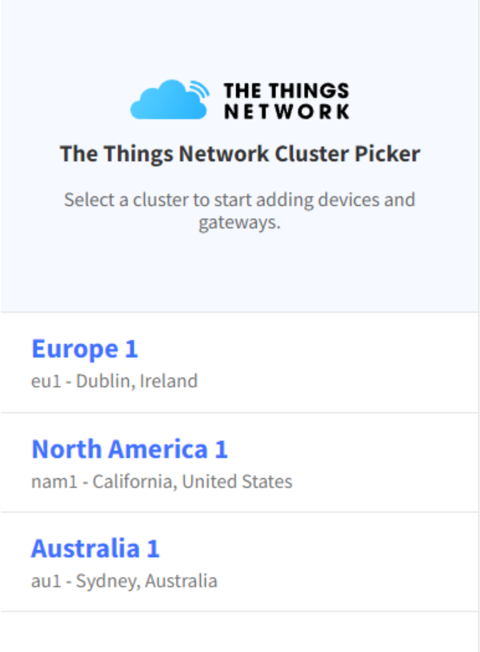
1111

AWS IoT will automatically create a policy with a prefix of "aws-iot-rule" under your IAM role selected.

TTN platform Configuration Example

Step 1: Power access to Web GUI, get the gateway ID on *FUNCTAION-ServerAccess* page of Web GUI.

Step 2: Prepare an TTN account, then login in TTN platform and click the corresponding Cluster thatyou want to use. I will use EU868 as example, so Europe 1 cluster will be my choice.



THE THINGS NETWORK

The Things Network Cluster Picker

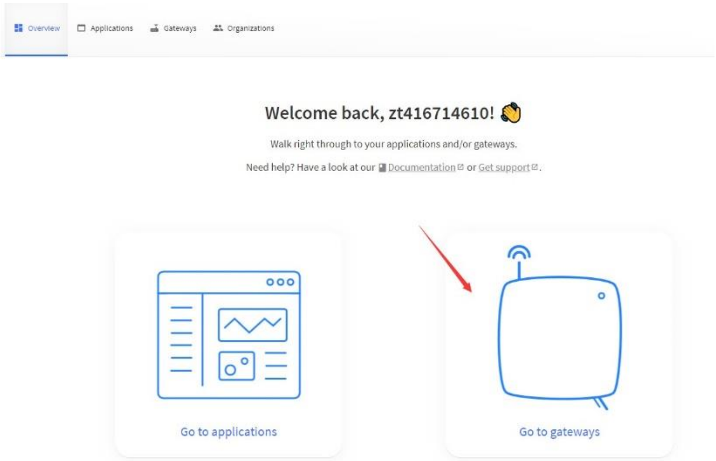
Select a cluster to start adding devices and gateways.

Europe 1
eu1 - Dublin, Ireland

North America 1
nam1 - California, United States

Australia 1
au1 - Sydney, Australia

Step 3: Go to gateway console on home page after you login in successfully.

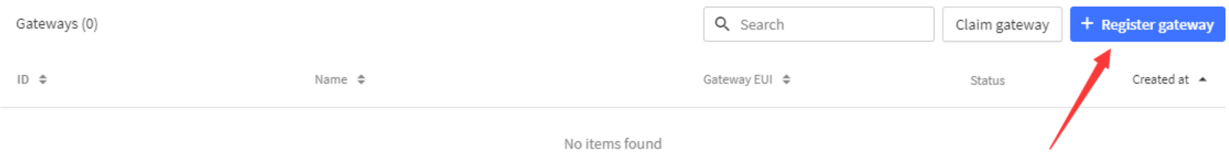


Welcome back, zt416714610! 👋

Walk right through to your applications and/or gateways.

Need help? Have a look at our Documentation or Get support.

