InHand Device Manager Platform

Simple and Efficient Device Management Solution

Quick Guide

Issue: V3.0 - 2023

InHand Networks
Global Leader in Industrial IoT
www.inhandnetworks.com

Contents

1 About the Platform

Device Manager ("DM") is an Internet of Things (IoT) device management cloud platform of the "new generation" independently developed and operated by InHand. With visual user interfaces (UIs) and easy-to-use processes, it allows you to conveniently manage and monitor hardware devices of InHand such as routers and gateways and quickly deploy and manage massive devices in one-click manner. You can just deploy your applications on the cloud without caring about maintenance, allowing you to focus on your core business and empower your enterprise.

Quick start with the platform:

Register an account -> Configure a router or gateway and connect it to the platform -> Enable management of the router or gateway device

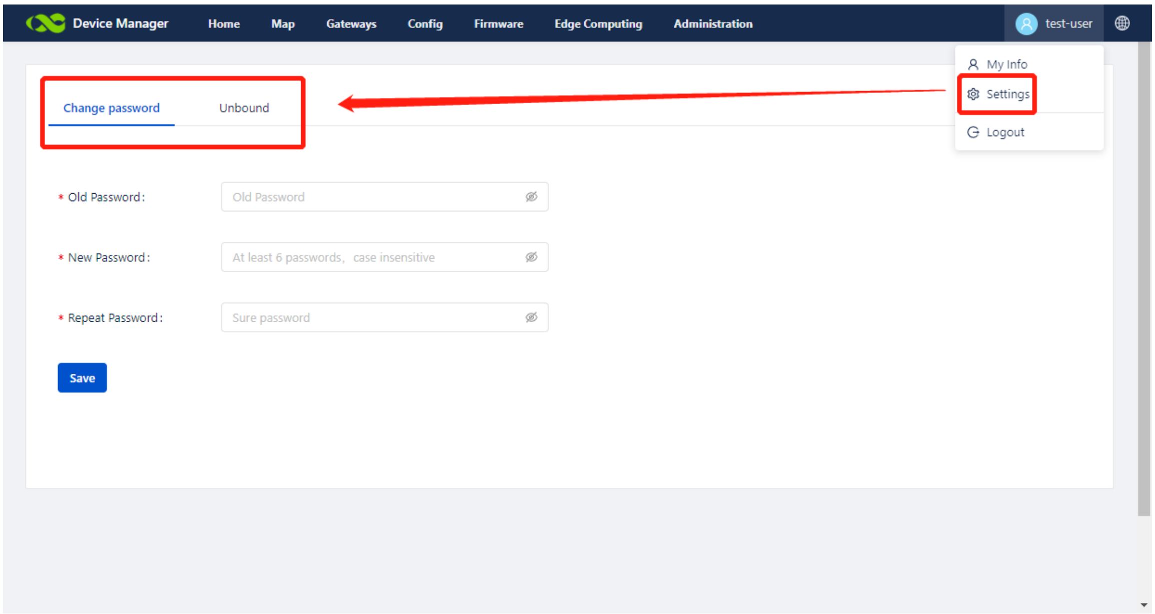
2 Registration and Login

1. Registration

On a browser, enter https://iot.inhandnetworks.com/ to visit the office website of Device Manager. Click **Register Account**, enter an email account and relevant information, and click **Submit**. The authenticity of your email account will be verified. Please activate the account as instructed.

2. Login

After registration, log in to the platform with the email account and password you used for registration. After login, choose **Personal Center** >> **Settings**, modify the login password and bind a phone number. Then, use the phone number and the verification code or the phone number and password for login. You can also use the phone number for recovering your password.



* Old Password: Old Password

* New Password: At least 6 passwords, case insensitive

* Repeat Password: Sure password

Save

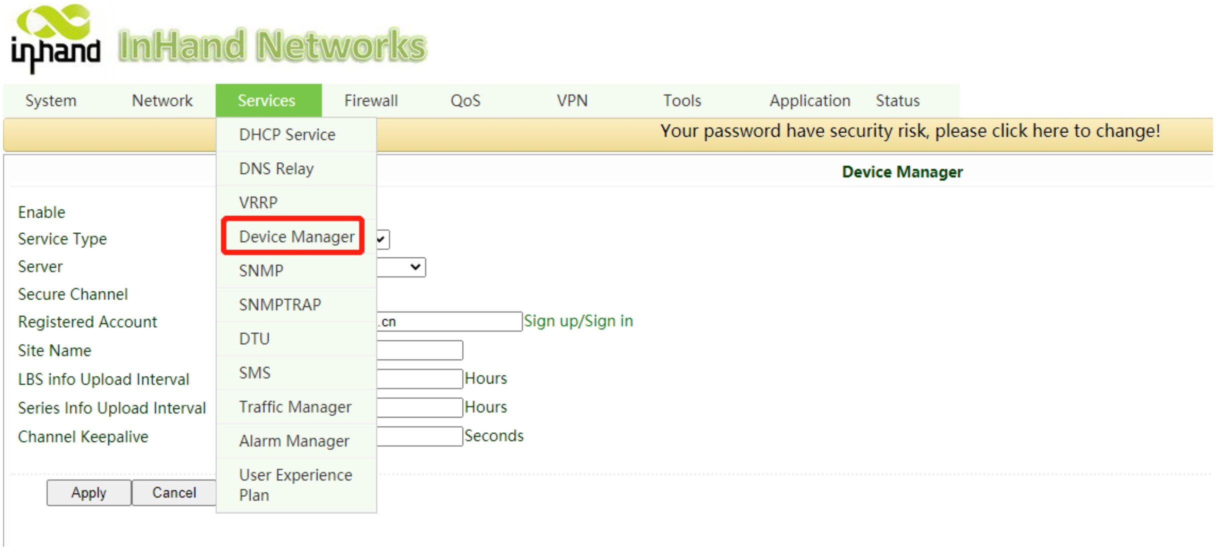
3 Connect Gateway Devices to DM

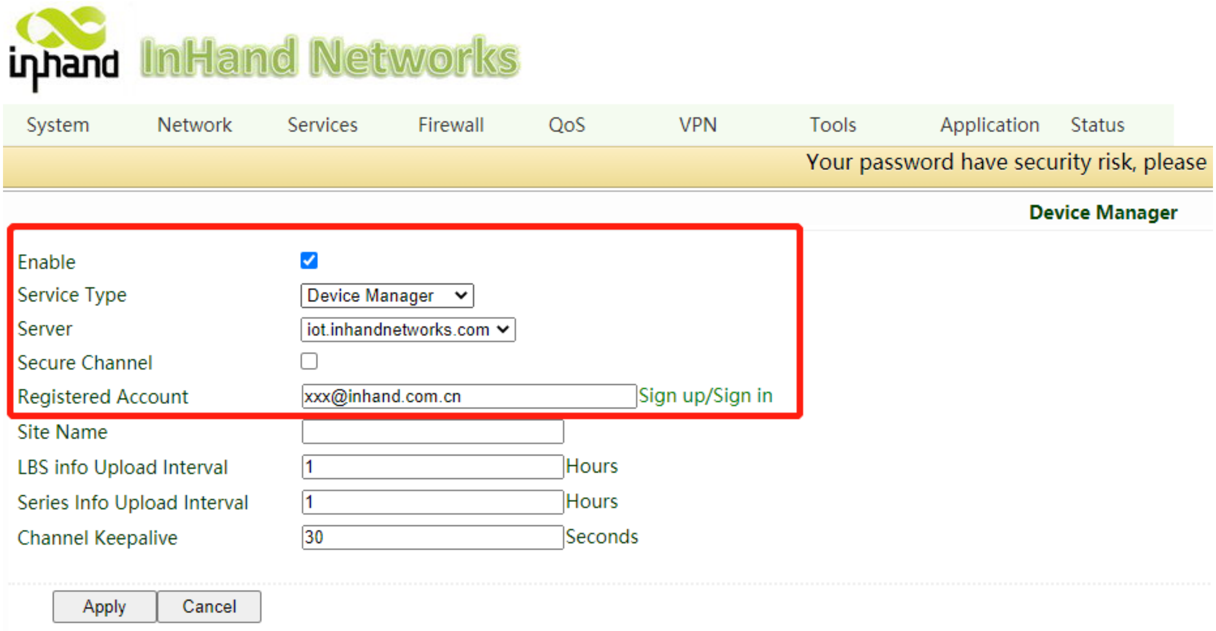
The following devices are supported to be managed on Device Manager platform: InRouter200, InRouter300, InRouter600, InRouter900, InGateway900, InGateway500, InVehicleG710, InVehicleG810. After connection configuration is made on the device, a new device data record is automatically added to DM. You do not need to manually record the device data on DM. The following describes the details.

Configure the router to connect it to DM. Before configuration, make sure that the router has been connected to the network. **For more information about networking operation, see the appendix.**

3.1 Connect IR300/IR600 to DM

After connecting the router to a PC, visit 192.168.2.1 or 192.168.1.1 on a browser, enter the login account **adm** and password **123456** to log in to the device web page. On the web page, choose **Services** >> **Device Manager**, choose **Service Type** as **Device Manager** and **Server** as **iot.inhandnetworks.com** and enter the email account you used for registration with DM in **Registered Account**:





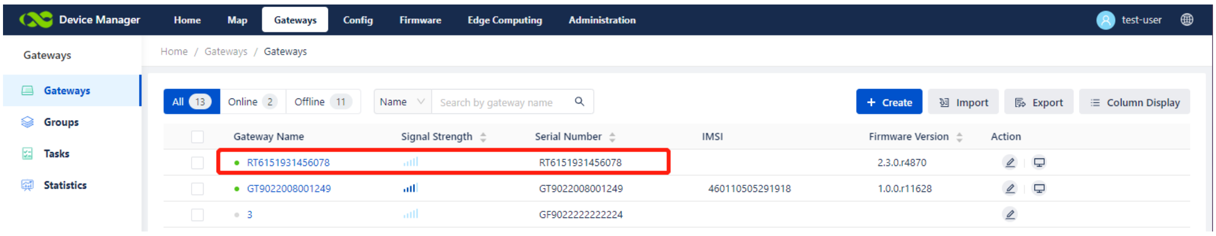
Device Manager

Enable	☑
Service Type	Device Manager
Server	iot.inhandnetworks.com
Secure Channel	□
Registered Account	xxx@inhand.com.cn Sign up/Sign in
Site Name	
LBS info Upload Interval	1 Hours
Series Info Upload Interval	1 Hours
Channel Keepalive	30 Seconds

Caution

The page varies with the device firmware version. The actual page shall prevail.

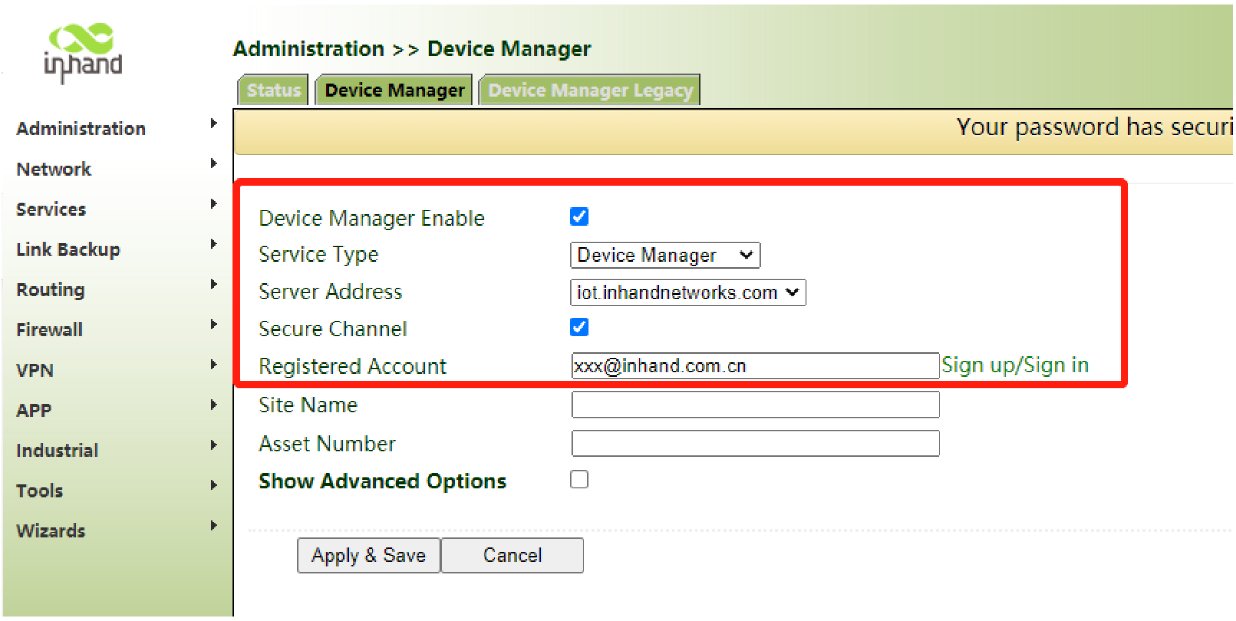
After the router is configured, a gateway data record is automatically added to the **Gateways** page on DM. You do not need to manually record the data. When the router status is **Online**, the device has been connected to DM:



Gateway Name	Signal Strength	Serial Number	IMSI	Firmware Version	Action
● RT6151931456078		RT6151931456078		2.3.0.r4870	
● GT9022008001249		GT9022008001249	460110505291918	1.0.0.r11628	
● 3		GF9022222222224			

3.2 Connect IR900/VG710 to DM

After connecting the router to a PC, visit 192.168.2.1 or 192.168.1.1 on a browser, enter the login account **adm** and password **123456** to log in to the device web page. On the web page, choose **Administration** >> **Device Manager**, set **Service Type** to Device Manager, select **iot.inhandnetworks.com** from **Server Address**, and enter the email account you used for registration with DM in **Registered Account**:



Administration >> Device Manager

Your password has securi

Device Manager Enable ☑

Service Type: Device Manager

Server Address: iot.inhandnetworks.com

Secure Channel ☑

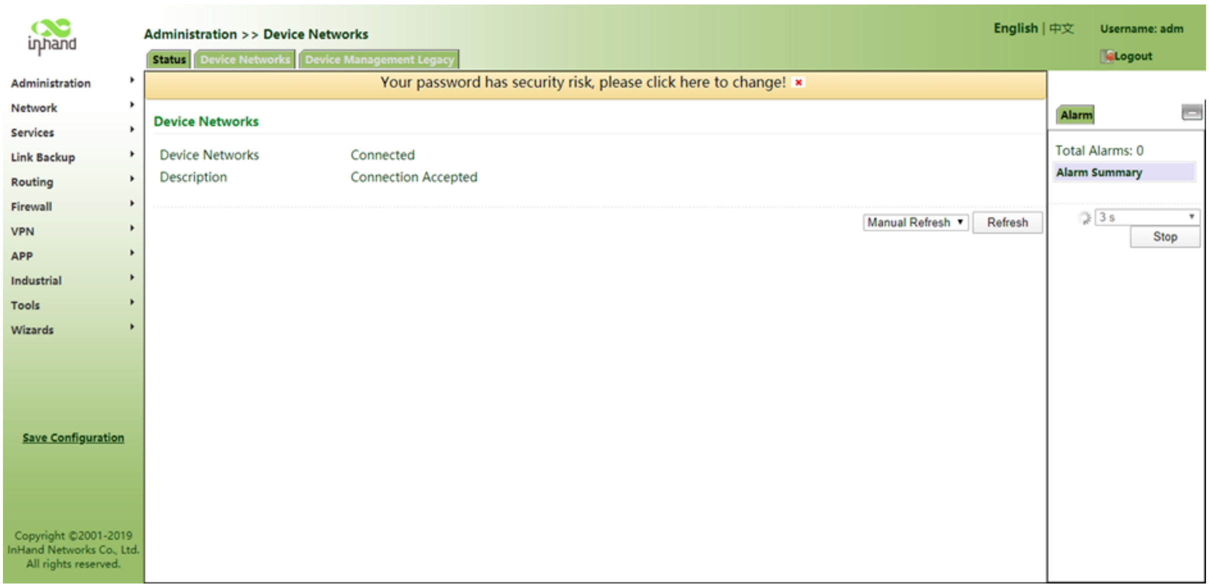
Registered Account: xxx@inhand.com.cn

Site Name:

Asset Number:

Show Advanced Options □

Click **Apply & Save**. If the status is **Connected**, the device has been connected to DM:



Administration >> Device Networks

Your password has security risk, please click here to change!

Device Networks

Device Networks: Connected

Description: Connection Accepted

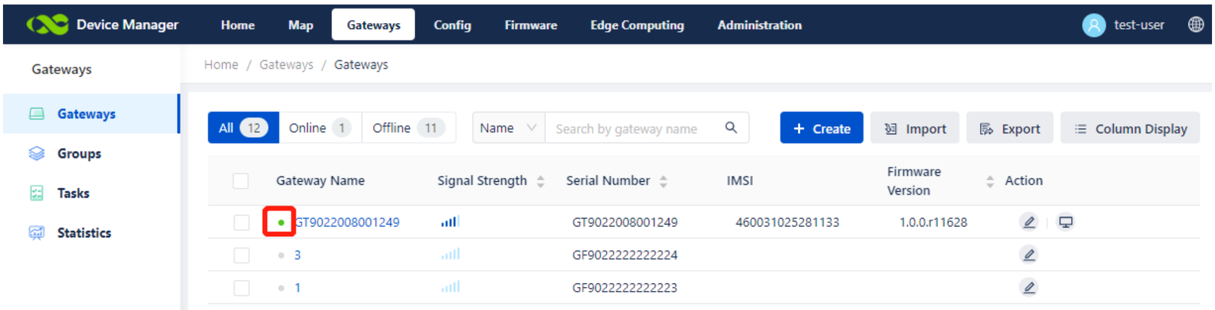
Total Alarms: 0

Copyright ©2001-2019 InHand Networks Co., Ltd. All rights reserved.

Caution

The page varies with the device firmware version. The actual page shall prevail.

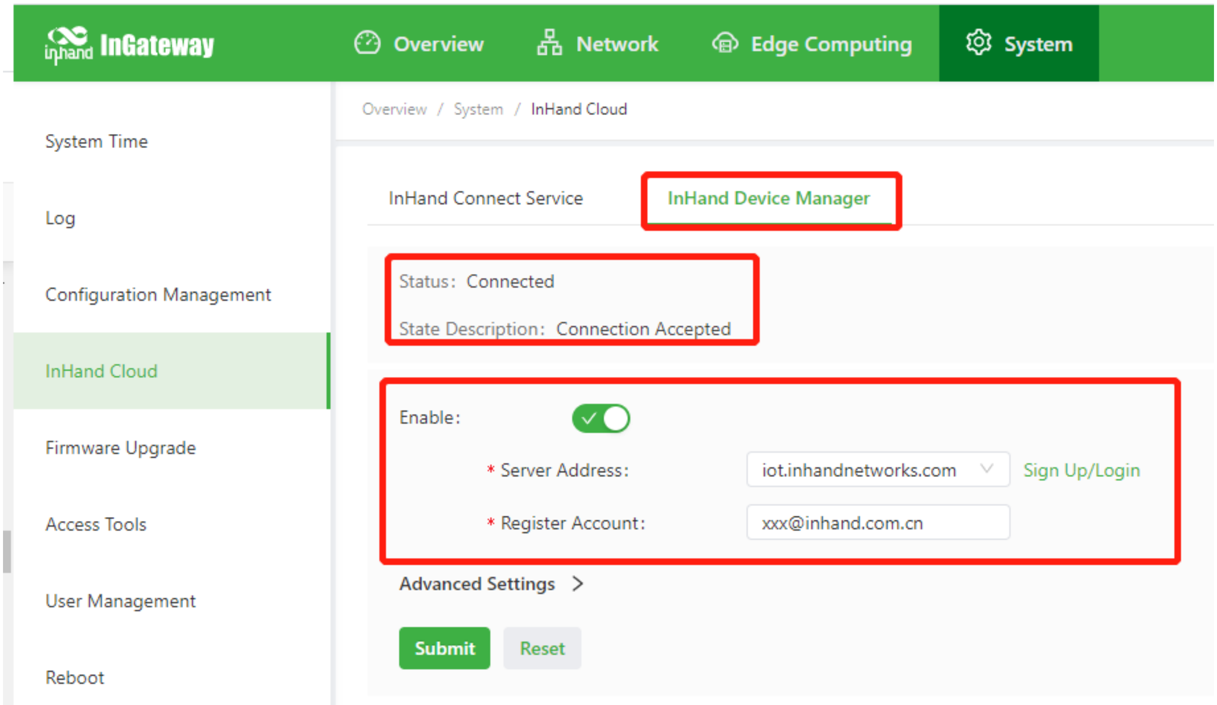
After the router is configured, a gateway data record is automatically added to the **Gateways** page on DM. You do not need to manually record the data. When the router status is **Online**, the device has been connected to DM:



Gateway Name	Signal Strength	Serial Number	IMSI	Firmware Version	Action
● GT9022008001249		GT9022008001249	460031025281133	1.0.0.r11628	
● 3		GF9022222222224			
● 1		GF9022222222223			

3.3 Connect IG500/IG900 to DM

After connecting the router to a PC, visit 192.168.1.1 on a browser, enter the login account **adm** and password **123456** to log in to the device web page. On the web page, choose **System >> InHand** Cloud, on the tab page of **InHand Device Manager** ，set **Server Address** to **iot.inhandnetworks.com**, and enter the email account you used for registration with DM in **Registered Account**:



