UC8000 IPPBX User Manual

Date: Sept. 31st, 2022

Author: Jesse Dai

Shenzhen Dinstar Co., Ltd.

Address: Floor 18, Building 7A, Vanke Cloud City Phase 1, Xingke 1st Street, Xili Sub-district, Nanshan District, Shenzhen.

Postal Code: 518052

Telephone: +86 755 2645 6664

Fax: +86 755 2645 6659

Email: sales@dinstar.com

Website: www.dinstar.com

Preface

Welcome

Thanks for choosing the **UC8000 IPPBX**! We hope you will make full use of this rich-feature product. If you need any technical support you can contact us at +86 755 2645 6664.

About This Manual

This manual provides information about the introduction of the UC8000 IPPBX, and about how to install, configure or use the UC8000 IPPBX. Please read this document carefully before using the UC8000 IPPBX.

Audiences

This manual is aimed primarily for the following people:

- Users
- Engineers who install, configure, and maintain the UC8000 IPPBX

Revision Record

Document Name	Document Version	Software Version
UC8000 IPPBX User Manual	V1.0	2.58.2.0

Conventions

All references to the system in this document refer to the UC8000 IPPBX. **"Note"** marked in the document is what users need to pay attention to.

Contents

1 Product Introduction

1.1 Overview

UC8000 is a new generation of large capacity unified communication system. It supports 20,000 extensions and 4,000 concurrent calls which are integrated voice, video, paging, conference, recording and other communication functions.

The UC8000 is deployed as a software based IPPBX when loaded on an X86 Architecture. It runs in a docker and can be loaded on Linux or Centos.

1.2 Application Scenario

The application scenario of UC8000 is shown as follow:

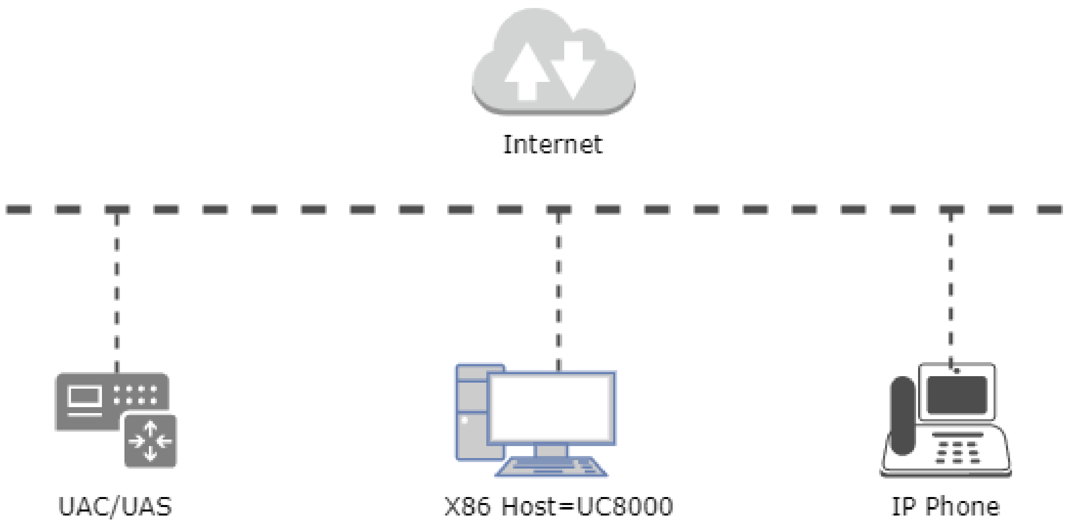


Figure 1.2 Application Scenario of UC8000

1.3 Product Form

Dinstar UC8000 is a software-based UC solution. It can be installed on any mainstream Linux based platform.

1.4 Features & Functions

1.4.1 Key Features

- Supports up to 20,000 extensions and 4,000 concurrent calls
- Support X86, ARM and Huawei KunPeng architecture, Docker, AWS, Google,

Alibaba and Microsoft cloud

- Provide very flexible call routing based on time profile and number prefix
- Supports Multi-level IVR, helps to build personalized voice navigation for enterprise
- Flexible dialing plans with routing policies based on time, number, source, IP, etc.
- Supports PBX services such as call forward, three-way conference, voice conference, broadcast, intercom, etc.
- Support voicemail/voice recording
- User-friendly web interface, classification of web user's permission
- Support HA solution（active and standby), active and standby switch to ensure stable operation of UC8000

1.4.2 Physical Specifications

- CPU Processor: 2 or more cores
- RAM: 2G or more
- Hard disk: 100G or more
- Ethernet interface: a 100/1000 Base-T RJ45 or more

1.4.3 Voice Capabilities

- SIP over UDP/TCP/TLS, RTP/SRTP
- SDP, RTP/RTCP, SSL
- Voice Codec：G.711a/u, G.723, G.729, G.722, G.726, Opus
- Video Codec: VP8, H261, H263, H264, H263-1998, H263-2000
- Voice Activity Detection (VAD)
- Comfort Noise Generator (CNG)
- Adaptive Dynamic Buffer
- Adjustable Gain Control
- FAX: T.38 and Pass-through
- NAT: STUN/DDNS
- DTMF: RFC2833/Signal/Inband

1.4.4 PBX Call Service

- Call Forward (Always/No Answer/Busy)
- Call Waiting

- Call Holding
- Call Transfer
- Do-not-disturb
- Three-Way Conference
- Ring Group
- Call Queue
- Route Group
- Caller/Called Number Manipulation
- Routing Based on Time Period
- Routing Based on Caller/Called Prefixes
- Dialing Rule
- Failover Routing
- Multi-level IVR
- Auto-attendant Function
- CDRs
- Voicemail
- Voice Recording
- Up to 20,000 SIP Extensions
- Up to 4,000 Concurrent Calls
- Paging Group
- Event Report
- Email Client
- Voicemail to Email
- Broadcast/Broadcast Group
- Intercom/Intercom Group
- Emergency Number
- Blacklist/Whitelist
- Feature Code
- SCA
- Follow Me
- Alarm Clock

1.4.5 Network Features

- Multi-service network port
- IPv4
- VALN, QoS, NAT and Fail2ban
- Double-device Hot Standby

1.4.6 Maintenance

- Web GUI Configuration
- Command line management configuration
- Configuration Restore/Backup
- Multi-language support
- HTTP/TFTP firmware upgrade
- Web password change
- Ping, Traceroute and Nslookup Test
- Network Capture
- Network Quality Test
- Call List query and export
- API interface support

2 Installation

2.1 Attentions before installing

- Users install the X86 host on their computer, then install a mainstream Linux or Centos system on the X86 host, and install the programs required for the UC8000, etc.
- To reduce the interference to telephone calls, please separate power cables from telephone lines;
- To guarantee stable running of the UC8000 IPPBX, please make sure that there is enough network bandwidth;
- The software license of UC8000 will be changed after reinstalling the docker.

2.2 Power on the System

- Plugging the host into a monitor, keyboard, mouse, etc.

- Connect the host computer's Ethernet port to the network.
- Refer to *UC8000 Installation Tutorial* to install the operating system and UC8000 tar file.

2.3 Network Connection

The UC8000 uses the IP address of the server's physical machine network interface, so the UC8000 does not require network configuration; when users need to use the active and standby functions, they can configure a floating IP address for active and standby management.

2.4 Connecting devices to the network

2.4.1 Preparations for Login

Connect the network interface of the host with UC8000 to Ethernet or LAN, and configure the accessible IP address in advance, e.g. 192.168.11.1.

- Take the Windows 7 operating system as an example, set the local computer to the same network segment address as the default IP of the system.

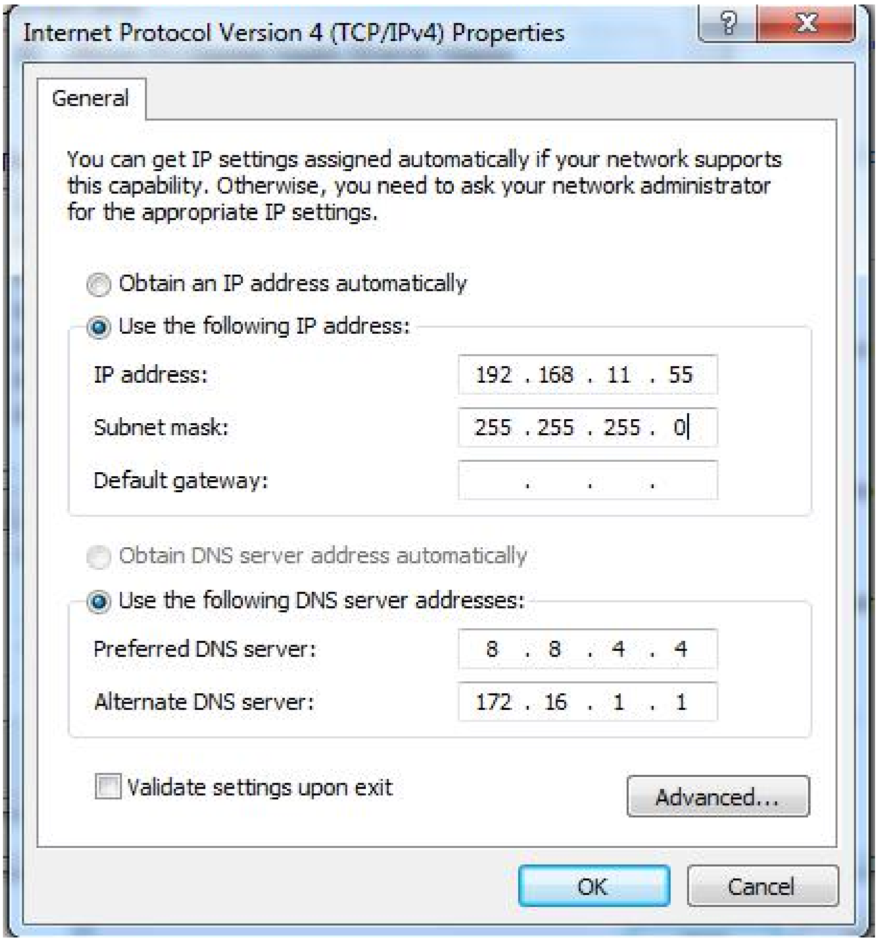


Figure 2.4.1 Modify the local computer address.

- Check the connectivity between the PC and the UC8000. Click **Start -> Run** of PC and enter **cmd** to execute ‘ping 192.168.11.1’ to check whether the IP address of the system is normal.

2.4.2 Log In Web

Enter the IP address of UC8000 in your browser, such as: "192.168.11.1", and press Login to enter the user login interface.

Figure 2.4.2-1 Login GUI of UC8000

Enter username and password (default is **admin/admin@123#**), and click **Login** to enter the web interface.

Note: The host name of the mainstream version of UC8000 is UC8000, and the host name of the neutral version of UC8000 is IPPBX.

For the security purpose, login of the web will be limited:

- If three consecutive login failures, users need to slide to validate their user account;
- If ten consecutive login failures, the IP address of the UC8000 will be blacklisted, and users need to reset a new IP address for the system;
- Successful login or system restart will wipe out login failure records.

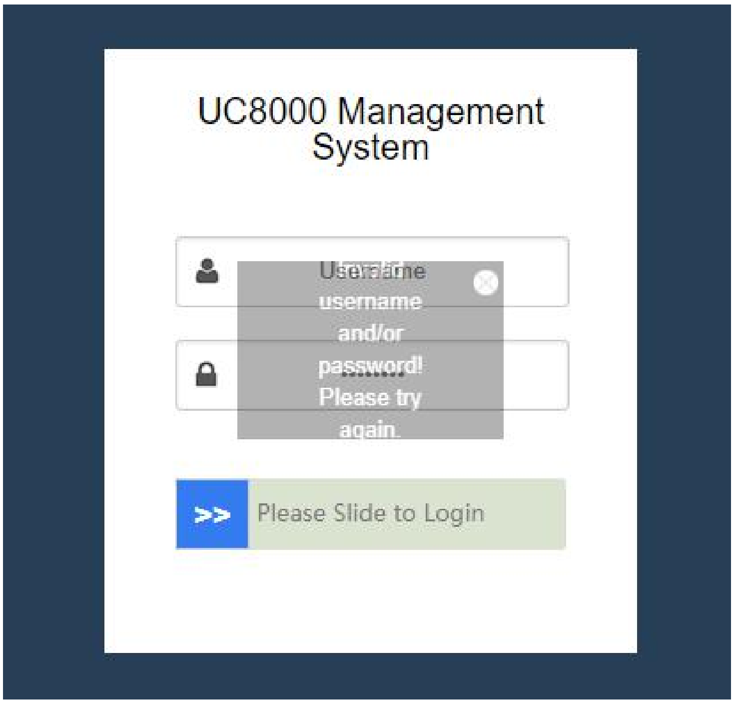


Figure 2.4.2-2 UC8000 sliding verification login interface

3 Basic Operation

There are a variety of basic call service operations in an IPPBX. The following examples describe only a few basic telephone operations. For a complete description of the IPPBX calling features, please refer to other sections of this document for instructions.

3.1 Phone call operation

There are two methods to dial telephone or extension number:

- Dial the called number and wait for 4 seconds for dialing timeout, or dial the called number directly (the system will judge whether the dialing is completed according to Digitmap and Regular Expression dialplans).
- Press # after dialing the called number to end.

3.2 Call Holding

The current call can be held by pressing the "flash" key on the phone (if available), and then pressing the "flash" key again to resume the held call. If there is no "flash" key, you can use "hook flash" instead.

3.3 Call Waiting

When call waiting is enabled, if you hear the call waiting voice during a call, it indicates that a new call is incoming. You can switch between the incoming call and the current call through the Flash key or hook flash.

3.4 Query IP Address and Restore Default Setting

Since UC8000 uses the IP address of the host system, and UC8000 cannot change this IP address, users can only check the IP address by logging into the host system, as shown in the following figure.

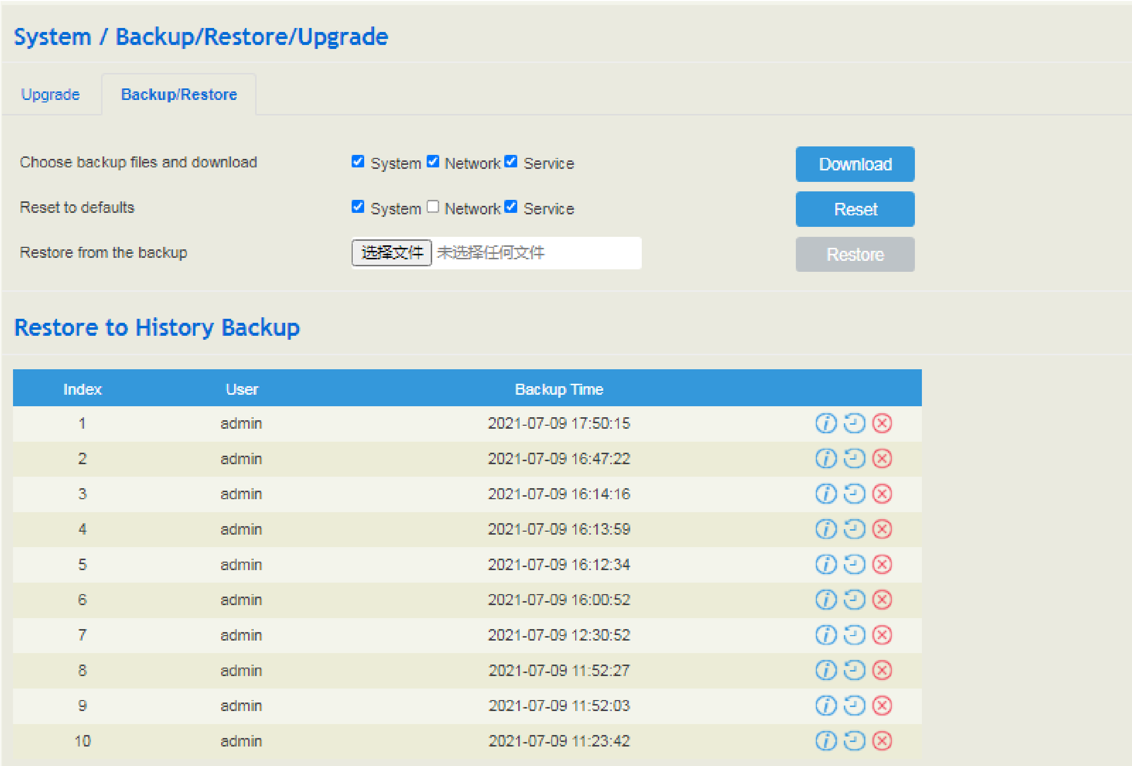
```
uc8000@uc8000:/$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:b6:ff:f2:ff  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp6s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.28.86.186  netmask 255.255.0.0  broadcast 172.28.255.255
        inet6 fe80::1ac0:4dff:fe28:d6b2  prefixlen 64  scopeid 0x20<link>
        inet6 2020::1e  prefixlen 128  scopeid 0x0<global>
        inet6 2020::1ac0:4dff:fe28:d6b2  prefixlen 64  scopeid 0x0<global>
        ether 18:c0:4d:28:d6:b2  txqueuelen 1000  (Ethernet)
        RX packets 6334676  bytes 666385565 (666.3 MB)
        RX errors 0  dropped 604253  overruns 0  frame 0
        TX packets 672593  bytes 144302741 (144.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8341064  bytes 1336805441 (1.3 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8341064  bytes 1336805441 (1.3 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

uc8000@uc8000:/$
```

After logging into the web, navigate to **System/Backup/Restore/Upgrade**, select the parts (system, network or service) that need to be restored in the "Restore to default settings" option, click **Reset** to reboot the system, and the selected parts will be restored to default settings.



Index	User	Backup Time
1	admin	2021-07-09 17:50:15
2	admin	2021-07-09 16:47:22
3	admin	2021-07-09 16:14:16
4	admin	2021-07-09 16:13:59
5	admin	2021-07-09 16:12:34
6	admin	2021-07-09 16:00:52
7	admin	2021-07-09 12:30:52
8	admin	2021-07-09 11:52:27
9	admin	2021-07-09 11:52:03
10	admin	2021-07-09 11:23:42

Figure 3.4.1 Restore default settings

Note: Restoring the factory settings does not change the IP address.

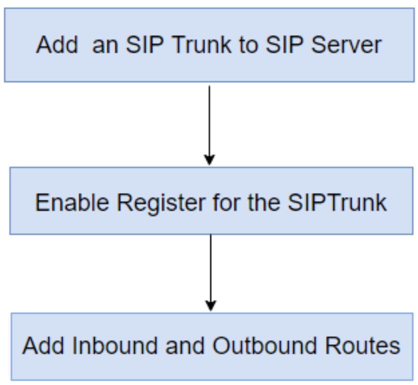
4 Configuration Wizard

4.1 Configuration Wizard

The following are the common ways to configure the UC8000 IPPBX.

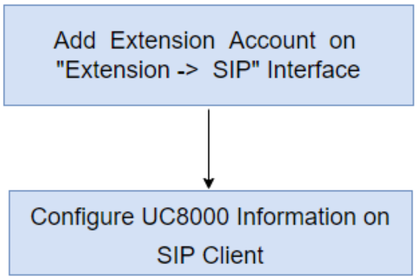
4.2 Register to the server as a terminal

The UC8000 is registered to the server as a terminal.

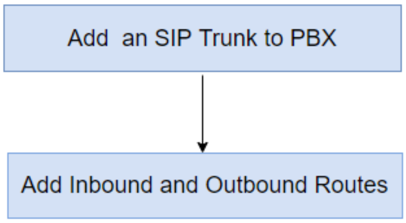


4.3 Other SIP Clients registered at UC8000

Under this mode, UC8000 is regarded as an SIP Server. Create an extension account first on the **Extension -> SIP** interface, and configure the listening port on the **Profile -> SIP** interface. Then configure the server and account on SIP client.



4.4 UC8000 Connected to PBX through SIP Trunk



5 Web configuration

5.1 Introduction to Web Interface

Enter the IP address of UC8000 in the browser, such as: "192.168.11.1", then enter username and password (default is **admin/admin@123#**), click "Login" to enter the web interface.

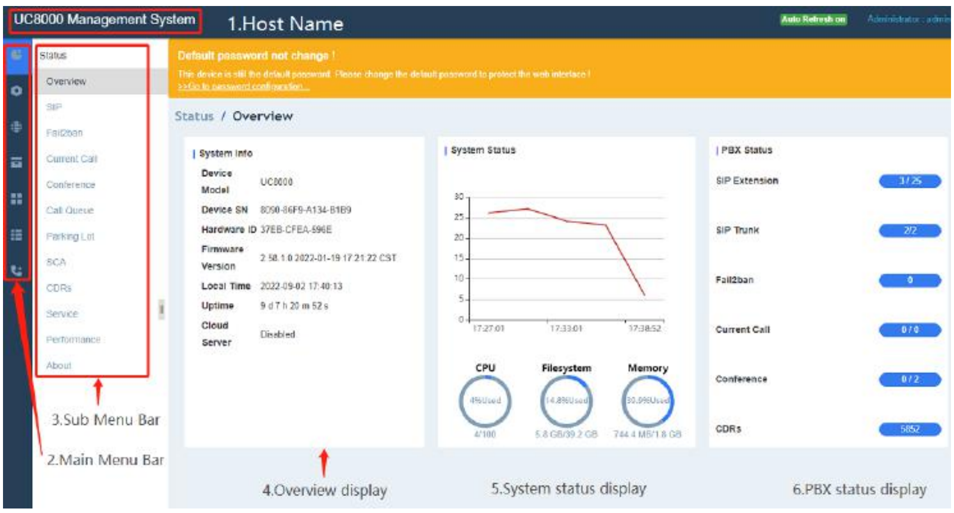


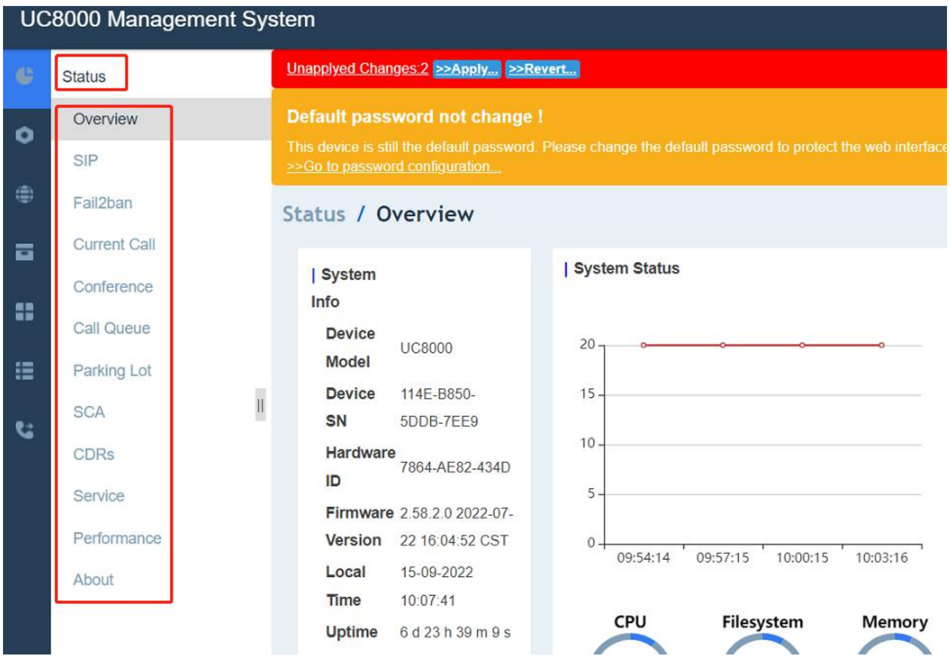
Figure 5.1.1 Introduction to login GUI

Table 5.1.1 Introduction of Web Interface

Index	Item	Description
1	UC8000	Host name, web cannot be modified, users can customize in the host.
2	Main Menu Bar	Main Menu of UC8000.
3	Sub Menu Bar	Specific functional items.
4	Overview display	Display the device model, device SN, firmware version, etc.
5	System Status	The chart displays the status information of the system.
6	PBX Status	SIP extension, SIP trunk, Fail2ban, current call, conference, CDRs and other statistical information.

5.2 Status

The Status menu mainly displays all kinds of status information. It includes overview, SIP, Fail2ban, current call, conference, call queue, parking lot, SCA, CDRs, service, performance and about etc.



5.2.1 Overview

The **Status->Overview** interface mainly displays device model, device SN, hardware ID, firmware version, local time, system status, PBX status, etc.

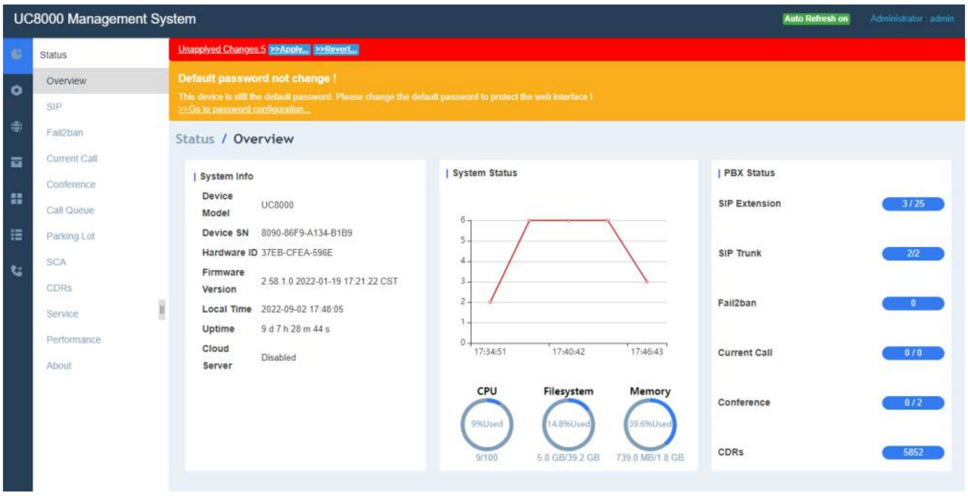


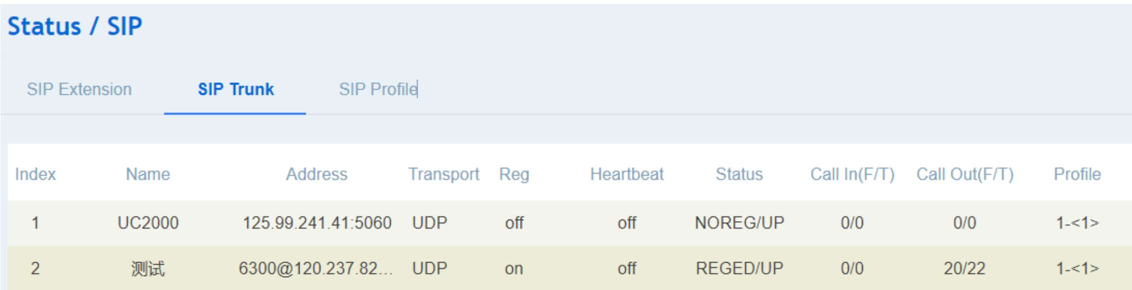
Figure 5.2.1 Overview

5.2.2 SIP

The **Status->SIP** interface displays the SIP information, including SIP Extension, SIP Trunk and SIP Profile.

