

PUSR DM Platform

User Manual



Industrial IoT Gateways Ranked First in China by Online Sales for Seven Consecutive Years

**Data from China's Industrial IoT Gateways Market Research in 2023 by Frost & Sullivan

Your Trustworthy Smart Industrial IoT Partner

Content

1. Product Overview	- 4 -
2. User Management	- 4 -
2.1. Registration and Login	- 4 -
2.1.1. Account Registration	- 4 -
2.2. User Center	- 5 -
2.3. Organization Management	- 6 -
2.3.1. Organization Management	- 6 -
2.3.2. Role Management	- 7 -
2.3.3. Member Management	- 8 -
3. Gateway Management	- 8 -
3.1. Gateway List	- 8 -
3.1.1. Adding Gateways	- 9 -
3.1.2. Gateway Basic Information	- 10 -
3.1.3. Remote Built-in Web Page	- 10 -
3.2. Firmware Upgrade	- 11 -
3.2.1. Single Device Upgrade	- 11 -
3.2.2. Batch Upgrade	- 12 -
4. SD-VPN Management	- 13 -
4.1. Mesh Network	- 14 -
4.1.1. Network Topology	- 14 -
4.1.2. Create mesh network	- 14 -
4.1.3. Add site	- 15 -
4.1.4. Add terminal device	- 15 -
4.1.5. Add users	- 15 -
4.1.6. Download and install client app	- 16 -
4.1.7. Verifying the mesh Network	- 17 -
4.2. Star Network	- 19 -
4.2.1. Create star network	- 19 -
4.2.2. Add the sub site	- 19 -
4.2.3. Add terminal device to the sub site	- 20 -
4.2.4. Add users	- 20 -

4.2.5. Download and install client app	- 20 -
4.2.6. Verifying the star Network	- 22 -
5. FAQ	- 25 -
6. Contact Us	- 26 -
7. Disclaimer	- 26 -

1. Product Overview

The DM Platform is a monitoring and operation platform powered by PUSR Cloud for PUSR gateways and routers. It provides online statistics, basic information viewing, firmware upgrades, and cross-region networking capabilities for routers. It supports remote access to PUSR routers and gateways and the device connected to the routers and gateways on Lay3. This service can replace complex VPN solutions, facilitating remote access to cameras, remote configuration of PLCs and industrial computers, remote program downloads for PLCs, file transfers to industrial computers or PLCs, and remote terminal upgrades. It helps customers manage routers and terminal devices in a unified and efficient manner.

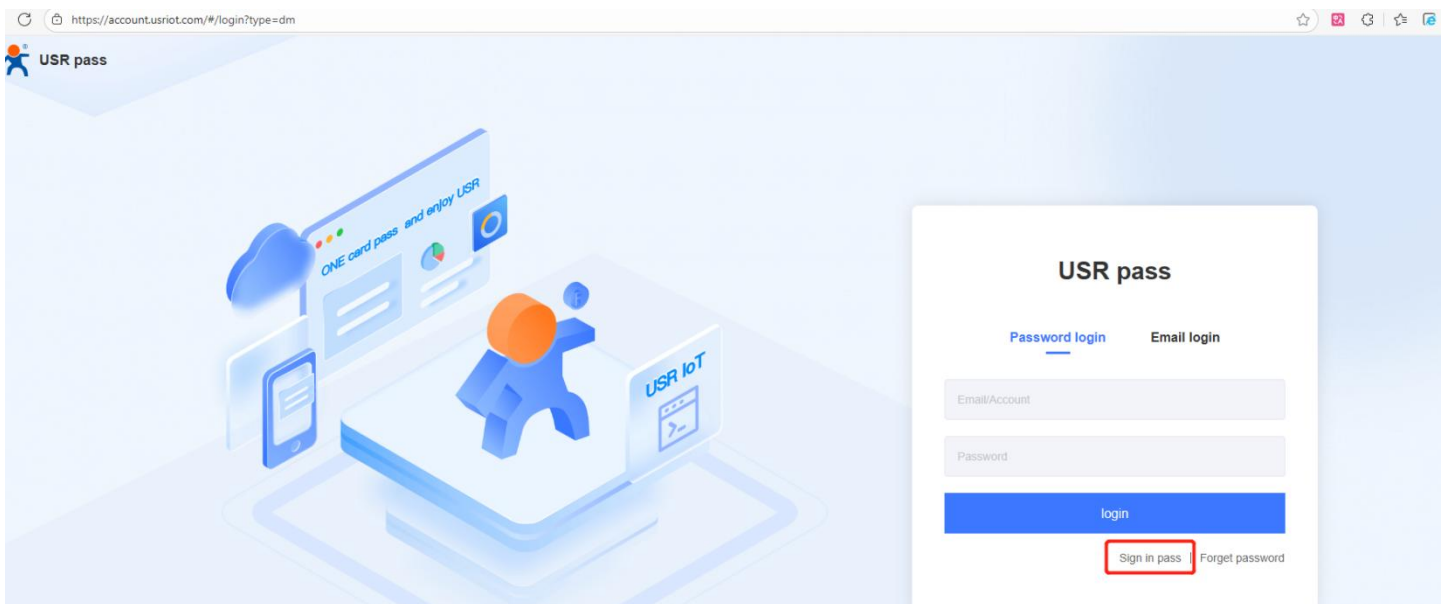
2. User Management

2.1. Registration and Login

DM Management Platform URL: <https://dm.usriot.com>

2.1.1. Account Registration

Users can register by filling in the required information and log in using a password or Email verification.



Registered pass account

* Email

* Verification Code

* Password

* Confirm Password

TimeZone

* Company

* Industry

☐ [Read and accept the USR agreement](#)

Existing account, [login](#)

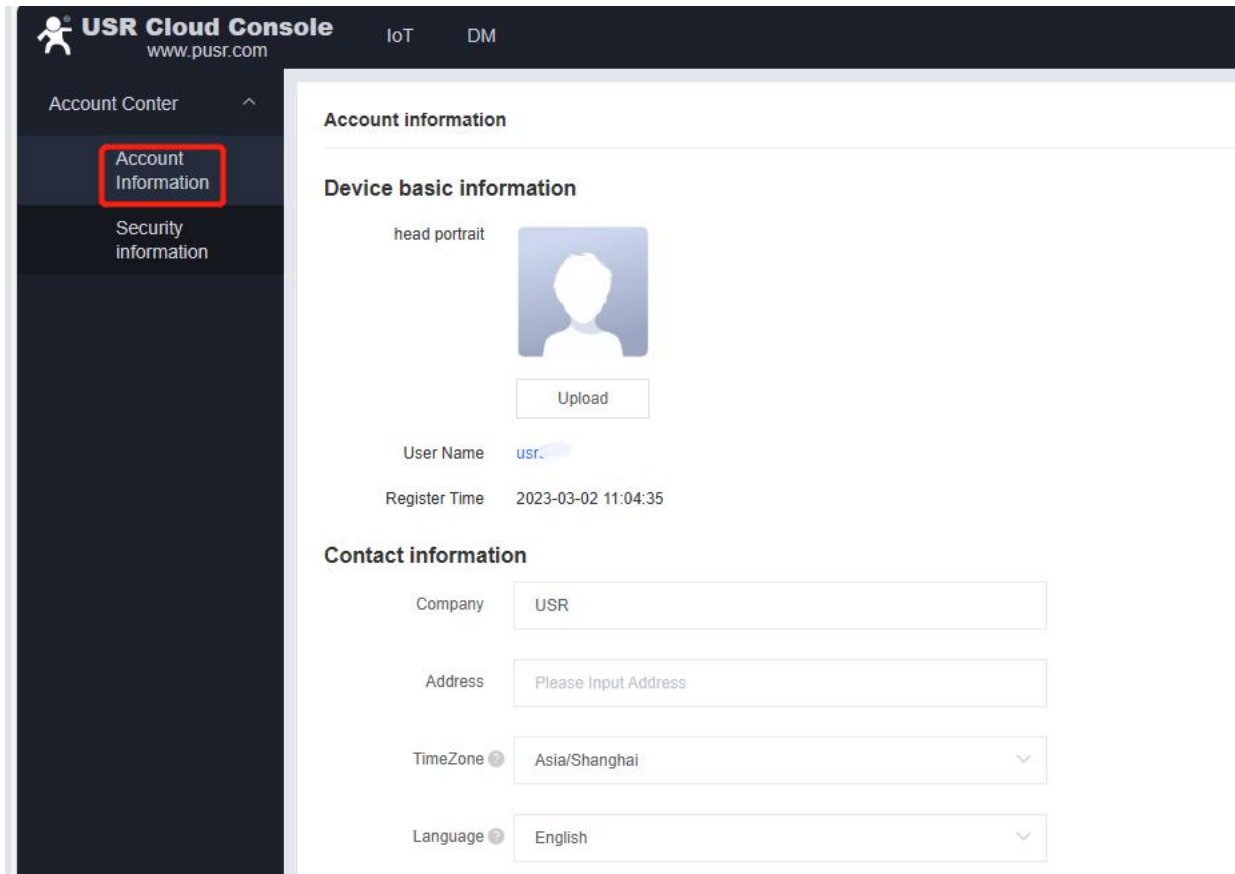
2.2. User Center

Users can view basic account information and security settings in the User Center.

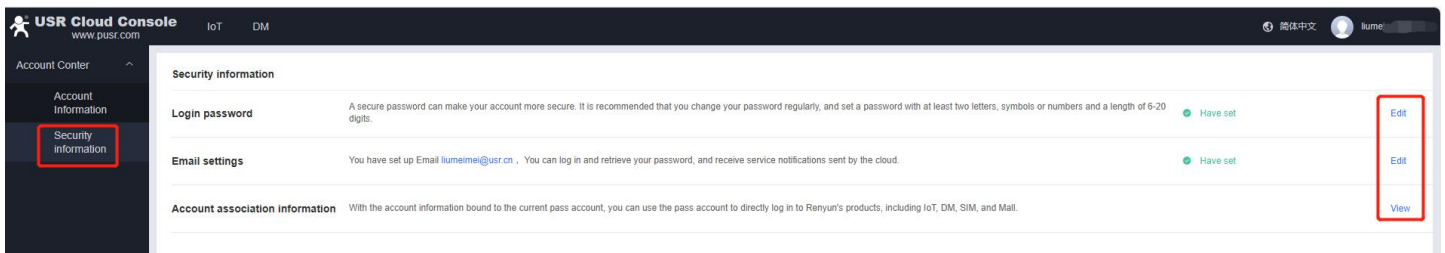
The screenshot shows the USR Cloud Console interface. On the left is a sidebar with navigation options: Gateway management, Gateway list, Batch configuration, Firmware upgrade, Parameter terminate, Network management, Value-added services, and Data center. The main area displays the 'Gateway list' with a table of gateways. At the top right of the main area, there is a 'User Center' menu item highlighted with a red box, along with 'Organization management' and 'Logout' options.

