



InHand Networks InConnect Service

"One-stop" Convenient Networking Service

User Manual

Issue: V3.2-2023

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

Declaration




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

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

Due to the continuous updating of products, information in this document cannot be completely consistent with actual products. The actual system functions shall prevail. InHand will update this document with the update of system functions. Please find the latest information in the official of InHand or the InConnect platform.

© 2019 InHand Networks. All rights reserved.

Conventions

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

Technical Support

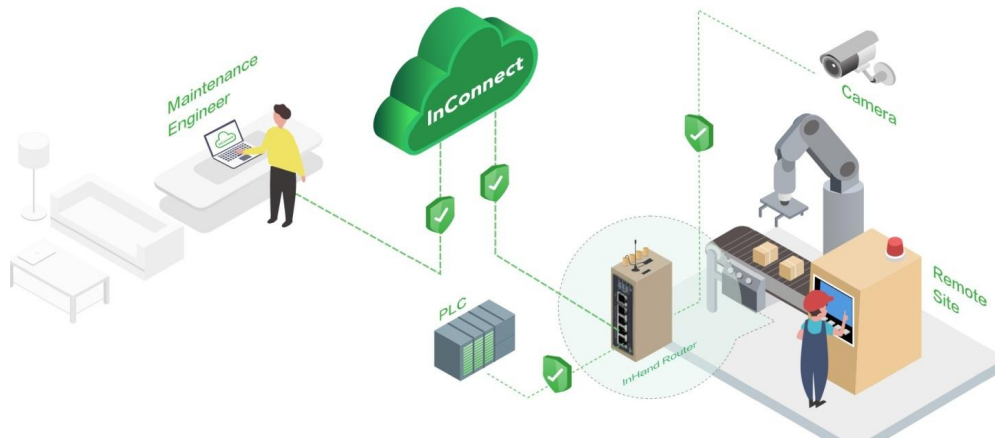
support@inhandnetworks.com

Contents

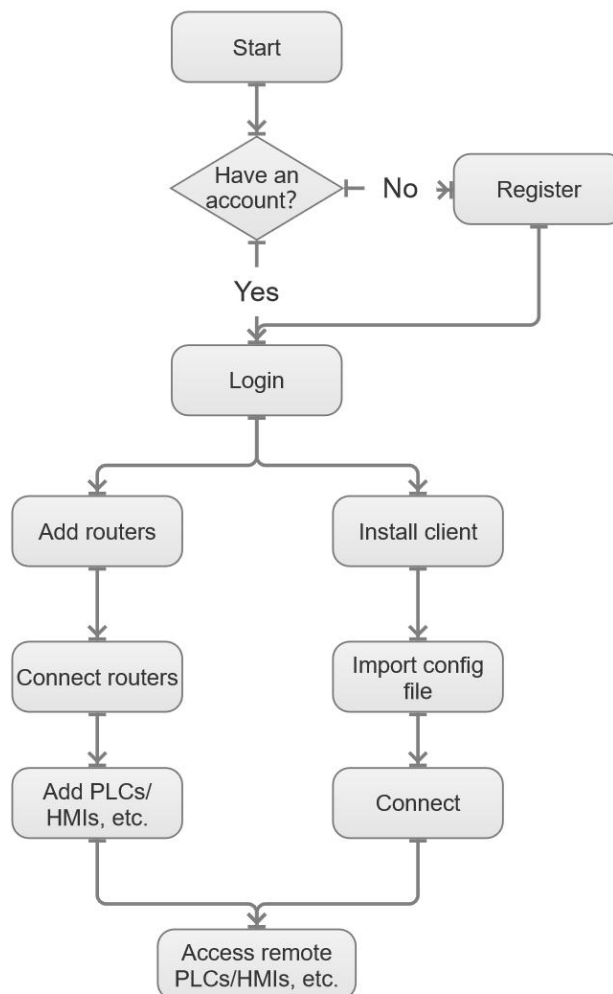
1. About InConnect	- 1 -
2. Registration and Login	- 2 -
3. Connecting a Router to InConnect	- 2 -
3.1. Adding the Router to InConnect	- 2 -
3.2. Connecting a Router to InConnect	- 4 -
3.2.1. IR300-Series Routers	- 4 -
3.2.2. IR600-Series Routers	- 5 -
3.2.3. IR900-Series Routers	- 6 -
3.2.4. IG500-Series Routers	- 7 -
3.2.5. IG900-Series Routers	- 8 -
3.2.6. VG710-Series Routers	- 9 -
3.3. Check the connection between the router and InConnect	- 10 -
4. Using the Client	- 10 -
4.1. Installing and Using OpenVPN in Windows	- 10 -
4.2. Installing and Using OpenVPN in Android	- 12 -
5. Connecting the Router's Downstream Devices	- 15 -
5.1. Access Through the Virtual IP Address	- 15 -
5.2. Access Through the Real IP Address	- 18 -
5.3. Access Through the Virtual IP Address and Real IP Address Simultaneously	- 20 -
6. Network Management	- 22 -
6.1. Configuring a Mesh Network	- 22 -
6.1.1. Adding a Mesh Network	- 22 -
6.1.2. Adding a Site or User to a Mesh Network	- 24 -
6.1.3. Deleting a Mesh Network	- 25 -
6.2. Configuring a Star Network	- 26 -
6.2.1. Adding a Star Network	- 27 -
6.2.2. Adding a Site or User to a Star Network	- 29 -
6.2.3. Deleting a Star Network	- 30 -
7. User Management	- 31 -
8. Router/Gateway Management	- 32 -
8.1. Router Details	- 32 -
8.2. Remote Web Management	- 33 -
8.3. Delivering the Connection Configuration	- 34 -
8.4. Remotely Updating the Router Configuration	- 34 -
8.5. Remotely Upgrading the Router Firmware	- 36 -
8.6. Tasks	- 37 -
9. Consumption	- 38 -
10. Billing	- 38 -
11. FAQs	- 39 -
12. Appendix: Router Networking	- 39 -
Method 1: Access the network through dial-up or SIM card	- 40 -
Method 2: Ethernet	- 41 -
Method 3: Wi-Fi	- 44 -

1. About InConnect

InHand Connect Service cloud platform (hereinafter referred to as InConnect) is a "one-stop" networking service provided for enterprise customers. It features user-friendly interface and simple operations. InConnect can be used together with InHand networking equipment highly recognized by global customers to help you quickly access global business outlets anytime anywhere, and achieve secure and stable interconnection of equipment and data exchange in different regions, promoting enterprise informatization construction and digital transformation.



How InConnect works:



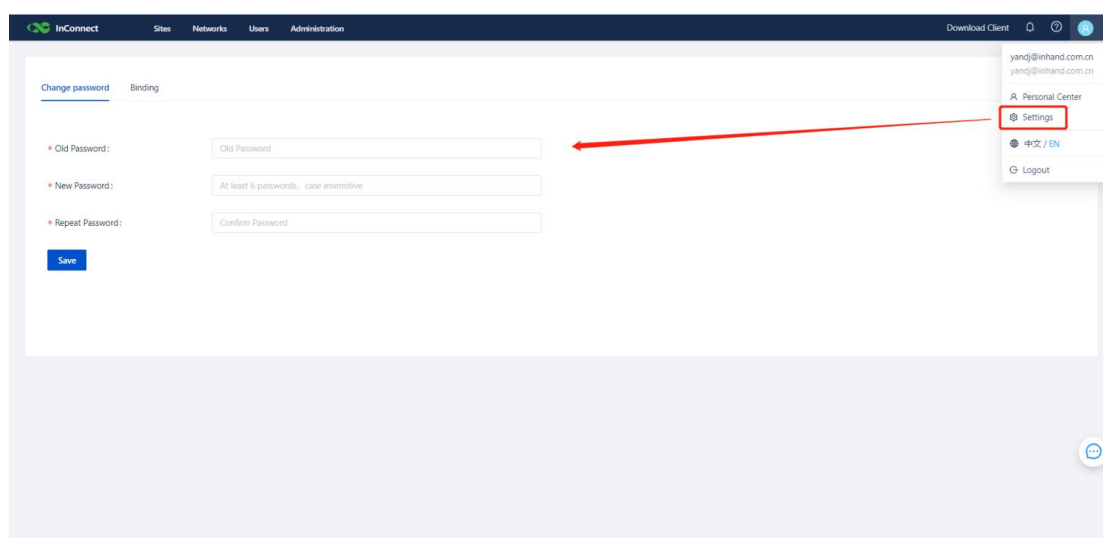
2. Registration and Login

1. Registration

In a browser, enter <https://ics.inhandnetworks.com> to access the registration page of InConnect. The Google Chrome browser is recommended.

2. Login

After successful registration, enter the email account used for registration and password to log in to InConnect. After login, **change the password** and **bind a mobile phone number** on the **Settings** page. Next time you can use the bound mobile phone number for login.



3. Connecting a Router to InConnect

After a router is added to InConnect, InConnect automatically delivers the running configuration to create a secure network connection. To connect a router to InConnect, perform the following steps:

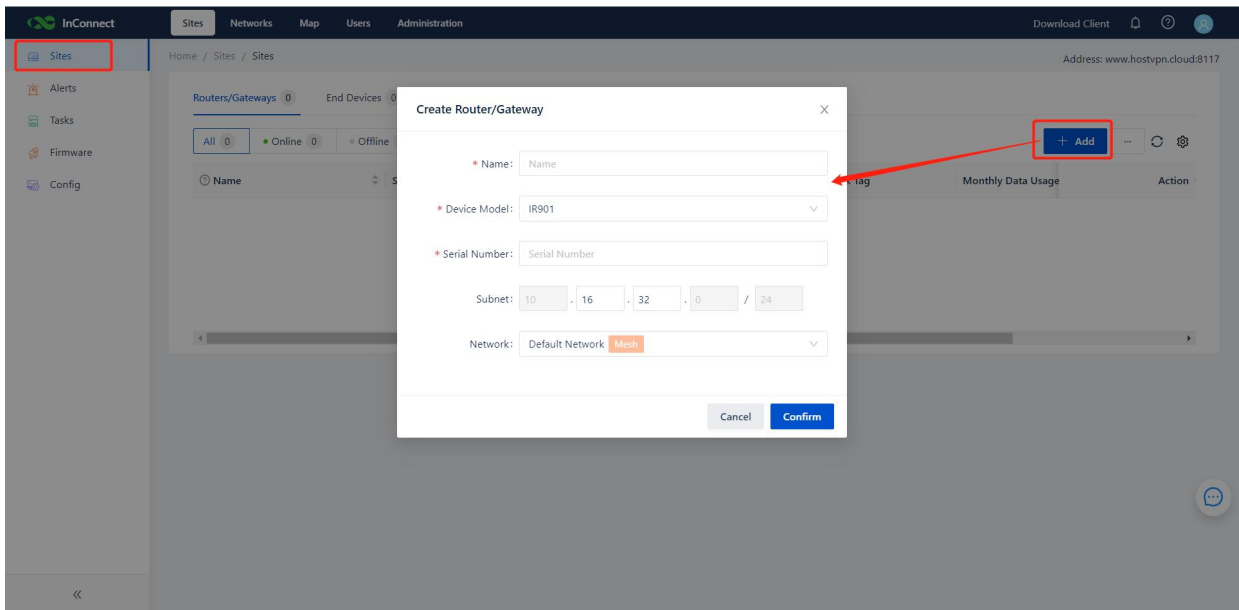
1. On the **Sites** page of InConnect, add the router.
2. On the web page of the router, connect the router to InConnect.
3. Check the connection between the router and InConnect.

The details are described below.

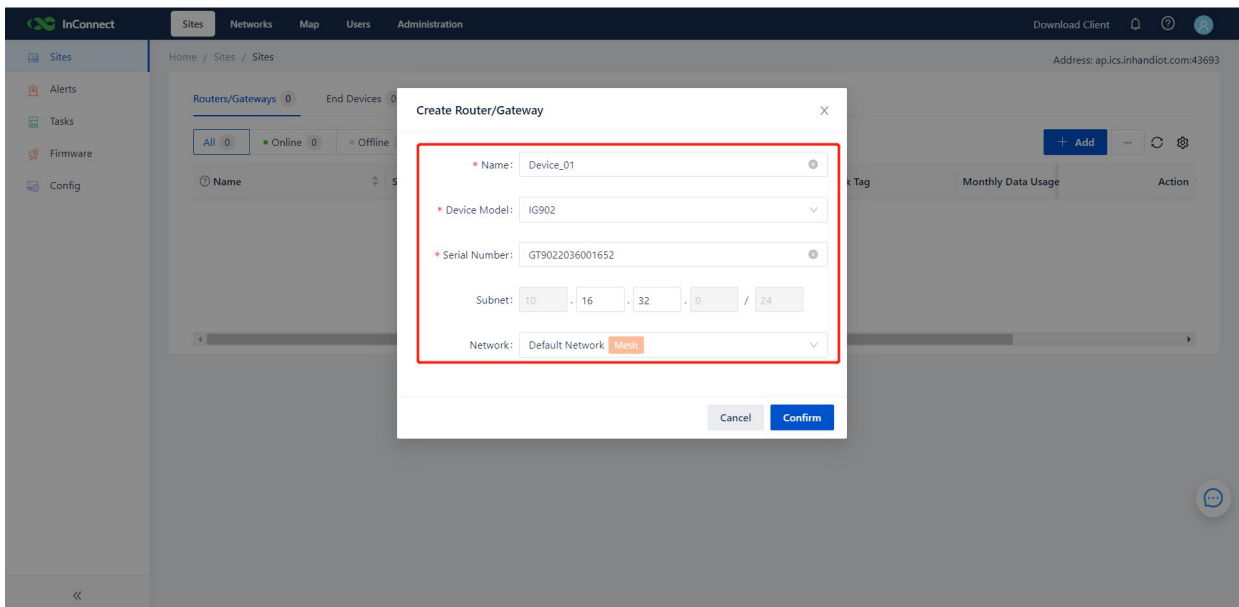
3.1. Adding the Router to InConnect

Before connecting the router to InConnect on the web page of the router, you need to add information about this router again on the InConnect platform. Then, the router will automatically connect to InConnect. InConnect can implement remote management on online routers.

1. Choose **Sites>Routers**, and click **Add**.



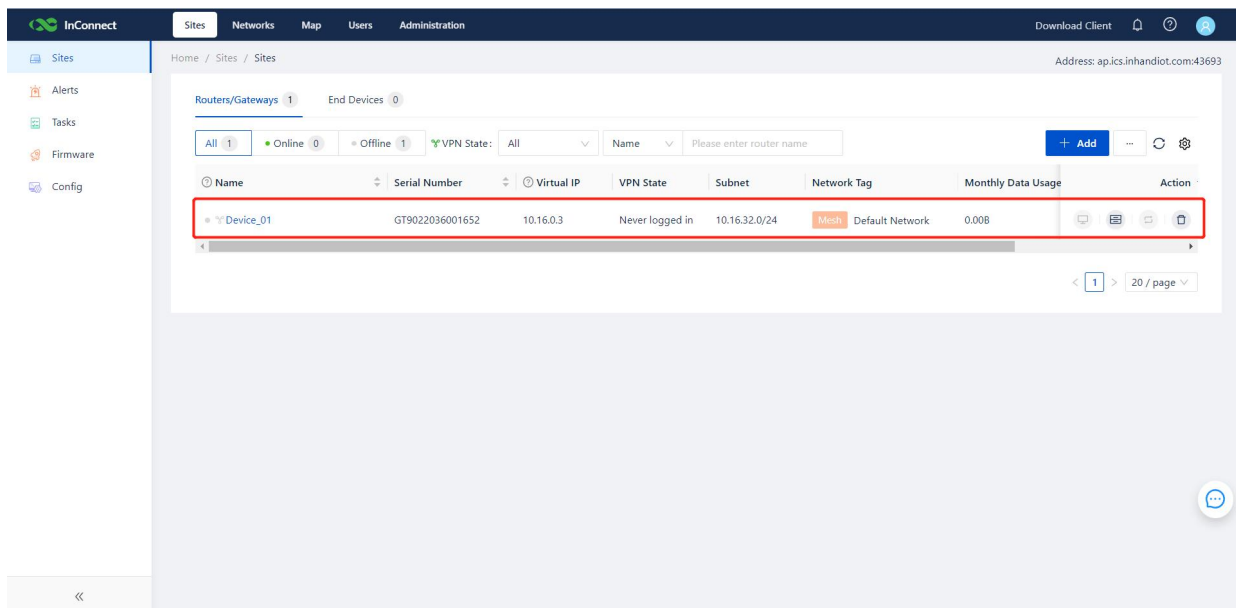
2. In the **Create Router** dialog box, enter the customized name and serial number of the router, select the router model, and click **OK**.



Caution

You can view the serial number on the router **nameplate** or on the **Web Management** page of the router. The selected router model must be correct; otherwise, connection to the router may fail.

3. If the router is displayed on the Routers tab page, the router is added.



4. InConnect allocates a virtual IP address for the added router. After the InConnect client is installed and configured, you can use this virtual IP address to remotely access the router. For details about how to install the client, see [4. Using the Client](#).

3.2. Connecting a Router to InConnect

After adding a router to InConnect, you need to connect the router to InConnect on the web page of the router. Before configuration, ensure that the router is already connected to the network. [For details about how to connect devices to the network, see the appendix.](#)



Caution

The configuration method varies with different product series. Ensure that you refer to the same series of products for configuration according to the equipment in your hand.

The interface varies with the firmware version of the router, and the actual interface should prevail.

3.2.1. IR300-Series Routers

1. After connecting a router to a PC, access **192.168.2.1** in the browser.
2. On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.



Caution

To ensure security, it is recommended that you change the default login password after the initial login, and properly keep the password.

3. On the web page of the router, choose **Services>Device Manager** and complete the following settings:
 1. Set **Service Type** to **InConnect Service**.
 2. Set **Server** to **ics.inhandnetworks.com**.
 3. In the **Registered Account** text box, enter the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.

4. Click **Apply**. If the status displayed on the **Services>Device Manager** page is **Connected**, the router is connected to InConnect. If the status is **Registering**, please check whether the router has been added to the platform.

3.2.2. IR600-Series Routers

1. After connecting a router to a PC, access **192.168.2.1** in the browser.
2. On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.



Caution

To ensure security, it is recommended that you change the default login password after the initial login, and properly keep the password.

3. On the web page of the router, choose **Services>Device Manager** and complete the following settings:
 1. Set **Service Type** to **InConnect Service**.
 2. Set **Server** to **ics.inhandnetworks.com**.
 3. In the **Registered Account** text box, enter the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.

InHand Networks

System Network Services Firewall QoS VPN Tools Application Status

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

Device Manager

Enable

Service Type

Server

Secure Channel

Registered Account [Sign up/Sign in](#)

LBS info Upload Interval Hours

Series Info Upload Interval Hours

Channel Keepalive Seconds

- Click **Apply**. If the status displayed on the **Services>Device Manager** page is **Connected**, the router is connected to InConnect. If the status is **Registering**, please check whether the router has been added to the platform.

InHand Networks

System Network Services Firewall QoS VPN Tools Application Status

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

Device Manager

Connect Status

3.2.3. IR900-Series Routers

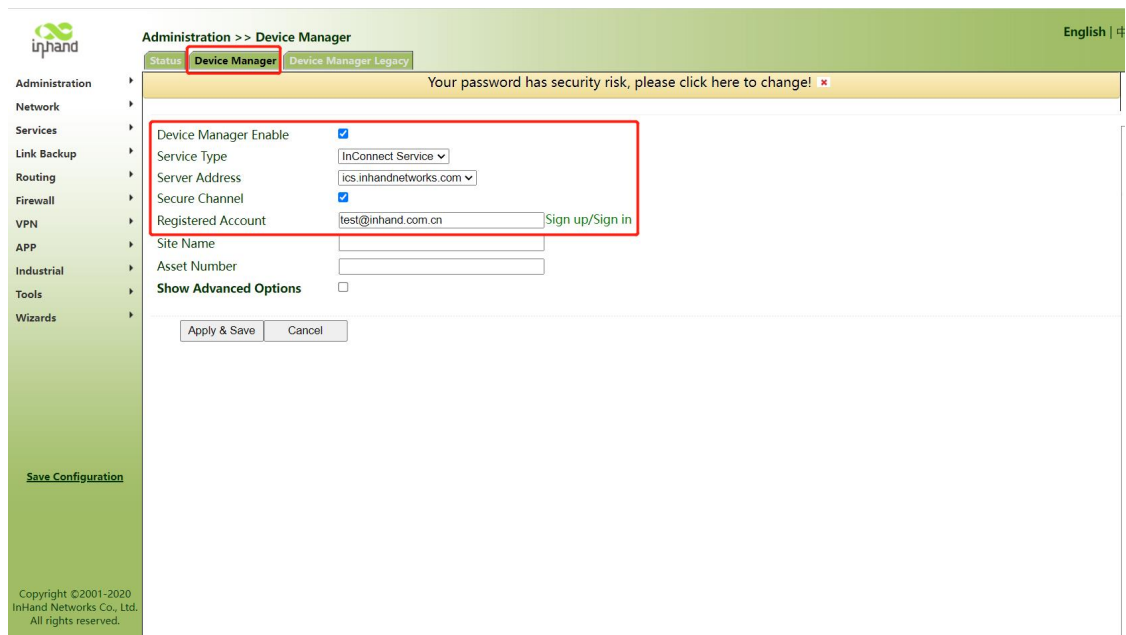
- Use a network cable to connect a PC to the LAN port of the router, and access **192.168.2.1** in the browser.
- On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.



Caution

To ensure security, it is recommended that you change the default login password after the initial login, and properly keep the password.

- On the web page of the router, choose **Administration>Device Manager** and complete the following settings:
 - Select **Device Manager Enable**.
 - Set **Service Type** to **InConnect Service**.
 - Set **Server Address** to **ics.inhandnetworks.com**.
 - In the **Registered Account** text box, enter the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.



5. Click **Apply & Save**. If the status displayed on the **Status** tab page is **Connected**, the router is connected to InConnect. If the status is **Registering**, please check whether the router has been added to the platform.



3.2.4. IG500-Series Routers

1. Use a network cable to connect a PC to the FE0/1 port of the router, and access **192.168.1.1** in the browser.
2. On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.

