EQUIINET™

justINA
配置使用说明书

NOT JUST A BOX,
A SOLUTION.

010.8244.9224 | info@equiinet.cn | www.Equiinet.cn

About this guide

Thank you for choosing justINA Fusion Communications Server. This guide aims to introduce you to the main features of each page of justINA, so that you can more fully understand the features and value that justINA can bring to you.

Before use, please read the packing list and safety instructions in this guide, and confirm with the system administrator whether the current network environment meets the requirements of justINA configuration.

summary

1. Content

This guide contains the following chapters: Home, Admin, System, Advanced, About and Diagnostics. We will go through each chapter in detail.

2. Properties

The justINA system configuration interface is divided into "Properties interface" and "Diagnostic interface". After logging in to the justINA system normally, the "Properties Interface" is displayed, and we can perform daily configuration in the properties interface;

When you need to perform diagnostics, such as viewing logs, registration status, and other information, we can enter the "diagnostic interface" to obtain the corresponding information.

3. System login

justINA default login IP address is 10.0.0.1, username and password are admin, eqpassword;

Enter https://10.0.0.1 in your browser and enter your username and password to log in to the justINA system.

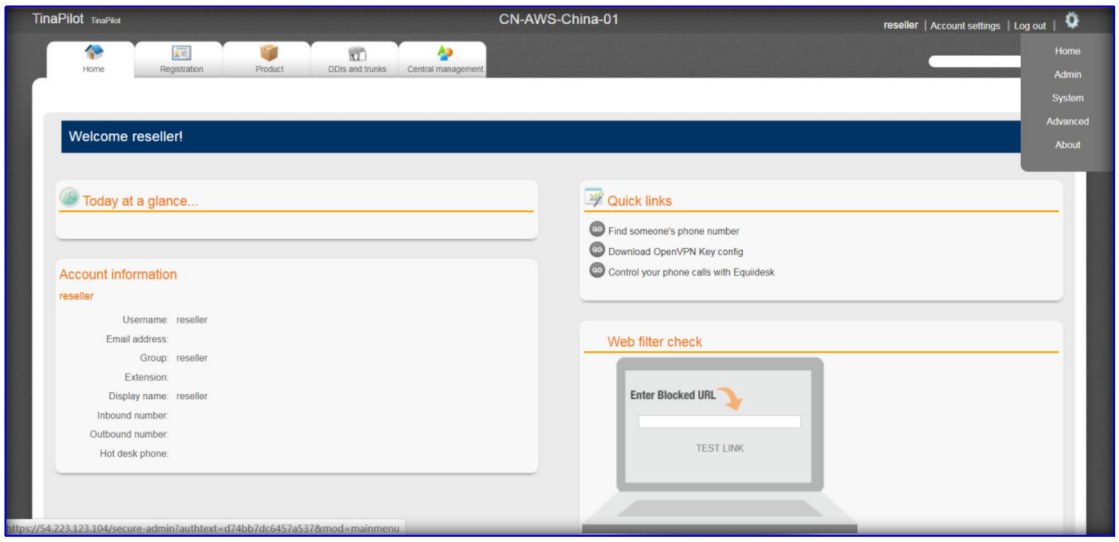
System Configuration

Chapter 1 Home

1. Home

Top right gear button-> Home-> Home

The main page is an overview of the basic situation of the system and quick links.



1.1. Account Information

User name: The user name for logging in to this system.

Email address: The email address of the user who logs in to this system.

Group: The group of the user logged in to this system.

Extension: user extension number.

Display name: The user display name.

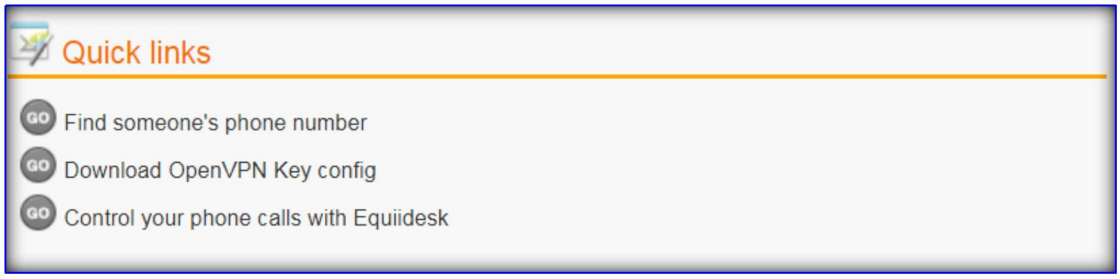
Inbound number: The inbound number of the user.

Outgoing number: Outgoing number of the user.

Note:

Because the login account information of reseller (senior administrator) is displayed here, reseller is generally not used to make calls, so the information about incoming and outgoing numbers is left blank.

1.2. Quick Links



After clicking the quick link, you can quickly find the extension number or download the OpenVPN key.

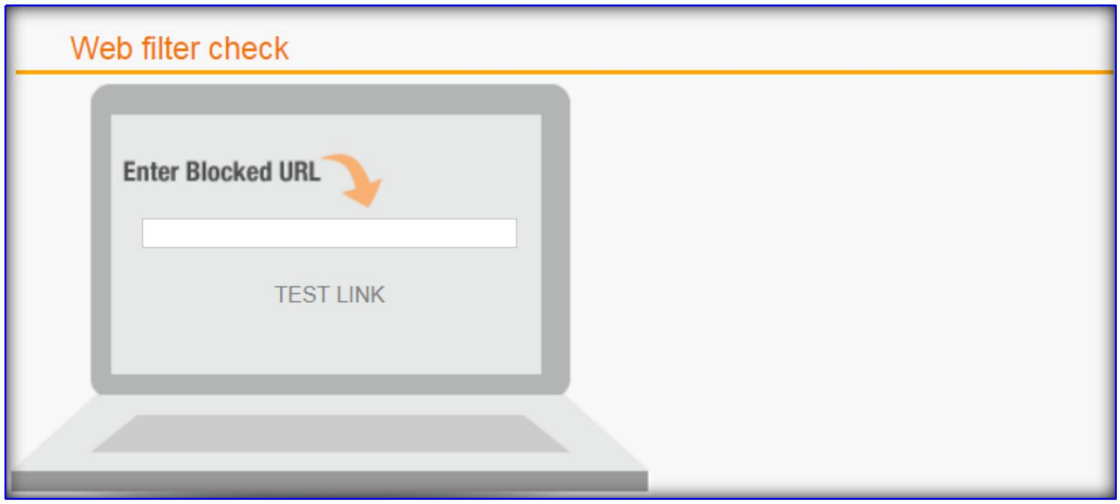
Find someone’ s phone number: After clicking the Find someone’ s phone number ,you can enter the following interface and see the current system users, call queues, conference rooms, call groups, and extension numbers for specific functions.

Download OpenVPN Key config : Click the Download OpenVPN Key Quick Link to enter the Download OpenVPN Key interface.

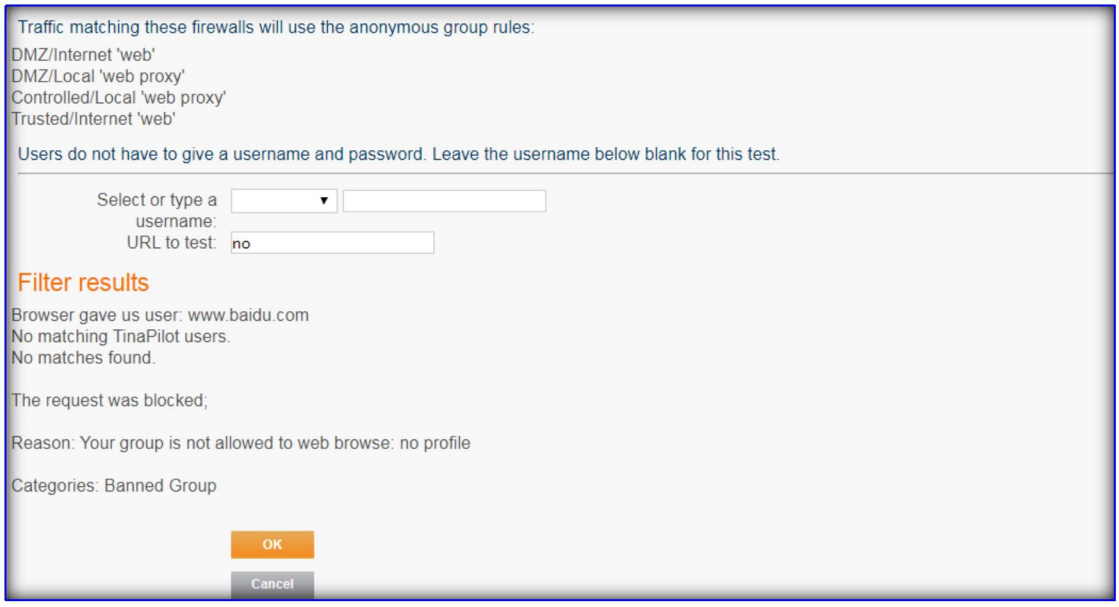
Control your phone calls with Equiidesk : drop this feature.

1.3. Web filter check

Web filter check are filtering checks for URLs. For example, enter www.baidu.com, press Enter or click TEST LINK to enter the test interface.



You can check the URL filtering status in the filtering result area.



Note:

This function is only applied when justINA is used as a gateway.

2. Registration

Top right gear button-> Home-> Registration

2.1 Registration

Service ID: Registration ID. Equiios system can be used completely after system registration.

Uname: The name of this device, and the logged-in user can set it freely.

Note:

This interface can only be seen by the senior administrator reseller.

3. Product

Top right gear button-> Home-> Product

3.1 Product

Manufacturer: The manufacturer of this system. We usually choose Equiinet.

Feature set: The product type of this system, we usually choose justINA.

Note:

This interface can only be seen by the senior administrator reseller.

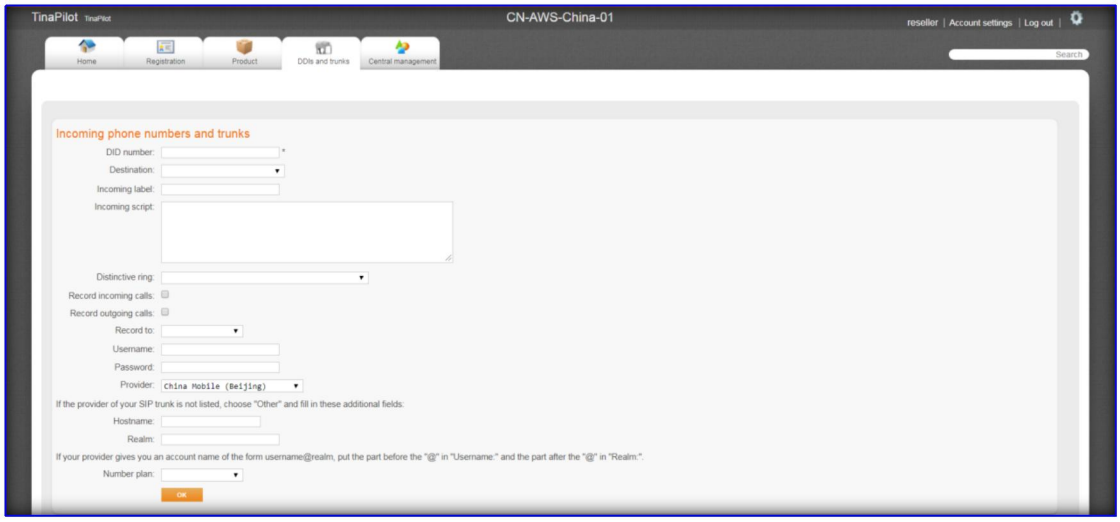
4. DDIs and trunks

Top right gear button-> Home-> DDIs and trunks

4.1 DDIs and trunks

The line information interface is mainly the SIP trunk configuration interface, including incoming call numbers and line rules.

Click Add to enter the configuration interface.



DID number: DID number of the SIP trunk line.

There are three types of lines

(1) Pure SIP line

If the SIP line number purchased from the SIP line provider is 53809789, the password is 4848472, and the registered address is 23.4.5.6, the DID number should be 53809789 here.

(2) Interfacing with FXO and E1 gateways

Interconnect with the FXO gateway. The DID number here must be the same as the calling number on the FXO.

Interconnect with the E1 gateway. Here, the DID number is arbitrary, as long as it is meaningful, it can be easily distinguished by the administrator.

(3) Interfacing with other PBX systems

When it comes to interfacing with other PBX systems, the DID number here is arbitrary, as long as it is meaningful, it can be easily distinguished by the administrator.

Destination: The destination of the DID number, such as a user, a voice menu, and a call queue.

If the target is a certain user such as 501, when the DID line is called, the 501 user rings.

Incoming lable: Incom label for this DID.

If an external customer calls in, the DID's incoming label and DID number will be displayed on your IP phone.

Incoming script:

Distinctive ring: The system has 14 ringtones by default. Users can set specific ringtones for DID to distinguish different DID lines.

This type of ringtone usually involves background modification and directly affects the ringing of the IP phone, so the configuration is troublesome, and currently this feature is rarely used in China.

Record incoming calls: Record the incoming direction of the call.

Record outgoing calls: Record the outgoing direction of the call.

Record to: Save the call recording (call-in recording, call-out recording) to a folder.

This folder is usually named after the user name of the extension number. For example, the user can save the recording in the reseller, admin, 554, record (a certain extension number) and other folders.

Username: DID username provided by the SIP Trunk line provider.

When the line is a pure SIP line, fill in the user name provided by the operator here, which is usually the same as the DID user name;

When the line is connected to the FXO gateway and E1 gateway and justINA, this disposal is empty.

Password: The DID password provided by the SIP Trunk line provider.

When connecting with a pure SIP line, fill in the password provided by the operator here.

When interfacing with FXO gateway, E1 gateway and justINA, this disposal is

empty.

Provider: SIP Trunk line provider name.

Hostname: The server IP address or domain name address of the SIP Trunk line provider.

Realm: the realm provided by provider

Number plan: dialing rules, such as international dialing rules, domestic dialing rules selection.

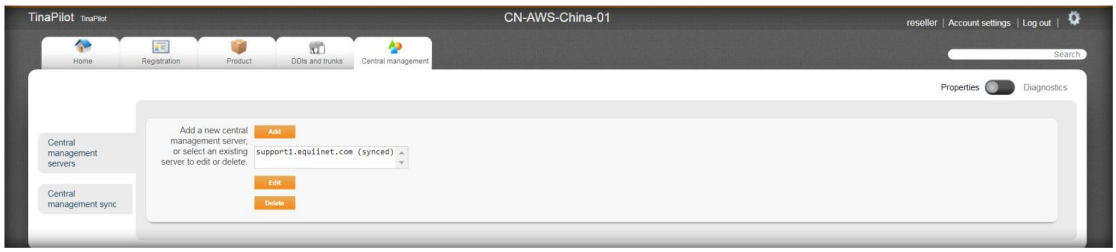
Note:

This interface can only be seen by the senior administrator reseller. After inbound recording and outbound recording are checked, "Save recording to" must be selected, otherwise the system buffer is too full and it will affect the use! !!

5. Central Management Server

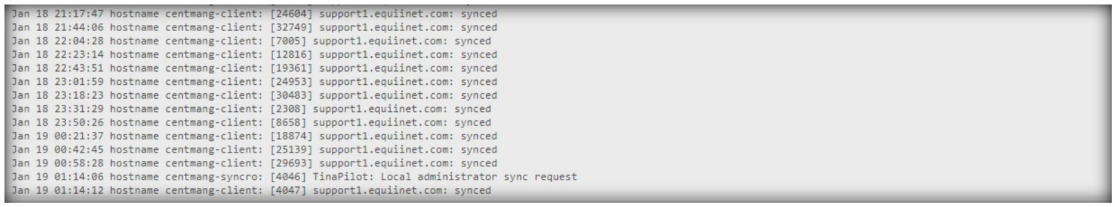
Top right gear button-> Home-> Central Management Server

The central management server interface mainly introduces central management server information and synchronization information with the central management server. No user configuration is required here, the system comes with it.



When this device is not synchronized with the central management server, it will prompt unsynced such as support.equiinet.com (unsynced). Enter the central management synchronization and update manually.

After clicking OK, you will automatically enter the log interface, and you will see the latest update status log.



```
Jan 18 21:17:47 hostname centmang-client: [24604] support1.equiinet.com: synced
Jan 18 21:44:06 hostname centmang-client: [32749] support1.equiinet.com: synced
Jan 18 22:04:28 hostname centmang-client: [7005] support1.equiinet.com: synced
Jan 18 22:23:14 hostname centmang-client: [12816] support1.equiinet.com: synced
Jan 18 22:43:51 hostname centmang-client: [19361] support1.equiinet.com: synced
Jan 18 23:01:59 hostname centmang-client: [24953] support1.equiinet.com: synced
Jan 18 23:18:23 hostname centmang-client: [30483] support1.equiinet.com: synced
Jan 18 23:31:29 hostname centmang-client: [2308] support1.equiinet.com: synced
Jan 18 23:50:26 hostname centmang-client: [8658] support1.equiinet.com: synced
Jan 19 00:21:37 hostname centmang-client: [18874] support1.equiinet.com: synced
Jan 19 00:42:45 hostname centmang-client: [25139] support1.equiinet.com: synced
Jan 19 00:58:28 hostname centmang-client: [29693] support1.equiinet.com: synced
Jan 19 01:14:06 hostname centmang-syncro: [4046] TinaPilot: Local administrator sync request
Jan 19 01:14:12 hostname centmang-client: [4047] support1.equiinet.com: synced
```

After the update is complete, it will prompt that the status is synced.

Note:

This interface can only be seen by the senior administrator reseller.

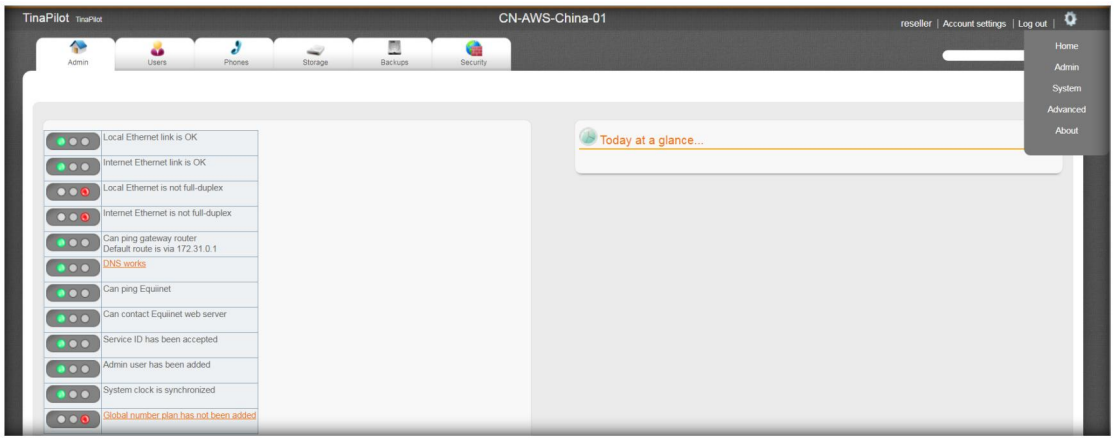
Chapter 2 User Configuration

1. Admin

Top right gear button-> Admin->Admin

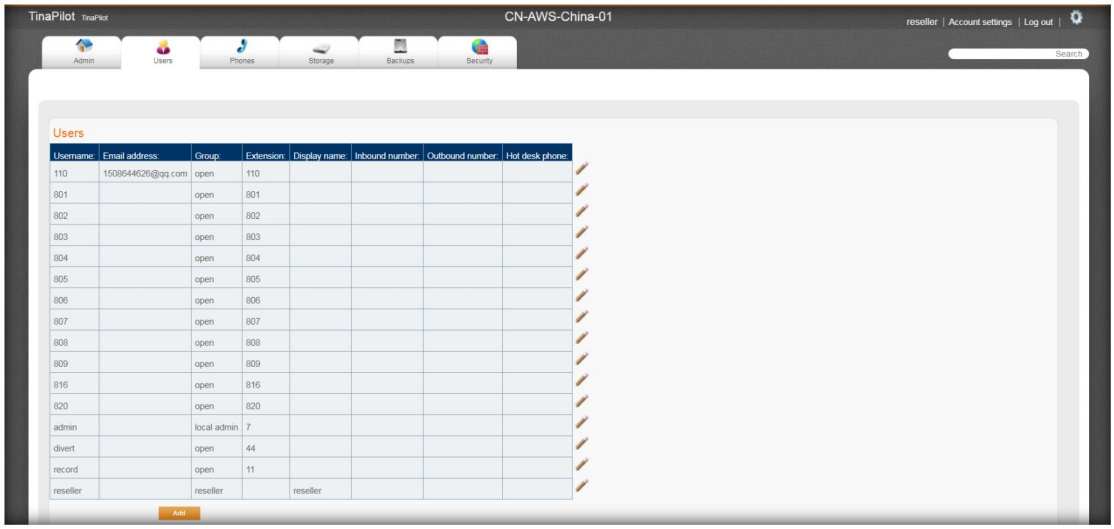
The Admin interface is mainly a admin (senior admin)user configuration overview interface, which includes statistics of the system network information and other status.

Green light means the configuration is correct and running normally; red light means no configuration.

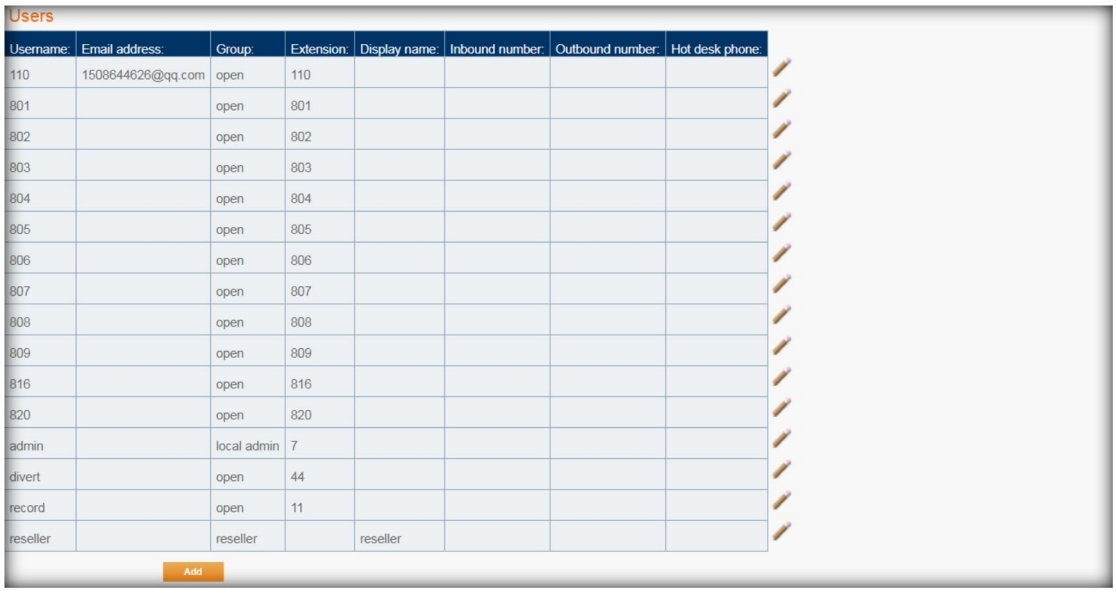


2. Users

The Users interface mainly introduces the addition of users and the configuration of corresponding information of users.



2.1 Users



Users

Username:	Email address:	Group:	Extension:	Display name:	Inbound number:	Outbound number:	Hot desk phone:
110	1508644626@qq.com	open	110				
801		open	801				
802		open	802				
803		open	803				
804		open	804				
805		open	805				
806		open	806				
807		open	807				
808		open	808				
809		open	809				
816		open	816				
820		open	820				
admin		local admin	7				
divert		open	44				
record		open	11				
reseller		reseller		reseller			

Add

Adding and configuring user extensions.

Click the Add button to enter the configuration interface.

User name: The user name of the extension, which can be a number such as 200 or a name such as record.

Password: The password used to log in to the web (cloud disk) when using the extension as the username.

Confirm password: Same as the password.

Email address: If this extension user wants to forward the voice message to his own mailbox, he needs to fill in the Email address here and configure it at the "User voicemail" section.

Group: To configure a common extension number, select the Open group (default); to configure an extension number with Admin or Reseller permissions (mainly used for management), select the Admin group or the Reseller group accordingly.

Extension: The extension number used for registration,which can be a number such as 200.

Note:

The User name is different from the Extension . When registering the Extension , the Extension shall prevail. The User name is only used for interface login or

cloud disk login.

Display name: The display name of the Extension, which can be arbitrary here, such as Amy, Tony, etc.

Incoming number: You can manually select the incoming line number for this extension. For example, if the line number of the incoming call for the 200 users is 53809795, then after the customer calls 53809795, the extension 200 rings.

Outgoing number: You can manually select the outgoing line number for the extension. If the outbound line number selected for 200 users is 53809797, then 200 users can use this line for outbound calls.

Hot desk phone: It is generally used for batch configuration (autoprovision) according to the mac address.

2.2. Select user group

The user group here is mainly used for web page filtering, that is, URL-filter, and can be filtered for different user groups.

This function is only used when justINA is used as the gateway, this function is not commonly used. I will explain here when I introduce the Web fileter later.

Among them, Controlled, open, email only, local administrator, agent, third

party and user group in the user configuration item are the same.

2.3. Quick Links

Quick links are quick links to some configuration items or download files, which are not often used.

2.4. User alternative phone numbers

Mainly used for call forwarding.

For example, an extension number 801 can have three backup numbers. When someone dials extension number 801 and is unavailable (ringing for 20s, no one answers), we can configure it to automatically go to standby number 1(alt.1), so that the call can be automatically transferred to standby number 1, until standby number 1 rings ,answer this call.

The backup number here can be the internal extension number, or the external mobile phone number or telephone landline number.