Gateway name	Gateway status	SN	Gateway model	parameter lock	column.Firmware_Version	Belonging organize	Gateway address	Tag
Gateway name90	Online	01603 311	USR-G809s-43	--	V1.0.05	My Project	--	
U200S	Offline	308023 727	U200S	--	V2.72	My Project	250101, Lixia Qu, Jinan Shi, Shandong, ...	
USR-G809s-GPS	Offline	000076 01	Unknown type	--	--	My Project	Automatic positioning	

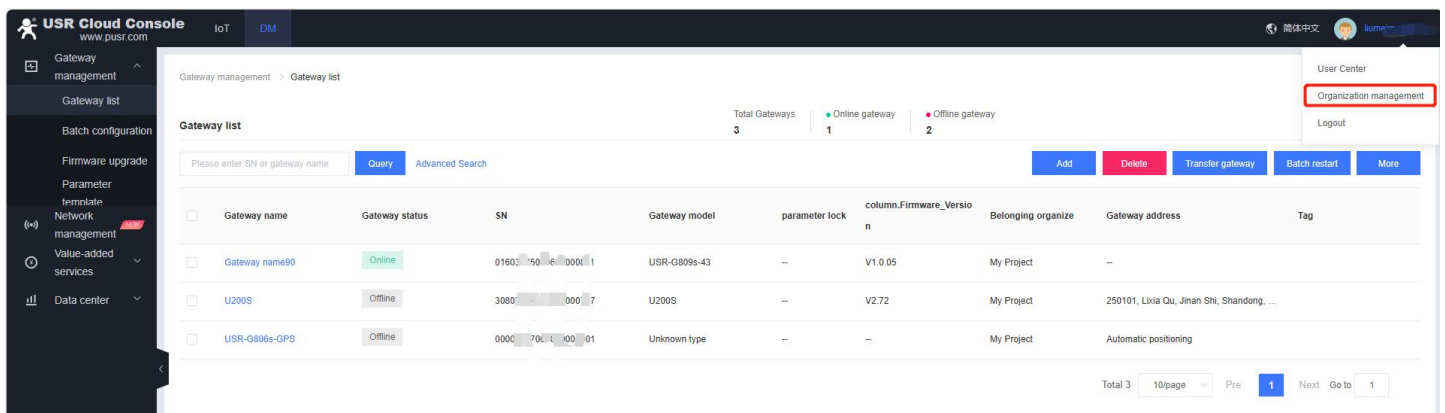
Account Information



Security Information: users can set password and email information on this page.

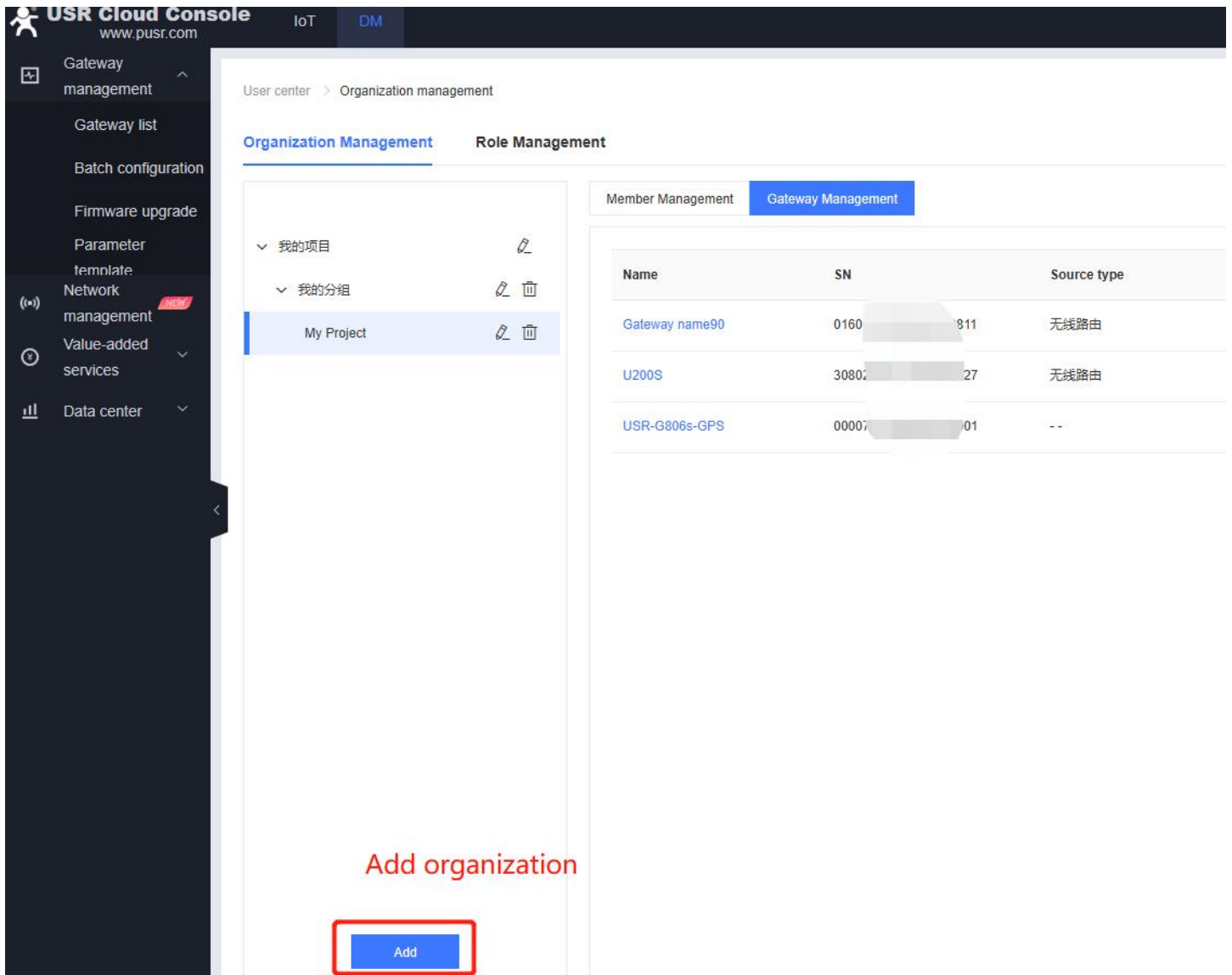


2.3. Organization Management



2.3.1. Organization Management

This function allows users to group gateways for easier management.



2.3.2. Role Management

Assigns different permissions to users based on their roles.

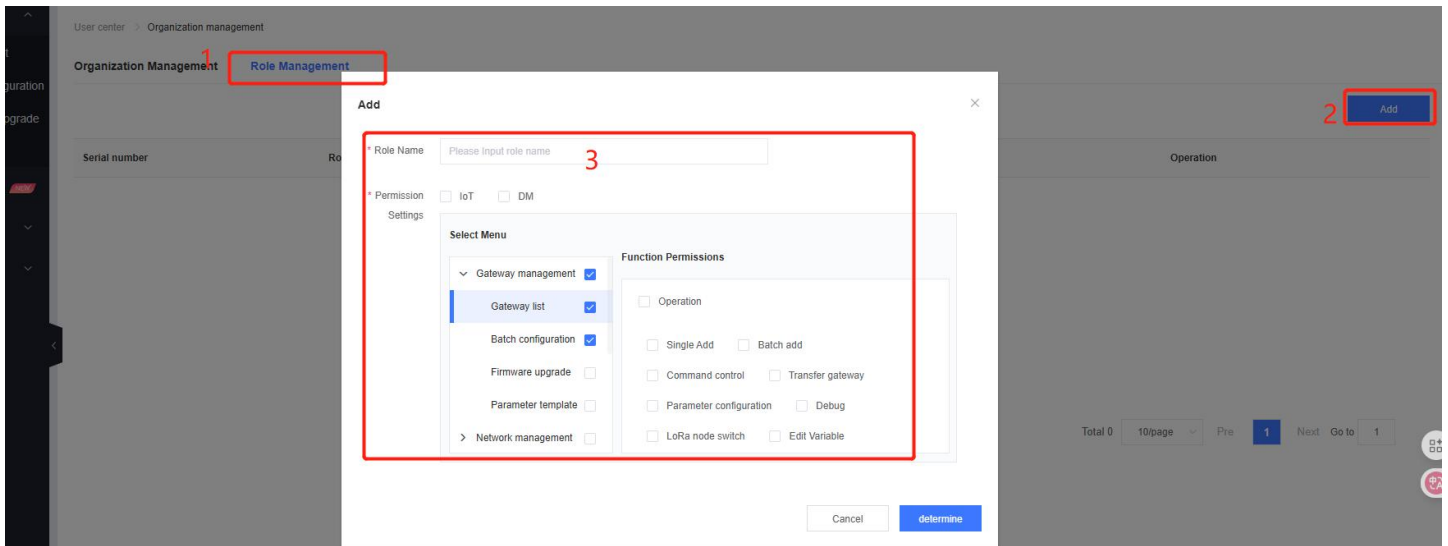
Role name: set the role name

IoT/DM: If it is checked, it means this role have the permission to the IoT/DM,

If it is not checked, it means this role have not the permission to the IoT/DM.

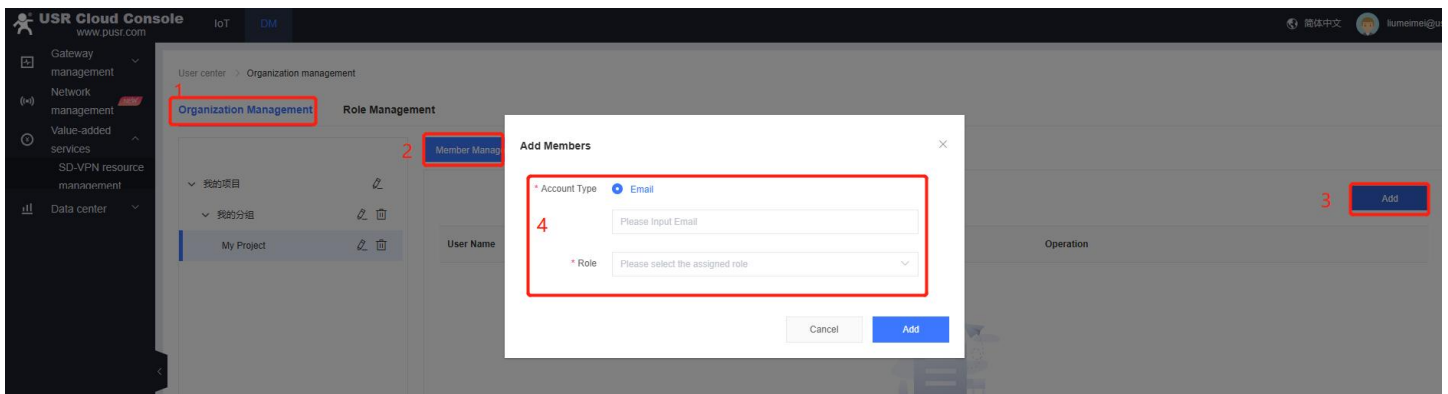
Select menus: Select the menu option displayed on the left side of this user interface