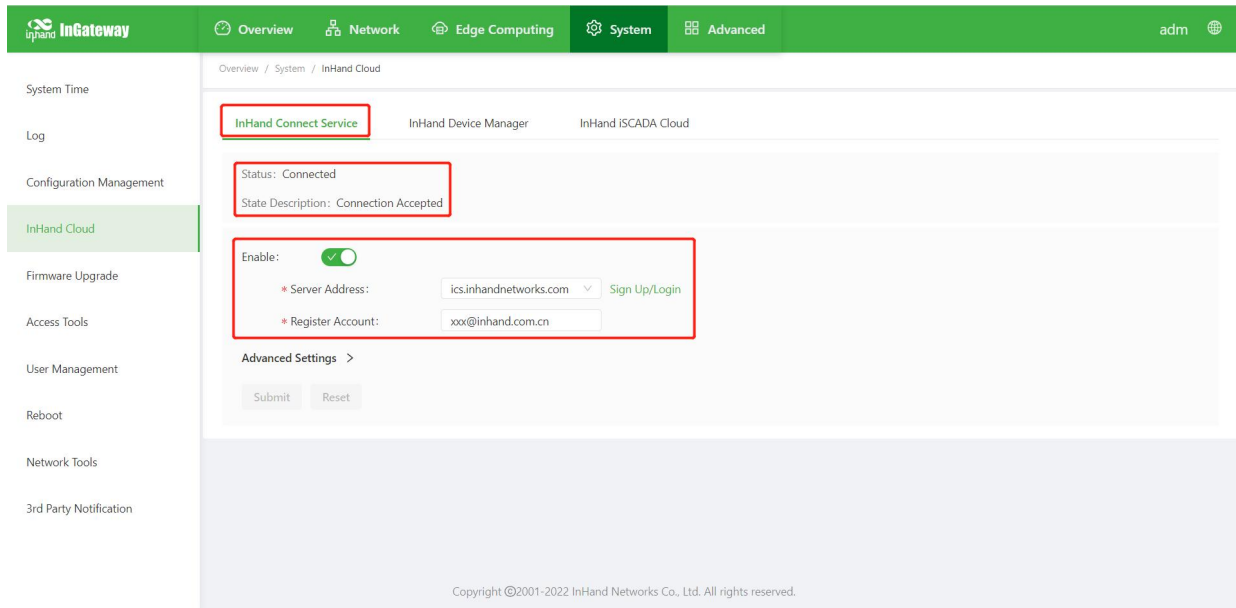


Caution

To ensure security, it is recommended that you change the default login password after the initial login, and

properly keep the password.

3. On the web page of the router, choose **System>InHand Cloud** and complete the following settings:
 1. On the **InHand Connect Service** tab page, set **Server Address** to **ics.inhandnetworks.com** and **Registered Account** to the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.
 2. Click **Submit**. The router starts to setting up a connection with InConnect. After the connection is set up, the following message is displayed on the status bar: "Status: Connected; State Description: Connection Accepted". If the status is **Registering**, please check whether the router has been added to the platform.



3.2.5. IG900-Series Routers

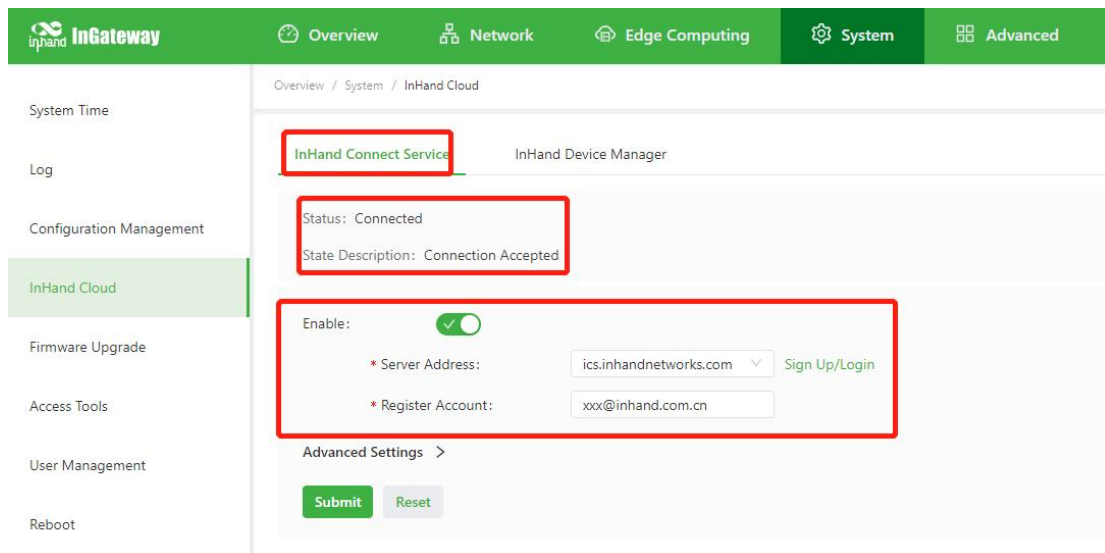
1. Use a network cable to connect a PC to the GE0/2 port of the router, and access **192.168.2.1** in the browser.
2. On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.



Caution

To ensure security, it is recommended that you change the default login password after the initial login, and properly keep the password.

3. On the web page of the router, choose **System>InHand Cloud** and complete the following settings:
 1. On the **InHand Connect Service** tab page, set **Server Address** to **ics.inhandnetworks.com** and **Registered Account** to the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.
 2. Click **Submit**. The router starts to setting up a connection with InConnect. After the connection is set up, the following message is displayed on the status bar: "Status: Connected; State Description: Connection Accepted".



3.2.6. VG710-Series Routers

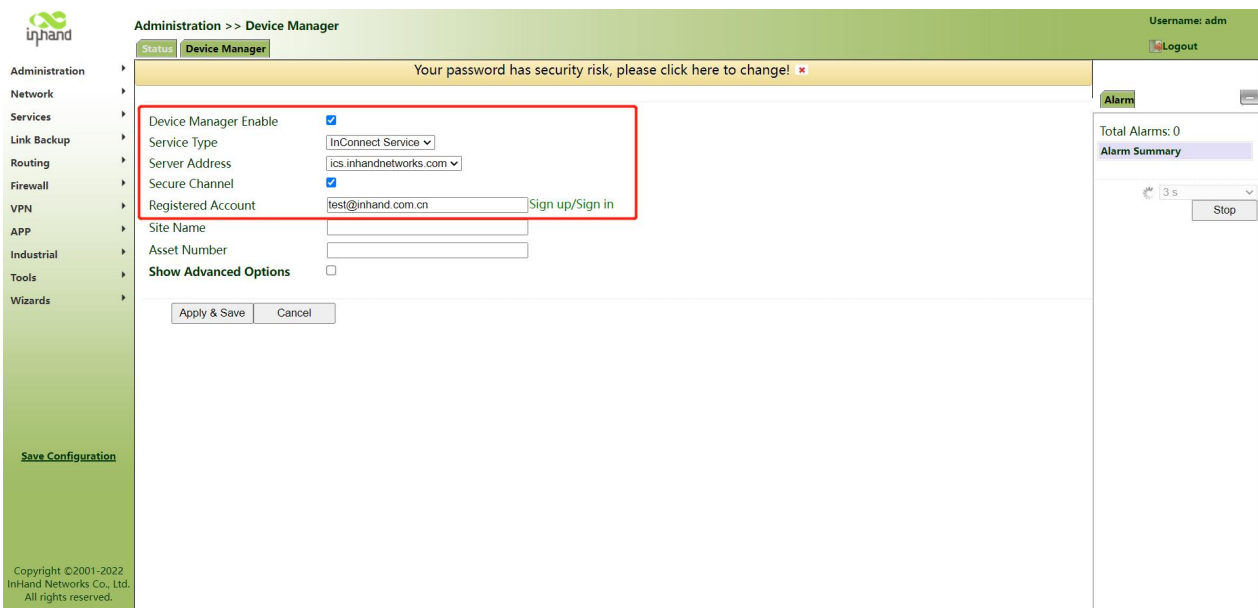
1. After connecting a router to a PC, access **192.168.2.1** in the browser.
2. On the login page, enter the initial login information to go to the web page of the router. The default login account is **adm** and the password is **123456**.



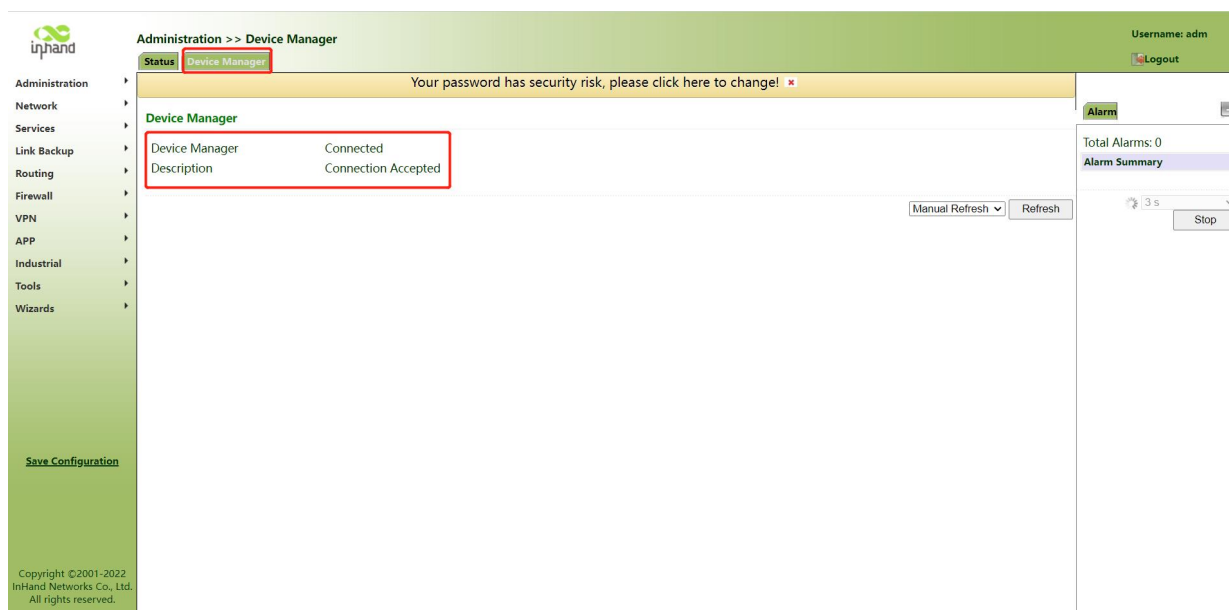
Caution

To ensure security, it is recommended that you change the default login password after the initial login, and properly keep the password.

3. On the web page of the router, choose **Administration>Device Manager** and complete the following settings:
 1. Select **Device Manager Enable**.
 2. Set **Service Type** to **InConnect Service**.
 3. Set **Server Address** to **ics.inhandnetworks.com**.
 4. In the **Registered Account** text box, enter the email account that you use to register the InConnect account. If you do not have an InConnect account, click **Sign up/Sign in** to register an account, and specify **Registered Account** here.



- Click **Apply & Save**. If the status displayed on the **Status** tab page is **Connected**, the router is connected to InConnect. If the status is **Registering**, please check whether the router has been added to the platform.



3.3. Check the connection between the router and InConnect

After the router is added to the platform and InConnect is configured on the router, check the online and VPN status of the router.

- After the router connects to the platform successfully, the online status of the router is displayed in green.

Name	Serial Number	Virtual IP	VPN State	Subnet	Network Tag	Monthly Data Usage	Action
Device_01	GT9022036001652	10.16.0.3	Logged in an hour ago	10.16.32.0/24	Mesh Default Network	240.13KB	[Icons]

- When the router's VPN is successfully established, its VPN status will be shown in green. If the connection between the device and the platform is online, but the VPN is offline, you can try to connect to the VPN again by manually triggering. Click "Send running Config" in the operation column of the "Routers/Gateways" page.

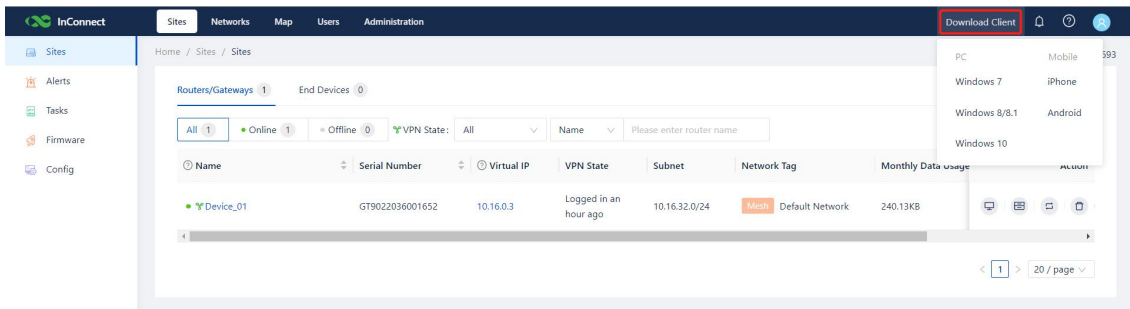
Name	Serial Number	Virtual IP	VPN State	Subnet	Network Tag	Monthly Data Usage	Action
Device_01	GT9022036001652	10.16.0.3	Logged in an hour ago	10.16.32.0/24	Mesh Default Network	240.13KB	[Icons]

4. Using the Client

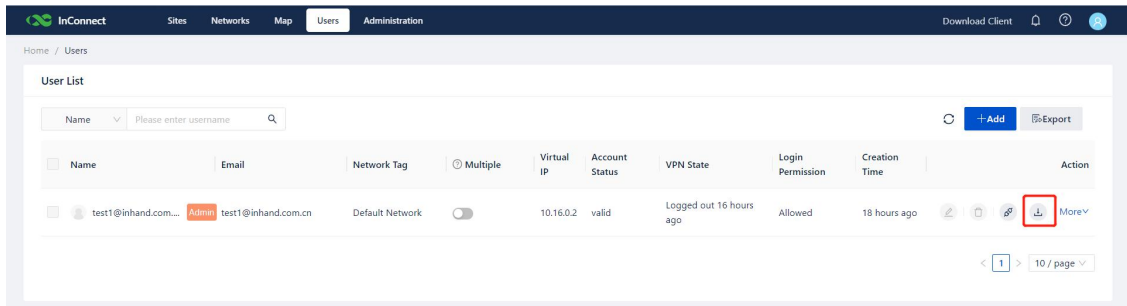
InConnect automatically creates a secure connection channel for the connected router. You can install and configure the client on a local PC or a mobile phone to access the secure connection channel. Then, you can use the virtual IP address to remotely access the router and its downstream devices, implementing remote access and control of onsite devices.

4.1. Installing and Using OpenVPN in Windows

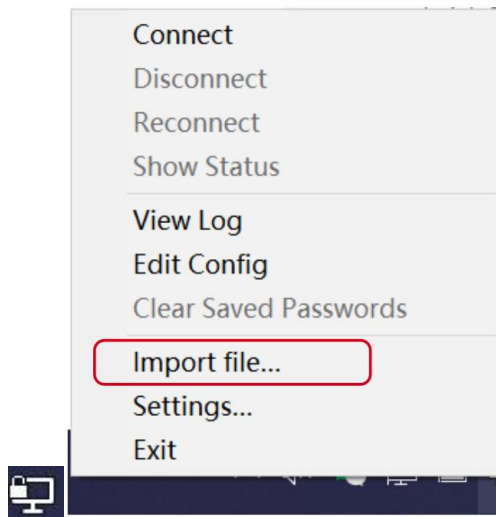
- Download the OpenVPN client to InConnect and install the client.



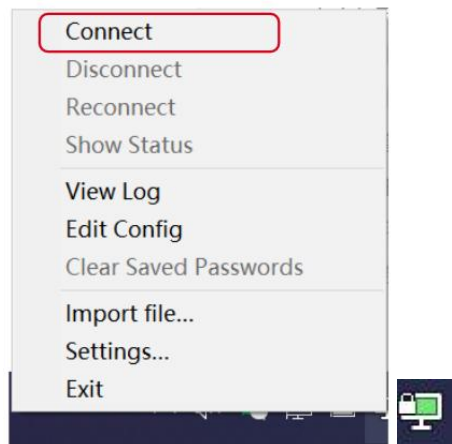
2. In the Users list of InConnect, download the configuration file.



3. Run the OpenVPN GUI as **administrator**. Right-click the icon in the lower-right corner, and choose **Import file** from the shortcut menu to import the configuration file to the OpenVPN client.

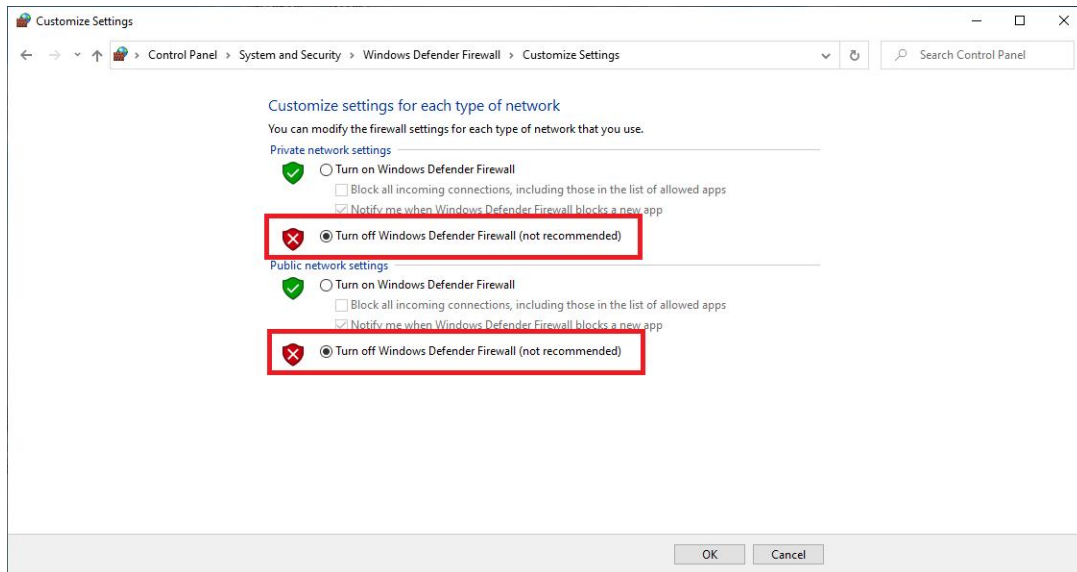


4. Click **Connect**. When the icon turns green, the current user is connected to the secure connection channel.

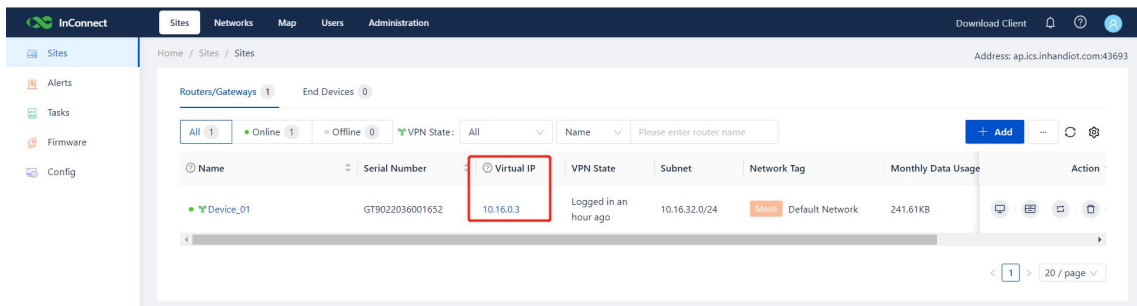


5. Test whether the virtual IP address of the router can be accessed.

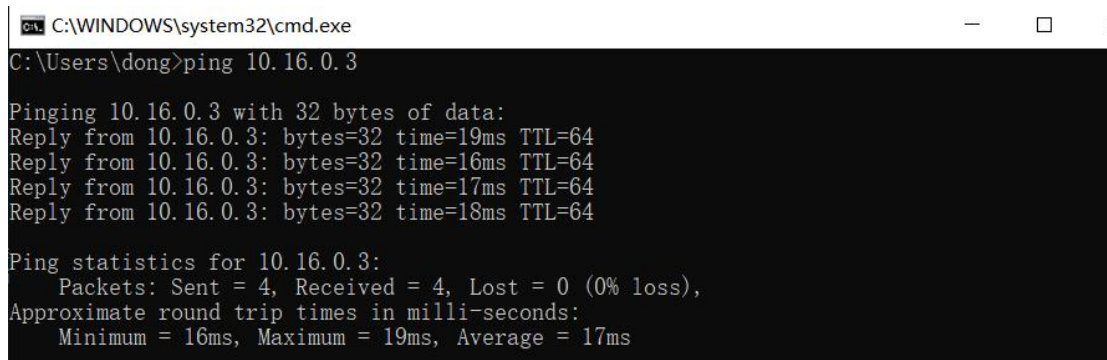
- The IP address cannot be pinged if Windows Defender Firewall is enabled. It is recommended that you disable the firewall or enable ICMP first.



- Open Command Prompt of Windows, and ping the router's virtual IP address **10.16.0.3**. You can obtain the virtual IP address by dragging the scroll bar on the **Sites** page of InConnect.

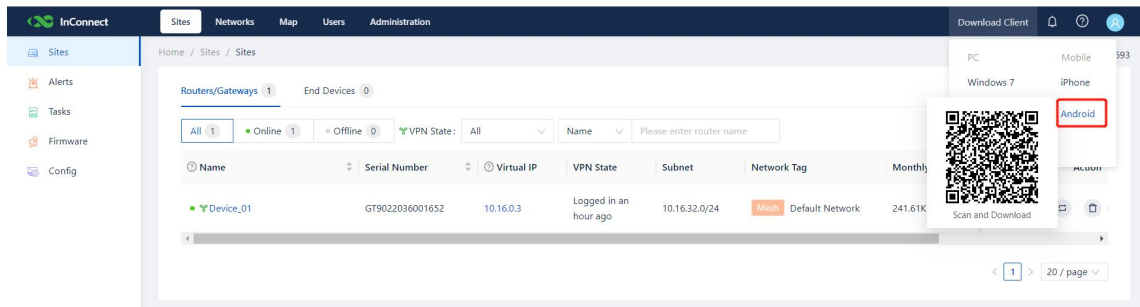


- If the IP address can be pinged, the current user is connected to the remote router, as shown in the figure below.