Status: Connected

State Description: Connection Accepted

Enable: ✓

* Server Address: iot.inhandnetworks.com

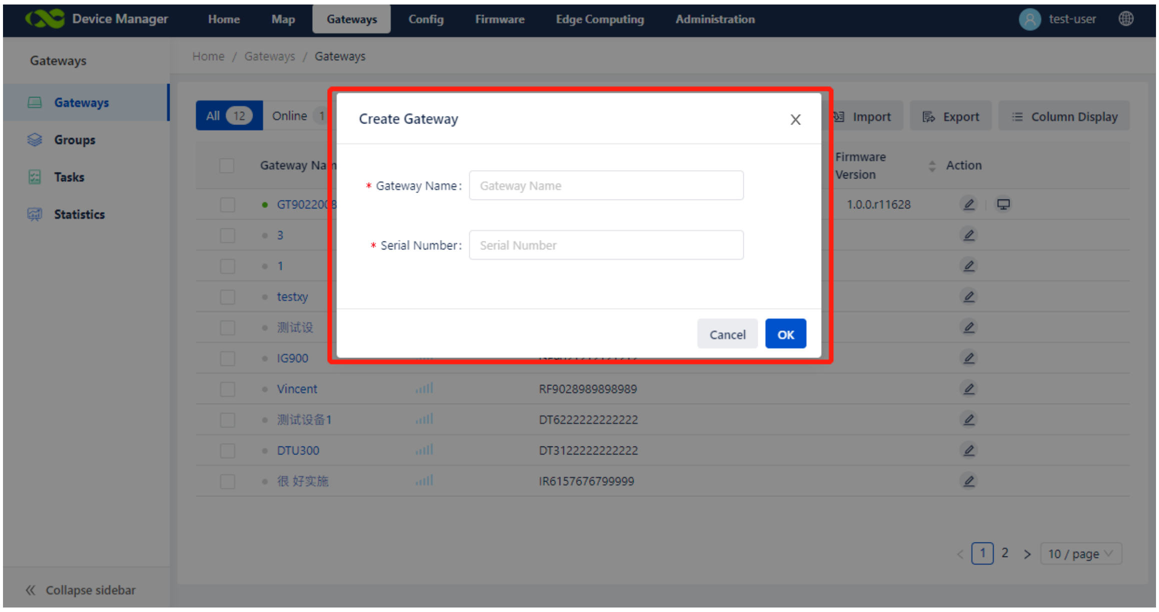
* Register Account: xxx@inhand.com.cn

3.4 Add Gateway to DM

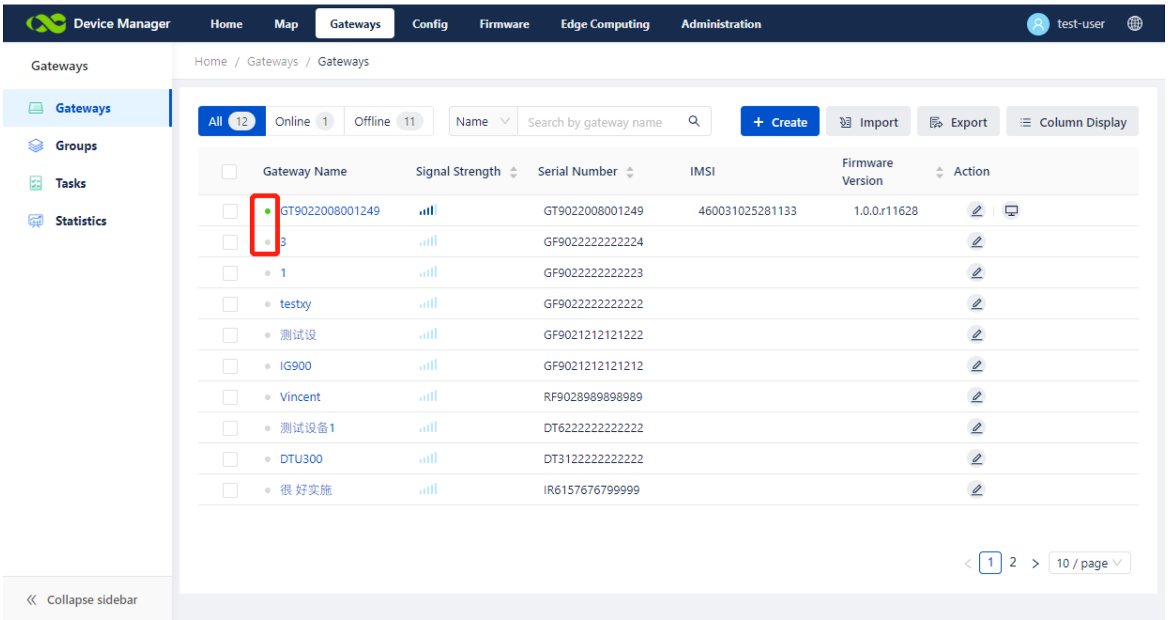
As mentioned above, after the router is configured, a gateway data record is automatically added to the **Gateways** page on DM. You can manually add the data before configuring the router. The status of the manually added gateway is **Offline**. After the gateway can be connected, its status changes to **Online**.

◆ Add a single gateway

1. Choose **Gateways** >> **+**. Enter a gateway name in **Gateway Name**, enter the serial number in **Serial Number**. To view the serial number, on the home page, choose **Administration** >> **System** >> **Status or Gateway Nameplate S/N**, and then click OK.



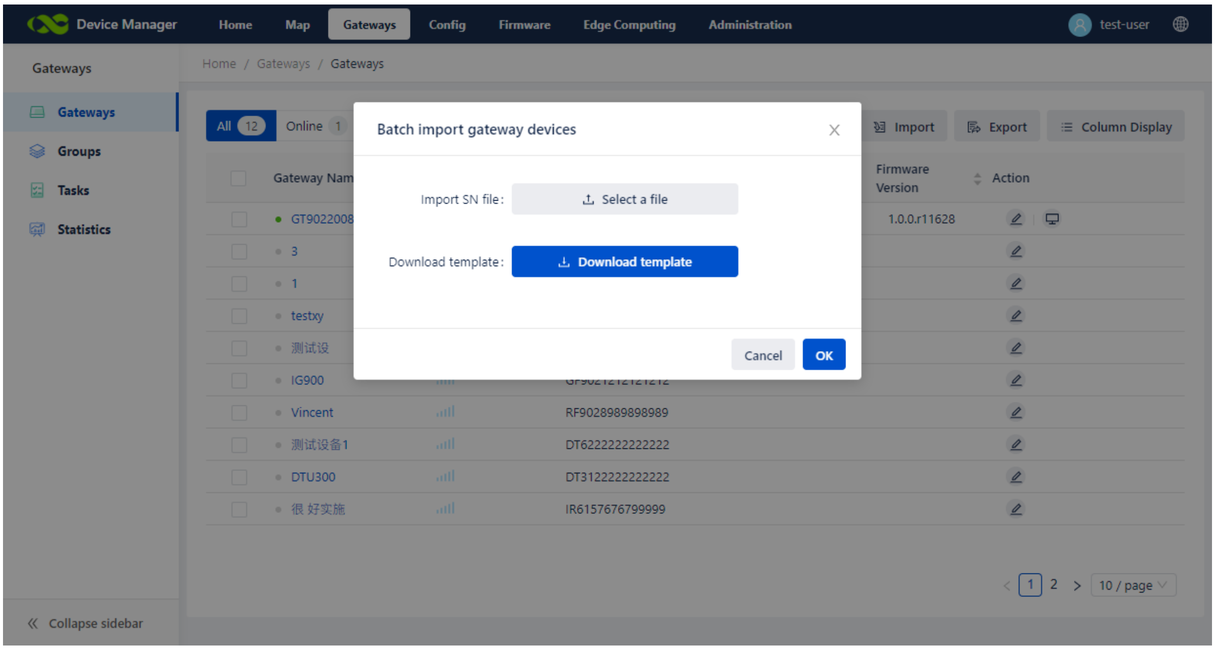
2. Return to the **Gateways** page. The device is added. If the dot before the gateway name turns green, the device is online and connected to DM and the network. If the dot is gray, the device is offline and disconnected from the network. DM cannot manage and monitor offline devices.



Gateway Name	Signal Strength	Serial Number	IMSI	Firmware Version	Action
● GT9022008001249		GT9022008001249	460031025281133	1.0.0.r11628	
● 3		GF9022222222224			
● 1		GF9022222222223			
● testxy		GF9022222222222			
● 测试设		GF9021212121222			
● IG900		GF9021212121212			
● Vincent		RF9028989898989			
● 测试设备1		DT6222222222222			
● DTU300		DT3122222222222			
● 很 好实施		IR6157676799999			

- Add gateways in batches

1. Choose **Gateways** >> **Import** >> Download Template, enter the gateway information, and save the template. Click **Select File**, select the saved template, and click OK.



Batch import gateway devices

Import SN file: Select a file

Download template: Download template

2. Return to the Gateways page to view the imported device.

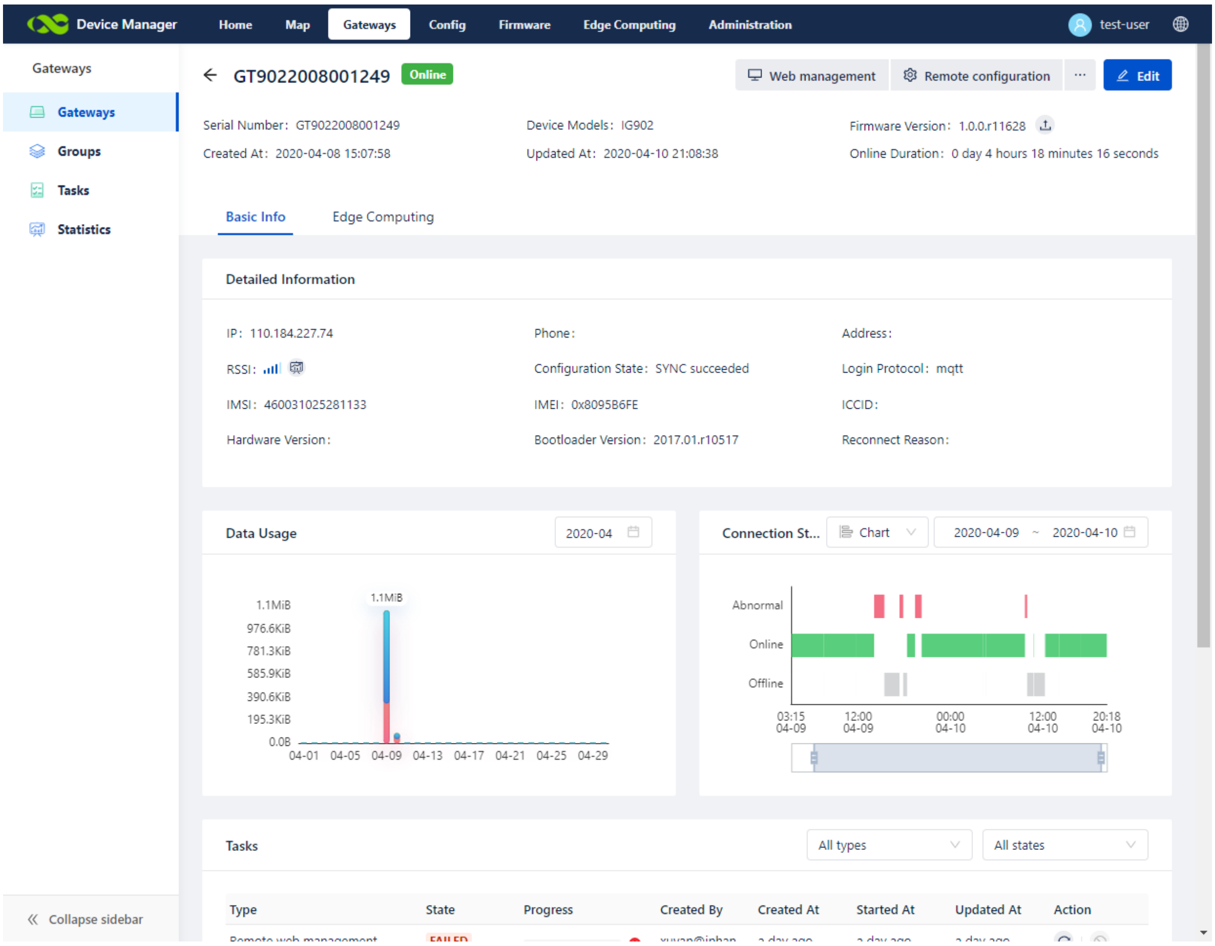
4 Gateway Management

After a gateway is connected to DM, you can manage the device on DM, such as device asset management, configuration update, firmware upgrade, position tracking, running monitoring, and operation command monitoring.

4.1 Basic Management

4.1.1 Information Management

In the **Details Information** section of the **Gateways** page, you can manage key information of the gateway, including basic information (such as the model, serial number, IP address, RSSI, and IMSI), running information (such as traffic statistics and online statistics), and control information (such as task list). Devices connected to DM regularly report their traffic, online status, and other running information to DM for real-time monitoring and analysis.



GT9022008001249 Online

Serial Number: GT9022008001249

Device Models: IG902

Firmware Version: 1.0.0.r11628

Created At: 2020-04-08 15:07:58

Updated At: 2020-04-10 21:08:38

Online Duration: 0 day 4 hours 18 minutes 16 seconds

Detailed Information

IP: 110.184.227.74

Phone:

Address:

RSSI:

Configuration State: SYNC succeeded

Login Protocol: mqtt

IMSI: 460031025281133

IMEI: 0x8095B6FE

ICCID:

Hardware Version:

Bootloader Version: 2017.01.r10517

Reconnect Reason:

Data Usage 2020-04

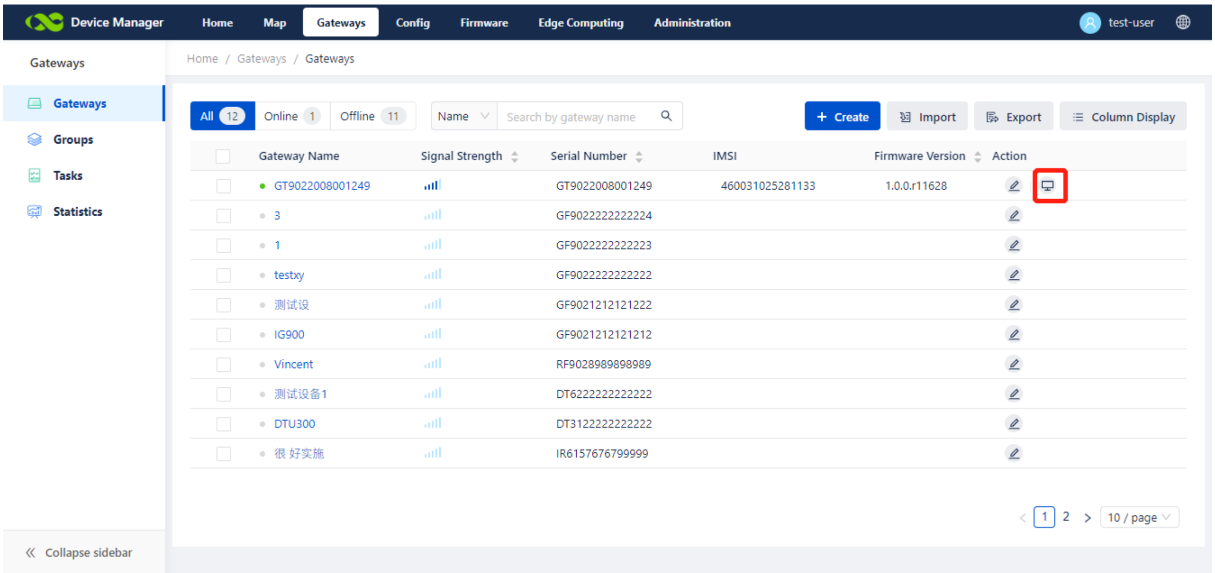
Connection St... Chart 2020-04-09 ~ 2020-04-10

Tasks All types All states

Type	State	Progress	Created By	Created At	Started At	Updated At	Action
Remote web management	FAILED		xuyan@inhan	a day ago	a day ago	a day ago	

4.1.2 Remote Web Access

1. On the **Gateways** or **Device Details** page, click the 🖵 icon to go to the **Web Management** page of the gateway. On this page, you can directly modify the device configuration locally. This function is only applicable for online devices.

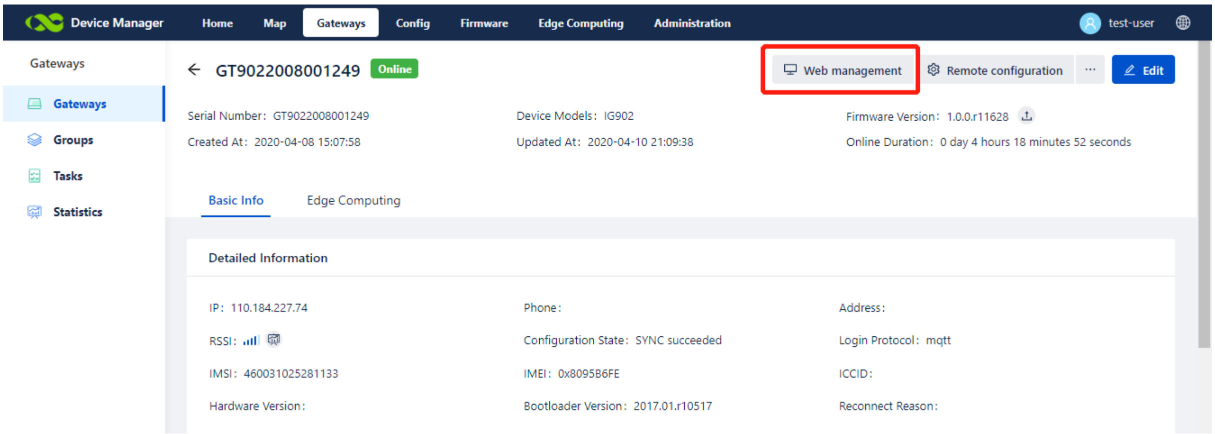


Home / Gateways / Gateways

All 12 | Online 1 | Offline 11 | Name | Search by gateway name

	Gateway Name	Signal Strength	Serial Number	IMSI	Firmware Version	Action
□	● GT9022008001249		GT9022008001249	460031025281133	1.0.0.r11628	🖉 🖵
□	● 3		GF9022222222224			🖉
□	● 1		GF9022222222223			🖉
□	● testxy		GF9022222222222			🖉
□	● 测试设		GF9021212121222			🖉
□	● IG900		GF9021212121212			🖉
□	● Vincent		RF9028989898989			🖉
□	● 测试设备1		DT6222222222222			🖉
□	● DTU300		DT3122222222222			🖉
□	● 很 好实施		IR6157676799999			🖉

< 1 2 > 10 / page



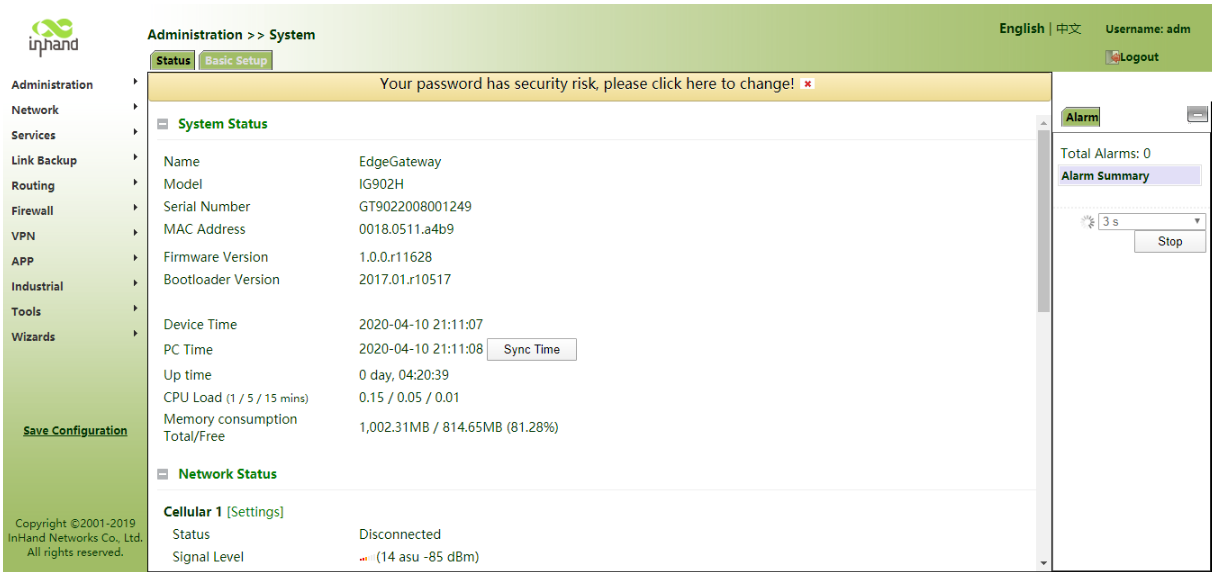
GT9022008001249 Online

Serial Number: GT9022008001249
Device Models: IG902
Firmware Version: 1.0.0.r11628
Created At: 2020-04-08 15:07:58
Updated At: 2020-04-10 21:09:38
Online Duration: 0 day 4 hours 18 minutes 52 seconds

Detailed Information

IP: 110.184.227.74
Phone:
Address:
RSSI:
Configuration State: SYNC succeeded
Login Protocol: mqtt
IMSI: 460031025281133
IMEI: 0x8095B6FE
ICCID:
Hardware Version:
Bootloader Version: 2017.01.r10517
Reconnect Reason:

2. Enter the username and password to go to the **Web Management** page of the gateway, and then remotely operate and control the device through commands.



Your password has security risk, please click here to change!