User alternative phone numbers

Username:	Cell (alt.1):	Home (alt.2):	Alternative 3:	Forward incoming caller-ID:
110				No
801	13688848602			No
802				No
803				No
804				No
805				No
806				No
807				No
808				No
809				No
816				No
820				No
admin				No

User alternative phone numbers

801

Username: 801

Cell (alt.1): 13688848602

Home (alt.2):

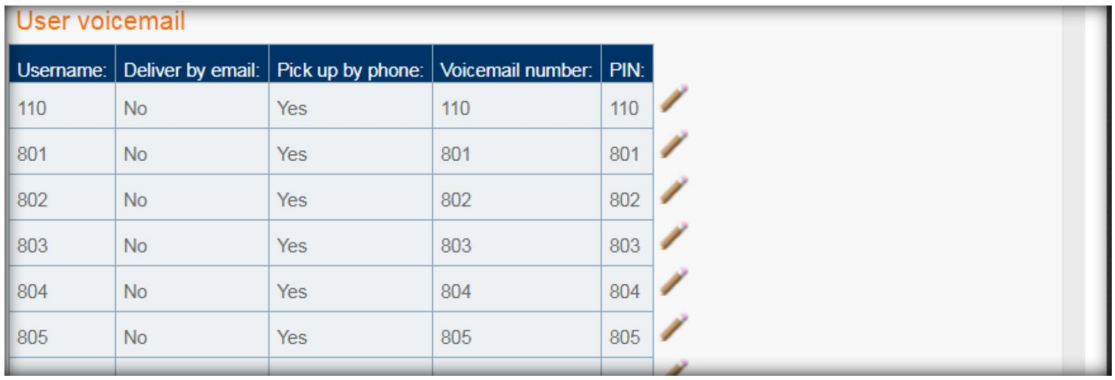
Alternative 3:

Forward incoming caller-ID:

OK

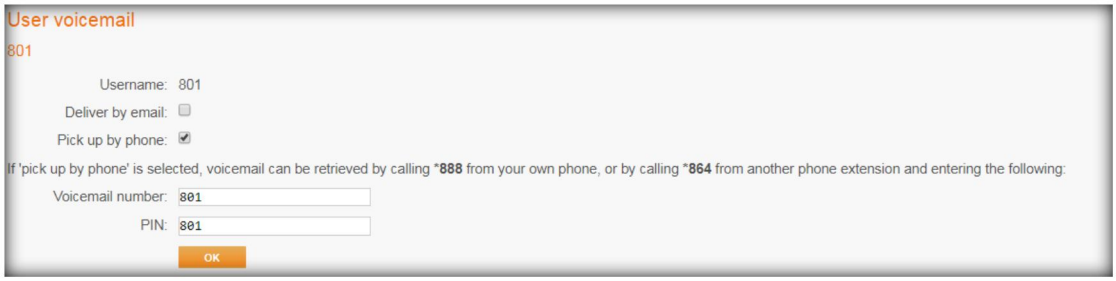
2.5. User voicemail

Mainly set the voice message settings for the extension, such as setting whether the voice message is sent to the e-mail box; you can also set the login password for this voice mailbox.



User voicemail

Username:	Deliver by email:	Pick up by phone:	Voicemail number:	PIN:
110	No	Yes	110	110
801	No	Yes	801	801
802	No	Yes	802	802
803	No	Yes	803	803
804	No	Yes	804	804
805	No	Yes	805	805



User voicemail

801

Username: 801

Deliver by email: ☐

Pick up by phone: ☑

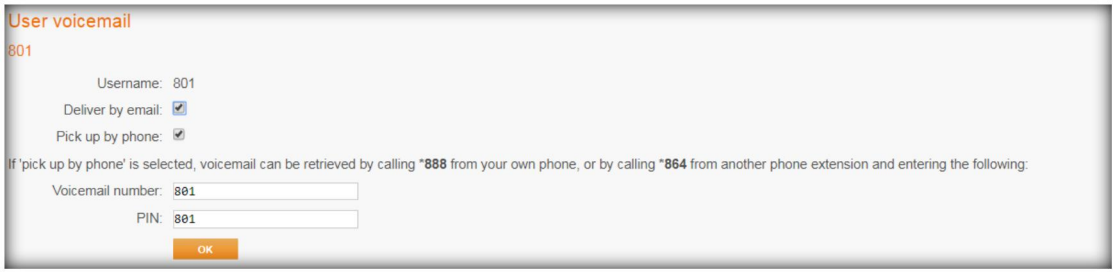
If 'pick up by phone' is selected, voicemail can be retrieved by calling ***888** from your own phone, or by calling ***864** from another phone extension and entering the following:

Voicemail number: 801

PIN: 801

OK

If you need to send a voice message to your e-mail address, just check the "Deliver by e-mail".



User voicemail

801

Username: 801

Deliver by email: ☑

Pick up by phone: ☑

If 'pick up by phone' is selected, voicemail can be retrieved by calling ***888** from your own phone, or by calling ***864** from another phone extension and entering the following:

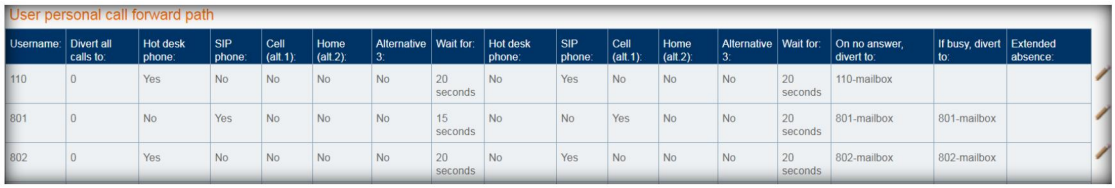
Voicemail number: 801

PIN: 801

OK

2.6. User personal call forward path

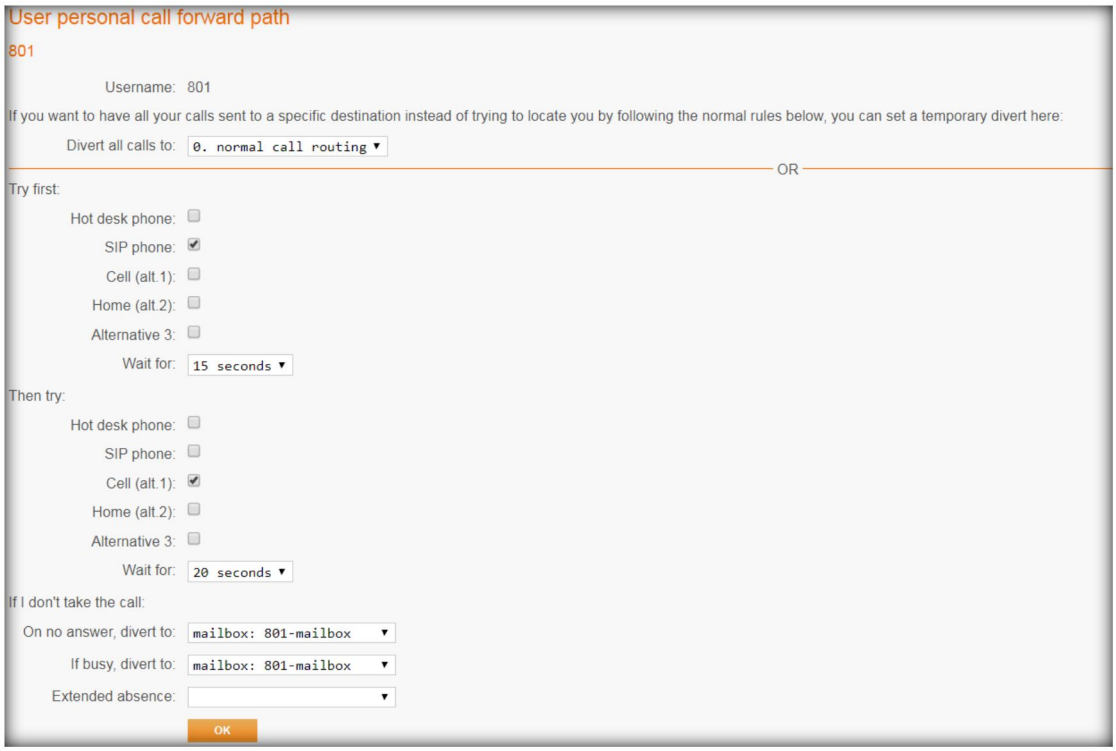
Modifications are mainly made for call transfer and route progress.



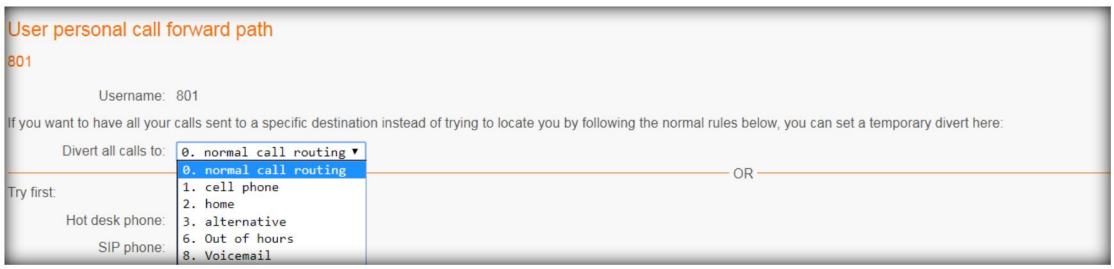
User personal call forward path

Username:	Divert all calls to:	Hot desk phone:	SIP phone:	Cell (alt.1):	Home (alt.2):	Alternative 3:	Wait for:	Hot desk phone:	SIP phone:	Cell (alt.1):	Home (alt.2):	Alternative 3:	Wait for:	On no answer, divert to:	If busy, divert to:	Extended absence:
110	0	Yes	No	No	No	No	20 seconds	No	Yes	No	No	No	20 seconds	110-mailbox		
801	0	No	Yes	No	No	No	15 seconds	No	No	Yes	No	No	20 seconds	801-mailbox	801-mailbox	
802	0	Yes	No	No	No	No	20 seconds	No	Yes	No	No	No	20 seconds	802-mailbox	802-mailbox	

Open the pencil icon for a user's user personal call forward path for editing.



Divert all calls to: Similar to the call forwarding function, when someone calls a user such as 801, if you configure alt1(cell phone), alt2(home), alternative for this 801 in advance; all incoming calls to 801 can be forwarded to alt1,alt2 or alternative3,801 will not ringing.



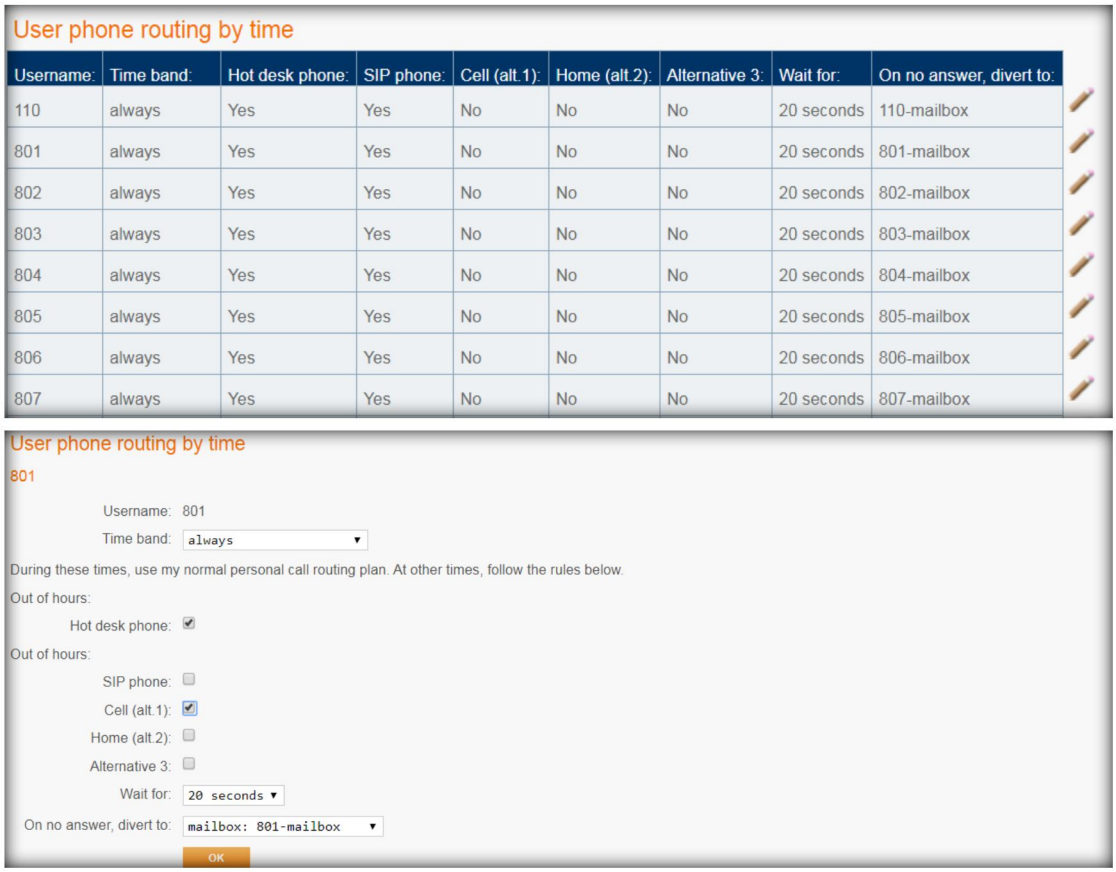
Try first, Then Try ,If I don't take the call: These three features are a series of features. The main purpose is to adjust the call sequence. For example, first call the SIP phone, and then call the alt.1. If I do not answer the call, I will transfer to mailbox: 801-mailbox.

The whole process is that when someone calls extension 801, the SIP phone of extension 801 rings first, if no one answers after 20s, then the alt.1 of extension 801

rings, if no one answers after 20s, and the call is transferred to 801 mailbox.

2.7. User phone routing by time

It is mainly used to configure how to transfer calls in different time periods. Click the pencil icon on the right side of a user as shown below to enter the configuration interface.



Username:	Time band:	Hot desk phone:	SIP phone:	Cell (alt.1):	Home (alt.2):	Alternative 3:	Wait for:	On no answer, divert to:
110	always	Yes	Yes	No	No	No	20 seconds	110-mailbox
801	always	Yes	Yes	No	No	No	20 seconds	801-mailbox
802	always	Yes	Yes	No	No	No	20 seconds	802-mailbox
803	always	Yes	Yes	No	No	No	20 seconds	803-mailbox
804	always	Yes	Yes	No	No	No	20 seconds	804-mailbox
805	always	Yes	Yes	No	No	No	20 seconds	805-mailbox
806	always	Yes	Yes	No	No	No	20 seconds	806-mailbox
807	always	Yes	Yes	No	No	No	20 seconds	807-mailbox

Time band: By default, the working time period of each extension is always, which means it works 24 hours a day. We can edit the time period for other time periods such as 9:00 am to 17:00 pm for working hours. The extension will work normally during this time period. Outside this time period, the rules you configure will be followed.

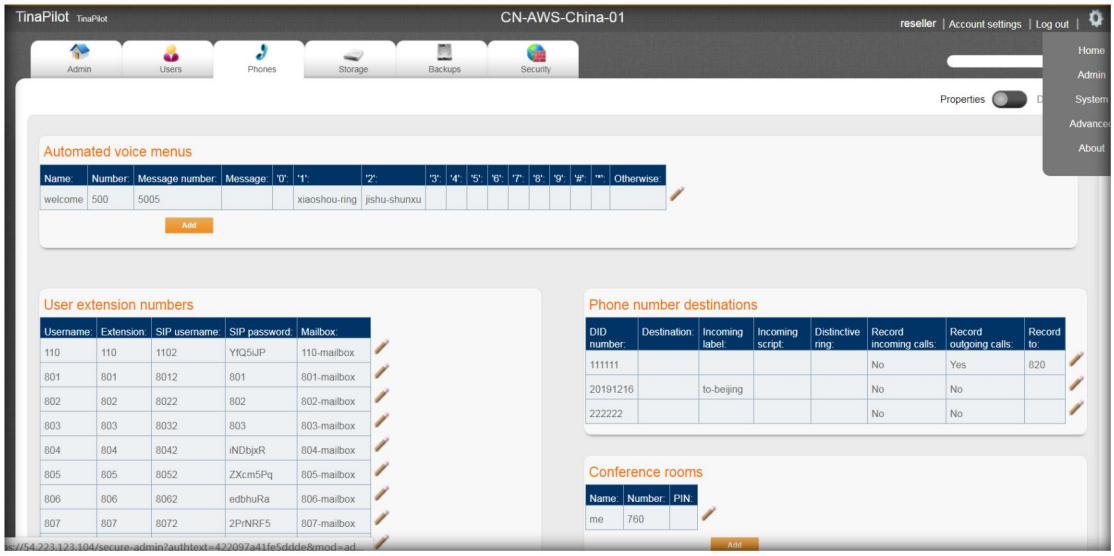
Out of hours: If extension 801 is configured with working hours from 9:00 am to

17:00 pm, and ‘Out of hours’ to alt.1.

Then this process indicates that extension 801 only rings during working hours, and not work in Out of hours. In Out of hours , the alt.1 rings,if alt.1 still does not answer the call after 20s, the call will be forwarded to 801 mailbox.

3. Phones

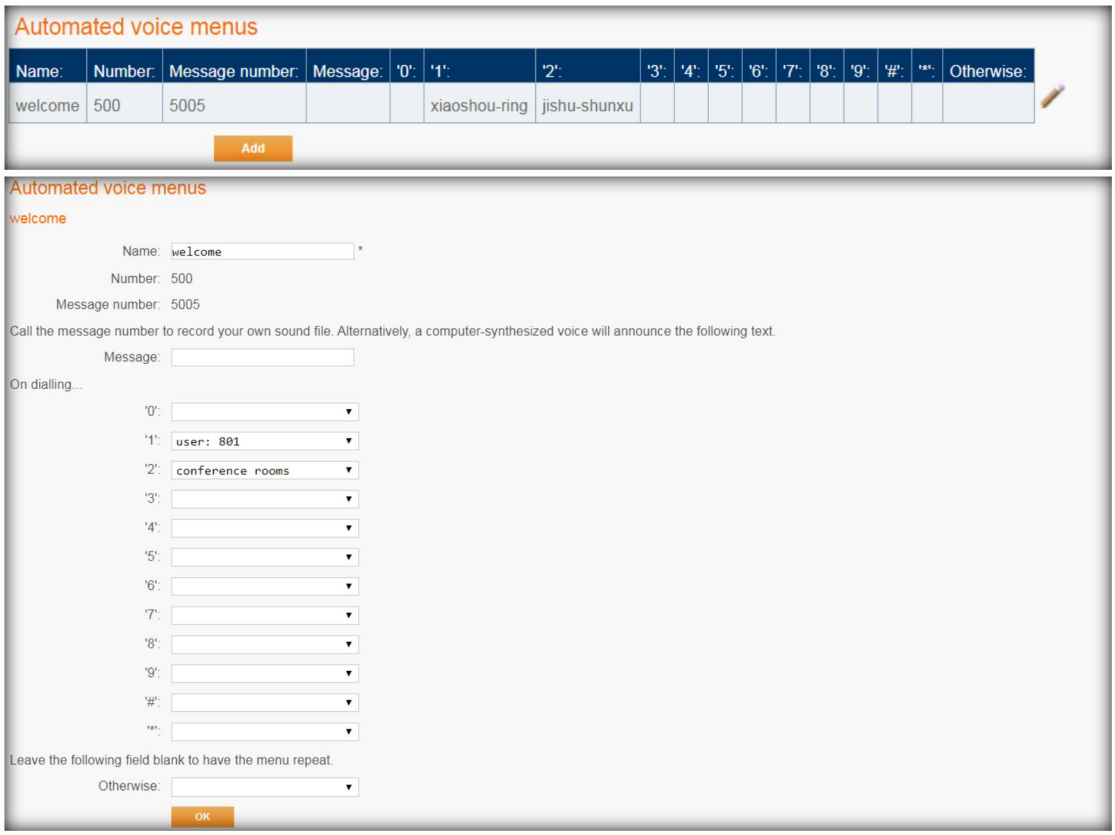
This page configures the voice-related settings for the user.



3.1. Automated voice menus

This page can be used to set the automated voice menu for incoming calls.

For example, press 1 to transfer extension 801, press 2 to transfer conference 760, and so on. Click Add to enter the voice menu configuration interface.



Name: The name of the automated voice menu.

Number: The system generates it by default.

Message number: generated by the system by default.

Message: When the user calls in, the automated voice will play the message here. At present, the system only recognizes English. If you input an English sentence in the text field, the system will automatically play the English content here when the user dials into this voice menu.

On dialing: There are a total of 10 options from 0-9. You can choose any content in the options, such as extension number, call queue, call sequence, etc.

Note:

Automated voice playback content, users can record by themselves. Enter the

message number on any phone registered to justINA (5015, each different automated voice menu has a different message number), there will be a voice prompt, prompting the user to record new voice content.

Automated voice playback of content, users can also find professionals to record and send the recording files to Equiinet. Equiinet's technical team will help you import the justINA system into the background.

3.2. User extension numbers

User extension numbers

Username:	Extension:	SIP username:	SIP password:	Mailbox:
110	110	1102	YfQ5iJP	110-mailbox
801	801	8012	801	801-mailbox
802	802	8022	802	802-mailbox
803	803	8032	803	803-mailbox
804	804	8042	iNDbjxR	804-mailbox
805	805	8052	ZXcm5Pq	805-mailbox
806	806	8062	edbhuRa	806-mailbox
807	807	8072	2PrNRF5	807-mailbox
808	808	8082	3fyHWWt	808-mailbox

Click the pencil icon on the right to enter the configuration interface:

User extension numbers

804

Username: 804

Extension: 804

SIP username: 8042

SIP password: iNDbjxR *

Mailbox: 804-mailbox

OK

User name: The user name when the user was created.

Extension: The extension number when the user was created.

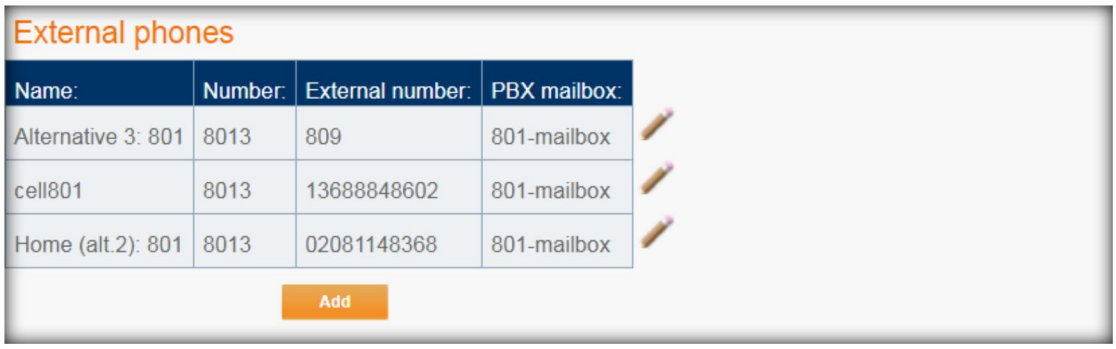
SIP username: Which means that when registering the extension number on the IP phone or softphone, add 2 after the extension number (2 represents registration).

SIP password: The password when registering the extension number.

Mailbox: Each user will have a voice mailbox by default.

3.3. Alternate Extension Number

If the backup number information is filled in the "User personal call forward path", the following information will be automatically generated here.



Name: The alternative number name of an extension. Such as Home(alt.2):801, it means it is alt.2 of extension 801.

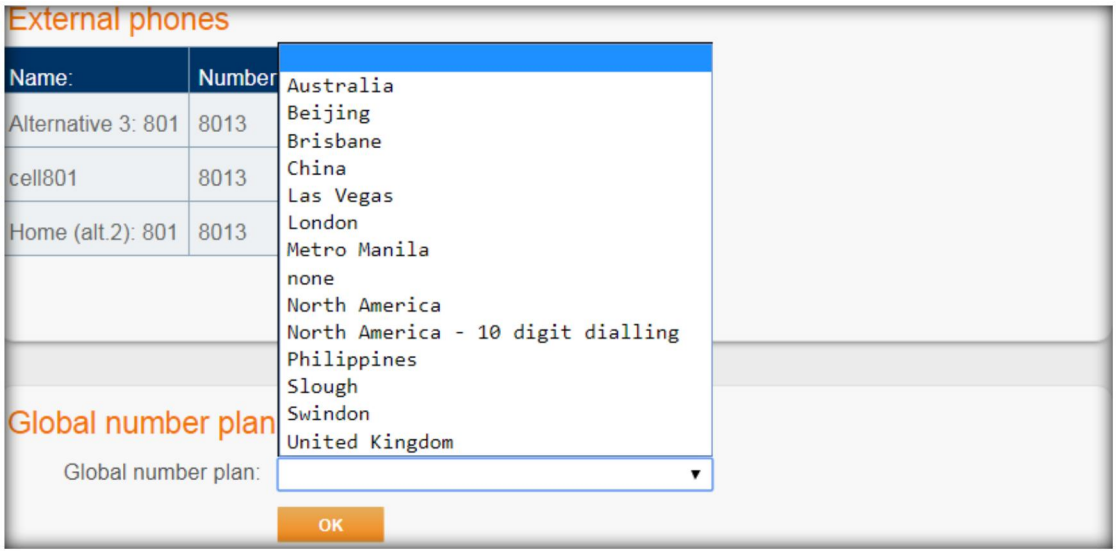
Number: The system will assign a number to this alternative number, which is

globally unique. For example, the alternative number of extension 801 is 8013.

External number: The external number is configured for the extension, such as 13052526354.

PBX mailbox: Each user will have a voice mailbox by default.

3.4. Global number plan



Global number plan: mainly used for fast dialing. For example, if we choose London, when calling a number in London, we can dial the number directly without adding an international prefix or area code.

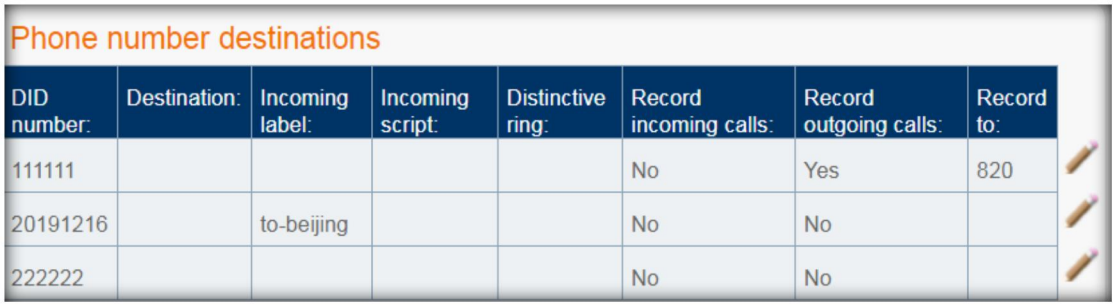
Due to inconsistent rules among the three major Chinese operators, Global number plan are rarely used in China.

3.5. Phone number destinations

It is mainly used for line information configuration. It is mainly used for Admin administrator. Because the Admin administrator does not have Reseller

permissions and does not have permission to add DID lines, only the permissions to edit lines are available here.

If Reseller is configured with line information, the corresponding information will be automatically generated here, which is convenient for Admin to modify.



Phone number destinations

DID number:	Destination:	Incoming label:	Incoming script:	Distinctive ring:	Record incoming calls:	Record outgoing calls:	Record to:
111111					No	Yes	820
20191216		to-beijing			No	No	
222222					No	No	

The information such as the Destination and the Incoming label are the same as those in the "DDIs and Trunks" described above.

3.6. Conference room

That is the conference room function, click Add to enter the add interface.

Conference rooms

Name:	Number:	PIN:
me	760	

Add

Conference rooms

me

Name: me *

Number: 760 *

PIN:

OK

Delete

Delete

Name: The name of the conference room.