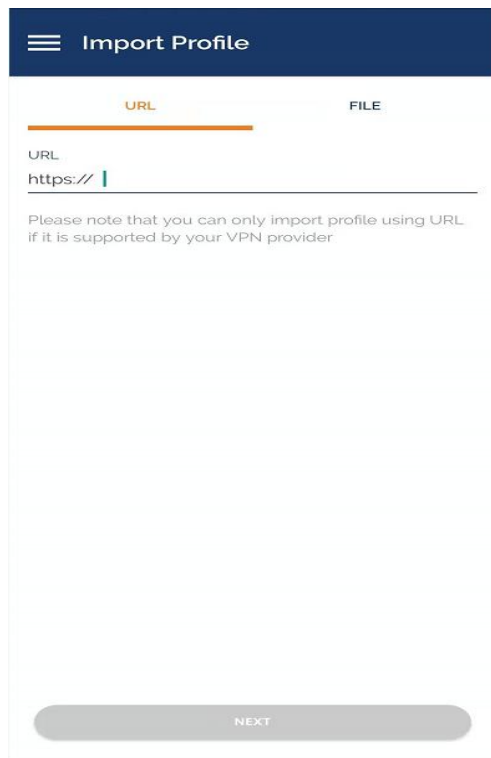


4.2. Installing and Using OpenVPN in Android

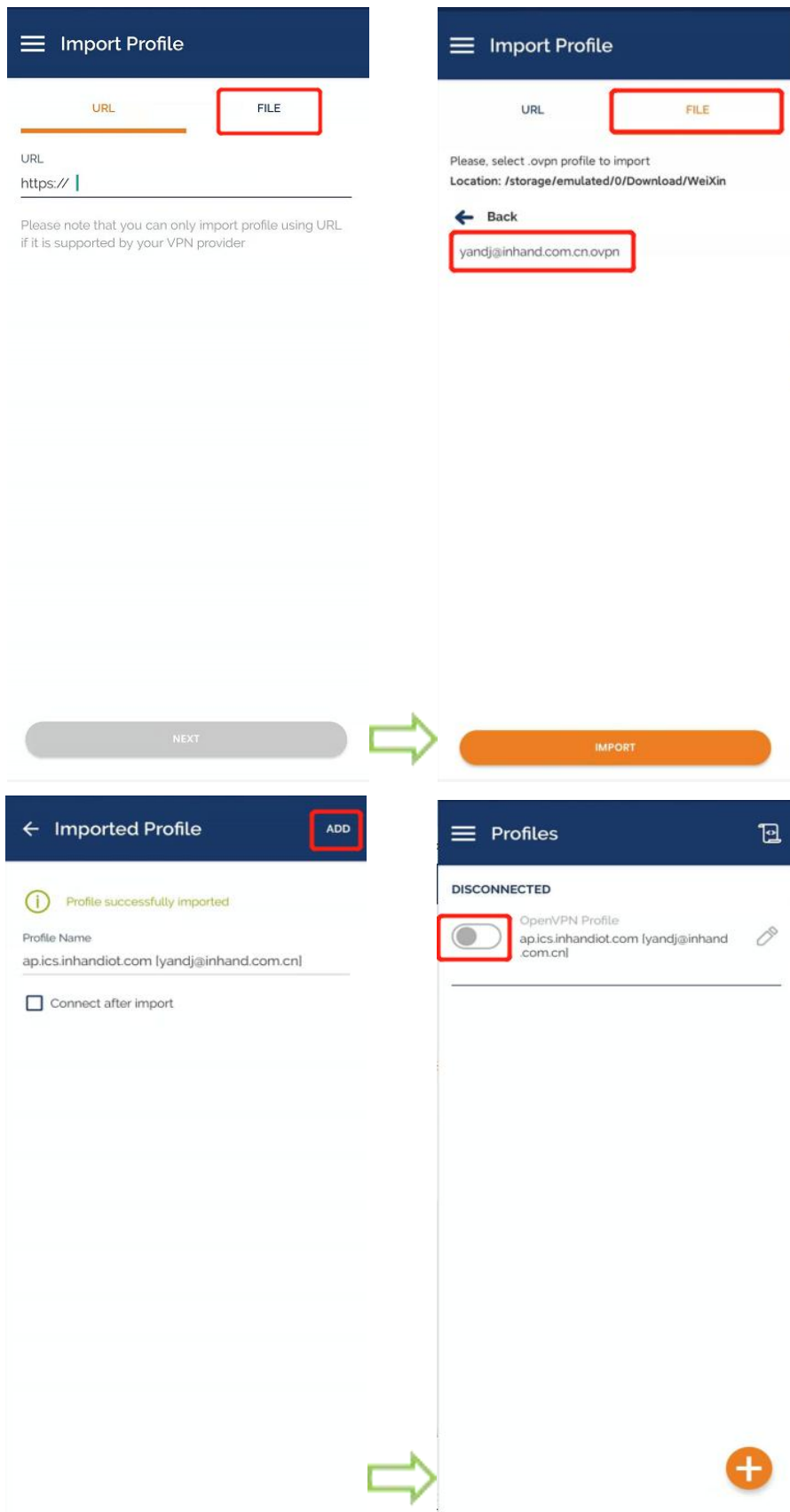
1. Scan the QR code in InConnect to download the OpenVPN client of the Android edition.



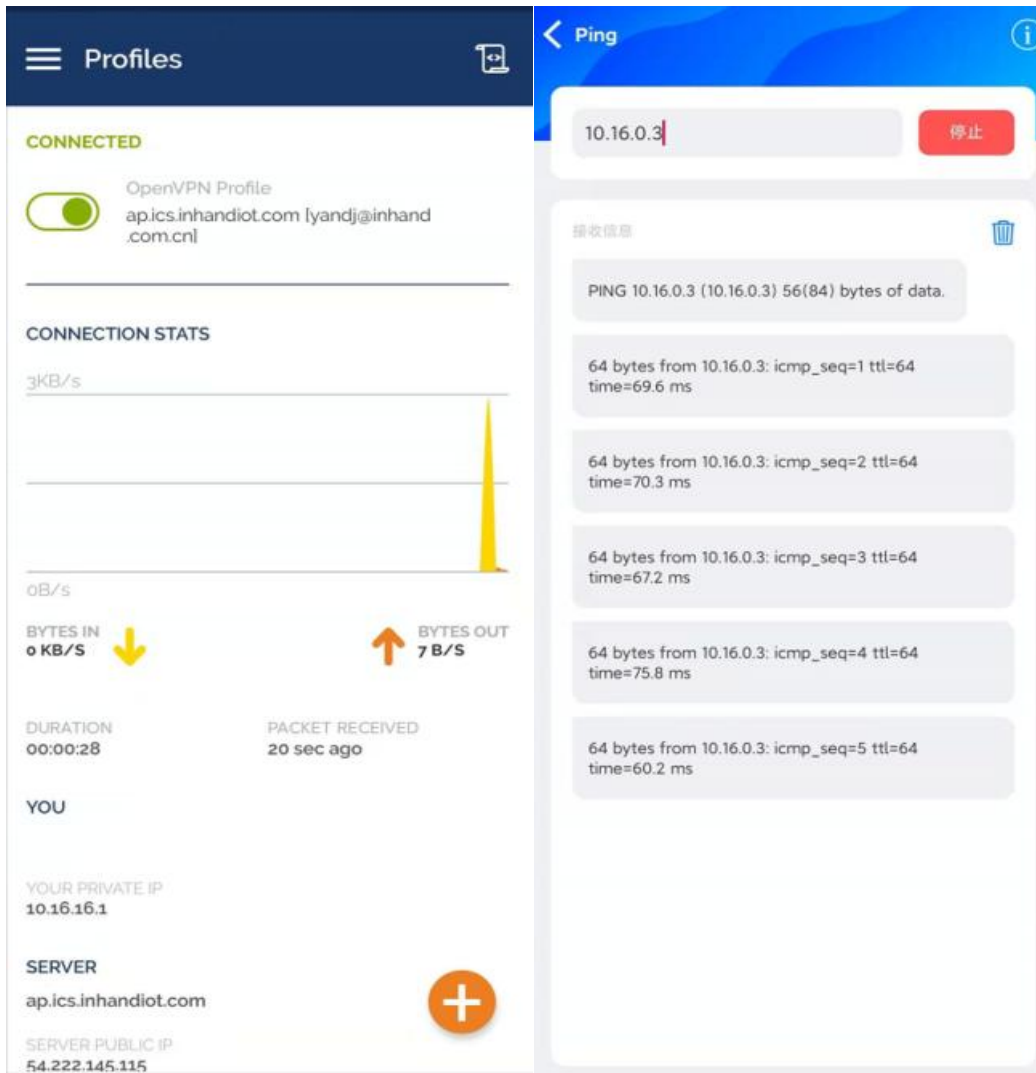
2. Install the client. The running page is as follows:



3. Download the OpenVPN configuration file from InConnect and send the file to your mobile phone.
4. Tap **FILE**, select a configuration file, choose **IMPORT>ADD**, and toggle on the OpenVPN profile.



5. After OpenVPN is connected, launch the ping tool of the mobile phone, enter the router's virtual IP address, and test whether the address can be pinged. If the address can be pinged, the current user is connected to the remote router.



5. Connecting the Router's Downstream Devices

You can add downstream devices of the router to InConnect so that you can remotely access and control these devices. After a downstream device is added, InConnect automatically delivers the running configuration to create a secure network connection.

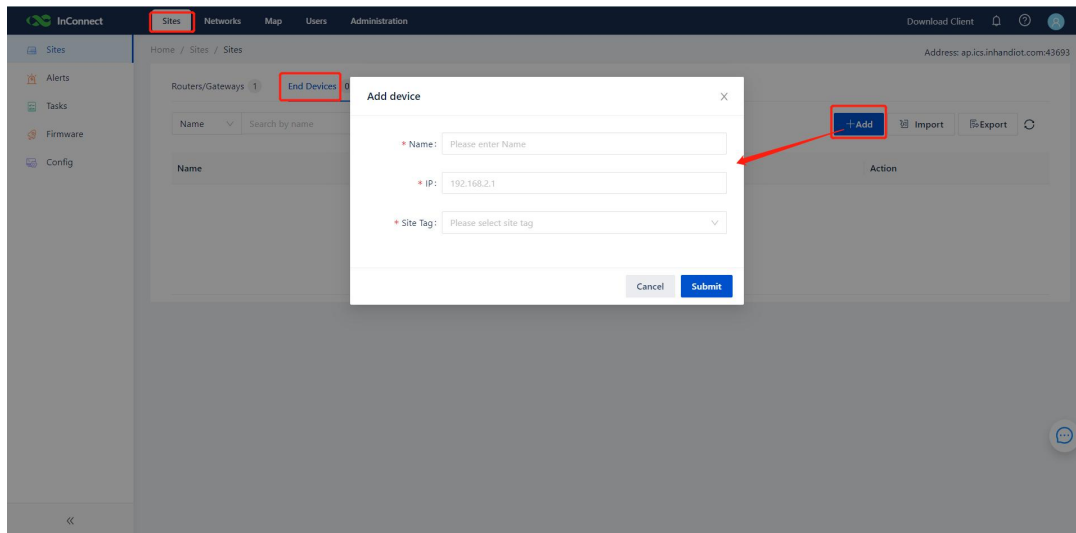
InConnect supports two access modes: access through the virtual IP address and access through the real IP address. The details are described below.

5.1. Access Through the Virtual IP Address

InConnect automatically maps an added downstream device (such as the PLC) to a virtual IP address. This auto mapping mechanism can prevent access conflicts. When you are not demanding on management and usage of real IP addresses, it is recommended that you use this access mode because it is more convenient. Access through the virtual IP address is also the default access mode of InConnect.

Operation method 1:

1. On the **Sites** page, choose **End Devices**>**Add**.



2. Enter the name and real IP address of the downstream device, and select the site of the device, that is, the device name added to the site.

Add device

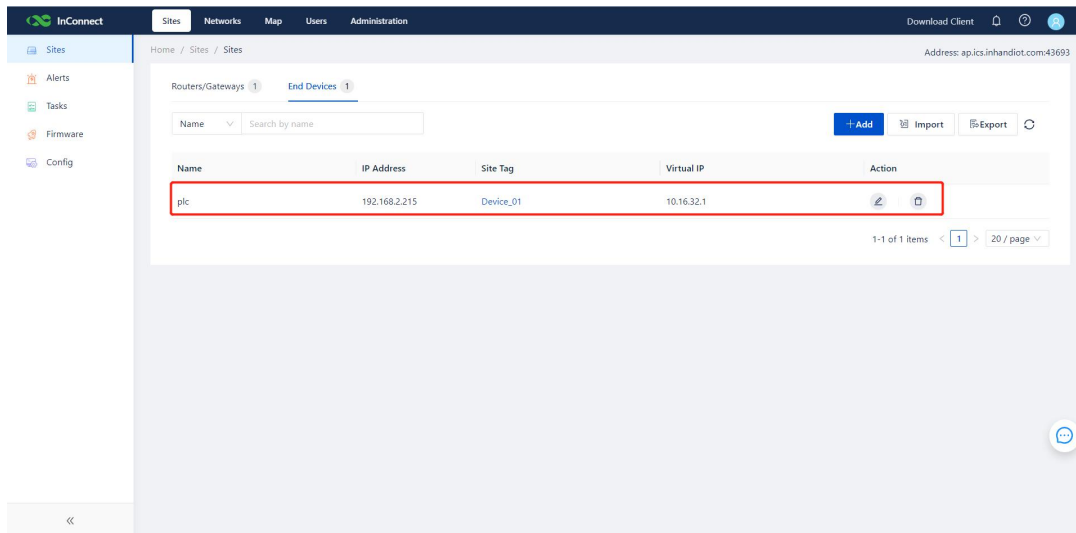
* Name:

* IP:

* Site Tag:

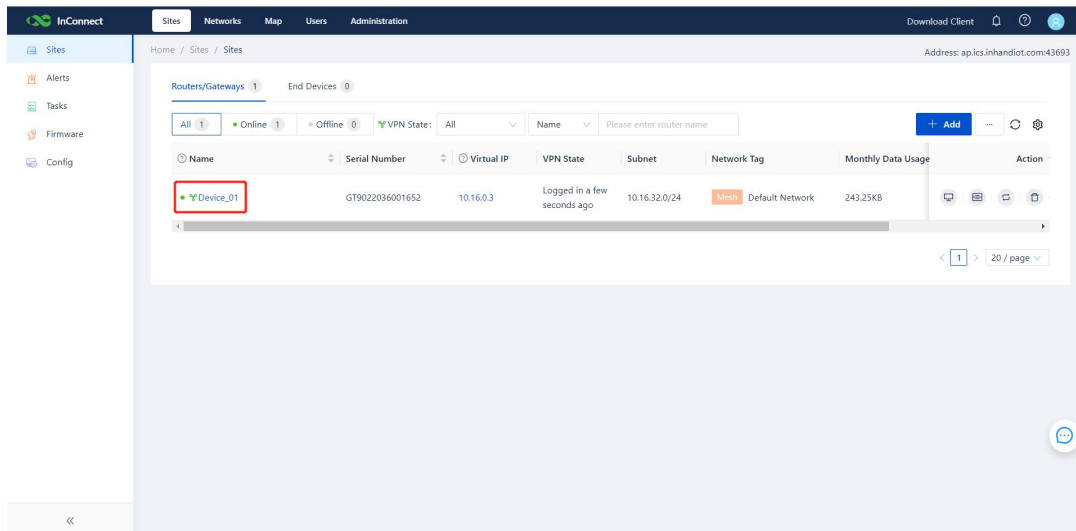
Virtual IP: . . .

3. Click **Submit**, and check the result. InConnect automatically maps the downstream device to a virtual IP address. You can add a maximum of 254 downstream devices for each router. As shown in the figure below, the real IP address of the downstream device on the Device01 site is 192.168.2.215, and the mapped virtual IP address is 10.16.32.1.

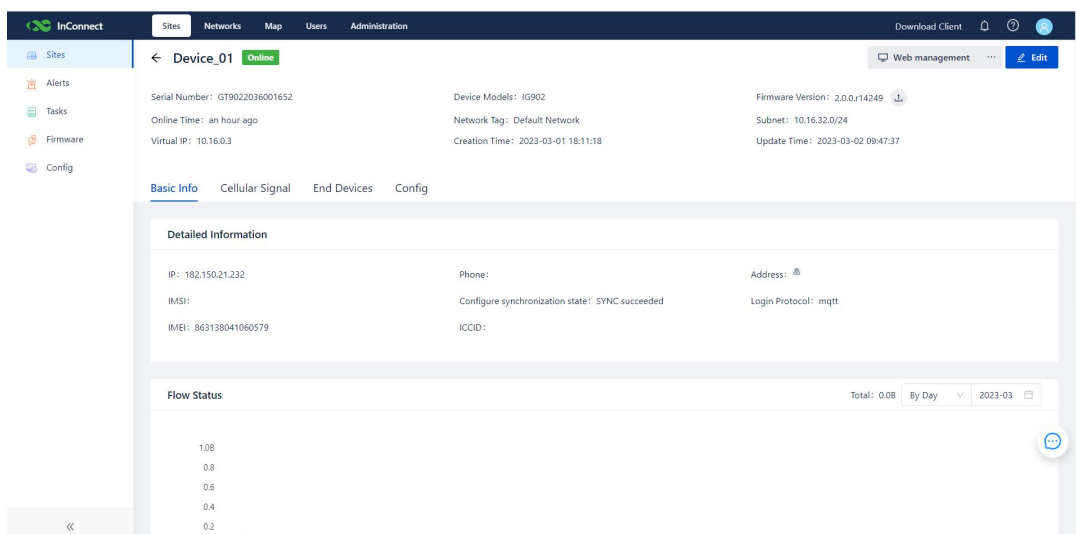


Operation method 2:

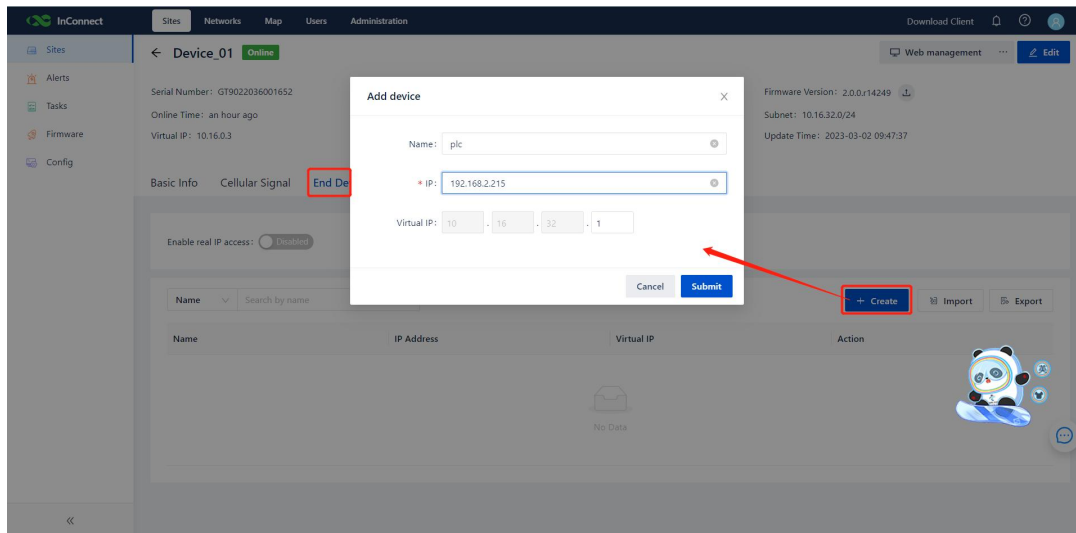
1. On the **Sites** page, click the router name of the target downstream device.



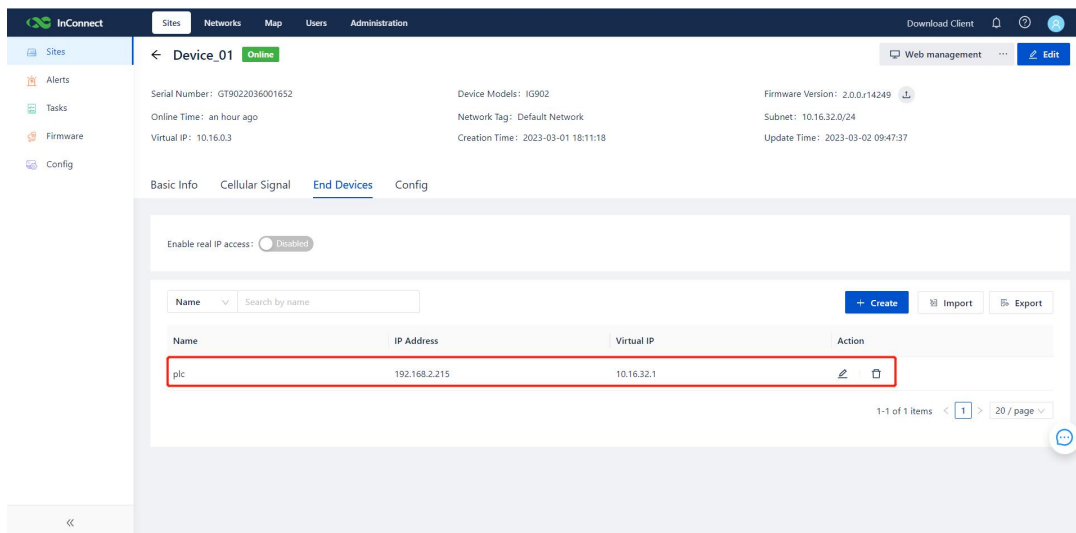
2. Go to the router management page.



3. Choose **End Devices**>**Add**, enter the related information, and click **Submit**.



4. InConnect automatically maps the downstream device to a virtual IP address. Here, the allocated virtual IP address is 10.16.32.1.