Index	Name	Extension	Online	Register Source	Status	Expires	Agent	Profile
1	2030	2030	0		Unregistered			1-< 1 >
2	2028	2028	0		Unregistered			1-< 1 >
3	2038	2038	0		Unregistered			1-< 1 >
4	1004	1004	0		Unregistered			1-< 1 >
5	1005	1005	0		Unregistered			1-< 1 >
6	2029	2029	0		Unregistered			1-< 1 >
7	2040	2040	0		Unregistered			1-< 1 >
8	8001	8001	1	113.89.14.212:5060	Registered(UDP)	732	Yealink SIP-T23P 44.84.0.140	1-< 1 >

Figure 5.2.2-1 SIP Extension



Index	Name	Address	Transport	Reg	Heartbeat	Status	Call In(F/T)	Call Out(F/T)	Profile
1	UC2000	125.99.241.41:5060	UDP	off	off	NOREG/UP	0/0	0/0	1-<1>
2	测试	6300@120.237.82...	UDP	on	off	REGED/UP	0/0	20/22	1-<1>

Figure 5.2.2-2 SIP Trunk

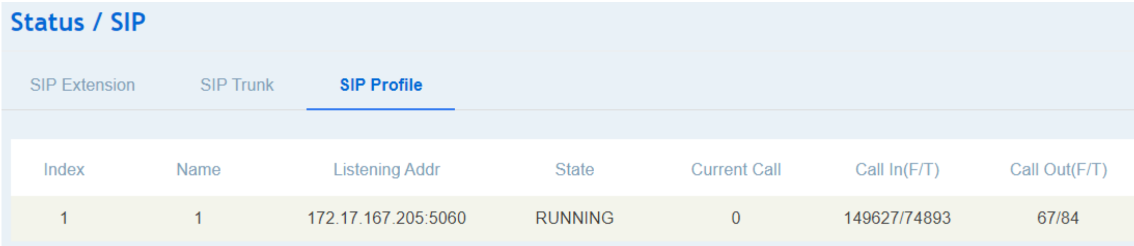


Figure 5.2.2-3 SIP Profile

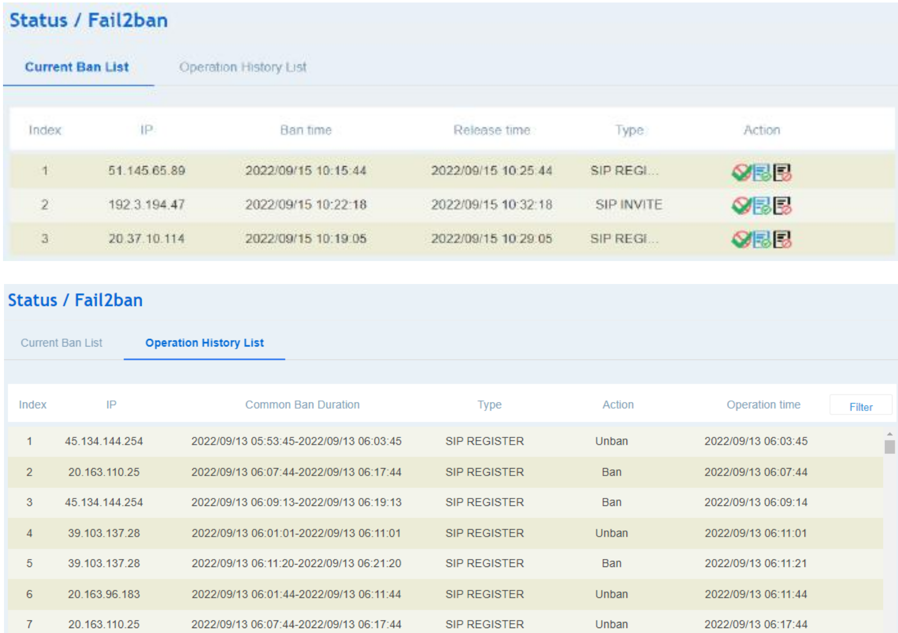
Table 5.2.2 Explanation of SIP Parameters

Belong To	**Parameter**	**Explanation**
SIP Extension	Profile	The profile that is used by the SIP extension.
	Status	SIP extension is registered or not. There are two statuses: Registered and Unregistered.
SIP Trunk	Heartbeat	If heartbeat is enabled, option message will be sent to peer device.
	Status	Green means available, while red means abnormal, unavailable or prohibited. There are five states. Running, Registered/Rising, Not Registered/Rising, Trying-Descending, Failed-Waiting.
	Profile	The profile that is used by the SIP trunk.
SIP Profile	Name	The name of the SIP profile.
	Listening Address	The current listening address and port of SIP.
	State	Green means normal running, while red means listening address and port of SIP is unavailable. There are two states: Running and Down.

5.2.3 Fail2ban

On the **Status->Fail2ban** interface, users can see banned IP addresses. They can also unblocked those IP addresses that have been blocked before.

Fail2ban is a log-parsing application that monitors system logs for symptoms of an automated attack on your system. When an attempted compromise is located, using the defined parameters, Fail2ban will add a new rule to block the IP address of the attacker, either for a set amount of time or permanently. Fail2ban can also alert you through email that an attack is occurring.


Status / Fail2ban

Current Ban List | Operation History List

Index	IP	Ban time	Release time	Type	Action
1	51.145.65.89	2022/09/15 10:15:44	2022/09/15 10:25:44	SIP REGI...	
2	192.3.194.47	2022/09/15 10:22:18	2022/09/15 10:32:18	SIP INVITE	
3	20.37.10.114	2022/09/15 10:19:05	2022/09/15 10:29:05	SIP REGI...	

Status / Fail2ban

Current Ban List | Operation History List

Index	IP	Common Ban Duration	Type	Action	Operation time
1	45.134.144.254	2022/09/13 05:53:45-2022/09/13 06:03:45	SIP REGISTER	Unban	2022/09/13 06:03:45
2	20.163.110.25	2022/09/13 06:07:44-2022/09/13 06:17:44	SIP REGISTER	Ban	2022/09/13 06:07:44
3	45.134.144.254	2022/09/13 06:09:13-2022/09/13 06:19:13	SIP REGISTER	Ban	2022/09/13 06:09:14
4	39.103.137.28	2022/09/13 06:01:01-2022/09/13 06:11:01	SIP REGISTER	Unban	2022/09/13 06:11:01
5	39.103.137.28	2022/09/13 06:11:20-2022/09/13 06:21:20	SIP REGISTER	Ban	2022/09/13 06:11:21
6	20.163.96.183	2022/09/13 06:01:44-2022/09/13 06:11:44	SIP REGISTER	Unban	2022/09/13 06:11:44
7	20.163.110.25	2022/09/13 06:07:44-2022/09/13 06:17:44	SIP REGISTER	Unban	2022/09/13 06:17:44

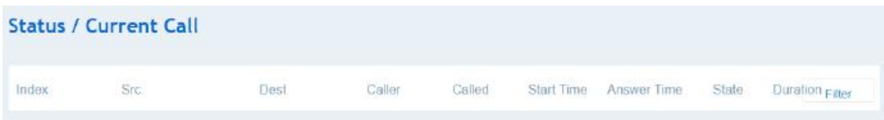
Filter

Figure 5.2.3 Fail2ban

Note: For the explanation of parameters related to Fail2ban, please refer to the Network ->Fail2ban section.

5.2.4 Current Call

On the **Status->Current Call** interface, the source, destination, caller number, called number, start time, answer time, state and duration of the current real-time call are displayed. If there is no current call, no information will be shown.


Status / Current Call

Index	Src	Dest	Caller	Called	Start Time	Answer Time	State	Duration

Filter

Figure 5.2.4 Current Call Information

5.2.5 Conference

The **Status -> Conference** interface displays the current conference status, conference information, operation records, etc.

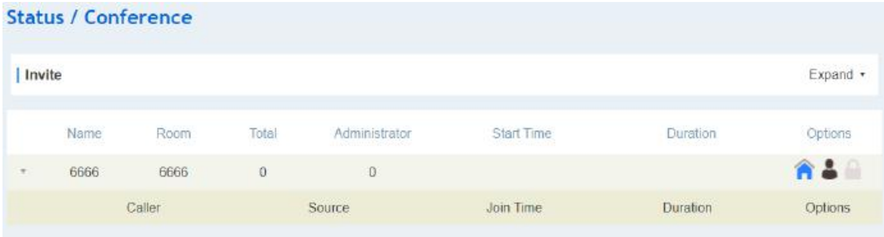
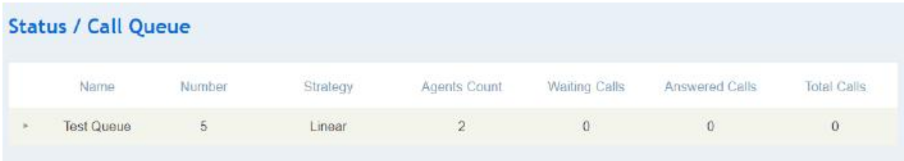


Figure 5.2.5 Conference Information

5.2.6 Call Queue

Users can view the related information of the queue status on the **Status -> Call Queue** interface, the queue configuration change will reboot the agent, and the dynamic agent will disappear.



Click the 'Inverted triangle symbolon' on the far left to view more detailed agent status.

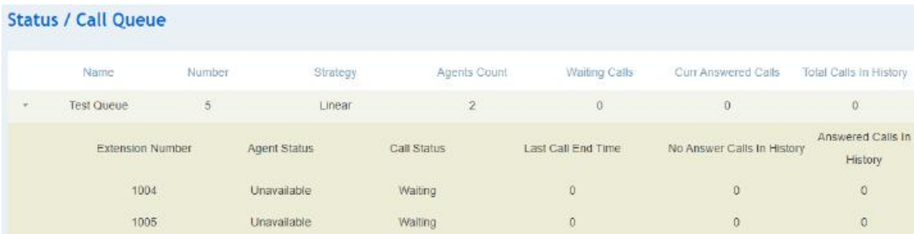


Figure 5.2.6 Call Queue

5.2.7 Parking Lot

You can use the parking feature to park a call, and then retrieve the call either from your phone or another phone. After you park a call, the call is placed on hold, you can continue the conversation after retrieving it.

On the **Status -> Parking Lot** interface, the numbers that are parked and the parking duration are shown.

Figure 5.2.7 Parking Lot

5.2.8 SCA

On the **Status -> SCA** interface, SCA information and SCA line status are shown.

Figure 5.2.8-1 SCA

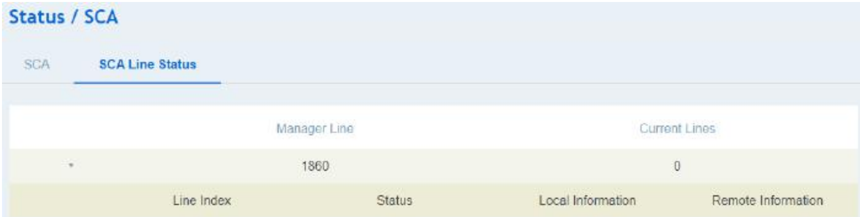


Figure 5.2.8-2 SCA Line Status

When there is a call, the SCA current line count is 1 and the corresponding message is shown.

Figure 5.2.8-3 SCA Line Status is 1

5.2.9 CDRs

On the **Status->CDRs** interface, if CDRs is enabled, CDRs will be saved automatically. 50000 CDRs call be saved at most and they can be queried on the Status ->CDRs interface; If it is disabled, CDRs will not be saved.

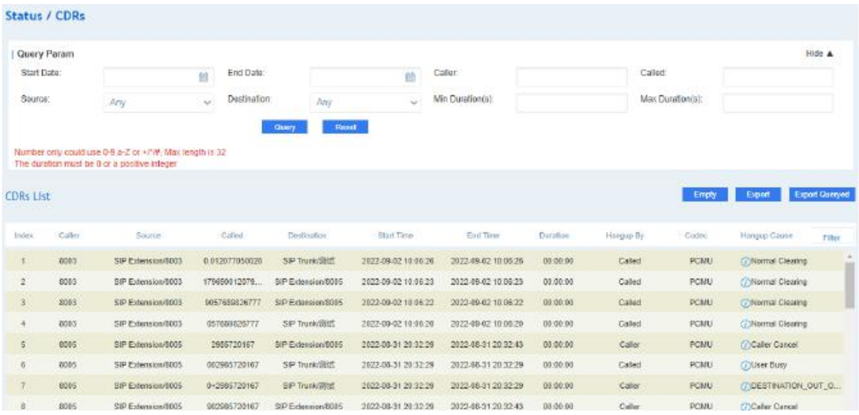


Figure 5.2.9 CDRs

5.2.10 Service

The **Status->Service** interface displays the current service status of the system. Switch Kernel Service, Log Service and Web Service are on by default, among which the web service can be closed and the port modified on the Network->Access Control interface. The other services cannot be closed, and if they are not running, it means the system is abnormal.

Besides, if syslog is disabled on the System -> Setting interface, the logs cannot be uploaded to the server, but log service is still running.

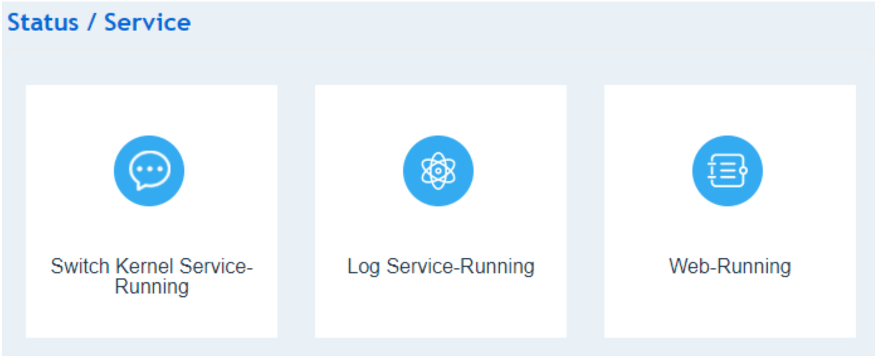


Figure 5.2.10 Service Status

5.2.11 Performance

The **Status ->Performance** interface displays the performance statistics of the system. The parameters of the system such as usr, sys, io, and sirq are displayed at the 5th second, 1 minute, 5 minutes, and 1 hour.

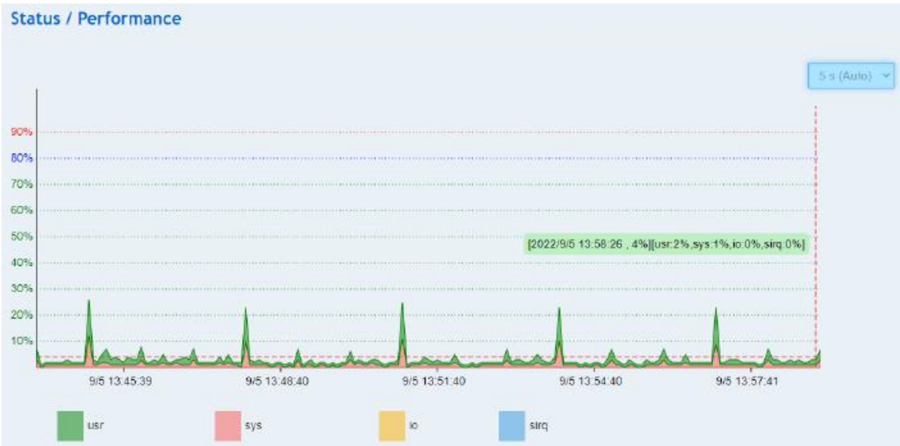


Figure 5.2.11 System Performance

5.2.12 About

On the **Status -> About** interface, the device model, device SN, hardware ID, MAC address and firmware version of the UC8000 are displayed.

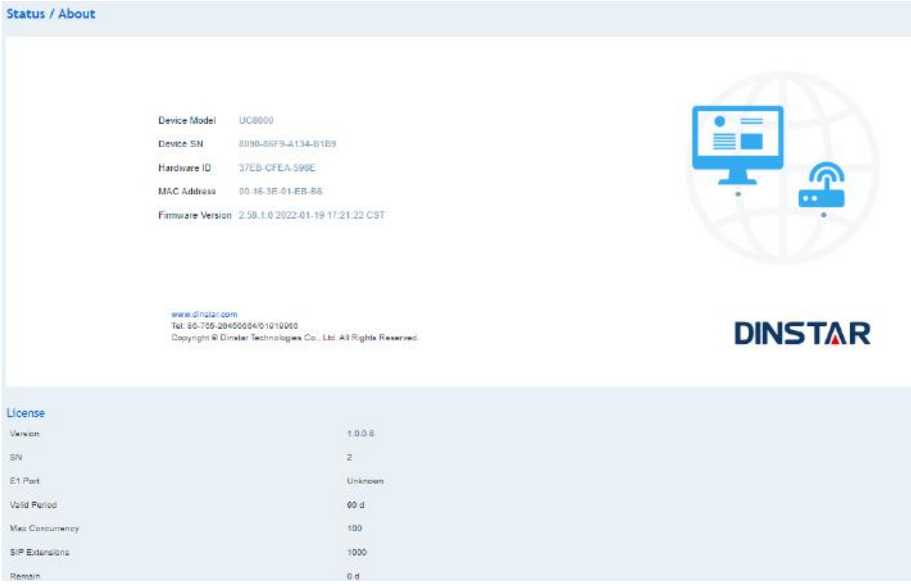
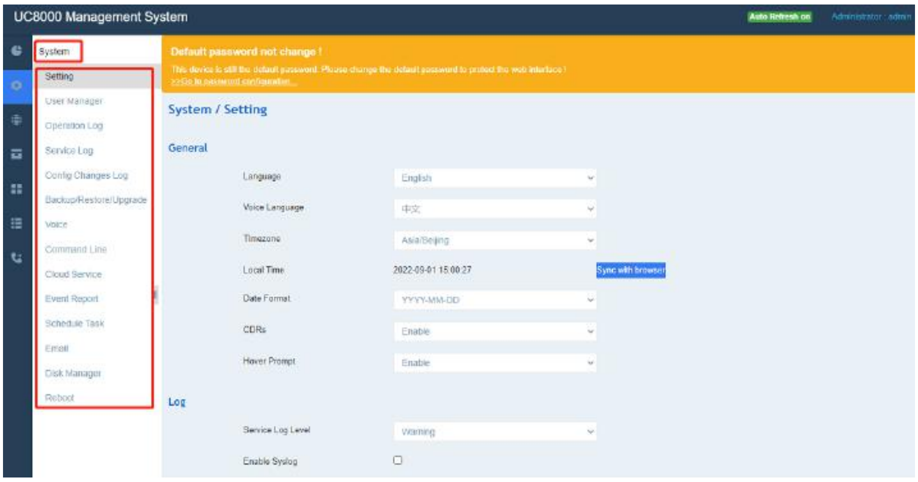


Figure 5.2.12 About

Note: After installing the UC8000, firstly users need to activate all functions of the software with the official license, otherwise the system will not work. If users need to obtain the software license, they can contact technical support to open the license.

5.3 System

Users can configure the time zone, login username and password, other user name, provision, operation log, service log, backup/restore/upgrade, command line, cloud service and reboot can be carried out in the System section.



5.3.1 Setting

On the **System -> Setting** interface, users can modify language and voice language, set a new time zone, synchronize local time and enable CDRs, Syslog.

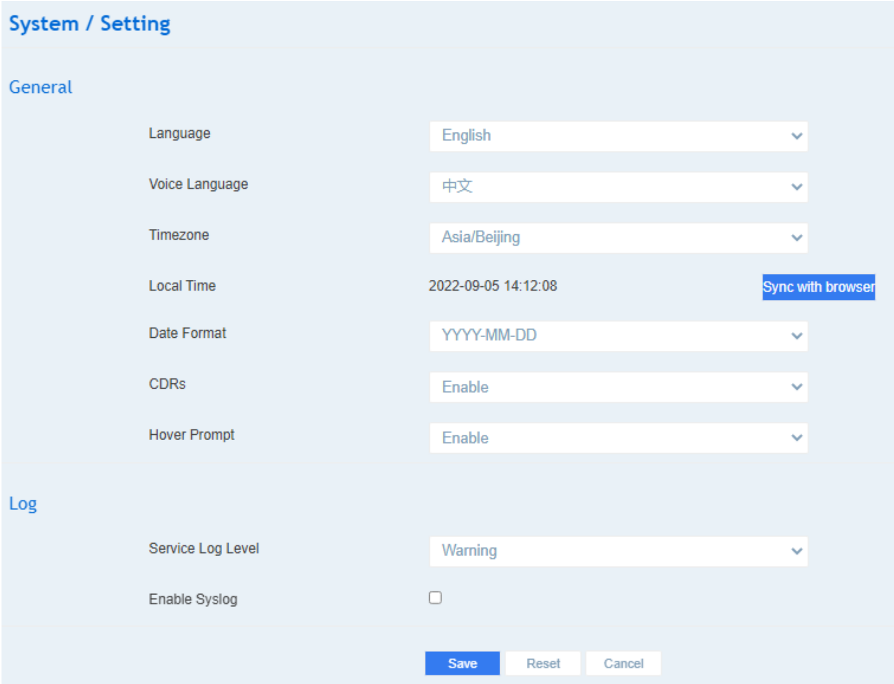


Figure 5.3.1 Basic Setting

Note:

Language: web interface language;

Voice language: preloaded media sound language played during the call. This is controlled by license. If users need to enable certain language features, please contact technical support.

Table 5.3.1 Explanation of Basic Setting Parameters

Parameter	**Explanation**
Language	Users can choose Chinese or English.
Voice Language	Users can choose Chinese, Spanish, Portuguese or English.
Timezone	Users can choose a time zone they want. The default value is UTC (Universal Time Coordinated).
Local Time	The current time based on current time zone. It is synchronized with NTP.
Data Format	Users can choose 'Year- Month-Day',' Day-Month-Year' or

	'Month-Day-Year'.
CDRs	If it is enabled, CDRs will be saved automatically. 50000 CDRs call be saved at most and they can be queried on the **Status ->CDRs** interface. If it is disabled, CDRs will not be saved.
Hover Prompt	Users can choose Enable or Disable.
Service Log Level	There are eight levels, including Debug, Info, Notify, Warning, Error, Critical, Alert and Emergency.
Enable Syslog	Whether to enable system logging.

5.3.2 User Manager

On the **System -> User Manager** interface, and users can set the username, password and manage other users. The default username and password are **admin and admin@123#**, so it is strongly advised to modify them for security.

The super administrator of the system can add different users to the system and assign different roles for them, like observer, operator, and administrator. Different roles can support different permissions to the functions.

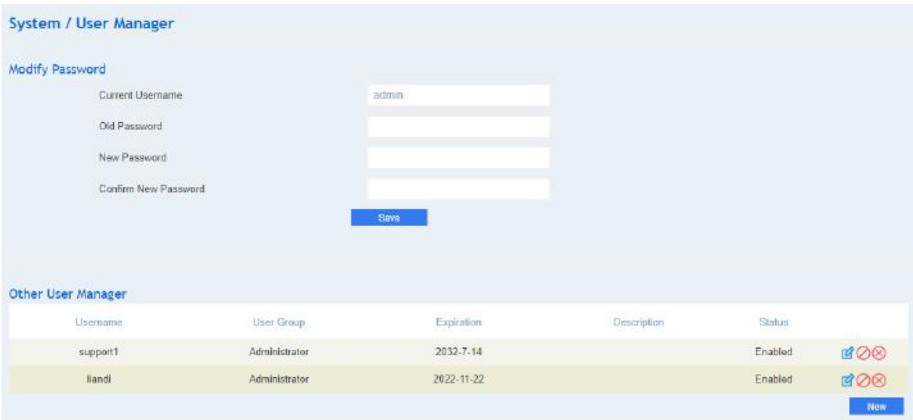


Figure 5.3.2-1 Modify username, password and user manager

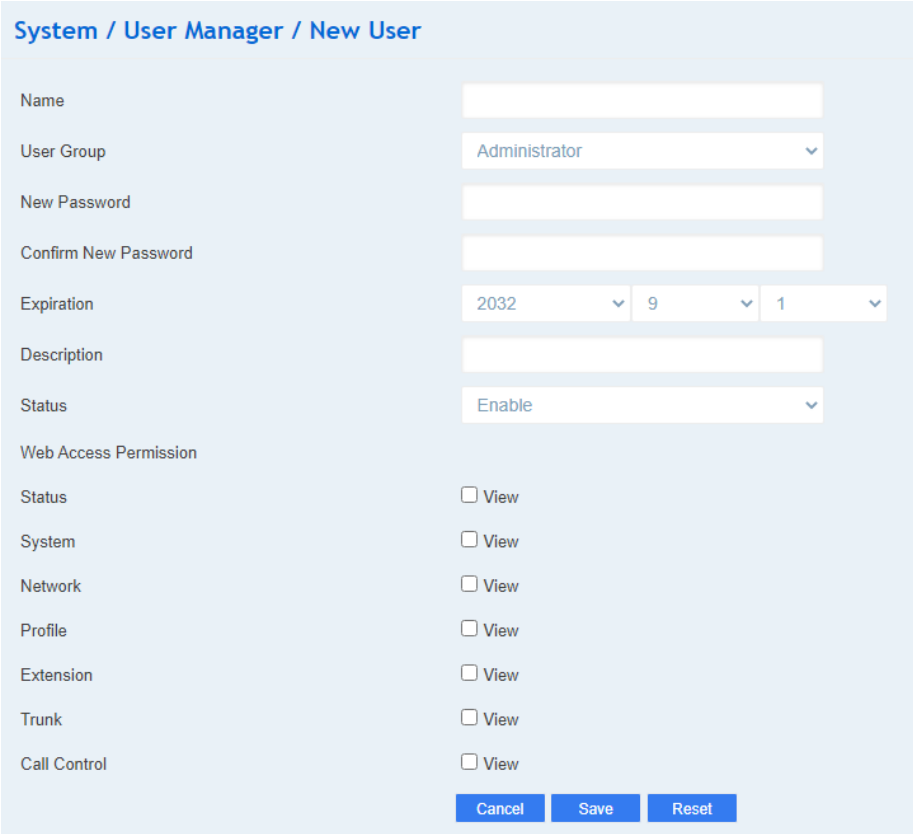


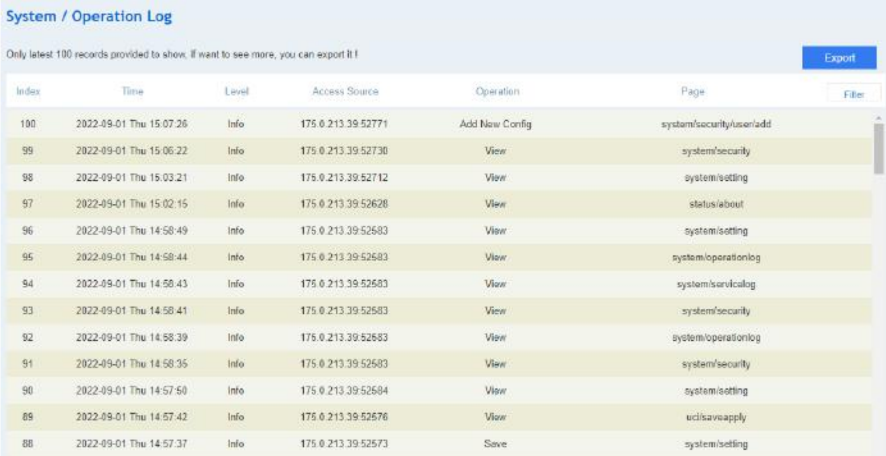
Figure 5.3.2-2 Add new user

Table 5.3.2 Explanation of Provision Parameters

Name	The name of the new user. After it is established, the name and the password will be used to log into the web interface of the system.
User Group	Users can choose a role for the new user, such as administrator, operator, and observer. The default value is administrator.
New Password	Setting the login password for the new user. The password needs to consist of 8 to 32 characters.
Expiration	The expiry date when the user cannot log into the system any more.
Status	Choose enable or disable.
Web Access Permission	The permissions to view status, system, network, profile, extension, trunk, and call control.