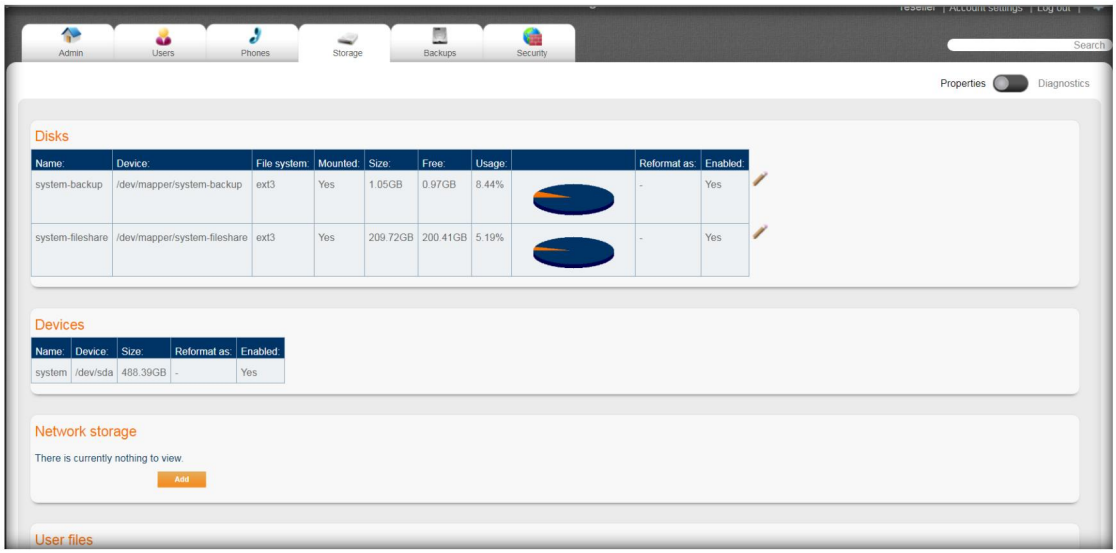
Number: The system will automatically generate a conference room number,

which can also be modified by the administrator.

PIN: Meeting room password.

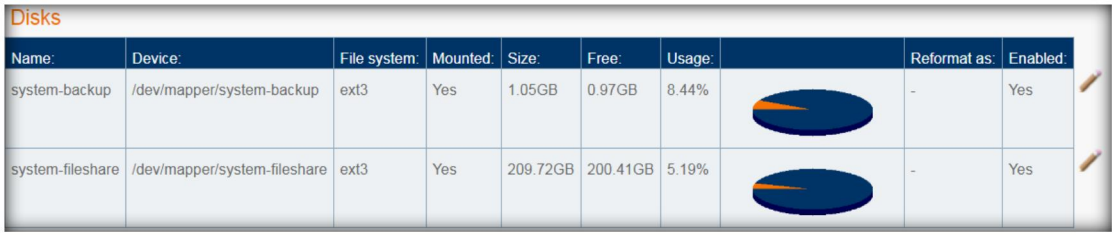
4. Storage

Storage information is mainly system storage information.



4.1. Disks

View the disk usage, mounting conditions, etc. Generally we don't need to do any configuration.



4.2. Devices

View device hard drive information detected on the device. Generally we don't need to do any configuration.

4.3. Network Storage

It is mainly used for network storage, such as a NAS server in your network. You can fill in the relevant information of this server here, so that corresponding users can store files on this NAS server through justINA, and click Add to enter the configuration interface.

Name: The name of the network storage.

Address: The address of the network storage.

Share: The path to the network storage shared space.

Username: Network storage access user name.

Password: Network storage access password.

Workgroup: WORKGROUP if it is a windows system.

Enabled: Just tick.

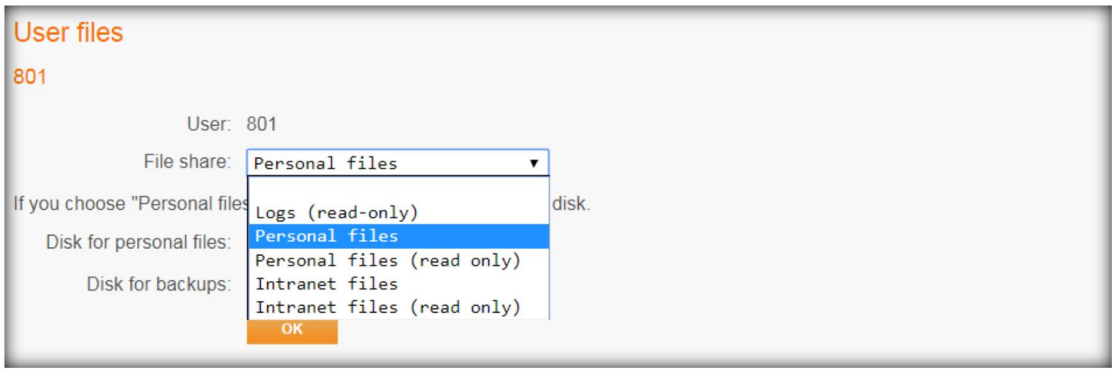
Finally click OK and wait for justINA to automatically identify the network storage. If the network storage is successfully identified, the values of Size, Free and Usage will automatically appear.

4.4. User Files

Each extension user will automatically generate a user file. The following configuration is the system default. Click the pencil icon to enter the configuration interface.

User files

User:	File share:	Disk for personal files:	Disk for backups:
110	Personal files	system-fileshare	system-backup
801	Personal files	system-fileshare	system-backup
802	Personal files	system-fileshare	system-backup
803	Personal files	system-fileshare	system-backup
804	Personal files	system-fileshare	system-backup
805	Personal files	system-fileshare	system-backup
806	Personal files	system-fileshare	system-backup



File share: Select the sharing attributes of the user files for this extension.

Logs (read-only): Shared files are logs and are read-only.

Personal files: Users can log in to shared folders and can edit, add, delete files, etc.

Personal files (read only): The content in the shared folder is read-only.

Intranet files: Same as Personal files.

Intranet files (read only): Same as Personal files (read only).

Disk for personal files: The disk where personal files are located. The system defaults, and generally does not need to be changed.

Disk for backups: The disk where the personal archive is backed up. The system defaults, and generally does not need to be changed.

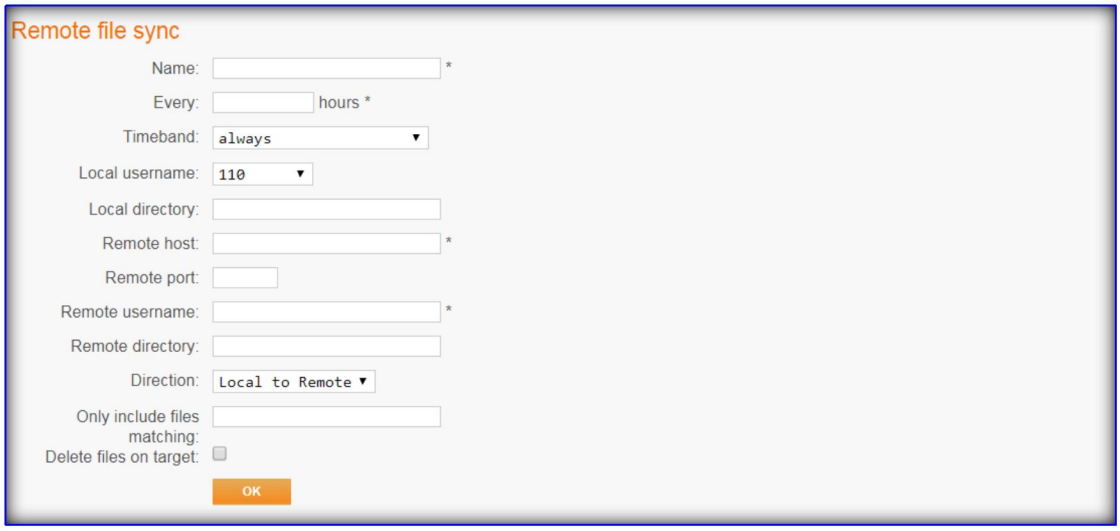
4.5. Remote file sync

It is mainly used for remote backup of local cloud disk files to other servers.

No server support has been tested in the market, but Equiinet has its own cloud server and charges.

The company can also build a backup server on the LAN itself, which needs to support the RSA key. Only the latest part is updated during backup, thus avoiding re-backup every time, which takes time.

Click Add to enter the remote synchronization file configuration interface.



Name: The name of this backup operation. The name is arbitrary.

Every: How often do you back up by hour.

Timeband: The system automatically backs up time. Generally, night is selected.

Local username: Back up files under a certain user. If it is 801 users, the cloud disk content of 801 will be backed up.

Local Directory: backup the folders under this user. By default, the entire folder is backed up.

Remote host: remote server address.

Remote port: The port opened by the remote server. This port is used for data transmission with the justINA system.

Remote username: The remote server username.

Remote Directory: A list of folders used by the remote server to store backup

files.

Direction: Direction can choose from local to remote server, or from remote server to local.

Only include files matching: Matches filtered files. For example, .mp3 only matches mp3 files for transmission.

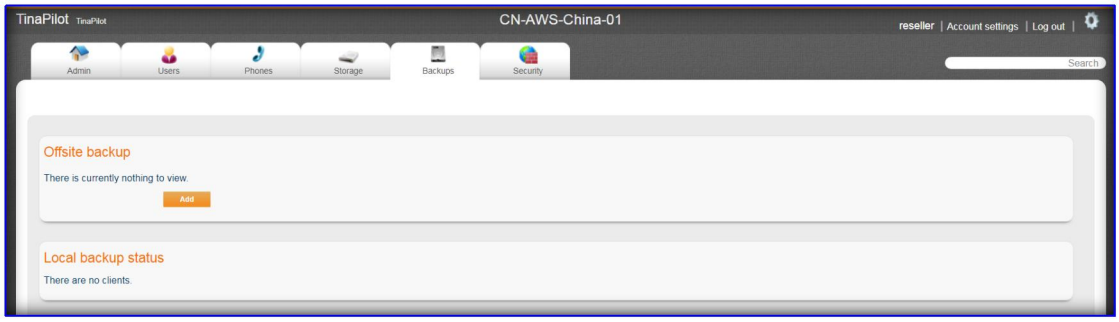
Delete files on target : transfer the file to the destination server folder, whether to delete the existing file under the destination server file.

4.6. RSA keys

RSA keys are used with remotely synchronized files. To back up files of a user in justINA, such as the 801 folder, you need to send 801 RSA keys to the remote server.

5. Backups

Back up the corresponding data of the local extension number user. There is no backup by default.



5.1. Offsite Backup

Used to remotely backup data to a third-party host. It' s the same with "Remote file sync"

Name: The name of this backup operation. The name is arbitrary.

Local username: Back up files under a certain user. If it is 801 users, the cloud disk content of 801 will be backed up.

Remote host: remote server address.

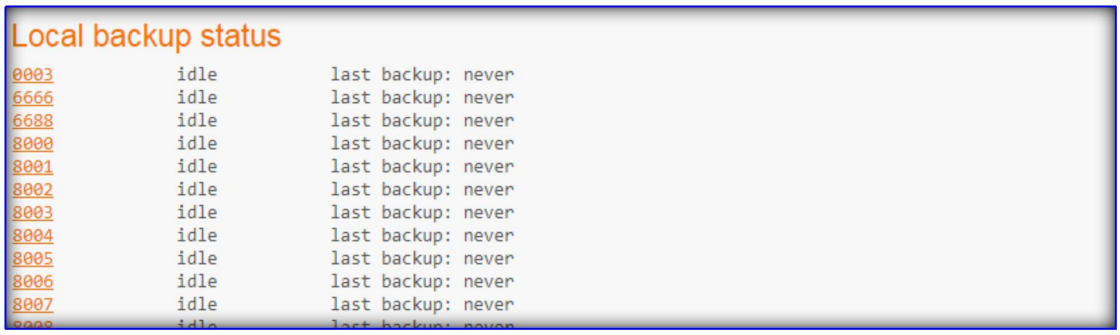
Remote port: The port opened by the remote server. This port is used for data transmission with the justINA system.

Remote username: The remote server username.

Remote directory: A list of folders used by the remote server to store backup files.

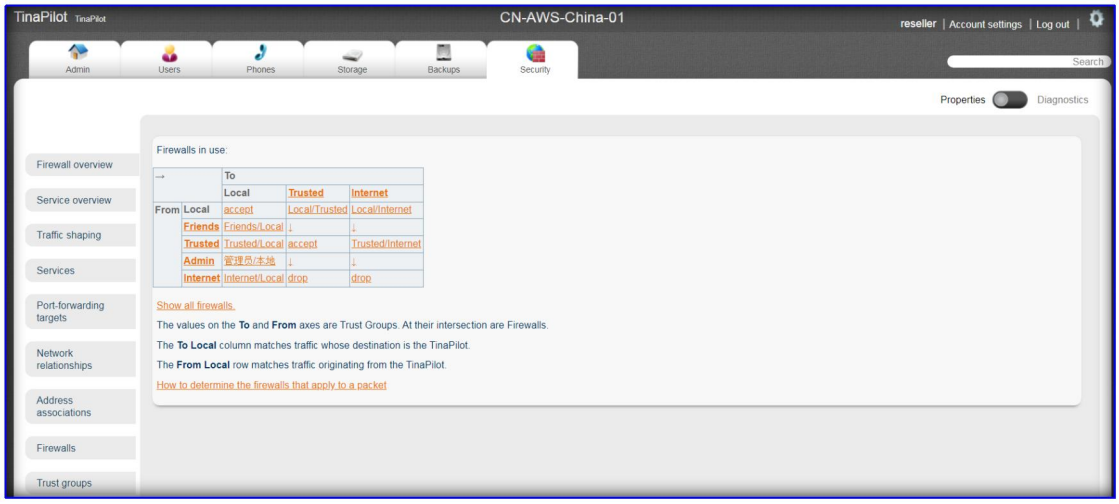
5.2. Local backup status

In default, the local backup status shows the backup status of local user.



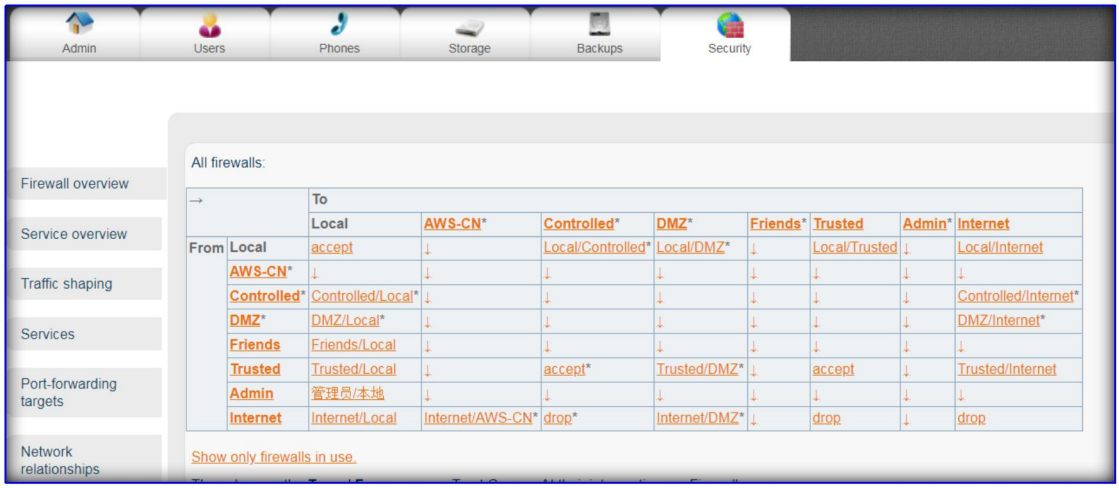
6. Security

The security page is mainly the UTM configuration page, which contains firewall, services, port forwarding and other information.



6.1. Firewall Overview

The default firewall overview only shows the firewalls in use. Click "Show all firewalls" to display all firewalls.



The firewall is mainly composed of various groups, each group is independent, and each group has its own attributes. For example, the Admin group has the Admin attribute. The Admin can assign a certain IP (a certain LAN) to the attribute of the Admin. Then this IP can play the role of Admin.

In All firewalls we see groups, and group-to-group combinations.

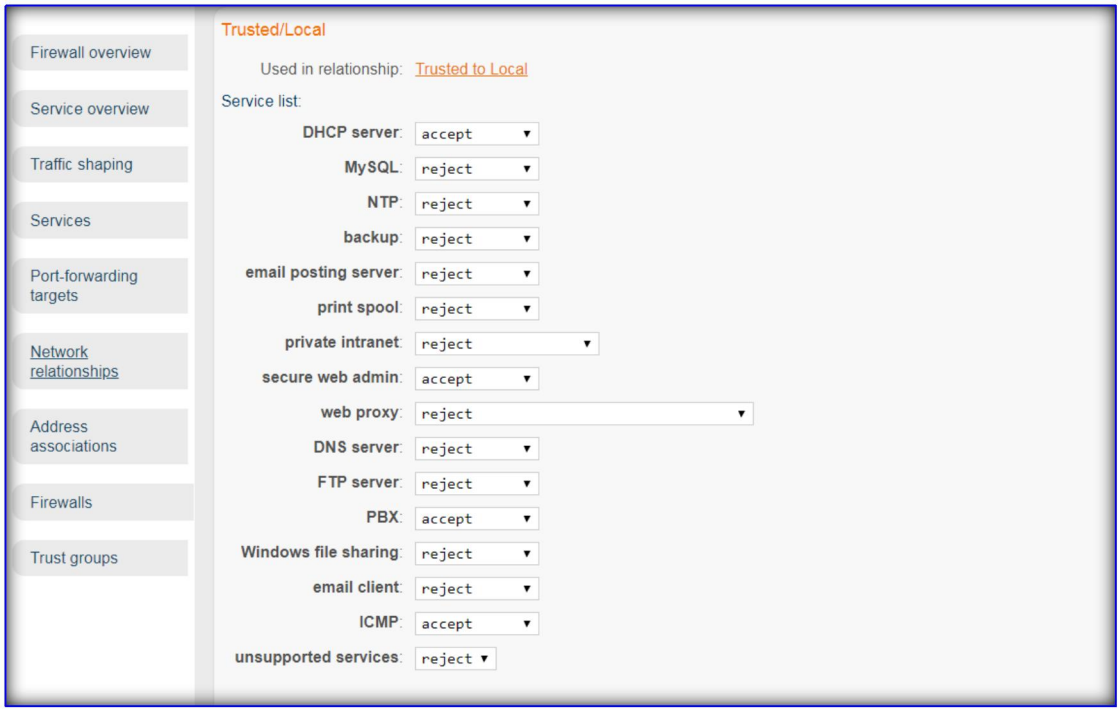
The real application of a firewall is a group-to-group combination.

Here is an example of the Trust / Local combination: As can be seen from the figure below, in this combination, the status of various protocols and services,

such as the device receiving ICMP, whether to allow https access, etc. The corresponding action can simply debug the firewall.

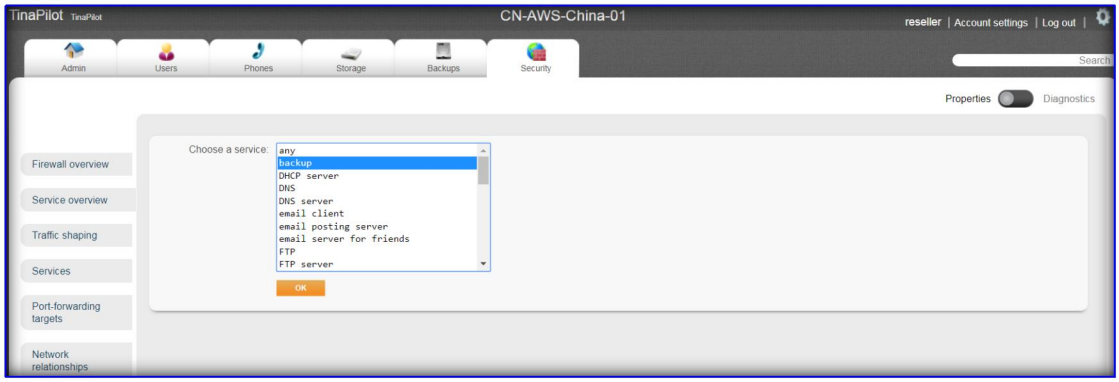
For example, if we choose to ignore the MySQL service, the trust group to the local MySQL service will be ignored.

→		To							
		Local	AWS-CN*	Controlled*	DMZ*	Friends*	Trusted	Admin*	Internet
From	Local	accept	↓	Local/Controlled*	Local/DMZ*	↓	Local/Trusted	↓	Local/Internet
	AWS-CN*	↓	↓	↓	↓	↓	↓	↓	↓
	Controlled*	Controlled/Local*	↓	↓	↓	↓	↓	↓	Controlled/Internet*
	DMZ*	DMZ/Local*	↓	↓	↓	↓	↓	↓	DMZ/Internet*
	Friends	Friends/Local	↓	↓	↓	↓	↓	↓	↓
	Trusted	Trusted/Local	↓	accept*	Trusted/DMZ*	↓	accept	↓	Trusted/Internet
	Admin	管理员/本地	↓	↓	↓	↓	↓	↓	↓
	Internet	Internet/Local	Internet/AWS-CN*	drop*	Internet/DMZ*	↓	drop	↓	drop

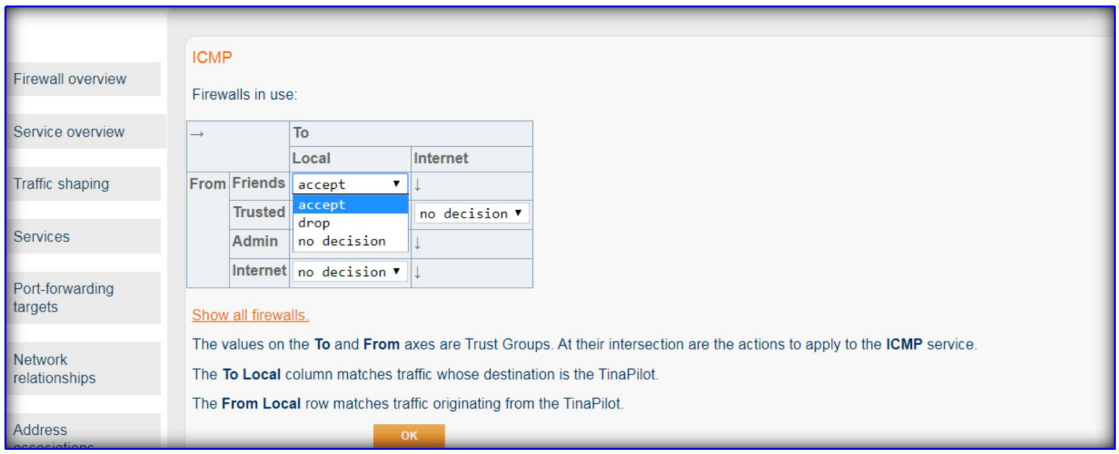


6.2. Service Overview

It is mainly for the overview of the existing services in the system.



Here is an example of ICMP service: After choosing ICMP service and clicking OK, it will list which groups in the firewall are being used by ICMP. Users can edit the status of ICMP service in each group relationship. For example, in the Friends / Local group, we can edit it to drop.

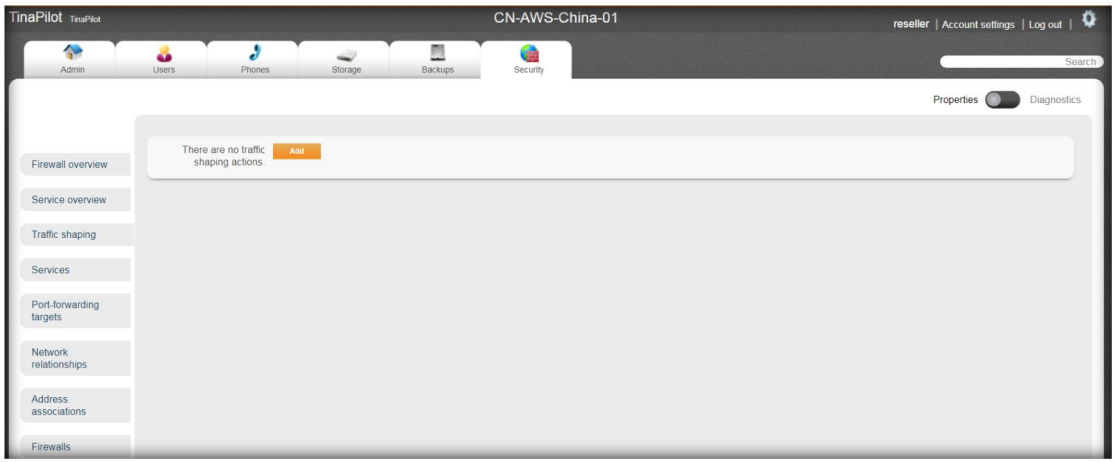


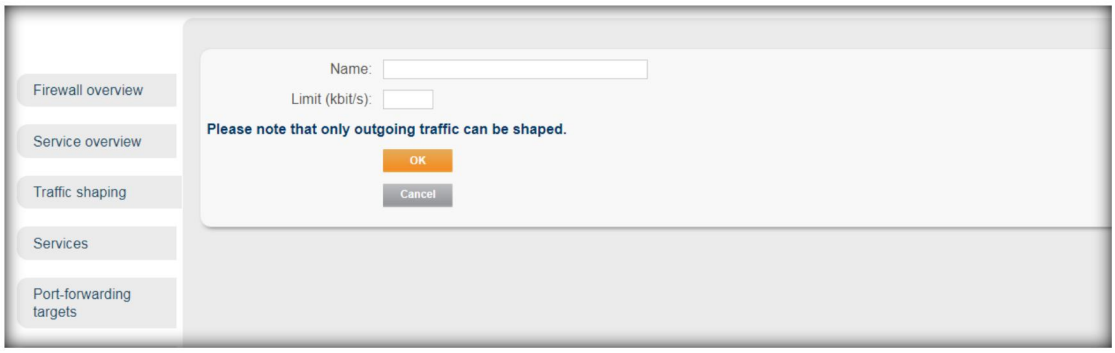
6.3.Traffic shaping

Traffic shaping is mainly for the control of justINA's egress traffic to ensure that justINA has enough traffic to access the network. Click Add to enter the editing interface.

Note:

This function is only used when justINA is used as a gateway.



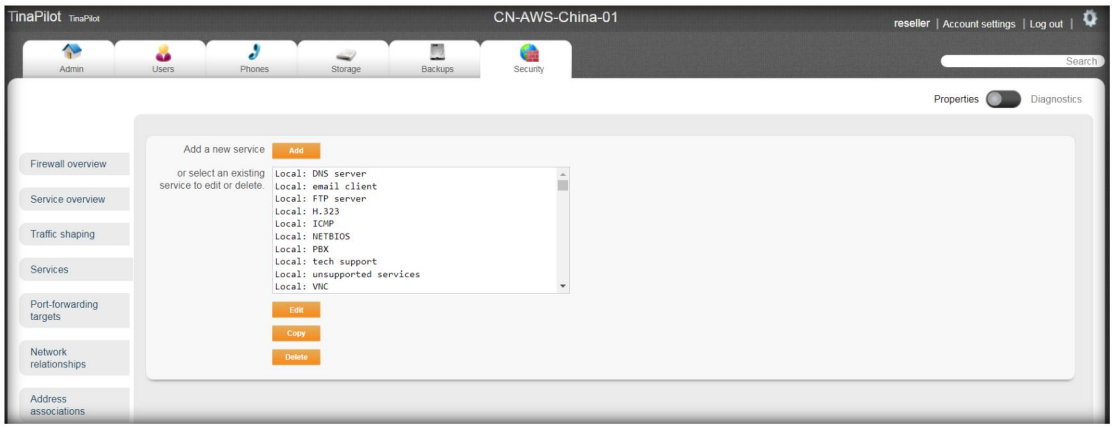


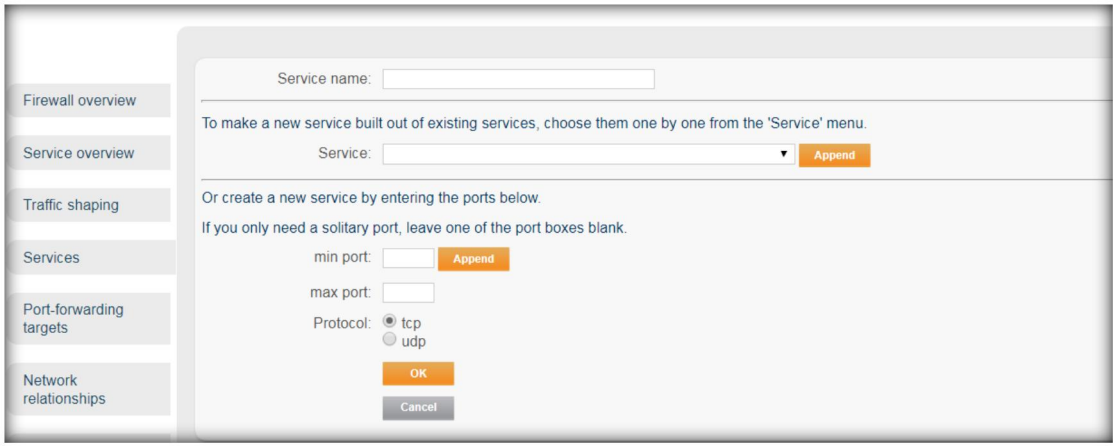
Name: The name of the Trafic shaping. The name is arbitrary.