Function permissions: Select to allow the user to use/view the functions under the corresponding menu



2.3.3. Member Management

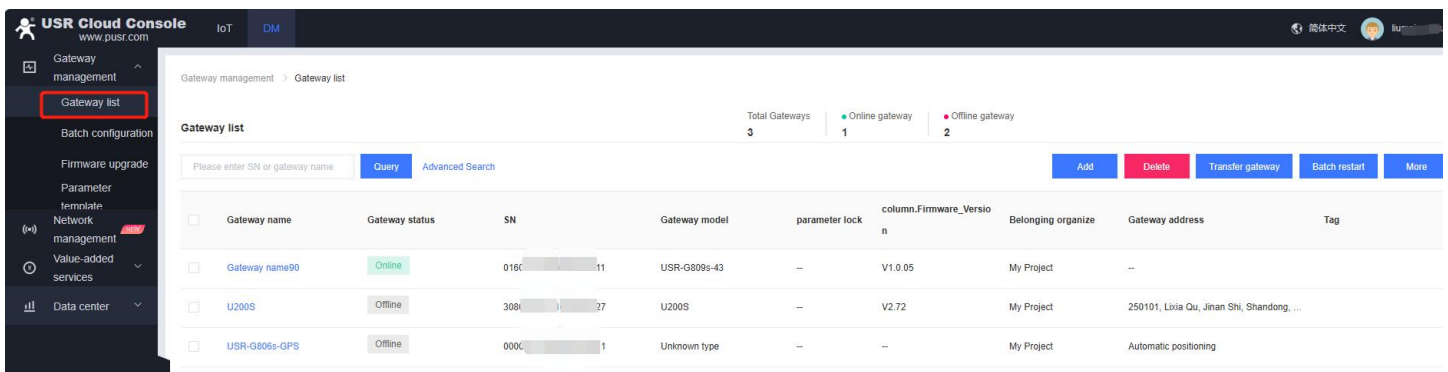
Adds sub-accounts using email and assigns permissions through role selection. Note: Sub-accounts cannot create secondary accounts.



3. Gateway Management

3.1. Gateway List

Provides basic functions such as adding, deleting, modifying, and querying gateways, as well as checking gateway status and online statistics.



3.1.1. Adding Gateways

Gateways can be added individually by entering the SN and MAC/IMEI from the router label or imported in bulk using a template.

Gateway list

Please enter SN or gateway name

Query

Advanced Search

Add

Delete

Transfer gateway

Batch restart

More

☐	Gateway name	Gateway status	SN	Gateway model	parameter lock	column.Firmware_Versio n	Belong	Single Add Batch Add	Gateway address	Tag
☐	Gateway name90	Online	016031-0000811	USR-G809s-43	--	V1.0.05	My Project		--	
☐	U200S	Offline	30802-00000727	U200S	--	V2.7.2	My Project		250101, Lixia Qu, jinan Shi, Shandong, ...	
☐	USR-G806s-GPS	Offline	00007-00000001	Unknown type	--	--	My Project		Automatic positioning	

Single add: the SN and IMEI/MAC is listed on the label pasted on the device, and the other parameters can be set by users.

USR Cloud Console
www.pusr.com

IoT DM

Gateway management > Gateway list > Add Gateway

Add Gateway

* Gateway name

* Belonging organize

* SN [SN does not support, click here](#)

* MAC / IMEI

Positioning method ☒ Manual positioning ☐ Automatic positioning

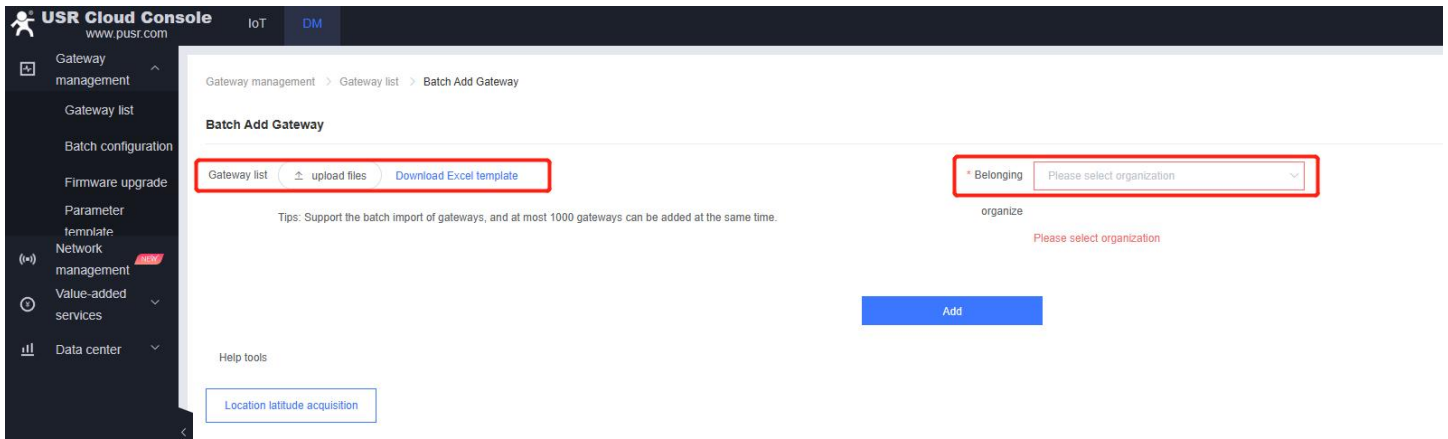
Gateway address [Map](#)

Tag

Network monitoring ☒

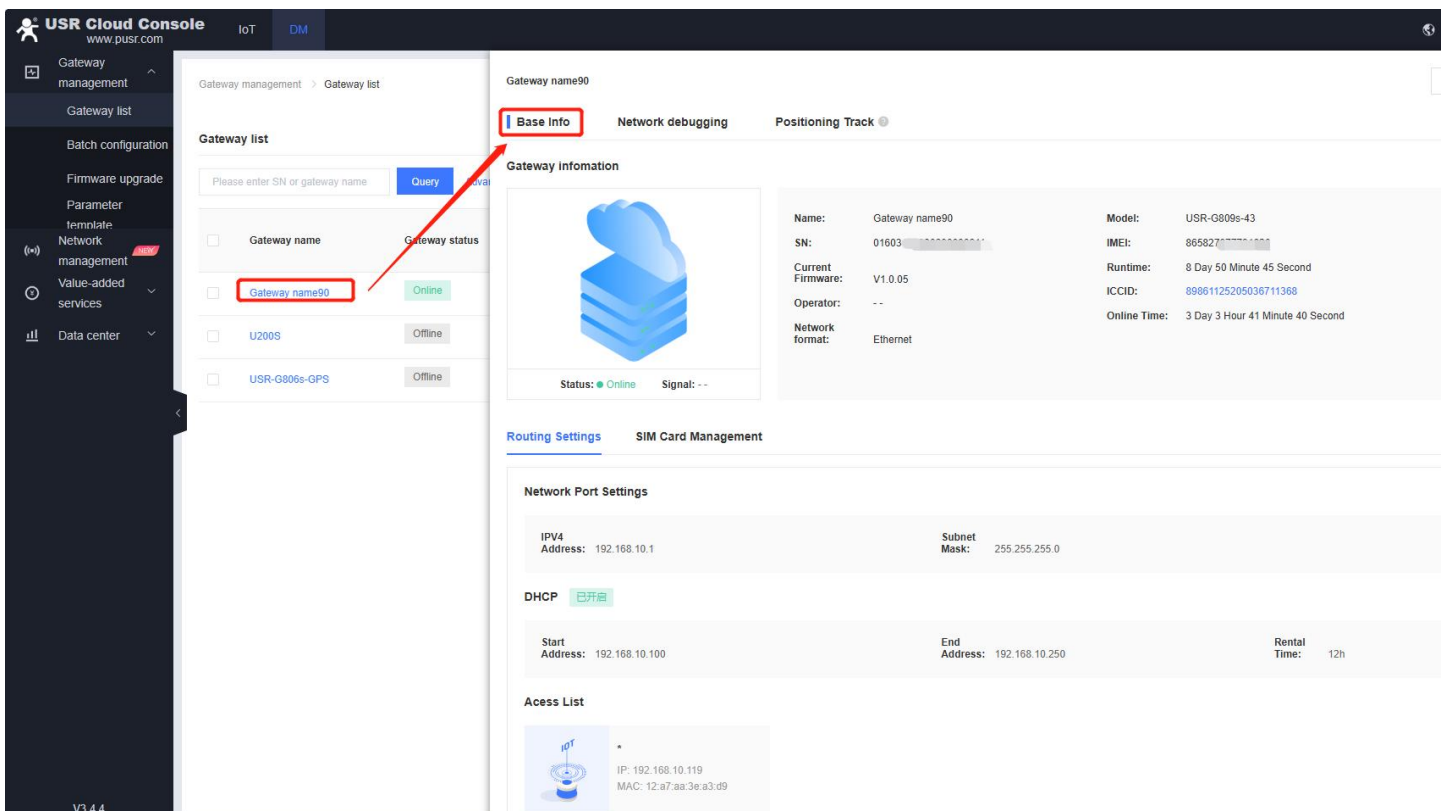
USR data transparency ☐

Batch add: users can download the excel template, and fill in the necessary information, and then upload the excel file to add multiple devices.



3.1.2. Gateway Basic Information

Displays basic router information, including SN, MAC, IMEI, network format, online time, and signal strength.



3.1.3. Remote Built-in Web Page

Allows remote access to the gateway/router's WEB interface via a public domain for visual configuration and efficient remote maintenance.

Note: Not all the gateway/routers support this function, if you need this function, please contact the sales man.

Gateway name90

Edit More

Base Info Network debugging Positioning Track

Gateway information



Name:	Gateway name90	Model:	USR-G809s-43
SN:	01603125000000000011	IMEI:	86582700000000000000
Current Firmware:	V1.0.05	Runtime:	8 Day 50 Minute 45 Second
Operator:	--	ICCID:	89861125205036711368
Network format:	Ethernet	Online Time:	3 Day 3 Hour 41 Minute 40 Second

Disable
Configuration page
Command control
Firmware Upgrade
Reboot gateway
Reload to factory settings
Delete

Click the configuration page, it opens a new tab page, after filling the password, users can log router's web page and can set/check router/gateway's parameters.

USR-G809

Auto | English | 中文

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

Authorization Required

Please enter your username and password.

Username: admin

Password:

Login Reset

USR-G809

Status

System

Hostname	USR-G809
Firmware Version	V1.0.05
SN	016031250806000000811
IMEI	865827077791820
Local Time	Fri Sep 19 17:29:36 2025
Uptime	8d 1h 4m 16s
Load Average	1.38, 1.52, 1.59

3.2. Firmware Upgrade

Supports single and batch firmware upgrades for routers/gateways.