5.3.3 Operation Log

The **System -> Operation Log** interface records the operation log when users access the web. Users can click "Filter" to enter filter criteria to query logs, and click "Export" to export log files.



Index	Time	Level	Access Source	Operation	Page
100	2022-09-01 Thu 15:07:26	Info	175.0.213.39:52771	Add New Config	system/security/user/add
99	2022-09-01 Thu 15:06:22	Info	175.0.213.39:52730	View	system/security
98	2022-09-01 Thu 15:03:21	Info	175.0.213.39:52712	View	system/setting
97	2022-09-01 Thu 15:02:15	Info	175.0.213.39:52628	View	status/about
96	2022-09-01 Thu 14:58:49	Info	175.0.213.39:52583	View	system/setting
95	2022-09-01 Thu 14:58:44	Info	175.0.213.39:52583	View	system/operationlog
94	2022-09-01 Thu 14:58:43	Info	175.0.213.39:52583	View	system/servicelog
93	2022-09-01 Thu 14:58:41	Info	175.0.213.39:52583	View	system/security
92	2022-09-01 Thu 14:58:39	Info	175.0.213.39:52583	View	system/operationlog
91	2022-09-01 Thu 14:58:35	Info	175.0.213.39:52583	View	system/security
90	2022-09-01 Thu 14:57:50	Info	175.0.213.39:52584	View	system/setting
89	2022-09-01 Thu 14:57:42	Info	175.0.213.39:52576	View	uci/saveapply
88	2022-09-01 Thu 14:57:37	Info	175.0.213.39:52573	Save	system/setting

Figure 5.3.3 Operation Log

Note: The operation log is mainly used by vendors to locate problems.

5.3.4 Service Log

Service logs can be exported on the **System -> Service Log** interface. Those logs are generally used to locate system problems.

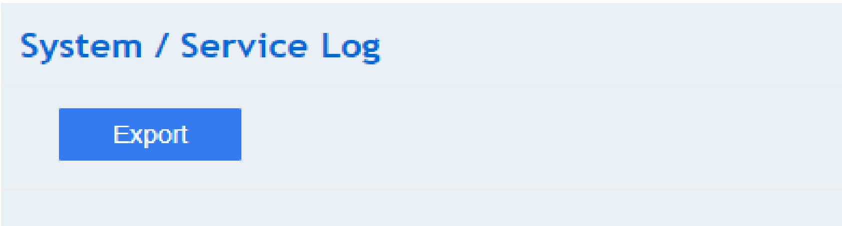


Figure 5.3.4 Service Log

5.3.5 Config Changes Log

On the **System ->Config Changes Log** interface, the configurations changed by administrator on the web of the UC8000 IPPBX are recorded.

Figure 5.3.5 Config Changes Log

5.3.6 Backup/Restore/Upgrade

On the **System ->Backup/Restore/Upgrade** interface, users can backup or restore configuration files, and can upgrade UC8000 to a new version. But users need to reboot the system for the change to take effect after executing restore or upgrade.

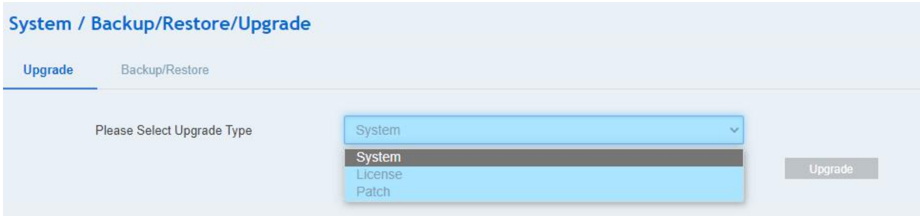


Figure 5.3.6-1 Upgrade the system

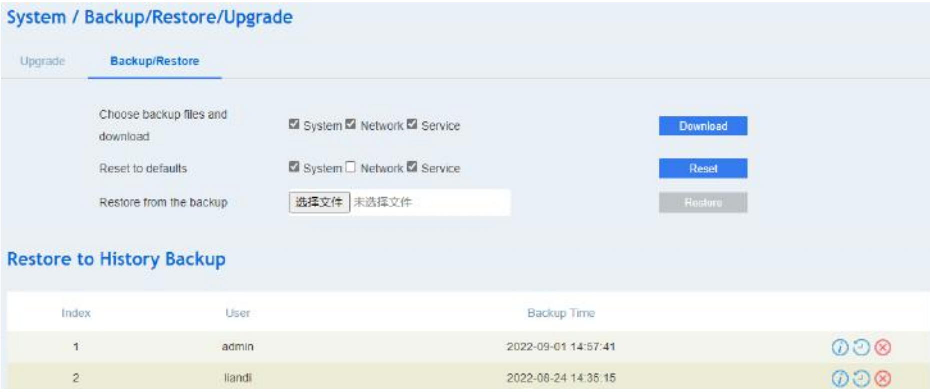


Figure 5.3.6-2 Backup/Restore files

Note: The file you choose to be upgraded on the above interface is a local file.

Table 5.3.6 Explanation of Backup/Restore/Upgrade

Download	Users can download the configuration data to be backed up. Select any of the checkboxes on the left of System, Network and Service, and then click **Download.**
Reset	Select any of the checkboxes on the left of System, Network and Service, and then click **Reset**, and configurations related to the selected part will be restored to factory defaults.
Restore	Choose a backup file, and then click **Restore**.
Upgrade	Choose a file to be upgraded, and then click **Upgrade**.

5.3.7 Voice

On the **System -> Voice** interface, users can upload an IVR file according to their requirement. At present, only a wav audio file is allowed. The format of the wav audio file uploaded must be: monaural, 8000hz, 16bit, and size of no more than 3M.

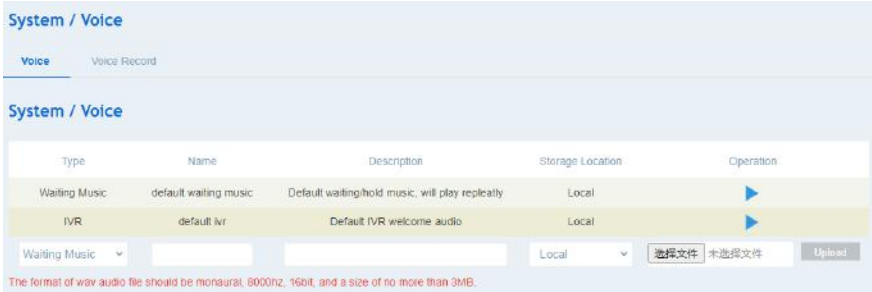


Figure 5.3.7 Upload IVR File

Note: UC8000 can upload 32 waiting music files and 32 IVR files (expandable).

5.3.8 Command Line

On the **System -> Command Line** interface, some commonly used command lines can be directly selected in the draw-down box, and therefore user has no need to enter command lines on Telnet. In this way, the efficiency of problem diagnostics is greatly improved. Commonly used command lines include sip status, sip profile and so on.

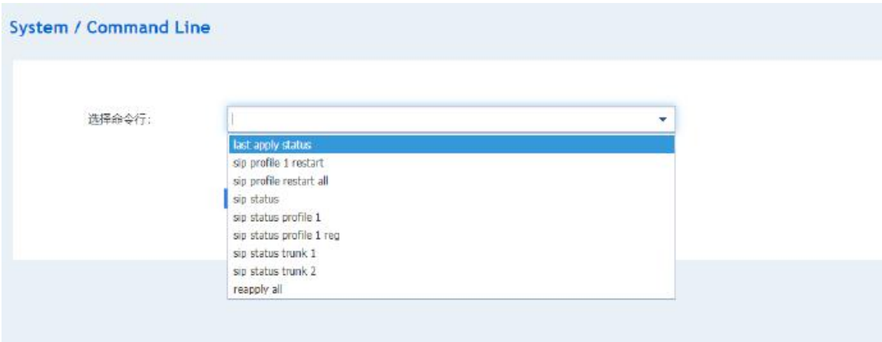


Figure 5.3.8 Command Line

Table 5.3.8 Explanation of Command Line

Execute	After selecting the corresponding command in the drop-down box, click "Execute" to execute the command.
Save	Click "Save" to download the execution results locally.
Empty	Clear the content of the command input box and the execution result.

5.3.9 Cloud Service

Cloud service is mainly used to centrally manage all kinds of devices. Through cloud service, users can query the system status, upgrade at batch, log in and configure remotely. UC8000 provides two cloud services: NMS and remote proxy, enter the IP address, service port and password of the cloud server, and then the UC8000 IPPBX will connect to the cloud server.

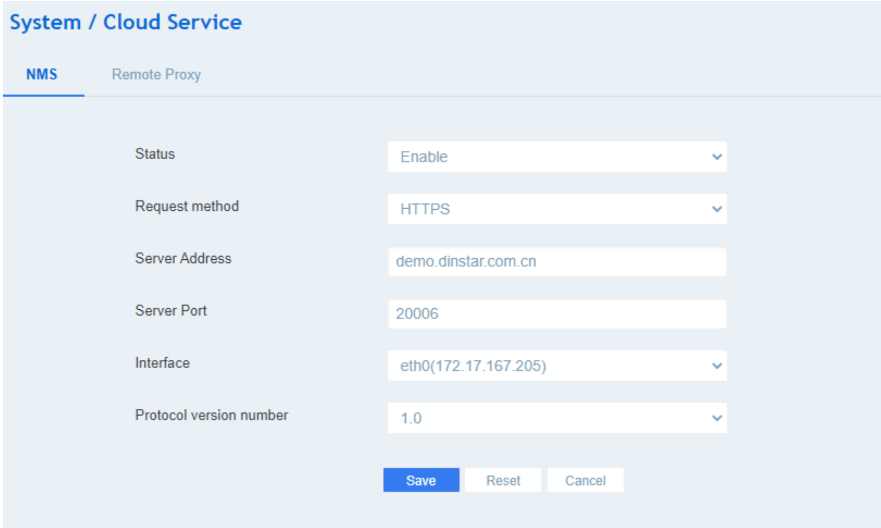


Figure 5.3.9-1 NMS Server Configuration

Operation steps：

- After enabling the NMS function, fill in the correct server address.
- The default server port is 20006, which can be configured by the user according to the NMS server built.
- Interface is the egress network interface of the current device.
- Protocol version numbers that are consistent with the server are sufficient.
- After saving the application, add the SN information of the device to the NMS server to see if the connection is successful.

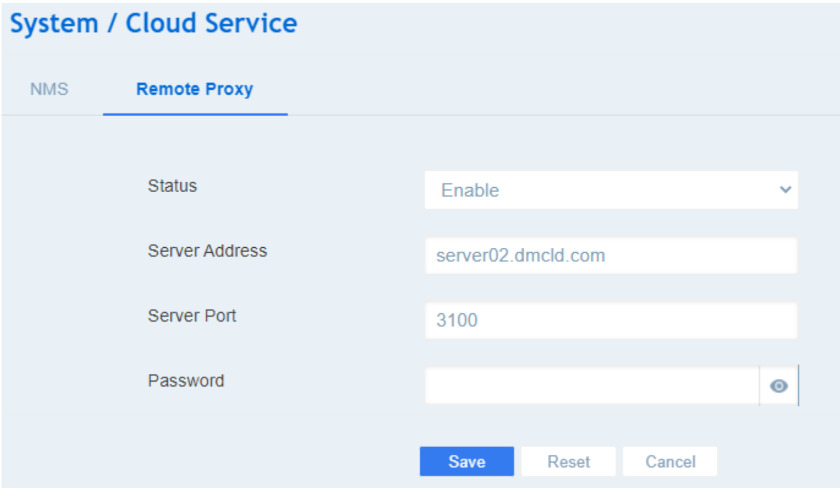


Figure 5.3.9-2 Remote Proxy server configuration

Operation steps：

- Enabling remote proxy function.
- The server address is the DRP server address.

- The default server port is 3100, which can be configured by the user according to the DRP server built.
- By default, users do not need to enter a password, and users can choose to enter password or not according to DRP server.
- After saving the application, users can add the serial number of the device on the DRP server to see if the connection is successful.

5.3.10 Event Report

The UC8000 supports the following events to be reported via URL: call status, CDRs, SIP extension register/unregister, SIP trunk available/unavailable, and recording to web server.

For event report through URL, please see the following example:

- On the **System -> Event Report** interface, select the events to be reported and the reporting method (URL);

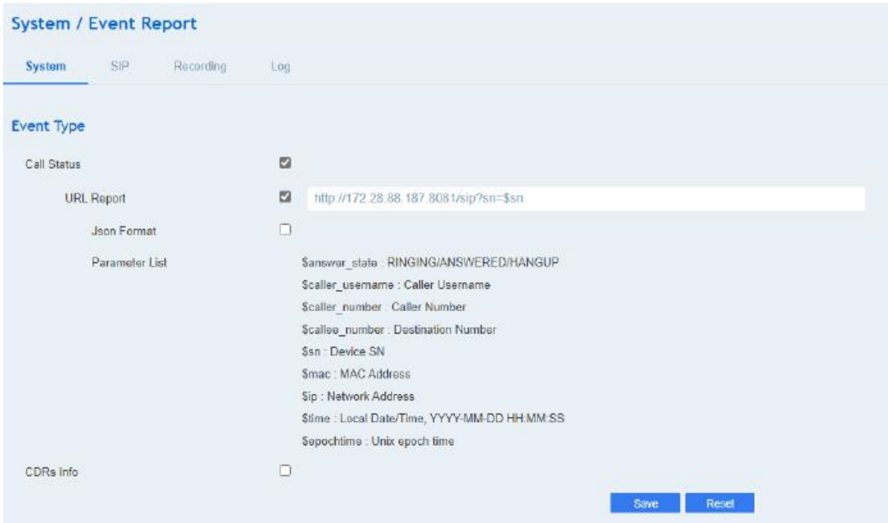


Figure 5.3.10-1 Check the reporting event and reporting method

- Input the URL Format:

`http://ip:port/event?key1=$value1&key2=$value2`

- Use a softphone to register to an extension of UC8000, and then the registration or logout of the softphone will be reported to UC8000 through the URL.
- On the System->Event Report/Log interface, users can view the report information.

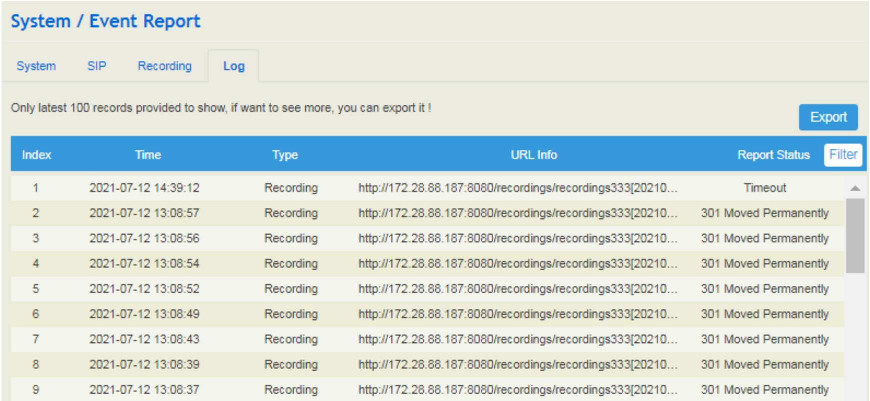


Figure 5.3.10-2 View Report Log

5.3.11 Schedule Task

On the **System -> Schedule Task** interface, users can set a schedule to reboot the UC8000, record backup, CDR backup, configuration, and log backup.

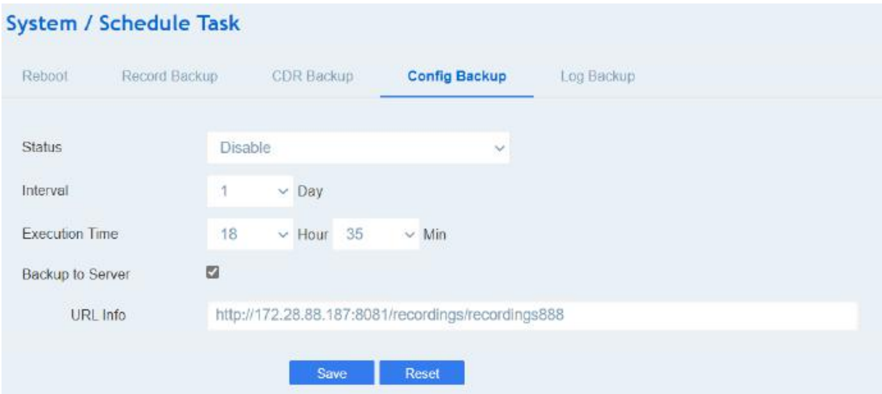


Figure 5.3.11 Schedule Task

5.3.12 Email

On the **System -> Email** interface, users can configure an email client, and can test the connection for sending mails. But the premise is that the configured email needs to open SMTP, IMAP and POP3 services. With voicemail, it can realize voicemail to email and will generate logs, users can go to System->Email/Log to check.

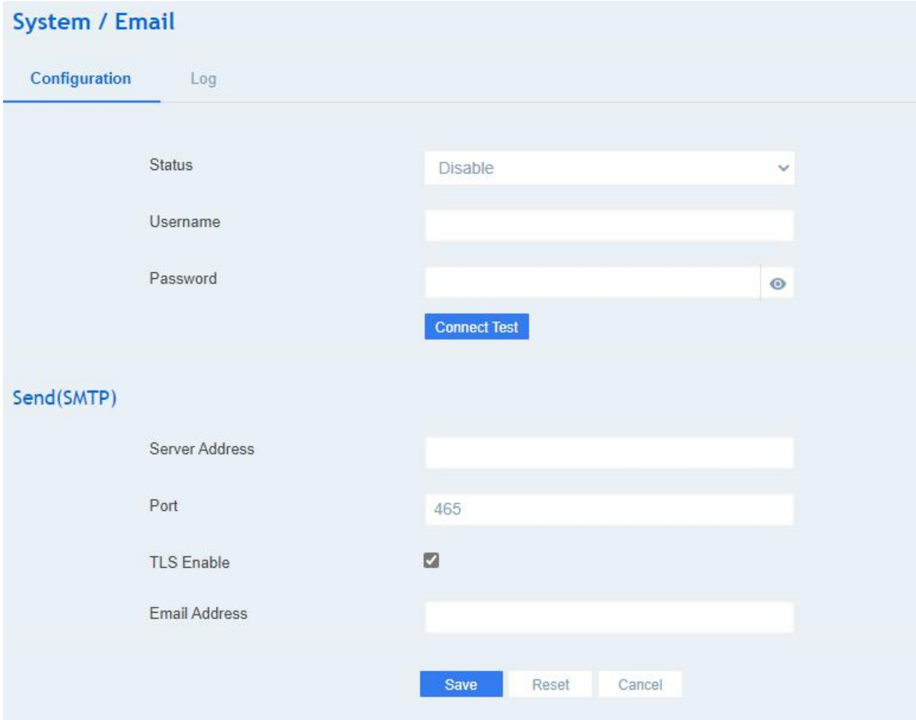


Figure 5.3.12 Email Configuration

Table 5.3.12 Explanation of Email Client Parameters

Username	Enter the address of email client.
Password	The password or authorization code of the email client.
Server Address	The address of the SMTP server, supported by the email client.
Protocol	Choose IMAP or POP3. When POPS is selected, TLS port is 995 by default.

5.3.13 Disk Manager

On the **System -> Disk Manager** interface, users can view the memory usage of system. The memory is divided into three categories, including recording (50%), voicemail (37%) and others (13%). They can also re-division the proportion of each category or execute formatting on this interface.

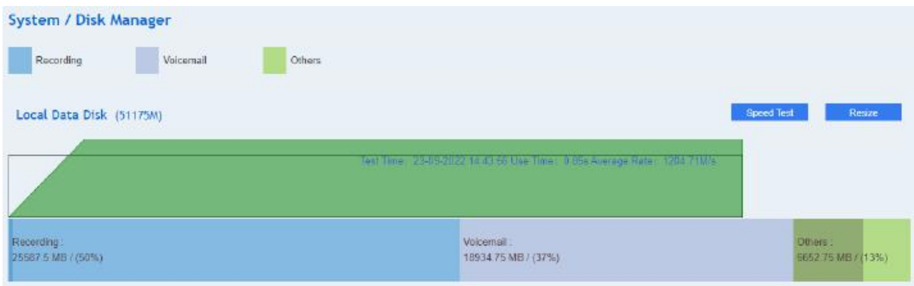


Figure 5.3.13 Disk Manager

Note: UC8000 currently does not support U disk/SD card.

5.3.14 Reboot

On the **System -> Reboot** interface, users can click Restart Device to reboot the UC8000 IPPBX. After the device is rebooted, those configurations that have been saved will remain unchanged.

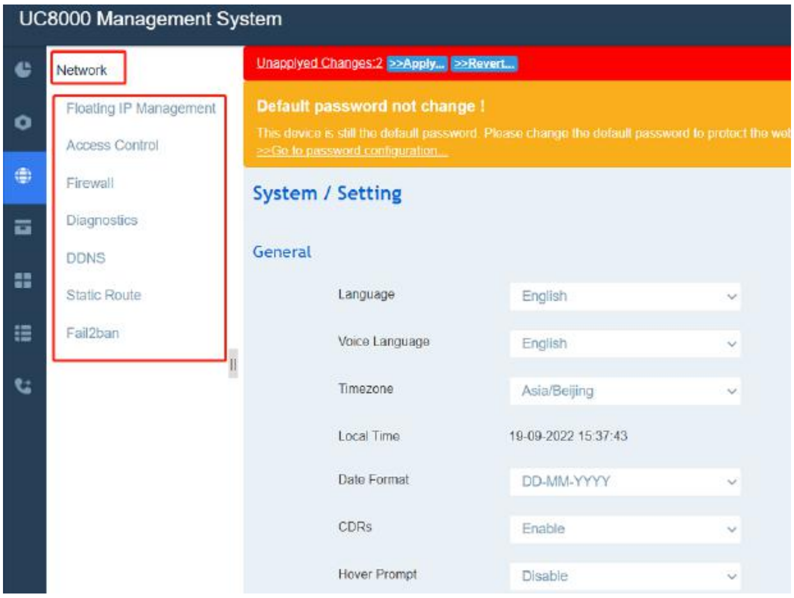
Figure 5.3.14 Reboot Device

Note: When Restart Device is selected, it means that the UC8000 reboots, the docker container and the host does not reboot.

5.4 Network

The UC8000 utilizes the IP address of the server's physical machine network interface, so the UC8000 does not require network configuration; If users want to use the active and standby feature, they can configure a floating IP address for active and standby management.

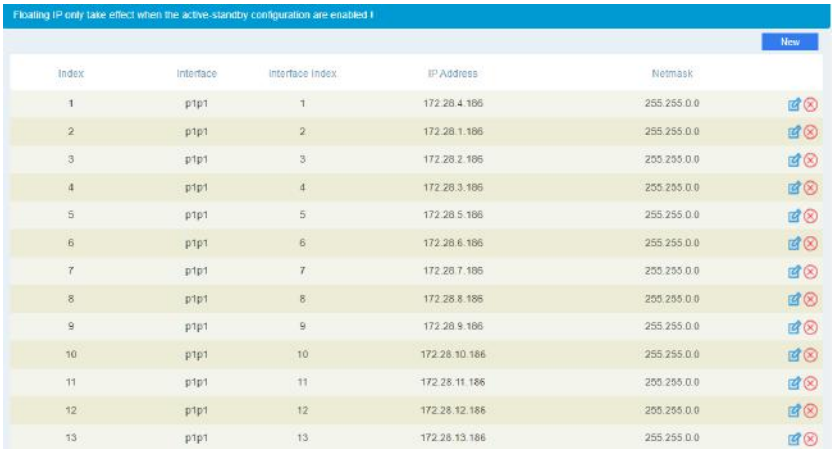
The network menu mainly manages/configures network-related functions, mainly including: floating IP management, access control, firewall, diagnostics, DDNS, static route and Fail2ban.



5.4.1 Floating IP Management

The floating IP takes effect only when the active and standby configuration is enabled, and the floating IP is used for management and service of the double-device active and standby. When the active and standby configuration is enabled, one or more floating IP addresses can be configured, and users can access the UC8000 based on this IP address.

In the profile, the bound interface will also become the interface corresponding to the floating IP address (e.g., enp6s01:1 (172.28.4.100)), and the call service data will be forwarded to the UC8000 via this floating IP address.


Floating IP only take effect when the active-standby configuration are enabled !

New

Index	Interface	Interface Index	IP Address	Netmask
1	p1p1	1	172.28.4.186	255.255.0.0
2	p1p1	2	172.28.1.186	255.255.0.0
3	p1p1	3	172.28.2.186	255.255.0.0
4	p1p1	4	172.28.3.186	255.255.0.0
5	p1p1	5	172.28.5.186	255.255.0.0
6	p1p1	6	172.28.6.186	255.255.0.0
7	p1p1	7	172.28.7.186	255.255.0.0
8	p1p1	8	172.28.8.186	255.255.0.0
9	p1p1	9	172.28.9.186	255.255.0.0
10	p1p1	10	172.28.10.186	255.255.0.0
11	p1p1	11	172.28.11.186	255.255.0.0
12	p1p1	12	172.28.12.186	255.255.0.0
13	p1p1	13	172.28.13.186	255.255.0.0

Floating IP configuration steps.

- On the Network/Floating IP interface, click New.

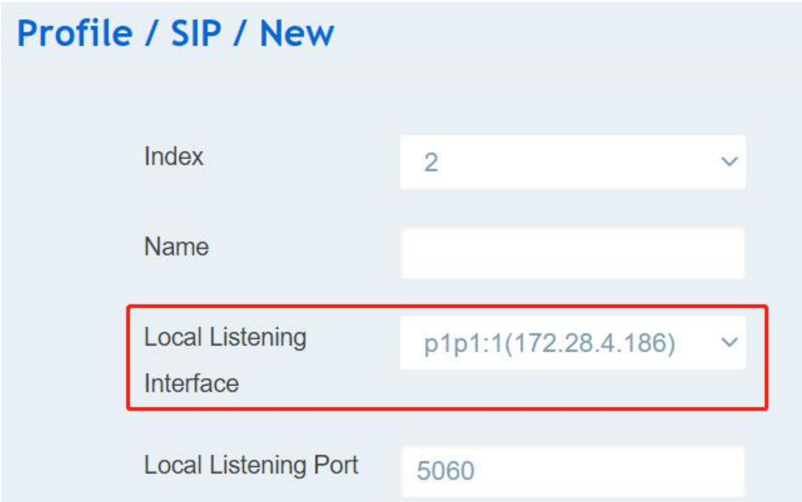
- Configure a floating IP address based on the interface and interface index.

Table 5.4.1 Floating IP parameters configuration instructions

Index	Floating IP entry numbering, up to 32 floating IP addresses can be created.
Interface	Select the interface to which the floating IP is bound, and drop

	down the selection to associated with the physical machine of the real network interface.
Interface Index	Network interface index number, the same network interface can be selected 32 interface indices, The same network interface cannot have duplicate interfaces Index.
IP Address	IP address for floating IP management, unduplicated IPv4 address format Enter.
Netmask	Floating IP address netmask, customizable input.

- After successfully creating a floating IP address, users can access the system in their browser by entering the floating IP address web.
- After successfully creating a floating IP address, creating or modifying the local listening interface as a new floating IP address, UC8000 will listen to the floating IP address for call service.