Limit (kbit / s): The limit unit is kbit / s. Users can fill in the corresponding data according to the actual network conditions.

6.4. Services

It mainly edits, adds, and deletes services in the justINA system. Click the Add button to enter the configuration interface for adding services.





Service name: Create a new service name. The name is arbitrary.

Services: New services can inherit existing services. Select the corresponding service and click Add.

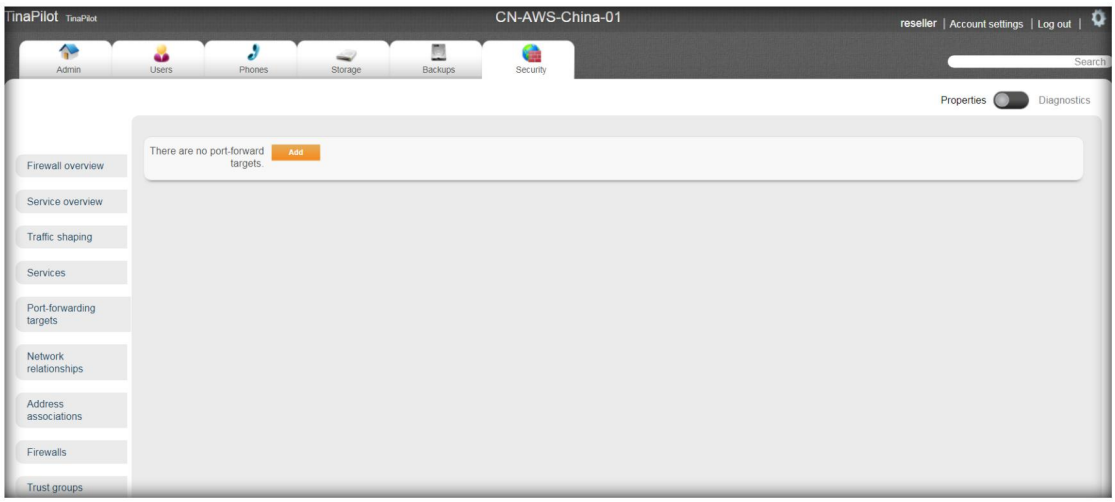
Min port: The port of the newly created service can be a port or a segment of port. When a port is created, the minimum port is the minimum value of this port.

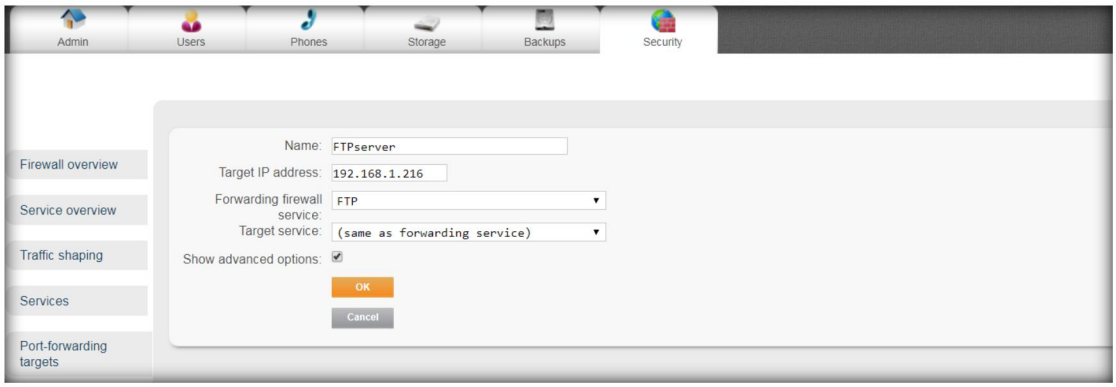
Max port: The maximum port is the maximum value of the port in this segment.

Protocol: The port protocol of the newly created service. You can choose TCP or UCP.

6.5. Port Forwarding targets

It is mainly used for port forwarding. If the server behind justINA needs to be accessed by the external network, you can configure port forwarding on justINA. Click Add to enter the configuration interface.





Name: Any name, such as FTPserver.

Target IP address: Internal server address.

Forwarding firewall service: Select the service you want to map, for example, you want to map the internal FTP server, so the service you need to select here is FTP.

Target service: Default (same as forwarding service)

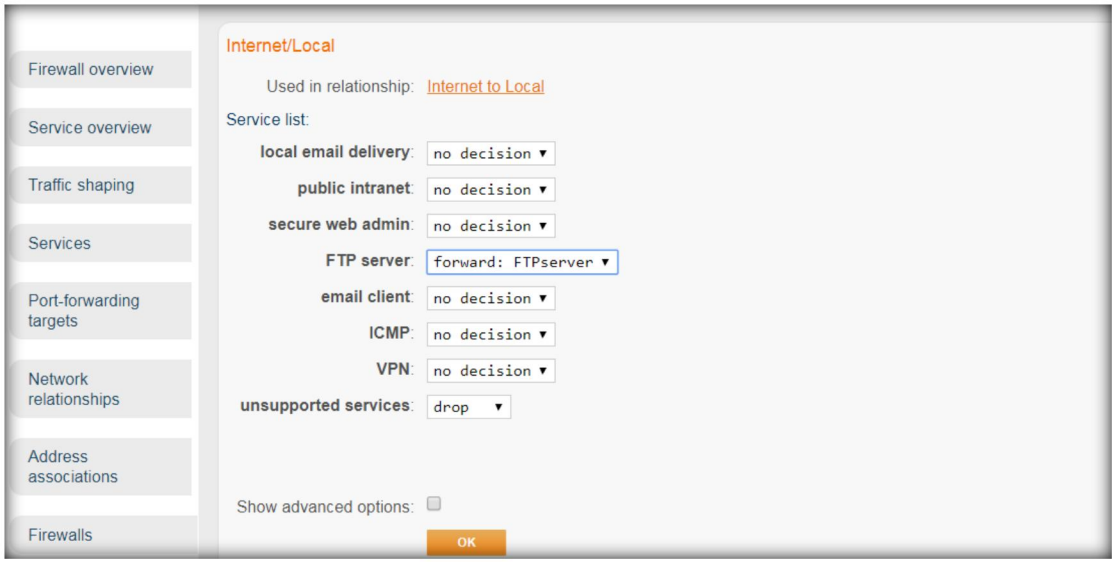
Show advanced options: The target service will not be displayed until you check it.

Finally click OK and save.

call of port forwarding target:

At this point, the port forwarding is done, but it also needs to be called. At this time, you need to call this mapping in the firewall to really achieve the desired effect.

For example, on the Internet / local, select the FTP server as forward: FTPserver. Anyone who comes in from the Internet and wants to access the FTP server must go through this forwarding to access the FTP server normally. Finally, click OK to save.

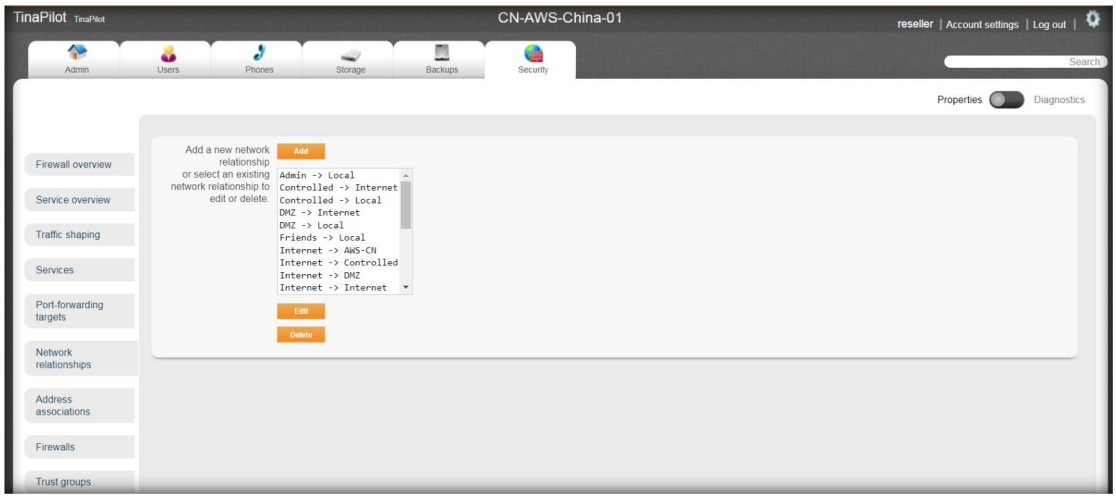


6.6. Network Relationships

Mainly configure the relationship between groups. For example, in the firewall configuration interface, all the relationships between groups are network relationships.

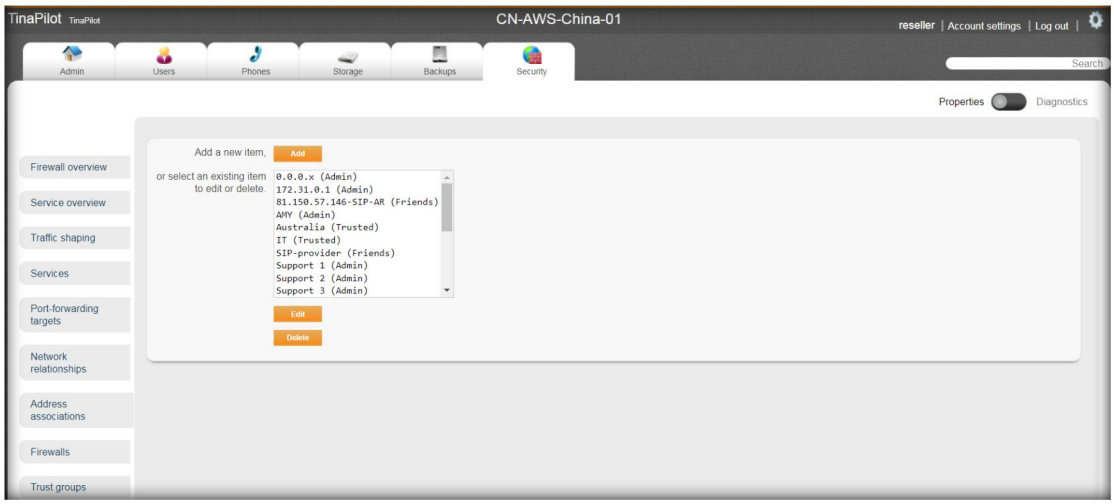
Users can configure network relationships on their own, and click Add to enter the network relationships configuration interface.

There is generally no configuration required here, just keep the default.

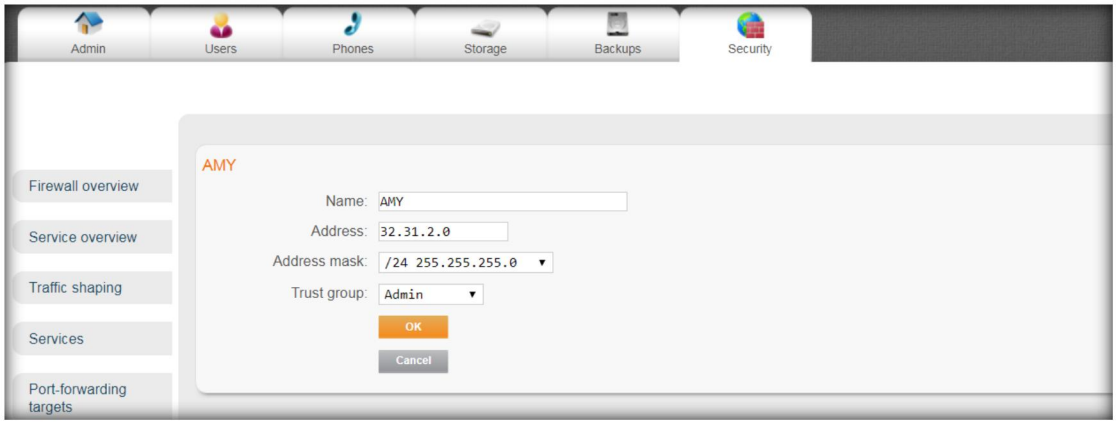


6.7. Address Association

Put the corresponding IP address in a certain group so that this IP has the permissions of some groups.



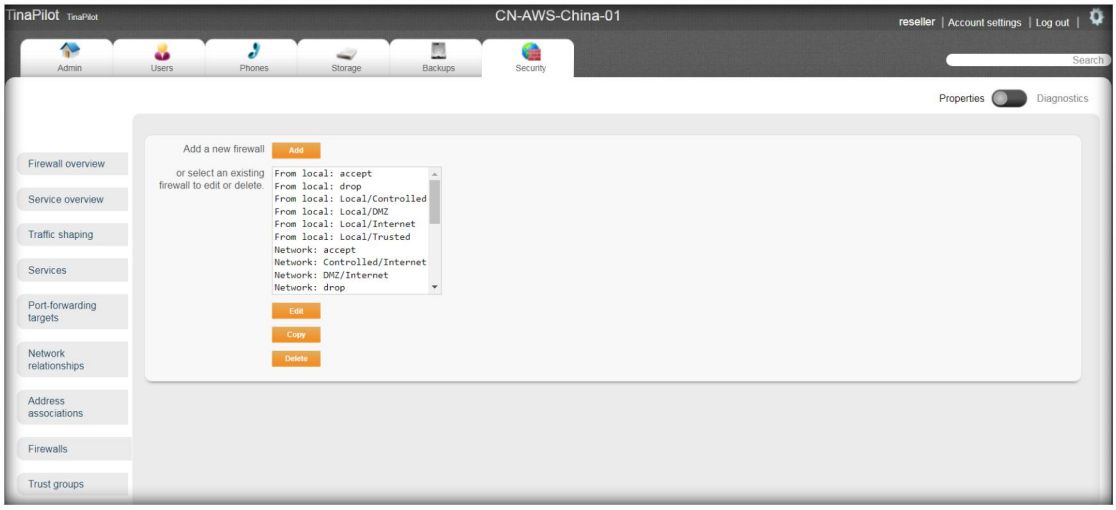
Click the Add button to enter the editing interface



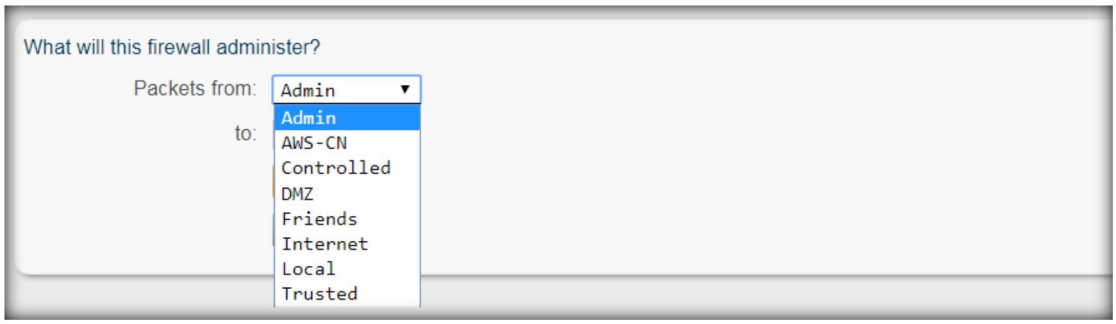
As shown in the figure above, the name is AMY, and the IP address with the address 32.31.2.0 is added to the Admin group. Then 32.31.2.0 has Admin rights and can access justINA as an administrator.

6.8. Firewalls

Edit, add, and delete all network relationships and behavior operations in the firewall.



Click Add to enter the interface



We can create a group-to-group combination to manage the data trend.

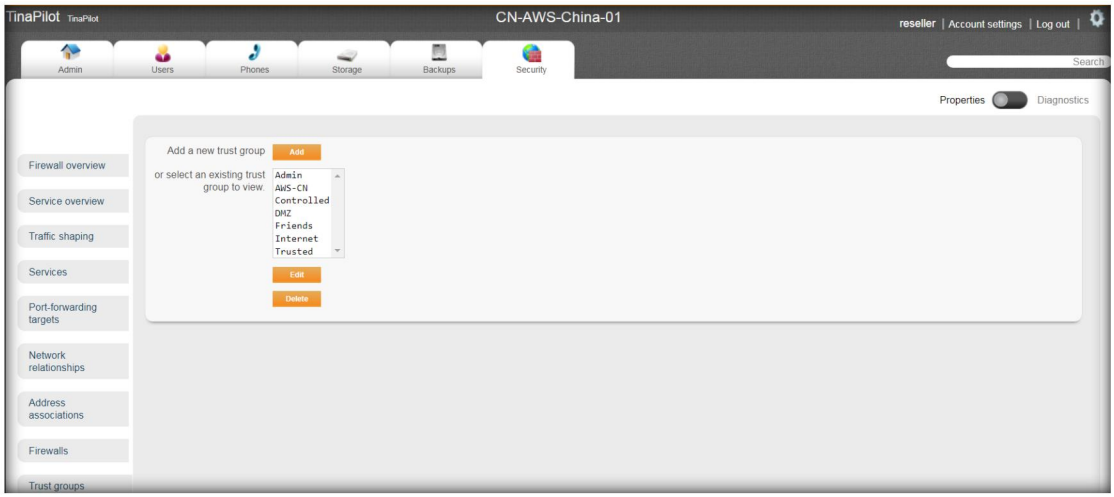
Note:

The system's default firewall configuration is not recommended for modification.

6.9. Trust groups

Edit, add, and delete operations of the Trust group. Used to add a new network group to the Trust group.

If a new group School is added, School appears in the firewall.



Chapter 3 System

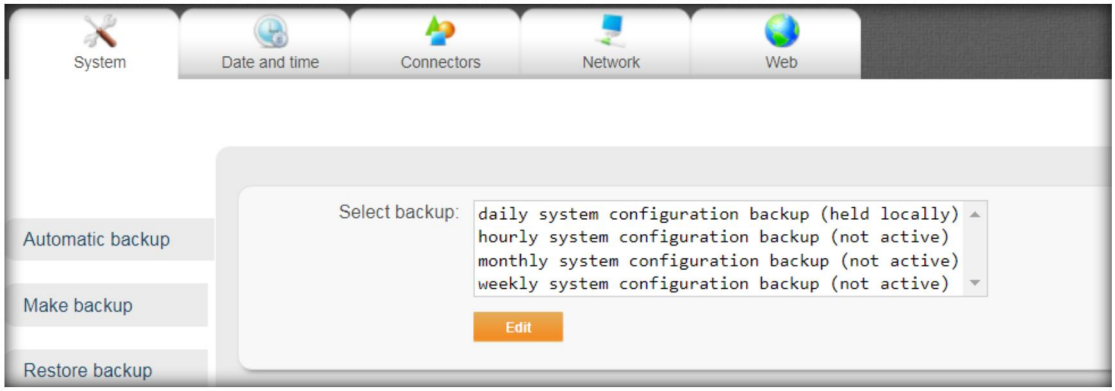
1. System

Top right gear button-> System

The system setting interface mainly displays the system information overview interface, which includes system backup, restart, shutdown and other settings.

1.1 Automatic backup

If you want to use the Automatic backup feature for daily or hourly. , please contact Equiinet staff if required contact.

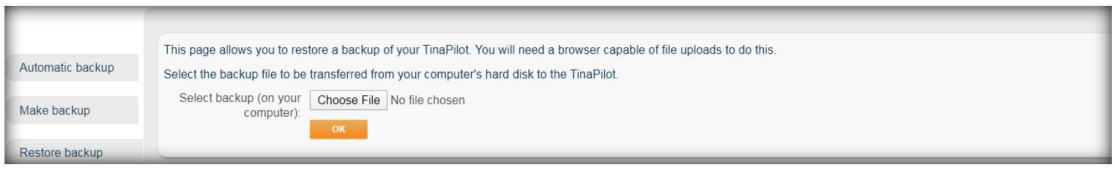


1.2 Make backup

We can make backup for system configuration manually. Click OK and the system configuration file will be downloaded automatically.

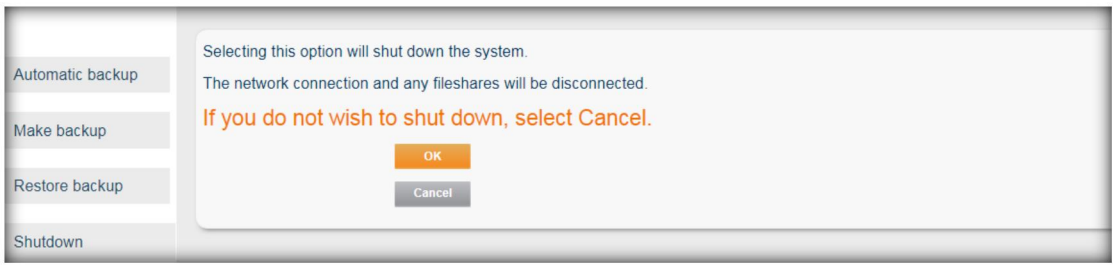
1.3 Restore backup

We can restore system by system backup configuration file.



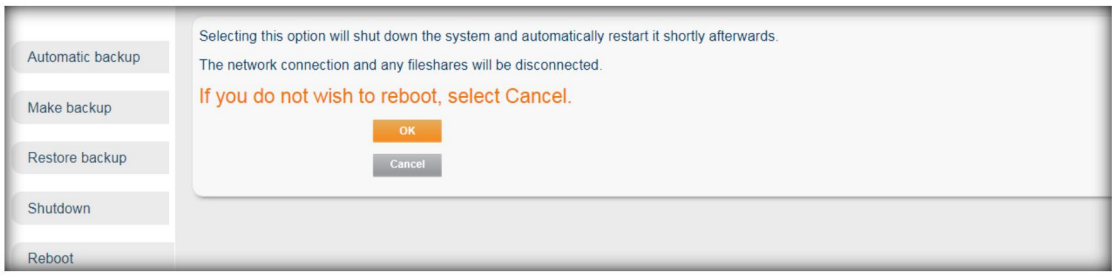
1.4 Shutdown

We can shutdown system on web



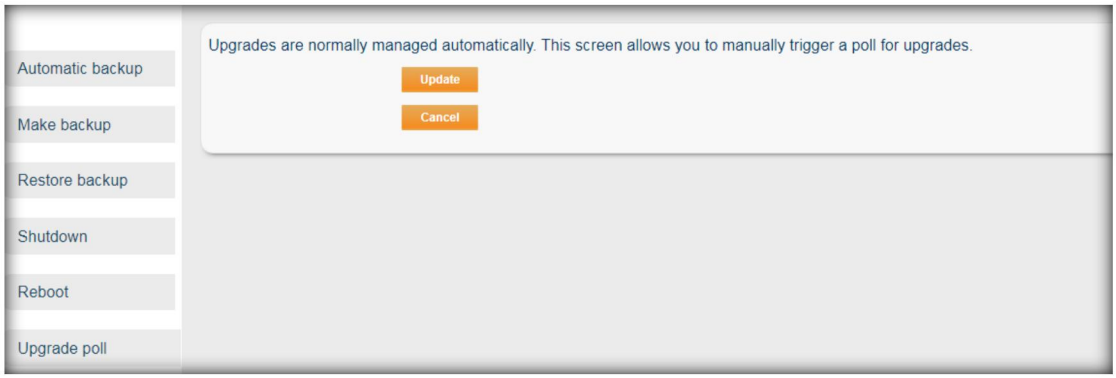
1.5 Reboot

We can reboot system on web



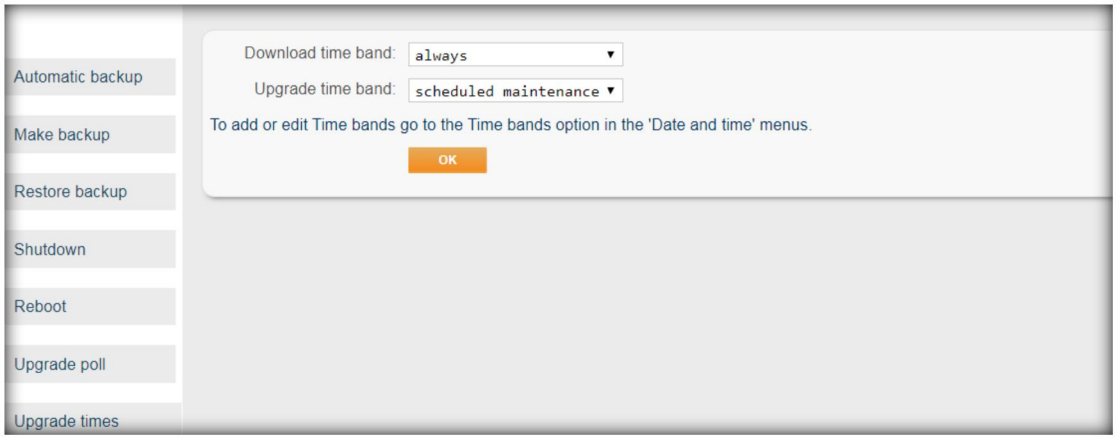
1.6 Upgrade pool

We can upgrade system on web



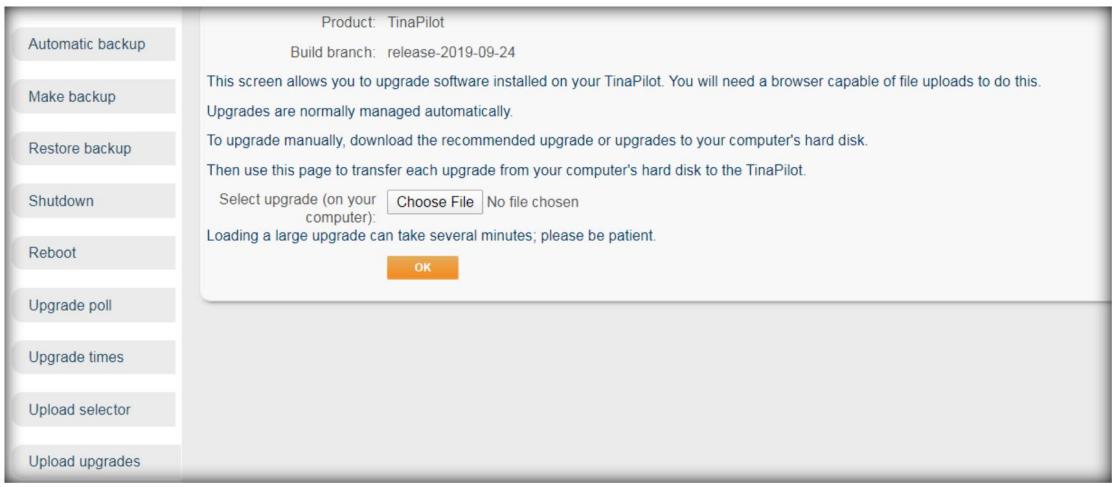
1.7 Upgrade times

We can choose download and upgrade time band system on web



1.8 Upload selector and Upload upgrades

They are default configuration , we do not need to edit it.