System Status

Name EdgeGateway
Model IG902H
Serial Number GT9022008001249
MAC Address 0018.0511.a4b9
Firmware Version 1.0.0.r11628
Bootloader Version 2017.01.r10517
Device Time 2020-04-10 21:11:07
PC Time 2020-04-10 21:11:08
Up time 0 day, 04:20:39
CPU Load (1 / 5 / 15 mins) 0.15 / 0.05 / 0.01
Memory consumption Total/Free 1,002.31MB / 814.65MB (81.28%)

Network Status

Cellular 1 [Settings]
Status Disconnected
Signal Level (14 asu -85 dBm)

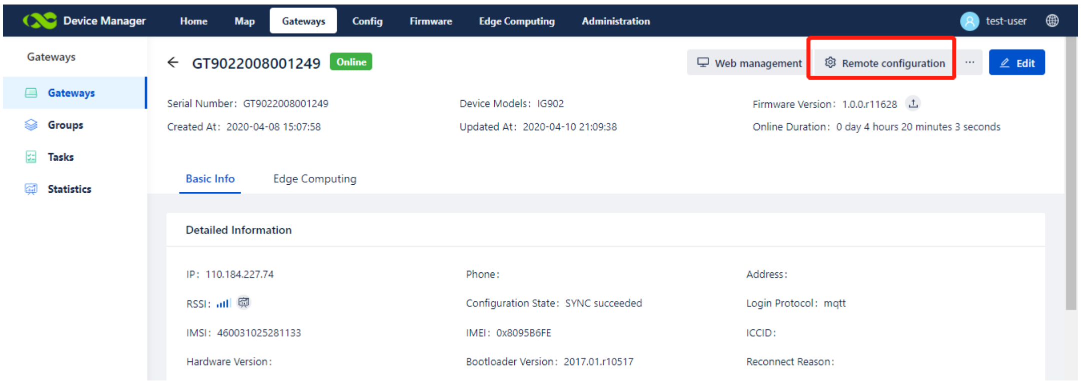
Total Alarms: 0
Alarm Summary
3 s

Copyright ©2001-2019 InHand Networks Co., Ltd. All rights reserved.

4.1.3 Update Configuration

You can only update the configuration of online devices.

On the gateway details page of an online device, click **Remote Configuration**. Edit and update the device configuration and then click **Deliver**. The device configuration is remotely updated, and a task record is generated in the task list on the details page. The task status is updated in real time to reflect the execution status in real time.

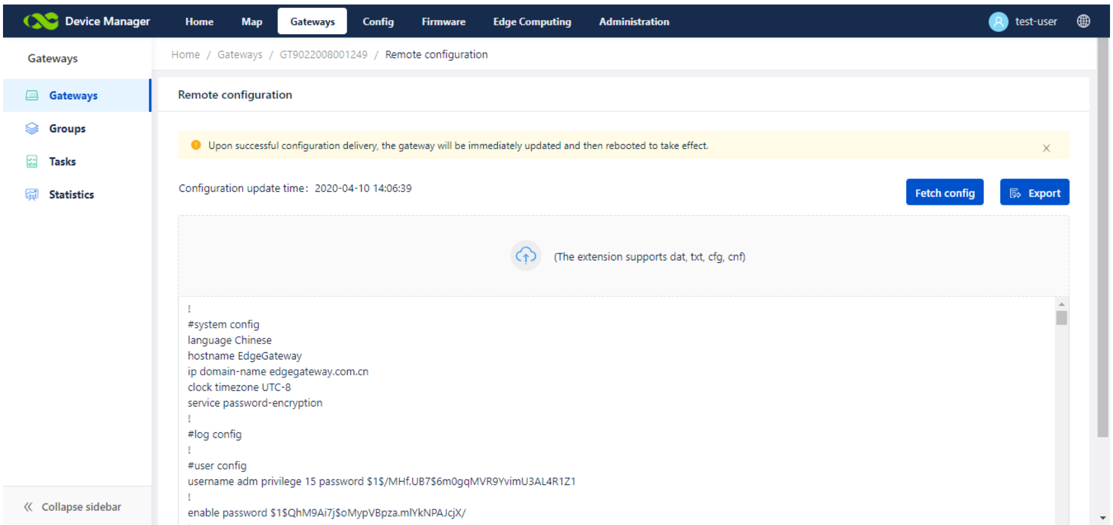


GT9022008001249 Online

Serial Number: GT9022008001249
Device Models: IG902
Firmware Version: 1.0.0.r11628
Created At: 2020-04-08 15:07:58
Updated At: 2020-04-10 21:09:38
Online Duration: 0 day 4 hours 20 minutes 3 seconds

Detailed Information

IP: 110.184.227.74
Phone:
Address:
RSSI:
Configuration State: SYNC succeeded
Login Protocol: mqtt
IMSI: 460031025281133
IMEI: 0x8095B6FE
ICCID:
Hardware Version:
Bootloader Version: 2017.01.r10517
Reconnect Reason:



Upon successful configuration delivery, the gateway will be immediately updated and then rebooted to take effect.

Configuration update time：2020-04-10 14:06:39

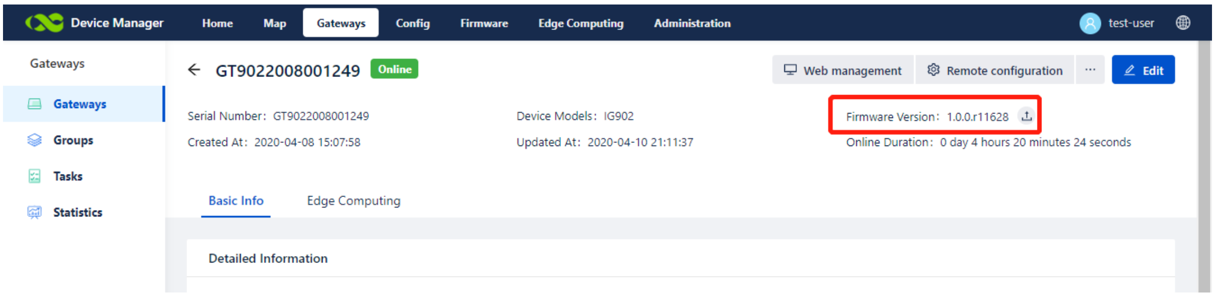
(The extension supports dat, txt, cfg, cnf)

```
!
#system config
language Chinese
hostname EdgeGateway
ip domain-name edgegateway.com.cn
clock timezone UTC-8
service password-encryption
!
#log config
!
#user config
username adm privilege 15 password $1$/MHf.UB7$6m0gqMVR9YvimU3AL4R1Z1
!
enable password $1$QhM9Ai7j$oMypVBpza.mlYkNPAJcjX/
```

4.1.4 Upgrade Firmware

On the device details page, click Firmware Version：1.0.0.r11628 next to **Firmware Version**, and upload a file. After the file is uploaded, a task record is generated in the task list on the details page. The task status is updated in real time to reflect the execution status in real time.

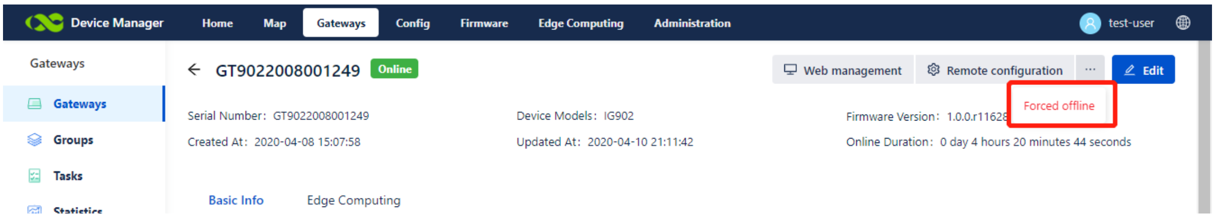
Online devices execute the upgrade task immediately, while offline devices will execute the upgrade task after they are online again.



Serial Number：GT9022008001249
Created At：2020-04-08 15:07:58
Device Models：IG902
Updated At：2020-04-10 21:11:37
Firmware Version：1.0.0.r11628
Online Duration：0 day 4 hours 20 minutes 24 seconds

4.1.5 Forced Offline

When configuration delivery and firmware upgrade fail for multiple times, you can try to force a gateway offline, connect it to DM again, and then try to deliver the configuration and upgrade the firmware again.

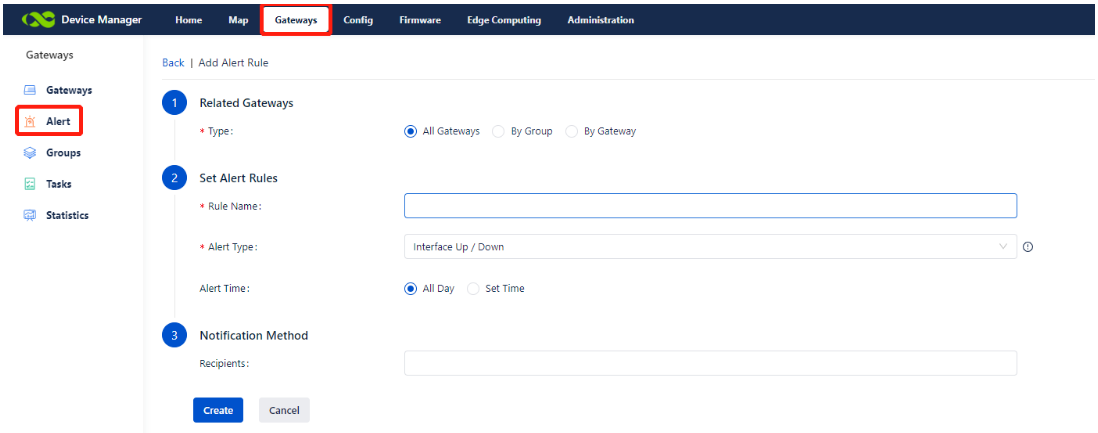


Serial Number：GT9022008001249
Created At：2020-04-08 15:07:58
Device Models：IG902
Updated At：2020-04-10 21:11:42
Firmware Version：1.0.0.r11628
Online Duration：0 day 4 hours 20 minutes 44 seconds

4.2 Alerts

The device Manager platform supports setting alerts to monitor some important events of the Devices. When an event occurs, it can push SMS or email messages to specified users. The support of each device is subject to the information displayed on the interface. IR600 for example, an offline alarm is used to perform operations.

1. Configure alert rules: On the page of " Gateways -> Alerts -> Alert Rules" , click " Add Rule " , select devices, alert rules and notification rules in the form as needed:



Back | Add Alert Rule

1 Related Gateways

* Type: ● All Gateways ○ By Group ○ By Gateway

2 Set Alert Rules

* Rule Name:

* Alert Type: Interface Up / Down

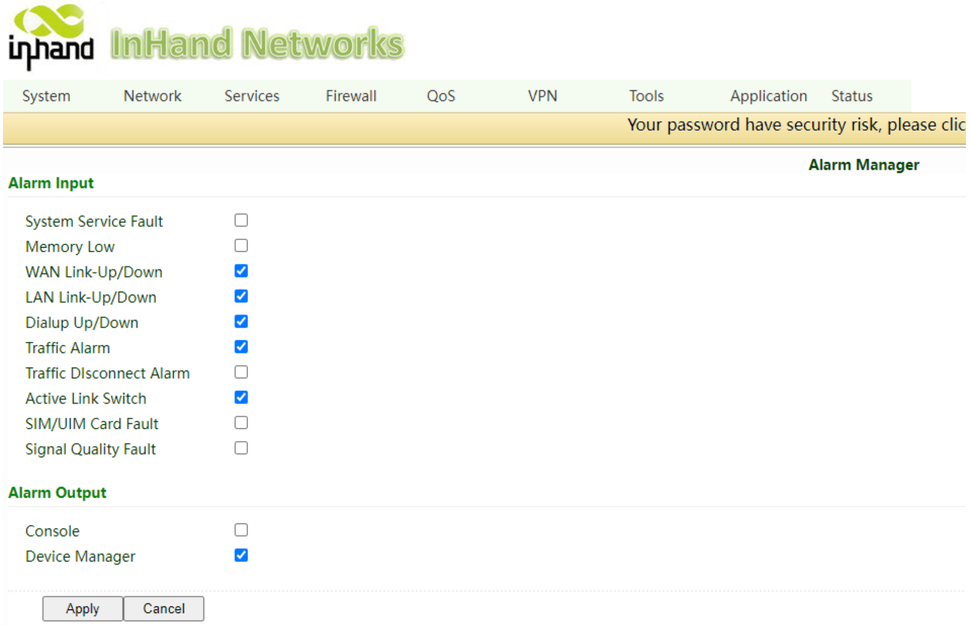
Alert Time: ● All Day ○ Set Time

3 Notification Method

Recipients:

Create Cancel

2. After the rule is added, click " save " , the rule takes effect immediately; As shown in the figure, an offline alarm rule is configured for a gateway: When the gateway is offline for 10 minutes, the user’s email “demo@inhand.com.cn” will receive an alert email, and the alert messages will be also recorded on the page “Gateways->Alerts->Alert Logs”.
3. For some specific alert types, you must enable alert reporting on the device before the alert takes effect. Take the IR600 for example: on the device WEB management page, visit the page “Services ->Alarm Manager”, select alarm type, select “Device Manager” as the alarm output, then click “Apply”.



Your password have security risk, please clic

Alarm Manager

Alarm Input

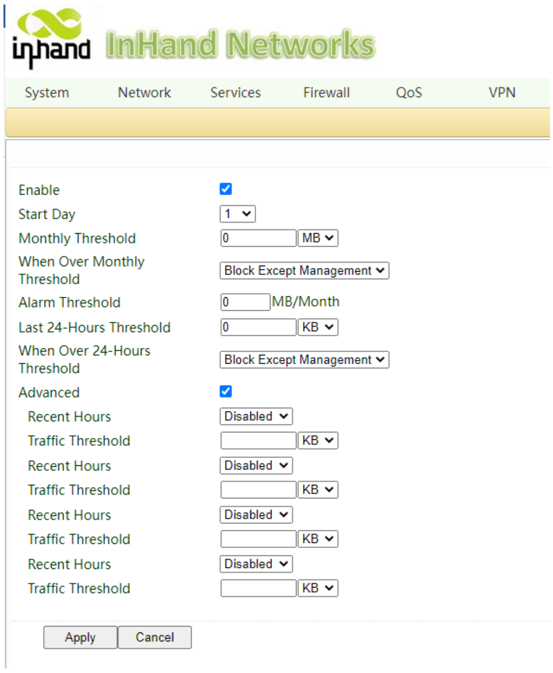
System Service Fault	☐
Memory Low	☐
WAN Link-Up/Down	☑
LAN Link-Up/Down	☑
Dialup Up/Down	☑
Traffic Alarm	☑
Traffic DIsconnect Alarm	☐
Active Link Switch	☑
SIM/UIM Card Fault	☐
Signal Quality Fault	☐

Alarm Output

Console	☐
Device Manager	☑

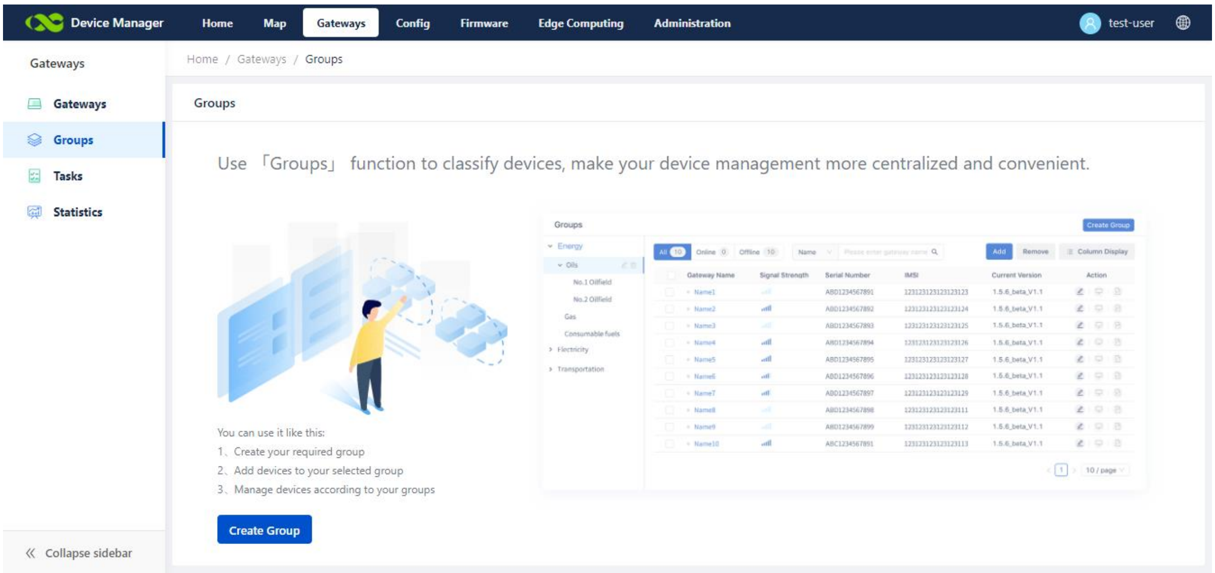
Apply Cancel

4. After the application is successful, when the device has the above event, it will send an event message to the platform, and the user will receive an email or SMS alert message according to the settings. The following table lists the alert types of the platform and the device:

Device Manager	**The WEB management page of device**
Hourly Traffic Alarm	The alarm type is "Traffic Alarm", and the traffic alarm threshold should be defined in the "Services -> Traffic Manager" section at the same time. After setting the required hourly, 24-hours (day) and monthly thresholds, the platform will send an alarm message when the specified alarm threshold is reached.  InHand Networks System Network Services Firewall QoS VPN Apply Cancel Enable ☑ Start Day 1 Monthly Threshold 0 MB When Over Monthly Threshold Block Except Management Alarm Threshold 0 MB/Month Last 24-Hours Threshold 0 KB When Over 24-Hours Threshold Block Except Management Advanced ☑ Recent Hours Disabled Traffic Threshold KB Recent Hours Disabled Traffic Threshold KB Recent Hours Disabled Traffic Threshold KB Recent Hours Disabled Traffic Threshold KB
Daily Traffic Alarm	
Monthly Traffic Alarm	
SIM Switch	Active Link Switch
Link Backup	Active Link Switch
Interface Up/Down	WAN Link-Up/Down, LAN Link-Up/Down, Dialup Up/Down

4.3 Device Group Management

When the system has a great number of devices, you can group devices for centralized management in the Groups table. For example, you can manage devices by industry, so that you can clearly know the scenarios of each device. You can also place abnormal groups in the same group for centralized management. When the device error is removed, move the device out of the group.

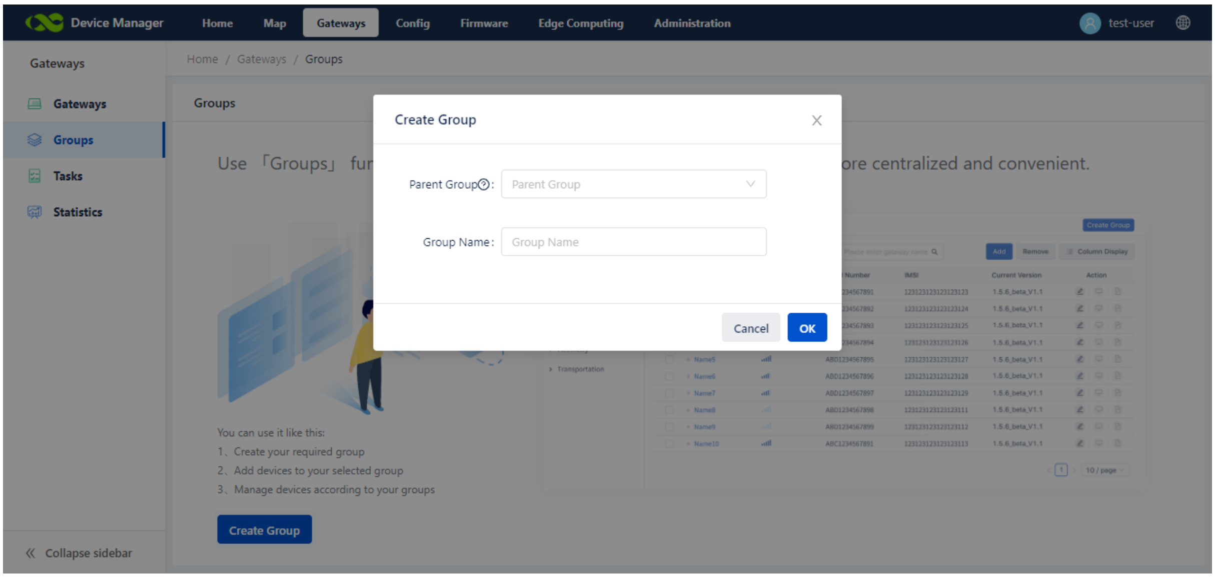


Use 「Groups」 function to classify devices, make your device management more centralized and convenient.