Note: After configuring the floating IP address with active and standby enabled, the local listening interface name is displayed as: "Interface Name: Interface Index (floating IP address)".

5.4.2 Access Control

The access ports of Web server, as well as relevant on-ff controls, can be configured on the **Network -> Access Control** interface. Which supports http and https, and the changes will take effect after saving. Both http and https access are enabled by default in the UC8000 configuration.

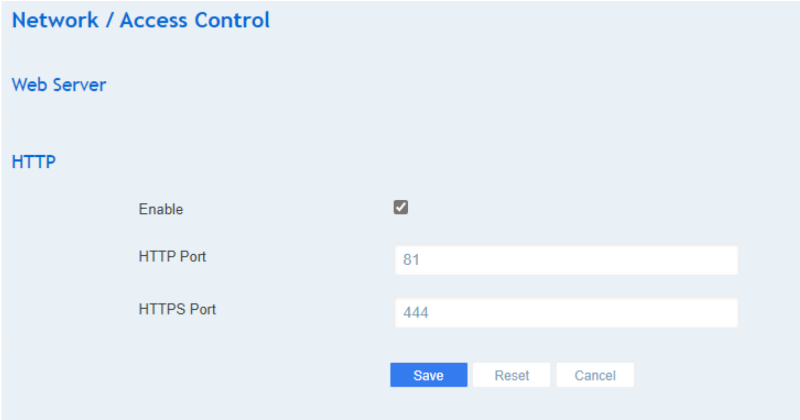


Figure 5.4.2 Access Control

5.4.3 Firewall

Users can choose to enable the firewall function and add filtering rules such as protocol/IP address/port /MAC address to accept or reject packets that meet the filtering rules from passing through the firewall.

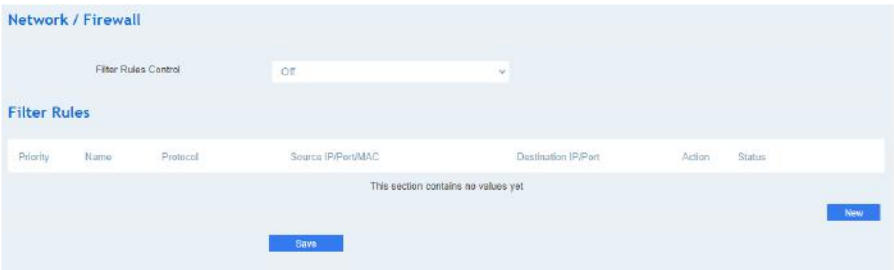


Figure 5.4.3-1 Firewall

Configuration Procedures:

- Select **On** in the drop-down box on the right of **Filter Rules Control**;
- Select filter action, accept or reject;
- Click the **New** button;
- Fill in information about filter rules (Filtering rule information: IP, port, MAC address can all be empty, no judgment will be made when it is empty, otherwise all three must be met after configuration);
- Click the **Save** button to save the configuration.

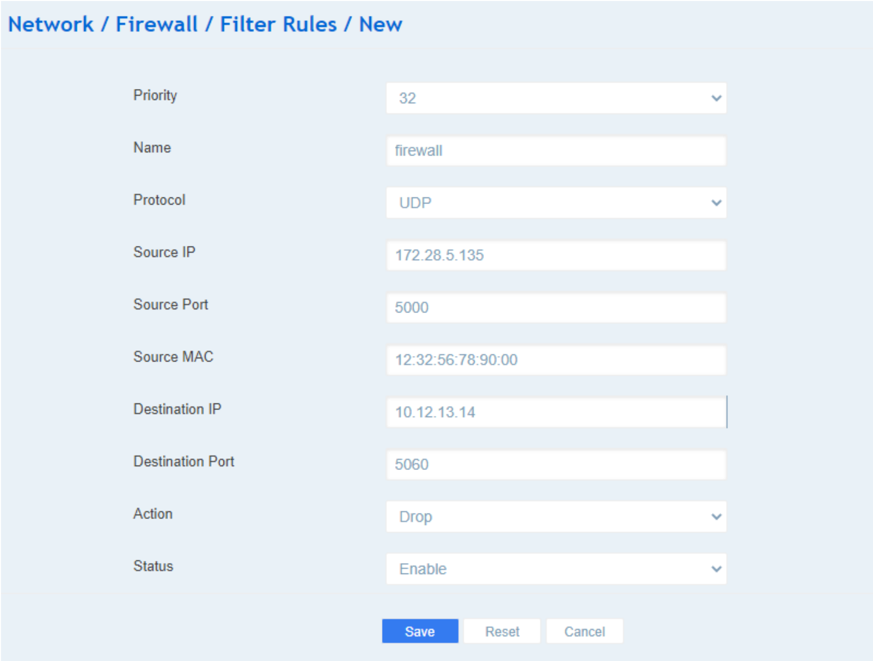


Figure 5.4.3-2 Create Filter Rule

Table 5.4.3 Explanation of Filter Rule

Priority	Users can choose 1-32.
Protocol	Users can choose TCP, UDP or All.
Source IP	The source IP address that users want UC8000 to accept or reject. It is the source IP address of the message; it can also be a string of IP addresses, for example, 172.16.11.1/15.
Source Port	The source port of host which the accepted or rejected IP address belongs to.
Source MAC	The source mac of the host which the accepted or rejected IP address belongs to.
Destination IP	The destination IP address that users want UC8000 to accept or reject. It is the destination IP address of the message; it can also be a string of IP addresses, for example, 152.16.11.11/19.
Destination Port	The destination port of host which the accepted or rejected IP address belongs to.
Action	Users can choose accept or reject.
Status	Users can choose enable or disable.

5.4.4 Diagnostics

On the **Network -> Diagnostics** interface, users can use three network utilities including Ping, Traceroute and Nslookup to diagnose the network, and can capture data packages of the available network ports.

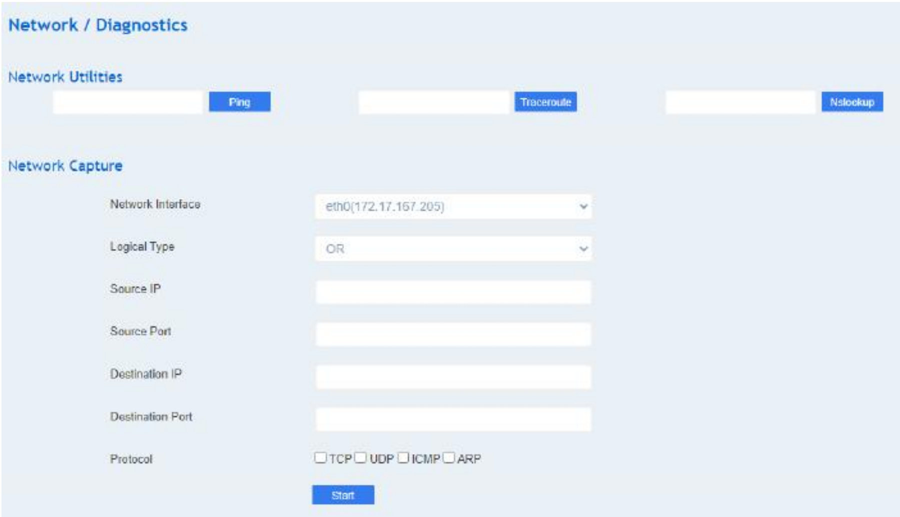


Figure 5.4.4 Network Diagnostics

Ping:

Ping is used to examine whether a network works normally through sending test packets and calculating response time.

Instructions for using Ping:

- Enter the IP address or domain name of a network, a website or a device in the input box of Ping, and then click Ping.
- If related messages are received, it means the network works normally; otherwise, the network is not connected or is connected faultily.

Traceroute:

Traceroute is used to determine a route from one IP address to another.

Instruction for using Traceroute:

- Enter the IP address or domain name of a destination device in the input box of Traceroute, and then click Traceroute.
- View the route information from the returned message.

Nslookup:

Nslookup (Name Server Lookup) is a network command-line tool to obtain domain name of internet or to diagnose the problems of DNS.

Instruction for using Nslookup:

- Enter a domain name and then click Nslookup.
- View the DNS information from the returned message.

Network Capture：

On the following interface, users can capture data packages of the available network ports. Users can also set source IP, source port, destination IP or destination port to capture the packages that they want.

There is a "and"/"or" logical type. The "and" relationship can only capture a one-way message, and "or" relationship to fetch the interaction message between a particular IP.

Note: If there are multiple source or destination IP addresses, please use '|' to separate them, for example, 172.16.115.12|172.16.115.15. After package capturing is completed, save the captured packages on a computer and then use a tool to analyze them.

5.4.5 DDNS

On the **Network -> DDNS** interface, users can use UC8000 as a dynamic domain name client to map the IP address of the network to the domain name server.

DDNS is to map the dynamic IP address to a static domain name server, and the client program will update the currently obtained dynamic IP address to the domain name resolution when the user connects to the network.

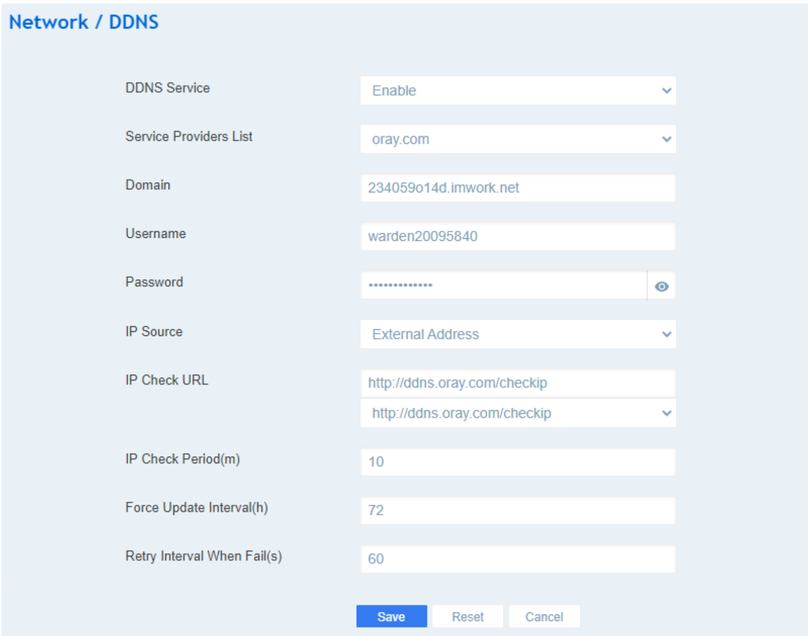


Figure 5.4.5 Dynamic Domain Name

Table 5.4.5 Explanation of DDNS Parameters

DDNS Service	Users can choose enable or disable.
Service Providers List	Dynamic domain name service providers.
Domain	Domain name applied for on the service provider website.
Username	The username when applying for a domain name on the service provider website.
Password	The password when applying for a domain name on the service provider website.
IP Source	The external address and the device address can be selected, the external address is the current network export public network IP address, and the device address is the GE0 port IP address.
IP Check URL	Server address that detects whether the IP address is updated.
IP Check Period(m)	Check whether the IP address has changed detection period.
Force Update Interval(h)	Force update within the configured time interval and report the IP address to the DDNS server.
Retry Interval When Fail(s)	Set the retry interval when updating the IP address fails.

5.4.6 Static Route

On the **Network -> Static Route** interface, users can configure static routes for the network.

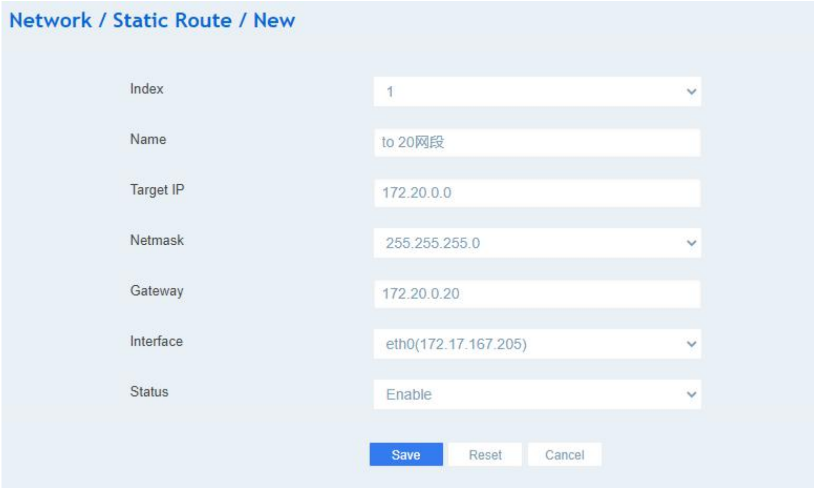


Figure 5.4.6 Create Static Route

Table 5.4.6 Explanation of Static Route Parameters

Index	Users can select indexes 1-10.
Name	The name of the static route.
Target IP	The destination IP address of the static route.
Netmask	The netmask of the static route, default: 255.255.255.0
Gateway	The IP address of the outbound UC8000 IPPBX of the static route.
Interface	The exit of the static route automatically identifies.
Status	The static route is enabled or disabled.

5.4.7 Fail2ban

On the "**Network -> Fail2ban**" interface, users can configure rules for Fail2ban. Fail2ban generally targets SIP.

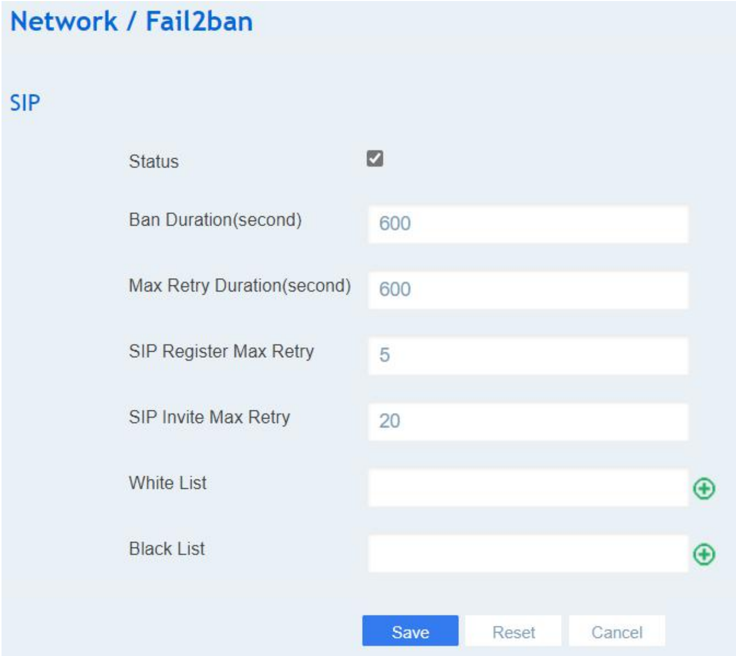


Figure 5.4.7 Fail2ban Rules

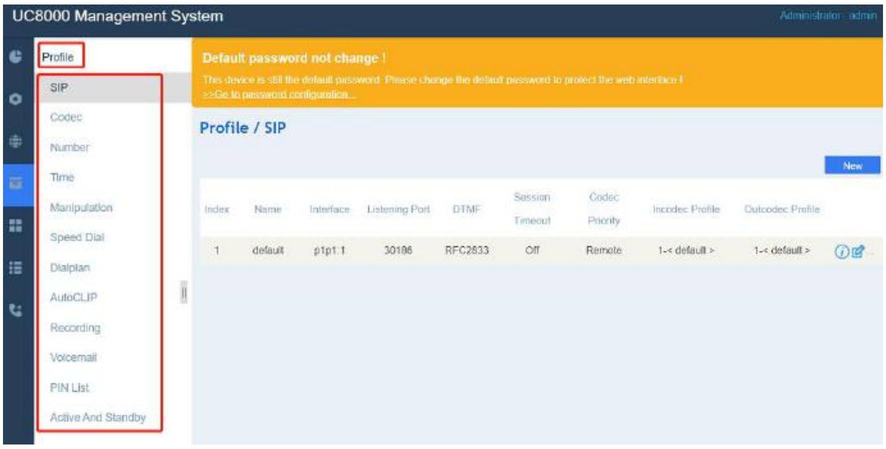
Table 5.4.7 Explanation of Fail2ban Parameters

Ban Duration (Second)	The time period during which the IP addresses that conform to the banning rule or are in the backlist are prohibited. Range: 60-315360000
Max Retry Duration(second)	The time period during which the maximum retries have been executed and then the corresponding IP address will be banned. For example, if this parameter is set as 60 seconds and the maximum number of retries is set as 10, an IP address will be banned in case that it has tried 10 times during 60 seconds. Range: 5-3600
Max Retry	The maximum number of retries during a specific time. For example, if this parameter is set as 10 and the max retry duration is set as 60 seconds, an IP address will be banned in case that it has tried 10 times during 60 seconds. Range: 5-3600
White List	Those IP addresses that are on the white list will not be banned by Fail2ban.
Black List	Those IP addresses that are on the black list will be banned by Fail2ban.

Note： If the SIP sent by an IP has an exception such as "The network is reachable but not responding", users can go to the **Status -> Fail2ban** interface to check whether the IP address is banned or not.

5.5 Profile

The Profile menu includes the following sub-menus: SIP, codec, number, time, manipulation, speed dial, dialplan, AutoCLIP, recording, voicemail, PIN list, active and standby.



5.5.1 SIP

On the **Profile -> SIP** interface, users can set SIP information such as listening port, which will be used in extension and trunk. Up to eight SIP profiles can be configured for a UC8000 system, so users can choose different SIP profiles according to different requirements.

Note: The UC8000 does not provide a default SIP profile configuration, users need to create a profile at Profile /SIP first when using the PBX function.

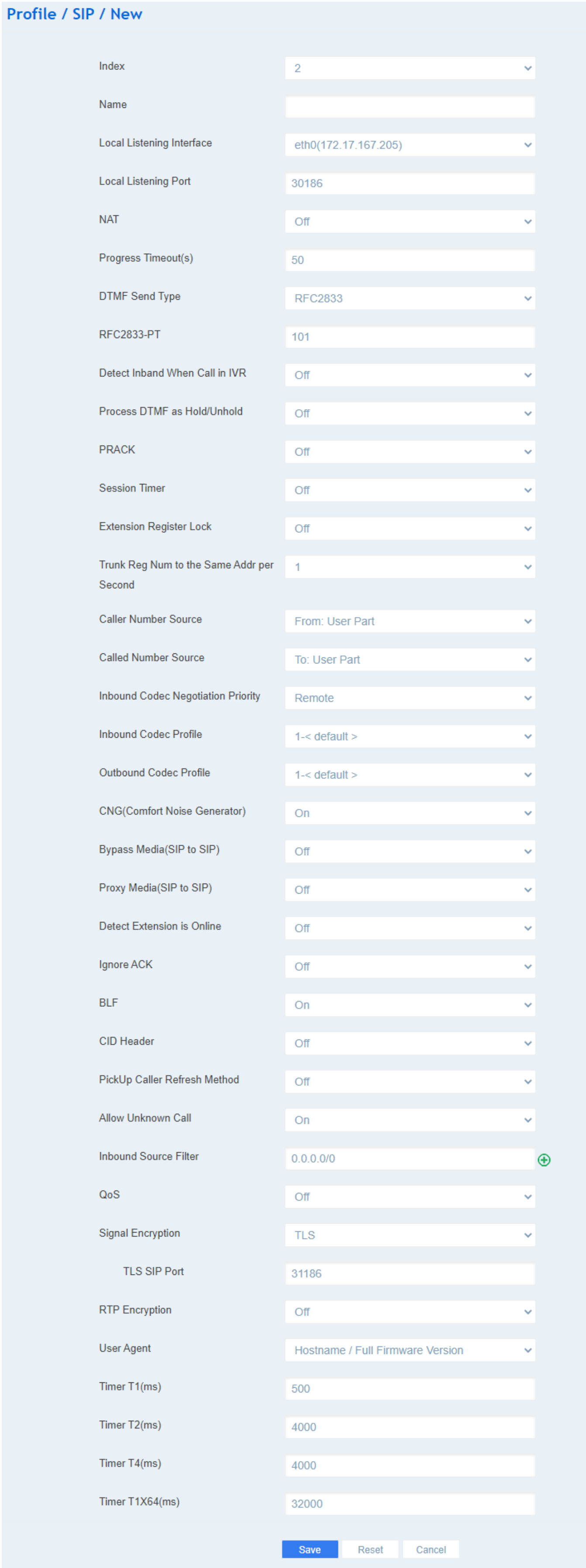


Figure 5.5.1 SIP Profile

Table 5.5.1 Explanation of SIP Profile

Name	The name of the SIP profile. Text input cannot be empty, maximum 32 characters, cannot contain double quotes.
Local Listening Interface	The local listening interface of this SIP profile. Display the floating IP address when the active and standby function is enabled.
Local Listening Port	The local listening port of this SIP profile. If the SIP profile is used by a SIP trunk, the port filled in here is the listening port for the SIP trunk.
NAT	NAT configuration of SIP messages, optional IP address, stun, dynamic domain name, rport, off, used to solve the problem of voice calls in NAT environment; this configuration should be configured by professionals.
Progress Timeout(s)	If the parameter is set as 50 seconds, it means that the call will be considered as timeout in case that no one answers the call during 50 seconds.
DTMF Send Type	DTMF is short for Dual Tone Multi Frequency. There are three DTMF modes, including SIP Info, INBAND, RFC2833.
RFC2833-PT	RFC2833 payload coding.
Detect Inband When Call in IVR	After enabling, the DTMF sent by the caller inband is supported in the IVR.
Process DTMF as Hold/Unhold	By default, this parameter is off. When it is set as on, DTMF will be addressed as call hold/unhold.
PRACK	Provisional Response ACKnowledgement.
Session Timer	**Session Expires**: The validity period of a SIP session. When a SIP session times out, an invite message needs to be sent to refresh the session, otherwise, the session ends; It is 1800 seconds by default **Min Session Expires**: the minimum validity period to respond to a SIP session.

	Session Refresh Method: re-INVITE or UPDATE
Extension Register Lock	When enabled, only the first successfully registered client is allowed to register.
Trunk Reg Num to the Same Addr per Second	When multiple trunks are registered at the same address, please set the interval for sending register messages during registration.
Caller Number Source	**From: User Part**: to obtain the caller number from the user part contained in the 'From' field. **From: Display Name**: to obtain the caller number from the display name contained in the 'From' field. **To: User Part**: to obtain the caller number from the user part contained in the 'To' field. **Contact: User Part**: to obtain the caller number from the user part contained in the 'Contact' field.
Called Number Source	**From: User Part**: to obtain the called number from the user part contained in the 'From' field. **From: Display Name**: to obtain the called number from the display name contained in the 'From' field. **To: User Part**: to obtain the called number from the user part contained in the 'To' field. **Contact: User Part**: to obtain the called number from the user part contained in the 'Contact' field.
Inbound Codec Negotiation Priority	To take the remote device or the local device as priority for inbound codec negotiation. Assume local device supports PCMA, PCMU, G.729 and G.723, while the remote device supports G.723 and G.729 If remote device is taken as codec negotiation priority, G.723 will be the codec mode, since the remote device supports G.723 and G.729 and G.723 is prior to G.729
Inbound Codec Profile	The codec supported by SIP for inbound calls.
Outbound Codec Profile	The codec supported by SIP for outbound calls.
CNG (Comfort Noise	This function is used to generate background noise for

Generator)	the call when there is a short silence during the call, which sounds very comfortable.
Inter SIP Call Enable Media Bypass	Whether to allow inter SIP calls media to communicate directly, bypassing the server.
Inter SIP Call Enable Proxy Media	Whether to allow inter SIP calls to be communicated by profile proxy media addresses.
Detect Extension is Online	Whether to detect the SIP extension using this SIP profile is online or not.
Ignore ACK	After enabling, the gateway will not retransmit *200 OK* if the remote end does not send an ACK, otherwise it will retransmit at intervals.
BLF	After enabling, you can monitor the working status of other extension through the preset indicator lights on a specified extension. The indicator lights will show different states according to the status of the monitored number.
CID Header	Add the CID header to the invite message sent by UC8000 IPPBX.
Allow Unknown Call	If this function is enabled, incoming calls from unknown sources are allowed. Unknown sources are those IP addresses that do not fall into the source range configured for SIP trunks or SIP extensions.
Inbound Source Filter	The source of inbound calls, which is allowed. It can be an IP address or a network segment. If it is a network segment, the format is 172.16.0.0/16 or 172.16.0.0/255.255.0.0, which means calls from the network segment of 172.16 are allowed to come in. 0.0.0.0 means calls of any source are allowed to come in.
QoS	Whether to enable QoS. QoS is a technology used to solve network delays or congestion.
Signal Encryption	After enabling, the UC8000 IPPBX will transmit signaling via TLS.

RTP Encryption	Select encrypted SRTP for RTP stream transmission. SRTP is a secure real-time transmission protocol to ensure the security of voice communication, SRTP is a secure real-time transmission protocol to ensure the security of voice communication.
User Agent	Then content of the 'user agent' field in SIP packets.
Timer T1	The value of timer T1 in SIP protocol. Default value is 500ms.
Timer T2	The value of timer T2 in SIP protocol. Default value is 4000ms.
TimerT4	The value of timer T4 in SIP protocol. Default value is 5000ms.
Timer T1X64 (ms)	The value of timer T1X64 in SIP protocol. Default value is 32000ms.

Description for SIP server

SIP server is the main part of the VoIP network, responsible for establishing all SIP calls. SIP server is also called SIP proxy server or registration server. Depending on the specifications, IPPBXs, softswitches can act as SIP servers. and UC8000 is set in the Extension->SIP interface to act as this role.

Note: For more details on how to configure SIP server, please refer to 5.7.1

5.5.2 Codec

At present, UC8000 supports voice codec and video codec, including G729, G723, PCMU PCMA, and all voice codecs and video codecs are enabled in the default configuration. Users can also group and prioritize any of the 16 codecs according to their requirements.

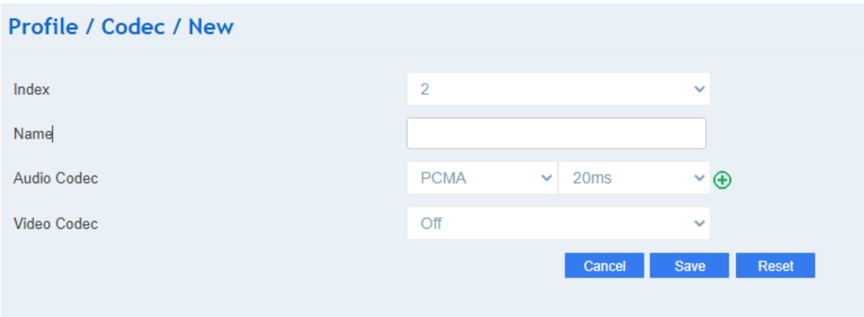


Figure 5.5.2 Add or Delete Codec Profile

5.5.3 Number

On the **Profile -> Number** interface, users can set a prefix for caller numbers or called numbers. When the prefix of a caller number or a called number matches the set prefix, the call will be passed to choose a route.