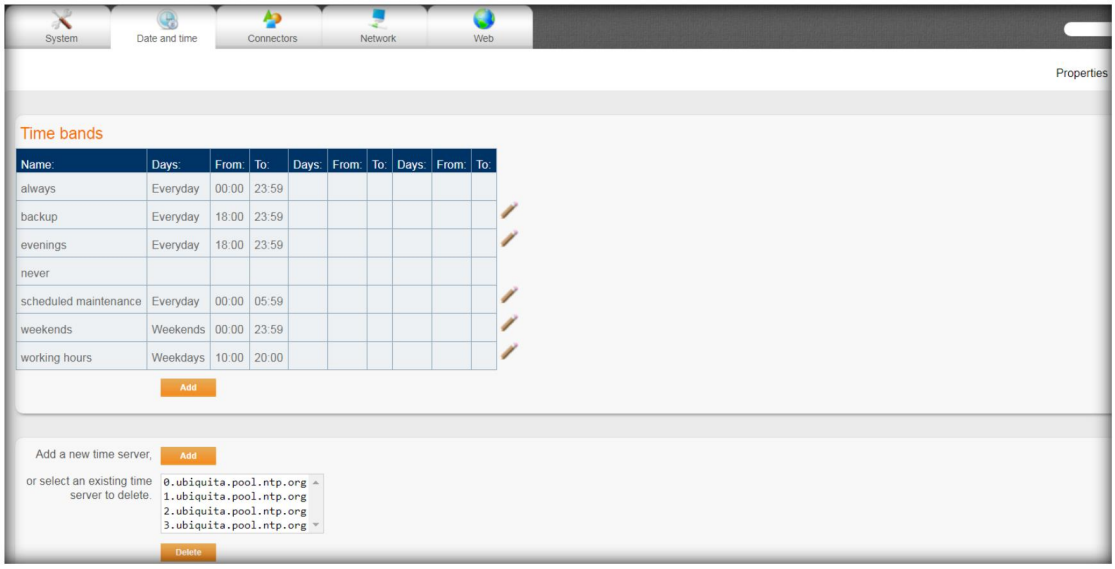


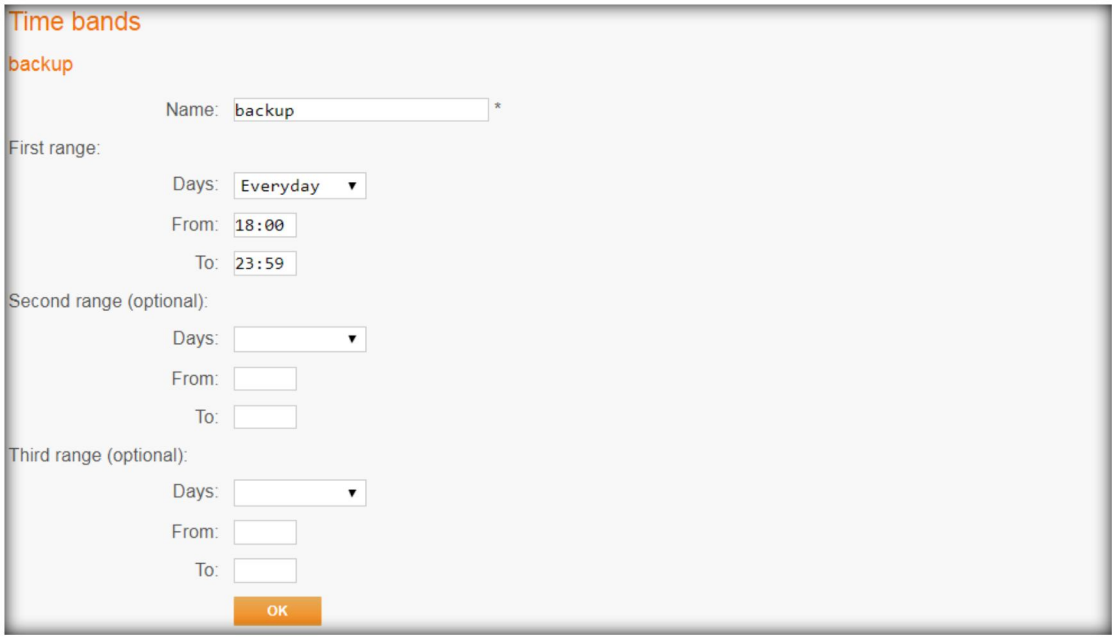
2. Date and time

The Date and time setting page is used to adjust the system time and time zone.

2.1. Time bands

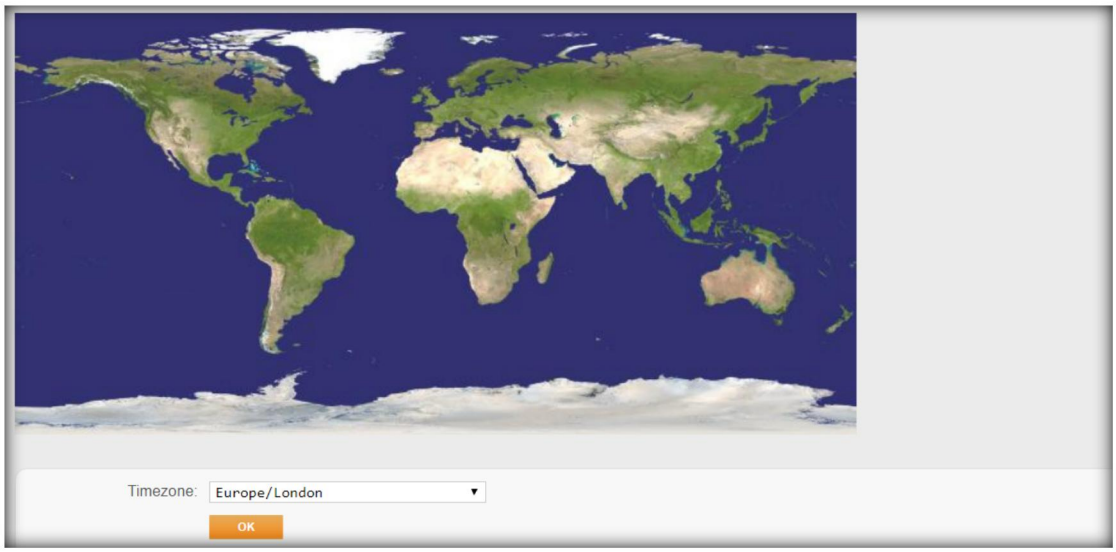
You can customize the time period, such as commute time, weekend time, etc., which can be called in the "User phone routing by time" function.





2.2. Time zone

We can choose time zone for system.

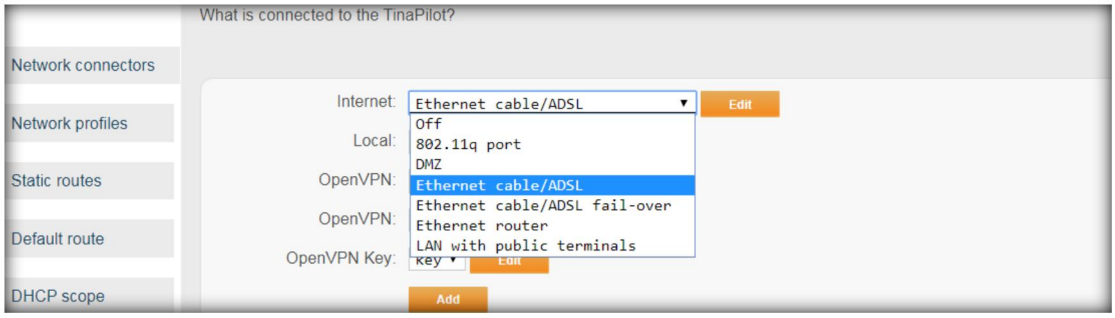


3. Connectors

The connectors interface is mainly used to configure the network of the device , including WAN port settings, LAN port settings, routing configuration, WIFI configuration, DHCP function configuration, VPN function configuration, etc. As shown in the figure below, configure the WAN port, LAN port, wireless, and add VPN functions on the "Network Connectors" page.

3.1. Network Connectors-WAN Port

The Internet is the WAN port.



The connection methods of the WAN port are:

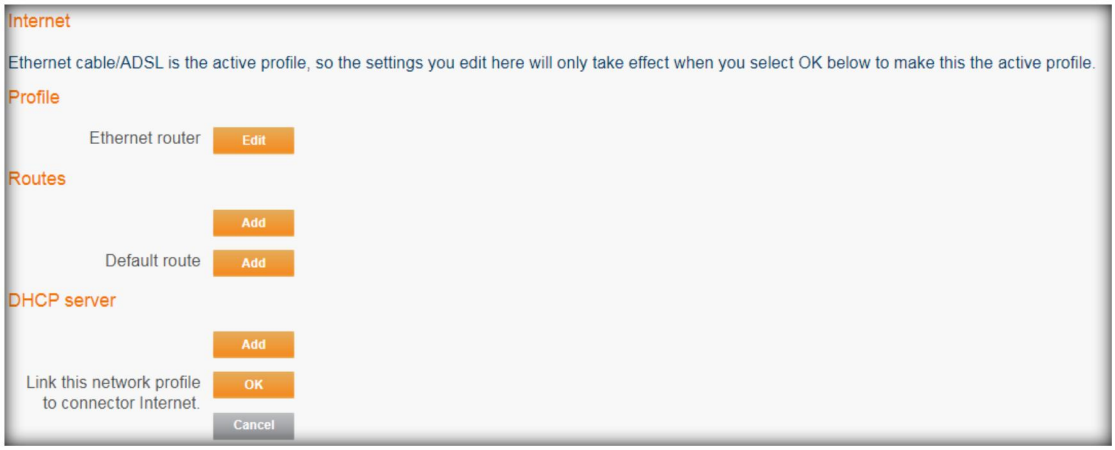
Off: Close this WAN port.

Ethernet cable / ADSL: Obtain an IP address automatically.

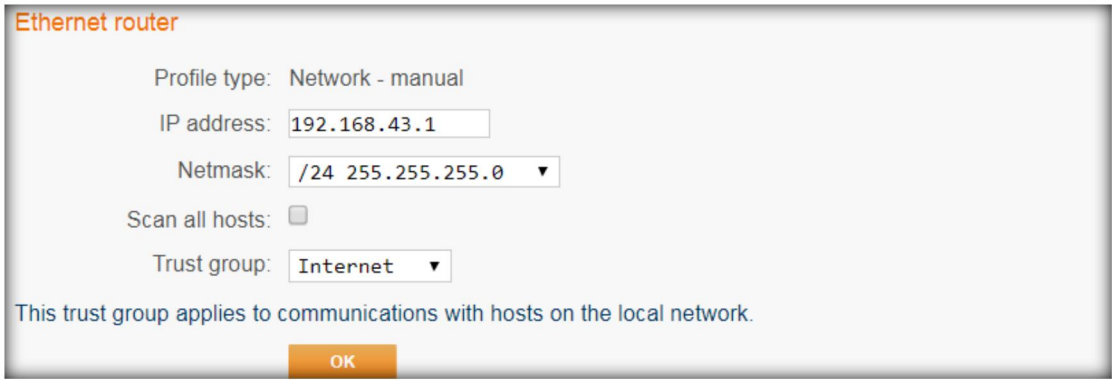
The usage scenario is that the WAN port is directly inserted under the ADSL dialler to directly obtain the IP address assigned by the operator. There are not many such application scenarios.

Ethernet router: Manually and statically configure the WAN port IP address, which is more common here. Here we take Ethernet router as an example to explain how to manually configure the WAN port IP address.

Select the WAN port type as Ethernet router, and click OK to save. Then, click Edit on the right side of the WAN port to enter the editing interface.



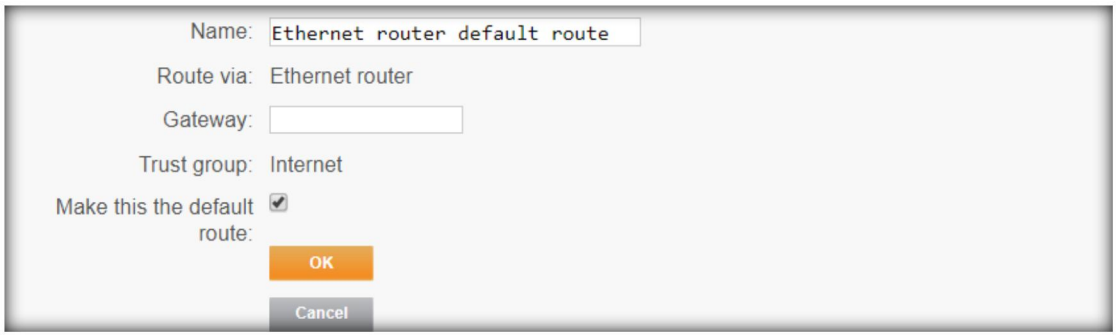
Configure in turn: Ethernet router, default route (click the "Add" button behind the default route).



IP address: The IP address of the WAN port, usually provided by the operator.

Netmask: The Netmask corresponding to the IP of the WAN port, usually provided by the operator.

Trust group: Internet group. The default is the Internet group. Because the WAN port is connected to the Internet, the default is the Internet group.



Name: The default is fine, or you can edit it yourself.

Gateway: The gateway address is given to you by the operator.

Trust group: The default Internet group.

Make this the default route: checked by default.

3.2. Network Connectors-Local Port

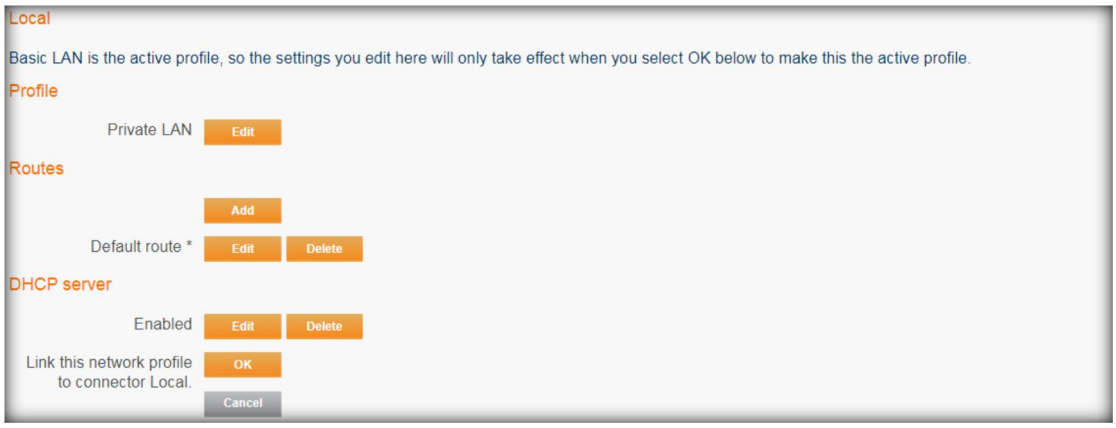
The Local port is also a LAN port. The connection methods are:

Off: Close the LAN port.

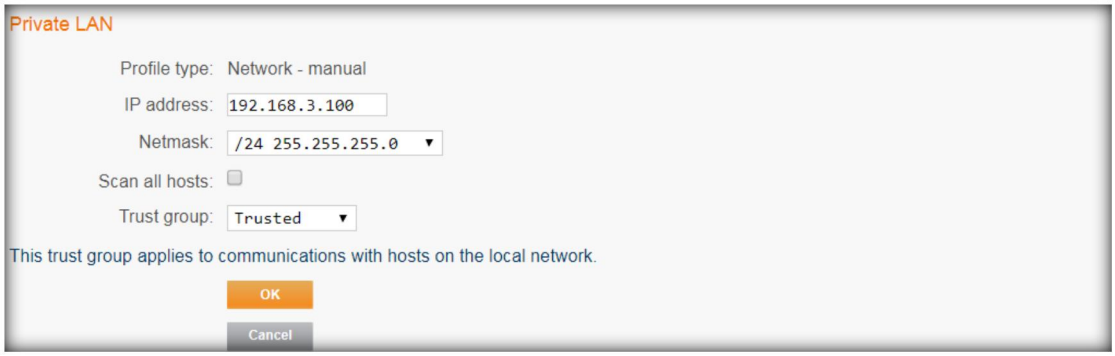
Private LAN: This is the default configuration. The other two connection methods are generally not used.

Below we take Private LAN as an example to show how to manually configure the LAN port IP address.

Click Edit on the right side of the Local port(on the Private LAN option) to enter the editing interface.



Configure in turn: Private LAN, default route.



IP address: The IP address assigned to the LAN port, which is usually assigned by

the network administrator.

Normally, justINA is a pure terminal. It only needs to connect the LAN port to the customer network switch, so you only need to configure a network management IP for the LAN port.

Netmask: The Netmask is assigned by the NMS.

Trust group: The default is the trust group.

Name: The default configuration, or you can edit it yourself.

Gateway: The local gateway address notified by the network management.

Trust group: The default is the Internet group.

Make this the default route: checked by default.

Note:

When justTINA is used as a pure terminal to access the network, it needs to be configured here, and DHCP is disabled. When justINA is used as the gateway, the WAN port is connected to the operator in the access network, and the LAN port is connected to the switch. The default route is not configured here and the DHCP is enabled.

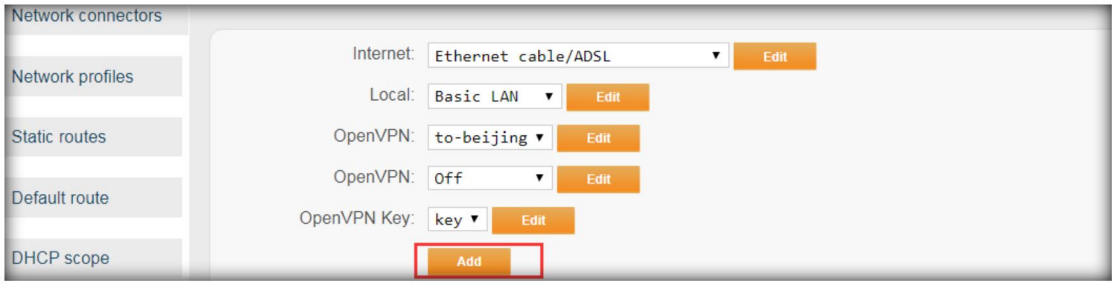
3.3. Network Connectors-VPN key

The VPN key usage scenario is: Customers at home or on business trips can import the VPN key on their mobile phones or computers to access the company intranet, make phone calls, or access network cloud disks. At this point, the customer feels like working in the company.

Before officially using a VPN key, we need to establish a VPN key, generate a VPN key, and download a VPN key.

Establish VPN key:

On the main interface of the network connector, click Add.



Select the OpenVPN key and click OK to enter the VPN key configuration interface.

Profile name: Custom, generally defined as "key".

Port: The system automatically generates it. For unified management, we configure it as 8326.

IP address: Any private address is sufficient (one IP or one network segment is acceptable). To unify management and avoid conflicts with daily IP addresses, we configure it to 172.16.1.0.

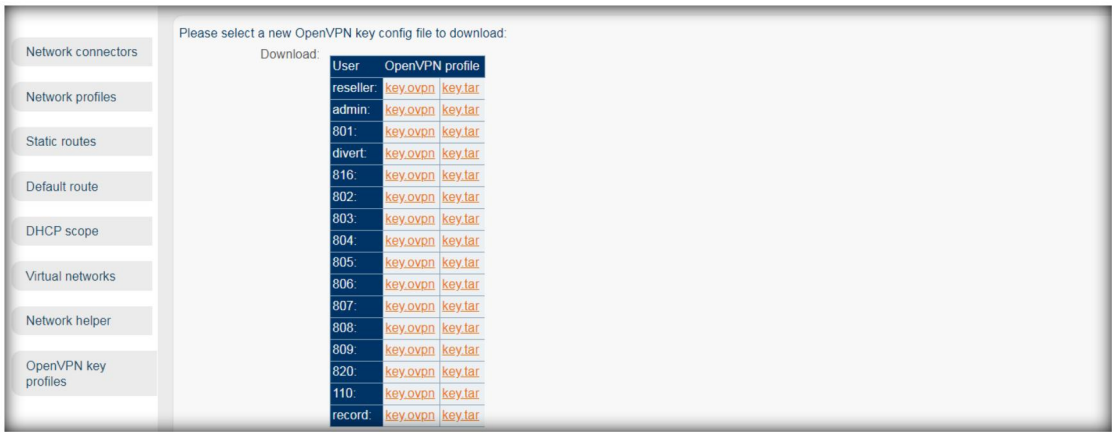
Netmask: Just select the corresponding netmask for this private address.

Trust group: Select as a trust group.

Generate VPN key:

After the configuration is completed, the system will automatically generate the key, we just need to wait 2-5min.

Download VPN key:



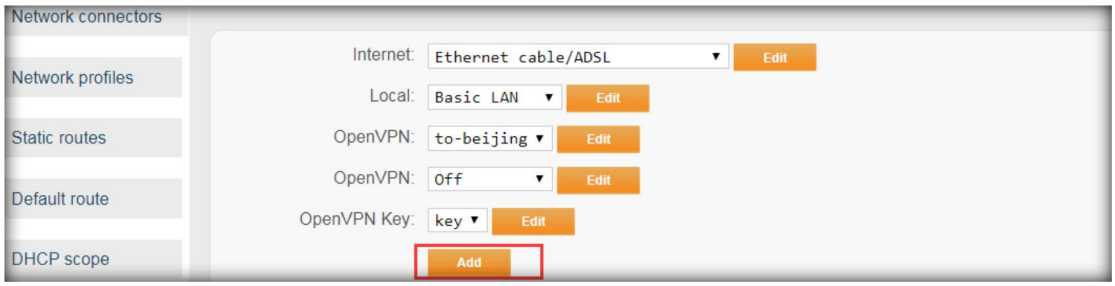
Click the OpenVPN key file to enter the key download interface. Users can download keys in .ovpn format or tar format according to their needs.

If you gave Jason a key a week ago for testing purposes only, and now you want to disqualify Jason, you can revoke this key. After the abolition,Jason's key will no longer take effect, but the system will generate a new key for you, you can download the new key and continue to use it.

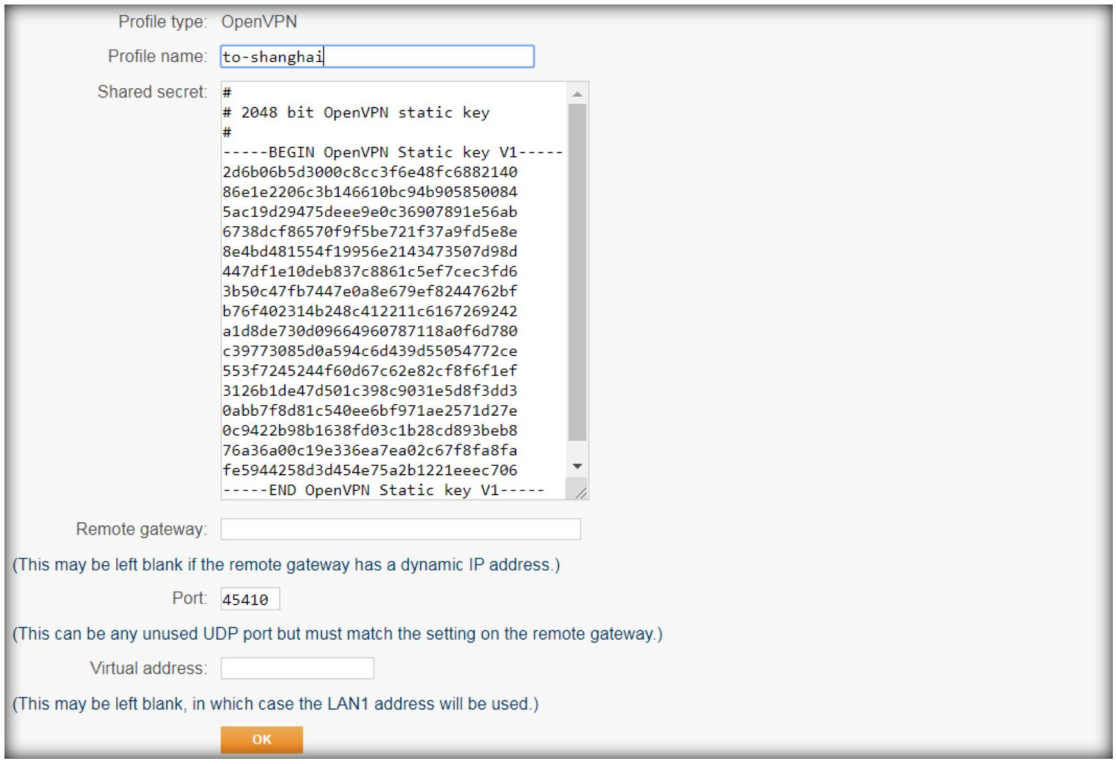
3.4. Network Connectors-VPN Tunnel

The use scenario of VPN tunnel is VPN networking, that is, when an enterprise has multiple branches, it can establish the VPN tunnel to make the network of each branch office interoperable, so as to achieve collaborative office functions such as extension dialing.

On the main interface of the network connector, click Add.



Select OpenVPN and click OK to enter the VPN tunnel configuration interface.



Profile name: Custom. For example, to-shanghai can indicate with whom to establish a VPN tunnel.

Shared secret: automatically generated by the system. The key of the remote justINA device must be consistent with this, that is, the justINA at both ends must have the same shared key.

Remote gateway: The public IP address or domain name of the remote justINA device. If the network where the remote justINA is located is a NAT network, that is, there is no public IP address or domain name, you can leave it blank here.

Port: Automatically generated by the system. The port of the remote justINA

device must be consistent with this, that is, the justINA at both ends must have the same port.

Virtual address: Generally left blank here.

The configuration of virtual addresses generally occurs when three or more JustINAs are in a VPN network, and two of them have IP address conflicts.

For example, there are IP segments 192.168.1.0/24 in both places. To prevent networking problems caused by IP address conflicts, we need to configure virtual IP addresses to distinguish these two places. After the virtual IP address is configured, the two justINAs can only communicate with each other by phone, but cannot communicate with the network.

Note:

In order to achieve full-network interworking in VPN networking (similar to the effect of IPsec networking), justINA must be a gateway.

Route addition:

After the configuration above is complete, you need to add a route to the other party.

Click Add to add a route. As shown in the figure below, the address here should be the network segment where the peer justINA is located. Only when the routes are written on both justINAs can the two justINAs communicate through the VPN tunnel.