You can use it like this:
1、Create your required group
2、Add devices to your selected group
3、Manage devices according to your groups

The following describes the details:

1. Click **Create Group** and enter the group name and other information:

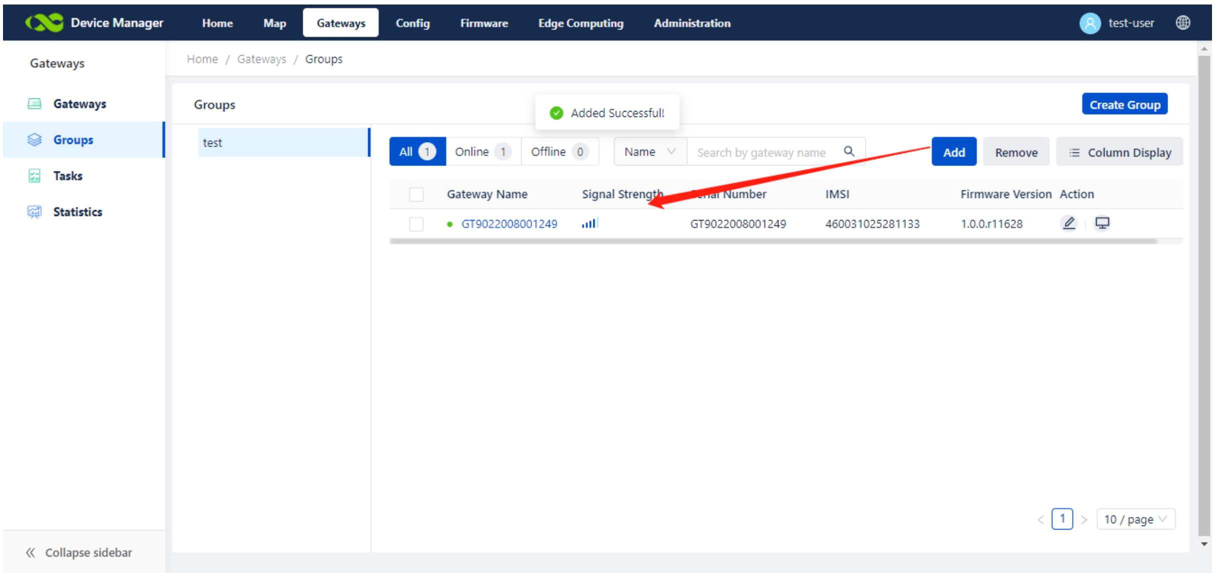


Create Group

Parent Group: Parent Group

Group Name: Group Name

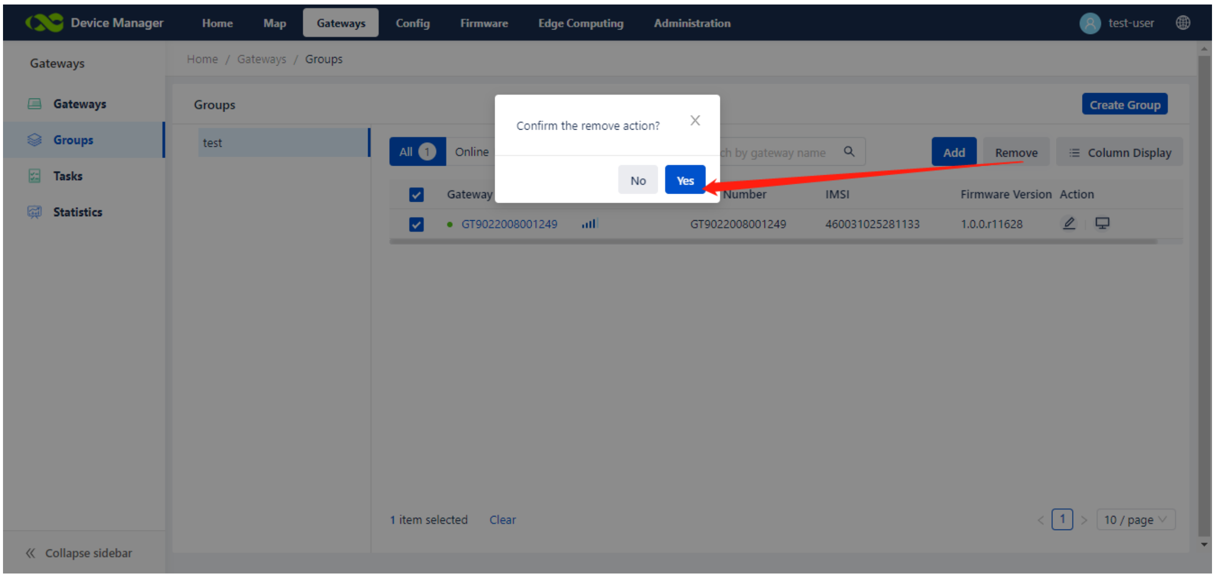
2. After the group is created, you can add devices to the current group:



Added Successful!

□	Gateway Name	Signal Strength	Serial Number	IMSI	Firmware Version	Action
□	● GT9022008001249		GT9022008001249	460031025281133	1.0.0.r11628	

3. If an added group has changed, select the group and then move it out of the current group.



Confirm the remove action?

Gateway	Number	IMSI	Firmware Version	Action
GT9022008001249	GT9022008001249	460031025281133	1.0.0.r11628	

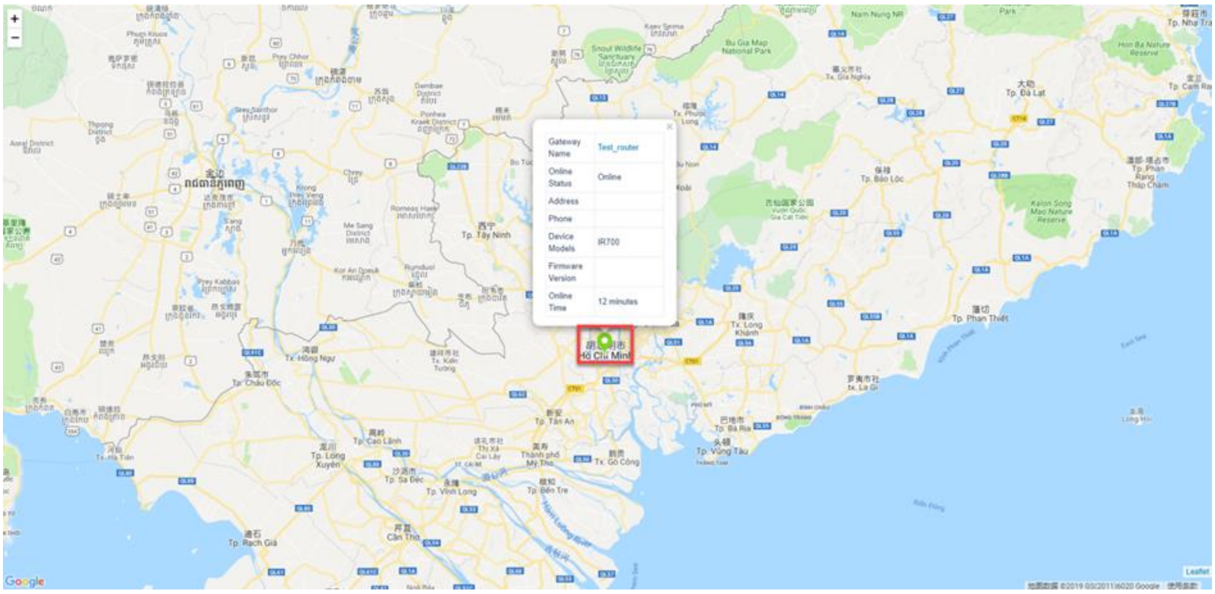
1 item selected Clear

10 / page

You can create groups of multiple levels based on service demands to manage devices by level.

4.4 Position Tracking

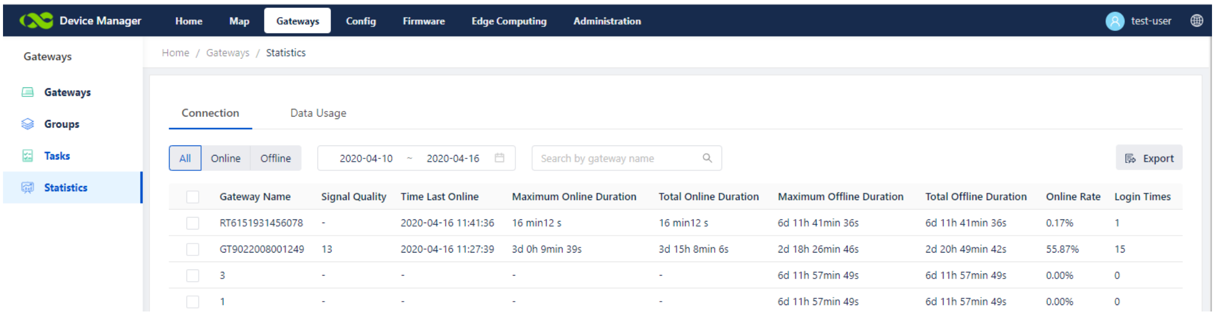
The **Map** page displays the real-time position and online status of the gateway. After you click the device icon on the map, the device basic information is displayed. Then, you can click the gateway name to view the device details.



Gateway Name	Test_router
Online Status	Online
Address	
Phone	
Device Models	IR700
Firmware Version	
Online Time	12 minutes

4.5 Gateway Running Monitoring

1. On the **Gateways->Statistics** page, you can view online duration statistics and traffic usage of a device and export the list of its online duration and traffic usage.



2020-04-10 ~ 2020-04-16

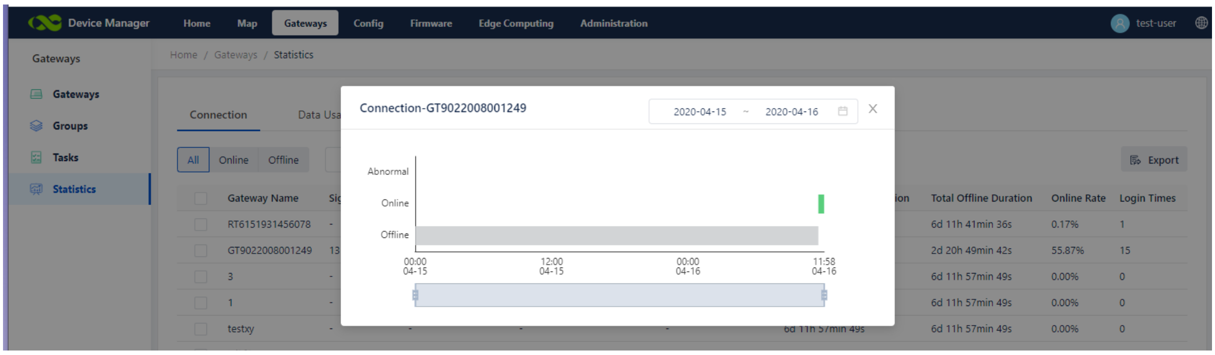
□	Gateway Name	Signal Quality	Time Last Online	Maximum Online Duration	Total Online Duration	Maximum Offline Duration	Total Offline Duration	Online Rate	Login Times
□	RT6151931456078	-	2020-04-16 11:41:36	16 min12 s	16 min12 s	6d 11h 41min 36s	6d 11h 41min 36s	0.17%	1
□	GT9022008001249	13	2020-04-16 11:27:39	3d 0h 9min 39s	3d 15h 8min 6s	2d 18h 26min 46s	2d 20h 49min 42s	55.87%	15
□	3	-	-	-	-	6d 11h 57min 49s	6d 11h 57min 49s	0.00%	0
□	1	-	-	-	-	6d 11h 57min 49s	6d 11h 57min 49s	0.00%	0

2. Click the device. The device status bar chart of the device is displayed.

Online: The device is connected to DM.

Offline: The device is disconnected from DM.

Abnormal: When the statistical period is less than three days, if the status changes for more than three times in two hours, it is abnormal. When the statistical period is more than three days, if the status changes for more than three times in one day, it is abnormal.



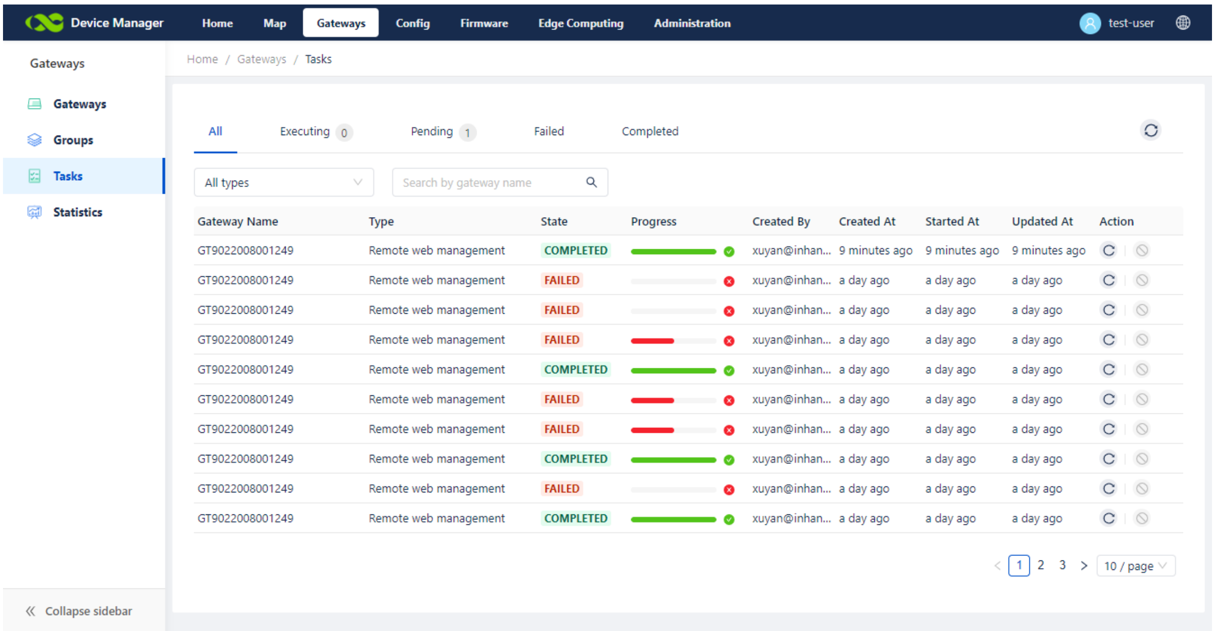
Connection-GT9022008001249

2020-04-15 ~ 2020-04-16

□	Gateway Name	Sig	ion	Total Offline Duration	Online Rate	Login Times
□	RT6151931456078	-		6d 11h 41min 36s	0.17%	1
□	GT9022008001249	13		2d 20h 49min 42s	55.87%	15
□	3	-		6d 11h 57min 49s	0.00%	0
□	1	-		6d 11h 57min 49s	0.00%	0
□	testxy	-	6d 11h 57min 49s	6d 11h 57min 49s	0.00%	0

4.6 Operation Command Monitoring

On the page of **Gateways-> Tasks**, you can view the execution status of the tasks sent from DM to devices. In the **Action** column, you can click to re-execute a task or cancel an in-progress task.

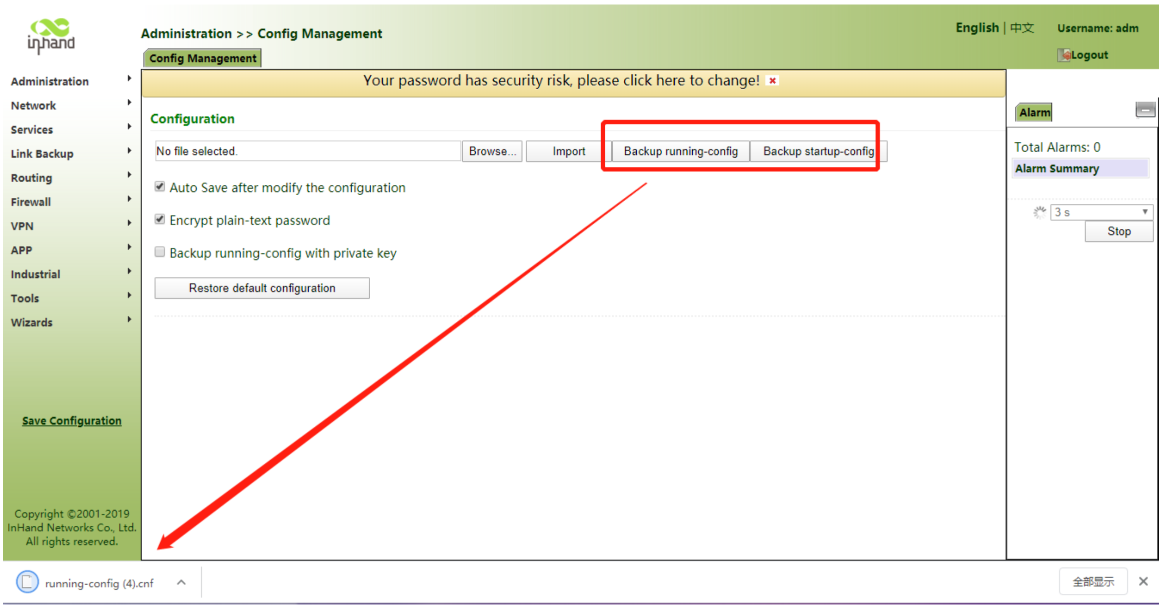


Gateway Name	Type	State	Progress	Created By	Created At	Started At	Updated At	Action
GT9022008001249	Remote web management	COMPLETED	✓	xuyan@inhan...	9 minutes ago	9 minutes ago	9 minutes ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	COMPLETED	✓	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	COMPLETED	✓	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	FAILED	✕	xuyan@inhan...	a day ago	a day ago	a day ago	
GT9022008001249	Remote web management	COMPLETED	✓	xuyan@inhan...	a day ago	a day ago	a day ago	

5 Update Gateway Configurations in Batches

When a large number of devices are connected to DM, it takes a great time to update the configuration device by device. You can update the configuration in batches on the **Config** page. The following describes the details:

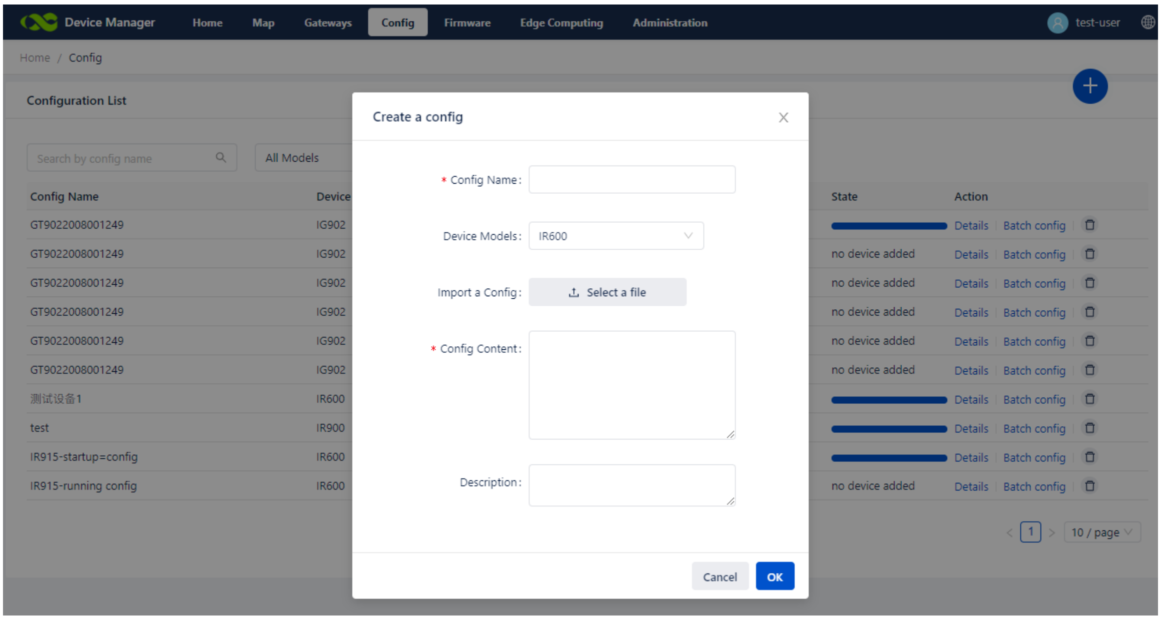
1. Choose **Gateways** >> **Config** >> **+** >> **Select File**. Select a configuration file (which can be exported from the **Web Management** page of the gateway, edited, and then applied), enter a name in **Config Name**, enter the model in the template in **Device Models**, and then click OK.