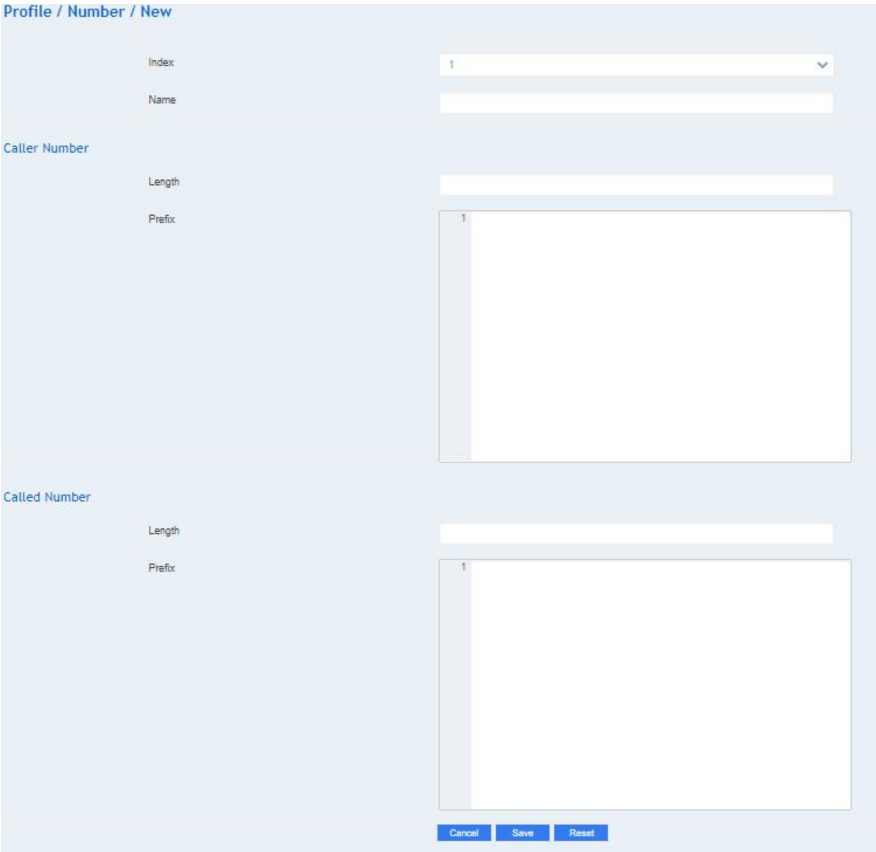


Figure 5.5.3 Create Number Profile

Table 5.5.3-1 Explanation of Number Parameters

Name	The name of the profile number.
Prefix of Caller Number	The prefix of the caller number. It supports multiple prefixes, multiple rules for "or" relationships. It supports the regular expression.
Prefix of Called Number	The prefix of the called number. It supports regular expression. It supports multiple prefixes, multiple rules for "or" relationships.
Length	The length of the caller number or called number. For example, : 4|6|7 means the caller number or called number must be 4 digits, 6 digits or 7 digits except the prefix.

Regex (Regular Expression) Syntax

Table 5.5.3-2 Explanation of frequently-used metacharacters in Regex

^	Matches the starting position in a number string. For example, ^134 matches the numbers starting with 134
$	Matches the ending position of a string. For example, 2$ matches the numbers ending with 2.
|	Separates alternate possibilities. For example, 2|3|4 means 2,3or 4.
\	Marks the next character as a special character, a literal, a backreference, or an octal escape
[ ]	Matches a single character that is contained within the bracket. For example, [123] matches 1, 2, or 3. [0-9] matches any digit from "0" to "9".
[^]	Matches any one character except those enclosed in [ ]. For example, [^9] matches any character except 9.
.	Matches any single character except the newline character. For example, 3.4 matches 314, 324, 334, 344.
?	Indicates there is zero or one of the preceding element. For example, colou?r matches both color and colour.
*	Indicates there is zero or more of the preceding element. For example, ab*c matches ac, abc, abbc, abbbc, and so on.
+	Indicates there is one or more of the preceding element. For example, ab+c matches abc, abbc, abbbc, and so on, but not ac
\d	Mark any digit, equal to [0-9]
\D	Mark any character that is not a digit, equal to [^0-9]
\s	Mark any blank character such as a space or a tab.
\S	Mark any character that is not a blank character.

Examples:

^0755	Matches the phone numbers with starting digits of 0755.
^0755|^8899|^01	Matches the phone numbers with starting digits of 0755, 8899 or

10	0110.
^[1][358][0-9]{9}$	Matches the phone numbers with the first digit as 1, the second digit as 3, 5 or 8, the left nine digits as any of 0 to 9.

Note: The matching of number prefix also supports some digits that do not conform to the format of regular expression. For example, 0755 matches the numbers starting with 0755, and 0755|8899|0110 matches the numbers starting with 0755, 8899 or 0110.

5.5.4 Time

On the **Profile -> Time** interface, users can set a time period for calls to choose routes. If the local time when a call is initiated falls into the set time period, the call will be passed to choose the corresponding route.

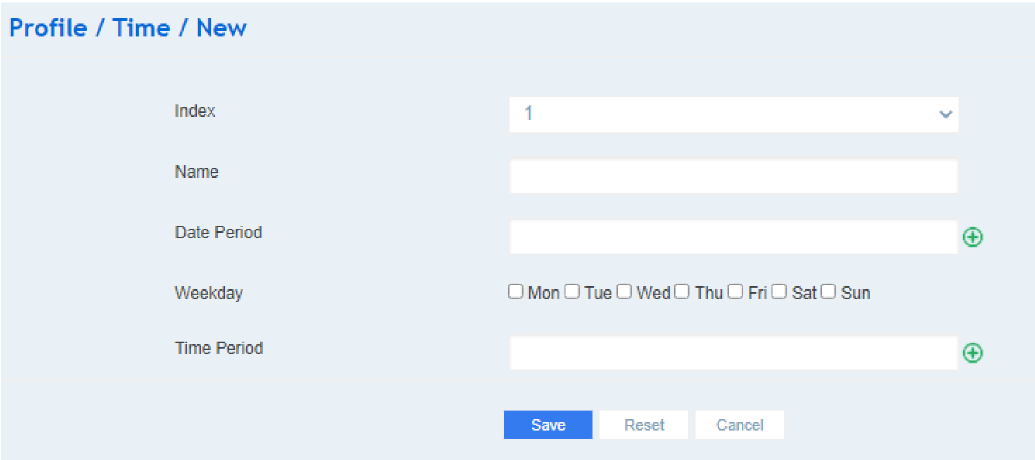


Figure 5.5.4 Time Profile

Table 5.5.4 Explanation of Time Parameters

Index	Users can choose indexes 1-32.
Name	The name of the profile number.
Date Period	Configure the starting date and ending date of a period. "+": Add a date period. "x": Delete a date period.
Weekday	Users can choose a weekday.
Time Period	Users can choose the starting time and ending time of a day.

5.5.5 Manipulation

Number manipulation refers to the change of a called number or a caller number during the calling process, when the called number or the caller number matches the preset rules.

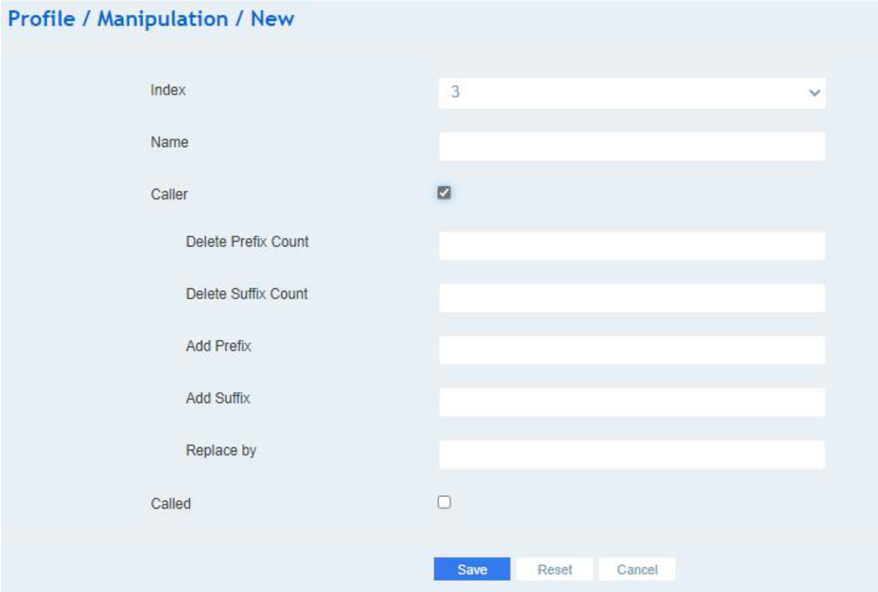


Figure 5.5.5 Create Manipulation Profile

Table 5.5.5 Explanation of Manipulation Parameters

Name	The name of this manipulation profile.
Delete Prefix Count	The number of digits that are deleted from the left of the caller number or calling number.
Delete Suffix Count	The number of digits that are deleted from the right of the caller number or calling number.
Add Prefix	The prefix is added to the caller number or the calling number.
Add Suffix	The suffix is added to the caller number or the calling number.
Replace by	The number which replaces the caller number or the calling number.
	If the checkbox on the right of Caller is selected, it means the caller number will be manipulated; if the checkbox on the right of called is selected, it means the called number will be manipulated.

Note: During number manipulation, deletion rules are carried out first, followed by adding rules. If ‘Replace by’ has been set, deletion rules and adding rules are invalid.

5.5.6 Speed Dial

On the **Profile -> Speed Dial** interface, users can configure the correspondence between short and long numbers. For example, if the short number (speed dial number) is set as 1, the long number is set as 8000, and this speed dial profile is applied to an SIP extension, the SIP extension only needs to dial 1 and the call will be directed to the extension number of 8000.

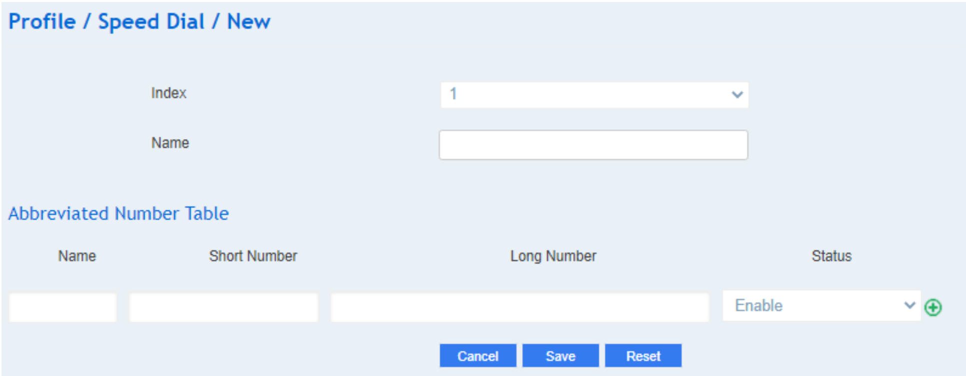


Figure 5.5.6 Add Speed Dial Profile

Table 5.5.6 Explanation of Speed Dail Parameters

Index	Numbering of speed dial rules; drop-down selection, 1-32.
Name	Name of speed dial rule; text input cannot be empty, less than 32 characters.
Abbreviated Number Table	Short numbers and long numbers correspond to the abbreviated number table, can add more than one, the maximum add 104.
Name	Name of the abbreviated number table; text input can be empty, less than 32 characters.
Short Number	Short number configuration; text input, support numbers 0-9/*/#, maximum support 2 characters.
Long Number	Short numbers corresponding to long numbers; text input, only numbers, less than 32 characters.

5.5.7 Dialplan

Dialing rules are used for dialing settings when an extension call occurs. It supports Regular Expression (Regex) and DigitMap.

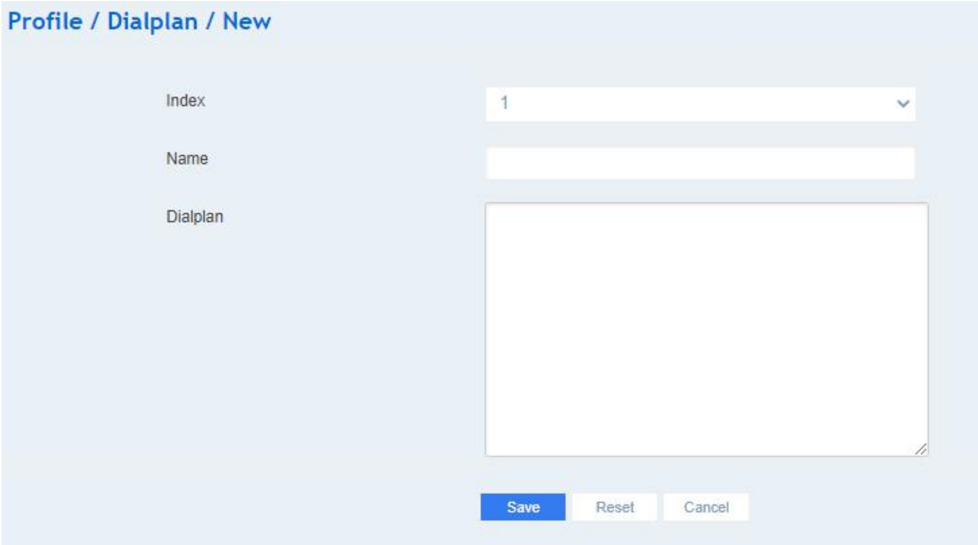


Figure 5.5.7 Add Dialplan

Regex (Regular Expression) Syntax

<table>
<tr><td>^</td><td>Matches the starting position in a number string. For example, ^134 matches the numbers starting with 134.</td></tr>
<tr><td>$</td><td>Matches the ending position of a string. For example, 2$ matches the numbers ending with 2.</td></tr>
<tr><td>|</td><td>Separates alternate possibilities. For example, 2|3|4 means 2,3or 4.</td></tr>
<tr><td>\</td><td>Marks the next character as a special character, a literal, a backreference, or an octal escape.</td></tr>
<tr><td>[ ]</td><td>Matches a single character that is contained within the bracket. For example, [123] matches 1, 2, or 3. [0-9] matches any digit from "0" to "9".</td></tr>
<tr><td>[^]</td><td>Matches any one character except those enclosed in [ ]. For example, [^9] matches any character except 9.</td></tr>
<tr><td>.</td><td>Matches any single character except the newline character. For example, 3.4 matches 314, 324, 334, 344.</td></tr>
<tr><td>?</td><td>Indicates there is zero or one of the preceding element. For example, colou?r matches both color and colour.</td></tr>
<tr><td>*</td><td>Indicates there is zero or more of the preceding element. For example, ab*c matches ac, abc, abbc, abbbc, and so on.</td></tr>
</table>

+	Indicates there is one or more of the preceding element. For example, ab+c matches abc, abbc, abbbc, and so on, but not ac.
/d	Mark any digit, equal to [0-9]
/D	Mark any character that is not a digit, equal to [^0-9]
/s	Mark any blank character such as a space or a tab.
/S	Mark any character that is not a blank character.

Examples of Regex Syntax:

^0755	Matches the phone numbers with starting digits of 0755.
^0755|^8899|^0110	Matches the phone numbers with starting digits of 0755, 8899 or 0110.
^[1][358][0-9]{9}$	Matches the phone numbers with the first digit as 1, the second digit as 3, 5 or 8, the left nine digits as any of 0 to 9.

DigitMap Syntax:

Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *
Range	[ ]	One or more DTMF symbols enclosed in the [], but only one DTMF symbol can be selected
Range	()	One or more expressions enclosed the (), but only one can be selected
Separator	|	Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by hyphen (-) which matches any digit between and including the two digits.
Wildcard	x	Matches any digit of 0 to 9

Modifiers	.	Matches 0 or more times of the preceding element
Modifiers	?	Matches 0 or 1 times the preceding element

Examples of DigitMap Syntax

(13 | 15 | 18)xxxxxxxxx	Matches the phone numbers with stating digits as 13, 15 or 18 and the left nine digits as any of 0 to 9.
[2-8] xxxxxx | 13xxxxxxxxx	Matches the phone numbers starting with any digit of 2 to 8 and the left six digits as any of 0 to 9; or matches the phone numbers starting with 13 and the left nine digits as any of 0 to 9.

5.5.8 AutoCLIP

AutoCLIP mainly applies to SIP trunk calls. According to the configured rules, users can record the inbound and outbound information of trunk.

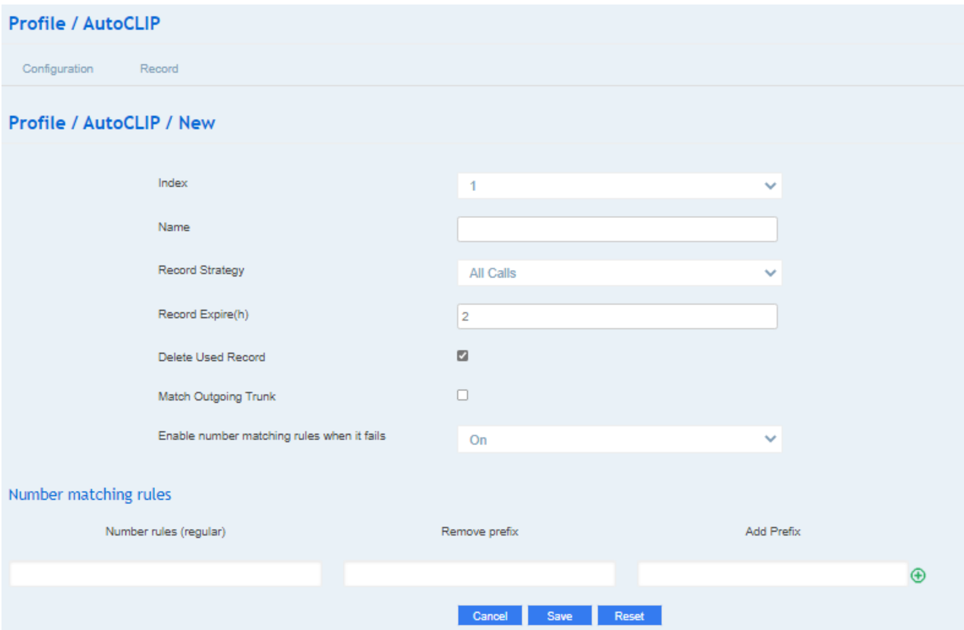


Figure 5.5.8 AutoCLIP

Table 5.5.8 Explanation of AutoCLIP Rule

Index	The index of AutoCLIP profile. Range: 1-32
Name	The name of AutoCLIP profile. Text input cannot be empty, up to 32 characters and cannot contain double quotes.

Record Strategy	Users can choose missed calls or all calls. If missed calls are selected, UC8000 will record the missed calls of the trunk; If all calls are selected, all the calls going through the trunk will be recorded.
Record Expire (hour)	The validity period of a record. For example, if this parameter is set as 2 hours, the record will be valid in 2 hours since the record is generated. During the validity period, if there is coming call for the extension number contained in the record, the call will directly led to the extension without routing.
Delete Used Record	By default, this parameter is disabled. If this parameter is selected, those records that have been used to match extension number or trunk will be deleted.
Match Outgoing Trunk	By default, this parameter is enabled. If this parameter is enabled, those calls going through the trunks in the record can coming in without routing.
Enable Number Matching Rules When It Fails	Enable number matching rules.

5.5.9 Recording

How to Record Calls:

Configure a recording profile (choose one of the two default recording profiles), and then add it to a SIP route. When there are calls going through the route and match the recording profile, the calls will be recorded.

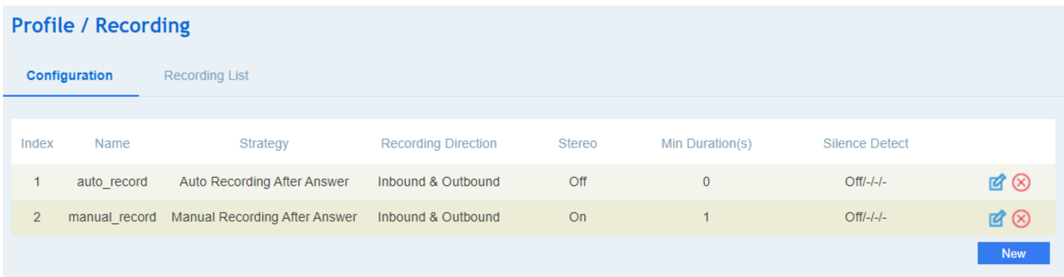


Figure 5.5.9-1 Add Recording Profile

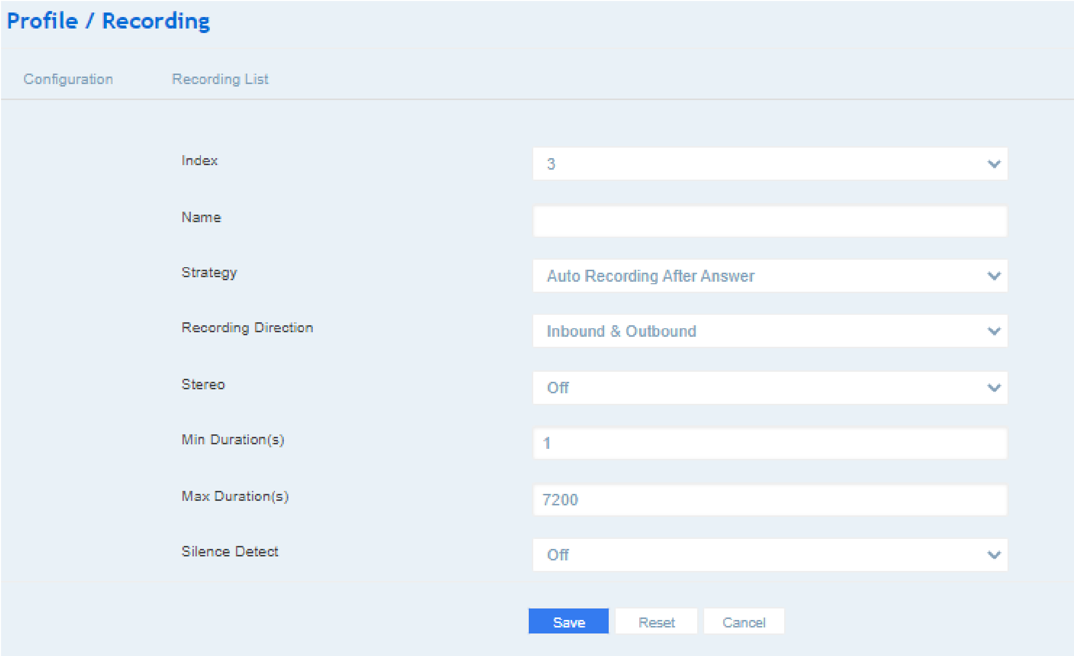


Figure 5.5.9-2 Recording

Table 5.5.9 Explanation of Recording Profile

Index	The index of the recording profile. Range: 1-32
Name	The name of the recording profile; Text input cannot be empty, up to 32 characters and cannot contain double quotes.
Strategy	Auto Recording after Answer: start recording after the callee pick up the phone. Ban Recording: ether caller or callee enables his function, and then the call in both directions will not be recorded. Manual Recording after Answer: press *3 to start recording after the callee answers the call.
Recording Direction	Inbound & Outbound: If this recording profile is added to SIP extension, both inbound and outbound calls will be recorded. Inbound: If this recording profile is added to SIP extension, only inbound calls will be recorded. Outbound: If this recording profile is added to SIP extension, only outbound calls will be recorded. Note: If this recording profile is added to routing, this parameter is invalid and all calls going through the routing will be recorded.
Stereo	When enabled, the file size will be twice that of mono for the

	same call duration.
Min Duration	If the actual recording time is shorter than this value, the recording file will not be saved.
Silence Detect	When silence is detected, no recording will be done during muting.

Users can click **Recording List** to view the recording files which show the caller/called number, recording duration and so on. Users can also play, download or delete the recording files on this interface.

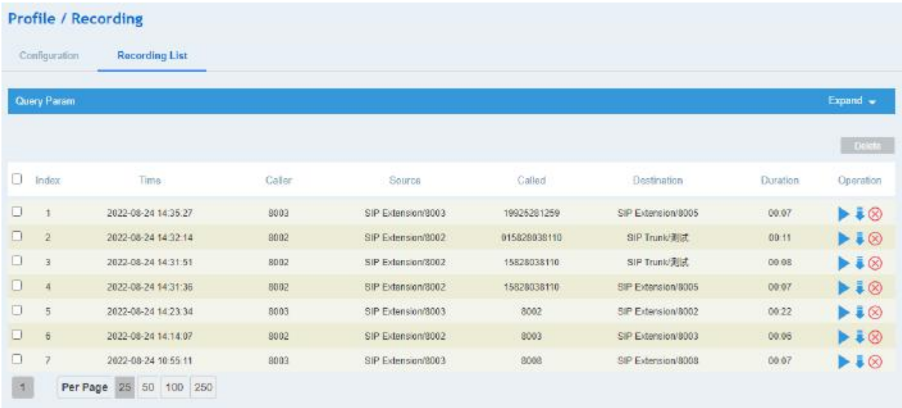


Figure 5.5.9-3 View Recording List

5.5.10 Voicemail

On the **Profile -> Voicemail** interface, users can configure the location, number and duration of a voicemail.

How to use voicemail:

Navigate to **SIP -> Extension** interface, enable the voicemail function, and the voicemail will be activated when the call times out.

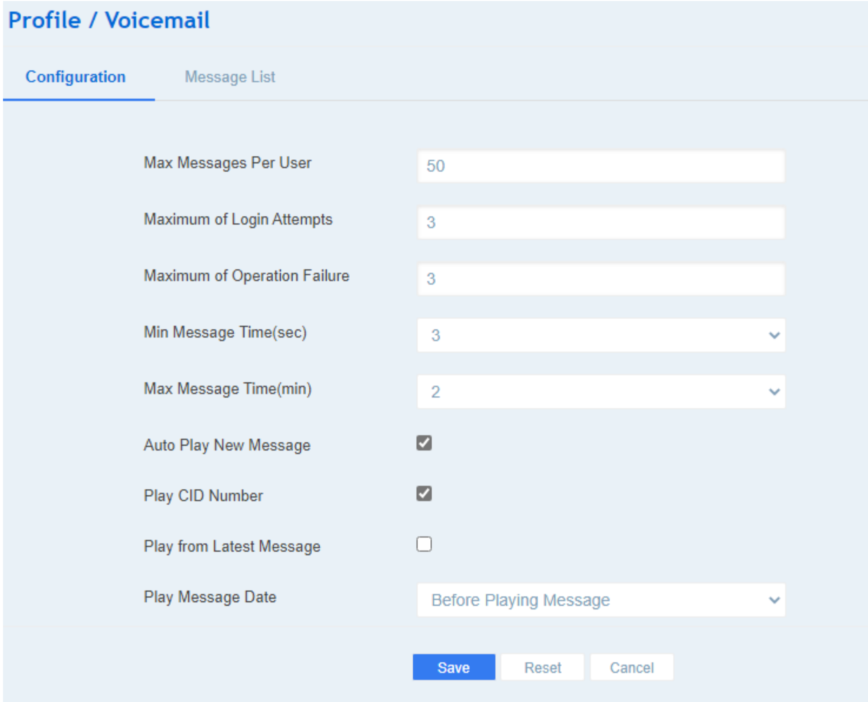


Figure 5.5.10-1 Voicemail Profile

Table 5.5.10 Explanation of Voicemail Profile

Max Message Per User	If this maximum number of messages is reached, a prompt voice “the mail box is full” will be played.
Maximum of Login Attempts	If this maximum number of attempts (by dialing *170*2 to log in the voice mailbox) is reached, the call will hang up.
Maximum of Operation Failure	When a call enters into the voice mailbox and the caller dial inexistent DTMF repeatedly, the caller will be forced to log out the voice mailbox after the repetition times exceed this value.
Min Message Time (second)	The minimum duration of a voicemail
Max Message Time (second)	The maximum duration of a voicemail.
Auto Play New Message	If this parameter is on, new messages will be played automatically. If it is off, a prompt voice “please dial 1 to listen to new message” will be given.