Step 4: Register a new gateway

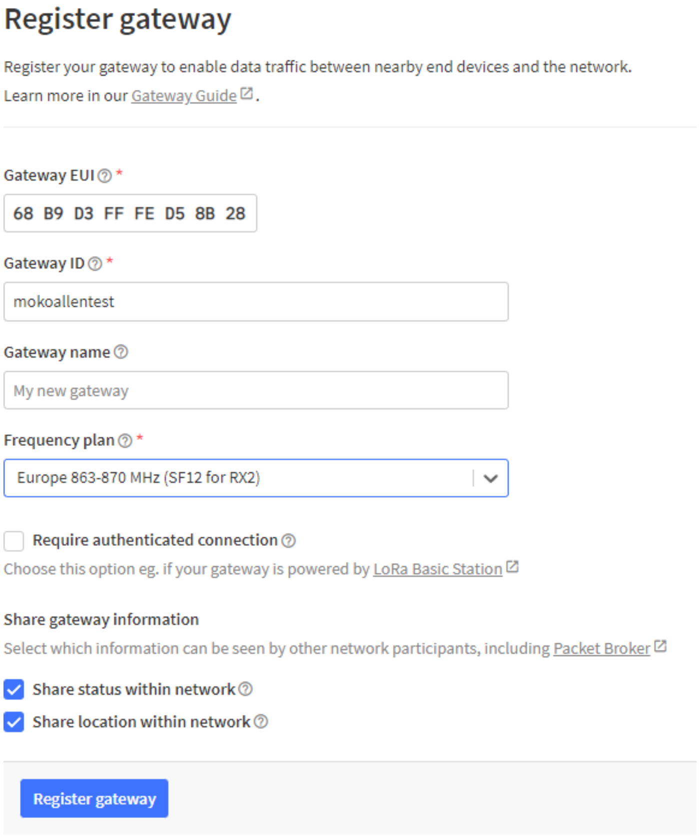


Gateways (0)

Search | Claim gateway | + Register gateway

ID	Name	Gateway EUI	Status	Created at

No items found



Register gateway

Register your gateway to enable data traffic between nearby end devices and the network. Learn more in our Gateway Guide.

Gateway EUI *
68 B9 D3 FF FE D5 8B 28

Gateway ID *
mokoallentest

Gateway name
My new gateway

Frequency plan *
Europe 863-870 MHz (SF12 for RX2)

□ Require authenticated connection
Choose this option eg. if your gateway is powered by LoRa Basic Station

Share gateway information
Select which information can be seen by other network participants, including Packet Broker

☑ Share status within network
☑ Share location within network

Register gateway

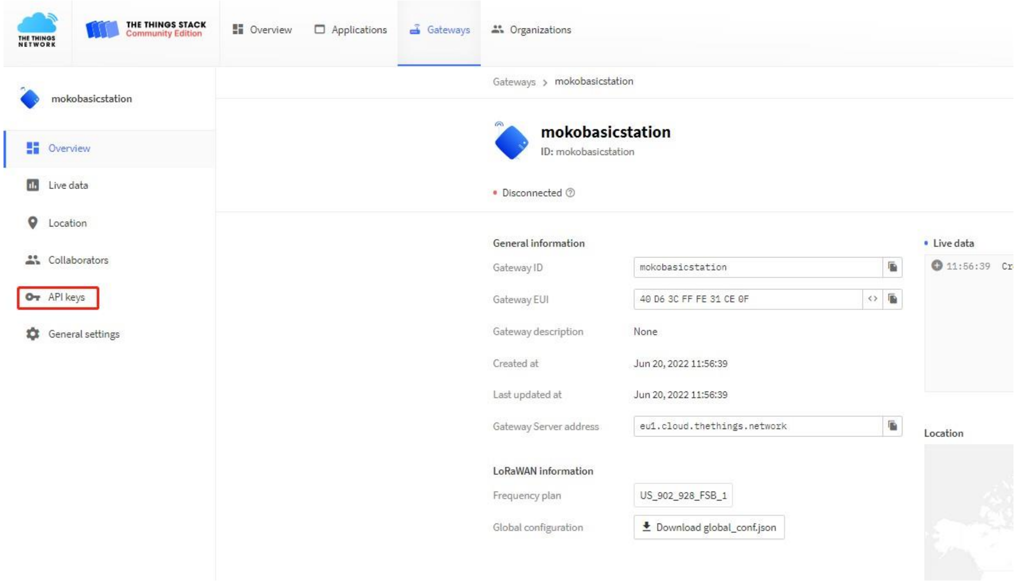
1. ill in Gateway EUI with the mkgw2-law’s gateway id which have been got inStep 1.