3.2.1. Single Device Upgrade

Gateway list--> click "gateway name" --> more--> firmware upgrade

Gateway management

Gateway list

Please enter SN or gateway name

Query

Gateway name

Gateway status

Gateway name90 Online

U200S Offline

Gateway name90

Base Info Network debugging Positioning Track

Gateway information

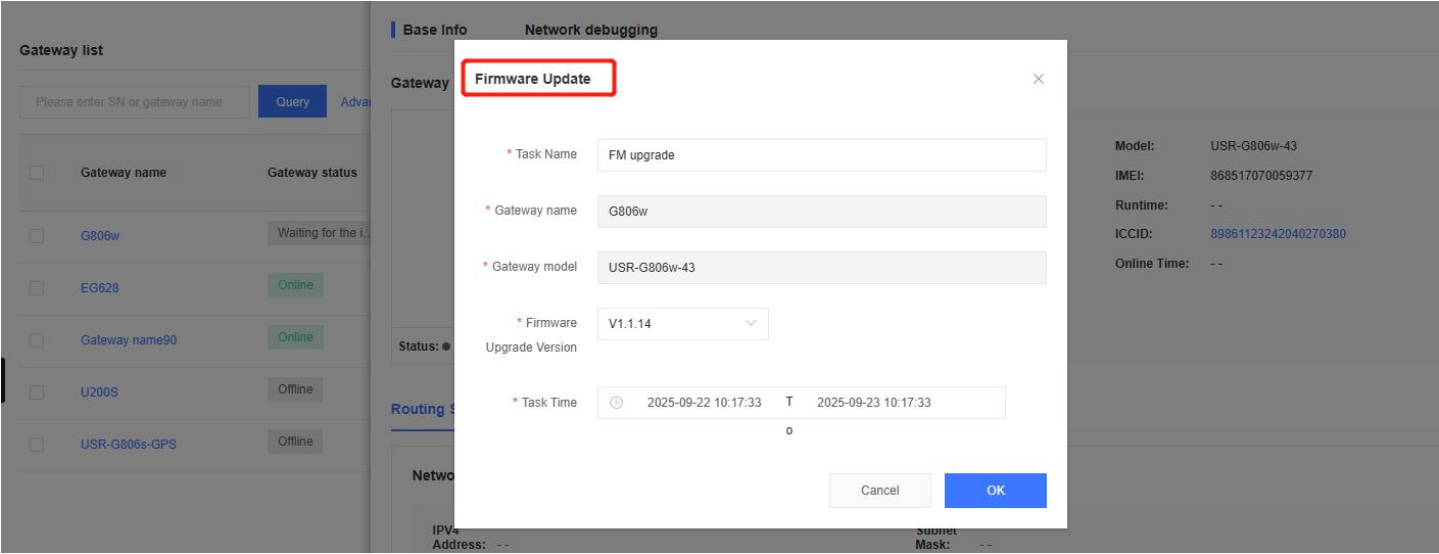


Name:	Gateway name90	Model:	USR-G809s-43
SN:	01603125000000000000	IMEI:	86582700000000000000
Current Firmware:	V1.0.05	Runtime:	8 Day 1 Hour 24 Minute 59 Second
Operator:	--	ICCID:	89861125205036711368
Network format:	Ethernet	Online Time:	3 Day 4 Hour 15 Minute 54 Second

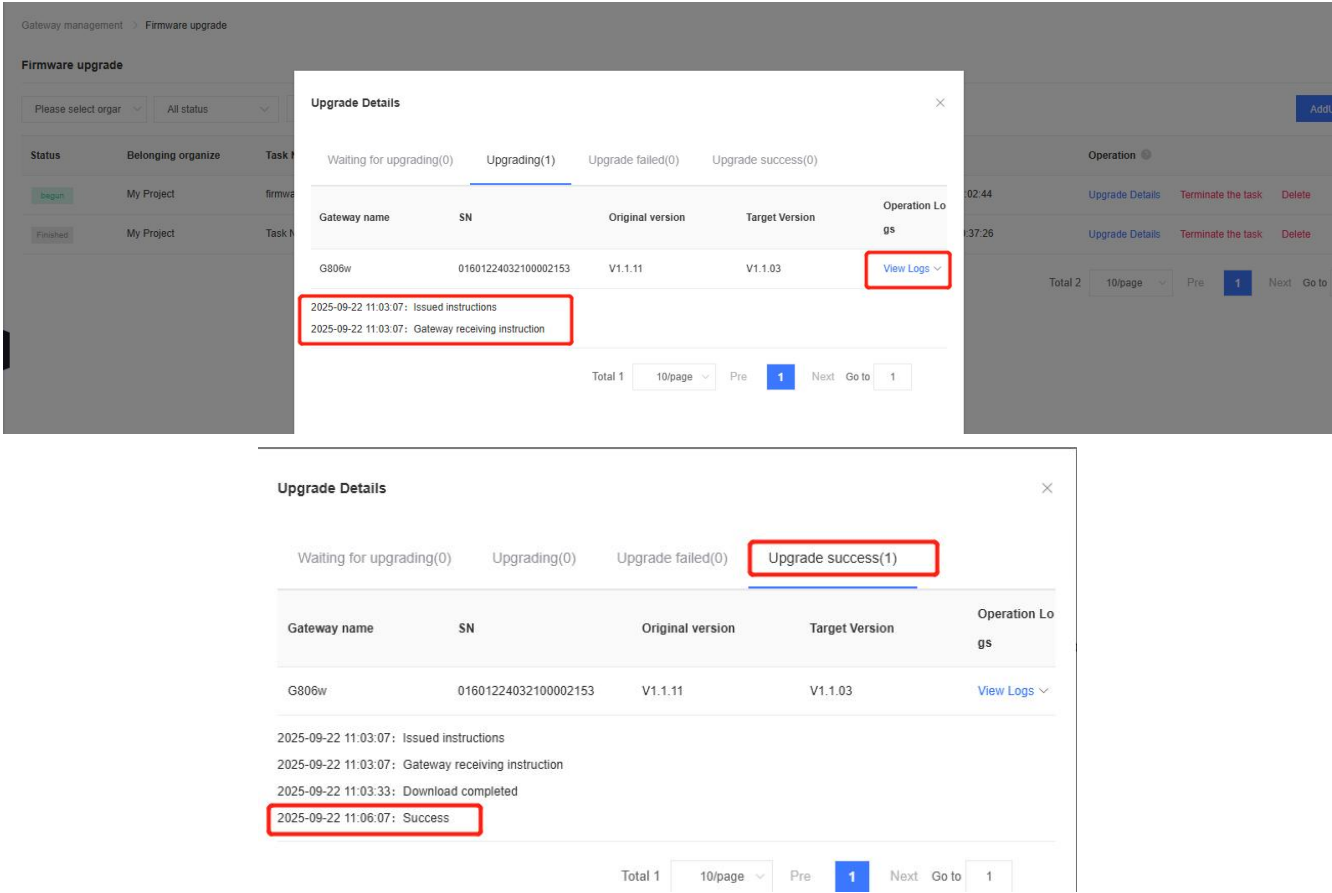
Edit More

Disable
Configuration page
Command control
Firmware Upgrade
Reboot gateway
Reload to factory settings
Delete

Set the task name and select the firmware version



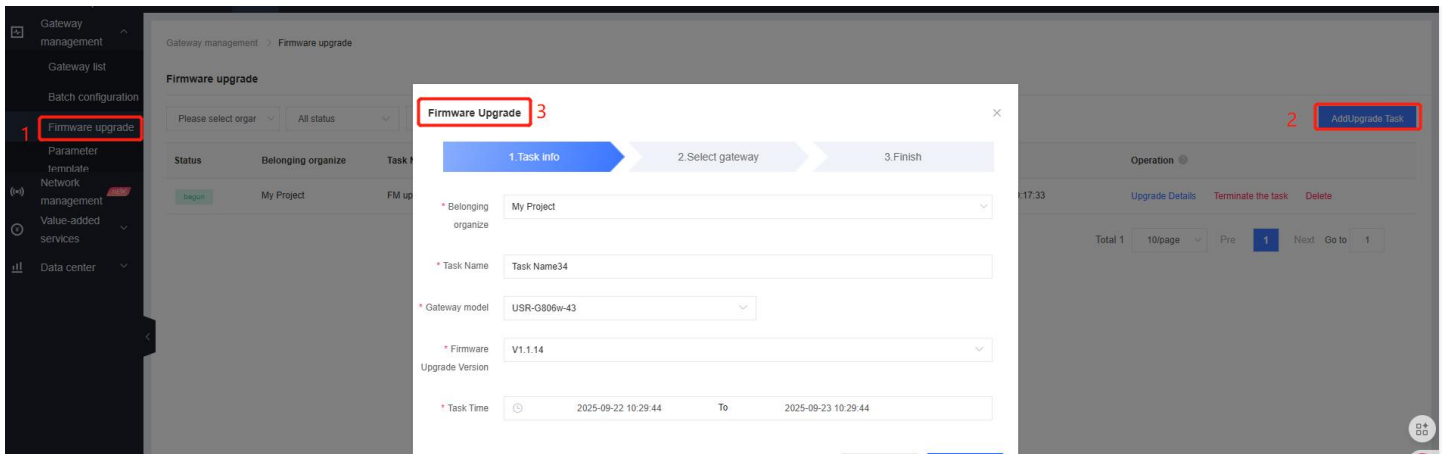
Users can check the upgrade detail



3.2.2. Batch Upgrade

Firmware upgrade -->add upgrade task

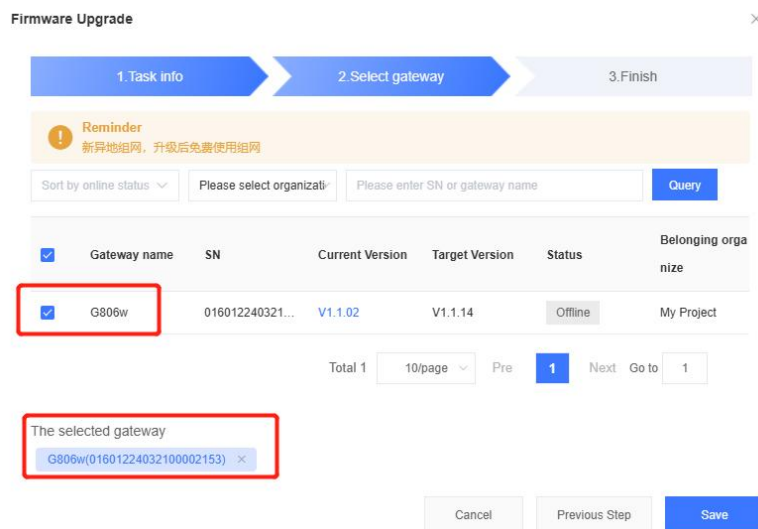
Select organization--> select gateway model-->select firmware version-->set task time



Select the specific gateway

Note:

1. Gateways that are offline at the scheduled task time will fail to upgrade
2. It is recommended to select <15 gateways per batch upgrade task. A maximum of 6 upgrade tasks can be created simultaneously.