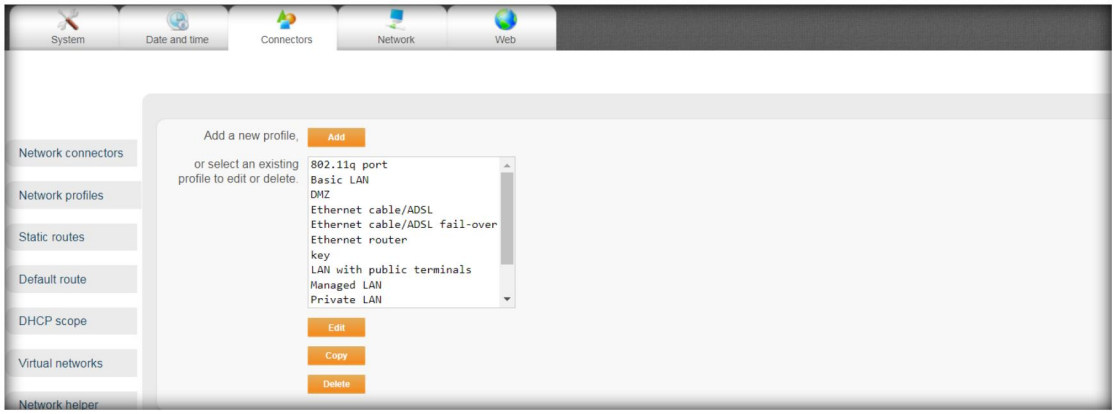
Note:

If you configure a virtual address when you configure the VPN file, you also need to configure a route to the justINA virtual address of the peer at this time. The realization of extension dialing at both ends of the VPN tunnel requires two justINAs for trunk connection, configuration and application of call rules.

3.5. Network profiles

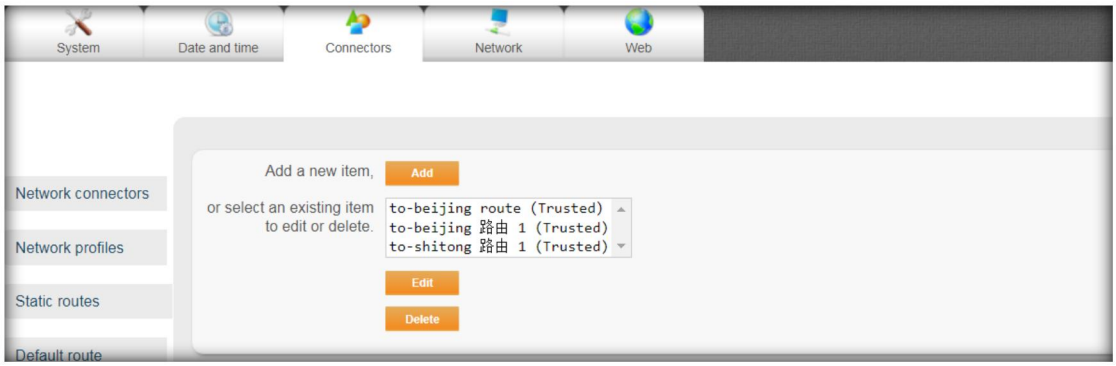
Mainly for all files related to network configuration, there is no need to configure here. The file here is a collation of all configurations in the network

connector. If you want to change a certain network segment, a certain route, etc., you only need to configure under the corresponding options in the network connectors.



3.6. Static routes

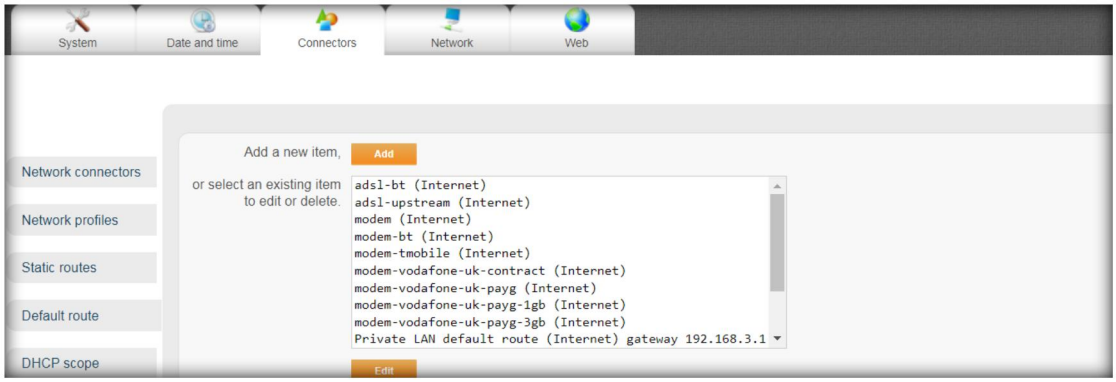
Mainly for all static routes configured on the network, there is no need to configure them here. The static route here is the classification of all routes in the network connector. If you want to change a certain route, you only need to configure it under the corresponding option in the network connectors.



3.7. Default route

Mainly for all default routes configured on the network, there is no need to

configure them here. The default route here is a classification of all default routes in the network connector. If you want to change a certain default route, you only need to configure it under the corresponding option in the network connectors.

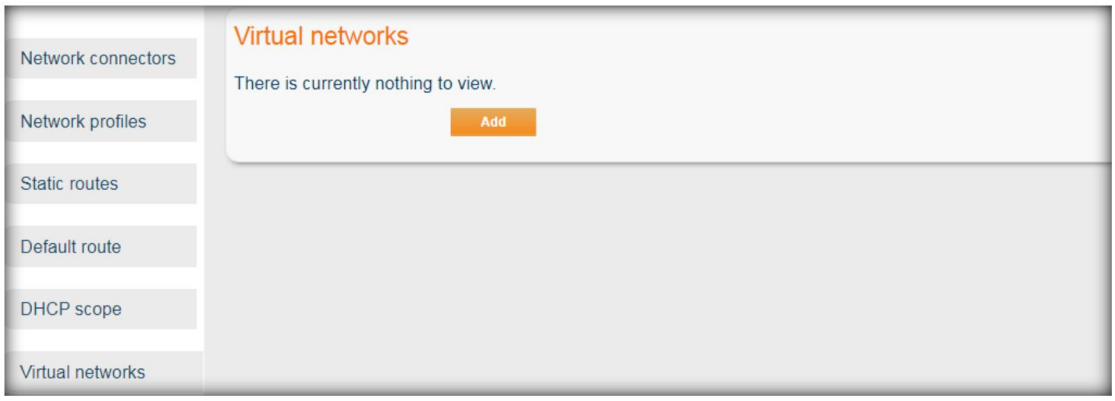


3.8. DHCP scope

For LAN port, wireless DHCP range. This is the default configuration and generally does not need to be modified by yourself.

3.9. Virtual Network

Mainly for the division of vlan, customers can configure accordingly according to their needs. Since vlans are divided according to ports, the number of vlans divided is relatively small and is rarely used.



3.10. Network helper

The network helper is a quick configuration entry for the latest configuration.

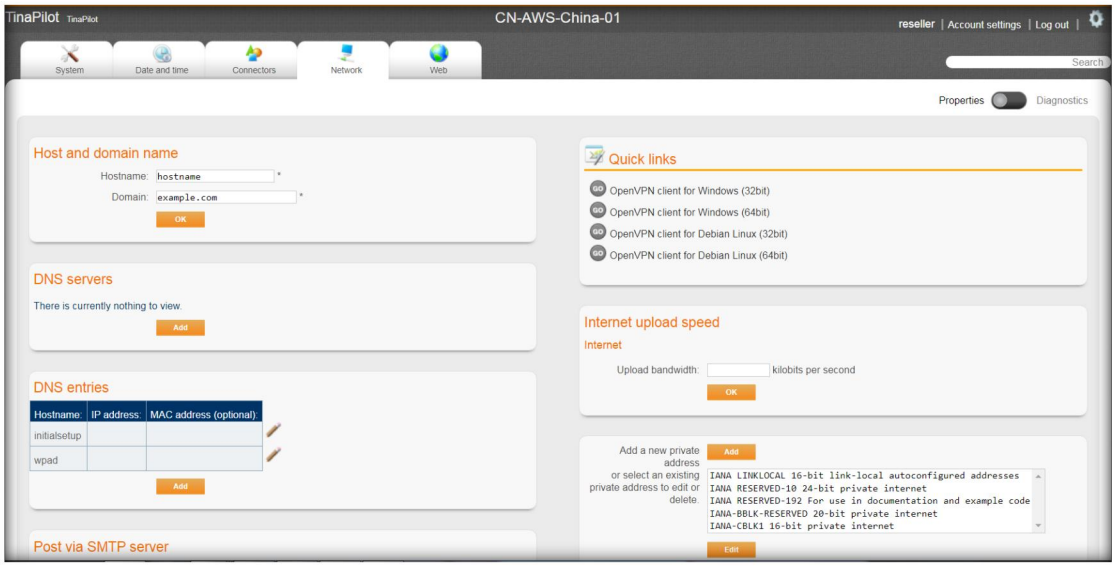
Click the network helper to enter the latest configuration interface.

3.11. OpenVPN Key File

List of all VPN keys, customers can download the corresponding keys here.

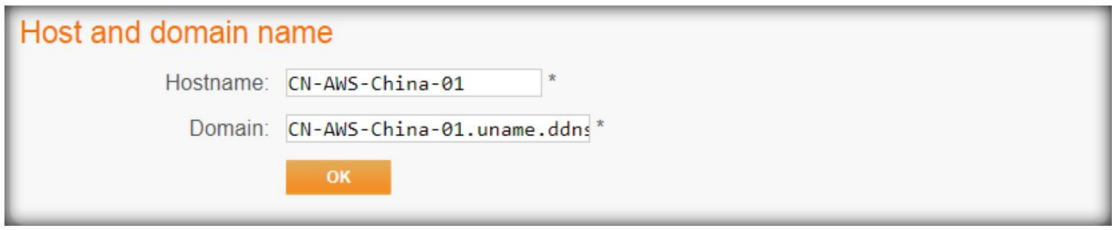
4. Network

The Network page is mainly for configuring network related information, such as DNS server, upload bandwidth, private address segment, mailbox server and other functions.



4.1. Host and domain name

Mainly add and edit the host name and domain name for some access to the intranet and extranet.



Hostname: The default is host name, here you need to modify the host name of the device such as CN-AWS-China-01, the hostname of the device is Home-> Registration.

Domain: The default is example.com. You can add a suffix after the host name based on the host name.

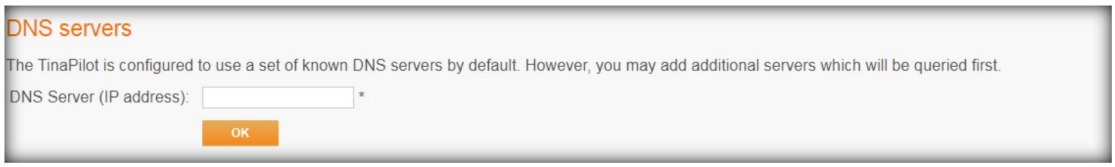
CN-AWS-China-01.uname.ddns.equiinet.com。

Note:

These two items can be left as default without modification. However, we usually modify it, because the modified domain name will be displayed on the cloud domain name server, which is helpful to distinguish each device and subsequent domain name access.

4.2. DNS Server

Click Add to enter the DNS configuration interface.



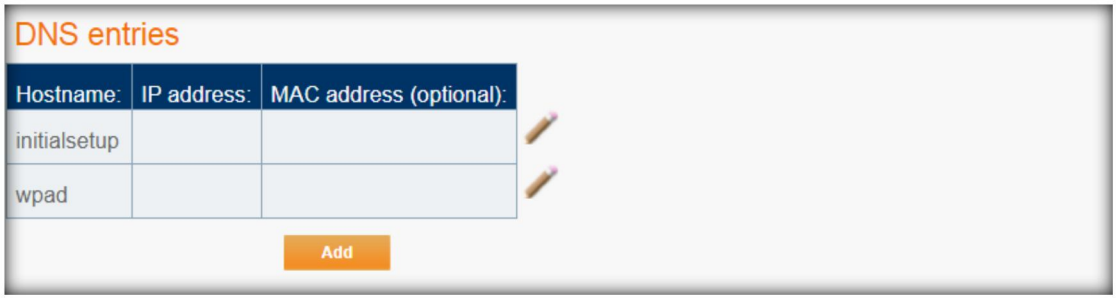
According to actual needs, fill in the corresponding DNS server address.

4.3. DNS entries

By default justINA can also be accessed through the DNS entry ,like initialsetup, and wpad.

When the IP address is empty, initialsetup, wpad represents justINA itself. At this time, you can use initialsetup, wpad to access justINA or map network cloud disk.

If the IP address of initialsetup is configured to the IP of other devices, you can access this device through initialsetup.



4.4. Post via SMTP Server

JustINA can use other mail servers to send its own information in the form of

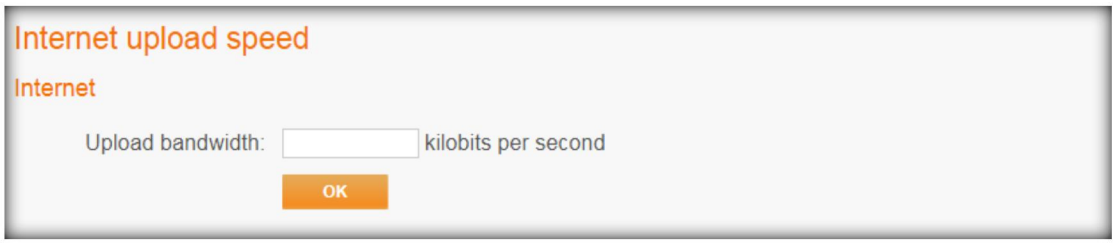
e-mail, such as 163, qq, 126, Sina, etc. You need to obtain user name and password authentication information from this server and fill in the following spaces.

4.5. Setting Internet Speed

The main purpose is to configure the upstream bandwidth for justINA. Only kb is supported here.

Note:

Only when justINA is used as a gateway, the role of this configuration here is to limit the upstream bandwidth.

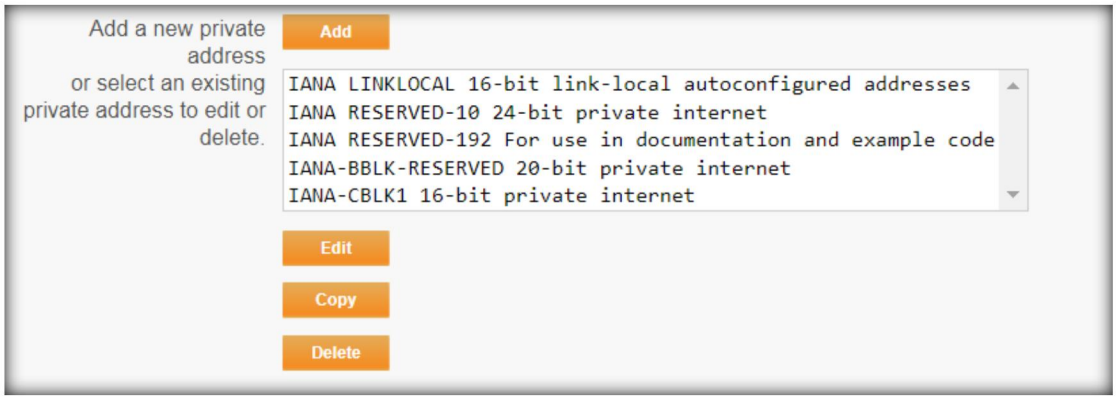


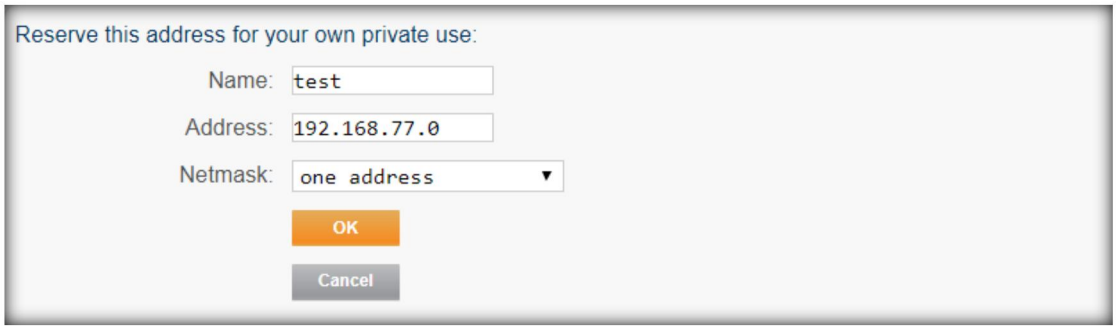
4.6. Adding a Private Address Segment

The purpose of adding a private address segment is to tell justINA that a segment of the address belongs to a private address.

The main application scenario is that if a customer sets a non-private IP address segment as his own intranet IP segment, such as 158.188.188.0 is an IP segment of the company's intranet, and if a public network server address is also in the 158.188.188.0 segment, Then the client cannot access this server on the intranet because the client computer will only search for this server within this network segment. At this point, we need to declare 158.168.188.0 as a private address.

Click Add to enter the add interface.





Name: You can name it by yourself, just make sense.

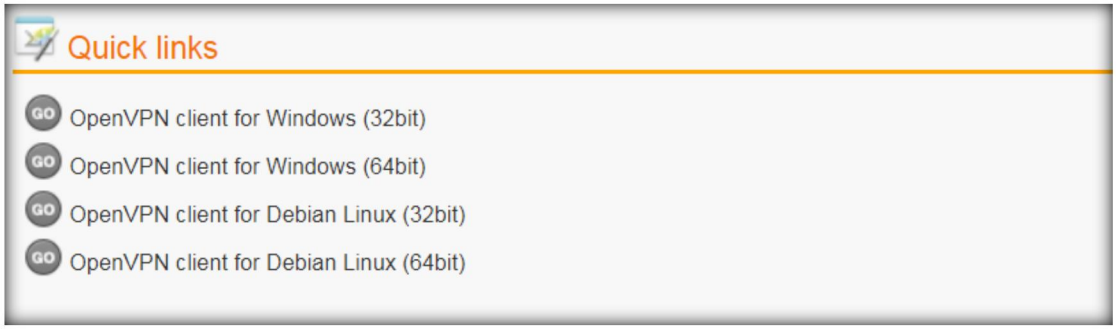
Address: The IP address segment you want to declare as justINA itself, such as

192.168.77.0

Netmask: The netmask of the IP address segment.

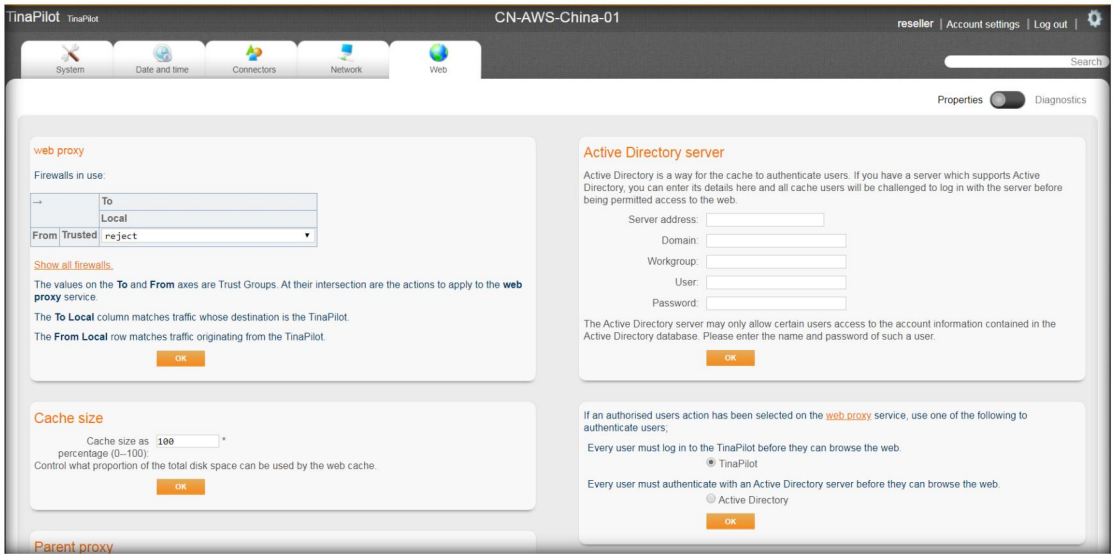
4.7. Quick Links

Mainly links to OpenVPN clients. When customers need to download the client to use the VPN key function, you can download the corresponding client here according to actual needs.



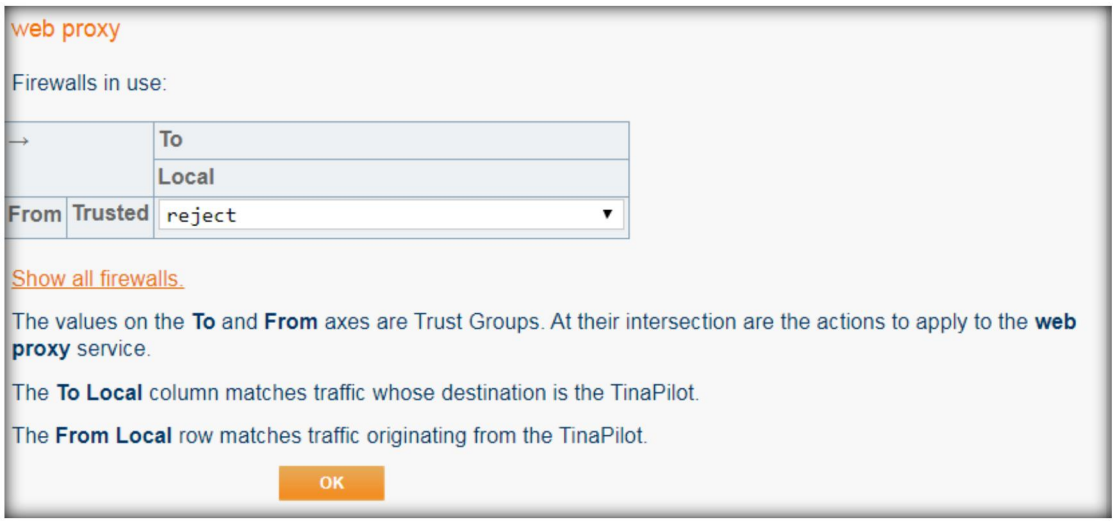
5. Web

The web page mainly introduces that when justINA is used as a gateway, some specific functions can be used in conjunction with related servers.

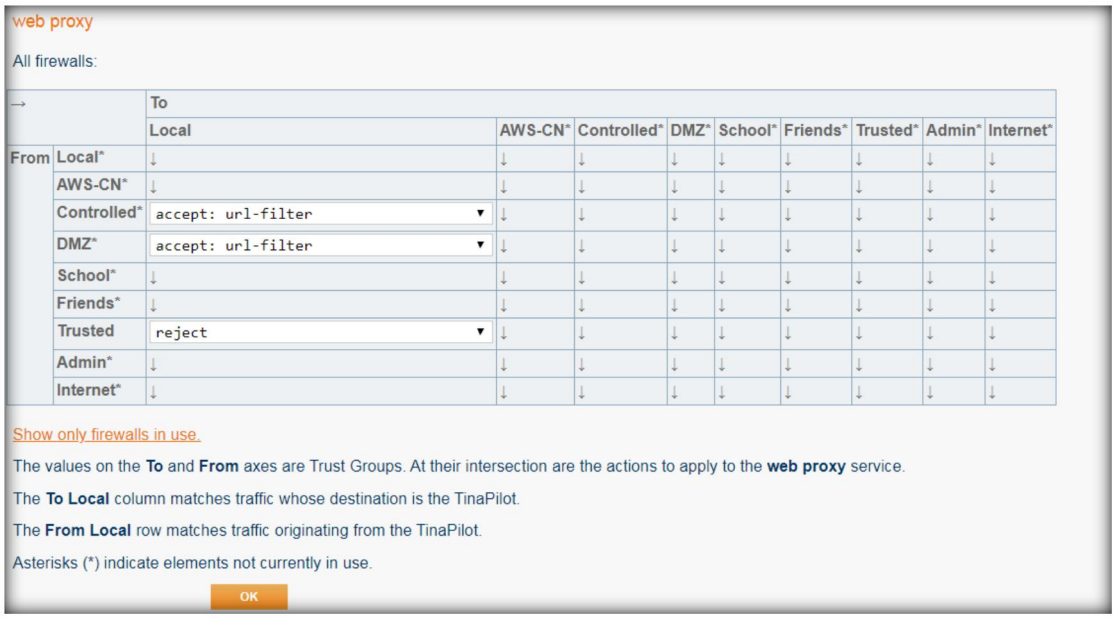


5.1. Web Proxy

When justINA is used as a gateway, it can be used as a web proxy server to filter Internet access behavior.



After clicking "Show all firewalls", the interface is as follows: As can be seen from the figure, by default we can filter the Internet behavior from DMZ / Local, Control Group / Local, Trust Group / Local.

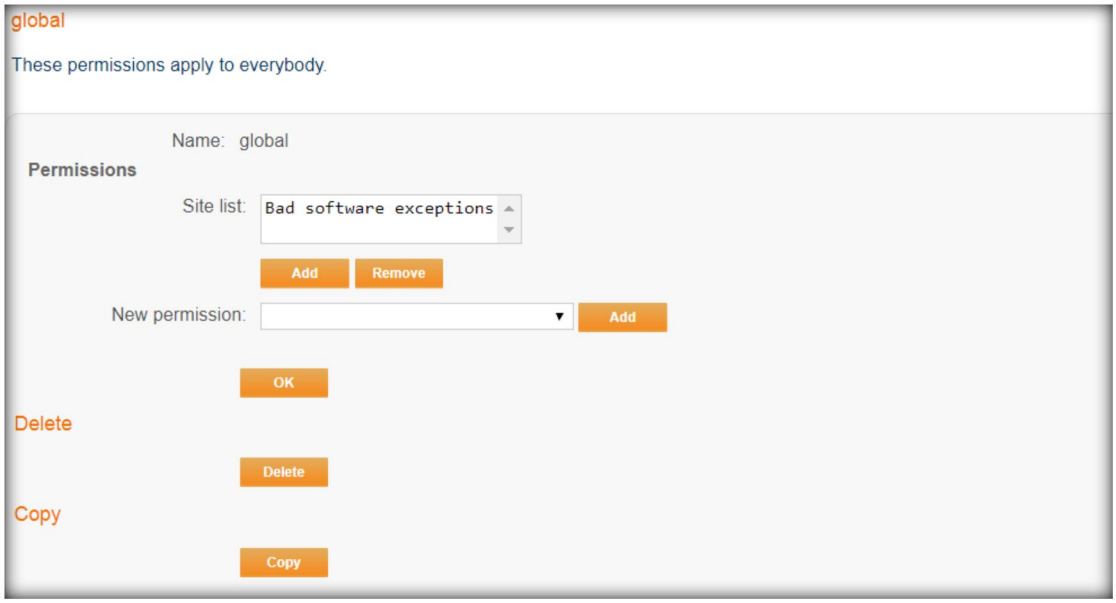


Filtering behavior configuration:

(1) Configure filtering rules

Admin->User->Select user group

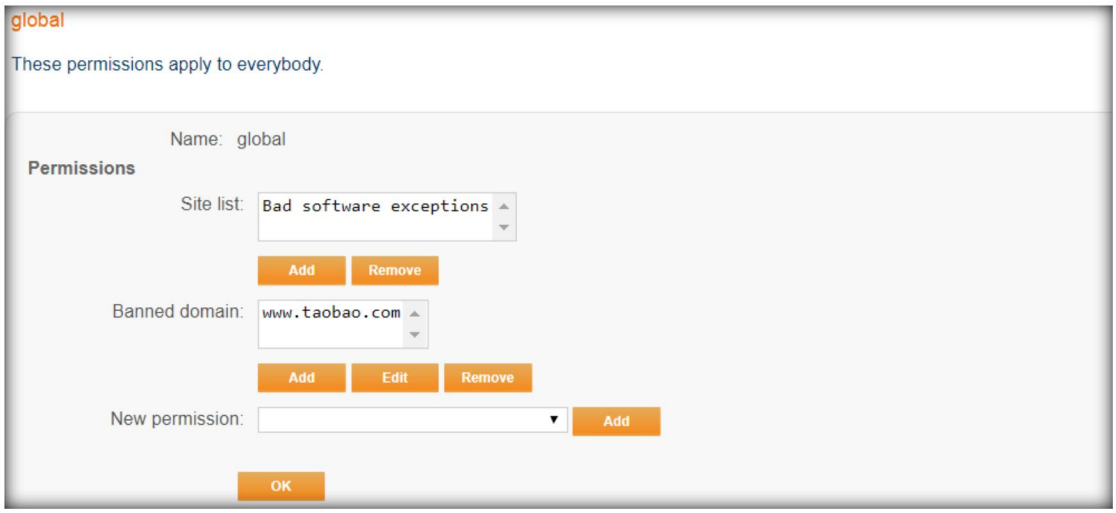
select global and click OK to enter the configuration interface.