☑ Auto Save after modify the configuration

☑ Encrypt plain-text password

□ Backup running-config with private key



* Config Name:

Device Models: IR600

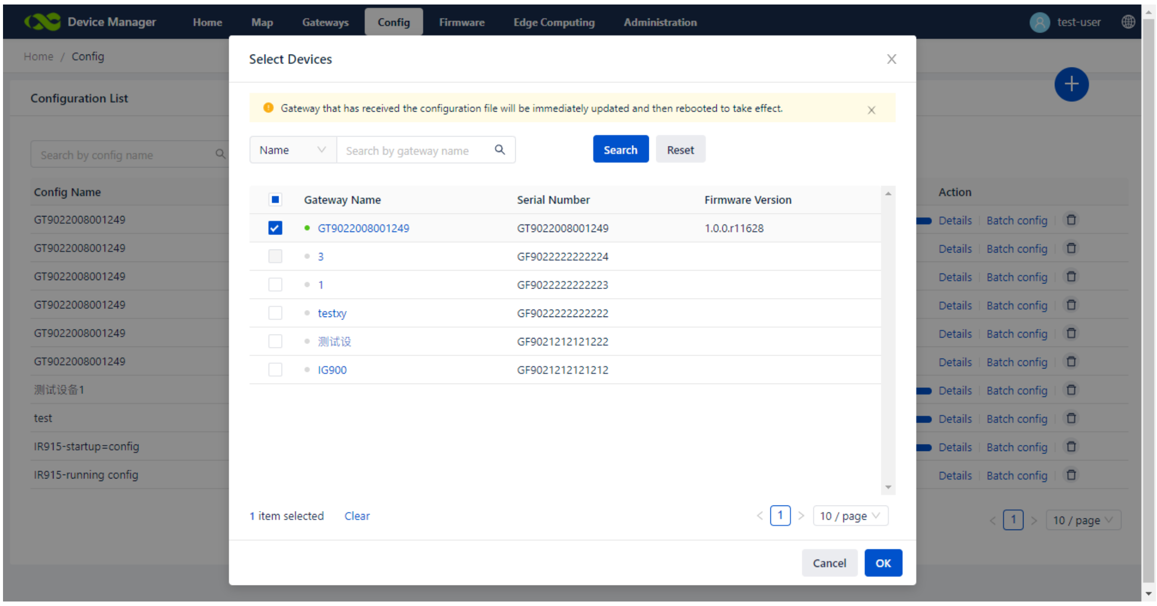
Import a Config:

* Config Content:

Description:

Config Name	Device	State	Action
GT9022008001249	IG902		Details | Batch config
GT9022008001249	IG902	no device added	Details | Batch config
GT9022008001249	IG902	no device added	Details | Batch config
GT9022008001249	IG902	no device added	Details | Batch config
GT9022008001249	IG902	no device added	Details | Batch config
GT9022008001249	IG902	no device added	Details | Batch config
测试设备1	IR600		Details | Batch config
test	IR900		Details | Batch config
IR915-startup=config	IR600		Details | Batch config
IR915-running config	IR600	no device added	Details | Batch config

2. Select the device to which you want to deliver the configuration and click OK.



Select Devices

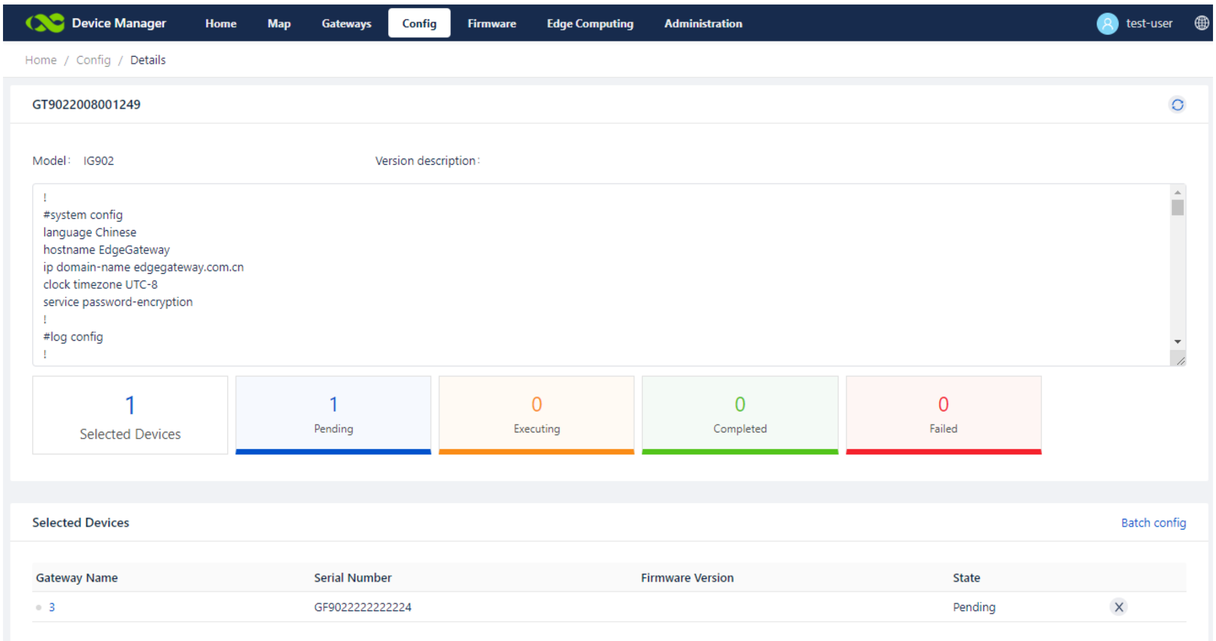
Gateway that has received the configuration file will be immediately updated and then rebooted to take effect.

	Gateway Name	Serial Number	Firmware Version
☑	GT9022008001249	GT9022008001249	1.0.0.r11628
□	3	GF9022222222224	
□	1	GF9022222222223	
□	testxy	GF9022222222222	
□	测试设	GF9021212121222	
□	IG900	GF9021212121212	

1 item selected Clear

Config Name
GT9022008001249
GT9022008001249
GT9022008001249
GT9022008001249
GT9022008001249
GT9022008001249
测试设备1
test
IR915-startup=config
IR915-running config

3. Return to the configuration list, click View details to view details of the current configuration, such as its update progress and status:



GT9022008001249

Model: IG902

Version description:

```
!
#system config
language Chinese
hostname EdgeGateway
ip domain-name edgegateway.com.cn
clock timezone UTC-8
service password-encryption
!
#log config
!
```

Selected Devices	Pending	Executing	Completed	Failed
1	1	0	0	0

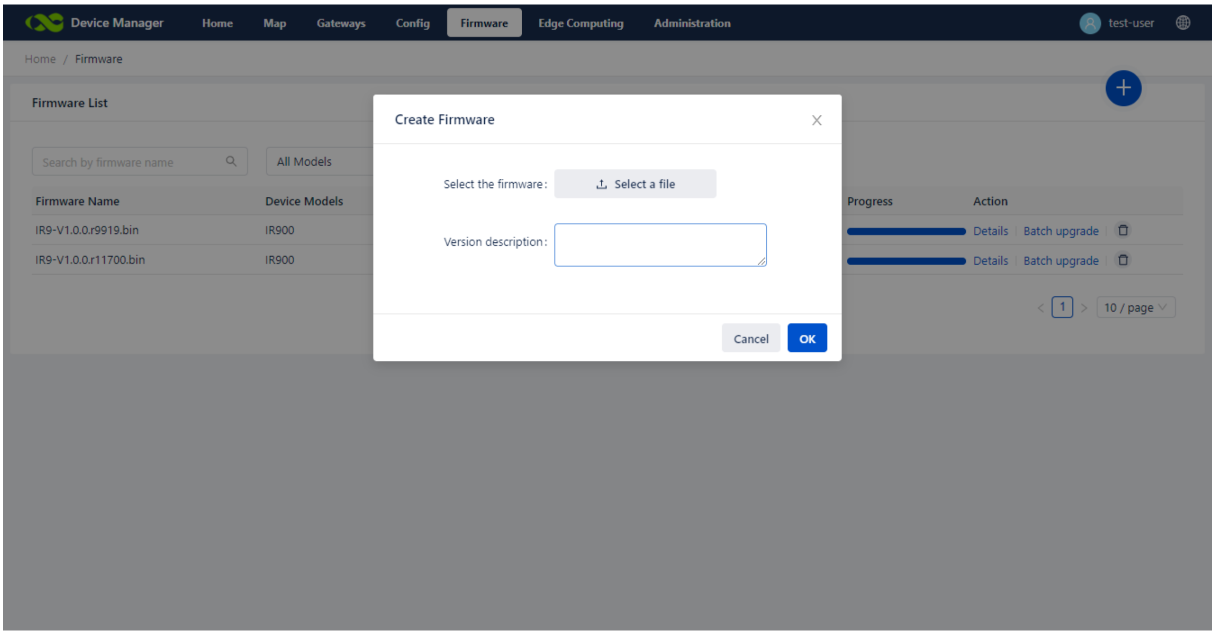
Selected Devices

Gateway Name	Serial Number	Firmware Version	State
3	GF9022222222224		Pending

6 Upgrade Gateway Firmware in Batches

When a large number of devices are connected to DM, it takes a great time to upgrade the firmware device by device. You can upgrade the firmware in batches through **Firmware**. The following describes the details:

1. Choose **Firmware** >> **+**. Select a gateway firmware and click OK.



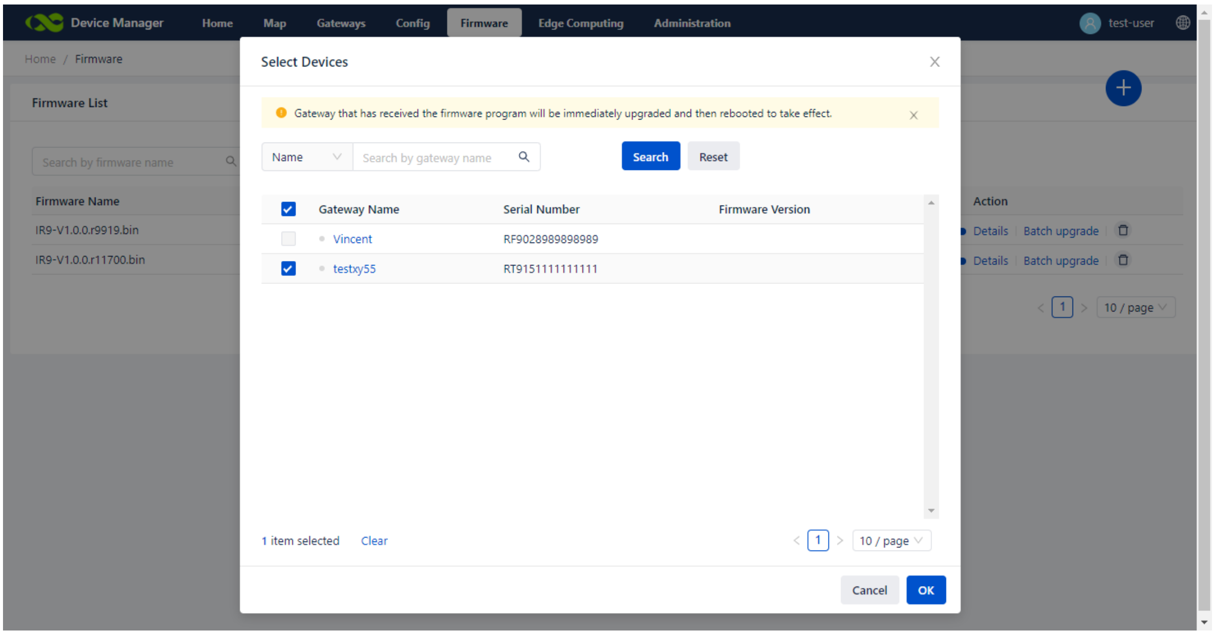
Firmware Name	Device Models	Progress	Action
IR9-V1.0.0.r9919.bin	IR900		Details | Batch upgrade
IR9-V1.0.0.r11700.bin	IR900		Details | Batch upgrade

Create Firmware

Select the firmware: Select a file

Version description:

2. Select the device for which you want to upgrade the firmware and click OK.



Select Devices

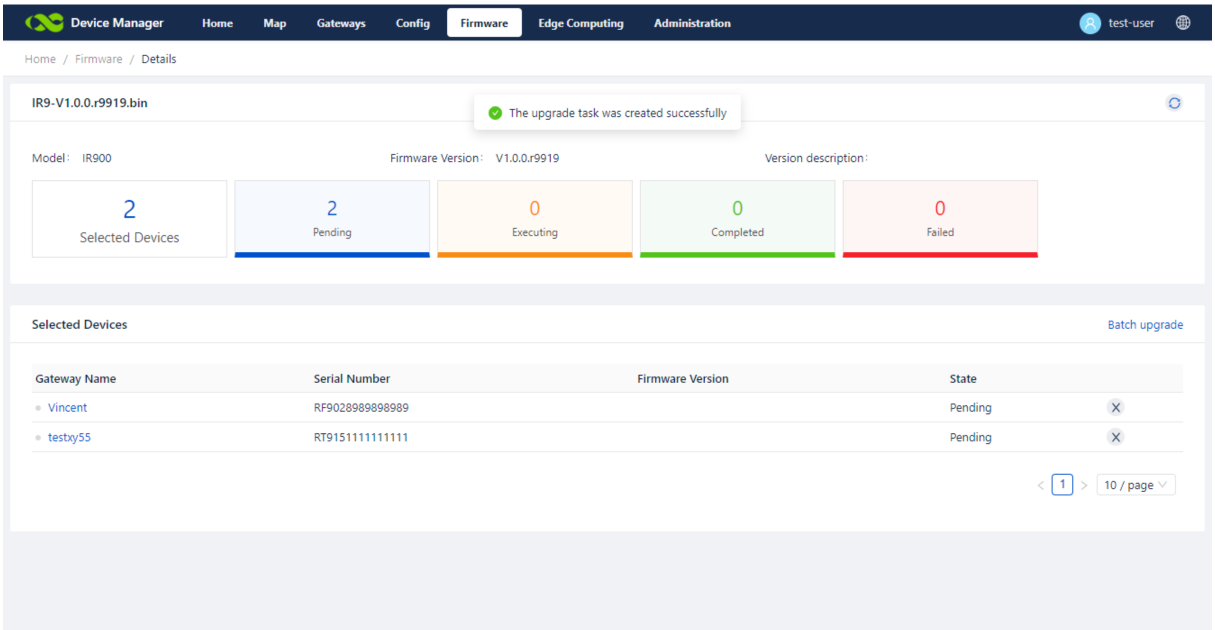
Gateway that has received the firmware program will be immediately upgraded and then rebooted to take effect.

☑	Gateway Name	Serial Number	Firmware Version
□	Vincent	RF9028989898989	
☑	testxy55	RT9151111111111	

1 item selected Clear

1 | 10 / page

3. Return to the firmware list, click **Details** to view the details of the current firmware, such as its upgrade progress and status:



IR9-V1.0.0.r9919.bin

The upgrade task was created successfully

Model: IR900 Firmware Version: V1.0.0.r9919 Version description:

2 Selected Devices | 2 Pending | 0 Executing | 0 Completed | 0 Failed

Selected Devices

Gateway Name	Serial Number	Firmware Version	State
Vincent	RF9028989898989		Pending
testxy55	RT9151111111111		Pending

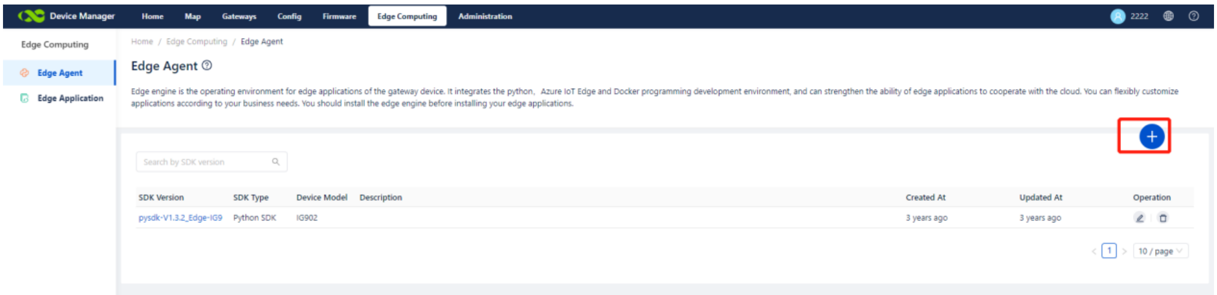
7 Edge Computing

As one of the core features of the Edge Gateway, edge computing function of DM platform are mainly applied to gateway devices with edge computing features of IG500, IG900, and VG series.

7.1 Edge Agent

Edge engine is the operating environment for edge applications of the gateway device. It integrates the python, Azure IoT Edge and Docker programming development environment, and can strengthen the ability of edge applications to cooperate with the cloud. You can flexibly customize applications according to your business needs. You should install the edge engine before installing your edge applications.

1. On the page of "Edge Agent": click "Add Edge Agent ", select the edge SDK from InHand Networks.

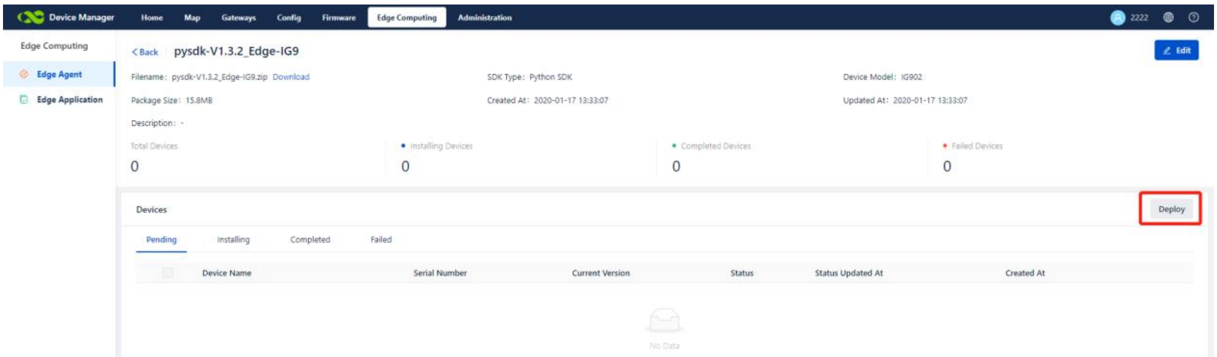


Edge Agent

Edge engine is the operating environment for edge applications of the gateway device. It integrates the python, Azure IoT Edge and Docker programming development environment, and can strengthen the ability of edge applications to cooperate with the cloud. You can flexibly customize applications according to your business needs. You should install the edge engine before installing your edge applications.

SDK Version	SDK Type	Device Model	Description	Created At	Updated At	Operation
pysdk-V1.3.2_Edge-IG9	Python SDK	IG902		3 years ago	3 years ago	

2. Then click “SDK Version" to view more information, click "Deploy" , select Gateways to install this SDK.
3. On the installation page, there displays the detailed progress status of each installation task, including "Pending" , "Installing" , "Completed", "Failed". For the failed task, you can view the failure reason in the task list.



pysdk-V1.3.2_Edge-IG9

Filename: pysdk-V1.3.2_Edge-IG9.zip Download | SDK Type: Python SDK | Device Model: IG902

Package Size: 15.8MB | Created At: 2020-01-17 13:33:07 | Updated At: 2020-01-17 13:33:07

Description: -

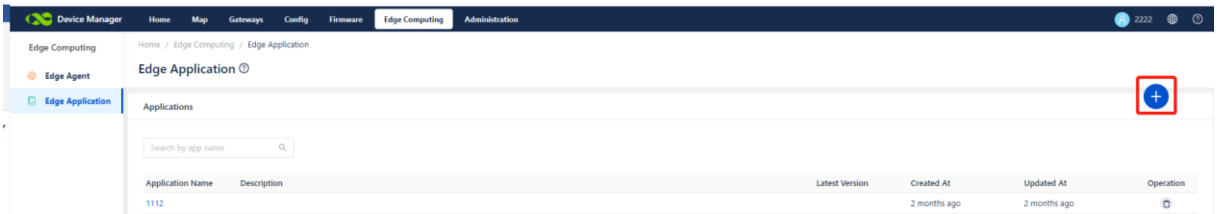
Total Devices	Installing Devices	Completed Devices	Failed Devices
0	0	0	0

Devices

	Device Name	Serial Number	Current Version	Status	Status Updated At	Created At

7.2 Edge Application

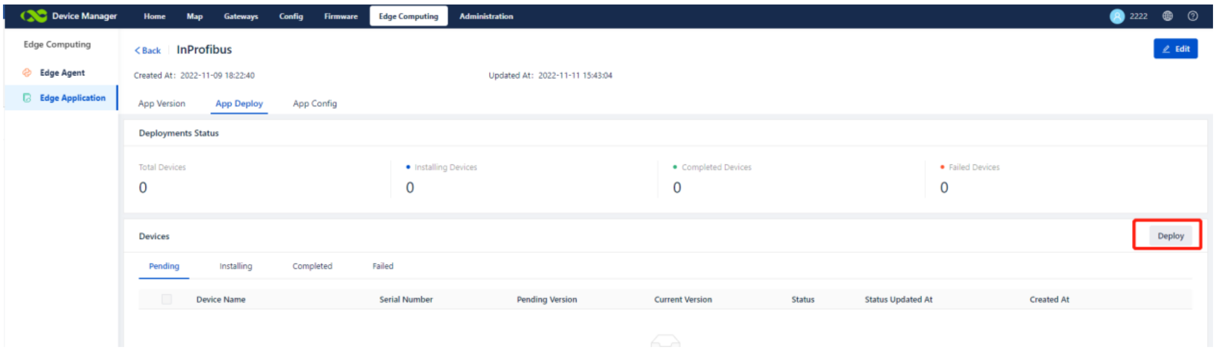
1. Click "Add Applications ", import the APP you want to install.



Application Name	Description	Latest Version	Created At	Updated At	Operation
1112			2 months ago	2 months ago	🗑

2. Then click "Application Name" to view the details. If you have a version update, you can also upload a new version here.

3. Click "App Deploy", Select "Deploy", select the required device, the system will automatically send the APP to these devices to make upgradation. On the installation page, there displays the detailed progress status of each installation task, including "Pending" , "Installing" , "Completed", "Failed". For the failed task, you can view the failure reason in the task list.



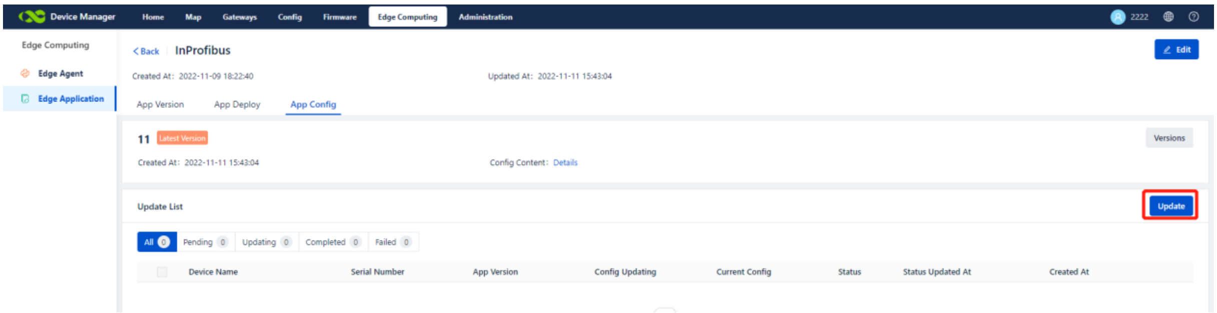
InProfibus

Created At: 2022-11-09 18:22:40 | Updated At: 2022-11-11 15:43:04

Total Devices	Installing Devices	Completed Devices	Failed Devices
0	0	0	0

	Device Name	Serial Number	Pending Version	Current Version	Status	Status Updated At	Created At

4. Click "App Config", maintain the app configuration or view the configuration details and the update records of the gateway configuration in detail.