The upgrade process starts approximately 10 minutes after the scheduled task start time. Check the upgrade status by clicking on the corresponding upgrade task in the [Firmware Upgrade] section.

4. SD-VPN Management

SD-VPN establishes a private network over the public internet via openVPN, enabling one-click interconnection between different branch nodes. It supports remote access, operation, maintenance, and monitoring. It facilitates mobile office, resource sharing, data transmission, and supports multi-cloud/hybrid cloud deployment. Suitable for small, medium, and large enterprises, catering, chains, and multi-branch organizations.

Applicable Scenarios:

※ Remote Monitoring: Real-time, 24/7 monitoring of facility operational status.

※ Remote Debugging of Industrial Computers and Instruments: Update device operating systems unrestricted by geographical location.

※ Remote PLC Upgrades: Avoid on-site visits, perform debugging directly from remote locations.

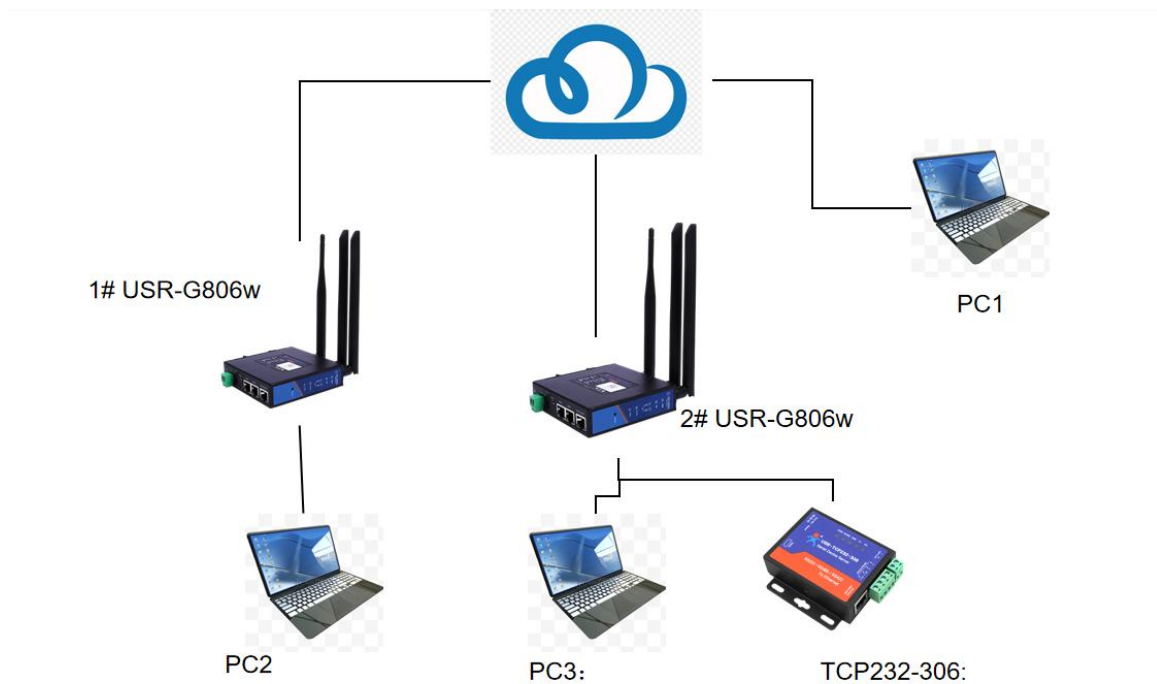
※ Flexible Remote Work: Create remote working environments for enterprise employees.

Products and Firmware Versions Supporting the SD-VPN Feature:

Product Model	Firmware Version	Max Networking Speed	Supported Network Types
USR-G806w-G	V1.1.10 and above	10M	Layer 3
USR-EG628	V1.0.11 and above	10M	Layer 3
USR-M300	V1.1.18 and above	10M	Layer 3

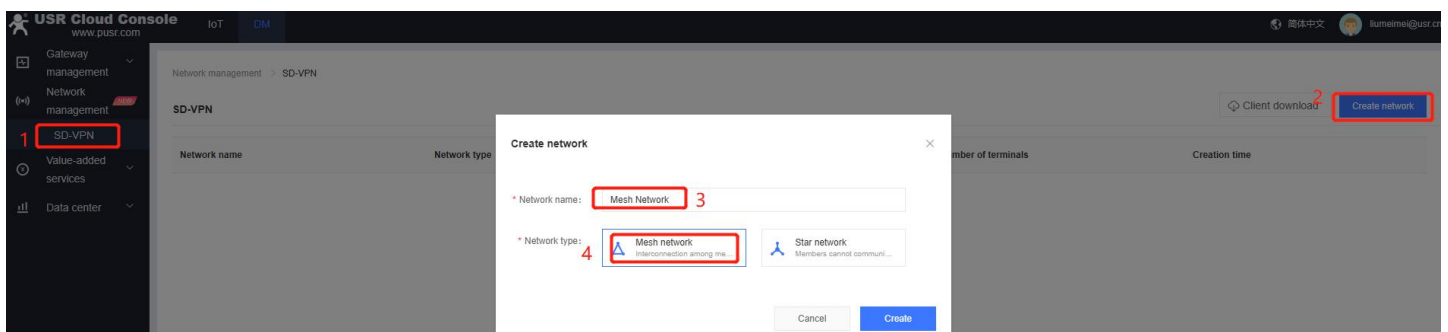
4.1. Mesh Network

4.1.1. Network Topology



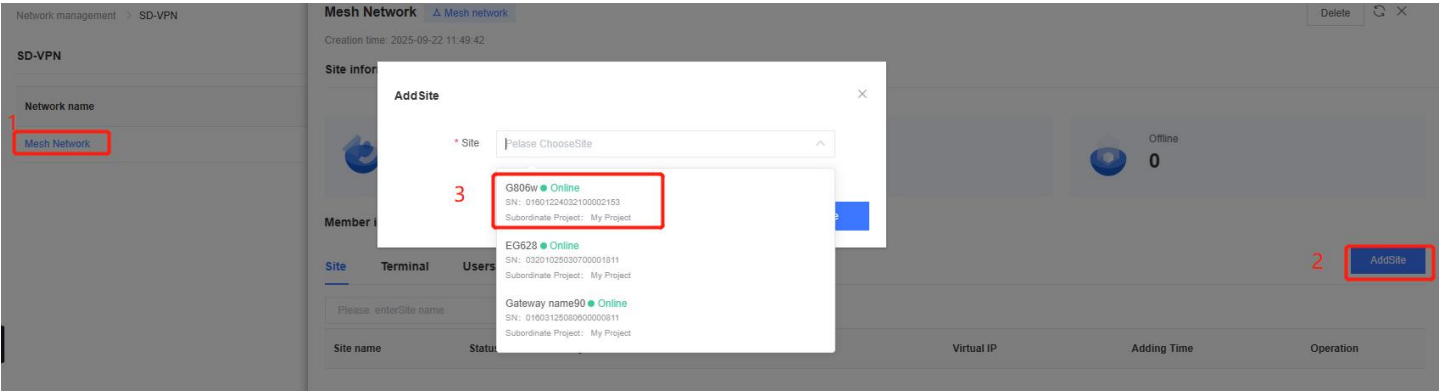
4.1.2. Create mesh network

Network management--> create network-->till the network name-->select mesh network--> create



4.1.3. Add site

Click the network name-->add site--> select gateways/routers



Site information

Number of sites 2	Online 2	Offline 0
----------------------	-------------	--------------

Member information

Site Terminal Users AddSite

Please enterSite name Query

Site name	Status	Monthly Flow	Number of terminals	Real IP	Virtual IP	Adding Time	Operation
Gateway name90	Connected	0.093MB	1	--	10.8.0.3	2025-09-22 11:51:56	Enable real IP Delete
G806w	Connected	0.098MB	2	--	10.8.0.2	2025-09-22 11:51:44	Enable real IP Delete

4.1.4. Add terminal device

The terminal devices are the device connected to the gateways/routers via WiFi or network cable. In the above network topology, the PC2, PC3 and the TCP232-306 are all the terminal devices.

Note: The real IP of the terminal device is recommended to set a static IP (if the terminal device uses DHCP, the IP assigned to the terminal device might change).

Member information

Site Terminal Users AddTerminal

All

Please enter the terminal name Query

TerminalName	Real IP	Virtual IP	Belonging site	Adding Time	Operation
TCP232-306	192.168.1.186	10.32.1.2	G806w	2025-09-22 12:26:05	Delete
PC3	192.168.1.185	10.32.1.1	G806w	2025-09-22 12:25:48	Delete
PC2	192.168.10.185	10.32.2.1	Gateway name90	2025-09-22 12:25:31	Delete

4.1.5. Add users

The following steps are not mandatory. If not needed, you can skip directly to Step 3 of section 2.2 to verify

the network.

Explanation: Adding users is not mandatory. When maintenance personnel need to operate and maintain devices within this network while on a business trip, they can join the network via the user method.

Site		Terminal		Users		AddUsers	
Please Input user name		Query					
User Name	Phone Number	Email	Monthly Flow	Virtual IP	Adding Time	Operation	
usr321	--	liumeimei@usr.cn	--	10.8.0.4	2025-09-22 14:46:17	Download Configuration File Delete	

4.1.6. Download and install client app

1. Download configuration file

Site		Terminal		Users		AddUsers	
Please Input user name		Query					
User Name	Phone Number	Email	Monthly Flow	Virtual IP	Adding Time	Operation	
usr321	--	liumeimei@usr.cn	--	10.8.0.4	2025-09-22 14:46:17	Download Configuration File Delete	