Play CID Number	If this parameter is on, the caller number will be played together with messages.
Play from Latest Message	If this parameter is on, the latest messages will be played first.
Play Message Date	When to play message date. You can choose 'Before Playing Message', 'After Playing Message' and 'Never'.

Users can click **Message List** to view the voicemail files which show the caller/called number, message duration and so on. Users can also play, download or delete the message files on this interface.

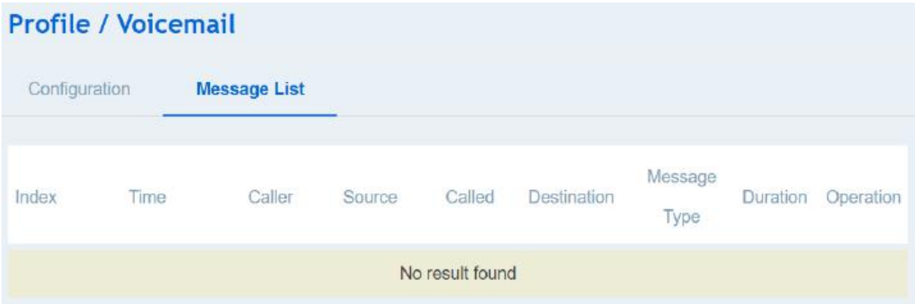


Figure 5.5.10-2 View Message List

5.5.11 PIN List

Users can configure the PIN code as needed, which is used to verify based on the matching PIN code when routing outbound calls, serving as a secure call.

PINs can be created either individually in a route or as a collection of PINs. Create a list of PIN collections as follow.

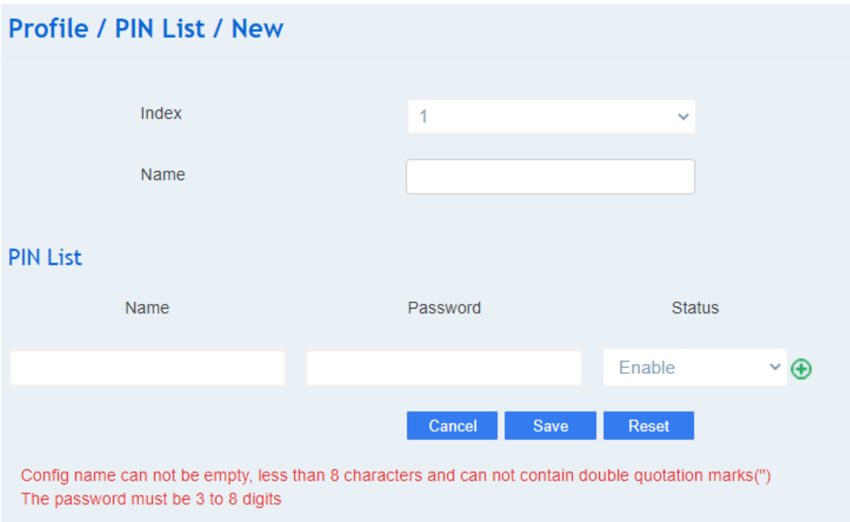


Figure 5.5.11 Create PIN List

Table 5.5.11 Explanation of PIN List Parameters

Name	The name of this PIN configuration, used to identify.
PIN List Name	The name of the password, which is used to distinguish who uses it.
Password	PIN code password.
Status	Disable/Enable status of this PIN code.

5.5.12 Active and Standby

In order to ensure that the UC8000 can work normally and stably, the UC8000 adds a double-device Hot Standby function.

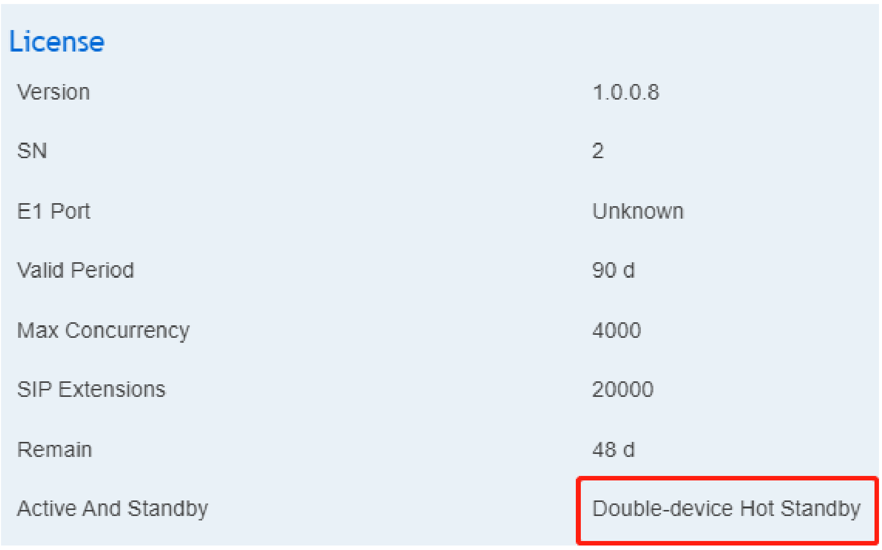
Users can configure two UC8000s of the same version, configuration, environment or similar as active and standby with a floating IP address. Under normal circumstances, management and call data are transmitted to the active via the floating IP address. When the active fails, it will switch to standby in time, which greatly guarantees the stable operation of UC8000.

I. Active and Standby configurations

Prerequisites:

The active/standby function of UC8000 is hidden and cannot be configured on the web. If users need to use this function, they need to apply for the corresponding license from dinstar.

On the **"Status->About"** interface, the feature is available when the active and standby is shown as Double-device Hot Standby, and is not available when it is displayed as other.



Operation steps.

- Prepare two hosts of similar configuration UC8000-A and UC8000-B, and follow the same steps to install and debug the UC8000 program.
- Load the license information that includes the Double-device Hot Standby feature, and restore factory settings on both UC8000s.
- Login to the UC8000-A web page, enter the Active and Standby configure information on the Active And Standby Profile.

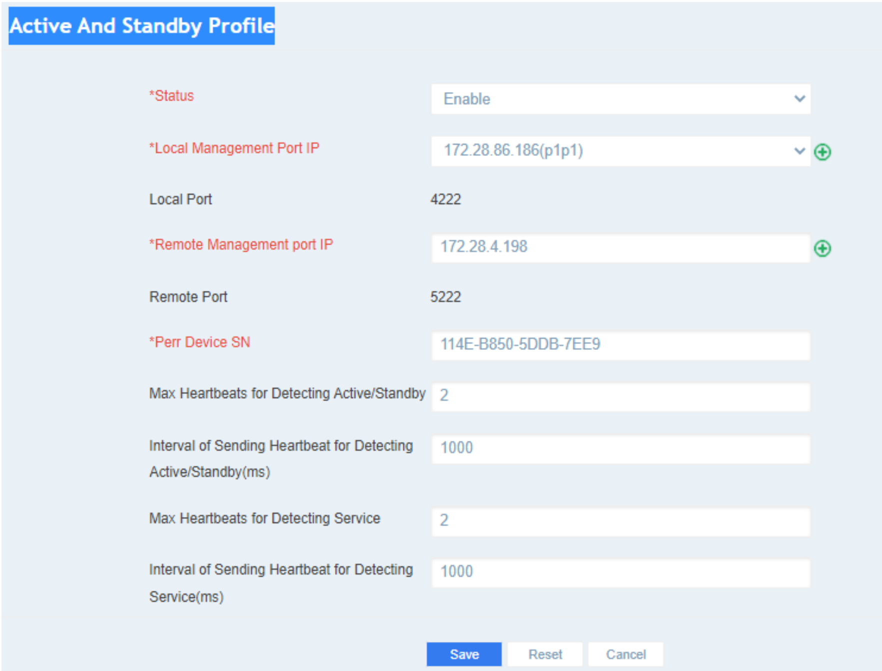


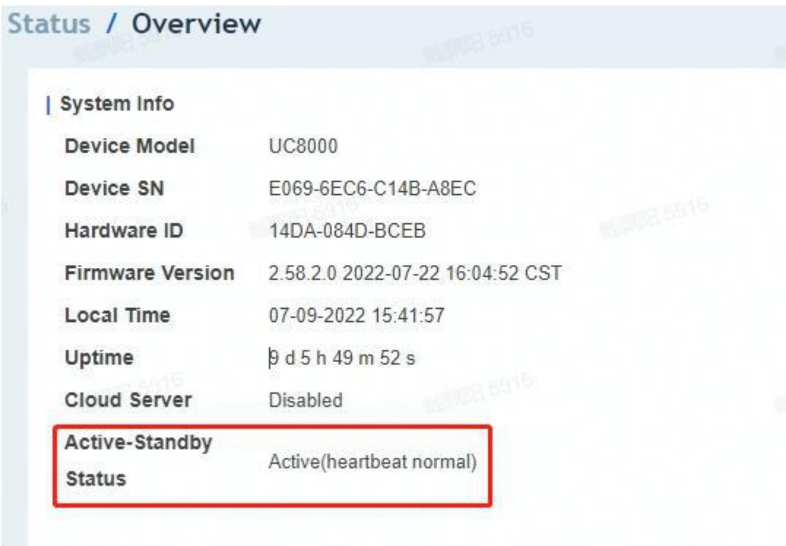
Figure 5.5.12 Enter the Active and Standby configuration information

Table 5.5.12-1 Explanation of the Active and Standby configuration parameters

Status	Enable/disable, turn on or off the active/standby function.
Local Management Port IP	Local management IP address, associated with the network interface of the physical machine.
Local Port	Local listening port, fixed 4222.
Remote Management Port IP	Remote management IP address.
Remote port	Port for sending management messages to the remote end, fixed 5222.
Per Device SN	Serial number of the peer device, available on the

	Status/About page of the peer device.
Maximum number of Active And Standby heartbeats	The maximum number of consecutive lost heartbeats between the dual-machine Active And Standby, default: 2, configurable from 2-100.
Interval of Sending Heartbeat for Detecting Active/Standby(ms)	The length of the heartbeat interval between active and standby, default is: 100, configurable from 100 to 1000.
Max Heartbeats for Detecting Service	Maximum number of consecutive losses of double-device service heartbeats, default: 2, configurable from 2-100.
Interval of Sending Heartbeat for Detecting Service(ms)	The length of the heartbeat interval of the double-device service, default: 100, configurable from 100 to 1000.

- Log in to the UC8000-B web page and enter the Active/Standby configuration information as described in previous step.
- The UC8000-A and UC8000-B are both configured with the same floating IP address.
- After the Active/Standby configuration and floating IP address are saved and applied, wait a few seconds. In the status/overview interface users can see the status of the active and standby: the active (heartbeat is normal) or the standby (heartbeat is normal) indicates the successful configuration of the active and standby.



Note: When two UC8000s are first configured for active and standby configuration, the device serial number is used to calculate and select the one active and one standby.

II. Network port detection

The network port detection only takes effect when the active/standby configuration is enabled, and is used in conjunction with switching rules. The UC8000 intelligently selects the one with higher weight as the host when the network may fail for some reason.

Prerequisites:

When the physical machine where the UC8000 is located has two or more network ports, network port detection function can be configured according to the actual situation; If it has only one network port, then no configuration is required.

Both the active and the standby need to configure network port detection and switching rules.

Operation steps:

- On the Profile/Active and Standby/Network Port Detection interface, create new detection entries for the network interfaces as appropriate.

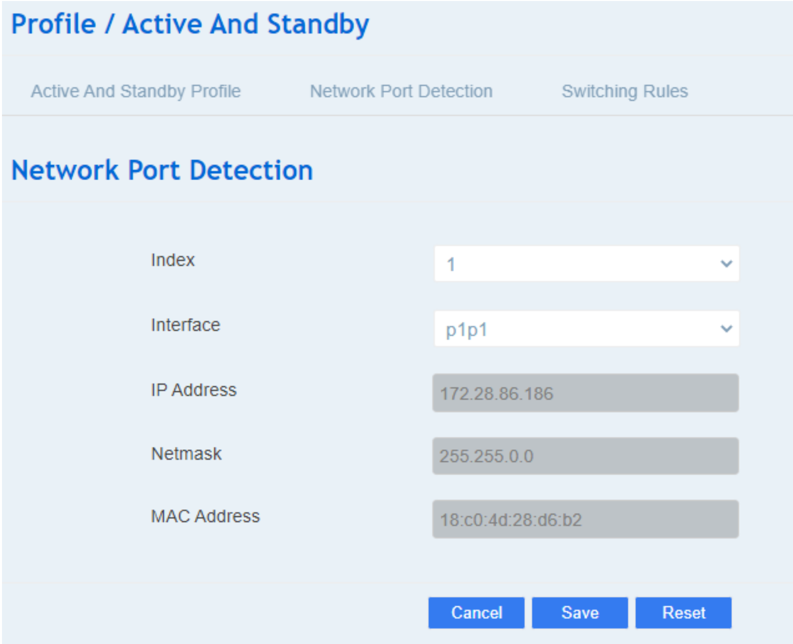
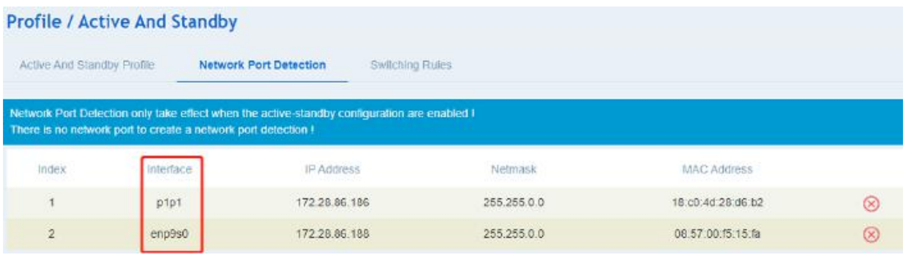


Table 5.5.12-2 Explanation of the Network port detection configuration parameters

Index	Net port detection entry number.
Interface	Select the network interface to be detected by the new network port, associated with the network interface of the physical machine.
IP Address	Automatic recognition of the IP address of the network interface without configuration.
Netmask	Automatic recognition of the Netmask of the network interface without configuration.
MAC Address	Automatic recognition of the MAC address of the network interface without configuration.

- Create separate network port detection entries for the corresponding network interfaces according to the current situation and requirements.



- With the same interface, only one network port detection entry can be created, the UC8000 automatically recognizes, after the creation of full cannot new creation.
- After creating a workable network port detection, use it in conjunction with the

switching rules.

III. Switching Rules

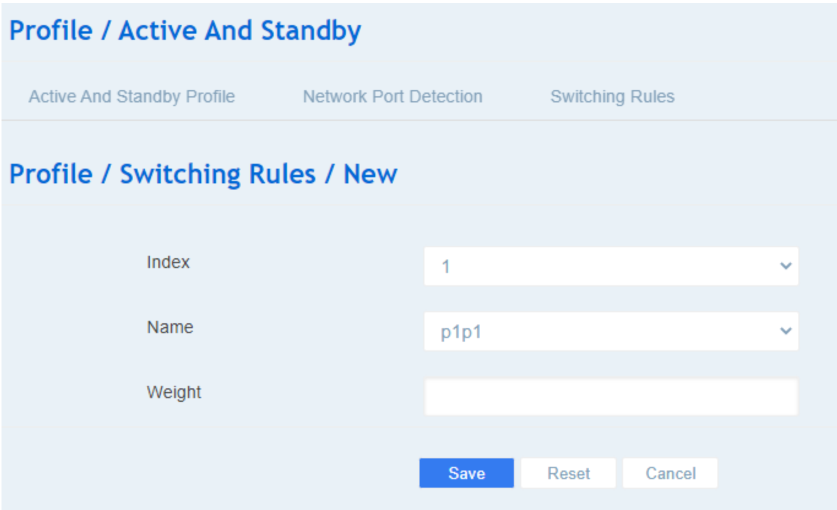
The switching rule takes effect only when the active and standby configuration is enabled. The higher the value, the higher the weight for that network port.

Prerequisites:

A network port detection entry has been created for the network port.

Operation steps:

- On the Profile/Active and Standby/Switching Rules Detection interface, new switching rules.



- Configure different weight for different network interfaces, with optional weight: 1-10.
- After configuring the network port detection and switching rules on both the active and the standby, save the application.

Instructions for using the network port detection and switching rules.

Under normal circumstances, the difference between the total weight of all network ports of the active and the total weight of all network ports of the standby is less than 10; When the active is dropped, then its weight is 0; Once the total weight of the active value is less than or equal to the total weight of the standby -10, then the active/standby switchover is triggered, and the standby machine with a stable network port is switched to active.

IV. Services that support active and standby switching

Simultaneous connected calls only	Call switching for the current call page connected works properly.
Configuration file	Call-related configuration files, active and standby

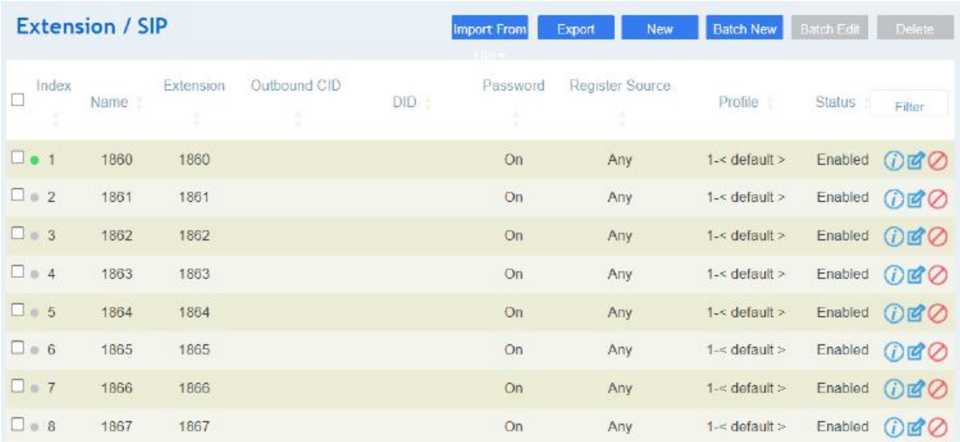
synchronization	synchronized at regular intervals.
Call Queue	Queue configuration synchronization, connected calls, switching works properly.
Fail2ban	Synchronize configurations at 10-minute intervals.
SIP Registration	Sip registration timing synchronization works properly.
Conference	The extension joins the conference and synchronizes to the standby machine, and the conference voice switches normally after the active and standby switch. Active web Mute or kick out action for conference members, can synchronize standby.
Parking Lot	After an active/standby switchover, the resumed session does not support accepting *4 feature codes to handle call parking.
SCA	The configuration can be synchronized to the standby machine.
CDRs	Only the active machine can store the list, not synchronized to the standby machine.
Voice Upload	Real-time synchronization to the standby machine.
Timed tasks	Timed reboot only supports active reboot, the rest of the timed task configurations are synchronized with the standby machine.
AutoClip	Configure the database to synchronize at 10-minute intervals.
Recording	Recording files are not synchronized, only the active recording, the call will not be recorded on standby to the active after switching.
Call back	Configure 10-minute intervals for synchronization.
Phones	Phone /etc/template /www/pnp etc. files are synchronized every 10 minutes.
Ring Group	Configure real-time synchronization to the standby,

	synchronization of calls being made.
Feature Code	Enable to disable call waiting or call forward, enable to disable the synchronization of no disturbance, etc. Voice after call surrogate active/standby switching. The redial database is synchronized at 10-minute intervals.
IVR	Calls received via IVR are synchronized to the standby, and can be voiced after switching.
Emergency Number	Emergency number call synchronization standby.
Follow Me	Simultaneous standby support for calls connected through Follow Me.
Alarm Clock	Active initiates call by alarm policy.
Concurrent count limit	Resumed calls are not counted in the current concurrent count after an active/standby switchover.
Video Synchronization	Normal audio and video call switching requires terminal support.
TLS or TCP	TLS and TCP calls are temporarily unable to resume after an active/standby switchover.
SRTP	SRTP calls are temporarily unable to resume after an active/standby switchover.

5.6 Extension

5.6.1 SIP

On the **Extension -> SIP** interface, users can configure the SIP accounts registered in the UC8000 by SIP clients (UC8000 is regarded as a SIP server). Parameters including: SIP extension name, SIP extension account, password, DID, register source, call waiting, do-not-disturb, call forward (always/no answer/busy) and SIP configuration.



Extension / SIP

Import From | Export | New | Batch New | Batch Edit | Delete

Index	Name	Extension	Outbound CID	DID	Password	Register Source	Profile	Status	Filter
1	1860	1860			On	Any	1-< default >	Enabled	
2	1861	1861			On	Any	1-< default >	Enabled	
3	1862	1862			On	Any	1-< default >	Enabled	
4	1863	1863			On	Any	1-< default >	Enabled	
5	1864	1864			On	Any	1-< default >	Enabled	
6	1865	1865			On	Any	1-< default >	Enabled	
7	1866	1866			On	Any	1-< default >	Enabled	
8	1867	1867			On	Any	1-< default >	Enabled	

Figure 5.6.1-1 Extension List

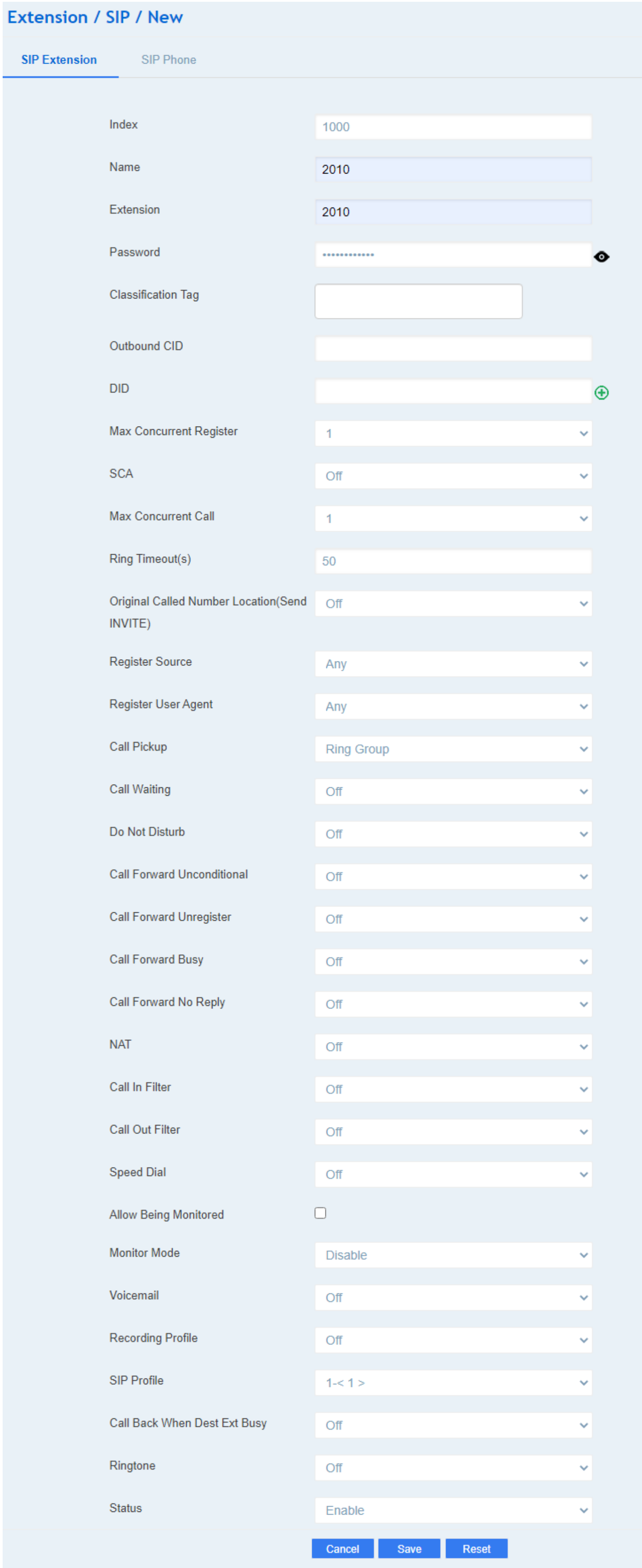


Figure 5.6.1-2 Configure SIP extension

Table 5.6.1 Explanation of SIP Extension Parameters

Name	The name of this SIP extension.
Extension	The SIP account of the extension was registered at UC8000 by a SIP client.
Password	The password of the SIP account was registered in UC8000 by a SIP client.
Classification Tag	Labels for extension classification.
Outbound CID	After the outgoing caller number is configured, the caller number dialed from the SIP extension is replaced with the number configured here.
DID	Direct Inward Dialing; if the called number is same with DID, the call will be directly forwarded to the extension, rather than choosing a route. Users can set multiple DID.
Max Concurrent Register	Number of clients that can register online at the same time.
Max Concurrent Call	The number of concurrent calls that can be made at the same time.
Ring Timeout(s)	The ringing timeout period for incoming calls to this extension, the default value is 50. If the extension does not go off-hook within 50s after ringing, the device will initiate disconnection.
Original Called Number Location (Send INVITE)	When sending INVITE, configure the location of the original called number
Register Source	If 'Any' is chosen, all SIP clients are allowed to register the SIP account of this extension; if ‘Specified’ is chosen, only the SIP client with the specified IP address or network segment is allowed to register the SIP account of this extension. For example, 172.16.0.0/16 means the register source is 172.16

Register User Agent	Filter the user agent field in the register message during registration.
Call Pickup	After configuration, the designated call can be picked up（ring group/local extension, the default is the ring group)
Call Waiting	If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear an IVR voice.
Do Not Disturb	If 'Do Not Disturb' feature is enabled, calls cannot reach the called party.
Call Forward Unconditional	If 'Call Forward Unconditional' feature is enabled, all coming calls will be forwarded to a preset number.
Call Forward Unregister	When the SIP extension is not registered, you can transfer all the calls to the set number.
Call Forward Busy	If 'Call Forward Busy' feature is enabled, new coming call will be forwarded when the corresponding local port is busy.
Call Forward No Reply	If 'Call Forward No Reply' feature is enabled, calls will be forwarded when nobody answer the calls during a specified period.
NAT	If NAT is enabled, the IP address of SIP extension in LAN will be turned into the outbound IP address of public network, thus making NAT traversal possible.
Call In Filter	When you breathe in to SIP, you match the relevant filter conditions.
Call Out Filter	When the SIP is called out, the filter conditions are matched.
Speed Dial	Configuration for Speed dial.

Voicemail	Choose to on or off the voicemail.
Password	Configure the password for logging in to the extension's voicemail.
Message Forward Email	Configure the e-mail address for voice mail messages, and make sure that the e-mail is normal.
Recording Profile	When the corresponding recording rule is selected, SIP extension calls will be recorded according to the corresponding recording rule; drop-down selection, off / rule in "Configure > Recording", default is off.
SIP Profile	The SIP profile that is selected for the extension.
Status	If it is enabled, this SIP extension is registered to UC8000; Otherwise, the SIP extension is not registered.

5.6.2 Phones

On the **Extension -> Phone** interface, users can deliver the configuration to the phone according to the template file. After enabling PNP, the phone will periodically send a subscribe message to the multicast address. If the PBX receives the multicast message, it will list the phone models in the PBX configuration list.