5. After you install the client on the local PC, create and configure a connection. Then, ping the virtual IP address of the downstream device to check whether this device can be remotely accessed. If the virtual IP address can be pinged, the remote access is successful. Now you can use the virtual IP address to remotely access the router and its downstream devices such as PLCs and HMIs through the InConnect maintenance channel.

```

C:\Windows\system32\cmd.exe
C:\Users\manji>ping 10.16.32.1

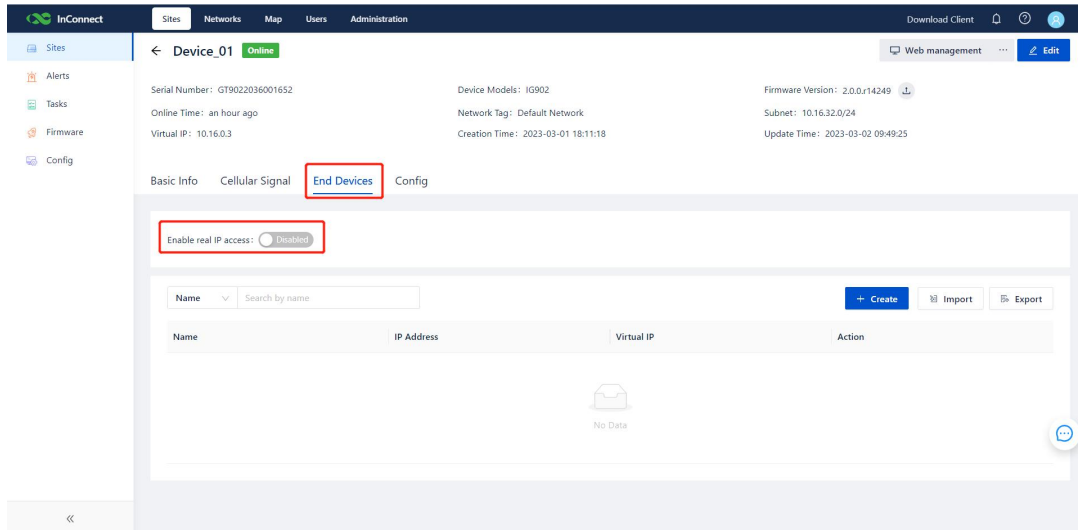
Pinging 10.16.32.1 with 32 bytes of data:
Reply from 10.16.32.1: bytes=32 time=71ms TTL=63
Reply from 10.16.32.1: bytes=32 time=73ms TTL=63
Reply from 10.16.32.1: bytes=32 time=73ms TTL=63
Reply from 10.16.32.1: bytes=32 time=80ms TTL=63

Ping statistics for 10.16.32.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 71ms, Maximum = 80ms, Average = 74ms
  
```

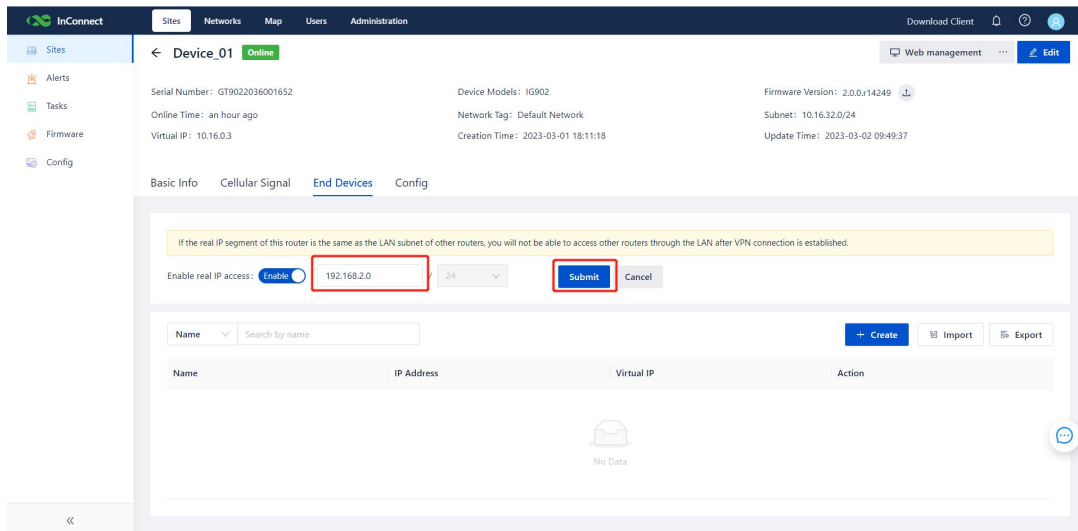
5.2. Access Through the Real IP Address

In addition to the virtual IP address, InConnect also allows you to access downstream devices such as PLCs using the real IP addresses. When you are very demanding on management and usage of real IP addresses, it is recommended that you use this access mode. If you use this access mode, pay attention to the IP conflict issue.

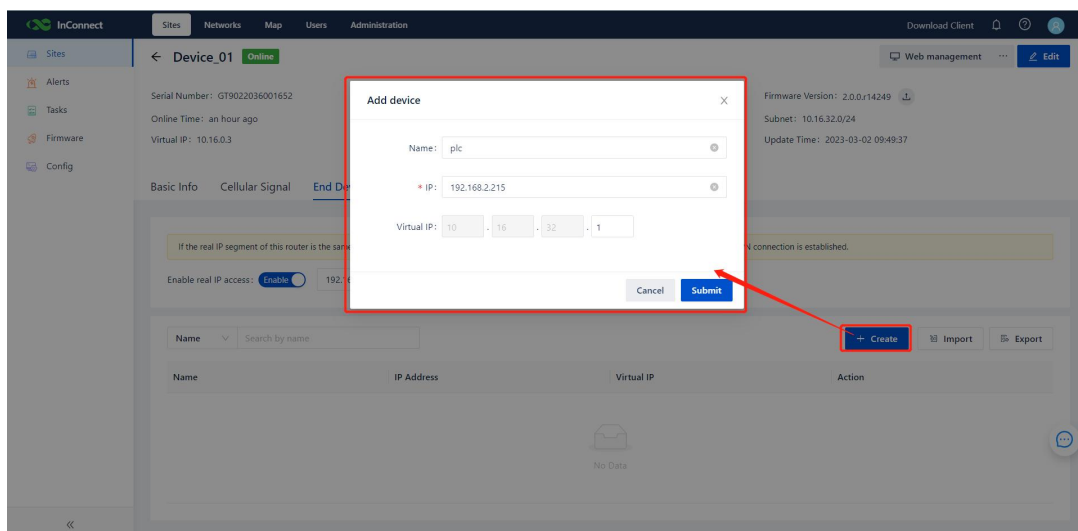
1. Choose **Sites>Routers**, and select the target device name to go to the device management page.



2. Select **Enable real IP access**, and configure the network segment of the target downstream device.



3. Add the downstream device that needs to be accessed through the real IP address.



4. Test the network connection.
Access through the real IP address:

```

C:\Windows\system32\cmd.exe

C:\Users\manji>ping 192.168.2.215

Pinging 192.168.2.215 with 32 bytes of data:
Reply from 192.168.2.215: bytes=32 time=72ms TTL=63
Reply from 192.168.2.215: bytes=32 time=72ms TTL=63
Reply from 192.168.2.215: bytes=32 time=73ms TTL=63
Reply from 192.168.2.215: bytes=32 time=70ms TTL=63

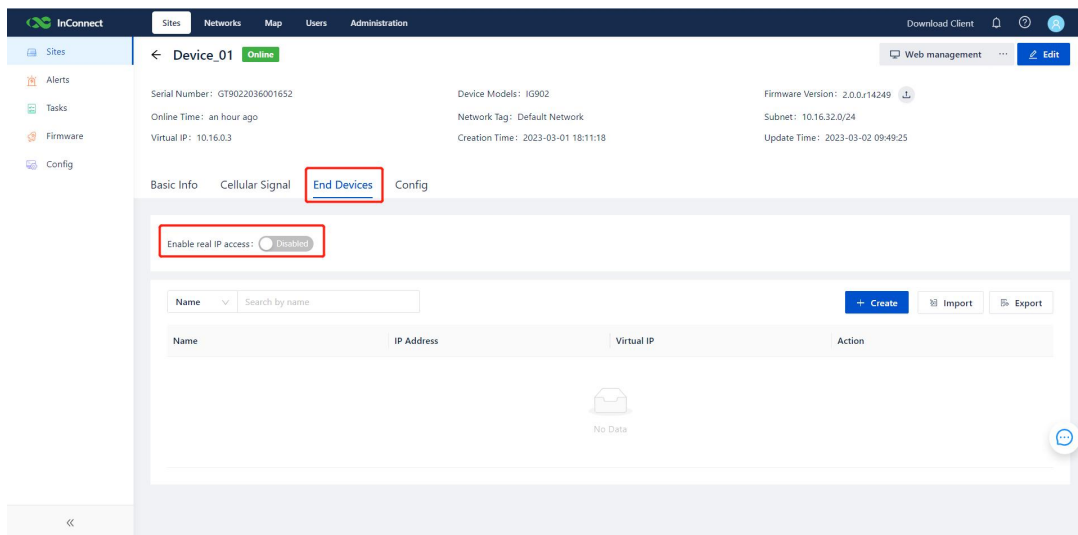
Ping statistics for 192.168.2.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 72ms, Maximum = 76ms, Average = 73ms

```

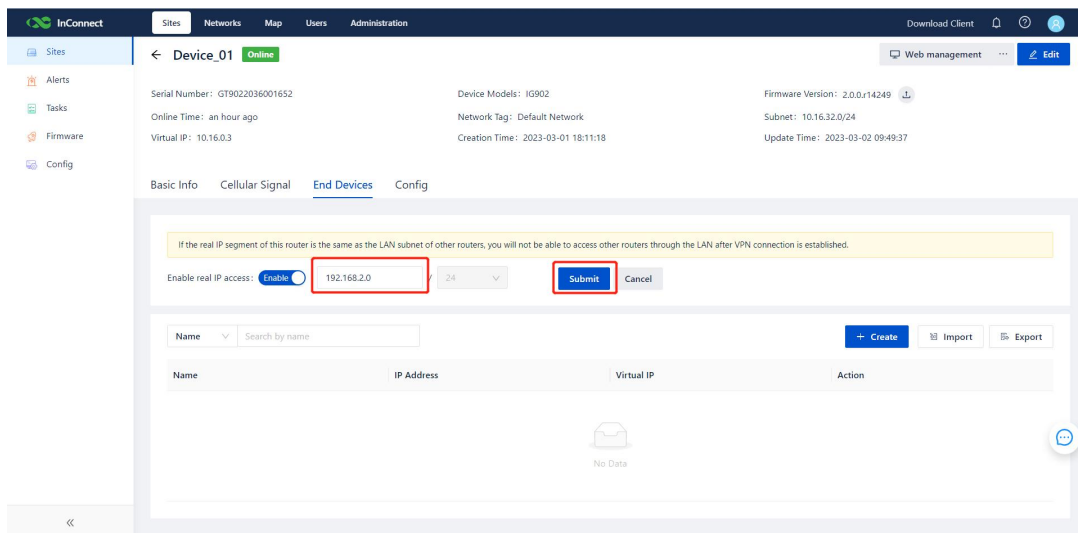
In this access mode, the IP address used is decided by you on site, and duplicate IP addresses will result in access conflicts. To avoid this problem, you can use the "Networks" module of InConnect. For details about this module, see 6. Network Management.

5.3. Access Through the Virtual IP Address and Real IP Address Simultaneously

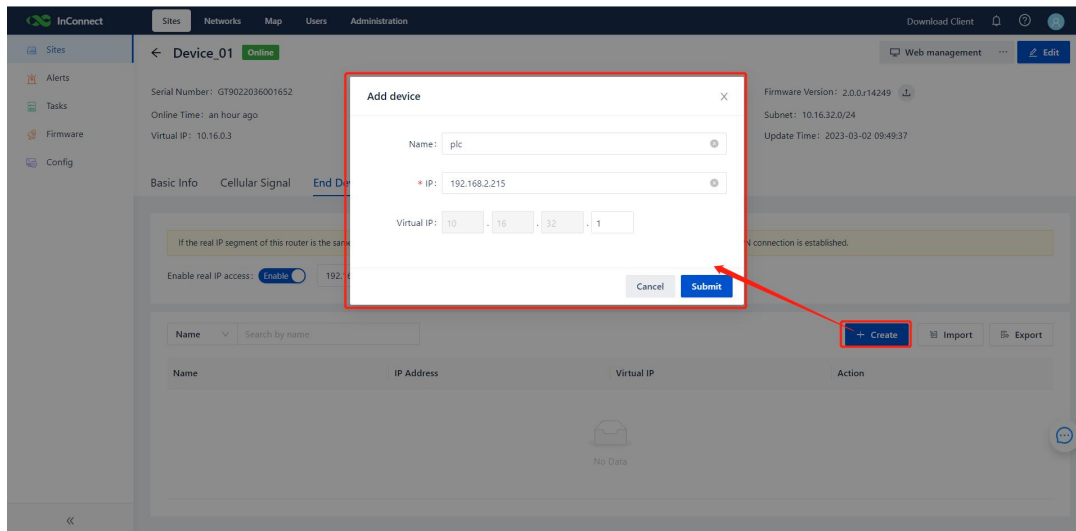
1. Choose **Sites>Routers**, and select the target device name to go to the device management page.



2. Select **Enable real IP access**, and configure the network segment of the target downstream device.



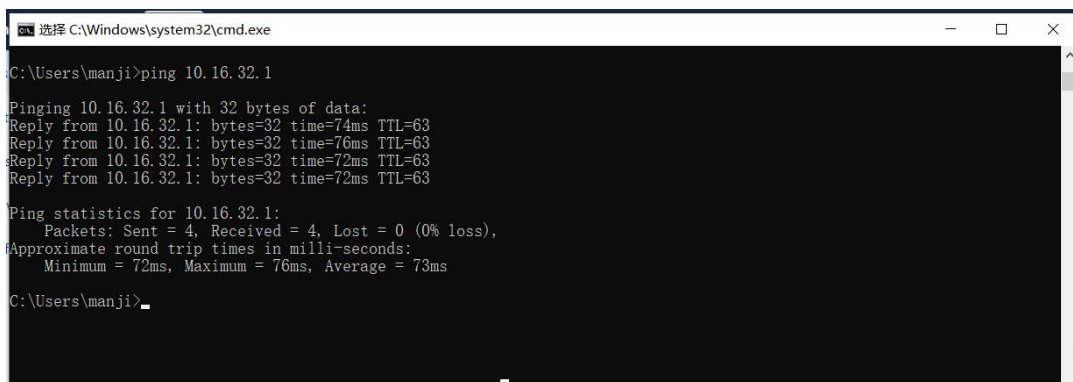
3. Add the downstream device that needs to be accessed through the real IP address.



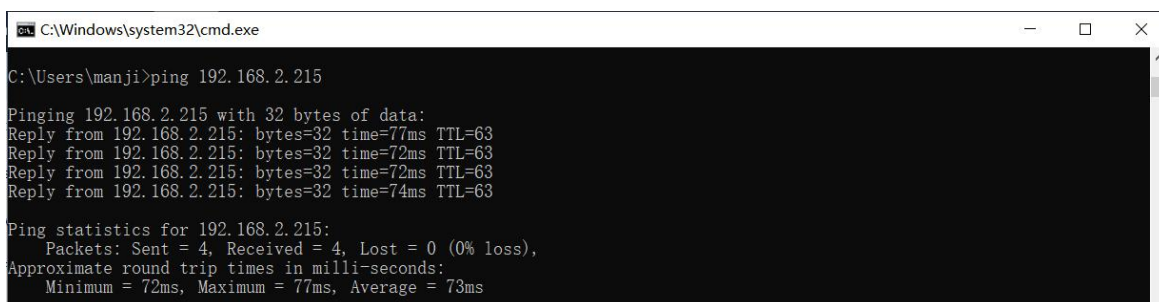
After the device is added, InConnect automatically allocates a virtual IP address for this device. You can use the entered real IP address and the virtual IP address allocated by the system to access the downstream device.

4. Test the network connection.

Access through the virtual IP address:



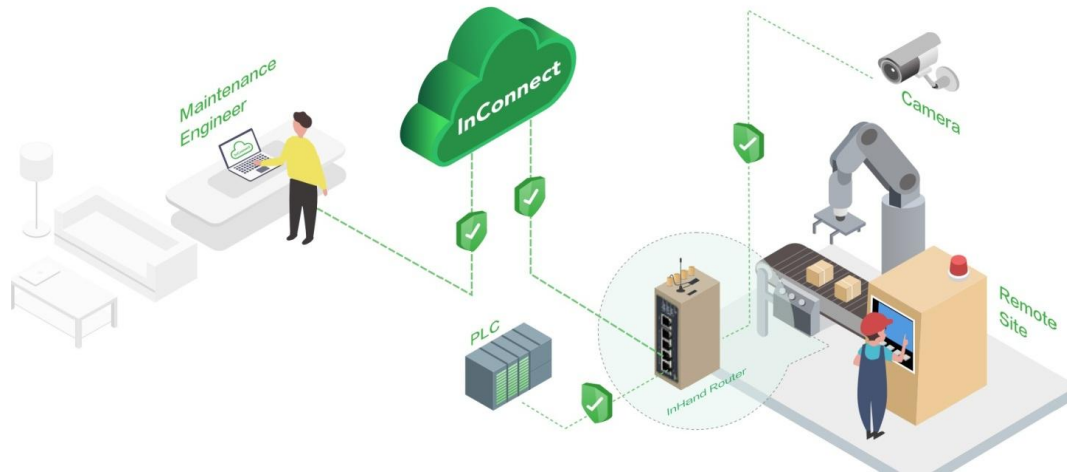
Access through the real IP address:



6. Network Management

6.1. Configuring a Mesh Network

Mesh networks are used to remotely maintain connections with devices, such as PLCs, HDIMIs, and cameras.

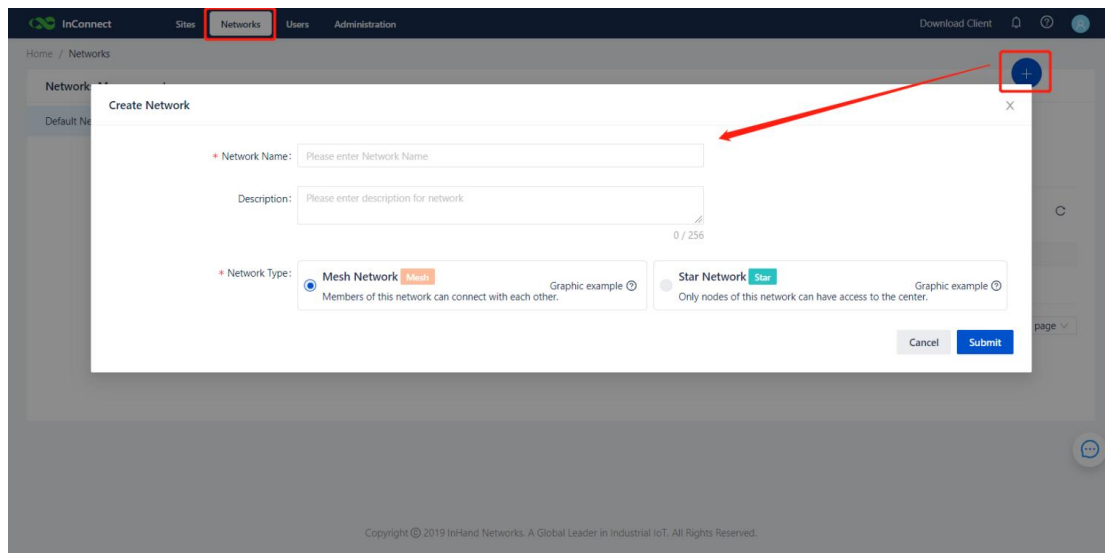


All the newly-added routers are in **Default Network**, which is a mesh network. For all routers in a mesh network, real IP access can be enabled, after which IP conflicts will be detected. If duplicated IP addresses are found, a new mesh network must be created to configure the real IP address of the router. Alternatively, you can enable or disable real IP addresses to avoid the conflicts and implement access through real IP address on demand.

You can also use the "Networks" module to implement authority control of network access. The details are described below.

6.1.1. Adding a Mesh Network

1. Select **Networks**, and click + to add a network.



2. Enter the network name, select the network type **Mesh Network**, and click **Submit**.

Create Network X

* Network Name:

Description: 0 / 256

* Network Type: Mesh Network Mesh Graphic example Star Network Star Graphic example

3. Select the network members and sites, and click **Submit**.

InConnect Sites Networks Users Administration Download Client

← Please select network members

Select User

Selected 1 Item Clear

Username	Email
<input type="checkbox"/> test	test@163.com
<input checked="" type="checkbox"/> yangdj@inhand.com.cn	yangdj@inhand.com.cn

1-2 of 2 items 1 > 20 / page

Select Site

Selected 1 Item Clear

Name	Serial Number
<input checked="" type="checkbox"/> Device01	RT6151944462424

4. The **Network Management** page is displayed.

InConnect Sites Networks Users Administration Download Client

Home / Networks

Networks Management +

Default Network Mesh

network01 Mesh Network

Creation Time: 2020-11-16 17:30:06 Update Time: 2020-11-16 17:30:06

Description:

Sites Users Add Members

Name	Signal	Serial Number	Subnet	Virtual IP	VPN State	Current Version	Action
<input type="checkbox"/> Device01	●●●●	RT6151944462424	10.16.32.0/24	10.16.0.3	Logged in a minute ago	2.3.0.r5355	B

1-1 of 1 items 1 > 20 / page

Copyright © 2019 InHand Networks. A Global Leader in Industrial IoT. All Rights Reserved.



Caution

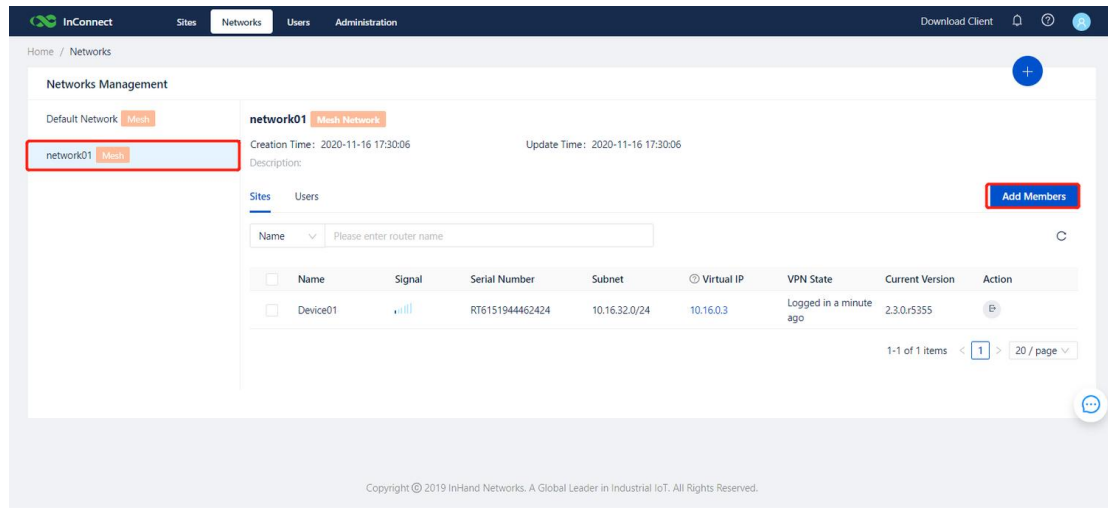
1. A mesh network isolates network access, that is, only users and site devices in the same mesh network can communicate with each other. Users in a mesh network cannot access site devices of another mesh network, and site devices in this mesh network also cannot be accessed by users of another mesh network.
2. **Default Network** is a mesh network. All the newly-added router sites and users are in **Default Network**. Only users and route sites in **Default Network** support mutual access.