Total 1 10/page Pre 1 Next Go to 1

2. Download client

Gateway management

Network management

SD-VPN

Value-added services

Data center

Network management

SD-VPN

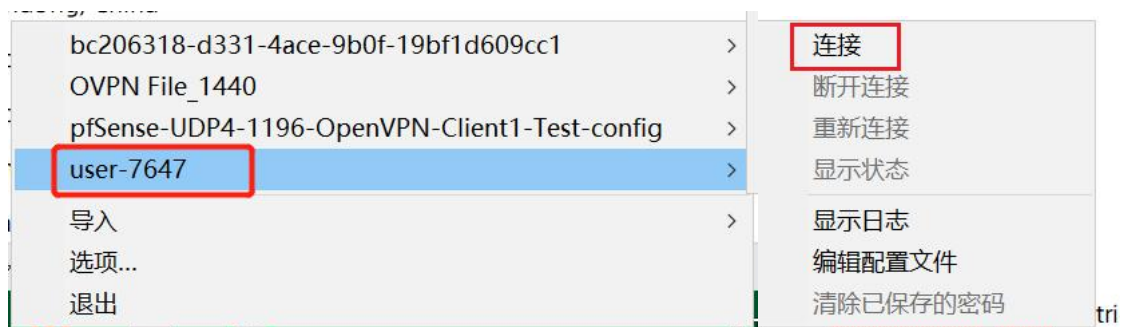
2

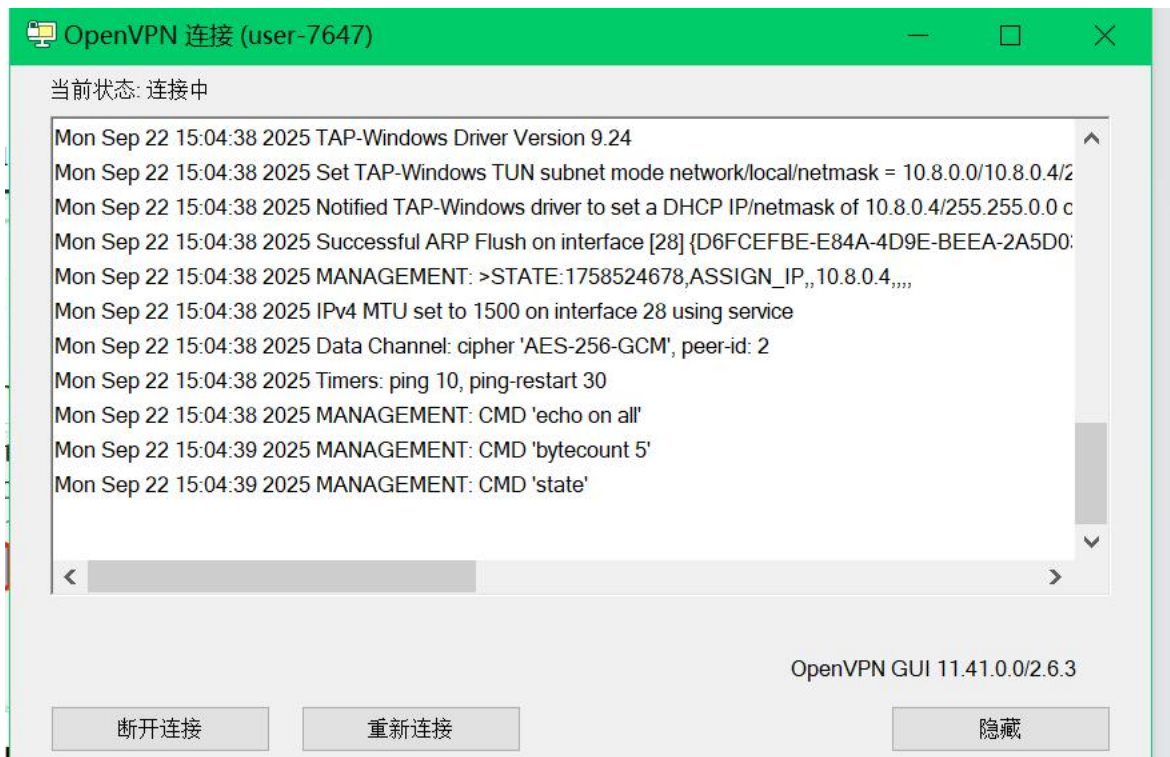
Client download

Create network

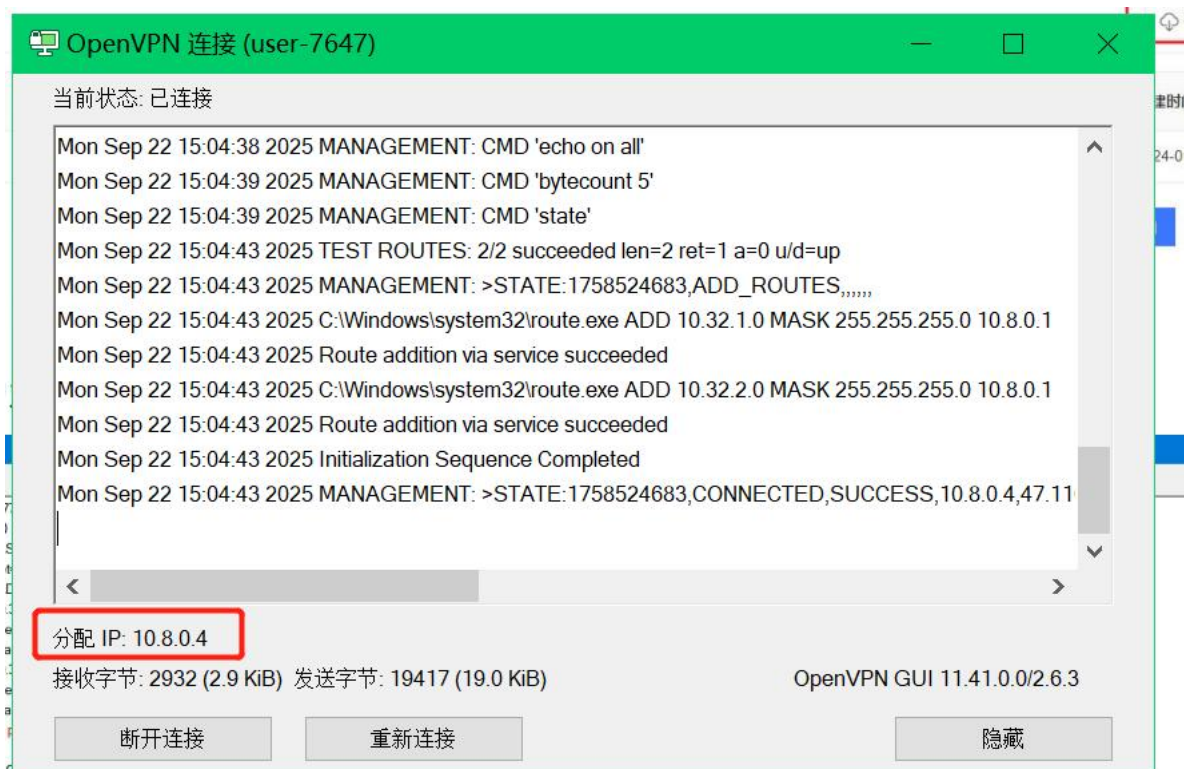
Network name	Network type	Number of sites	Number of terminals	Creation time
Mesh Network	Mesh network	2	3	2025-09-22 11:49:42

3. Run client and import the downloaded configuration file,the connect



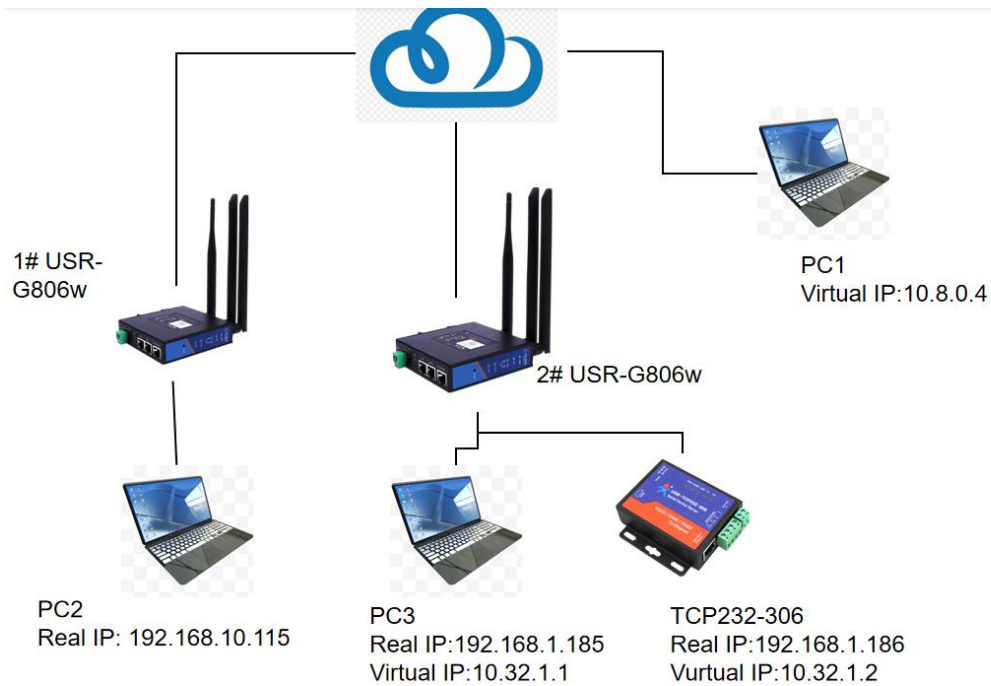


When the client connect to SD-VPN successfully, the client app will get an IP like shown in the following figure.



4.1.7. Verifying the mesh Network

The real IP and the virtual IP of the terminal device is shown in the following figure.



As a maintenance engineer, I may access the TCP232-306 anytime anywhere. Now I will ping and access the TCP232-306 via webUI. From the following figure, we can find that the ping command is success.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2486]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 10.32.1.2

正在 Ping 10.32.1.2 具有 32 字节的数据:
来自 10.32.1.2 的回复: 字节=32 时间=99ms TTL=254
来自 10.32.1.2 的回复: 字节=32 时间=100ms TTL=254
来自 10.32.1.2 的回复: 字节=32 时间=124ms TTL=254
来自 10.32.1.2 的回复: 字节=32 时间=101ms TTL=254

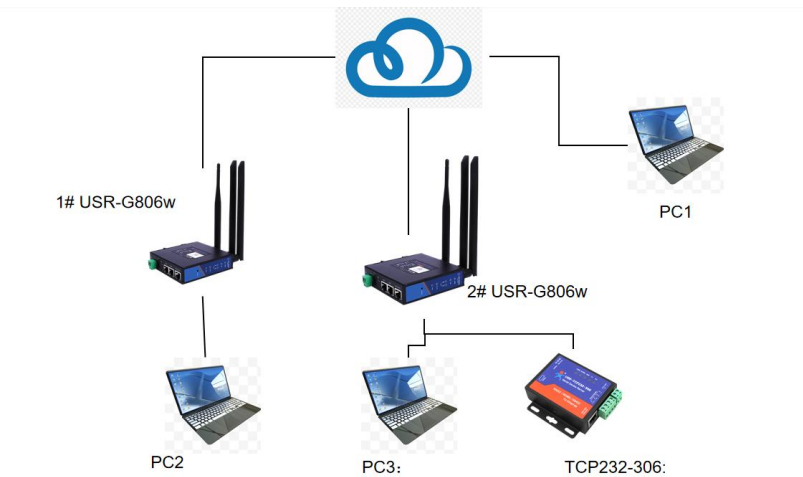
10.32.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 99ms, 最长 = 124ms, 平均 = 106ms