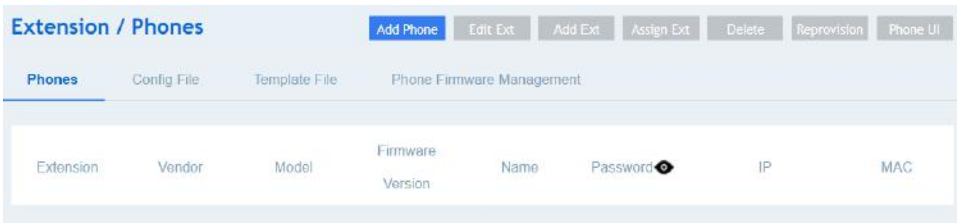


Figure 5.6.2-1 Phones

If the phone is in the configuration list of UC/IPPBX, after selecting, users can assign the phone to an existing extension, or can create a new extension through "Add phone".

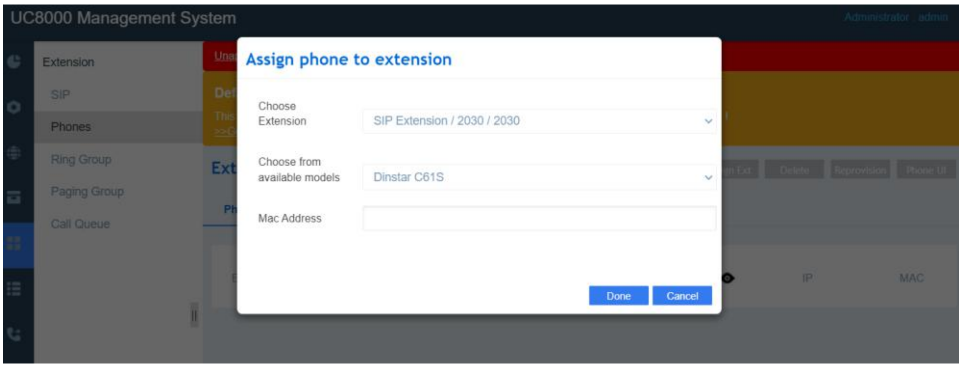


Figure 5.6.2-2 Add phone

At this time, UC will automatically generate a configuration file suitable for the phone model, and send a SIP NOTIFY message to the phone, carrying the download address of the configuration file in the body, and notify the phone to download. After the phone receives it, you can use the assigned extension to register.

5.6.3 Ring Group

On the **Extension ->Ring Group** interface, users can combine multiple SIP extensions and set ringing policies to ring incoming calls according to the set policies, which is widely used in call centers.

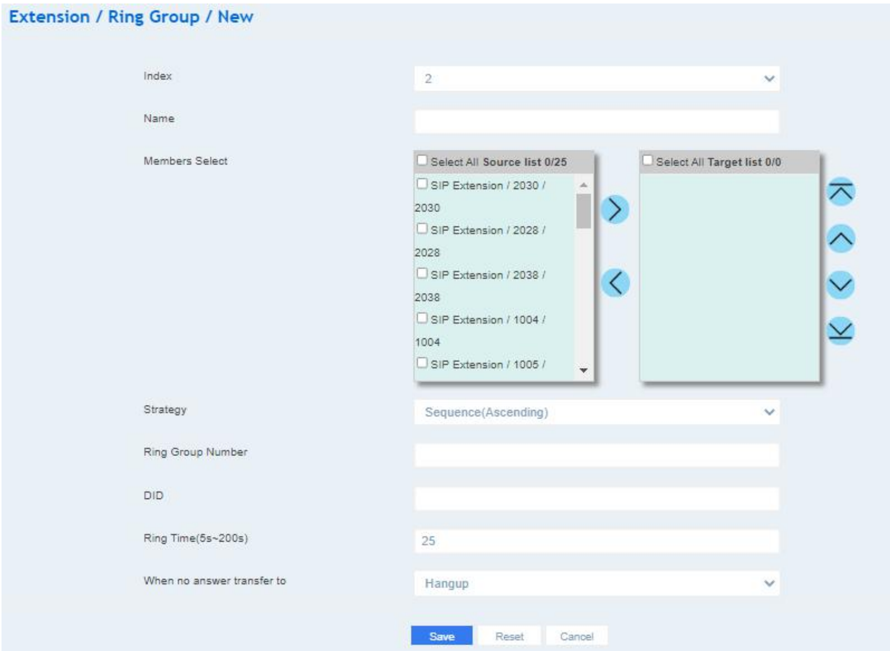


Figure 5.6.3 Ring Group

Table 5.6.3 Explanation of Ring Group Parameters

Name	The name of this ring group.
Members Select	Select the SIP extension, and an extension cannot exist in two ringing groups at the same time.

	"+": Add an extension to the ring group; "x": Delete an extension from the ring group.
Strategy	The strategies for choosing which SIP extension to ring, including Sequence (Ascending), Sequence (Cyclic Ascending), Simultaneous and Random.
Ring Group Number	The number of the ring group is generally the same as DID.
DID	Same with Ring Group Number; it is optional to fill in.
Ring Time（5-60s）	The duration of ring when there is a coming call. Range: 5s to 60s.
When No Answer Transfer To	When none of the members in the ring group answer, you can transfer the call to a specified extension or hang up.

Note： If ring group function has been set, the call forward function is unavailable.

5.6.4 Paging Group

On the **Extension -> Paging Group** interface, users can group SIP extensions into a paging group and then if there are calls given from SIP to the paging group, the calls will be led to one extension of the paging group according to the preset strategy.

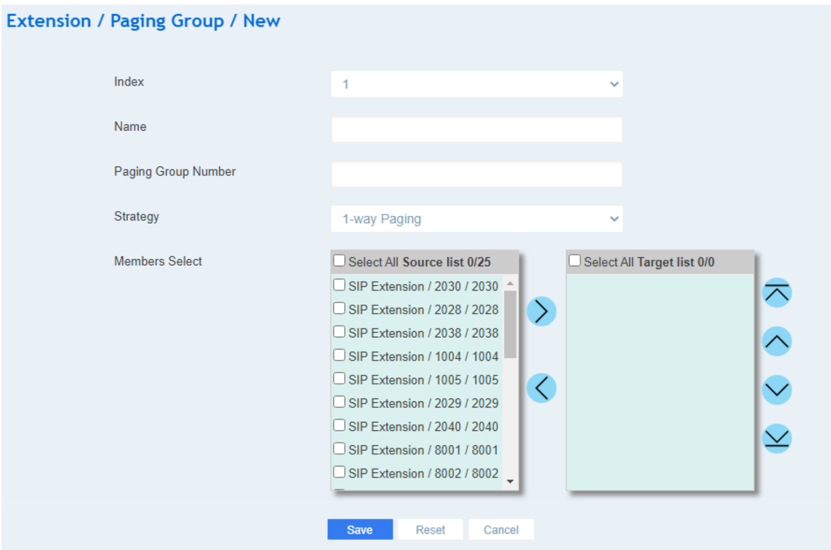


Figure 5.6.4 Paging Group

Table 5.6.4 Explanation of Paging Group Parameters

Name	The name of this Paging Group.

Paging Group Number	The number of the paging group.When there are calls given from SIP to this number, the calls will be led to one extension of the paging group according to the preset strategy.
Strategy	Include one-way paging and two-way intercom. **one-way paging：** members of the paging group only can listen to the voice of presenter and cannot answer the call. **two-way intercom：** members of the paging group can have conversation with the presenter, but members cannot talk to each other.
Members Select	Select the SIP extensions that are added into the paging group. An SIP extension cannot exist in two paging groups at the same time. "+": Add a member to the paging group; "x": Delete a member from the paging group.

5.6.5 Call Queue

On the **Extension -> Call Queue** interface, users can add the local extension to a queue. When calling into the call queue, the system will transfer the call to the queue member/agent to answer the call according to the strategy.

For example, when a large number of customers call in at the same time, and the customer service staff is limited, queue the incoming and play a voice waiting tone or custom music file. At the same time, the agent can answer the call according to the preset call queue strategy.

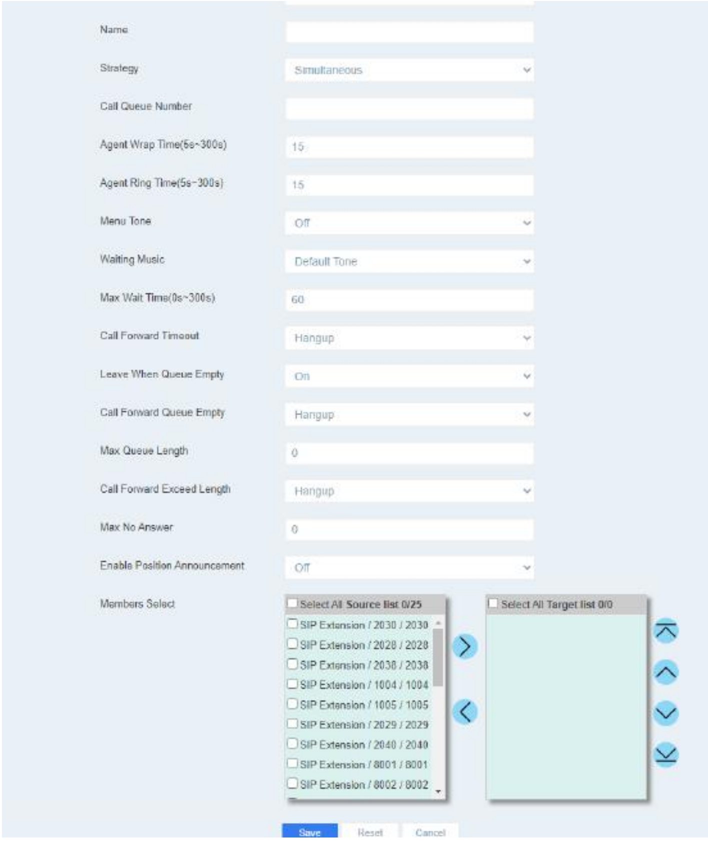


Figure 5.6.5 New Call Queue

Table 5.6.5 Explanation of Call Queue Parameters

Name	The name of the queue call.
Strategy	Calls into the queue, the agents ring according to the strategy. Simultaneous: The agents ring together. Sequential Mode: When there is no incoming call, a new user calls in, each time it rings sequentially from the first agent). Random: one is randomly selected for ringing. Memory rotation mode: When there is no incoming call, a new user calls in, and the ringing starts from the next agent who hangs up last before. Max idle time: Idle time, namely the time from the end of the agent's last call to the present; ringing in the order from longest to shortest time. Min talk time: The ringing starts from the least to the most according to the times of calls.

Call Queue Number	The number of the call queue can be called into the queue.
Agent Wrap Time(5s-300s)	The interval time between the next ringing after the agent call hangs up.
Agent Ring Time(5s-300s)	If the ringing exceeds the time, it will call the next agent.
Menu Tone	The first Menu Tone the remote end hears when calling in.
Waiting Music	The remote end waits for the agent to answer the waiting tone after calling in.
Max Wait Time(0s-300s)	The longest time the caller waits. The caller will exit after this time. 0 means no limit, but it should be noted that this time is not necessary. For example, an agent is ringing and the caller has reached the timeout. The caller will wait until the agent answers or hang up after the timeout.
Call Forward Timeout	If the caller times out, other actions can be configured.
Leave When Queue Empty	If there is no agent in the queue, it will exit the queue (if there is ON-Break, it is still an agent), and the call transfer will be performed when the queue is empty.
Max Queue Length	How many users are waiting, those connected are not counted, 0 means no limit, hang up if the maximum number of queues is exceeded.
Max No Answer	If the times that the agent does not answer is exceeded, it will enter On-Break state. In this state, it will not ring again until the agent answers.
Enable Position Announcement	Timely notify the user of the waiting position in the queue, the first one does not notify.

5.7 Trunk

5.7.1 SIP

SIP trunk can be used to create a connection between UC8000 and SIP based IPPBX or SIP servers.

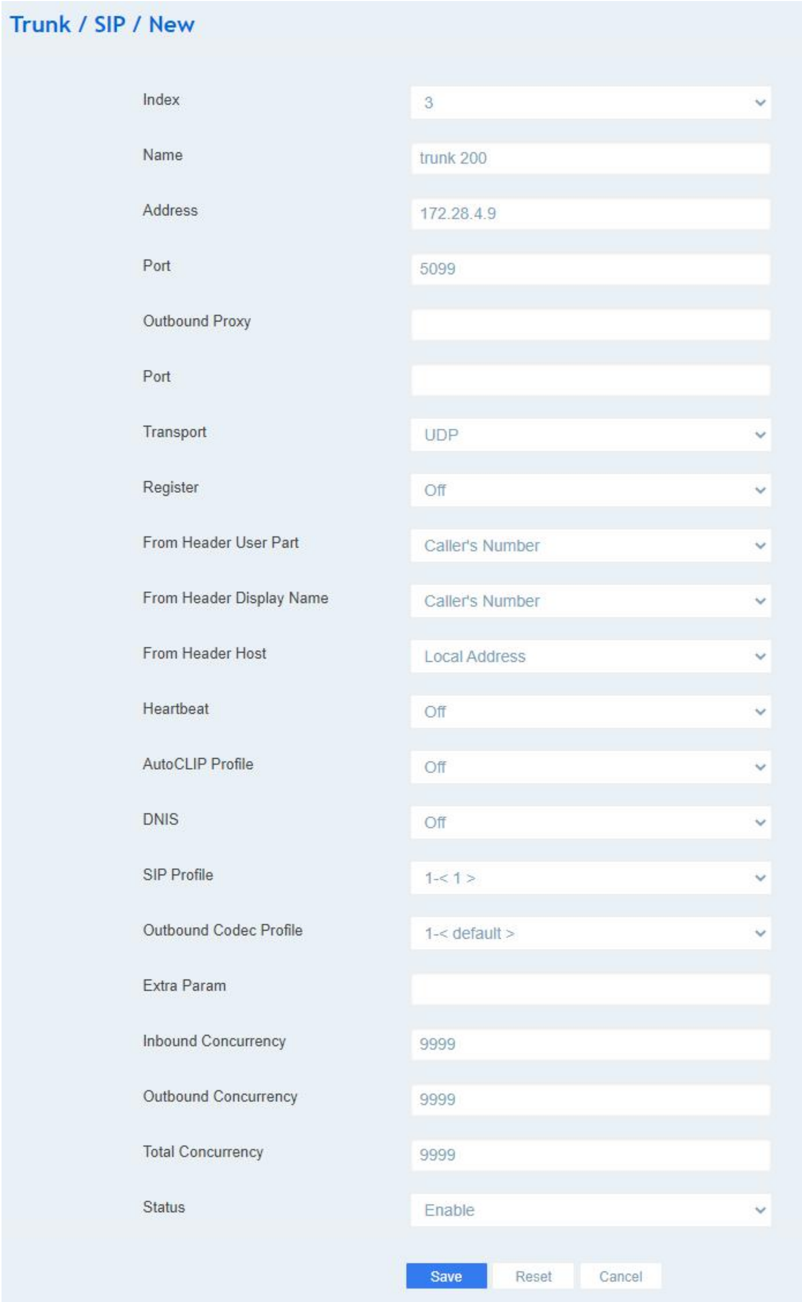


Figure 5.7.1 SIP Trunk

Table 5.7.1 Explanation of SIP Trunk Parameters

Name	The name of the SIP trunk.
Address	The IP address or domain name of the peer SIP devices or servers.
Port	The SIP listening port of the peer SIP devices or servers; 5060 is the default port.

Outbound Proxy	If an outbound proxy is used, enter the IP address or domain name of the proxy server.
Port	If an outbound proxy is used, enter the listening port of the proxy server.
Transport	Transport protocol: TCP or UDP.
Register	If it is on, the SIP trunk will send register request to the peer device.
Username	The username of this SIP trunk is generally a phone number.
Auth Username	The username used for register authentication by this SIP trunk.
Password	The password is used for register authentication by this SIP trunk.
From Header Display Name	Choose the registered username or the true caller ID for the ‘from header’ of the invite message when a call goes out.
Heartbeat	If heartbeat in on, heartbeat (options) messages will be sent to examine the connection with servers; The default value is ‘Off’.
AutoCLIP Profile	AutoCLIP is mainly used on SIP trunks and it helps record the outgoing and incoming calls of a trunk.
DNIS	When the SIP trunk calls in, the called number matches the DNIS, then the *display name.*
Expire Seconds	The validity period after the SIP trunk is registered successfully. When the time expires, the SIP trunk will send register request to the server. Default value is 1800s.
SIP Profile	The SIP profile of the SIP Trunk, make reference to Profile -> SIP section.
Status	If it is enabled, it means the SIP Trunk can be used;

	otherwise, the SIP trunk is unavailable.

5.8 Call Control

This section is to configure routes or route groups for incoming and outgoing calls through UC8000, as well as IVR, SMS and so on.

5.8.1 Setting

On the **Call Control->Setting** interface, users can enable voice interruption protection and configure tones.

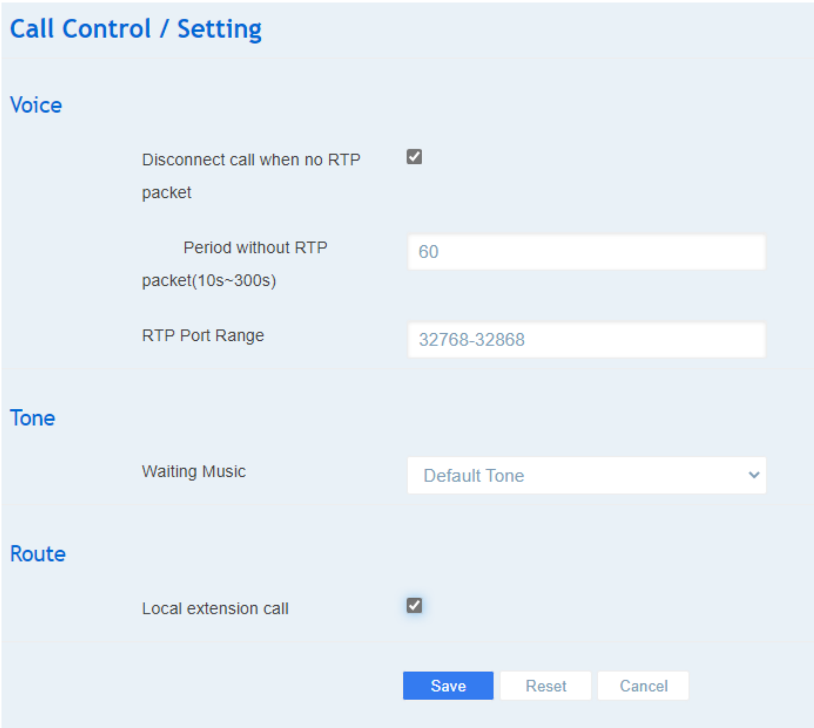


Figure 5.8.1 Basic Setting of Call Control

Table 5.8.1 Explanation of Call Control Parameters

Disconnect call when no RTP packet	If it is enabled, and no RTP packets are received within the preset time, calls will be disconnected.
Period without RTP packet(10s~300s)	The maximum time after an RTP message interruption is used to determine whether the voice interruption is protected.
RTP Port Range	The range of the local SDP RTP port, the default is: 32768-65000, change it and reboot to take

	effect.
Waiting Music	Select the waiting music.
Local extension call	On means local extensions can call each other directly, off means local extensions When calling other local extensions, the call path is changed from.

5.8.2 Route Group

On the **Call Control ->Route Group** interface, users can group SIP trunks and SIP extensions together according to their needs and set strategy for choosing which trunk or extension as the destination route under a route group.

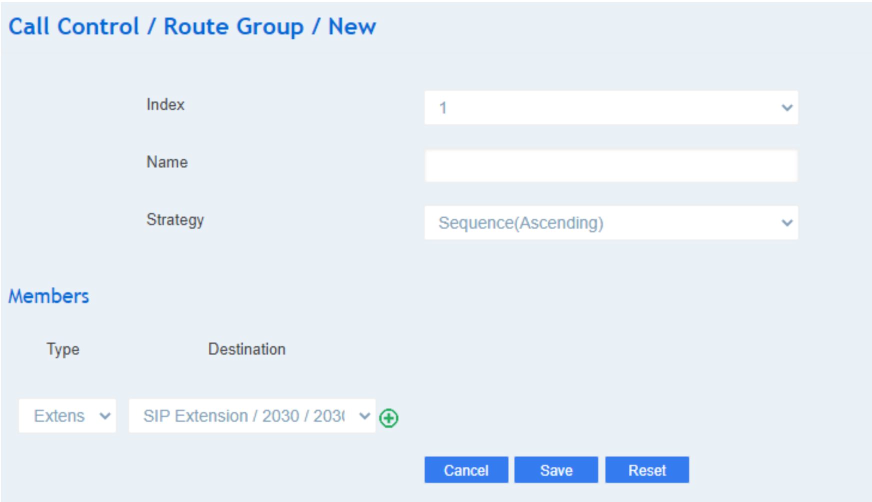


Figure 5.8.2 Create Route Group

Table 5.8.2 Explanation of Route Group Parameters

Name	The name of the route group.
Members Select	Select SIP extension or SIP trunk.
Strategy	The strategies for choosing which route under the route group as the destination route.

5.8.3 Route

On the **Call Control -> Route** interface, users can configure routes for incoming calls and outgoing calls.

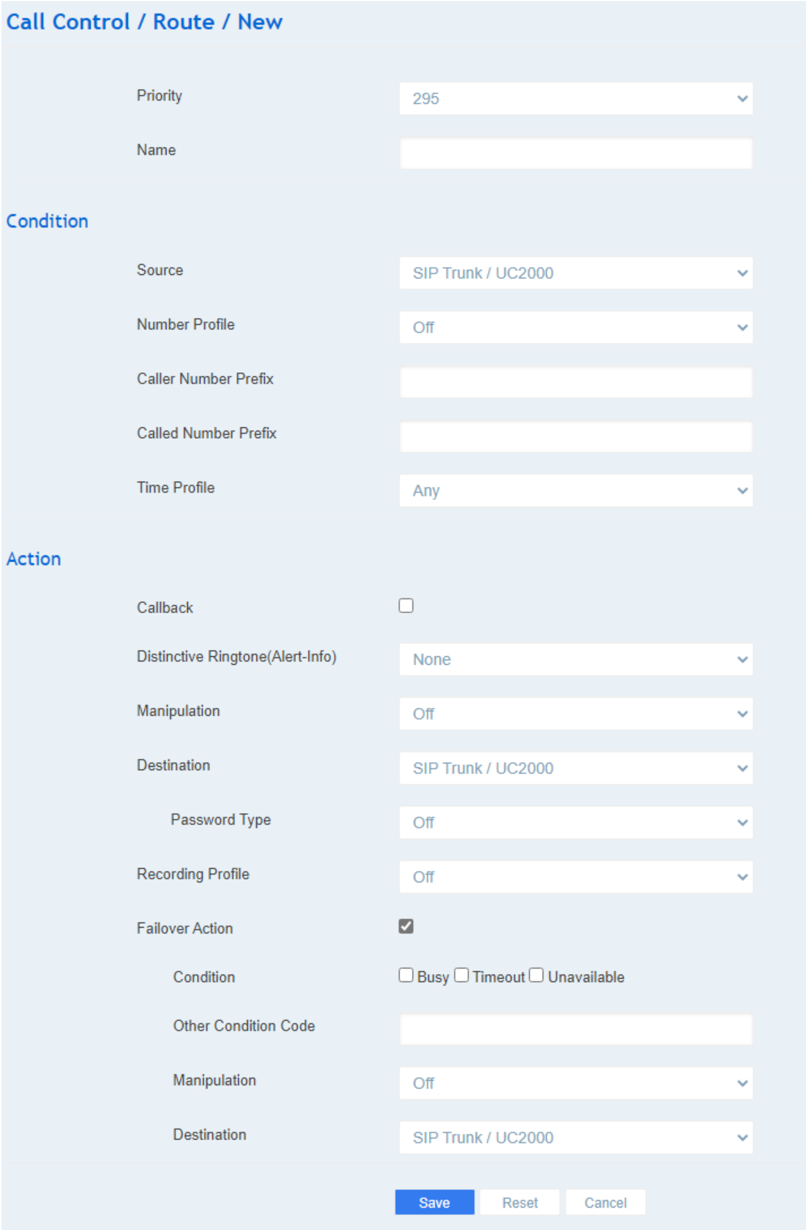


Figure 5.8.3 Create a route

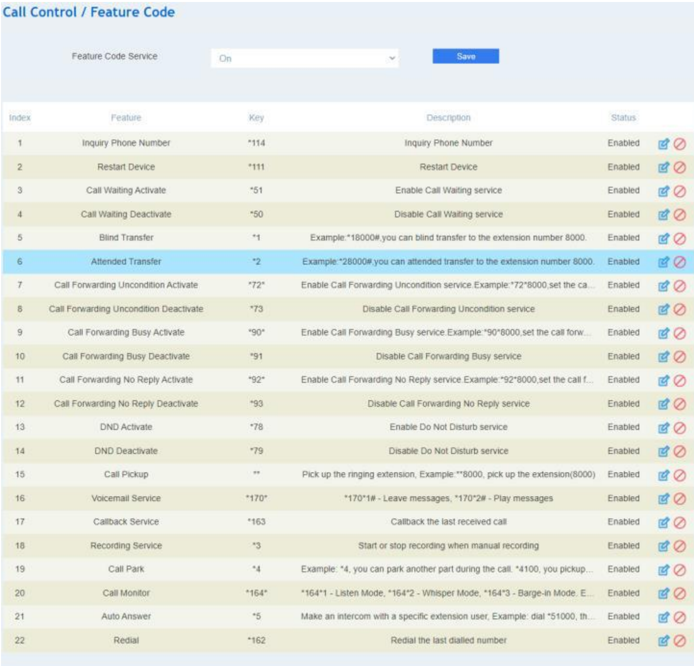
Table 5.8.3 Explanation of Route Parameters

Priority	The priority for choosing the route; the higher value, the lower priority.
Name	The name of the route; the text input cannot be empty, up to 32 characters and cannot contain double quotes.
Condition	The condition under which the route will be used.
Source	The source of the call can be either a trunk or an extension. Selecting "Custom" allows the user to combine any combination of trunks and extensions, and selecting "Any"

	means there is no restriction on the source.
Number Profile	The profile of the caller number and the called number; please make reference to the Profile Number section. The default value is 'Off'. Note: it cannot be simultaneously used with the following parameters of 'caller number prefix' and 'called number prefix'.
Caller Number Prefix	The prefix of caller number; it supports regular expression.
Called Number Prefix	The prefix of called number; it supports regular expression.
Time Profile	The profile of time during which the route can be used; make reference to the Profile -> Time section
Action	Include manipulating number and sending call to destination
Callback	After enabling, the caller who configures this route will directly hang up after the incoming call, and then initiate a call to the called after the waiting time expires, and then initiate a call to the caller after the called picks up.
Manipulation	If it is on, the caller number or called number of the route will be manipulated; make reference to the Profile ->Manipulation section.
Destination	The destination of the route.
Recording Profile	Record according to the configured rules.
Failover Action	The processing when a call through this route fails.

5.8.4 Feature Code

Users can achieve the corresponding function by dialing the feature code after the local extension is off-hook. The function of the feature code is shown in the following figure.