2. Customize a TTN gateway id and fillin.

3. Select the EU868 in Frequency Plan.

4. Click “Register gateway”.

Step 5: Click “API keys”,



Gateways > mokobasicstation

mokobasicstation
ID: mokobasicstation

• Disconnected

General information

Gateway ID: mokobasicstation

Gateway EUI: 40 D6 3C FF FE 31 CE 0F

Gateway description: None

Created at: Jun 20, 2022 11:56:39

Last updated at: Jun 20, 2022 11:56:39

Gateway Server address: eu1.cloud.thethings.network

LoRaWAN information

Frequency plan: US_902_928_FSB_1

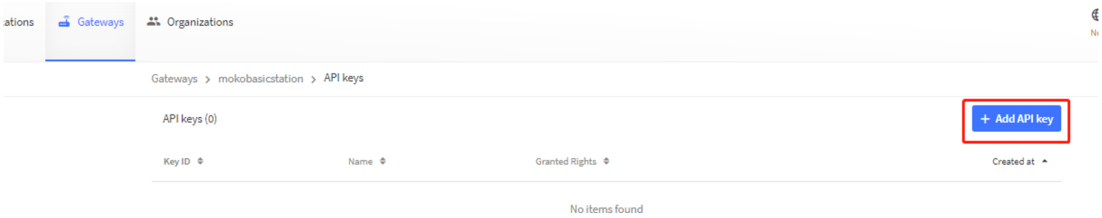
Global configuration: Download global_conf.json

• Live data

11:56:39 Cr

Location

Click “Add API key”.

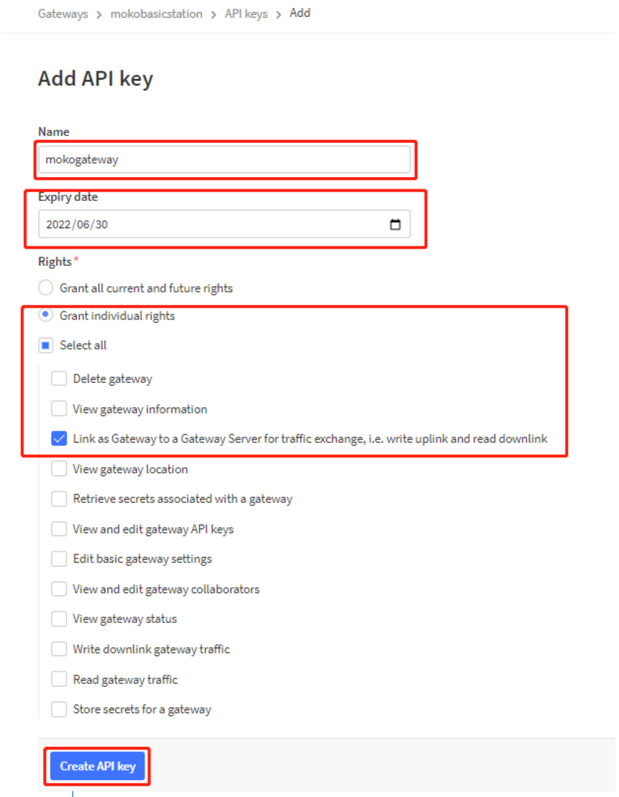


Gateways > mokobasicstation > API keys

API keys (0)