3. Configuration of multiple mesh networks can prevent conflicts of real IP addresses. When a user needs to use the real IP address to access multiple terminals with the same real IP address, use either of the following management methods:

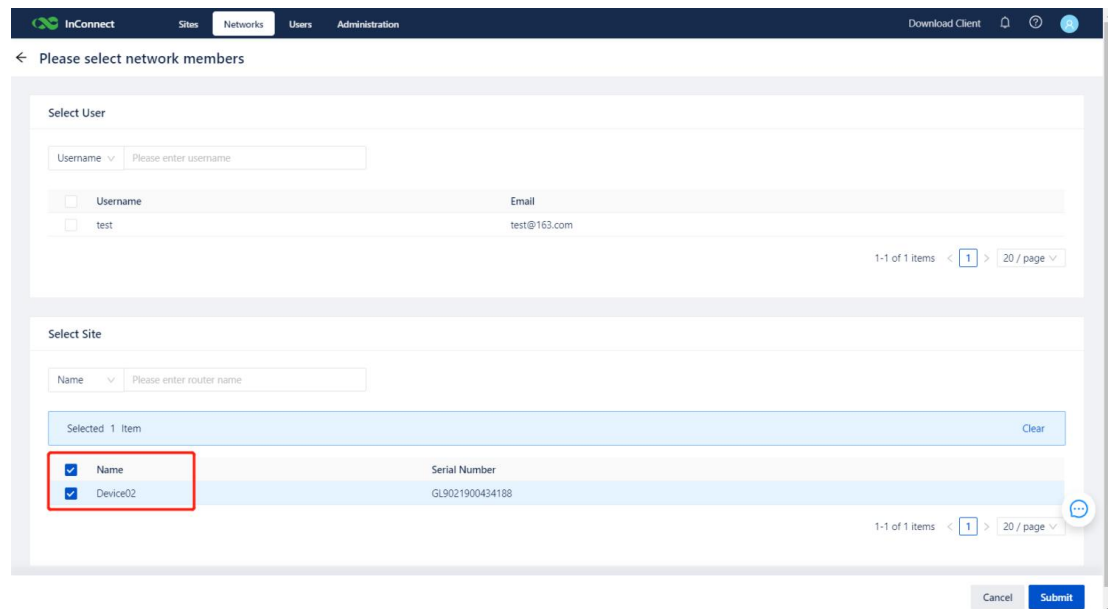
- 1) The user and all terminals are in the same mesh network. When necessary, the user enables the real IP address of a site on demand to avoid the IP conflict.
- 2) Add the terminals with the same real IP address to different mesh networks. When necessary, add the user to the corresponding mesh network to obtain the access permission, which avoids the IP conflict.

6.1.2. Adding a Site or User to a Mesh Network

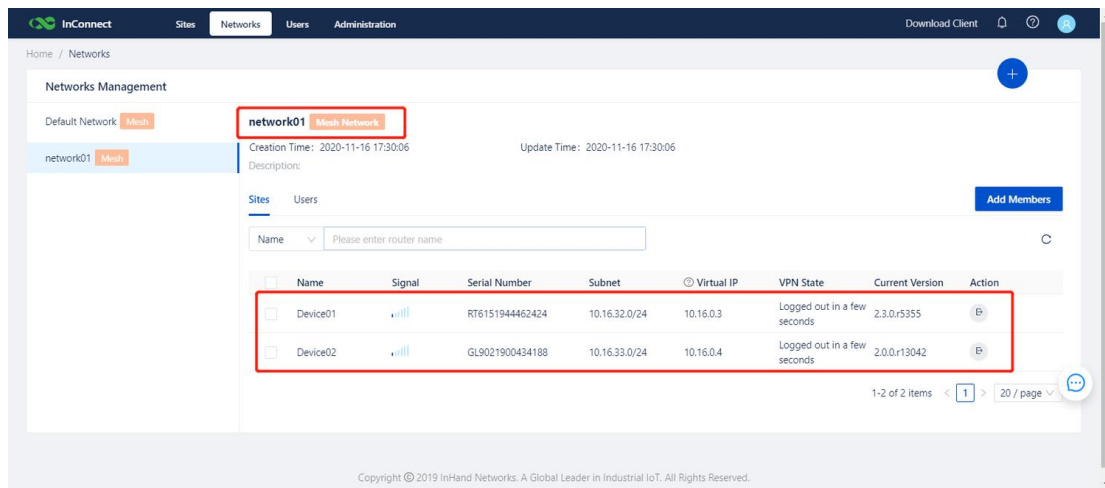
1. Select the target mesh network, and click **Add Members**.



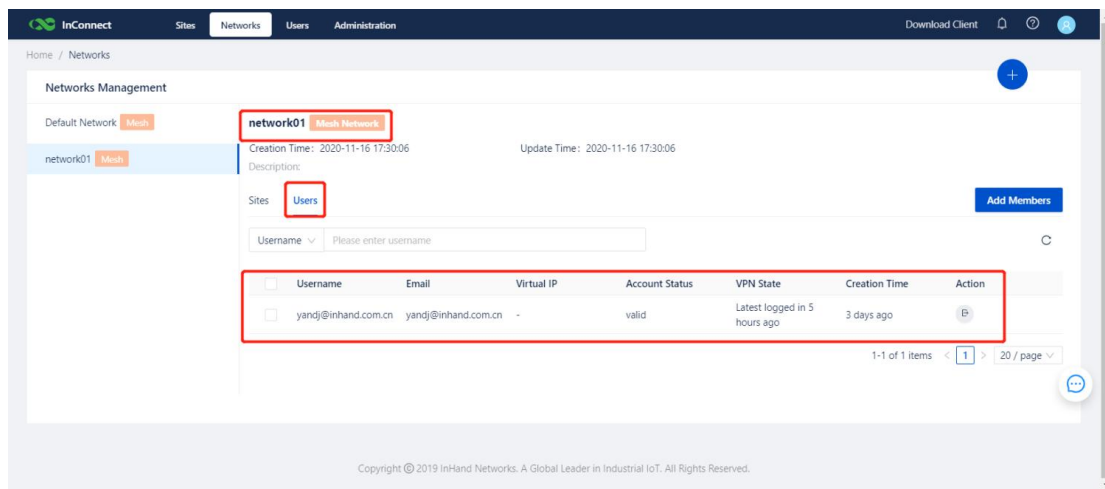
2. Select the user name and site name, and click **Submit**. If an IP conflict occurs between the real IP-enabled router and any other routers in the mesh network, this router cannot be added to the mesh network.



3. Check all sites in the mesh network, and select **Sites**.



4. Check all users the mesh network, and select **Users**.



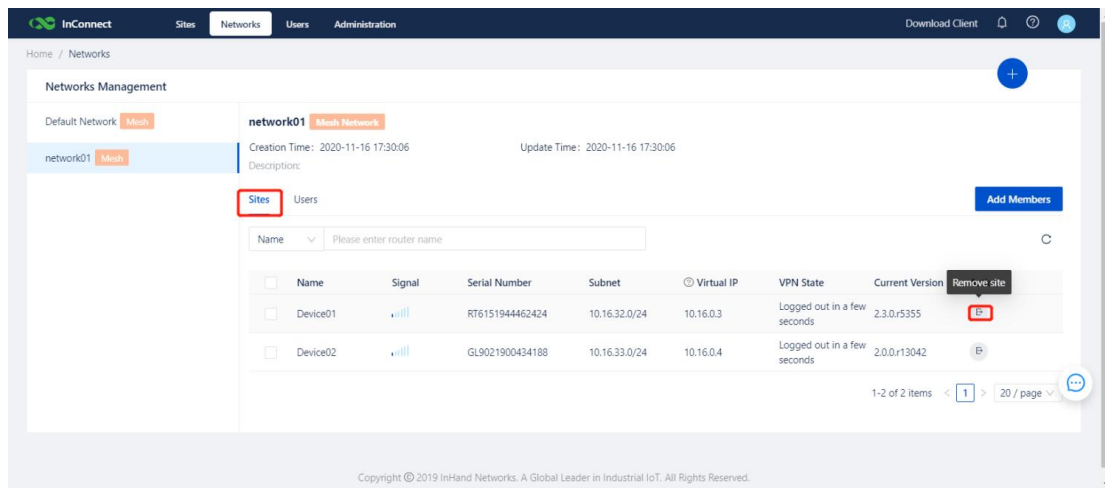
Caution

If an IP conflict occurs between the real IP-enabled router and any other routers in the mesh network, this router cannot be added to the mesh network.

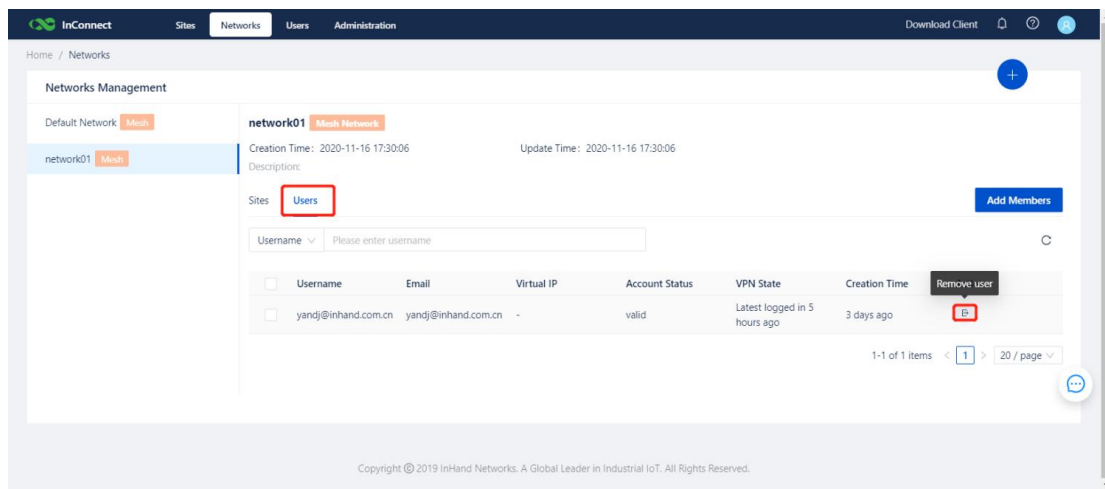
Note: 192.168.2.0 already exists in the mesh network. If the IP address of the device to be added is also 192.168.2.0, an IP conflict occurs and therefore this device cannot be added to the mesh network.

6.1.3. Deleting a Mesh Network

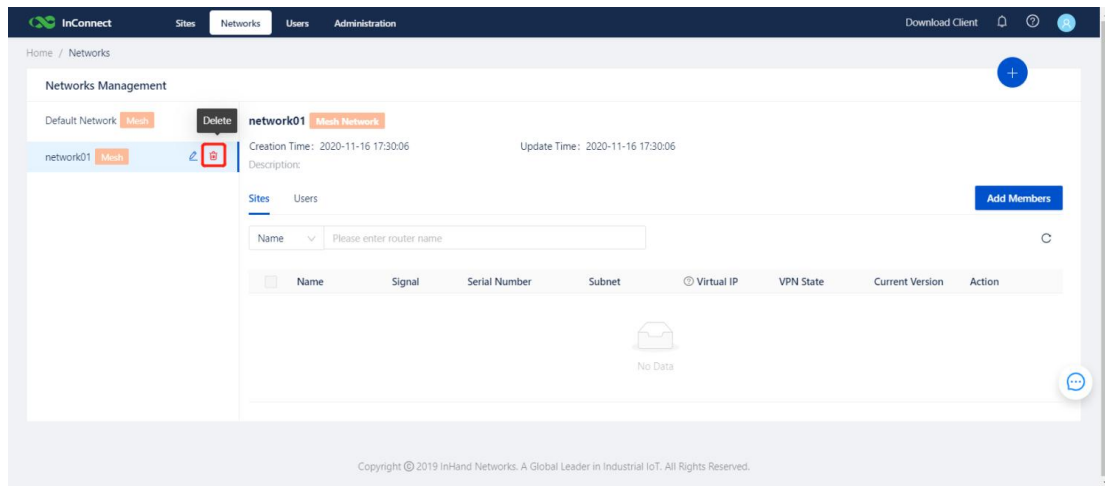
1. Before deleting a mesh network, delete all users and sites in the mesh network. Removed sites will be added to the default mesh network. Choose **Sites>Removesite** on the **Networks** page.



2. Choose **Users**>**Remove user** to delete all users of the mesh network.



3. Select the target mesh network name, and click the **Delete** icon to delete the mesh network.



Caution

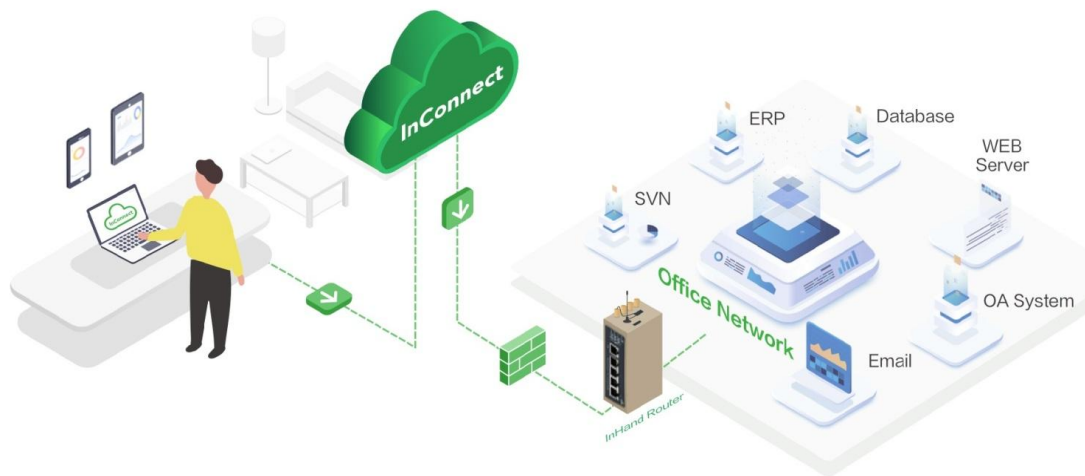
If an IP conflict occurs between the real IP-enabled router and any other routers in **Default Network**, this router cannot be removed from the existing mesh network.

Note: 192.168.2.0 already exists in **Default Network**. If the IP address of the router to be deleted is also 192.168.2.0, an IP conflict occurs and therefore this router cannot be removed from its existing mesh network.

6.2. Configuring a Star Network

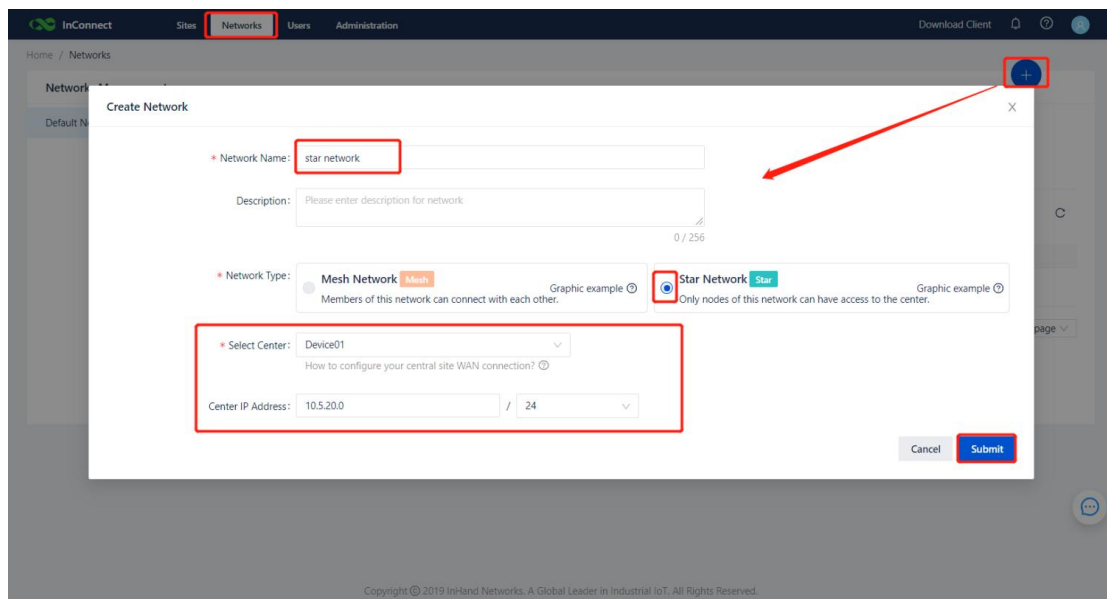
The star network is used for telecommuting. It allows you to access servers in the company's intranet through the InConnect channel when you are at home or on a business trip.

The star network is only applicable to the telecommuting scenario. If you need to remotely access onsite devices such as PLCs, select **Mesh Network**.

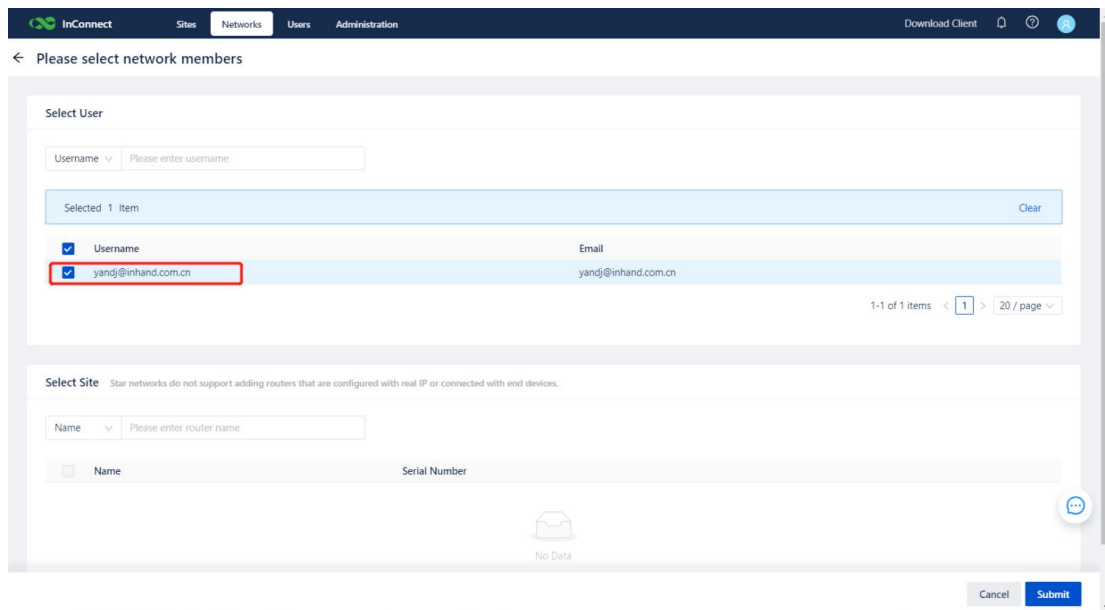


6.2.1. Adding a Star Network

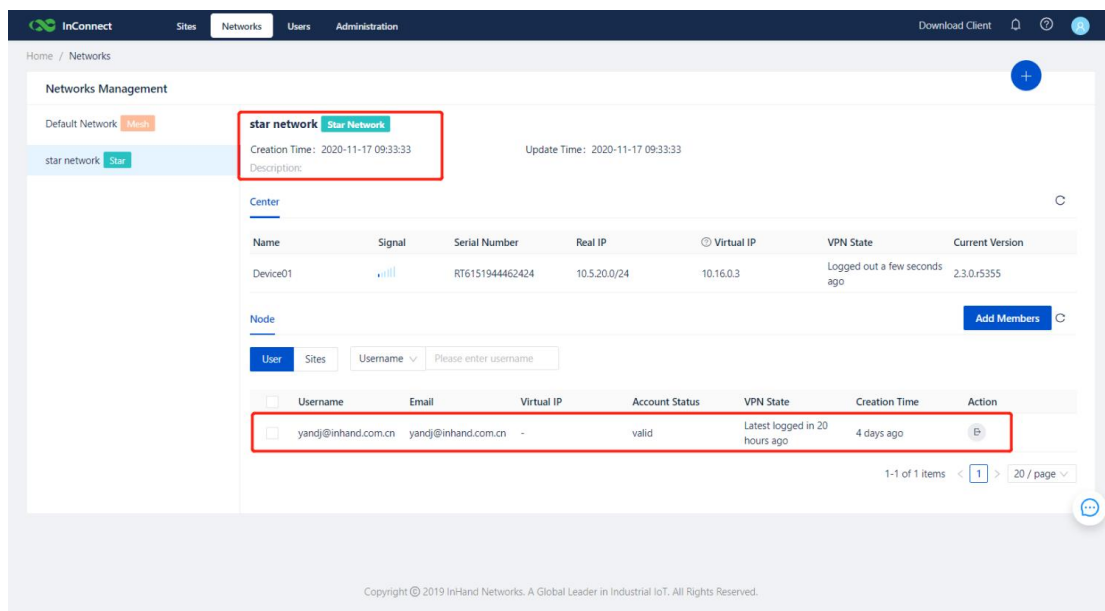
1. Select **Networks**, click **+**, enter the network name, select **Star Network**, enter the center IP address, and click **Submit**.



2. Select the user name and site name, and click **Submit**.




3. Check the information about the newly created network.



4. Use the WAN port of the router to access the network. Check the network information obtained through the WAN port.



5. Use the OpenVPN client to access the network segment of the WAN port of the router. Note: Ensure that you enable the OpenVPN connection .