New permission: choose Banned domain and click Add, it will automatically jump into the interface of adding Banded domain.

If you want to prevent internal employees from visiting Taobao, we can fill in www.taobao.com here and click OK to save.

After saving, we can see the Bannerd domain displayed in the interface, and we can add other websites such as www.vip.com. Finally click OK for the final save.



(2) Applying filtering rules

Enter the web proxy interface or the firewall and select URL filtering for the web proxy service.

(3) Implement web filtering

To truly implement web filtering, we also need to configure the PC. Ensure that the PCs in the company use justINA as the proxy server. If the proxy server is not justINA, the Internet behavior cannot be controlled.

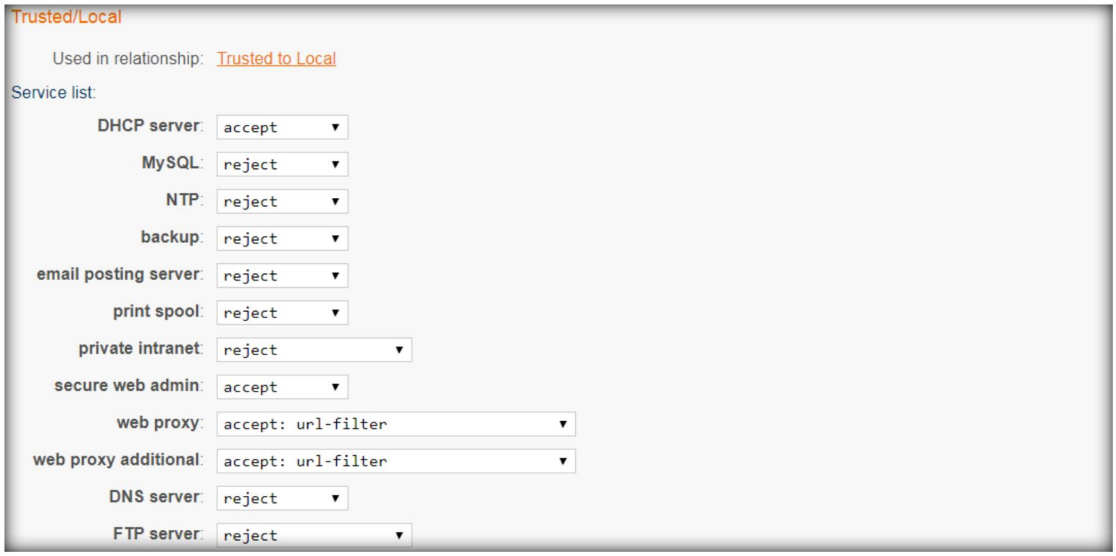
Change proxy server to justINA in PC browser settings

Web proxy additional:

Since some websites have port 8080 attributes, we can also add a web proxy option to allow websites with port 8080 attributes to have certain filtering attributes (can be url-filter or cache only, etc.).

In the System -> Web interface ,Scroll down and find "Additional Listening Port" to add port 8080.

There is an additional web proxy service on the firewall corresponding service. The original web proxy service status of this service is equal, it is only a supplement to the web proxy service.

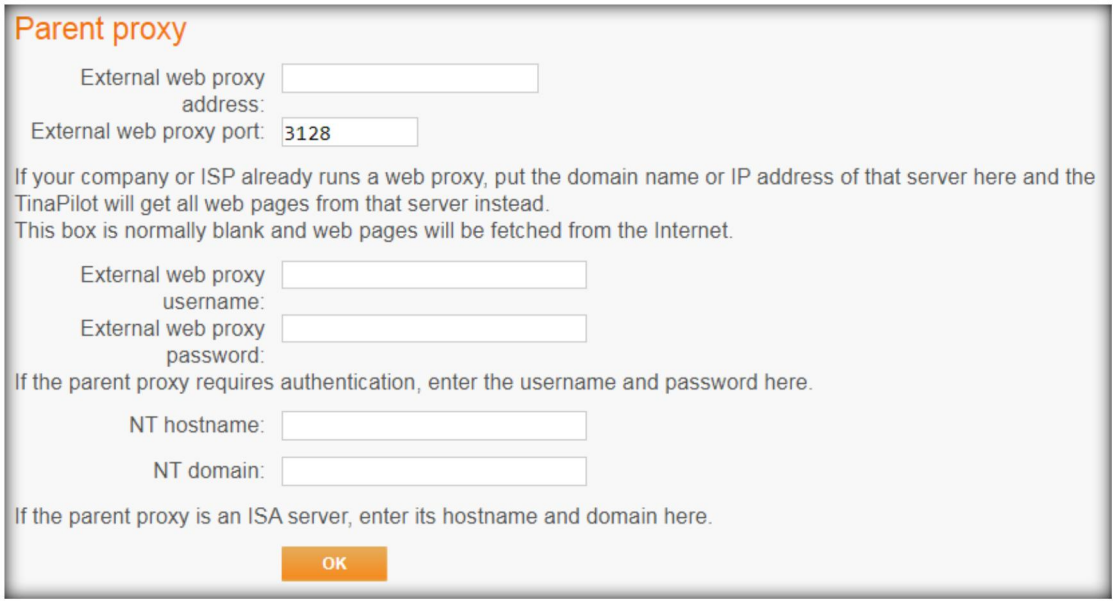


5.2. Cache size

When justINA acts as a gateway, it can be web cached. When justINA is really used as a gateway, it is recommended to configure the cache size here to 80%.

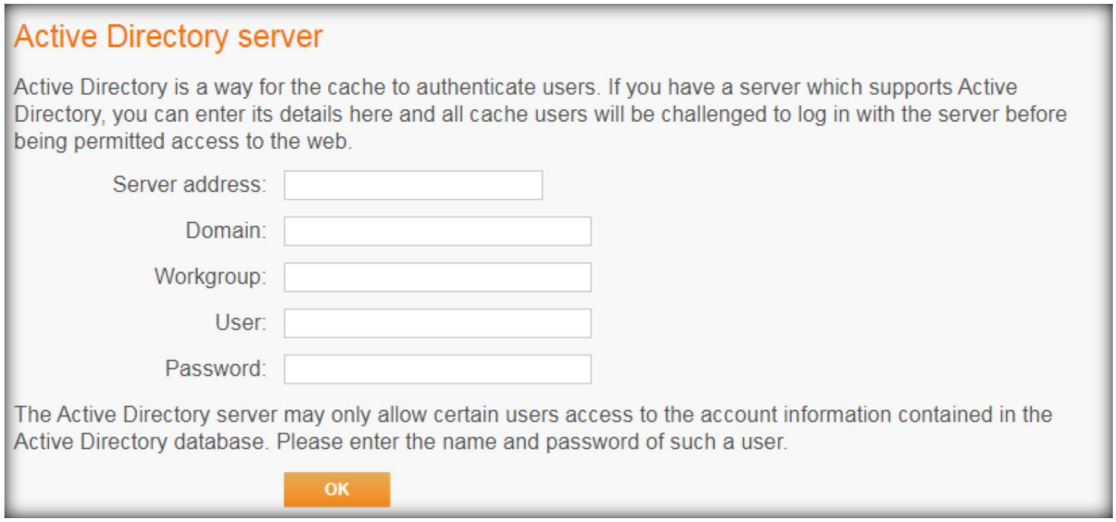
5.3. Parent proxy

Since justINA is rarely used as a gateway or as a parent proxy, it will not be explained here.



5.4. Active Directory Server

Since the customer's network has its own AD server, and justINA is rarely used as a gateway, the AD server will not be explained here.



5.5. Clear cache

When justINA is used as a gateway, the web-side cache is too full, which will affect the speed of accessing the network, so you can clear the cache here.

Chapter 4 Advanced Options

Top right gear button-> Advanced options

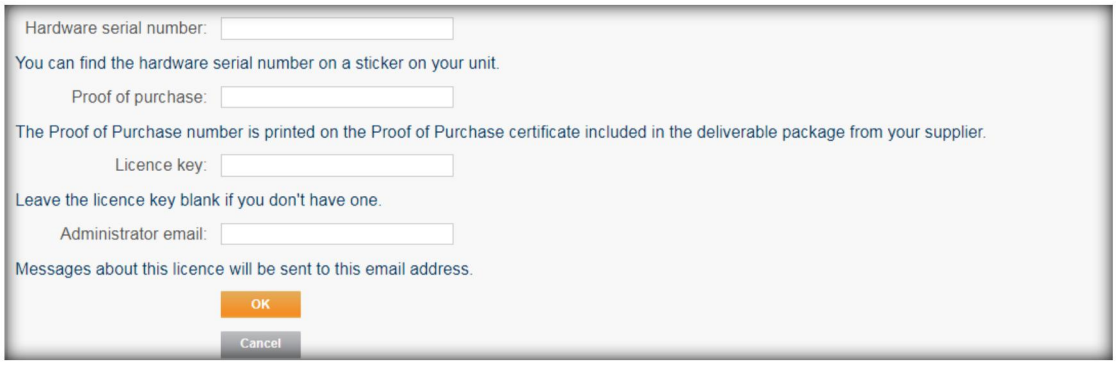
1. User accounts

The functions of Batch edit, Save CSV user list, and Load CSV user list are no longer used. We can add users in batches through the batch add tool.

2. Licences

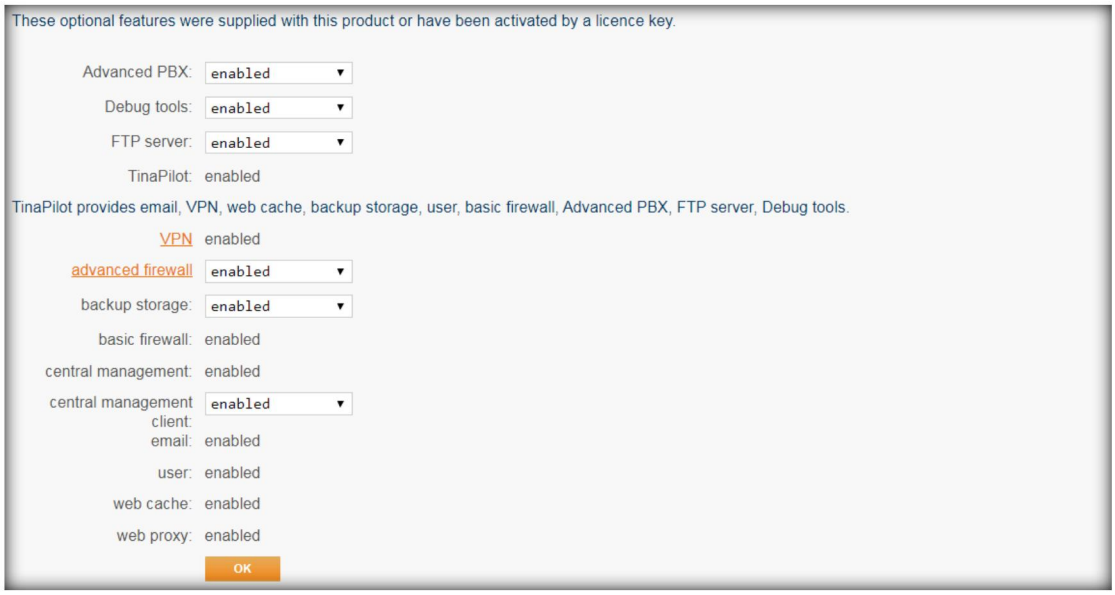
2.1. Add or delete

After clicking Add, you can see the following interface. No configuration is required here. The devices sent to customers by default are already authorized.



2.2. Enable

It is activated by default, and the customer does not need to do any configuration.

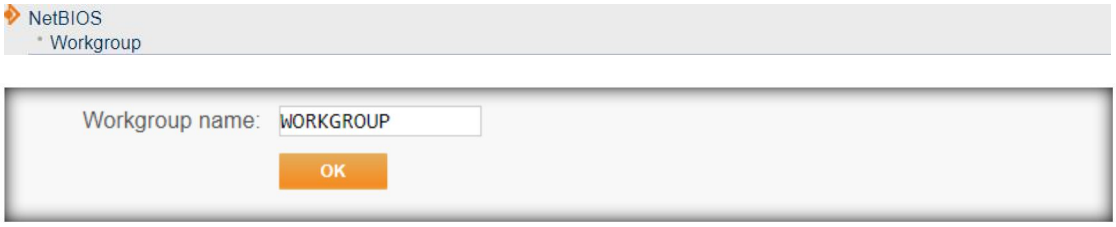


3. LVM

It is mainly used to modify the size of the logical disk. Customers are not recommended to change it by themselves.

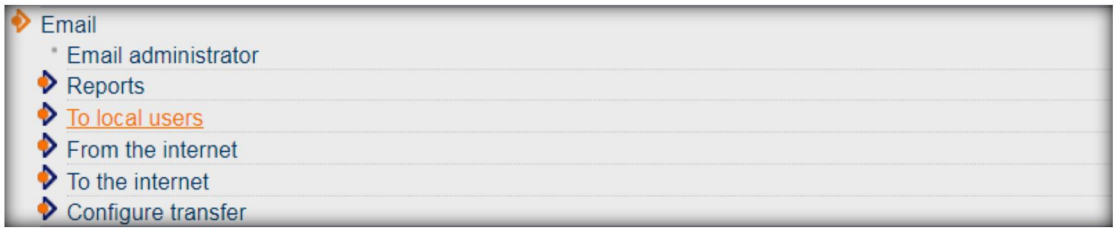
4. NETBIOS

The default workgroup is WORKGROUP, and no configuration is required by default.



5. Email

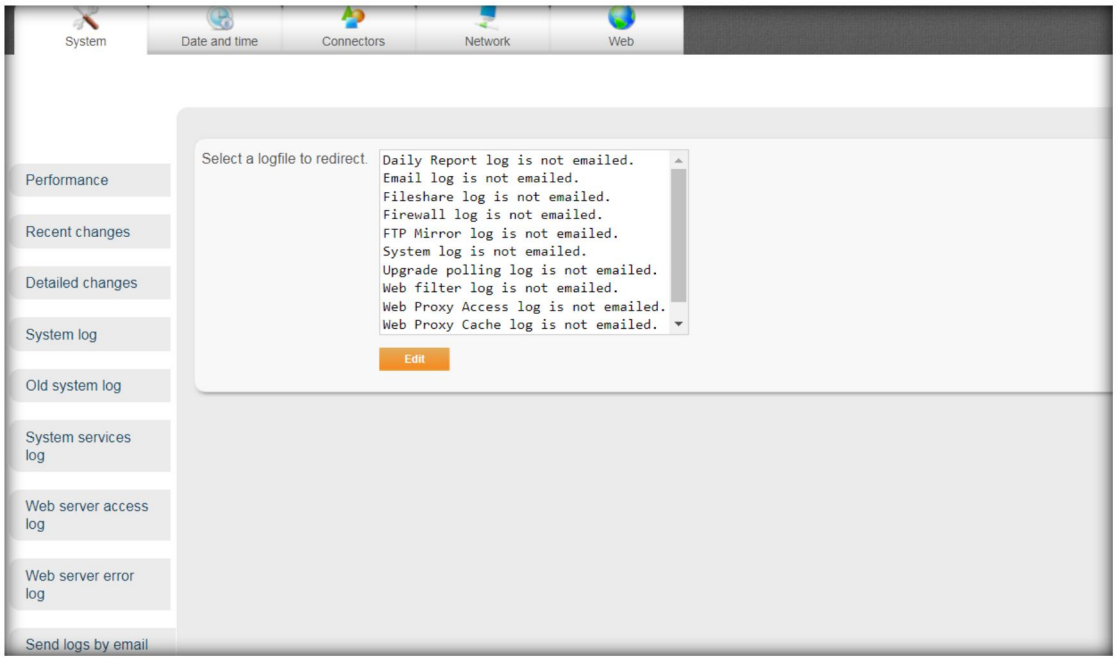
This function has been replaced by other functions and is no longer used here.



If the customer needs justINA to send some log reports to the mailbox, it can be configured elsewhere.

Such as the diagnostics interface :

System -> Send logs by email. Customers can send the corresponding logs to the corresponding mailboxes according to their actual needs.



6. Store Information

For disk storage configuration and other information, customers are not recommended to modify it.

7. Admin

All permissions are configured by default and customers do not need to modify them.

8. PBX

It is mainly the configuration of PBX related functions.

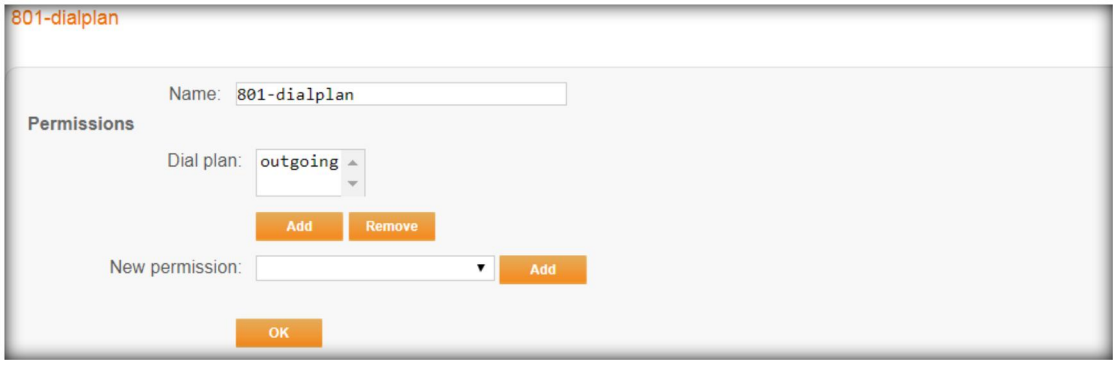
8.1. Dial plans

All dial plan of the system are in this place. You can control the dial plan of an extension number, as well as the dial plan of one direction.

Let ' s take the most common extension number as an example.

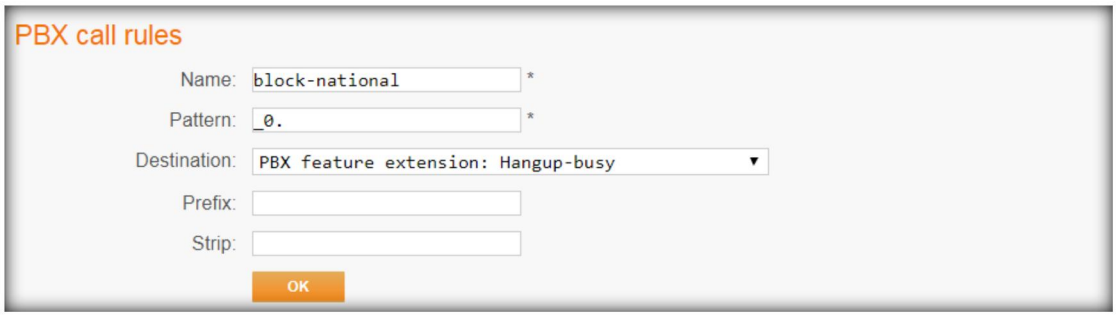
(1) Do not allow extension numbers to have a call function

Click 801-dialplan to enter the configuration interface, and then remove outgoing, then this extension number will not have the outbound call function.

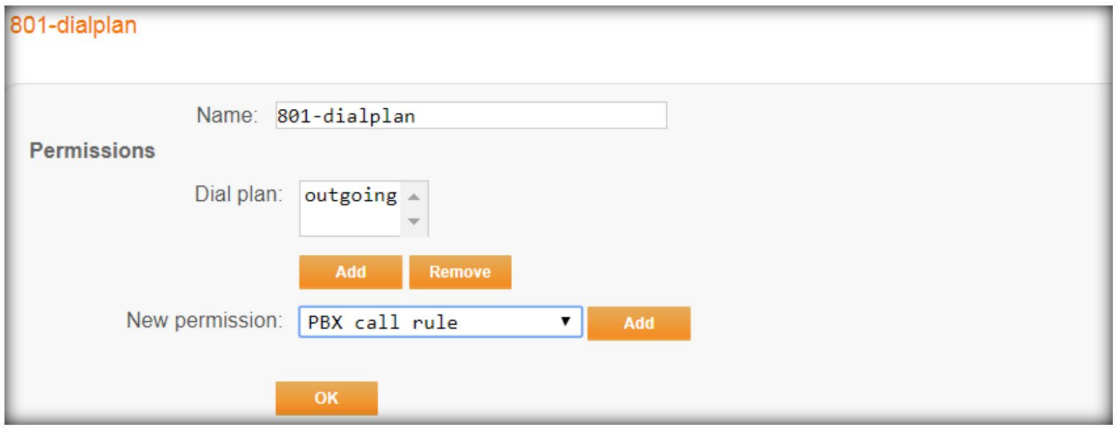


(2) Do not allow extensions to make long distance calls

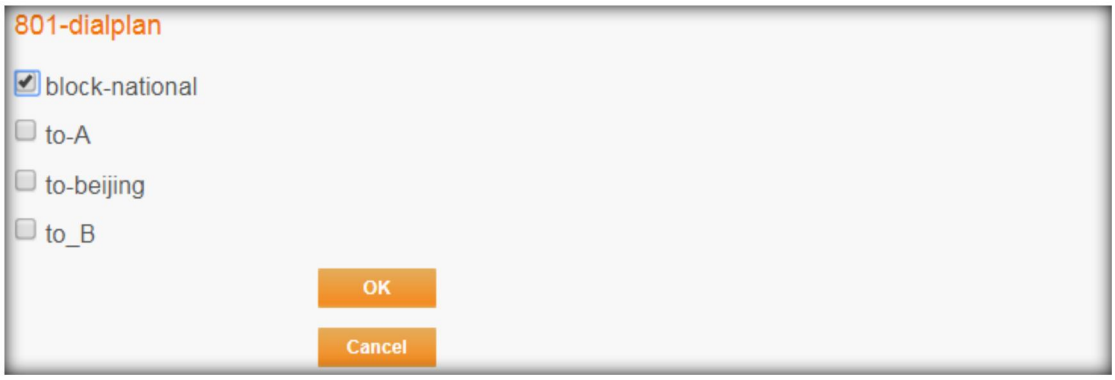
The prerequisite is to create a call rule, as shown in the figure below. Anything that starts with 0 is hung up.



Enter the dial plan interface of 801 and add a new permission PBX call rule.



Then enter the call rule selection interface. Note that you need to check the call rule here.

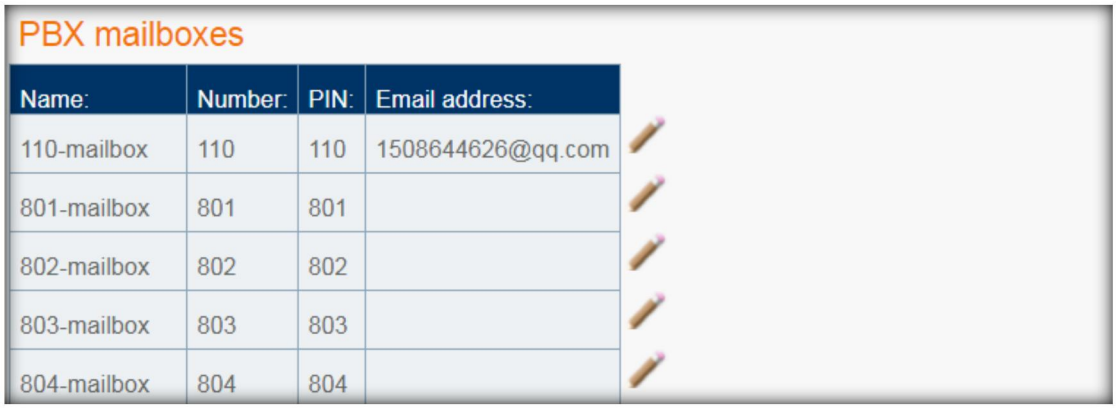


After the block-national option is selected, extension 801 cannot call foreign numbers.

In this regard, the configuration of the incoming and outgoing outgoing calls is substantially the same as that described above.

8.2. Email

It is mainly to forward the voice message to the mailbox. We have already explained when we explained the mailbox. For details, see Chapter 2->2.5, User voicemail.

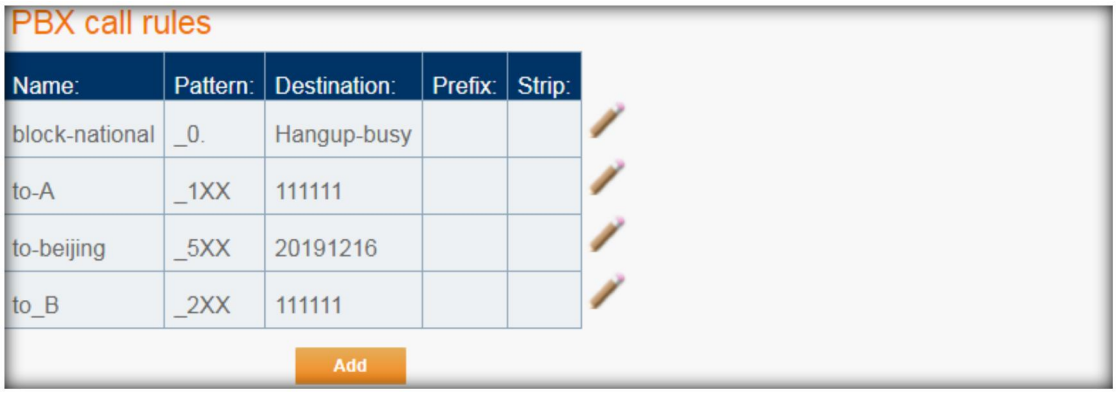


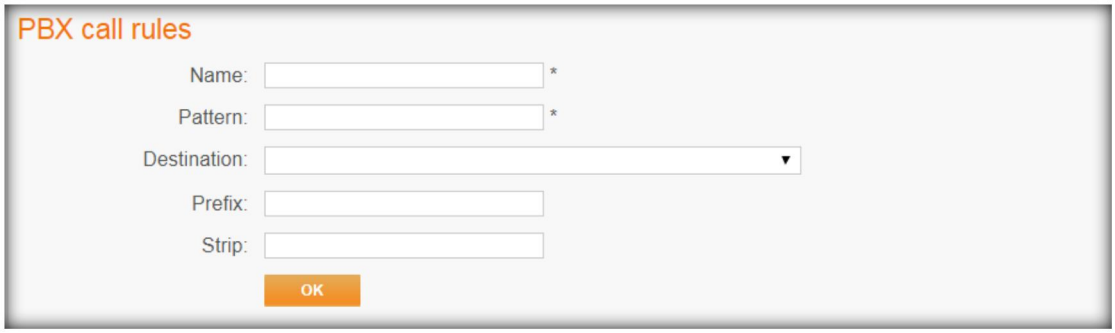
8.3. SIP Phones

It is used to add the SIP extension number, but it doesn’ t work well, so it is not recommended to add SIP users here. If we create one user, it will generate the SIP information here automatically.