Key ID	Name	Granted Rights	Created at

No items found



Gateways > mokobasicstation > API keys > Add

Add API key

Name: mokogateway

Expiry date: 2022/06/30

Rights *

○ Grant all current and future rights

● Grant individual rights

■ Select all

□ Delete gateway

□ View gateway information

☑ Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink

□ View gateway location

□ Retrieve secrets associated with a gateway

□ View and edit gateway API keys

□ Edit basic gateway settings

□ View and edit gateway collaborators

□ View gateway status

□ Write downlink gateway traffic

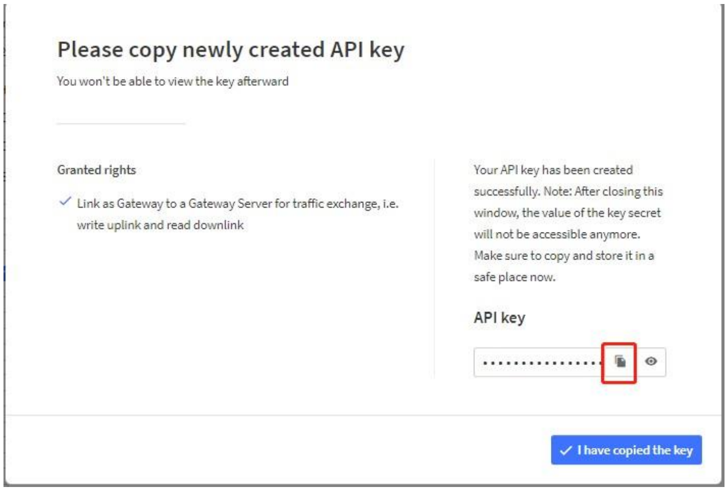
□ Read gateway traffic

□ Store secrets for a gateway

1. Fill the name and expiry data.

2. Check “Grant individual rights” and select“Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink”.

3. Click “Create API key”.



Please copy newly created API key

You won't be able to view the key afterward

Granted rights

✓ Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink

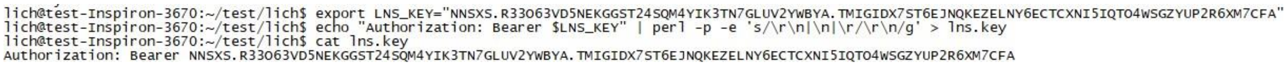
Your API key has been created successfully. Note: After closing this window, the value of the key secret will not be accessible anymore. Make sure to copy and store it in a safe place now.

API key: ················

Copy the “API key”.

Step 6: In Linux system, set LNS_KEY equal to the API key copied on Step 5.Linux cmd as following:

export LNS_KEY="XXXXXX"
echo "Authorization: Bearer $LNS_KEY" | Perl -p -e 's/\r\n|\n|\r/\r\n/g' > ins.
keycat ins. key



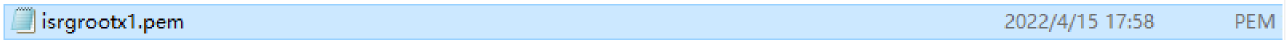
```
lich@test-Inspiron-3670:~/test/lich$ export LNS_KEY="NNSXS.R33O63VD5NEKGGST24SQM4YIK3TN7GLUV2YWBYA.TMIGIDX7ST6EJNQKEZELNY6ECTCXNI5IQTO4WSGZYUP2R6XM7CFA"
lich@test-Inspiron-3670:~/test/lich$ echo "Authorization: Bearer $LNS_KEY" | perl -p -e 's/\r\n|\n|\r/\r\n/g' > lns.key
lich@test-Inspiron-3670:~/test/lich$ cat lns.key
Authorization: Bearer NNSXS.R33O63VD5NEKGGST24SQM4YIK3TN7GLUV2YWBYA.TMIGIDX7ST6EJNQKEZELNY6ECTCXNI5IQTO4WSGZYUP2R6XM7CFA
```

Save the ins. key file, it will be used in following steps.