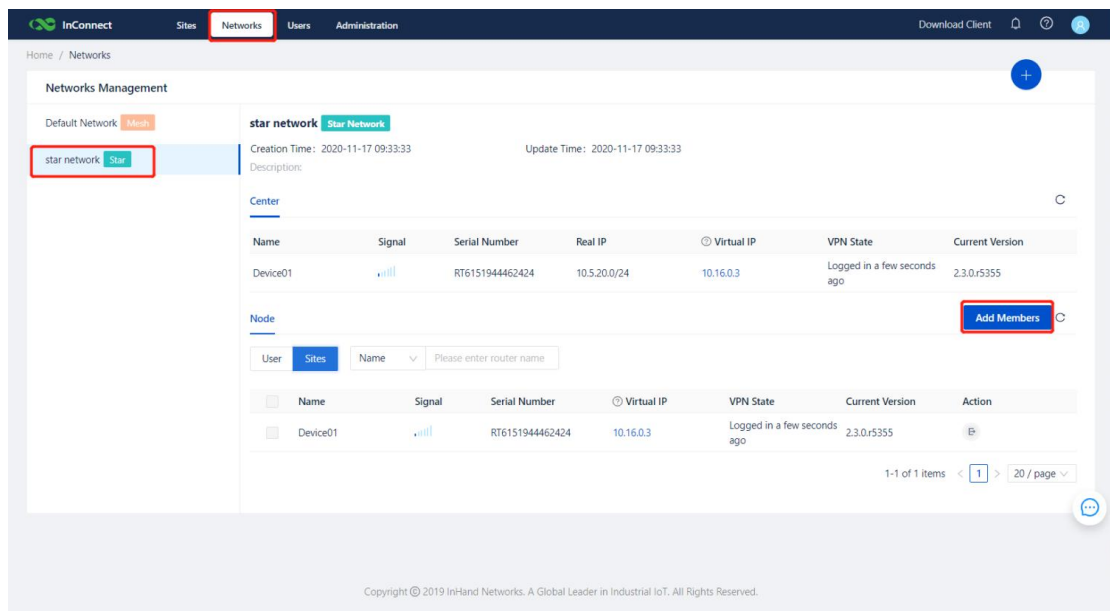
```
C:\Users\dong>ping 10.5.20.254

Pinging 10.5.20.254 with 32 bytes of data:
Reply from 10.5.20.254: bytes=32 time=2ms TTL=64
Reply from 10.5.20.254: bytes=32 time=2ms TTL=64
Reply from 10.5.20.254: bytes=32 time=2ms TTL=64
Reply from 10.5.20.254: bytes=32 time=2ms TTL=64

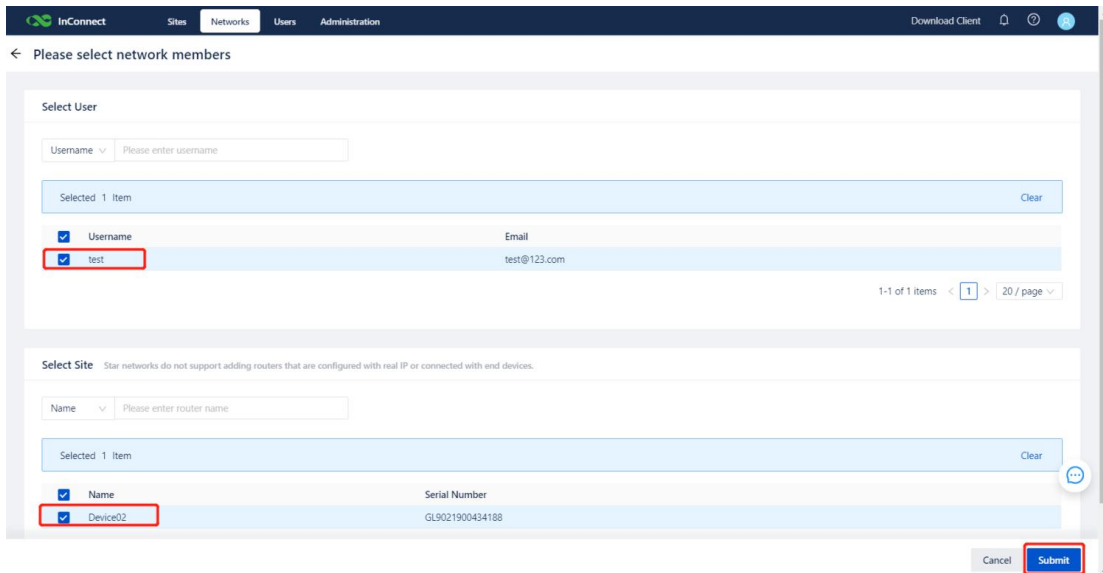
Ping statistics for 10.5.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

6.2.2. Adding a Site or User to a Star Network

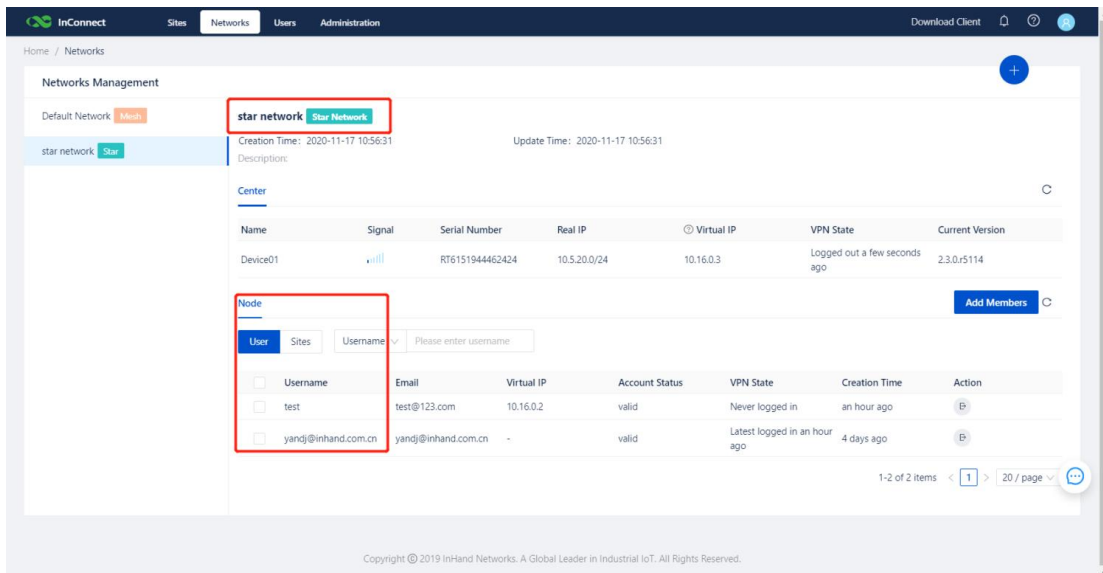
1. Choose **Networks>Add Members**.



2. Select the user name and site name, and click **Submit**.

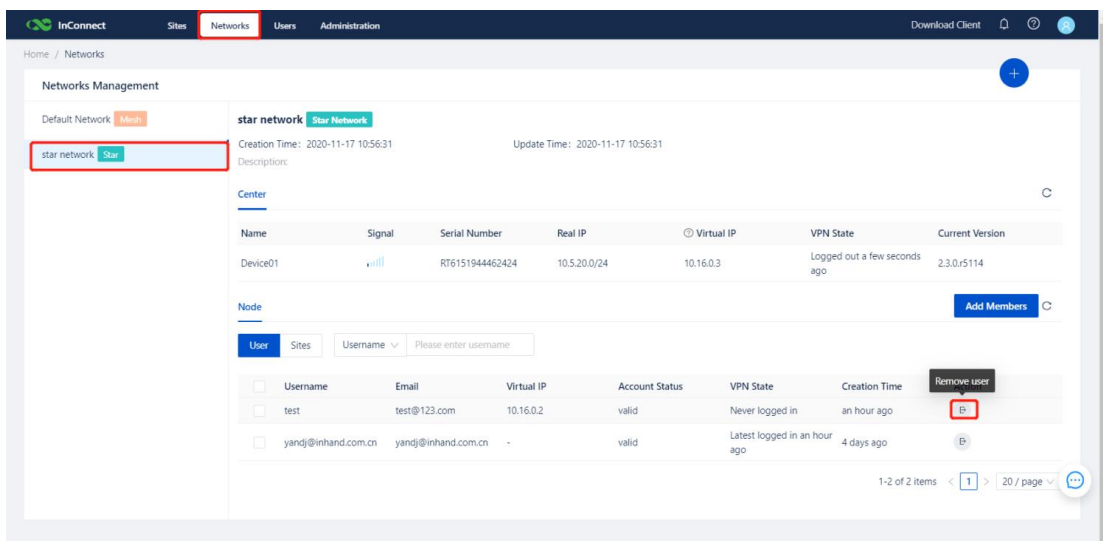


3. Check the information about the added network.

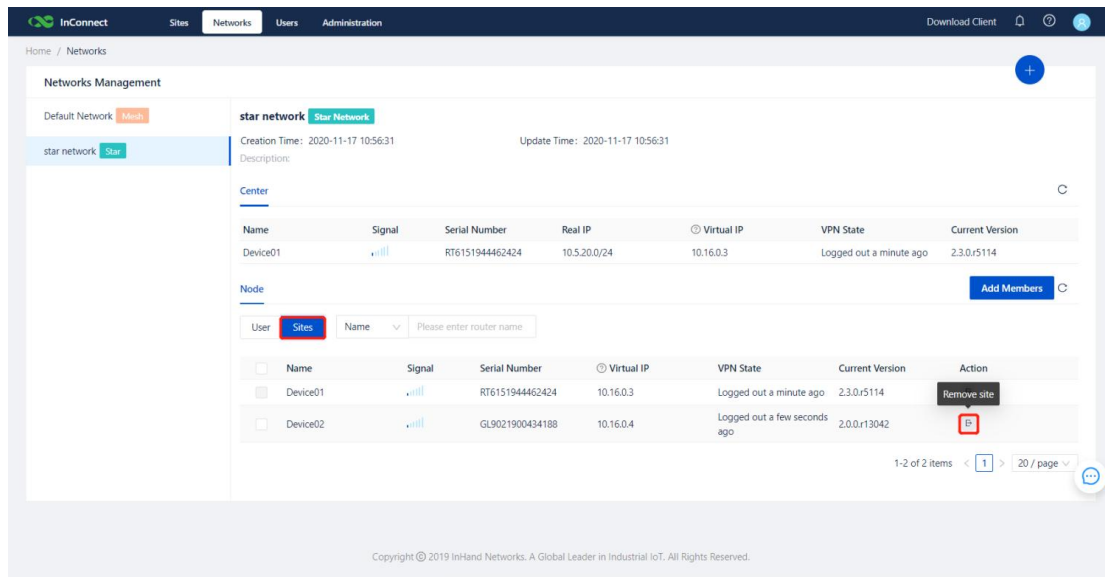


6.2.3. Deleting a Star Network

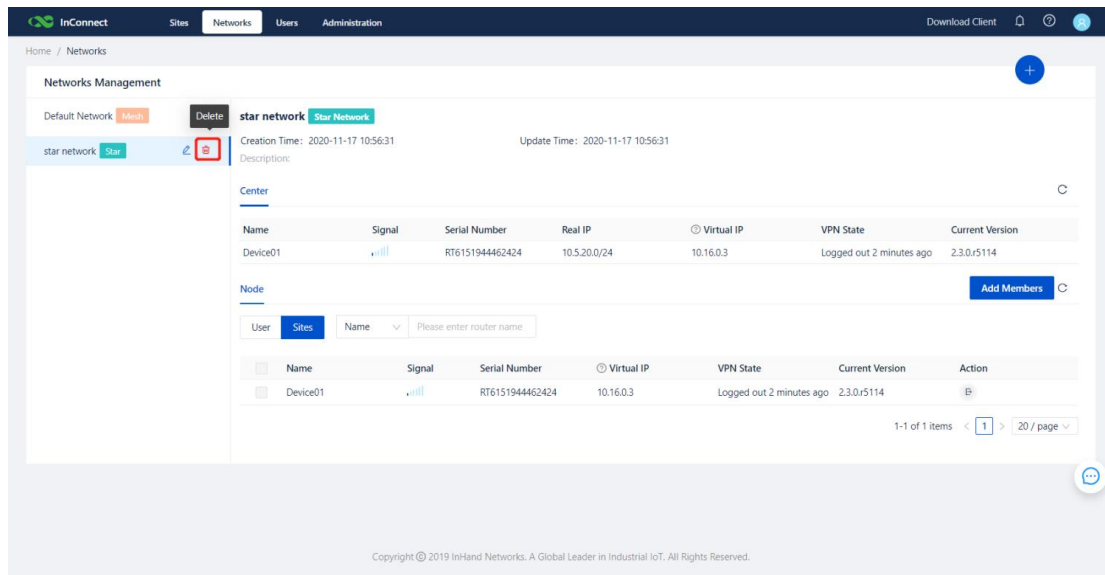
1. Select Networks, and click the target network name in the Network Management list.



2. Select **Sites**, and click the **Remove site** icon.

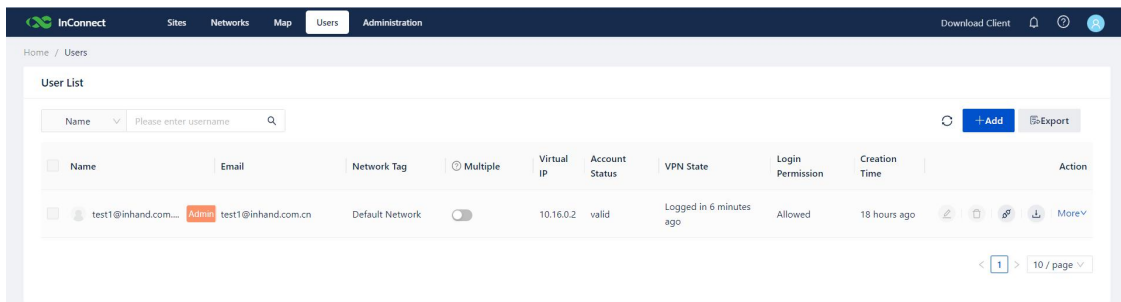


3. Select the target network name, and click the **Delete** icon to delete the star network.



7. User Management

1. Adding a user
 - a. Click **Users** and then **Add** to create an account for another system user.



- b. Fill in the information of the added user.



Caution

Login Permission: indicates whether to allow the user to log in to InConnect. After a user with **Login Permission** set to **Allowed** is added, InConnect will send an email containing the login information to the mailbox of the user. If you want to create an account that can only be used to access the network but cannot log in to InConnect, set **Login Permission** to **Not Allowed**.

2. Role description: InConnect supports two user roles that have different permissions on system functions.
 - Administrator: has the permission to view all the data and the network management permission.
 - Common user: only has the permission to perform basic operations on the devices in the specified type of network.
3. Multi-terminal description:

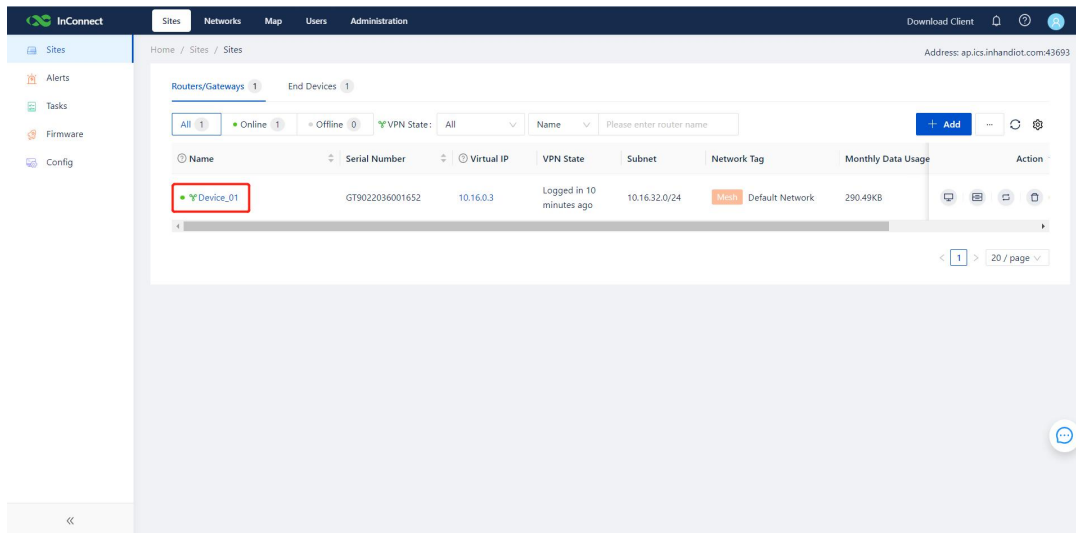
Name	Email	Network Tag	Multiple	Virtual IP	Account Status	VPN State	Login Permission	Creation Time	Action
test1@inhand.com...	test1@inhand.com.cn	Default Network	<input type="checkbox"/>	10.16.0.2	valid	Logged in 8 minutes ago	Allowed	18 hours ago	More

- If **Multiple** is enabled for a user, the user can access remote devices on multiple terminals in a secure manner.
- The virtual IP addresses of multiple terminals are different. Therefore, after **Multiple** is enabled, the **Virtual IP** column is no longer displayed on the web page.

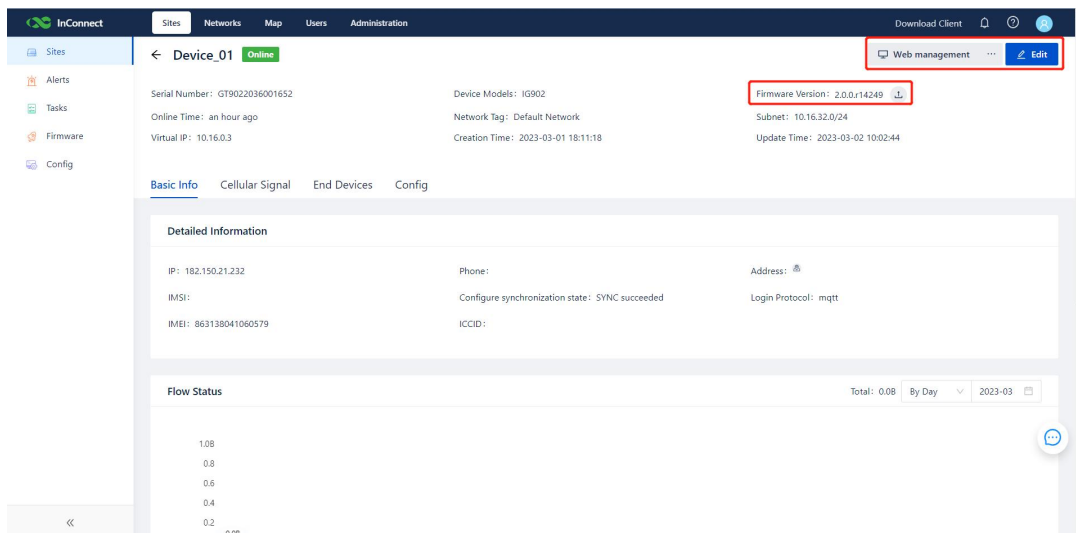
8. Router/Gateway Management

8.1. Router Details


- Click **Sites**, and select a router name on the **Routers** page to check the router details.

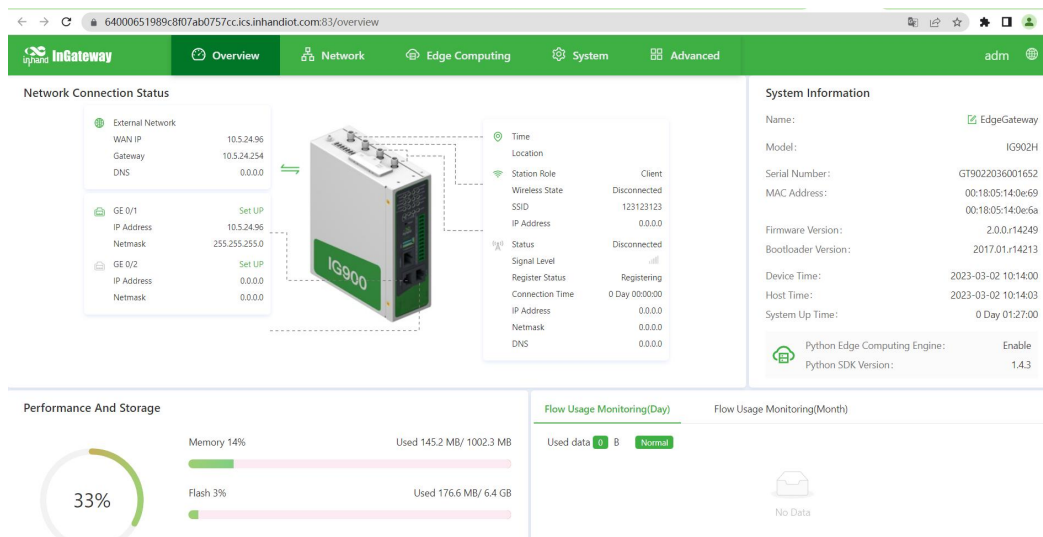
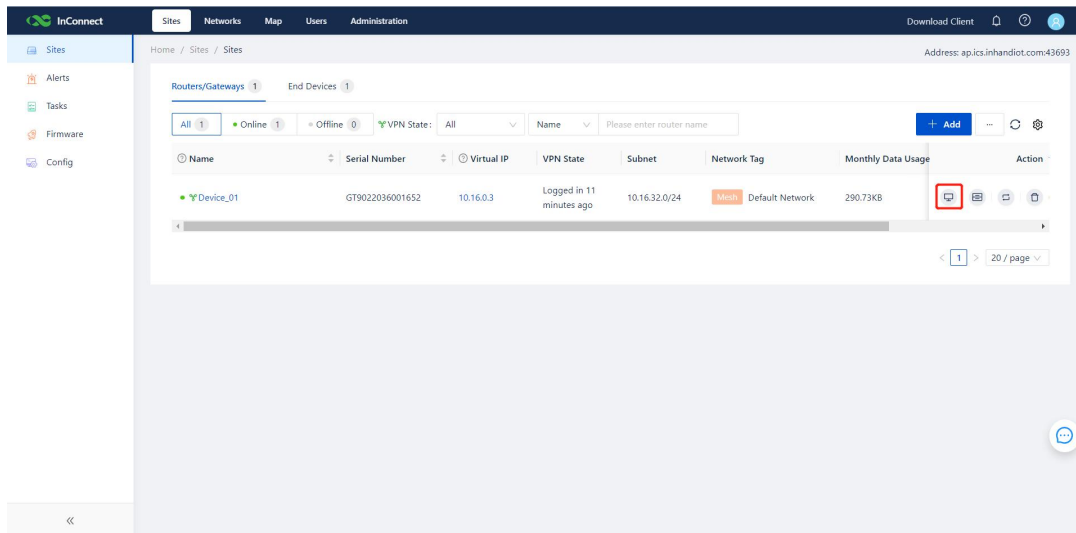


- You can perform operations on online routers, such as remote web management, remote configuration, forced offline, and firmware upgrade.



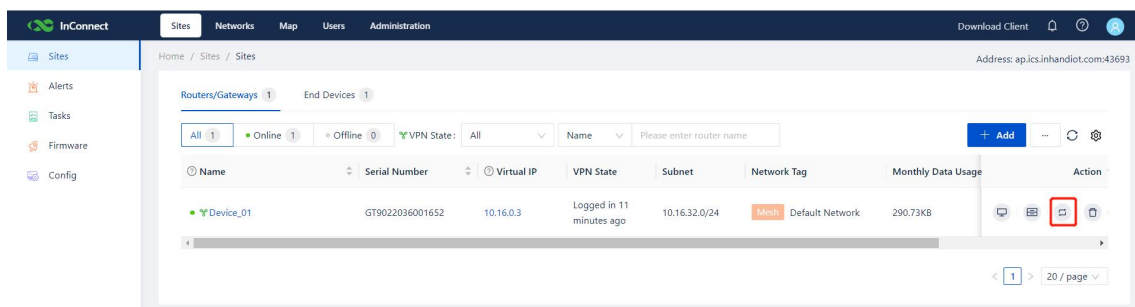
8.2. Remote Web Management

- You can access the router's web management page remotely through InConnect.
- Click  to go to the router's web management page, and perform remote router management on this page.



8.3. Delivering the Connection Configuration

- After a router or a downstream device is added, InConnect automatically delivers the running configuration to create a secure network connection.
- When a router is online but VPN is in logout state, you can click the running configuration delivery button to set up the connection again.

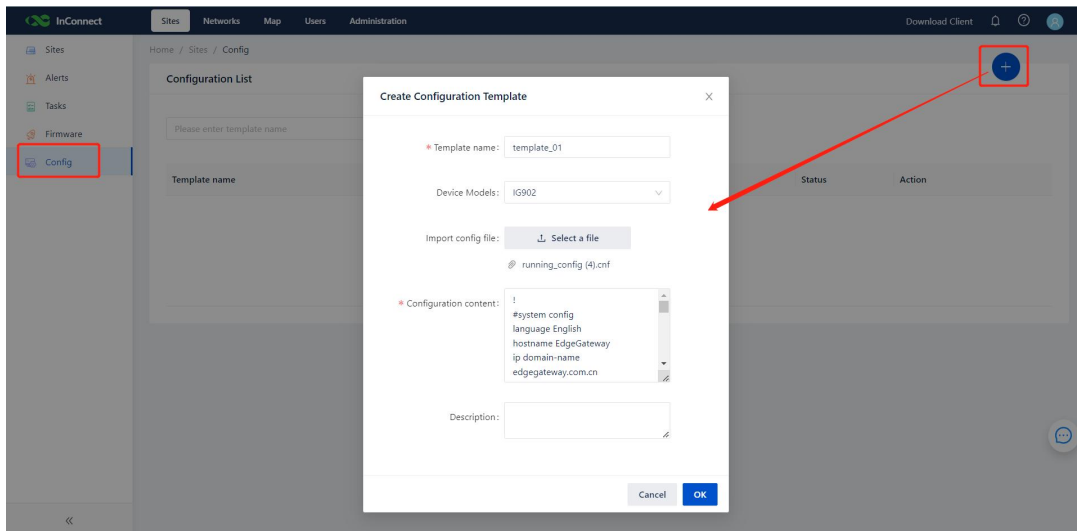


8.4. Remotely Updating the Router Configuration

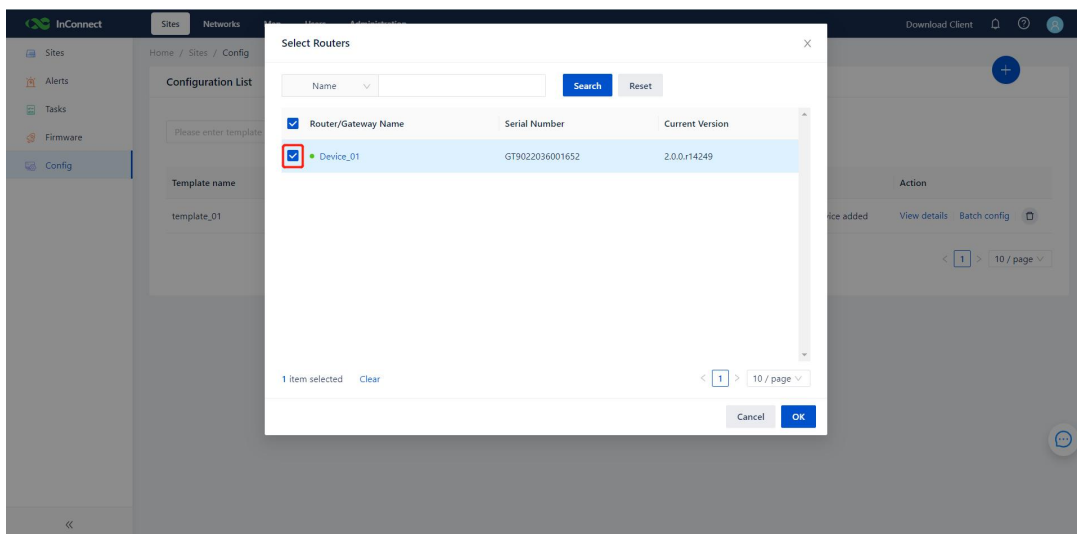
You can use this function to update the configurations of routers connected to InConnect in batches.

1. Adding a configuration template
 1. Click **Config** and then **+**. Select a configuration file or enter the configuration content.

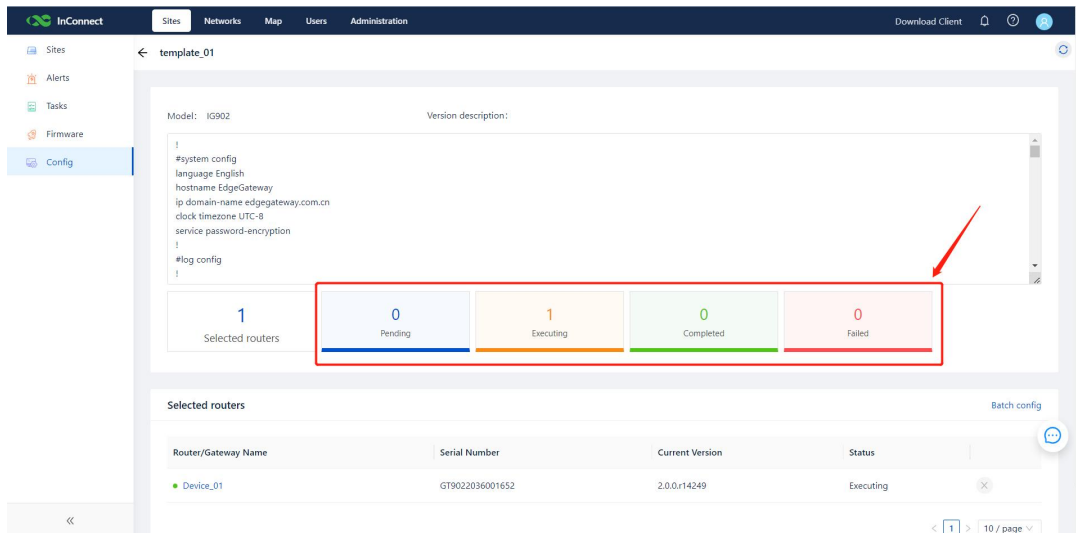
2. On the local management page of the router, you can download the original configuration file, modify the configuration file as needed, and then upload the file to InConnect to update the router configurations in batches.



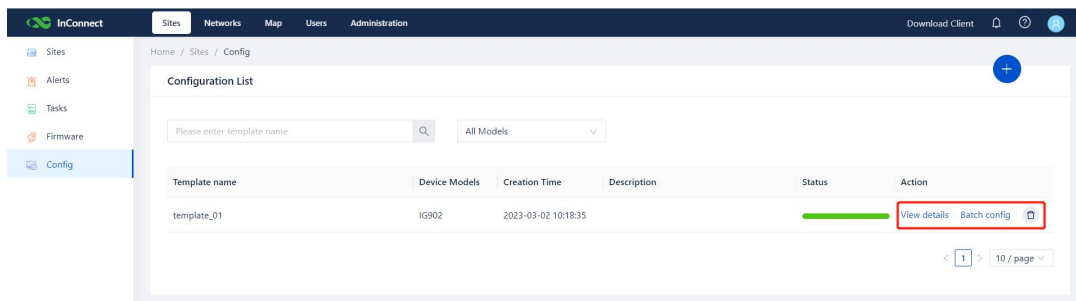
2. Select the routers to which you want to deliver the configurations. Then, the configurations are updated in batches.
 1. Online routers update their configurations as soon as they receive the configuration command.
 2. Offline routers will update their configurations after they are online again.



3. On the configuration details page, you can view the update progress and status of all the routers to which this configuration is applied.



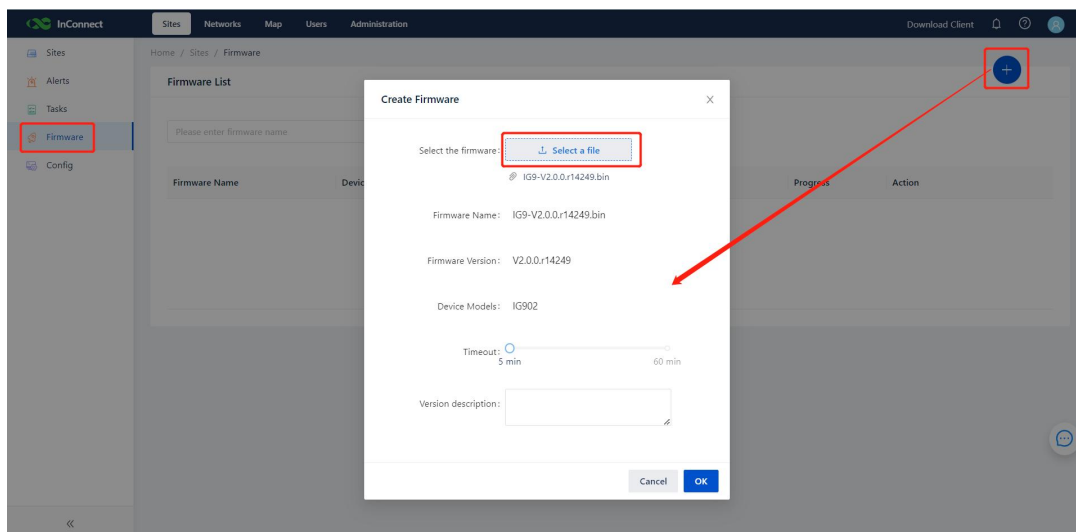