InProfibus

Created At: 2022-11-09 18:22:40 | Updated At: 2022-11-11 15:43:04

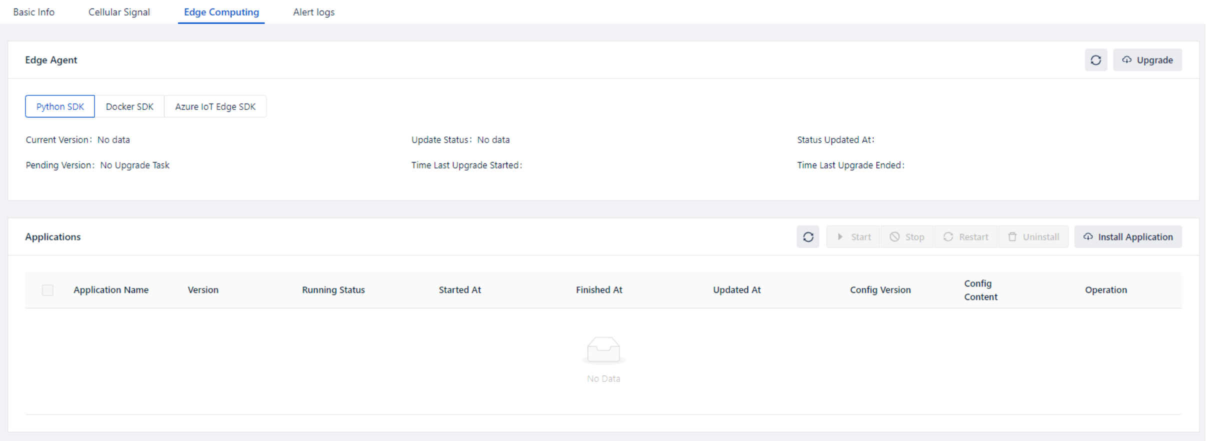
11

Created At: 2022-11-11 15:43:04 | Config Content: Details

	Device Name	Serial Number	App Version	Config Updating	Current Config	Status	Status Updated At	Created At

7.3 Gateway Details

1. In the details of a gateway with edge features, you can also view the current status of the device's SDK and APP installation history.
2. You can directly update the SDK and APP of a single gateway in the gateway details. The updated SDK and APP need to be added in the "Edge Agent" and "Edge Application" in advance.



Current Version: No data

Update Status: No data

Status Updated At:

Pending Version: No Upgrade Task

Time Last Upgrade Started:

Time Last Upgrade Ended:

Application Name	Version	Running Status	Started At	Finished At	Updated At	Config Version	Config Content	Operation

No Data

8 System Management

8.1 User

8.1.1 Add a User

To manage devices through multiple users, you can add multiple accounts in the Users list, and grant different roles and permissions to different accounts for permission security control.

The system roles and their permissions are as follows:

Function Page		Organization Manager	Device Manager	Device Monitor
Home		✓		
Map		✓	✓	✓
Gateways	Gateways	✓	✓	✓
	Groups	✓	✓	✓
	Tasks	✓	✓	✓
	Ststistics	✓	✓	✓
Config		✓	✓	
Firmware		✓	✓	
Edge Computing	Edge Agent	✓		
	Edge Application	✓		
Administration	Users	✓		

	Access Control	✓		
	Company Info	✓		
	Operation Log	✓		

The operation is described below:

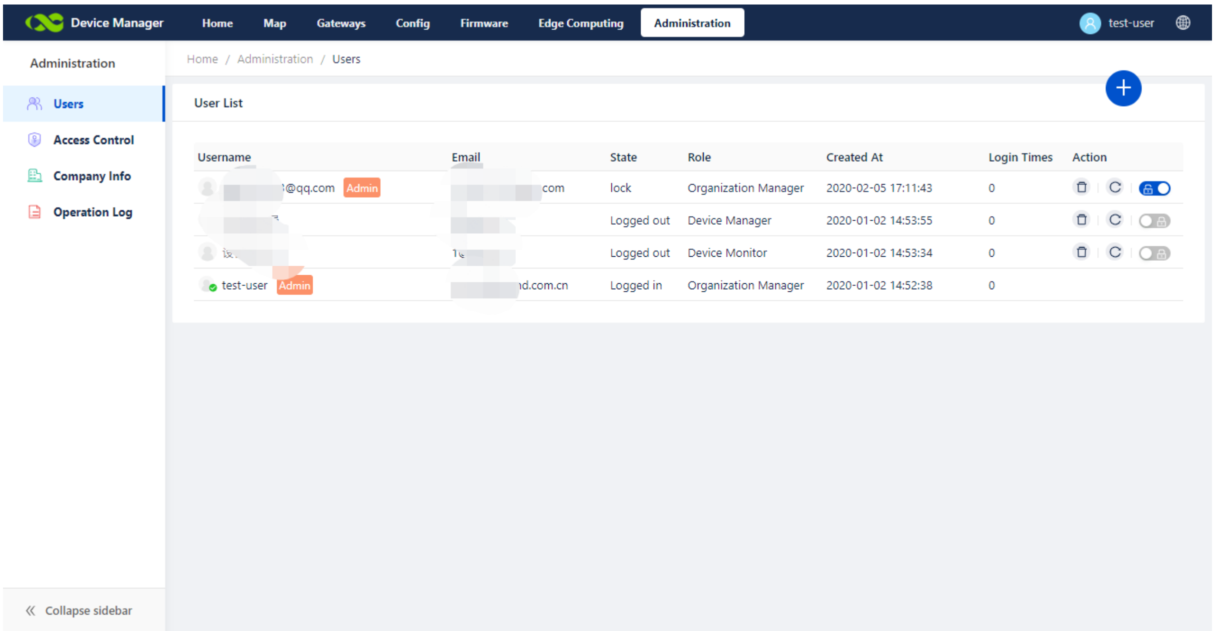
Choose **Administration** >> **Users** >> **+**, and add a user. The system automatically sends the password to the email account of the new user. The new user can use the email account and the password in the email to log in to DM.

8.1.2 Delete a User, Reset User Password, and Lock a User

Delete user: It is used to delete a user.

Reset password: It is used to reset the password for a user. The new password is sent to the login email account of the reset user through email.

Lock user: After a user is locked, it cannot log in to DM.



User List

Username	Email	State	Role	Created At	Login Times	Action
[redacted]@qq.com Admin	[redacted]com	lock	Organization Manager	2020-02-05 17:11:43	0	
[redacted]	[redacted]	Logged out	Device Manager	2020-01-02 14:53:55	0	
[redacted]	[redacted]	Logged out	Device Monitor	2020-01-02 14:53:34	0	
test-user Admin	[redacted]d.com.cn	Logged in	Organization Manager	2020-01-02 14:52:38	0	

8.2 Access Control

When the system has multiple users and devices, for secure device management and control, you can grant the management permissions of gateway devices for each user in the **Access Control** list.

The **Access Control** module is used to divide the users' permission to view and manage gateway devices. It allows you to customize multiple permission group and the gateway devices in each permission group can only be viewed and managed by users in the current group.

Example:

The user A has 120 devices, 50 in Beijing and 50 in Chengdu. Two persons are required to manage these devices separately, wherein Zhang San just manages the 50 devices in Beijing, while Li Si just manages the 50 devices in Chengdu.

Procedure:

The user creates two permission groups on the **Access Control** page, places Zhang San and the 50 devices in Beijing in one permission group, and places Li Si and the 50 devices in Chengdu in the other permission group. And places the left 20 devices in another permission group.

Specific functions:

1. New non-admin users are grouped into "Unallocated" by default. And they can vie all ungrouped devices by default.

2. The newly added devices are grouped into "Unallocated" by default, and all users can view them.

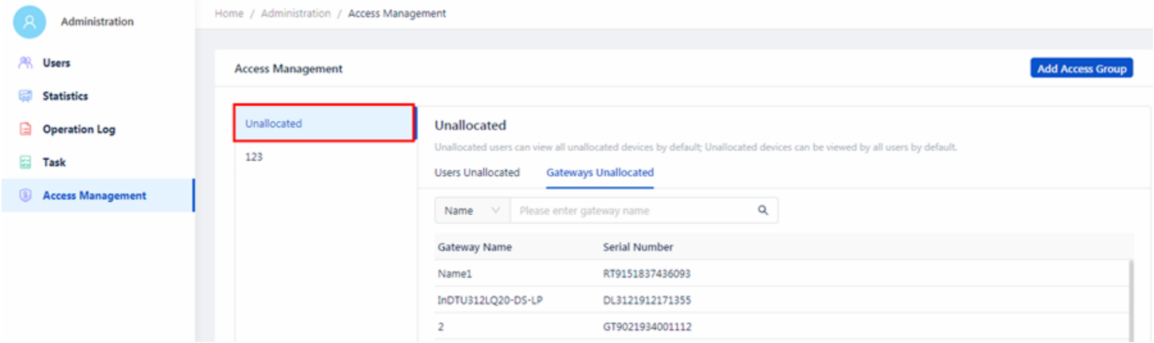
3. Users in unallocated can view all unallocated devices.

4. Users in a self-built group can view the devices in the current group and the devices in the "unallocated" group.

5. The organization administrator (admin) does not participate in the permission grouping, and can view all device data.

6. A user can be divided into multiple groups.

7. A device can only be divided into one group.



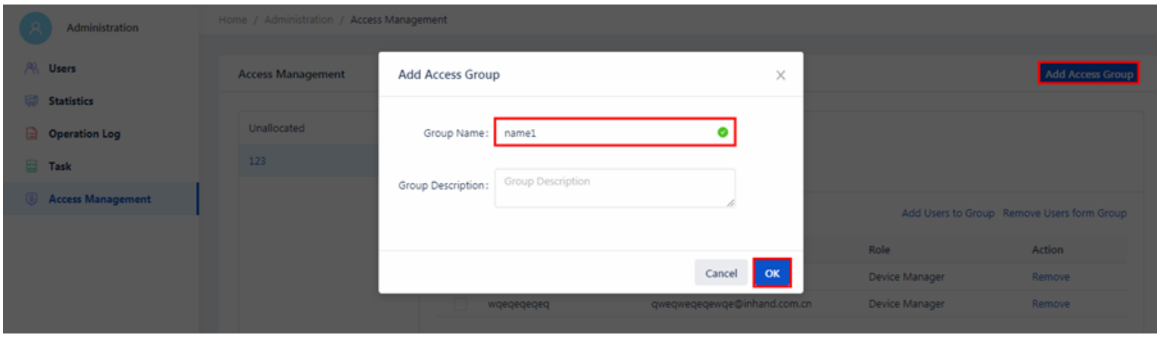
Unallocated

Unallocated users can view all unallocated devices by default; Unallocated devices can be viewed by all users by default.

Gateway Name	Serial Number
Name1	RT9151837436093
InDTU312LQ20-DS-LP	DL3121912171355
2	GT9021934001112

1. Create a permission group.

Step 1: Choose **Access Control** >> **Add Access Group**. Enter a name for the permission group and click OK.



Add Access Group

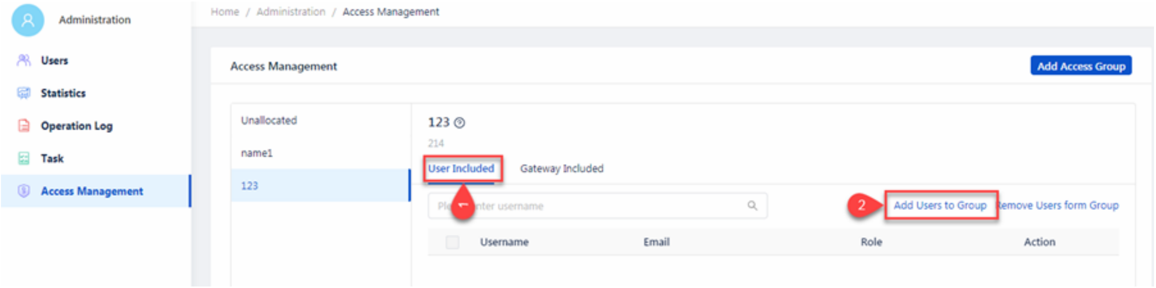
Group Name: name1

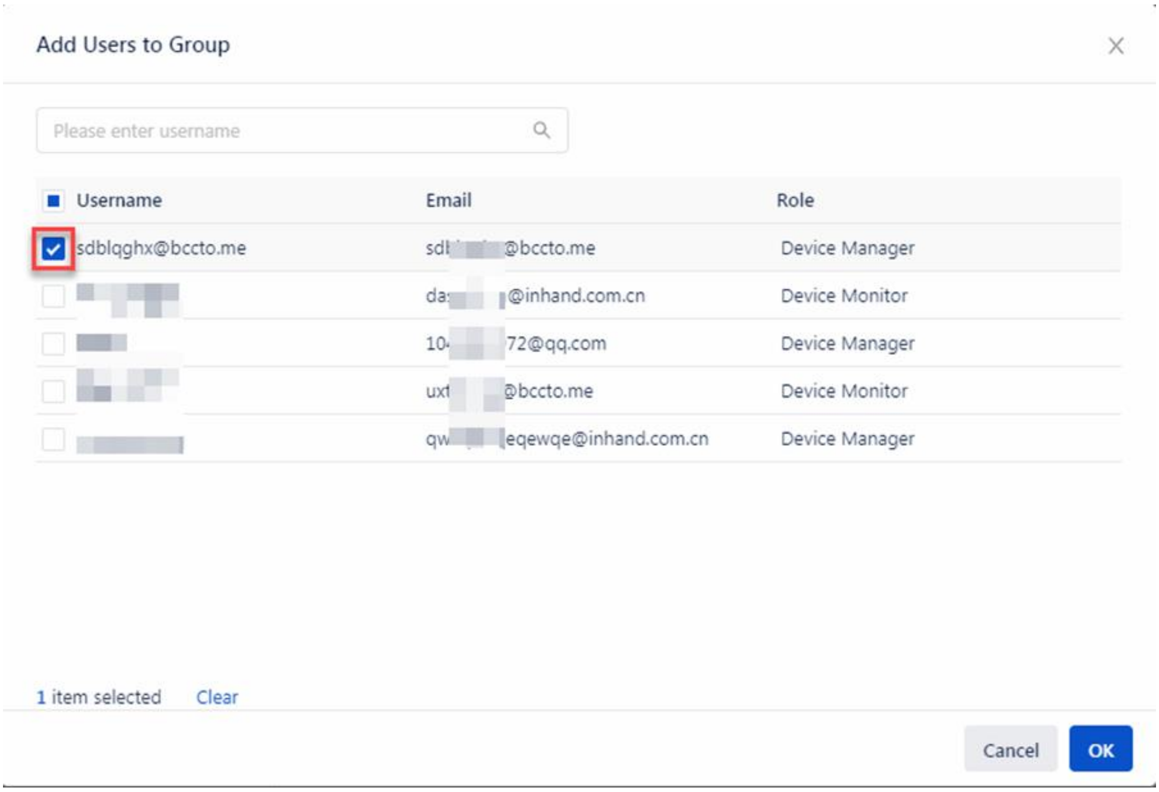
Group Description: Group Description

		Role	Action
		Device Manager	Remove
wqeqeqeqeq	qweqweqeqewqe@inhand.com.cn	Device Manager	Remove

Step 2: Allocate users for the created permission group.

Choose **User Included** >> **Add Users to Group**, select users, and then click OK.

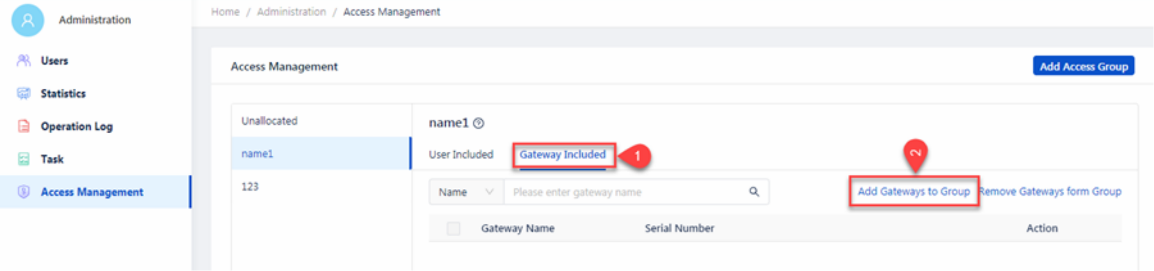


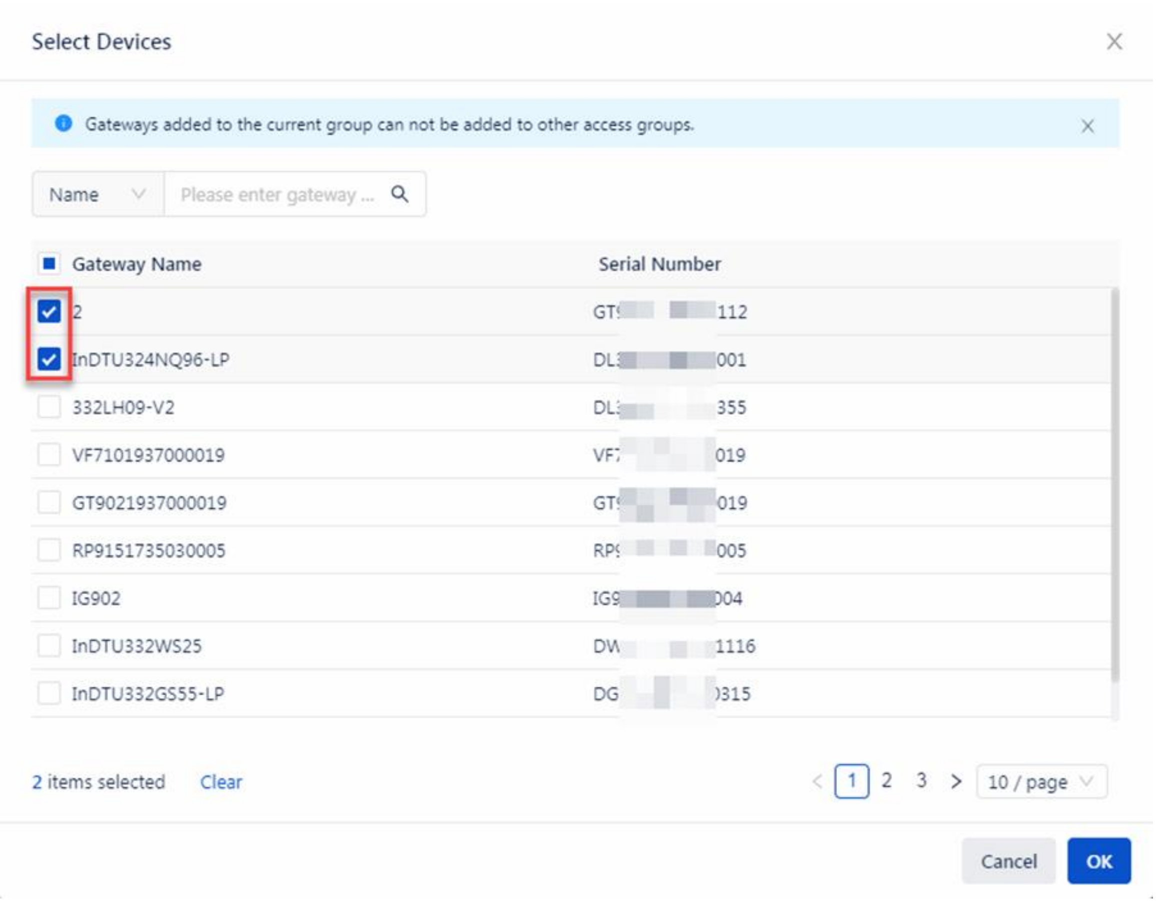


☐	Username	Email	Role
☑	sdblqghx@bccto.me	sd[redacted]@bccto.me	Device Manager
☐	[redacted]	da[redacted]@inhand.com.cn	Device Monitor
☐	[redacted]	10[redacted]72@qq.com	Device Manager
☐	[redacted]	ux[redacted]@bccto.me	Device Monitor
☐	[redacted]	qw[redacted]eqewqe@inhand.com.cn	Device Manager

Step 3: Allocate gateways to the created permission group.

Choose **Gateway Included** >> **Add Gateways to Group**, select gateways, and then click OK. Then, the permission is created. Devices in the permission group can only be viewed and managed by users in this permission group.





Select Devices

Gateways added to the current group can not be added to other access groups.

Name | Please enter gateway ...