C:\Users\Administrator>
  
```

Access the configuration web page

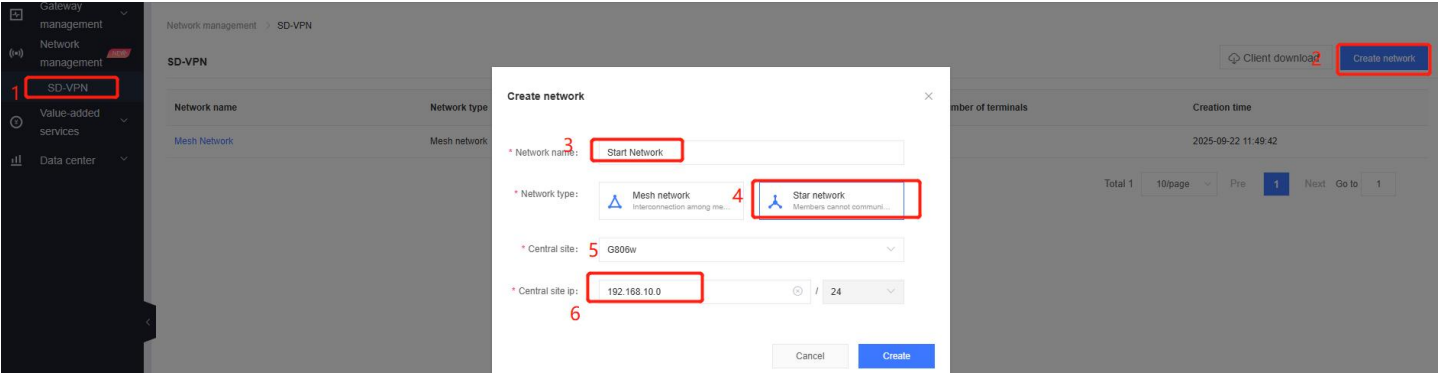


4.2. Star Network



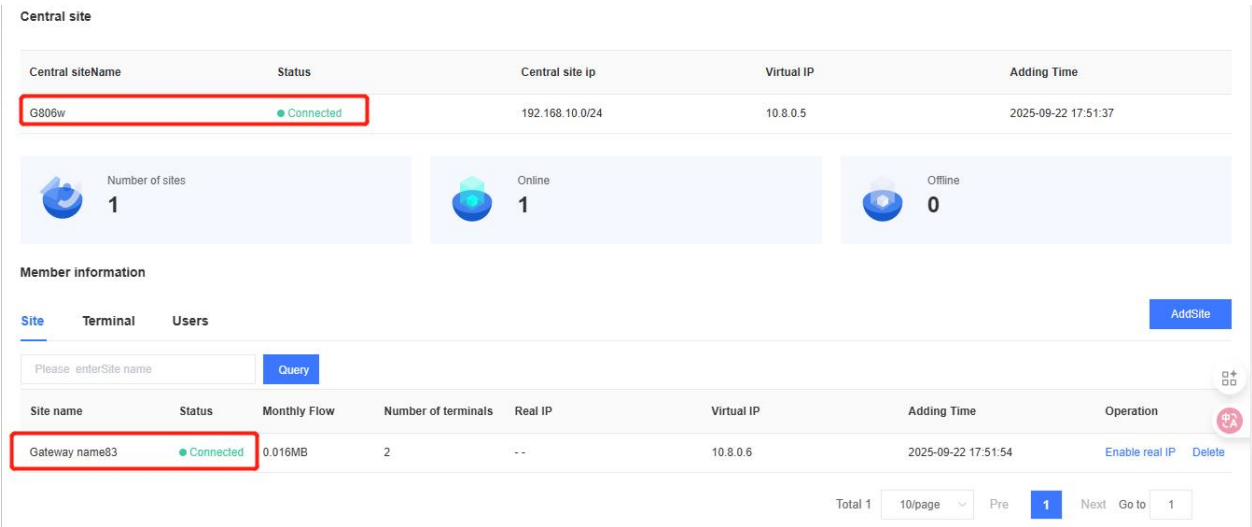
4.2.1. Create star network

Central site IP: 1# USR-G806w
Central site IP: the sub network segment of the central site.



4.2.2. Add the sub site

2# USR-G806w is added as the sub site.



Note: On the sub site, it has an operation "Enable real IP" . If you need to access a terminal using its real IP, you

should enable the real IP function in the sub site settings, and the sub nets under each sub site in this network must not be on the same network segment.

SiteTerminalUsersAddSite

Please enterSite nameQuery

Site name	Status	Monthly Flow	Number of terminals	Real IP	Virtual IP	Adding Time	Operation
Gateway name83	Connected	0.870MB	2	--	10.8.0.6	2025-09-22 17:51:54	Enable real IPDelete

4.2.3. Add terminal device to the sub site

SiteTerminalUsersAddTerminal

AllGateway name83

Please enter the terminal nameQuery

TerminalName	Real IP	Virtual IP	Belonging site	Adding Time	Operation
TCP232-306	192.168.1.186	10.32.2.2	Gateway name83	2025-09-22 17:52:49	Delete
PC3	192.168.1.185	10.32.2.1	Gateway name83	2025-09-22 17:52:24	Delete

4.2.4. Add users

The following steps are not mandatory. If not needed, you can skip directly to Step 3 of section 2.2 to verify the network.

Explanation: Adding users is not mandatory. When maintenance personnel need to operate and maintain devices within this network while on a business trip, they can join the network via the user method.

SiteTerminalUsersAddUsers

Please Input user nameQuery

User Name	Phone Number	Email	Monthly Flow	Virtual IP	Adding Time	Operation
usr321	--	liumeimei@usr.cn	--	10.8.0.4	2025-09-22 14:46:17	Download Configuration FileDelete

4.2.5. Download and install client app

4. Download configuration file

SiteTerminalUsersAddUsers

Please Input user nameQuery

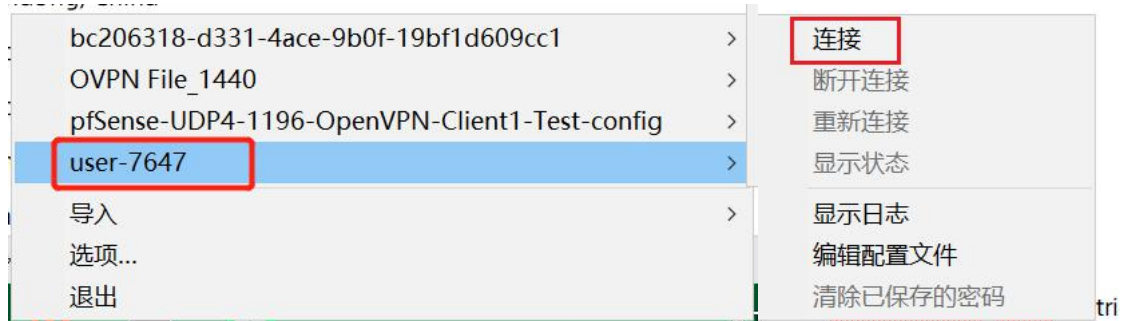
User Name	Phone Number	Email	Monthly Flow	Virtual IP	Adding Time	Operation
usr321	--	liumeimei@usr.cn	--	10.8.0.4	2025-09-22 14:46:17	Download Configuration FileDelete

Total 110/pagePre1NextGo to 1

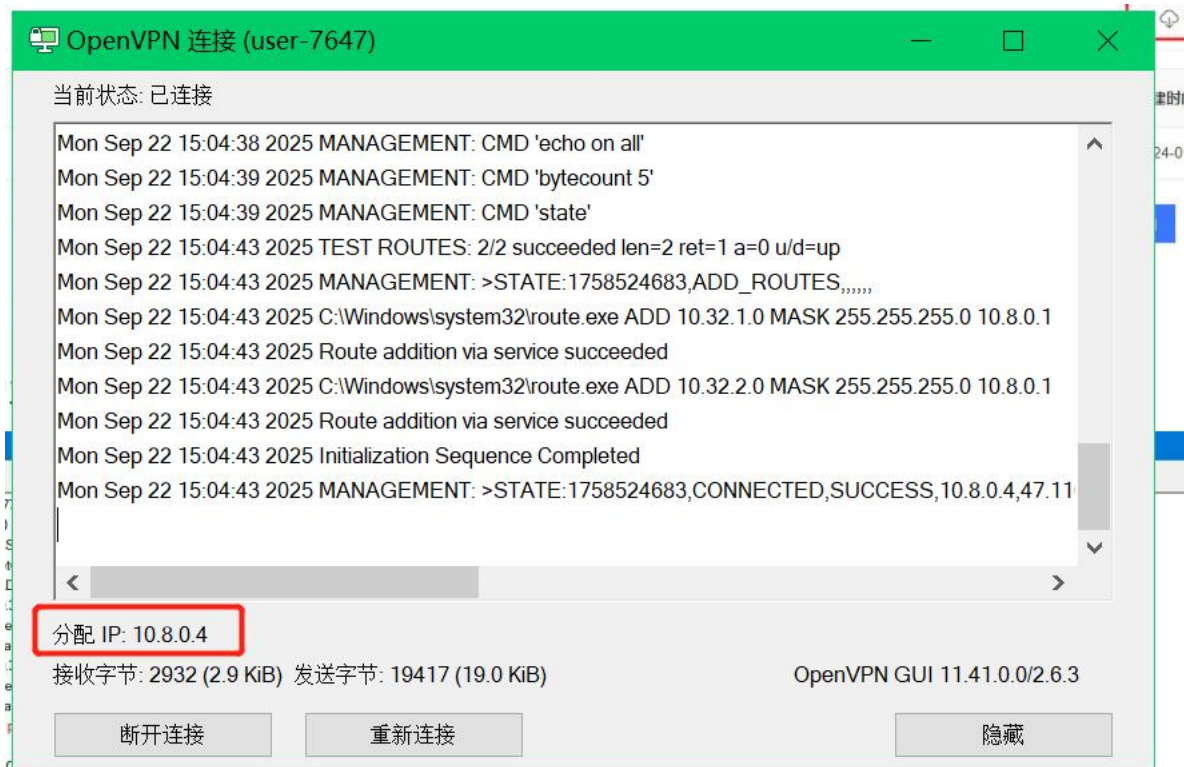
5. Download client



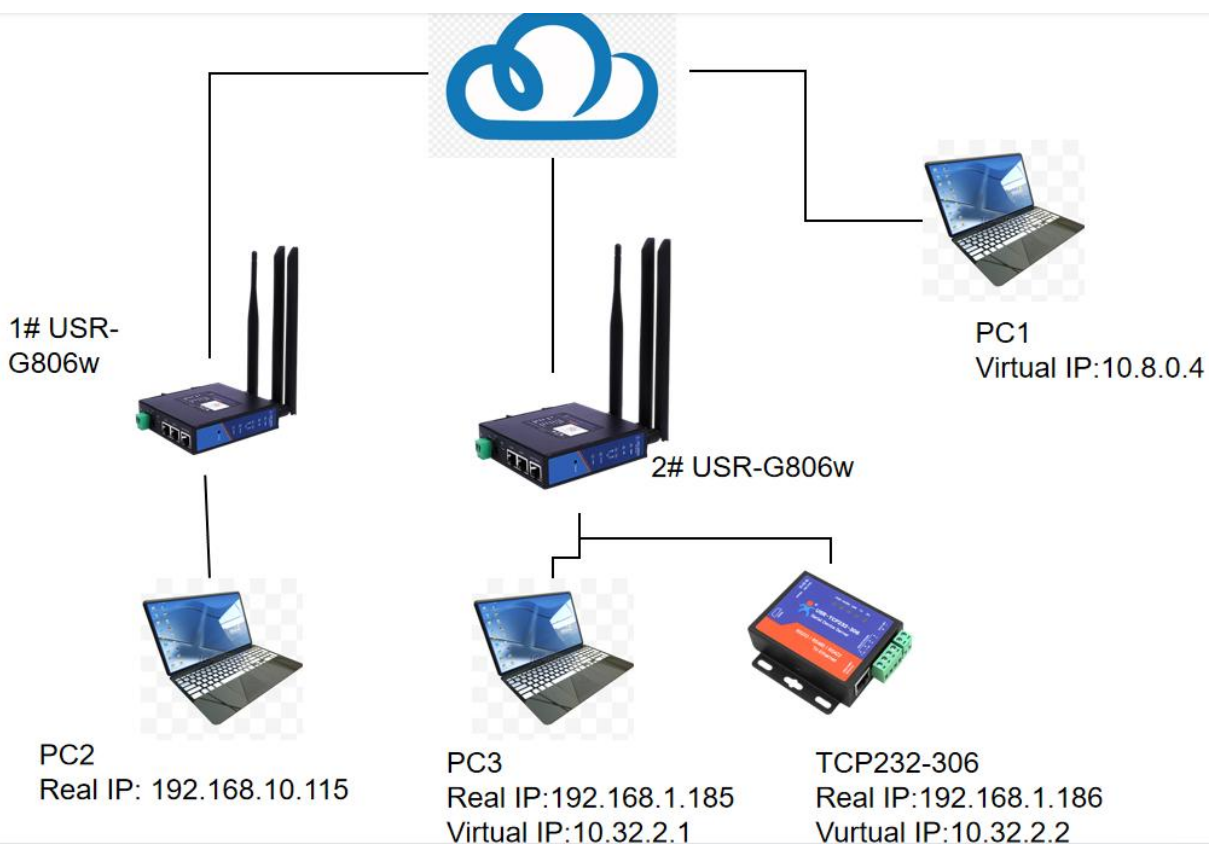
6. Run client and import the downloaded configuration file, the connect



When the client connect to SD-VPN successfully, the client app will get an IP like shown in the following figure.



4.2.6. Verifying the star Network



1. Use terminal PC2 at the central site 1# 806w to access the TCP232-306 under 2# 806w.