lns.key 2022/6/20 15:56 KEY 文件 1 KB

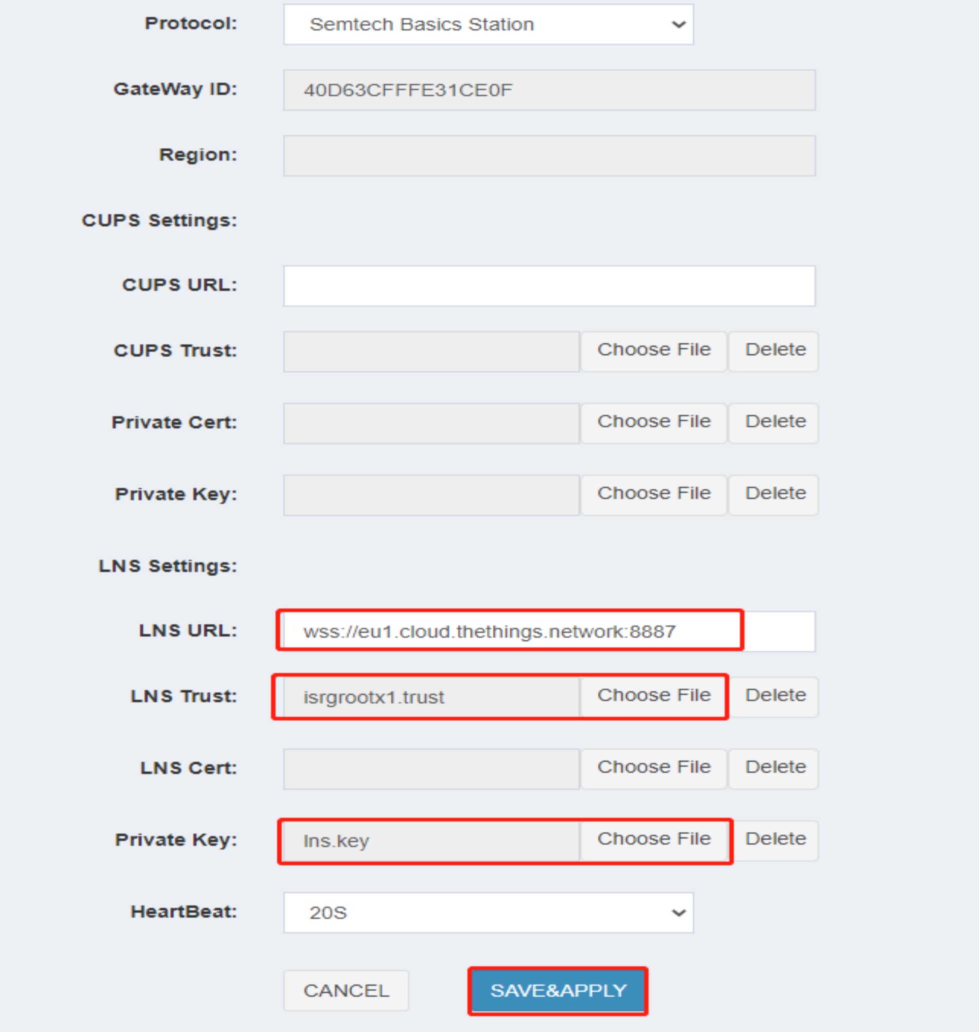
Step 7: Open https://letsencrypt.org/certs/isrgrootx1.pem in browser.

And save the file, it will be used in following steps.



isrgrootx1.pem 2022/4/15 17:58 PEM

Step 8: Access to Web GUI, get the gateway ID on *FUNCTAION-Server Access* page of Web GUI.



Protocol:	Semtech Basics Station
GateWay ID:	40D63CFFFE31CE0F
Region:	
CUPS Settings:	
CUPS URL:	
CUPS Trust:	
Private Cert:	
Private Key:	
LNS Settings:	
LNS URL:	wss://eu1.cloud.thethings.network:8887
LNS Trust:	isrgrootx1.trust
LNS Cert:	
Private Key:	lns.key
HeartBeat:	20S

1. Fill “wss://eu1.cloud.thethings.network:8887”in LNS URL box.

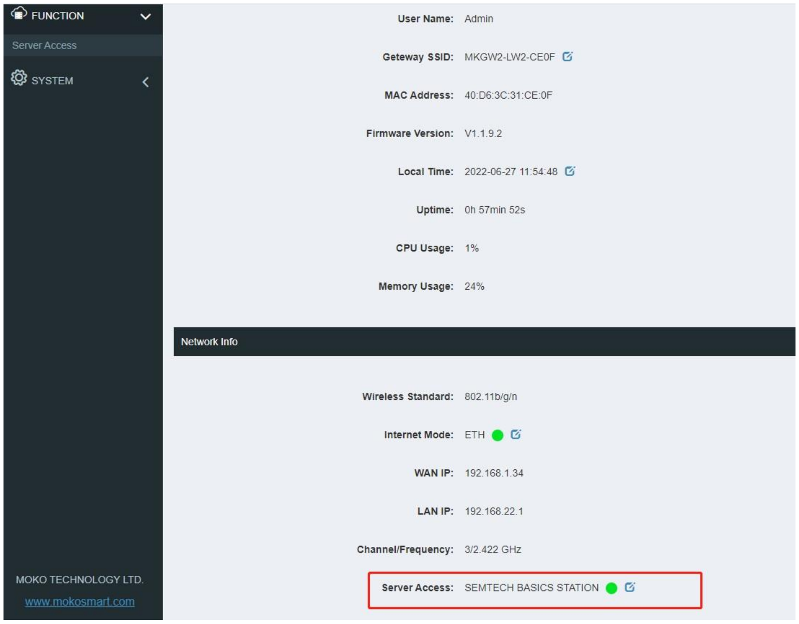
2. Load isrgrootx1.pem file on LNS Trust item.