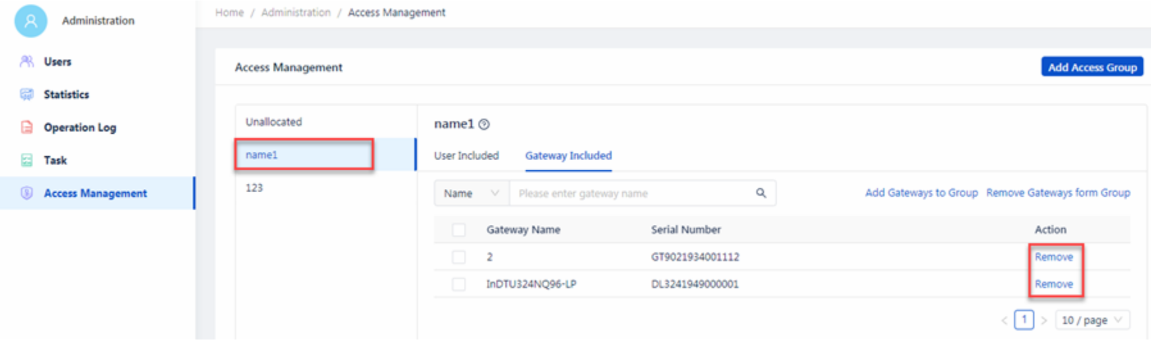
■	Gateway Name	Serial Number
☑	2	GT[redacted]112
☑	InDTU324NQ96-LP	DL[redacted]001
□	332LH09-V2	DL[redacted]355
□	VF7101937000019	VF[redacted]019
□	GT9021937000019	GT[redacted]019
□	RP9151735030005	RP[redacted]005
□	IG902	IG[redacted]004
□	InDTU332WS25	DW[redacted]1116
□	InDTU332GS55-LP	DG[redacted]315

2 items selected Clear

< 1 2 3 > 10 / page

Cancel OK

2. When you need to modify users and devices in a permission group after permissions have changed, select a permission group, remove one or multiple devices or users from the permission group and then add some devices or users to the permission group.



Home / Administration / Access Management

Administration

Users

Statistics

Operation Log

Task

Access Management

Access Management

Add Access Group

Unallocated

name1

123

name1

User Included Gateway Included

Name | Please enter gateway name

Add Gateways to Group Remove Gateways form Group

□	Gateway Name	Serial Number	Action
□	2	GT9021934001112	Remove
□	InDTU324NQ96-LP	DL3241949000001	Remove

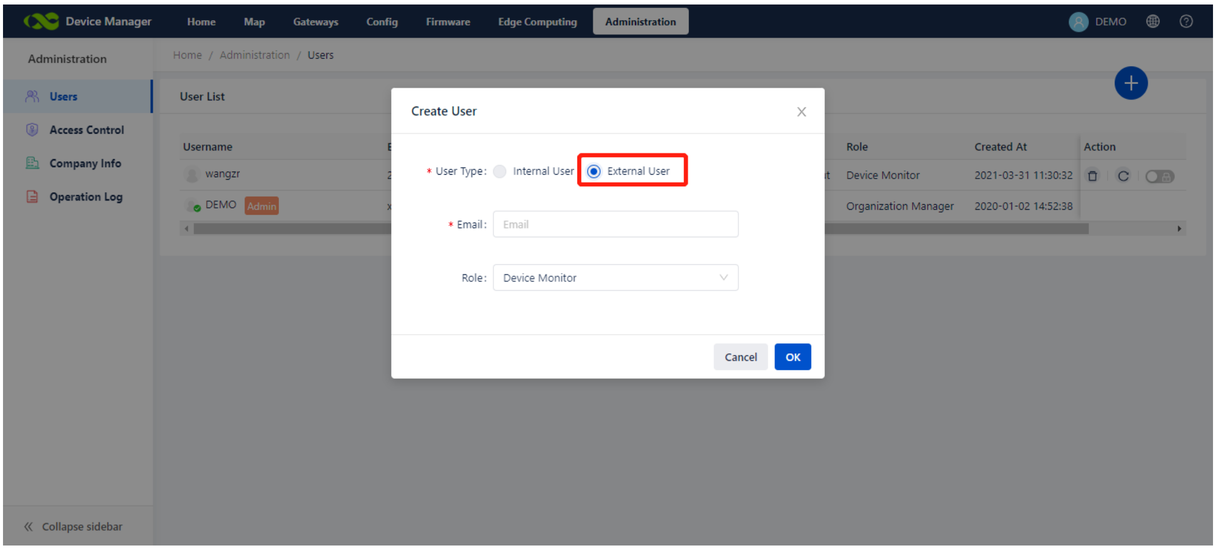
< 1 > 10 / page

⚠ Caution

New gateway devices and users are in the state of **Unallocated** by default, that is, new gateways can be viewed by all users and new users can view all unallocated gateway devices by default. Therefore, after creating a user or gateway device, grant permissions for the user and gateway as soon as possible.

8.3 Switch Organization

When you need an company external user to join your organization to provide external support, if the external user has registered an email account in DM, you can invite him to join your current organization by adding it as a "external user".



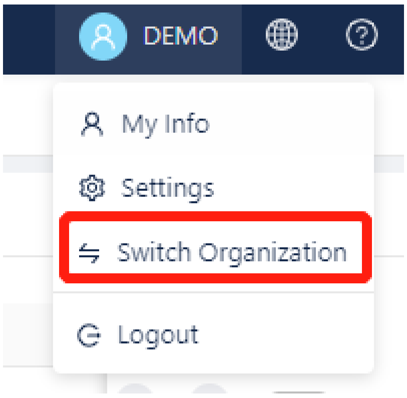
Username	Role	Created At	Action
wangzr	Device Monitor	2021-03-31 11:30:32	
DEMO Admin	Organization Manager	2020-01-02 14:52:38	

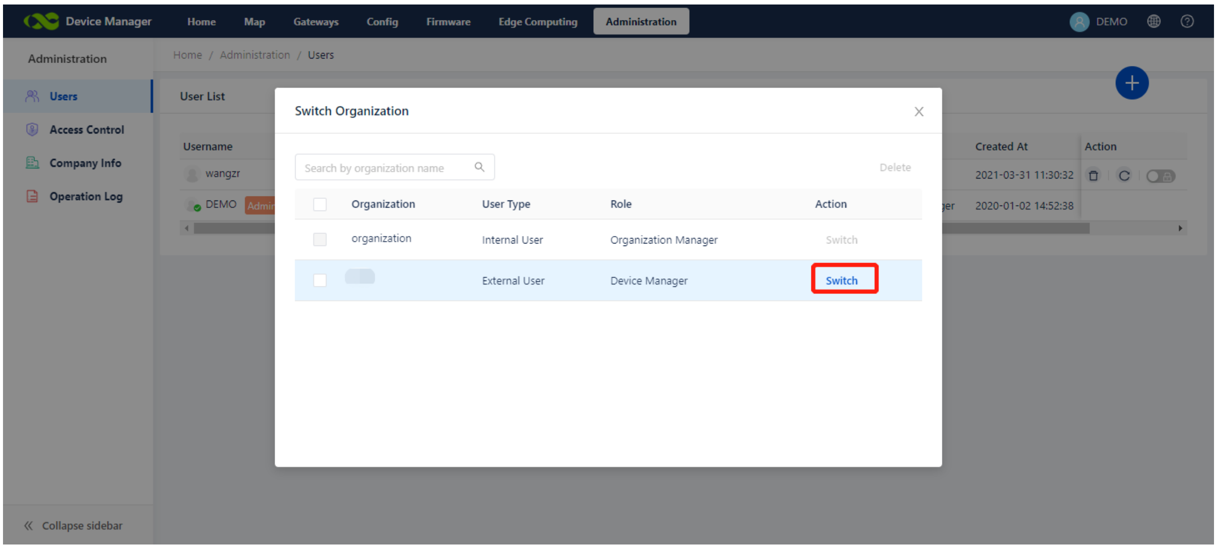
* User Type: ○ Internal User ● External User

* Email: Email

Role: Device Monitor

On the **Administration->Users** page, click add and select “**User Type**” as “**External User**”, fill in the email address of the external user and submit your input. Then an invitation email will be sent to this email. External users can join your current organization after accepting the invitation. At the same time, they can switch between multiple organizations in the personal center of their accounts:





□	Organization	User Type	Role	Action
□	organization	Internal User	Organization Manager	Switch
□	[redacted]	External User	Device Manager	Switch

You can set user roles and add gateway permissions to this external user so that this external user can provide full technical support when accessing your organization without causing unnecessary data leakage.

8.4 Company Information

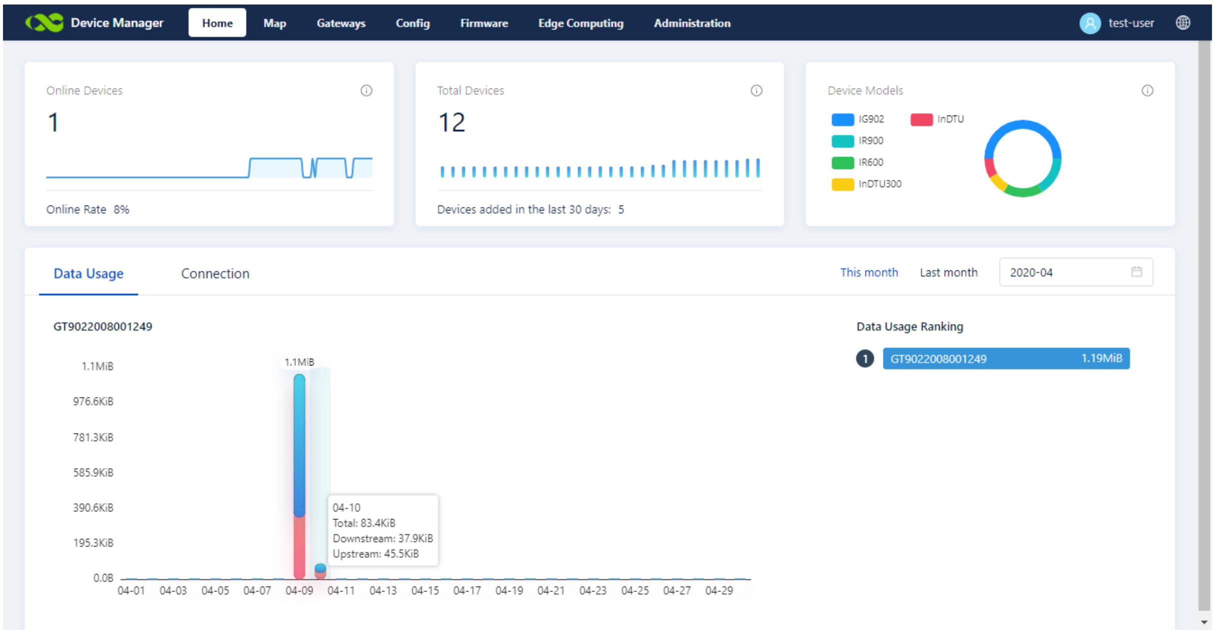
On the **Administration->Company Info** page, you can maintain the background information of the current account’s owner.

8.5 System Logs

On the **Administration->Logs** page, you can view system records about user login, device operation, firmware upgrade, and other information of the platform.

9 DashBoard

On the **Home** page of DM, recent running status of gateway devices and system device information are displayed by charts:



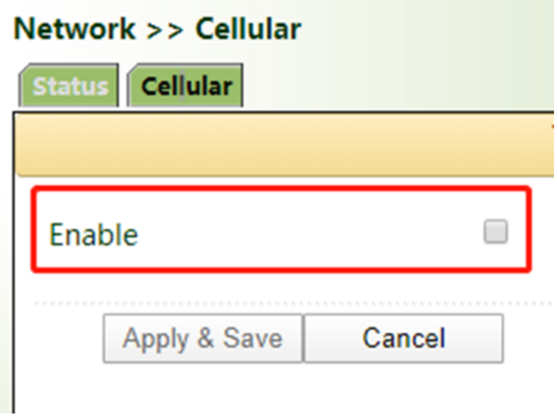
10 Appendix How to Connect Device to Network

Taking IR915 as an example, devices can be connected to the network in any of three ways: Ethernet (wired), SIM card, and Wi-Fi.

For more information about other networking methods, see the hardware user manual or visit the official website of InHand:

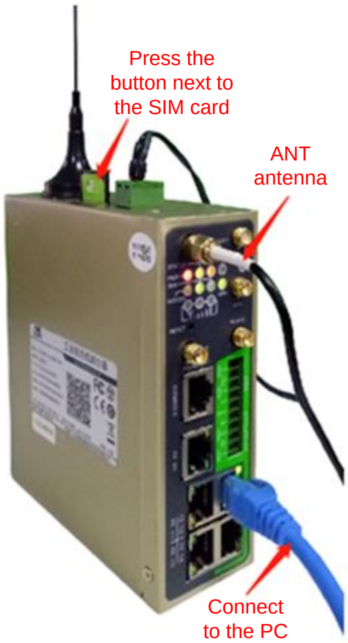
https://www.inhandnetworks.com/

Disable the "cellular interface" when accessing the network without the SIM card; otherwise repeated dial-up is performed, interfering the network connection.



10.1 Method 1: Access the network through dial-up or SIM cad

Step 1: Insert the SIM card to the slot 1 and tighten the 4G LTE antenna to the ANT terminal. Connect the network cable to a PC and connect to the power supply.

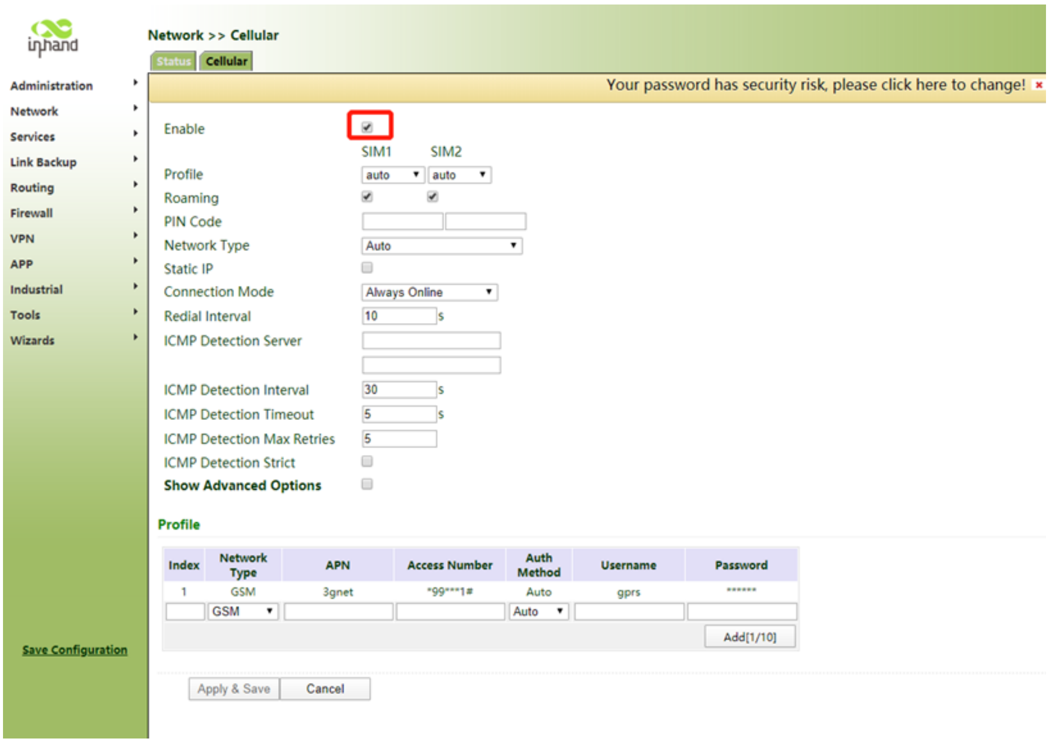


Caution

Note: When inserting or removing the SIM card, you must disconnect the device from the power supply to avoid data loss or damage to the device.

Step 2: Open the browser and log in to the web page of the device. (See Method 2: Ethernet.)

Step 3: Choose **Network** >> **Cellular** >> **Enable**, and then click Apply & Save.



Your password has security risk, please click here to change!

Enable ☑

	SIM1	SIM2
Profile	auto	auto
Roaming	☑	☑
PIN Code		

Network Type: Auto

Static IP: □

Connection Mode: Always Online

Redial Interval: 10 s

ICMP Detection Server:

ICMP Detection Interval: 30 s

ICMP Detection Timeout: 5 s

ICMP Detection Max Retries: 5

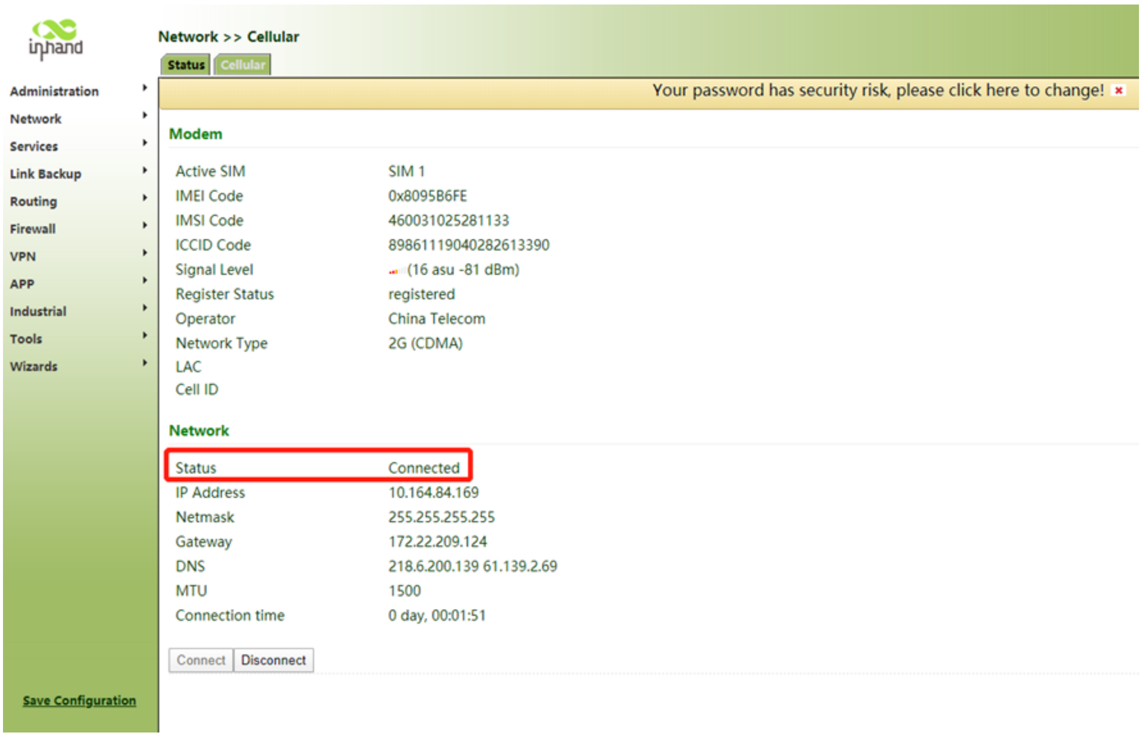
ICMP Detection Strict: □

Show Advanced Options: □

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99***1#	Auto	gprs	******
	GSM			Auto		

Step 4: Wait until the network connection status is **Connected** and an IP address is allocated. Then, the network is connected through the SIM card.



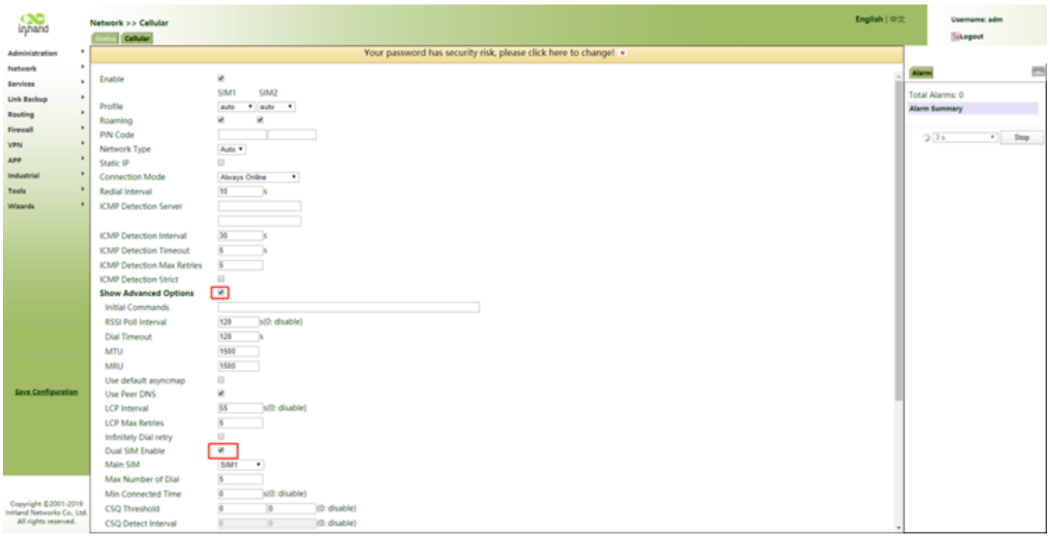
Modem

Active SIM	SIM 1
IMEI Code	0x8095B6FE
IMSI Code	460031025281133
ICCID Code	89861119040282613390
Signal Level	(16 asu -81 dBm)
Register Status	registered
Operator	China Telecom
Network Type	2G (CDMA)
LAC	
Cell ID	

Network

Status	Connected
IP Address	10.164.84.169
Netmask	255.255.255.255
Gateway	172.22.209.124
DNS	218.6.200.139 61.139.2.69
MTU	1500
Connection time	0 day, 00:01:51

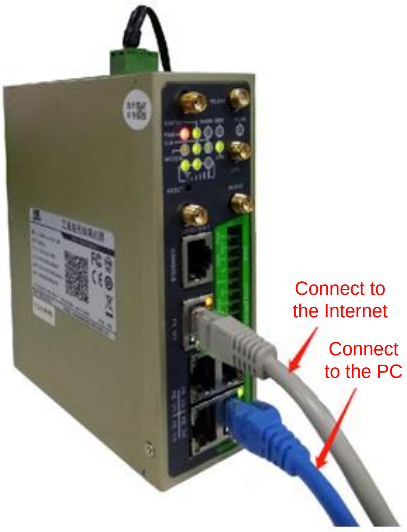
Step 5: For devices that support the dual-card mode and the SIM card is inserted to the slot 2, select **Dual SIM Enable**.