4. On the **Configuration List** page, you can view or delete a configuration or update configurations in batches.



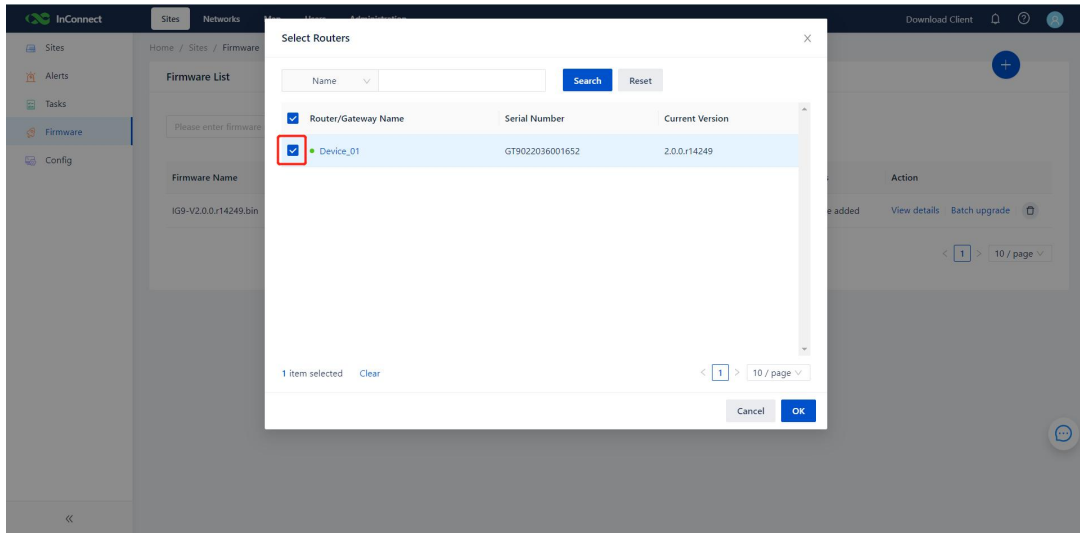
8.5. Remotely Upgrading the Router Firmware

You can use this function to upgrade the firmware for routers connected to InConnect in batches.

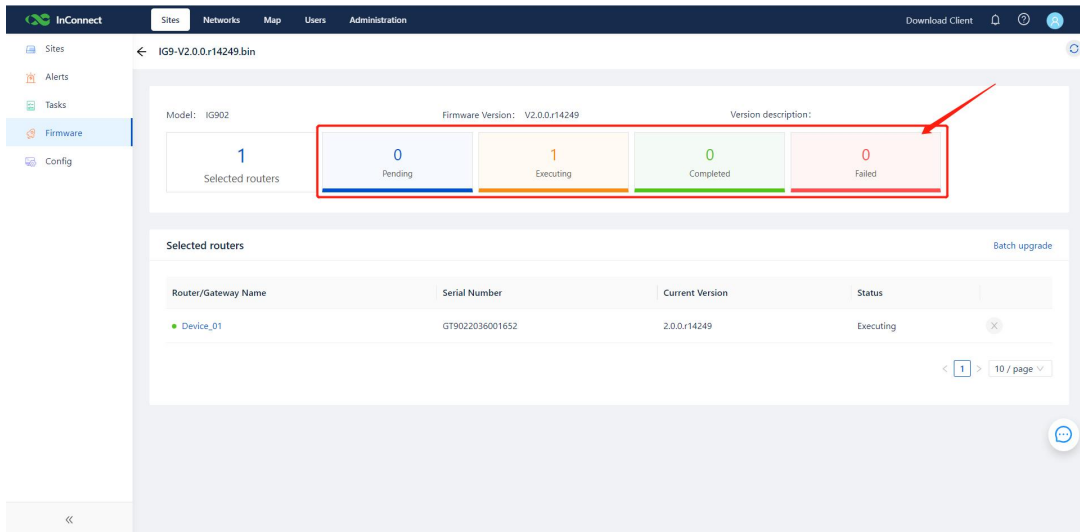
1. Adding the firmware
 1. Click **Firmware** and then **+**. Select the firmware you want to upgrade and click **OK**. The firmware is uploaded to InConnect.



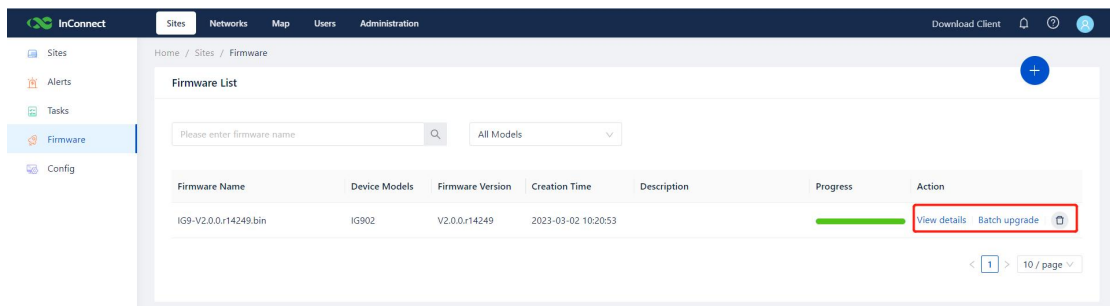
2. In the router list, select routers, and click **OK** to upgrade the firmware of the selected routers.
 1. Online routers perform the upgrade task as soon as they receive the upgrade command.
 2. Offline routers will perform the upgrade task after they are online again.



- On the firmware details page, you can view the firmware upgrade progress and status of the related routers.



- On the **Firmware List** page, you can view or delete a firmware record or upgrade the firmware in batches.



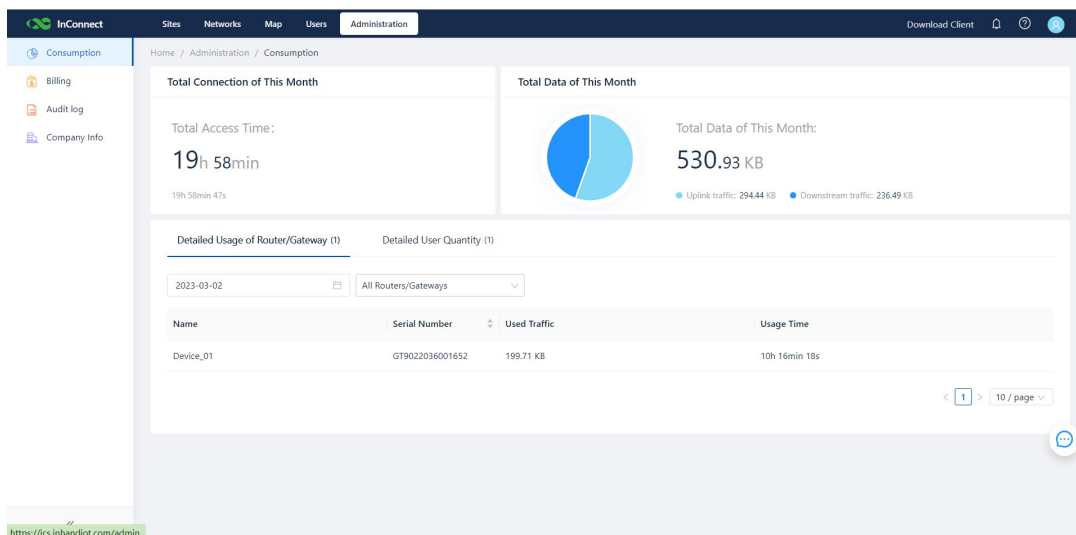
8.6. Tasks

- On the **Tasks** page, you can view the tasks delivered by InConnect to routers, and redeliver or cancel these tasks.

Router/Gateway Name	Type	Status	Progress	Created By	Creation Time	Start Time	Update Time	Action
Device_01	Import Firmware Package	COMPLETED	<div style="width: 100%;"></div>	System	2 minutes ago	2 minutes ago	a minute ago	C D
Device_01	run config apply	COMPLETED	<div style="width: 100%;"></div>	System	4 minutes ago	4 minutes ago	4 minutes ago	C D
Device_01	Remote Web Management	COMPLETED	<div style="width: 100%;"></div>	test1@inhand.com.cn	9 minutes ago	9 minutes ago	9 minutes ago	C D
Device_01	run config apply	COMPLETED	<div style="width: 100%;"></div>	test1@inhand.com.cn	20 minutes ago	20 minutes ago	20 minutes ago	C D
Device_01	run config apply	COMPLETED	<div style="width: 100%;"></div>	System	25 minutes ago	25 minutes ago	25 minutes ago	C D
Device_01	run config apply	CANCELED	<div style="width: 100%;"></div>	System	33 minutes ago	33 minutes ago	25 minutes ago	C D
Device_01	run config apply	CANCELED	<div style="width: 100%;"></div>	System	34 minutes ago	34 minutes ago	33 minutes ago	C D
Device_01	run config apply	CANCELED	<div style="width: 100%;"></div>	System	35 minutes ago	35 minutes ago	34 minutes ago	C D
Device_01	run config apply	CANCELED	<div style="width: 100%;"></div>	System	36 minutes ago	36 minutes ago	35 minutes ago	C D
Device_01	fetch running config	COMPLETED	<div style="width: 100%;"></div>	System	16 hours ago	3 minutes ago	3 minutes ago	C D

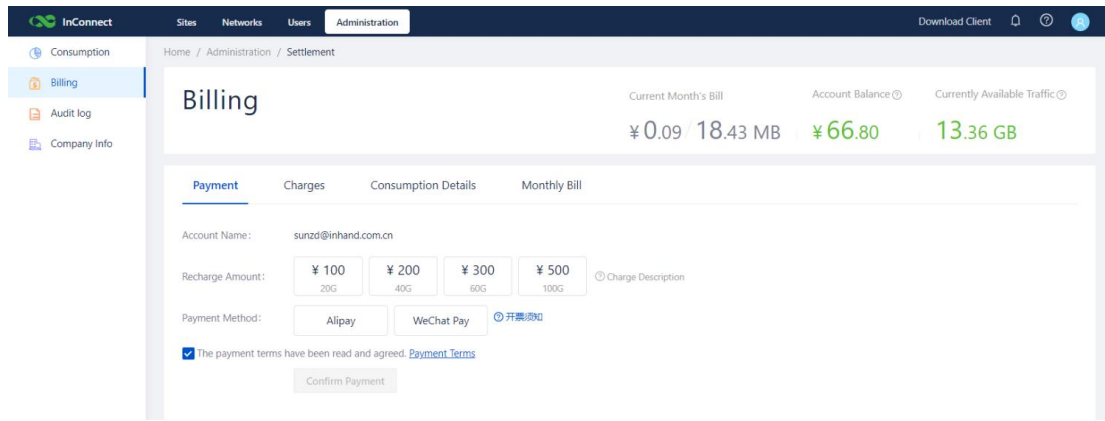
9. Consumption

- On the **Consumption** page, you can view the traffic consumed by a router or user to create the secure connection.
- The total connection duration and total traffic are updated every hour, and the detailed usage of routers and users is updated every minute.



10. Billing

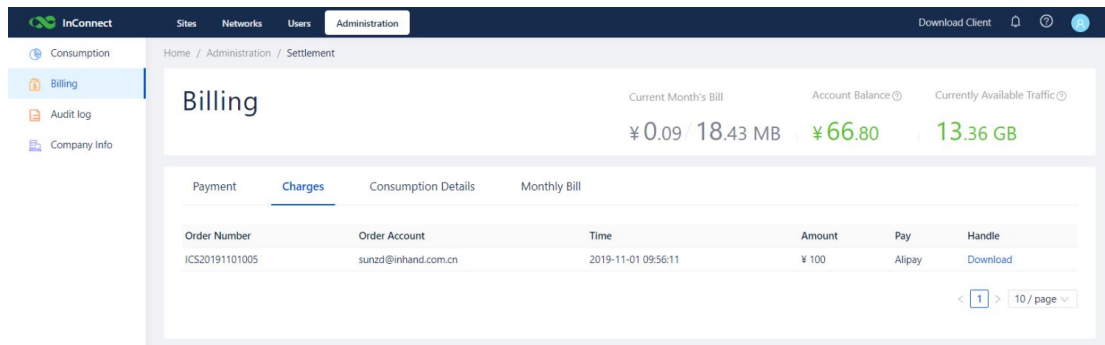
- The InConnect service is billed based on the traffic that is used to create the secure connections between all clients and users.
- On the Billing page, you can recharge the account for the networking services provided by InConnect. Before payment, you must agree with the Payment Terms.



Caution

To ensure normal service connection, InConnect provides a 10-GB traffic credit. If you do not recharge your account after the 10-GB traffic credit is used up, your InConnect service is suspended. After you recharge your account to the traffic credit, your service is restored immediately.

- After recharging, you can view your charges details on the **Charges** tab page or download the receipt to view your order details.
- InConnect updates your consumption logs periodically on the **Billing** page based on your usage.
- It sends a monthly bill through email on the first day of each month, and the bill records your traffic consumption and billing information of the previous month.



11. FAQs

- **Q1: How many user accounts and routers can I add to one InConnect account?**

A1: You can add a maximum of 4,000 user accounts and routers. A router can connect to a maximum of 254 downstream devices.

- **Q2: How is the InConnect service billed?**

A2: It is billed by the data traffic generated by the VPN channel communication between routers, end devices and users at a unit price of US\$ 2.5/GB.

- **Q3: What is the minimum monthly traffic for a router if it does not generate any traffic data and the network is normal?**

A3: About 30-40 MB.

- **Q4: Where is the InConnect server deployed? Amazon in U.S. and Amazon in China?**

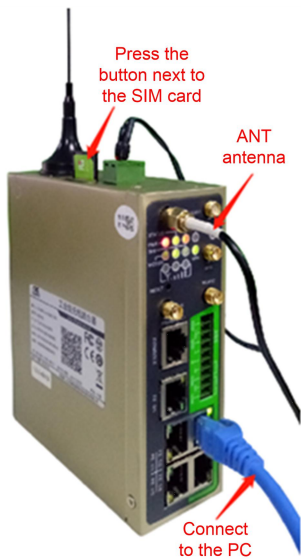
A4: For users in China, the server is deployed in Amazon in China. For users outside China, the server is deployed in Amazon in U.S.

12. Appendix: Router Networking

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