8.4. Call rules

Mainly the rules formulated for outbound calls. Click Add to enter the call rule configuration interface.





Name: Customers can name it by themselves.

Pattern: "_" is the starting symbol of the rule. "X" represents any digit, and "." Represents any N digit.

So _00. Represents any number starting with 00

Destination: Any number that matches this format will be sent to this destination. This destination can be a real line, extension, or music, rejection, and other actions.

Prefix: You can add prefix N digits such as 123 before the dialed number.

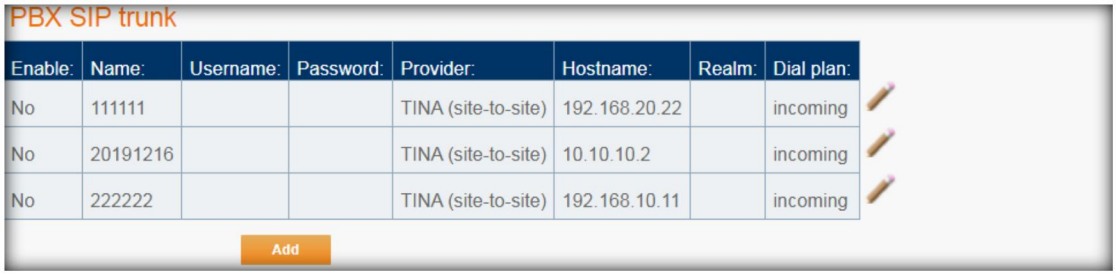
Strip: You can delete the N number from the left of the dialed number. For example, if you dial the number 13056567899 and delete 2 digits from the left, the last number sent is 056567899.

8.5. Trunks

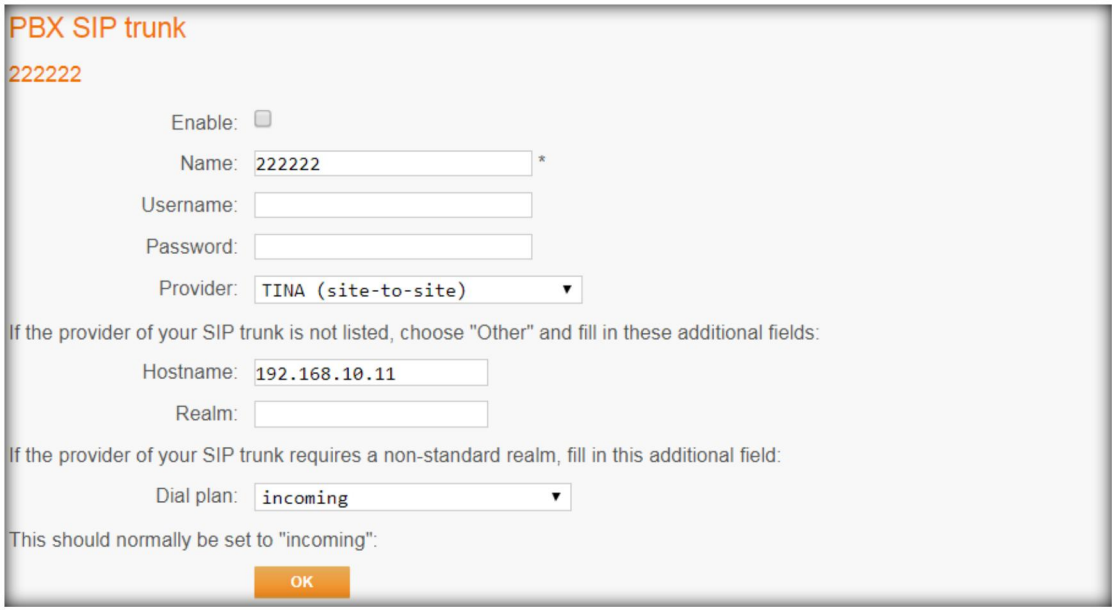
Mainly the configuration of the trunk

(1) SIP

Background information for all line information. Line information, we have already said in the Home-> DDIs and Trunks.



Enable:	Name:	Username:	Password:	Provider:	Hostname:	Realm:	Dial plan:
No	111111			TINA (site-to-site)	192.168.20.22		incoming
No	20191216			TINA (site-to-site)	10.10.10.2		incoming
No	222222			TINA (site-to-site)	192.168.10.11		incoming



Home-->DDIs and Trunks configuration is consistent with the configuration

The main difference is the "Enable" function. Enable here to temporarily disable this line without deleting the line information. When you need to enable this line again next time, just turn on the enable function.

(2) Specific ringtones

It is mainly used to configure the ringtone of the IP phone in the background. In the Home-> DDIs and Trunks, we have already said.

PBX distinctive ring

Name:	Label:	URL:
hanlong-dr1	EQ-Phone ring 1 (Tinkerbell)	<http://127.0.0.1>\;info=dr1
hanlong-dr2	EQ-Phone ring 2 (Ascent)	<http://127.0.0.1>\;info=dr2
hanlong-dr3	EQ-Phone ring 3 (Trimble)	<http://127.0.0.1>\;info=dr3
hanlong-dr4	EQ-Phone ring 4 (Cantina)	<http://127.0.0.1>\;info=dr4
hanlong-dr5	EQ-Phone ring 5 (Pastoral)	<http://127.0.0.1>\;info=dr5
hanlong-dr6	EQ-Phone ring 6 (Granval)	<http://127.0.0.1>\;info=dr6
hanlong-dr7	EQ-Phone ring 7 (Carlsbad)	<http://127.0.0.1>\;info=dr7
hanlong-dr8	EQ-Phone ring 8 (Shire)	<http://127.0.0.1>\;info=dr8
hanlong-dr9	EQ-Phone ring 9 (long ring)	<http://127.0.0.1>\;info=dr9
bellcore-dr1	Ring 1 (1 long ring)	<http://127.0.0.1/Bellcore-dr1>
bellcore-dr2	Ring 2 (2 long rings)	<http://127.0.0.1/Bellcore-dr2>
bellcore-dr3	Ring 3 (short-long-long, or 1 low ring)	<http://127.0.0.1/Bellcore-dr3>
bellcore-dr4	Ring 4 (short-long-short, or 2 low rings)	<http://127.0.0.1/Bellcore-dr4>
bellcore-dr5	Ring 5 (1 short ring)	<http://127.0.0.1/Bellcore-dr5>

Add

(3) National number plan

The PBX national number plan here are described in Admin-> Phones-> Global number plan.

PBX national number plan

Name:	International prefix:	Country code:	National prefix:	National pattern:	Full national pattern:	Emergency 1:	Emergency 2:	Emergency 3:
Australia	0011	61	0	ZXXXXXXX	none	000	112	none
China	00	86	0	ZXXXXXXXX.	none	11X	12X	1XXXXXXXXXX
none		none	none	none	none	none	none	none
North America	011	1	1	ZXXXXXXXXX	ZXXXXXXXXX	911	none	none
Philippines	00	63	0	ZXXXXX.	none	117	112	911
United Kingdom	00	44	0	ZXXXXX.	none	999	112	101

Add

(4) Local number plan

The local number plan here are the same with PBX national number plan.

PBX local number plan

Name:	National number plan:	Local code:	Local pattern:
Australia	Australia		
Beijing	China	10	ZXXXXXXX
Brisbane	Australia	7	NXXXXXXX
China	China		
Las Vegas	North America	702	XXXXXXX
London	United Kingdom	20	NXXXXXXX
Metro Manila	Philippines	2	NXXXXXX
none	none	none	none
North America	North America	none	none
North America - 10 digit dialling	North America		ZXXXXXXXXX
Philippines	Philippines		
Slough	United Kingdom	1753	NXXXXX
Swindon	United Kingdom	1793	NXXXXX
United Kingdom	United Kingdom		

Add

(5) Telcos

It is mainly used for PRI docking with operators. The use and adjustment of the parameters depend on the actual line.

Digital telco providers

Name:	Line build out:	Framing:	Coding:	Switch type:	Dial plan:
BT	0 dB (CSU) / 0 - 133 feet (DSX-1)	CCS (E1 or BRI)	HDB3 with CRC4 (E1)	EuroISDN	Dynamic
LV	0 dB (CSU) / 0 - 133 feet (DSX-1)	ESF (T1)	B8ZS (T1)	AT&T 4ESS	National

Add

(6) Analog

PBX analog line statistics.

(7) Digital

PBX digital line statistics.

8.6. Voice menu

Mainly related to the voice menu configuration.

(1) Language

It is mainly used to configure the language type of justINA background tone. Generally, the default background tone is English. For example, "The user you are calling is temporarily unavailable, please leave a message." However, Chinese customers generally need to listen to the Chinese prompt. At this time, we need to adjust the language to Mandarin (CN).

(2) Message

Mainly the voice messages in the voice menu, here we have already said in the Admin-> Phones-> Automated voice menu.

8.7. Groups

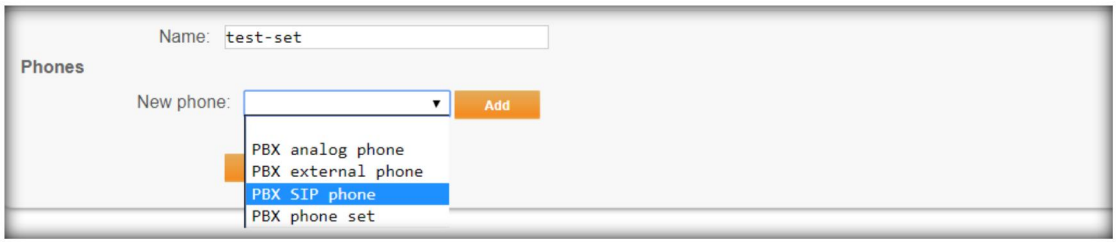
It contains four functions: Sequences, Sets, Page and Queues. Among them, Sequences, Page, and Queues are more commonly used PBX functions. These three functions can call Sets.

(1) Sets

The Sets is to form a group of SIP extensions, which is then called by the other three PBX functions. A single set has no meaning, it only has meaning after

being called.

Choose "Add new...."

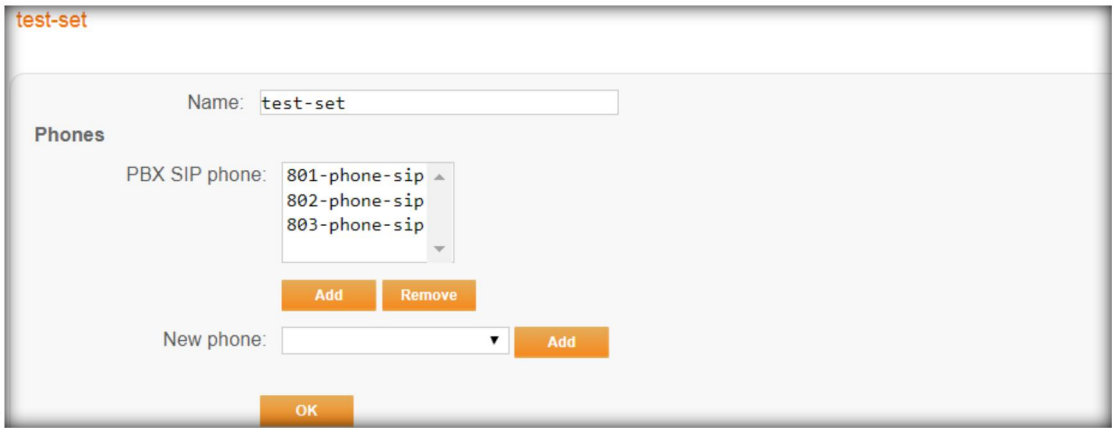


Name: Customer autonomous naming .

New phone: Select PBX SIP Phone.

Then click Add to enter the add interface. Select the appropriate extension and click OK.

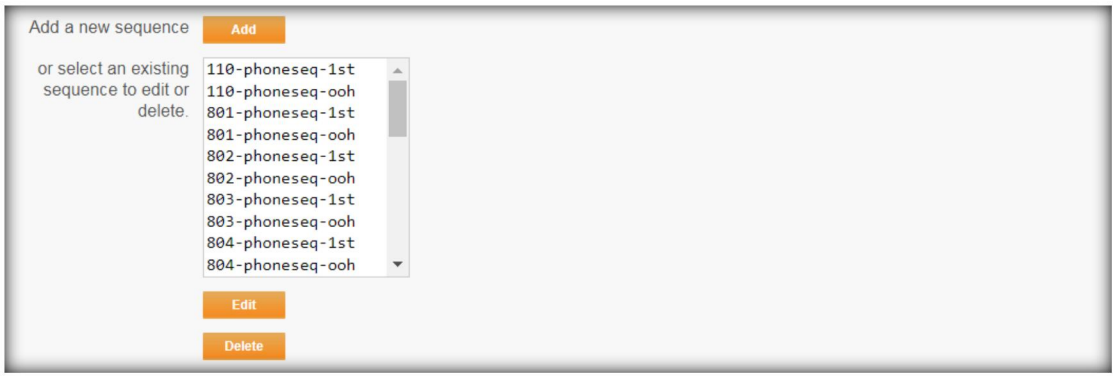
Then there are two SIP extensions in the test-set set. The test-set can be called by three other PBX functions.

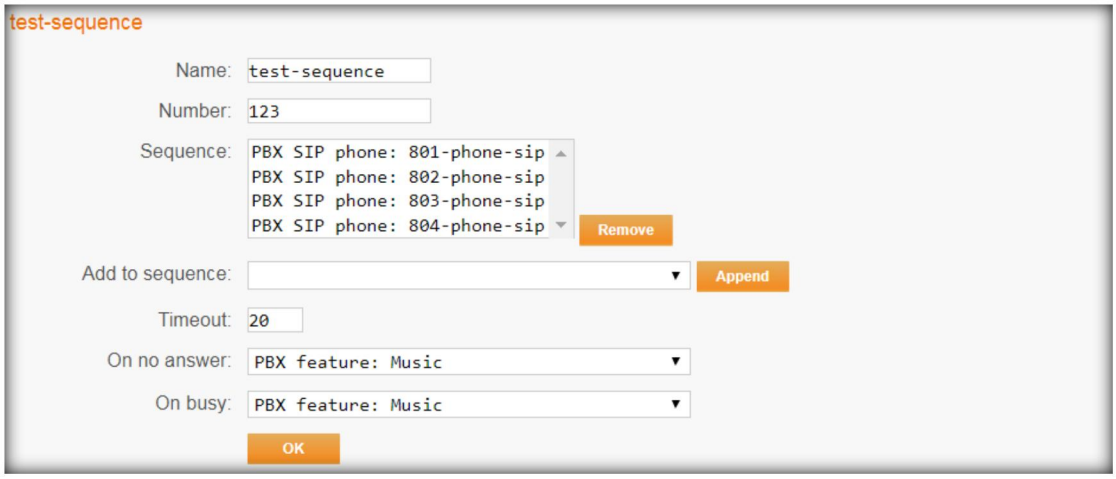


(2) Sequences

Sequences means that the extension numbers ring in a certain order. For example, after the sequence function is triggered, extension 1 in the sequence rings first, if no one answers after 20s, then extension 2 rings; if no one answers after 20s, extension 3 rings;

Click Add to enter the sequence configuration interface.





Name: Customer autonomous naming.

Number: user-defined, make sure that the number here does not conflict with the number in other places.

Sequence: Add extensions here, and the extensions appears in the order you added them.

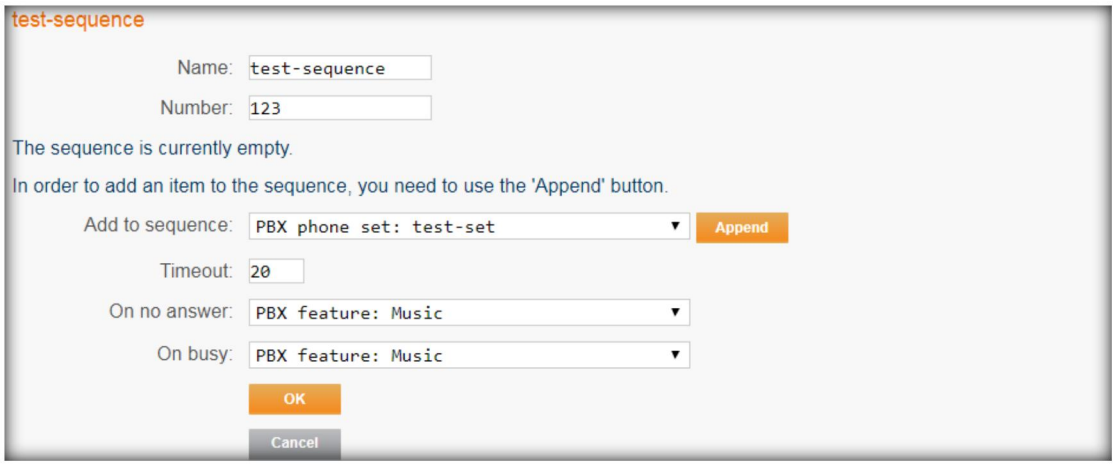
Add to sequence: Select the PBX SIP phone you need and click Append, then this PBX SIP phone will be added to the sequence.

Timeout: The default is 20, that is, 20s. It means that when the sequence is triggered, the first extension rings and the second extension does not answer the phone after 20 seconds.

On no answer: When all extensions do not answer the call, you can specify the call to a certain destination, such as music.

ON busy: When the line is busy, you can specify the call to a certain destination, such as music.

In addition, sequences can call sets, as shown in the following figure:



For example, if the PBX extension sequence selects the sets like test-set, and clicks Append, the sequence can be successfully created. The effect of the call after joining the sequence is:

When this sequence is triggered, all the extensions in the test-set ring at the same time. If no one answers after 20 seconds, the call will be automatically transferred to music.

(3) Page

Page is similar to multicast. When the call function is triggered, all extensions in page automatically enter the call state.

Click Add to enter the configuration interface.

Name: Customer autonomous naming.

Number: The system automatically generates it. The customer can also edit it by himself. Note that it does not conflict with other numbers.

Type: Divided into one-way page and Two-way page.

The effect of the One-way page is that the caller can listen and speak, and the callee can only listen but not speak;

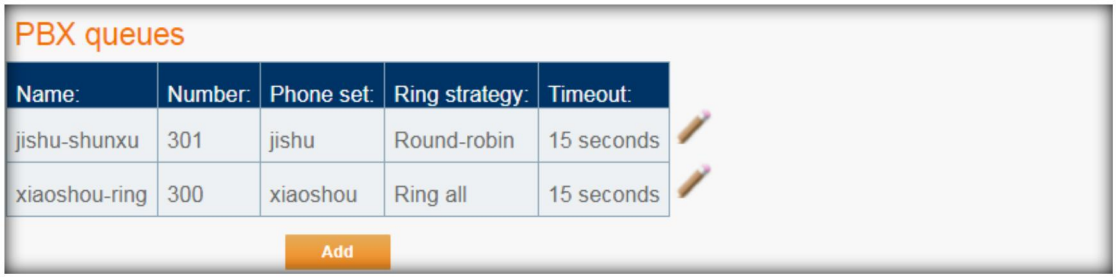
The effect of the Two-way page is that both the caller and the callee can listen or speak;

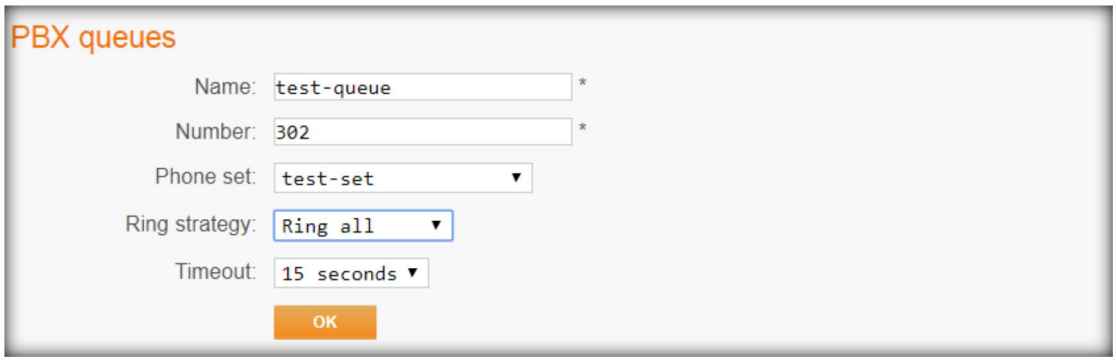
Phone set: Here the test-set must be called.

(4) Queues

A queue is a queue of all extensions. When the queue is triggered, all extensions in the queue ring. As long as the caller does not hang up, all extensions in the queue continue to ring and the caller will hear something like "You are in the queue now, please be patient."

Click Add to enter the configuration interface.





Name: Customer autonomous naming.

Number: Automatically assigned by the system.

Phone set: Select the set be created, such as test-set.

Ring stratery: it has Ring all, Fewest calls, Least recent,Ring all, Round-robin. We can choose is according to the requirement.

Timeout: The default is 20, that is, 20s. It means that when the sequence is triggered, the first extension rings and the second extension does not answer the phone after 20 seconds.

8.8. Analog

PBX analog number, no longer described here.

9. Web

It is mainly web filtering and other information. We have already mentioned it in System-> Web-> Web Proxy.

Chapter 5 About

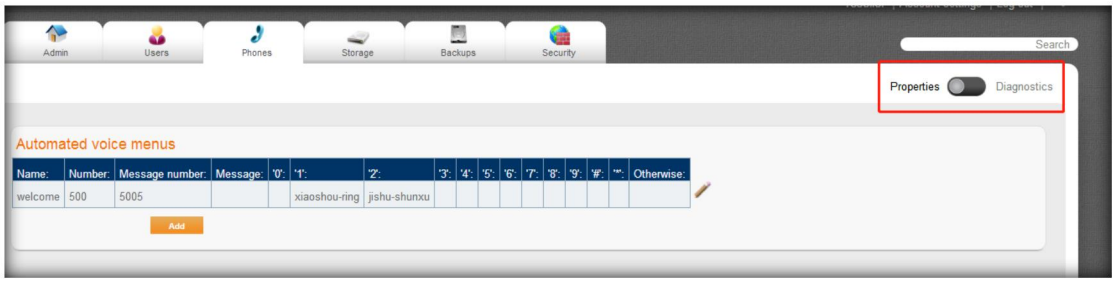
About the introduction of the system status, you can see the system hardware, network and other information.

Chapter 6 Diagnostic

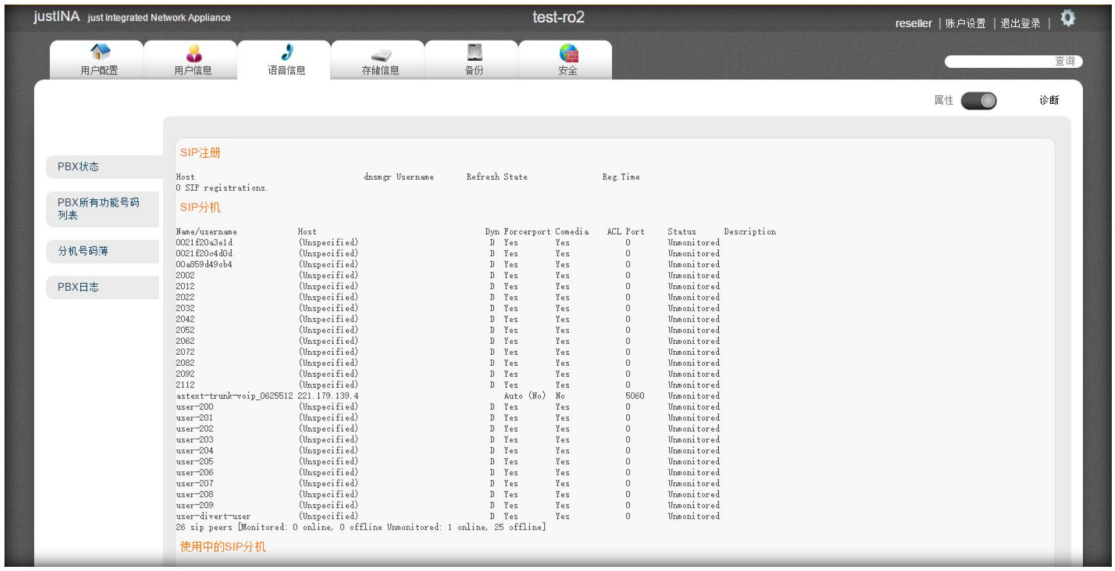
The characteristics of justINA compared to other products are: coexistence of

diagnostic interface and configuration interface, multiple diagnostic items, and easy to find.

For example, in the "Phones" interface, click the Properties-Diagnosis button,



after entering the diagnostic interface, you can see the PBX status, PBX all number list , Phone directory, and PBX log .



Note:

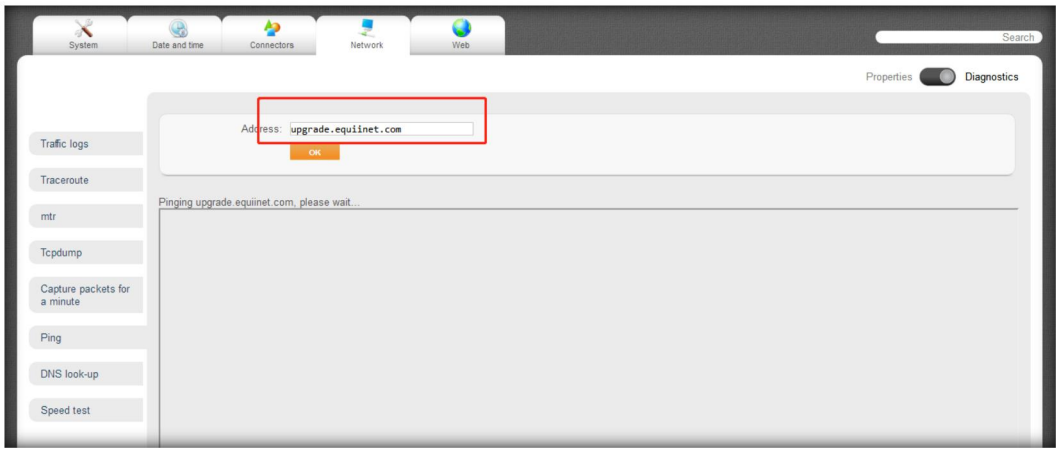
In each interface, anyone who has the property-diagnosis button,you can enter the diagnostic interface, and then view the diagnostic information of the corresponding configuration options in this interface.

justINA has a search bar (below the gear button in the upper right corner), and

users can search for corresponding functions by keywords.

For example, if you enter ping in the search bar in the upper right corner, the ping function will be searched. Click ping to enter the ping interface.

The user can fill in the corresponding address according to the actual situation.



For detailed diagnosis introduction, please see EQ_justINA diagnosis manual