Enable	☑	
	SIM1	SIM2
Profile	auto	auto
Roaming	☑	☑
PIN Code		
Network Type	Auto	
Static IP	☐	
Connection Mode	Always Online	
Redial Interval	10 s	
ICMP Detection Server		
ICMP Detection Interval	30 s	
ICMP Detection Timeout	5 s	
ICMP Detection Max Retries	5	
ICMP Detection Strict	☐	
Show Advanced Options	☑	
Initial Commands		
RSSI Poll Interval	120 s(0: disable)	
Dial Timeout	120 s	
MTU	1500	
MRU	1500	
Use default asyncmap	☐	
Use Peer DNS	☑	
LCP Interval	55 s(0: disable)	
LCP Max Retries	5	
Infinitely Dial retry	☐	
Dual SIM Enable	☑	
Main SIM	SIM1	
Max Number of Dial	5	
Min Connected Time	0 s(0: disable)	
CSQ Threshold	0	0 (0: disable)
CSQ Detect Interval	0	0 (0: disable)

10.2 Method 2: Ethernet

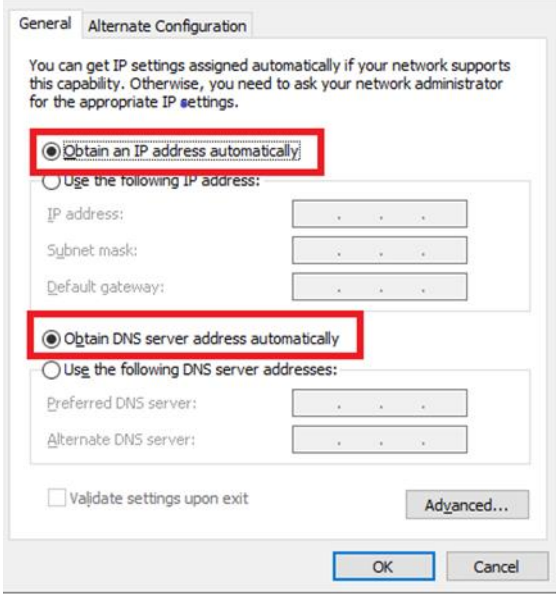
Step 1: Connect the power supply and network cable to the device, and connect the LAN (FE 1/1 or FE1/2 or FE1/3 or FE1/4) port to a PC and the WAN(FE0/1) port to the Internet.



Step 2: Set the IP addresses of the PC and gateway to be in the same network segment.

Method 1: Automatically get the IP address (recommended)

Method 2: Use a fixed IP address and set the PC and gateway to be in the same network segment. Set the initial IP address of the device to **192.168.2.1** and the subnet mask to **255.255.255.0**. Select **Use the following IP address**. Enter an IP address ranging from 192.168.2.2 to 192.168.2.254, a subnet mask 255.255.255.0, and the default gateway 192.168.2.1, and then click OK.



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

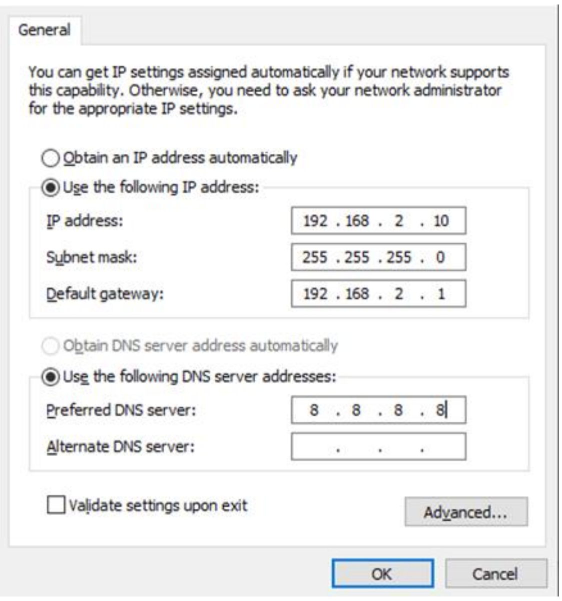
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Automatically get the IP address



General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

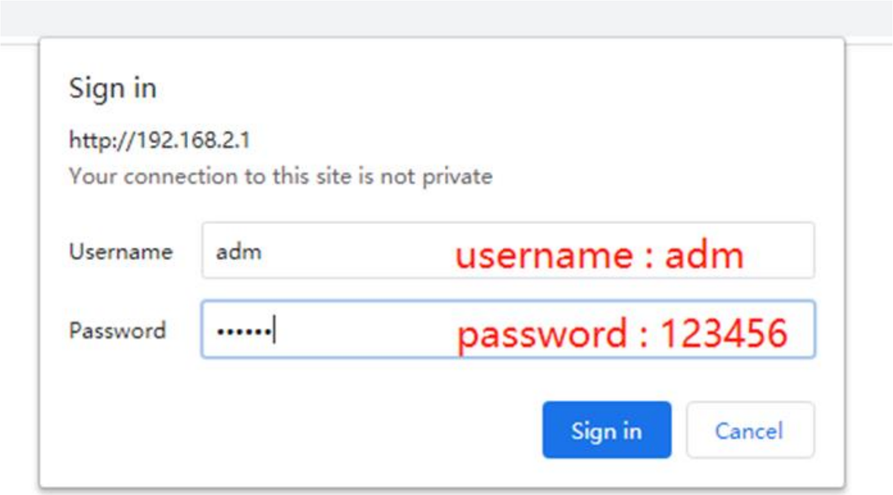
□ Validate settings upon exit

Use a fixed IP address

Step 3: In the address bar of the browser, enter the default device address **192.168.2.1** to enter the device web management page.

(If it prompts that the website is insecure, unfold the menu and click **Go Still**.)

Step 4: Log in to the device.



Sign in

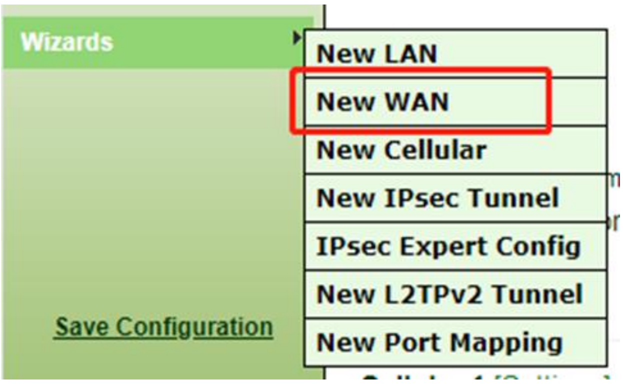
http://192.168.2.1

Your connection to this site is not private

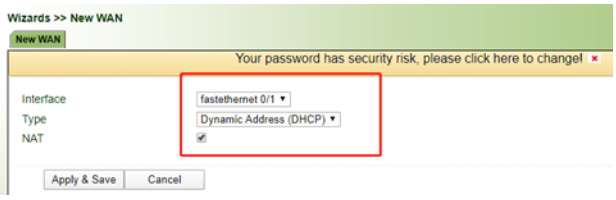
Username adm

Password ••••••

Step 5: Choose **Network** >> **New WAN**. Configure an IP address for the WAN port to connect the router to Internet.

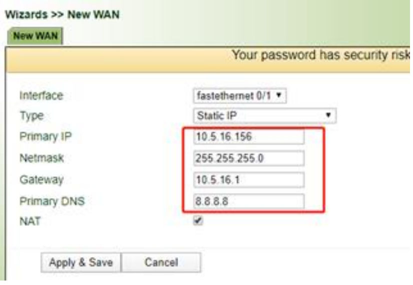


Step 6: We recommend that you select **Dynamic Address (DHCP)**. If you select **Static IP Address**, manually configure the network parameters, and then click Apply & Save.


Wizards >> New WAN
New WAN
Your password has security risk, please click here to change!
Apply & Save
Cancel

Interface: fastethernet 0/1
Type: Dynamic Address (DHCP)
NAT: ☑

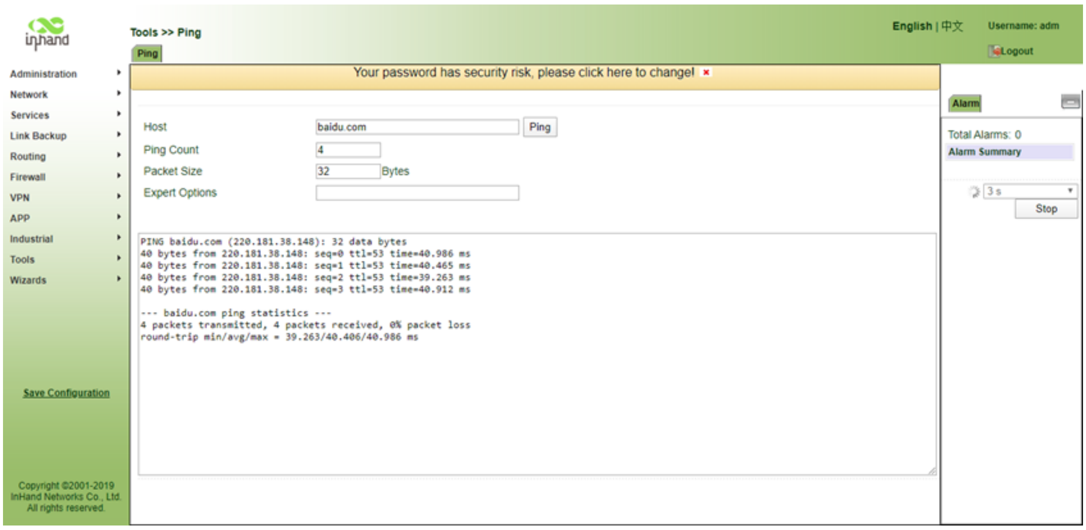
Dynamically allocate the IP address



Interface: fastethernet 0/1
Type: Static IP
Primary IP: 10.5.16.156
Netmask: 255.255.255.0
Gateway: 10.5.16.1
Primary DNS: 8.8.8.8
NAT: ☑

Configure parameters of the static IP address

Step 7: Choose **Tools** >> **Ping**. In the **Host** field, enter a common Chinese website to test whether the device can connect to the Internet. If data transmission is displayed, the device can connect to the Internet.



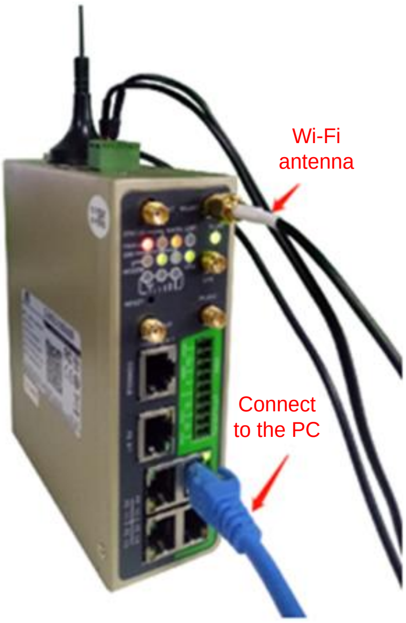
Host: baidu.com
Ping Count: 4
Packet Size: 32 Bytes
Expert Options:

```
PING baidu.com (220.181.38.148): 32 data bytes
40 bytes from 220.181.38.148: seq=0 ttl=53 time=40.986 ms
40 bytes from 220.181.38.148: seq=1 ttl=53 time=40.465 ms
40 bytes from 220.181.38.148: seq=2 ttl=53 time=39.263 ms
40 bytes from 220.181.38.148: seq=3 ttl=53 time=40.912 ms

--- baidu.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 39.263/40.406/40.986 ms
```

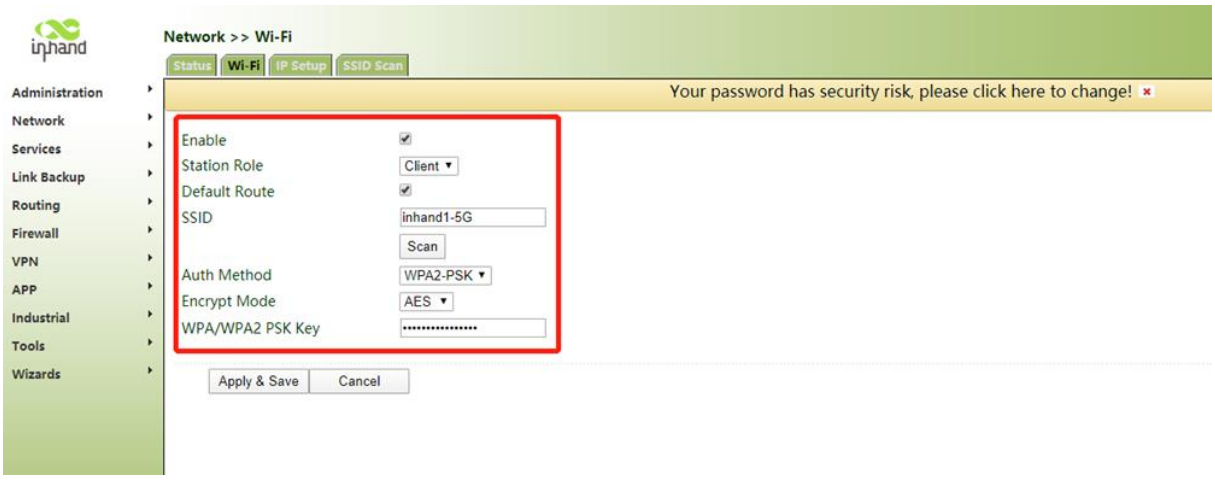
10.3 Method 3: Wi-Fi

Step 1: Connect the Wi-Fi antenna to the WLAN port and use a network cable to connect the PC and the power supply.



Step 2: Set the IP addresses of the PC and the gateway to be in the same network segment. On a browser, visit the web management page of the gateway. (See Ethernet).

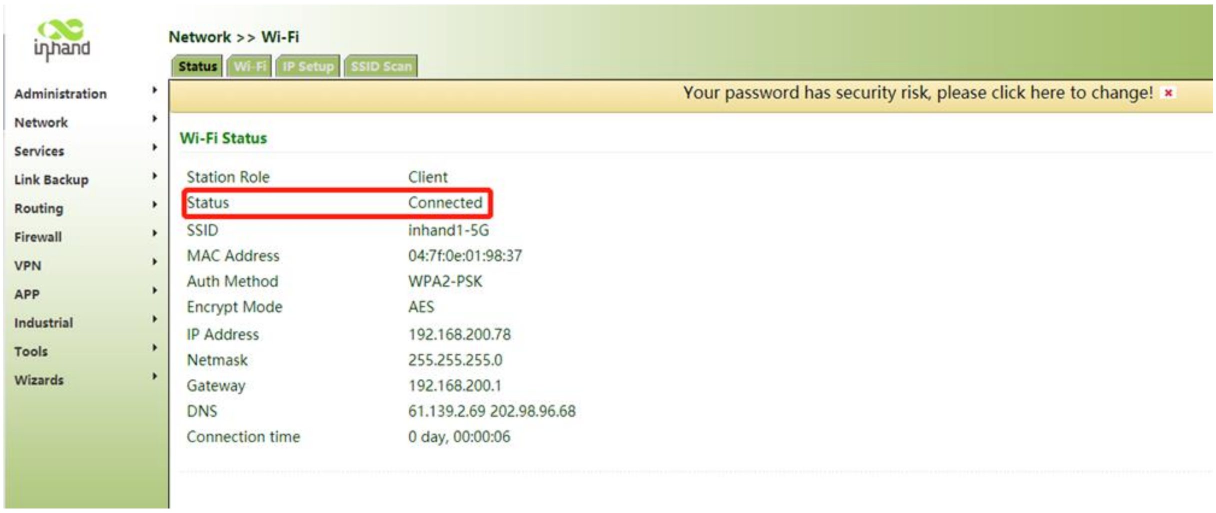
Step 3: Choose **Network** >> **WLAN**, enable the WLAN port, and configure the parameters.



Your password has security risk, please click here to change!

Enable	☑
Station Role	Client
Default Route	☑
SSID	inhand1-5G
Auth Method	WPA2-PSK
Encrypt Mode	AES
WPA/WPA2 PSK Key	•••••••••••••••

Step 4: Click the **Status** tab. The network connection status is **Connected**.

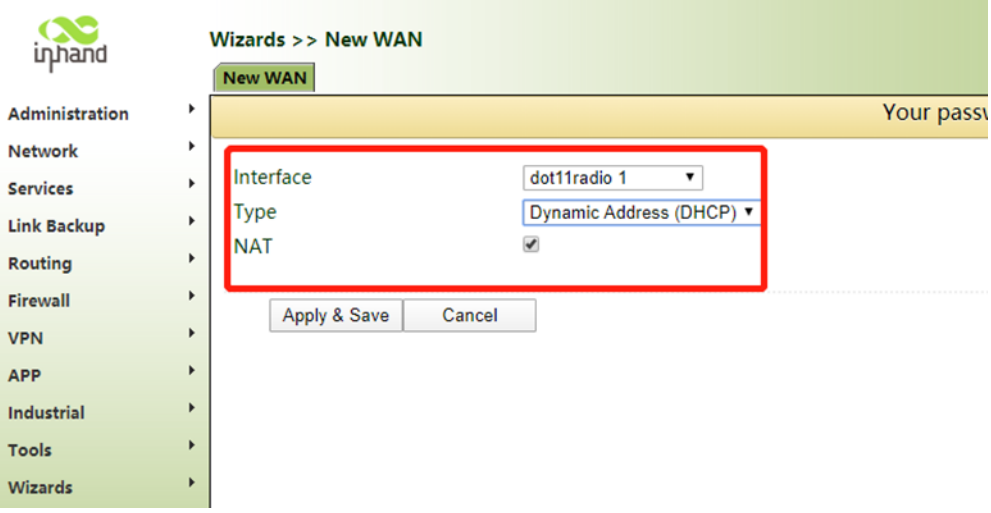


Your password has security risk, please click here to change!

Wi-Fi Status

Station Role	Client
Status	Connected
SSID	inhand1-5G
MAC Address	04:7f:0e:01:98:37
Auth Method	WPA2-PSK
Encrypt Mode	AES
IP Address	192.168.200.78
Netmask	255.255.255.0
Gateway	192.168.200.1
DNS	61.139.2.69 202.98.96.68
Connection time	0 day, 00:00:06

Step 5: Choose **Wizards** >> **New WLAN**, and configure the parameters.



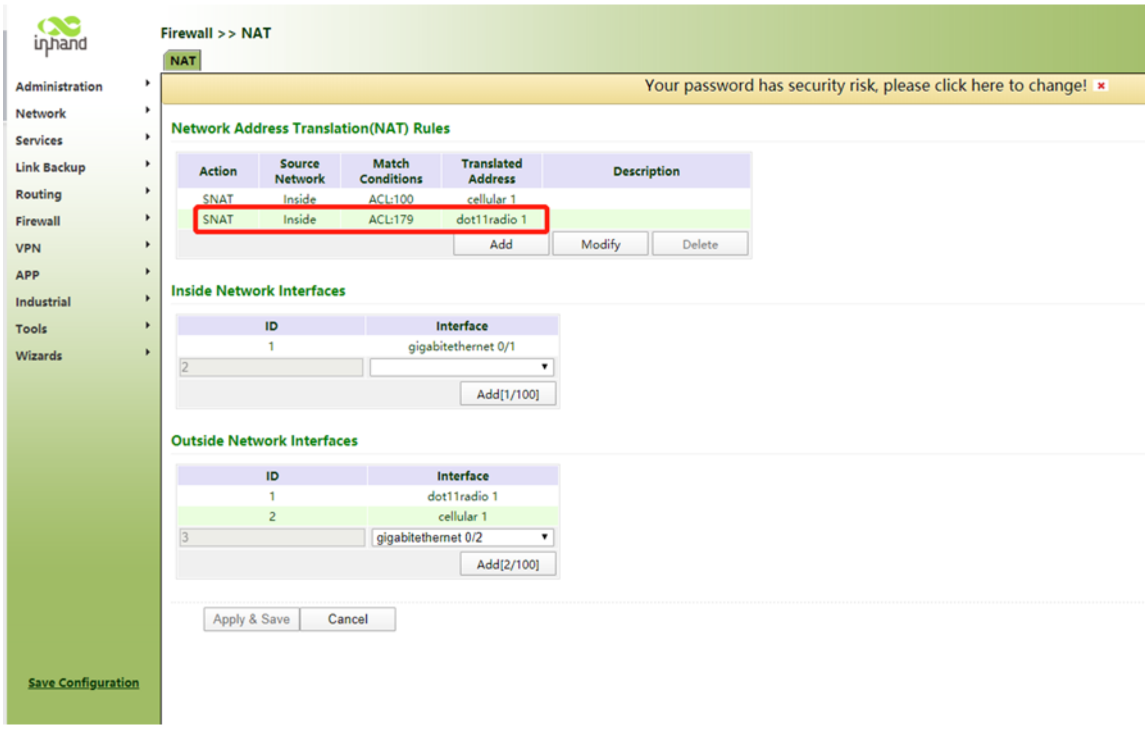
Wizards >> New WAN

New WAN

Your pass

Interface	dot11radio 1
Type	Dynamic Address (DHCP)
NAT	☑

Step 6: Choose **Firewall** >> **Network Address Translation (NAT)**. If a connection named dot11radio 1 is displayed, Wi-Fi is connected.



Firewall >> NAT

NAT

Your password has security risk, please click here to change!

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	dot11radio 1	

Inside Network Interfaces

ID	Interface
1	gigabitethernet 0/1
2	

Outside Network Interfaces

ID	Interface
1	dot11radio 1
2	cellular 1
3	gigabitethernet 0/2