The following takes IR915 as an example. For details about networking of other devices, see the hardware user manual or visit <https://www.inhandnetworks.com/>.

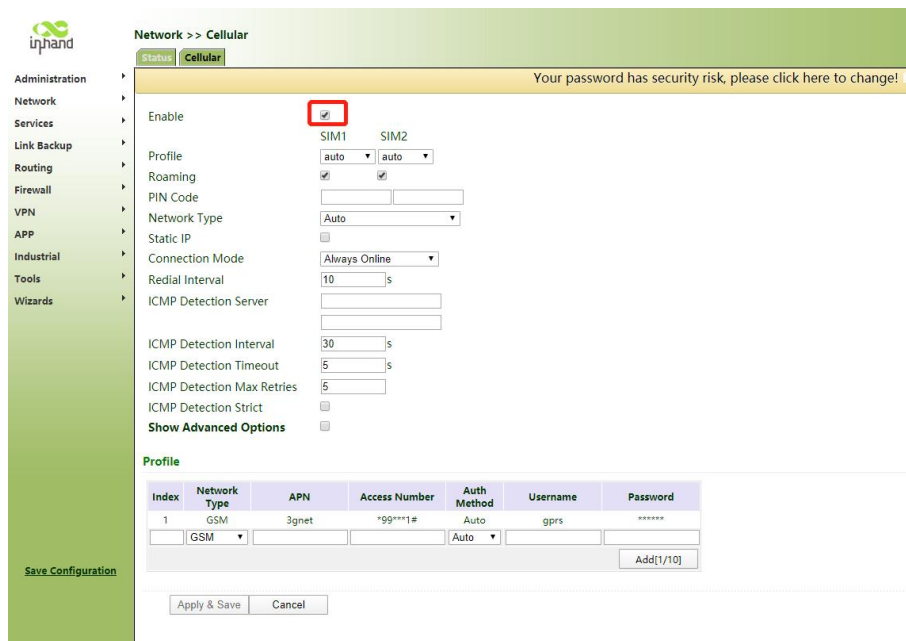
1. Insert the SIM card to the slot 1 and tighten the 4G LTE antenna to the ANT terminal.



Caution

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.

2. Open the browser and log in to the device. (See [Method 2: Ethernet](#)).
3. Choose **Network>>Cellular>>Enable**. Wait until the network connection status is **Connected** and an IP address is allocated. Then, the network is connected through the SIM card. If a private network card is still used, fill in the dial-up parameter set.



Network >> Cellular

Status: Cellular

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

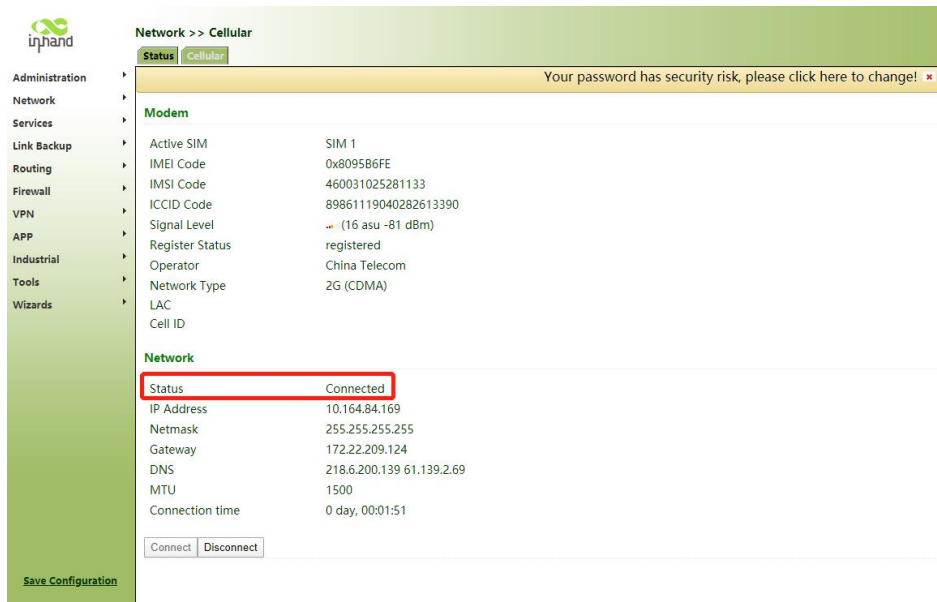
Enable

Profile: 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:

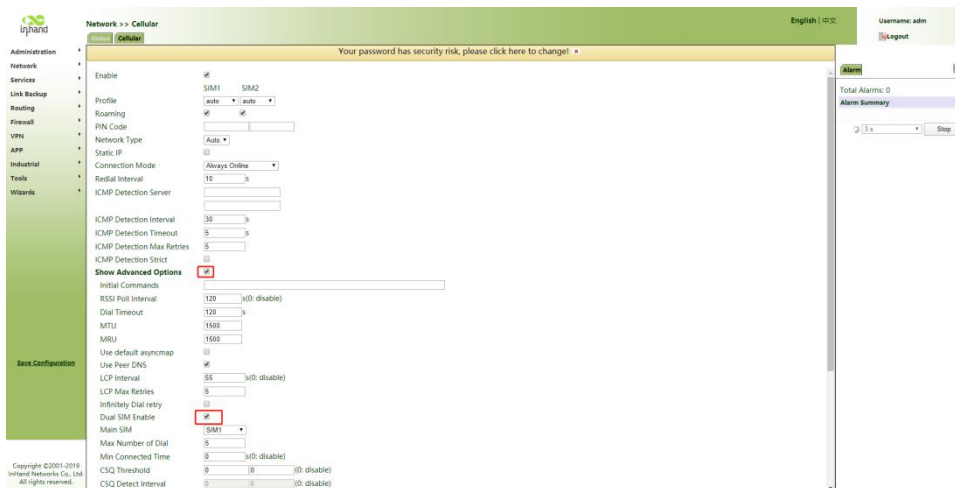
Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99**1#	Auto	gprs	*****

Save Configuration

Apply & Save Cancel



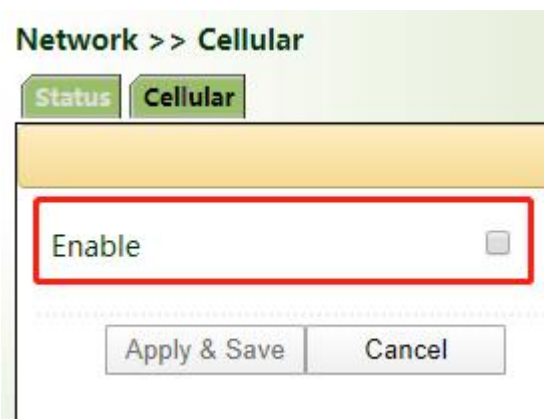
4. When two SIM cards are inserted to the device, select **Dual SIM Enable**.



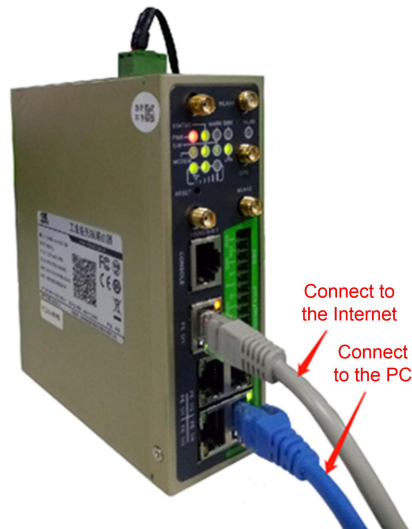
Method 2: Ethernet

The following takes IR915 as an example. For details about networking of other devices, see the hardware user manual or visit <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.



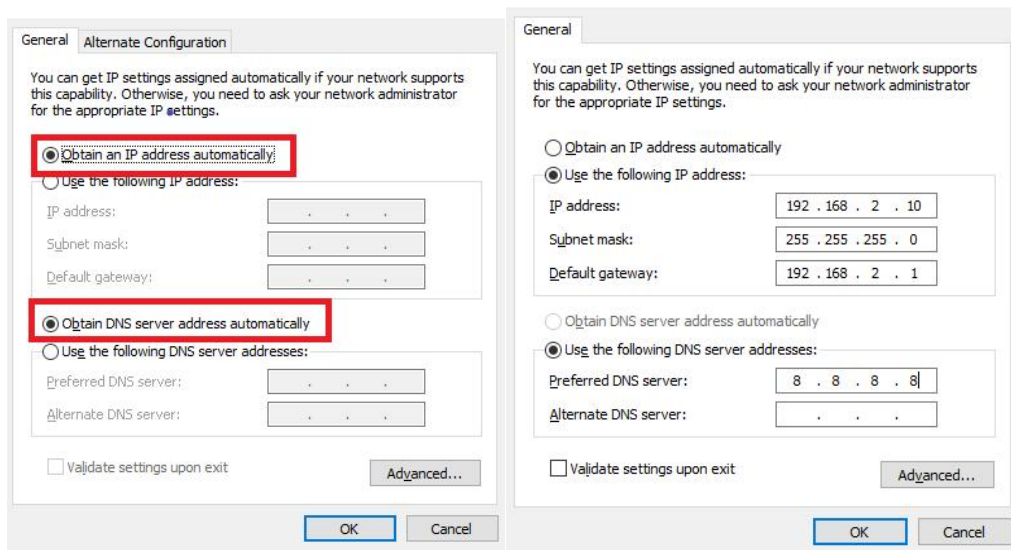
1. Connect the LAN (FE 1/1 or GE1/1) port to a PC and the WAN port to the Internet.



2. Set the IP addresses of the PC and router to be in the same network segment.

Method 1: Automatically get the IP address (recommended)

Method 2: Use a fixed IP address. Set the EF/GF ports of the PC and router to be in the same network segment. Set the initial IP address of the router 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**.



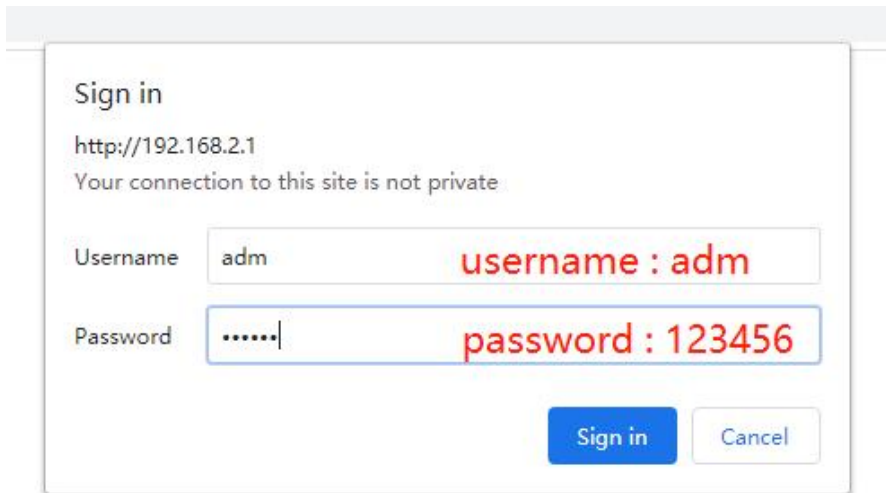
Automatically get the IP address

Use a fixed IP address

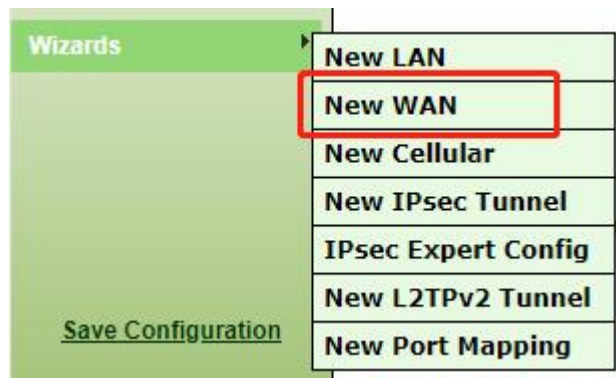
3. In the address bar of the browser, enter the default gateway address 192.168.2.1 to enter the gateway web login page.



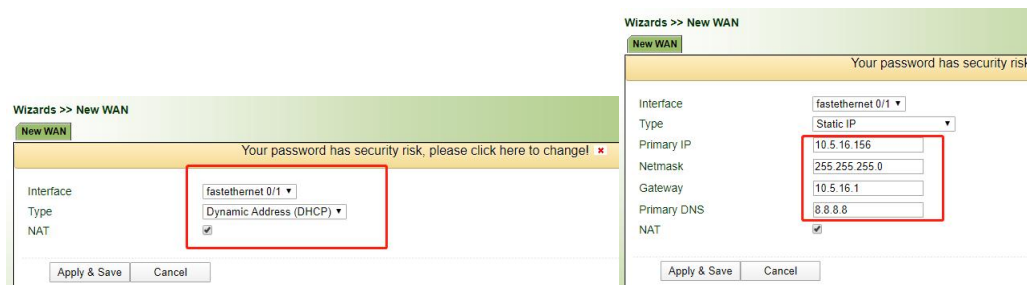
4. Enter the username and password and then click **Sign In**.



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

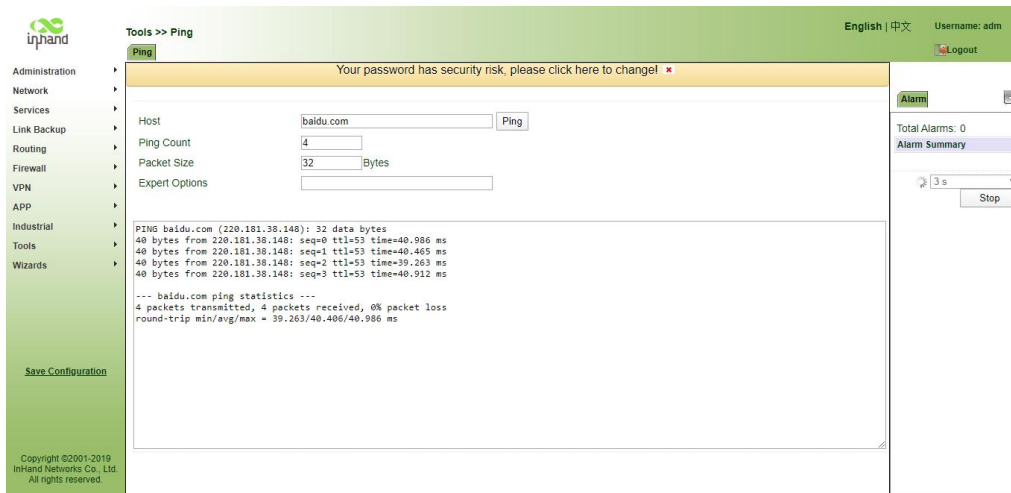


6. We recommend that you select **Dynamic Address (DHCP)**. If you select **Static IP Address**, manually configure the network parameters and then save the configuration.



Dynamically allocate the IP address Configure parameters of the static IP address

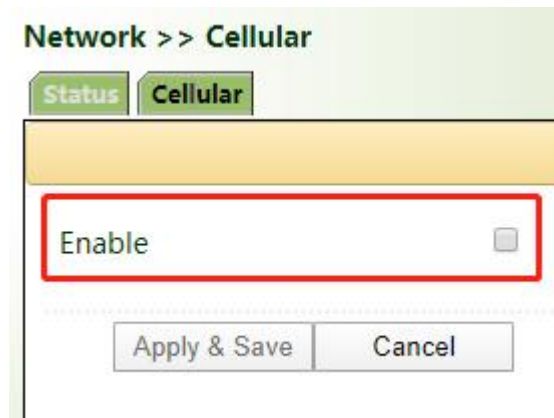
7. Choose **Tools**>>**Ping**. In the **Host** field, enter a common Chinese website to test whether the router can connect to the Internet. If the following figure is displayed, the router can connect to the Internet.



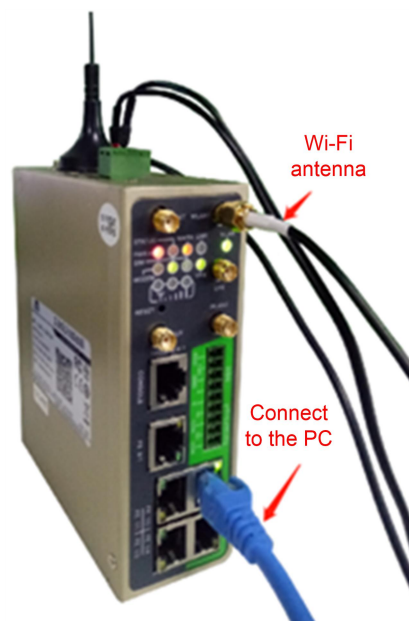
Method 3: Wi-Fi

The following takes IR915 as an example. For details about networking of other devices, see the hardware user manual or visit <https://www.inhandnetworks.com/>.

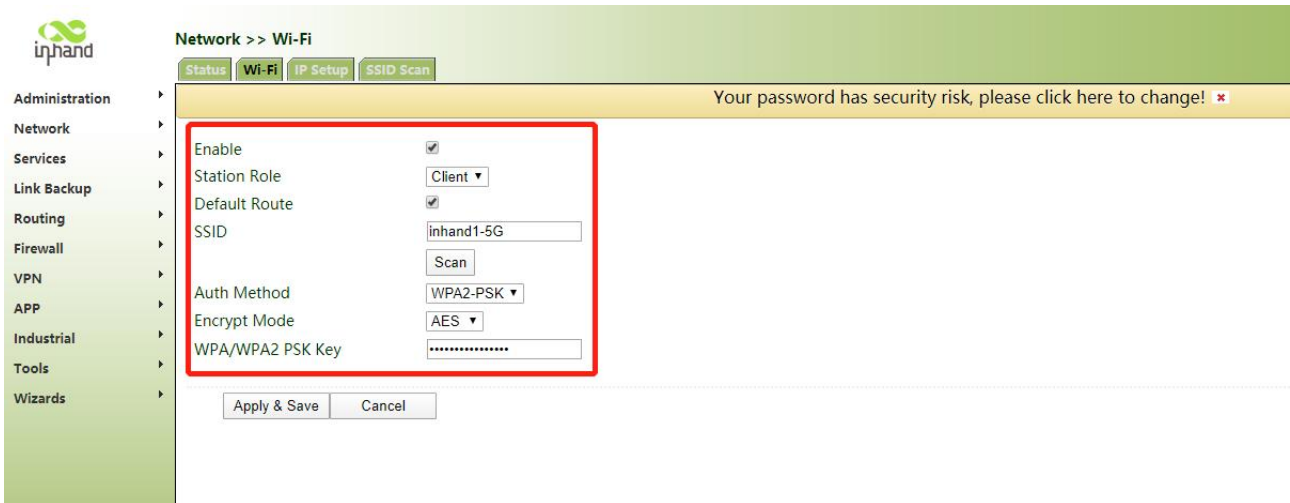
Disable the "cellular interface" when accessing the network without the SIM card; otherwise repeated dial-up is performed, interfering the network connection.



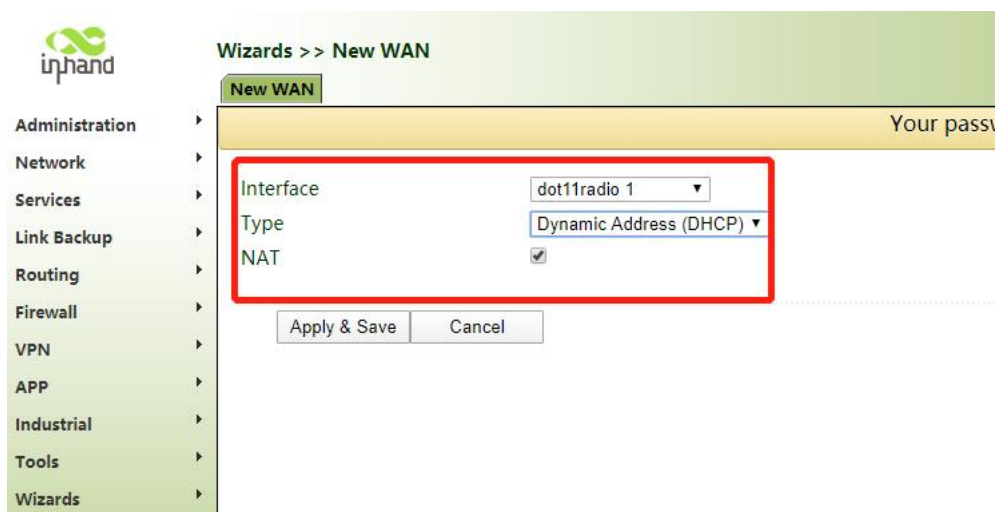
1. Use a network cable to connect the PC to the gateway LAN port, and connect the Wi-Fi antenna to the WLAN1/2 port.



2. Set the IP addresses of the PC and the router to be in the same network segment. (See [Method 2: Ethernet](#)).
3. Access the device web management page. (See [Method 2: Ethernet](#)).
4. Choose **Network>>WLAN**, select **Client** from **Interface Type**, enter the Wi-Fi parameters, and then click **Apply & Save**. Click the **Status** tab. The network connection status is **Connected**.



5. Choose **Wizards>>New WAN**, and configure the parameters as follows:



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

The screenshot shows the configuration page for NAT rules in the iphond interface. The page title is "Firewall >> NAT". A warning message at the top states: "Your password has security risk, please click here to change! ✖".

The main section is "Network Address Translation(NAT) Rules". It contains a table with the following data:

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

Below the table are "Add", "Modify", and "Delete" buttons. The "Add" button is highlighted in green.

The "Inside Network Interfaces" section contains a table with the following data:

ID	Interface
1	gigabitethernet 0/1
2	

The "Outside Network Interfaces" section contains a table with the following data:

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

At the bottom of the page are "Apply & Save" and "Cancel" buttons. A "Save Configuration" link is located in the bottom left corner of the sidebar.