3. Load ins. key file on Private Key item.

4. Click “SAVE&APPLY”.

Step 9: Check the Server Access status.

If the indicator is green, it means that the gateway had been connected successfully.



User Name: Admin

Geteway SSID: MKGW2-LW2-CE0F

MAC Address: 40:D6:3C:31:CE:0F

Firmware Version: V1.1.9.2

Local Time: 2022-06-27 11:54:48

Uptime: 0h 57min 52s

CPU Usage: 1%

Memory Usage: 24%

Network Info

Wireless Standard: 802.11b/g/n

Internet Mode: ETH ●

WAN IP: 192.168.1.34

LAN IP: 192.168.22.1

Channel/Frequency: 3/2.422 GHz

Server Access: SEMTECH BASICS STATION ●

Appendix 3 Gateway Default Frequency

Frequency	Channel NO.	Uplink Frequency (MHZ)
EU868	0-7	867.1, 867.3, 867.5, 867.7, 867.9, 868.1, 868.3, 868.5
IN865	0-7	865.0625, 865.2625, 865.402, 865.6625, 865.985, 866.185, 866.385, 866.585
US915	0-7,64	902.3, 902.5, 902.7, 902.9, 903.1, 903.3, 903.5, 903.7, 903.0
	8-15,65	903.9, 904.1, 904.3, 904.5, 904.7, 904.9, 905.1, 905.3,904.6
	16-23,66	905.5, 905.7, 905.9, 906.1, 906.3, 906.5, 906.7, 906.9, 906.2,
	24-31,67	907.1, 907.3, 907.5, 907.7, 907.9, 908.1, 908.3, 908.5, 907.8
	32-39,68	908.7, 908.9, 909.1, 909.3, 909.5, 909.7, 909.9, 910.1, 909.4
	40-47,69	910.3, 910.5, 910.7, 910.9, 911.1, 911.3, 911.5, 911.7, 911
	48-55,70	911.9, 912.1, 912.3, 912.5, 912.7, 912.9, 913.1, 913.3, 912.6
	55-63,71	913.5, 913.7, 913.9, 914.1, 914.3, 914.5, 914.7, 914.9, 914.2
AU915	0-7,64	915.2, 915.4, 915.6, 915.8, 916.0, 916.2, 916.4, 916.6, 915.9
	8-15,65	916.8, 917.0, 917.2, 917.4, 917.6, 917.8, 918.0, 918.2, 917.5
	16-23,66	918.4, 918.6, 918.8, 919.0, 919.2, 919.4, 919.6, 919.8, 919.1
	24-31,67	920.0, 920.2, 920.4, 920.6, 920.8, 921.0, 921.2, 921.4, 920.7
	32-39,68	921.6, 921.8, 922.0, 922.2, 922.4, 922.6, 922.8, 923.0, 922.3
	40-47,69	923.2, 923.4, 923.6, 923.8, 924.0, 924.2, 924.4, 924.6, 923.9

	48-55,70	924.8, 925.0, 925.2, 925.4, 925.6, 925.8, 926.0, 926.2, 925.5
	56-63,71	926.4, 926.6, 926.8, 927.0, 927.2, 927.4, 927.6, 927.8, 927.1
AS923	0-7	923, 923.4, 923.6, 923.8, 924.0, 924.2, 924.4, 924.6
AS923-1	0-7	923, 923.4, 923.6, 923.8, 924.0, 924.2, 924.4, 924.6
AS923-2	0-7	921.4, 921.6, 921.8, 922, 922.2, 922.4, 922.6, 922.8
AS923-3	0-7	916.6, 926.8, 916.4, 917.0, 917.2, 917.4, 917.6, 917.8
AS923-4	0-7	917.3, 917.5, 917.7, 917.9, 918.1, 918.3, 918.5, 918.7
KR920	0-7	922.1, 922.3, 922.5, 922.7, 922.9, 923.1, 923.3, 921.9