```

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : lan
    本地链接 IPv6 地址. . . . . : fe80::2cff:fa3c:6311:3405%33
    IPv4 地址 . . . . . : 192.168.10.115 real IP of the PC2
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.10.1

C:\Users\Administrator>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
Control-C
^C
C:\Users\Administrator>ping 10.32.2.2 Virtual IP of TCP232-306

正在 Ping 10.32.2.2 具有 32 字节的数据:
来自 10.32.2.2 的回复: 字节=32 时间=71ms TTL=253
来自 10.32.2.2 的回复: 字节=32 时间=81ms TTL=253
来自 10.32.2.2 的回复: 字节=32 时间=91ms TTL=253
来自 10.32.2.2 的回复: 字节=32 时间=78ms TTL=253

10.32.2.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 71ms, 最长 = 91ms, 平均 = 80ms

```

Access the web page of USR-TCP232-306



2. Access the TCP232-306 via the PC1, Virtual IP of PC1:10.8.0.4,.

From the following figure, we can find the the PC1 can not access the TCP232-306 successfully. It's a normal phenomenon,because in star network, only the terminal connected to the central site can access and communicate with the terminal devices connected to the sub site.

```

管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2486]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 10.32.2.2

正在 Ping 10.32.2.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

10.32.2.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Administrator>

```

OpenVPN GUI
已连接至: user-7647
连接白: 2025/9/22 18:13
分配 IP: 10.8.0.4

3. Access the PC1 from the PC2, it can ping successful.

User Name	Phone Number	Email	Monthly Flow	Virtual IP	Adding Time	Operation
usr321	--	liumeimei@usr.cn	1.5 MB	10.8.0.7	2025-09-22 18:33:54	Download Configuration File Delete

```
C:\Users\Administrator>
C:\Users\Administrator>ping 10.8.0.7

正在 Ping 10.8.0.7 具有 32 字节的数据:
来自 10.8.0.7 的回复: 字节=32 时间=363ms TTL=63
来自 10.8.0.7 的回复: 字节=32 时间=245ms TTL=63
来自 10.8.0.7 的回复: 字节=32 时间=426ms TTL=63
来自 10.8.0.7 的回复: 字节=32 时间=64ms TTL=63
```

4. Access the 1# USR-G806w from PC1

Central siteName	Status	Central site ip	Virtual IP	Adding Time
G806w	Connected	192.168.10.0/24	10.8.0.5	2025-09-22 17:51:37

PC1 ping the virtual IP 10.8.0.5 of 1# USR-G806w, from the following figure, we can find that it can ping successfully.

```
C:\Users\Administrator>ping 10.8.0.5

正在 Ping 10.8.0.5 具有 32 字节的数据:
来自 10.8.0.5 的回复: 字节=32 时间=102ms TTL=64
来自 10.8.0.5 的回复: 字节=32 时间=59ms TTL=64
来自 10.8.0.5 的回复: 字节=32 时间=83ms TTL=64
来自 10.8.0.5 的回复: 字节=32 时间=88ms TTL=64

10.8.0.5 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 59ms, 最长 = 102ms, 平均 = 83ms
```

And users can access the webpage of 1# USR-G806w from PC1 via the virtual IP, as shown in the following figure.

The screenshot shows the USR IOT web interface for the USR-G806w device. The browser address bar displays the URL `10.8.0.5/cgi-bin/luci/stok=c6b3776812d4b119a07004d81986e69`. The interface includes a sidebar with navigation options like Overview, Routes, Services, Network, VPN, Firewall, System, and Logout. The main content area shows the device's status, system information (Hostname, Firmware Version, SN, IMEI, Local Time, Uptime, Load Average), memory usage (Total Available, Free, Cached, Buffered), and network configuration (IPv4 WAN Status, Type: dhcp, Address: 192.168.66.103, Netmask: 255.255.255.0, Gateway: 192.168.66.1, DNS 1: 192.168.66.1).

5. FAQ

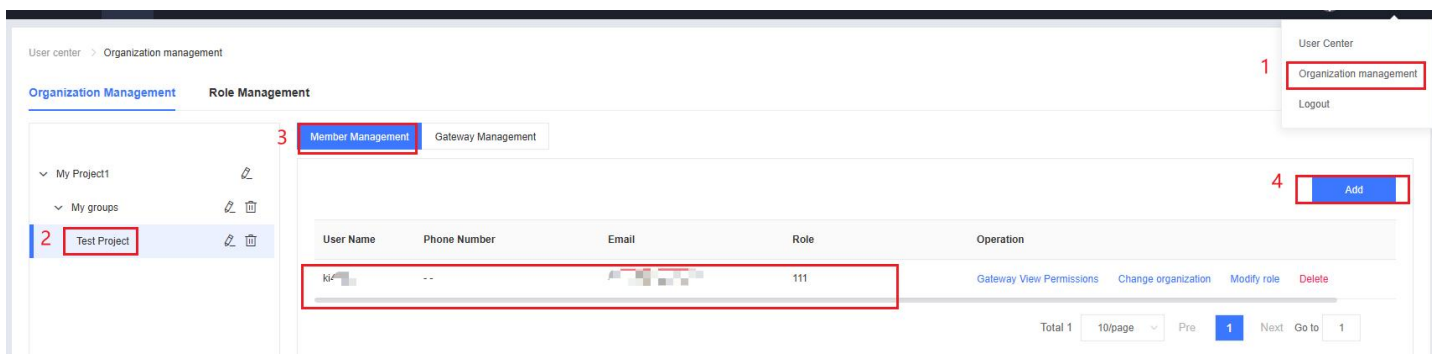
1. Q: Can the same user's configuration file be used simultaneously on multiple PCs?

A: No, because each certificate corresponds to one virtual IP. Using it on multiple PCs will cause conflicts.

2. Q: How can multiple PCs access this network simultaneously?

A: Step 1: Organization management--Test project--Member management--add--fill in the email, and the platform will send an confirmation email.

Then you can refer to [Add users] section and download and import configuration file section to add new users to achieve that multiple PCs access this network simultaneously.



3. Q: Does having terminals under a site use DHCP affect the networking function?

A: There is a risk. Because DHCP assignment may cause the IP to change, and the platform uses the terminal's actual IP to add it to the network. Therefore, using a static IP is recommended.

4. Q: How to troubleshoot if a PC cannot ping other terminals within the network?

A: Please check if the firewall on both the PC and the terminal is turned off. The firewall can affect ping probes.

5. Q: In a star network, failure occurs when a terminal at the central site tries to access a terminal at a sub-site. How to handle it?

A: The LAN of the sub-site and the LAN of the central site need to be set to different network segments for normal operation.

6. Q: How to solve packet loss when using the network?

A: It is recommended to set the terminal MTU to 1500 or below and verify again.

7. Q: The PLC only supports access from the same network segment, but using remote networking involves different segments. How to solve it?

A: You can use G806w's SNAT function. Try the following settings:

Source NAT				
Name	Protocol	Action	Enable	Sort
SNAT	Any tcp, udp From any host in wan To any host in lan	Rewrite to source IP 192.168.10.1	☒	Up Down Edit Delete

6. Contact Us

Jinan USR IOT Technology Limited

Address : Floor 12 and 13, CEIBS Alumni Industrial Building, No. 3 Road of Maolingshan, Lixia District, Jinan, Shandong, China

Official website: <https://www.pusr.com>

Official shop: <https://shop.usriot.com>

Technical support: <http://h.usriot.com/>

Email : sales@usriot.com

Tel : +86-531-88826739

Fax : +86-531-88826739-808

7. Disclaimer

The information in this document provided in connection with Jinan USR IoT technology ltd. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of USR IoT products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, USR IoT AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL USR IoT AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF USR IoT AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. USR IoT and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes

to specifications and product descriptions at any time without notice. USR IoT and/or its affiliates do not make any commitment to update the information contained in this document.



Your Trustworthy Smart IOT Partner



Official Website: www.pusr.com

Official Shop: shop.usriot.com

Technical Support: h.usriot.com

Inquiry Email: inquiry@usriot.com

Skype & WhatsApp: +86 13405313834

关注有人微信公众号 登录商城快速下单

Click to view more: [Product Catalog](#) & [Facebook](#) & [Youtube](#)