Call Control / Feature Code

Feature Code Service: On

Save

Index	Feature	Key	Description	Status
1	Inquiry Phone Number	*114	Inquiry Phone Number	Enabled
2	Restart Device	*111	Restart Device	Enabled
3	Call Waiting Activate	*51	Enable Call Waiting service	Enabled
4	Call Waiting Deactivate	*50	Disable Call Waiting service	Enabled
5	Blind Transfer	*1	Example:*18000#,you can blind transfer to the extension number 8000.	Enabled
6	Attended Transfer	*2	Example:*28000#,you can attended transfer to the extension number 8000.	Enabled
7	Call Forwarding Uncondition Activate	*72*	Enable Call Forwarding Uncondition service.Example:*72*8000,set the ca...	Enabled
8	Call Forwarding Uncondition Deactivate	*73	Disable Call Forwarding Uncondition service	Enabled
9	Call Forwarding Busy Activate	*90*	Enable Call Forwarding Busy service.Example:*90*8000,set the call forw...	Enabled
10	Call Forwarding Busy Deactivate	*91	Disable Call Forwarding Busy service	Enabled
11	Call Forwarding No Reply Activate	*92*	Enable Call Forwarding No Reply service.Example:*92*8000,set the call f...	Enabled
12	Call Forwarding No Reply Deactivate	*93	Disable Call Forwarding No Reply service	Enabled
13	DND Activate	*78	Enable Do Not Disturb service	Enabled
14	DND Deactivate	*79	Disable Do Not Disturb service	Enabled
15	Call Pickup	**	Pick up the ringing extension, Example:**8000, pick up the extension(8000)	Enabled
16	Voicemail Service	*170*	*170*1# - Leave messages, *170*2# - Play messages	Enabled
17	Callback Service	*163	Callback the last received call	Enabled
18	Recording Service	*3	Start or stop recording when manual recording	Enabled
19	Call Park	*4	Example: *4, you can park another part during the call. *4100, you pickup...	Enabled
20	Call Monitor	*164*	*164*1 - Listen Mode, *164*2 - Whisper Mode, *164*3 - Barge-in Mode. E...	Enabled
21	Auto Answer	*5	Make an intercom with a specific extension user, Example: dial *51000, th...	Enabled
22	Redial	*162	Redial the last dialled number	Enabled

Figure 5.8.4-1 Feature Code

Note: All feature codes are enabled by default. Any feature code can be customized and edited.

Table 5.8.4-1 Explanation of Feature Code Parameters

Inquiry Phone Number	Inquiry Phone Number.
Restart Device	Restart Device.
Call Waiting Activate	Enable Call Waiting service.
Call Waiting Deactivate	Disable Call Waiting service.
Blind Transfer	Example: *18000#, you can blind transfer to the extension number 8000.
Attended Transfer	Example: *28000#, you can attend transfer to the extension number 8000.
Call Forward Unconditional Activate	Enable Call Forwarding Unconditional service. Example: *72*8000, set the call forwarding number to 8000.
Call Forward Unconditional	Disable Call Forwarding Conditioning service.

Deactivate	
Call Forward Busy Activate	Enable Call Forwarding Busy service. Example: *90*8000, set the call forwarding number to 8000.
Call Forward Busy Deactivate	Disable Call Forwarding Busy service.
Call Forward No Reply Activate	Enable Call Forwarding No Reply service. Example: *92*8000, set the call forwarding number to 8000.
Call Forward No Reply Deactivate	Disable Call Forwarding No Reply service.
DND Activate	Enable Do Not Disturb service.
DND Deactivate	Disable Do Not Disturb service.
Call Pickup	Pick up the ringing extension, Example: **8000, pick up the extension (8000).
Voicemail Service	*170*1# - Leave messages, *170*2# - Play messages.
Callback Service	Callback the last received call.
Recording Service	Start or stop recording when manual recording.
Call Park	Example: *4, you can park another part during the call. *4100, you pick up the number 100 from the parking lot.
Call Monitor	*164*1 - Listen Mode, *164*2 - Whisper Mode, *164*3 - Barge-in Mode. Example: *164*28000, you can monitor extension 8000 in whisper mode.
Auto Answer	Make an intercom with a specific extension user. Example: dial *51000, then extension 1000 will be automatically picked up.
Redial	Redial the last dialled number.

Any feature code below can be customized.

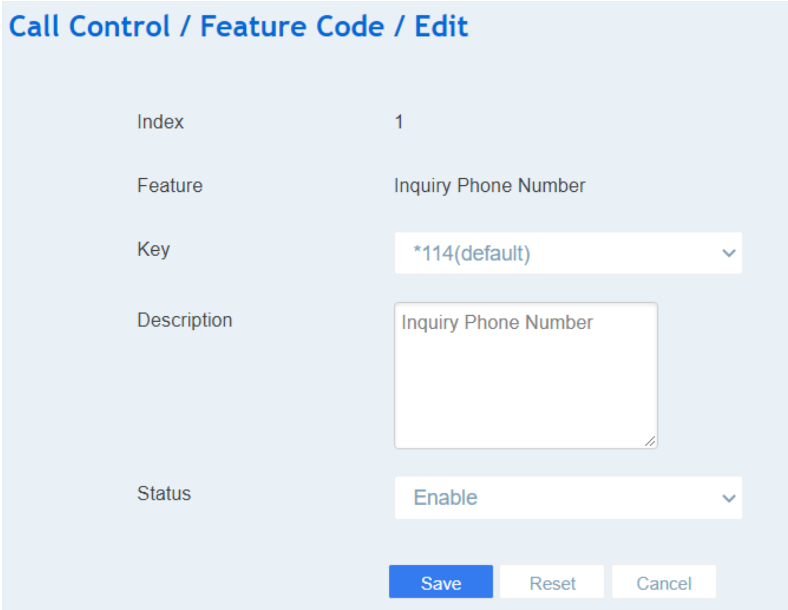


Figure 5.8.4-2 Edit Feature Code

Table 5.8.4-2 Explanation of Feature Code Editor Parameters

Index	Non-editable
Feature	Non-editable
Key	Drop-down selection, default/custom; when customizing, text input can only start with *, can contain numbers 0-9 and *, and cannot be the same as configured.
Description	Text input, non-empty.
Status	If it is enabled, it means the feature code can be used; otherwise, the feature code is unavailable.

Note: After the feature code is set successfully, the phone will give a voice prompt of "set successfully", so hang up the phone after hearing this prompt and proceed to the next operation. By default, the feature code function is on.

5.8.5 IVR

On the **Call Control -> IVR** interface, users can carry out specific configurations for the IVR which has been uploaded from the **System -> Voice** interface. IVR is often used for voice prompts in call centers.

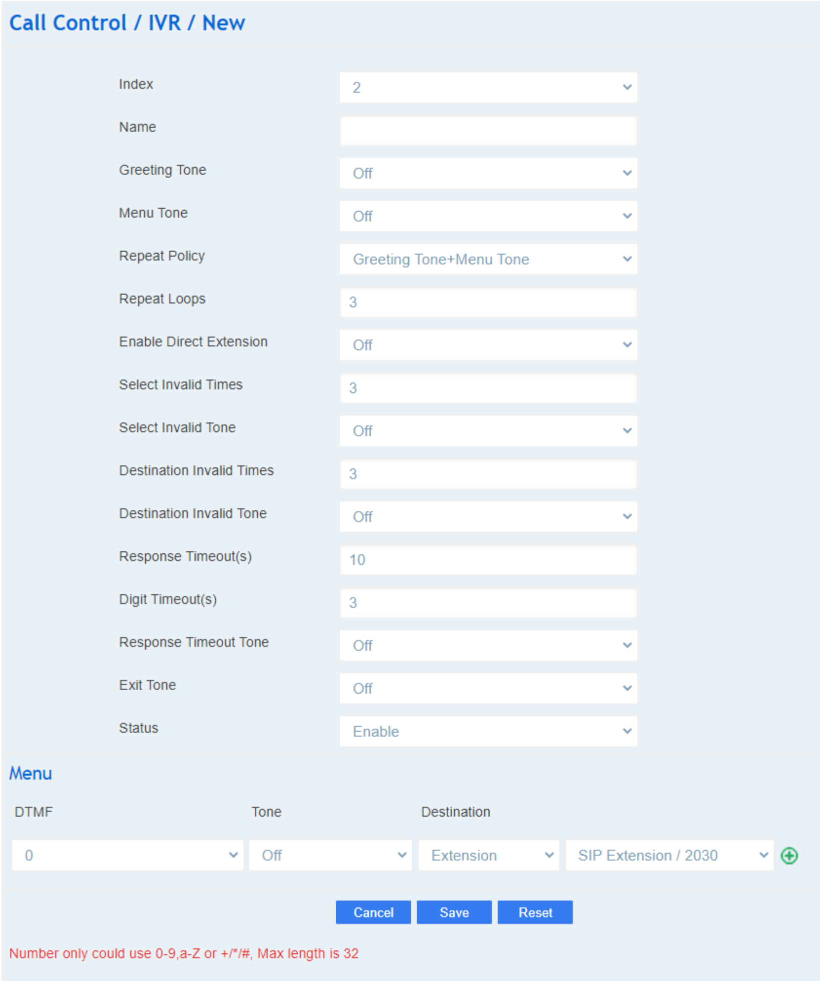


Figure 5.8.5 IVR Setting

Table 5.8.5 Explanation of IVR Parameters

Name	The name IVR.
Menu Tone	When a call comes to the IVR, the menu tone heard.
Enable Direct Extension	Whether to allow direct dialing of extensions during the playing of IVR.
Repeat Loops	If it is set as ‘3’, the call will be hanged up after the IVR has been repeated for three times during timeout.
Select Invalid Times	When a call comes to the IVR, according to the voice prompt, if you receive two dialings that do not match the DTMF, then the dialing is invalid, and the invalid prompt tone is played. When the invalid times are exceeded, the voice prompts: Goodbye.

Select Invalid Tone	When an invalid dial is received, an invalid tone will be played.
Destination Invalid Times	It takes effect when the direct extension is enabled. When you call into the IVR, and the entered number does not exist, the destination invalid prompt will be played. When the time of entries exceeds the set value, the voice prompts: Goodbye.
Destination Invalid Tone	When receiving an invalid destination dial, the invalid tone will be played.
Response Timeout(s)	When a call comes to the IVR, according to the voice prompt, the second dial is not received within the set time, the response is timed out, and the timeout tone is played.
Digit Timeout(s)	The timeout for dialing DTMF.
Response Timeout Tone	When the second dialing timeout, the timeout will be played after being enabled.
Exit Tone	When exiting IVR, the exit tone will be played.
Status	If it is disabled, the IVR cannot be seen in the destination of route.
Menu	DTMF: It can be 0-9 quick-dial numbers, *, #, others or timeout. Destination: the destination of the IVR; it can be an extension or a trunk. For example, if DTMF is configured as 1,2,3 and others, and the telephone key that is pressed is not 1, 2 or 3, the IVR will choose the destination of ‘others’. When the playing of the IVR times out, and user does not press any telephone key, the IVR will choose the destination of ‘timeout’. When the destination is a trunk, user does not need to pre-configure the called number, and the system will prompt the user to dial the called number.

5.8.6 Conference

On the **Call Control -> Conference** interface, users can create a conference room, and the caller can create a multi-party conference by dialing the number of the conference room.

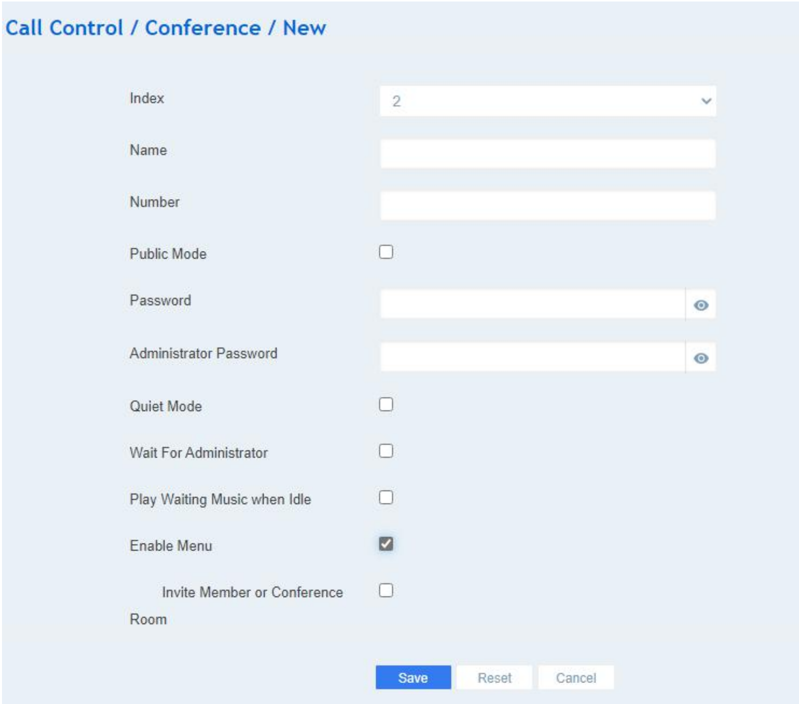


Figure 5.8-6 Conference

Table 5.8.6-1 Explanation of Conference Parameters

Name	The name of the conference room.
Number	Conference room number, the extension can join the conference by dialing this number.
Public Mode	No password is required to join the conference in public mode.
Password	The password for users to join the conference in non-public mode.
Administrator Password	Administrator password: the password for the administrator to join the conference in non-public mode. A conference can have multiple administrators, and the administrator password cannot be blank.
Quiet Mode	When the quiet mode is enabled, the conference will not hear any voice.
Wait For Administrator	Once enabled, the conference will only start after the administrator join the conference, otherwise it will be idle

Play Waiting Music When Idle	When the conference is idle, the waiting tone will be played after being enabled.
Enable Menu	After activation, everyone can use the menu through DTMF.
Invite Member or Conference Room	After enabling the menu, non-administrators can invite members to join the conference room.

Table 5.8.6-2 Conference Menu

DTMF	Description	Notes
1	Invite members	Non-administrators need to enable configuration
2	Invite members, need to be confirmed by the invitee	Non-administrators need to enable configuration
3	Initiate a conference	Non-administrators need to enable configuration
4	Decrease the volume of the handset	
6	Increase the volume of the handset	
7	Decrease the volume of the microphone	
9	Increase the volume of the microphone	
*	Mute	
0	All non-administrators are muted	Administrator permissions
#	Exit all non-administrators from the conference	Administrator permissions

Menu instructions:

Invite members: Invite multiple SIP extensions

After pressing 1, it will prompt to enter the number and the extension number;

The extension rings;

After the extension is connected, join the conference as a non-administrator.

Invite members (requires confirmation):

After pressing 2, it will prompt to enter the number and the extension number;

The extension rings;

After the extension is connected, you hear the prompt that you will join the conference, press 1 to join the conference as a non-administrator, press 2 or other to hang up.

Invite a conference: The conference room is activated.

After pressing 3, it will prompt to enter the conference room number;

If there is a password, you will be prompted to enter the conference room password;

Connect to the meeting.

5.8.7 Emergency Number

Emergency numbers are used for more urgent call scenarios, such as: 120, 119, 110, 911 in UAS etc. Users dial the emergency number in case of emergency. The emergency number will be paged directly to the emergency number according to the configured routing, without the need to walk by.

Operation steps.

- On the Call Control/Emergency Number interface, users can create a new emergency number.

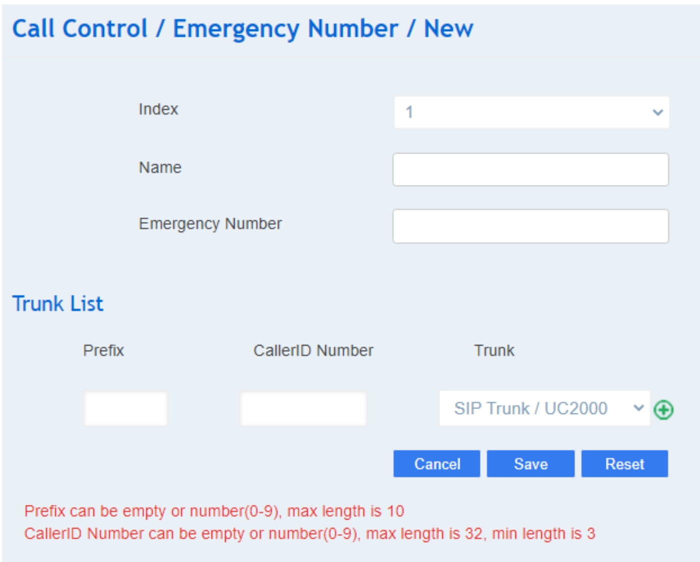


Figure 5.7.1 Create a new emergency number

Table 5.7.1 Explanation of parameters

Index	Can be selected arbitrarily, the only non-repeatable, that is, after the selection of a new item does not include the

	selected item.
Name	The configuration name cannot be empty, up to 32 characters and cannot contain English double quotes.
Emergency Number	Numbers to dial at critical moments, for example: 110, 12580.
Trunk List Prefix	Can be empty, if set, it will be added to the number when calling in front of the number.
Trunk List Caller ID Number	Caller ID number requires carrier support to work.
Trunk	Reaching the destination via Trunk.

- After configuration, save the application.
- When users call an emergency number, any local extension number will be called out according to the configured routing.

Note:

- If the trunk concurrency of the emergency number is full, it will force the call of this trunk so that the emergency number can continue. This means that the emergency number has the highest priority.
- Emergency number calls cannot be forced to remove the emergency number call.
- If the emergency number and the extension number are duplicated, it will also be considered as an emergency number call out.

5.8.8 SCA

When someone calls a company manager, the secretary will receive the call first and determine whether to forward the person's call to the manager. Sometimes the manager wants to answer the call directly, so a switch is used to control whether the manager can receive the call directly. Managers and secretaries can also call each other.

Operation steps.

On the **Extension ->SIP** interface, users can select the extension where they want to open the SCA.

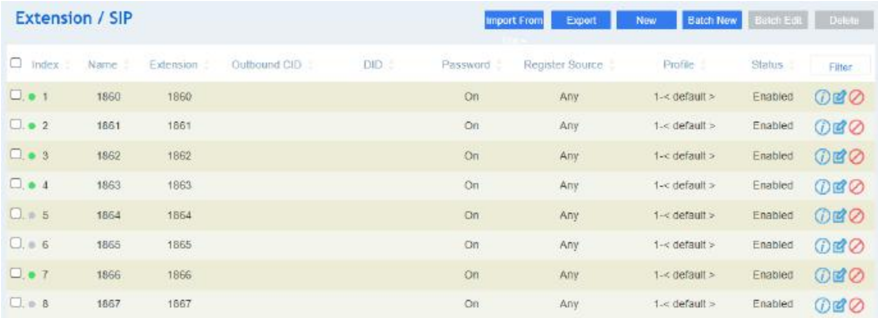


Figure 5.8.8-1 Select the extension

Edit the SIP extension to be on and open the SCA.

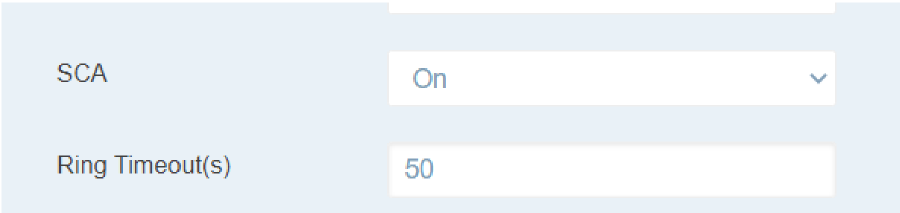


Figure 5.8.8-2 Open the SCA

On the Call Control/SCA interface, users click on new, and select each option as follow.

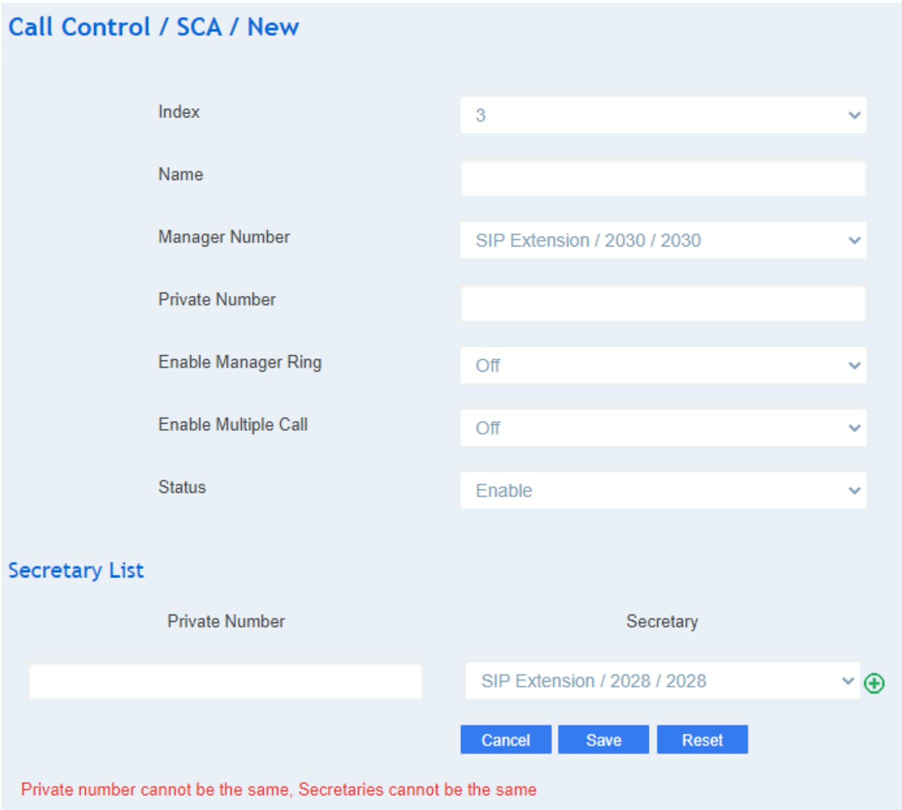


Figure 5.8.8-3 New SCA

Table 5.8.8 Explanation of parameters

Index	Can be selected arbitrarily, the only non-repeatable, that is, after the selection of a new item does not include the selected item.
Name	The configuration name cannot be empty, up to 32 characters and cannot contain English double quotes.
Manager Number	Only SIP extensions with SCA enabled can be selected.
Private Number	Manager's private number cannot be duplicated with other numbers, it can only be used for calls between managers and secretaries in the same business.
Whether the manager's extension is ringing	If turned on, it will ring with the secretary and you can answer the call directly to the call manager.
Allows multiple calls	If turned on, you can have multiple calls coming in at the same time. Allowed the maximum number of incoming calls is the number of secretaries.
Secretary List - Private Number	Secretary's private number cannot be duplicated with other numbers, it can only be used for calls between managers and secretaries in the same business.
Secretary List - Secretary	Select the appropriate SIP extension as the manager's secretary, a manager can have multiple secretaries.

After saving the application, SCA in the status bar allows you to view SCA information and SCA line status.

Figure 5.8.8-4 SCA

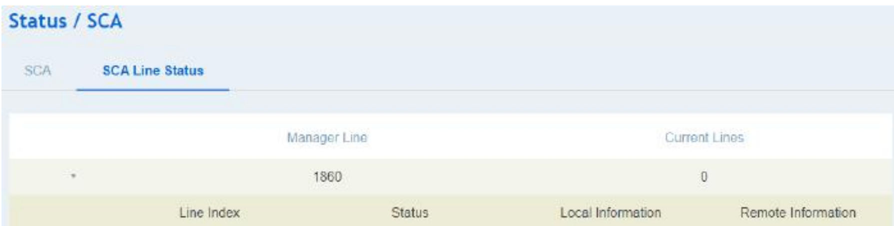


Figure 5.8.8-5 SCA Line Status

When there is a call, the SCA current line count is 1 and the corresponding message is displayed.

Ringing Description.

Whether the manager is ringing or not.

- Any extension to the manager number 8808, the secretary 9999 ring to connect, to determine whether to transfer the manager.
- The same group manager or secretary to another group manager, are the secretary ringing, the secretary connected to determine whether to transfer the manager.
- The same group of managers and secretaries can call each other directly, or dial each other's private numbers.

Whether to turn on the manager's extension ringing.

- Any extension to call the manager number 8808. The manager and the secretary ring at the same time. If the manager is connected, the secretary hangs up; if the secretary is connected, the manager hangs up. At this time, the secretary will judge whether to transfer to the manager.
- The same group manager or secretary to another group manager, the manager and secretary ring at the same time. If the manager is connected, the secretary hangs up; if the secretary is connected, the manager hangs up. At this time, the secretary judges whether to transfer to the manager.
- The same group of managers and secretaries can call each other directly by extension number, or dial each other's private number to call each other.

Note: SIP extensions with SCA on cannot be used as secretary extensions.

5.8.9 Follow Me

After the operator opens Follow Me, users can unify their common various communication numbers (cell phone, pager, office phone, voice mail, residential phone) into a new phone number, so that anyone can simply dial this phone number to find the user in the future.

An extension can be tied to a string of extensions and trunks, so that when no one answers a call to that extension number, it will go ring its list.

Operation steps.

- On the Call Control/Follow Me interface, click New.

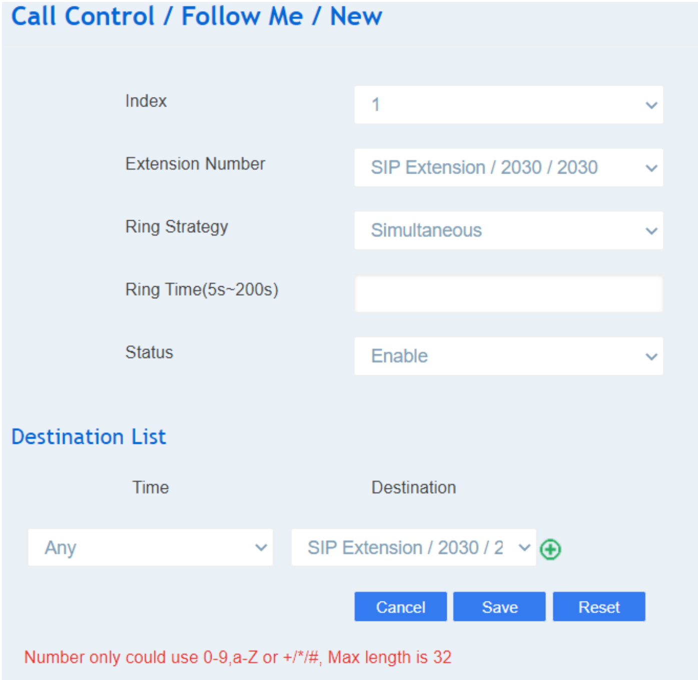


Figure 5.8.9 Create a new extension number

Table 5.8.9 Explanation of parameters

Index	Optional, unique and non-repeatable.
Extension Number	Select the extension to enable this feature, users cannot select the SIP extension with the SCA enabled and the SIP extension as secretary.
Ring Strategy	Support simultaneous and sequence(ascending). simultaneous is all numbers ring together, and the sequence starts from the extension and rings from top to bottom.
Ring Time(5s~200s)	Ringing time per number.
Status	This feature is only available when enabled.
Destination List-Time	Any is unlimited; if users choose to set the time period as shown above1-<Time>, they will only be called during this time period.
Destination List-Destination	Other numbers for this extension， you can select SIP extension, SIP trunk Relay, fill in the extension number to be called when selecting the relay.

- Save the application.
- Any number dialing the extension number such as 100, will ring based on the

corresponding ringing strategy. If it is sequential (incremental), it will ring from the extension 100, and after the timeout, it will ring the next number in turn according to the order of the extension following list; if it is resonant, the extension 100 will ring together with other destination numbers until it is connected or timeout.

Note:

- Extension call forward is not valid for Follow Me.
- The same SIP extension cannot be used for both SCA and Follow Me.

5.8.10 Alarm Clock

The alarm clock rings the destination number at the time when the system has been pre-configured. The system matches the time user set before, then the system will ring an extension selected.

Operation steps.

- On the Call Control/Alarm Clock interface, click New.

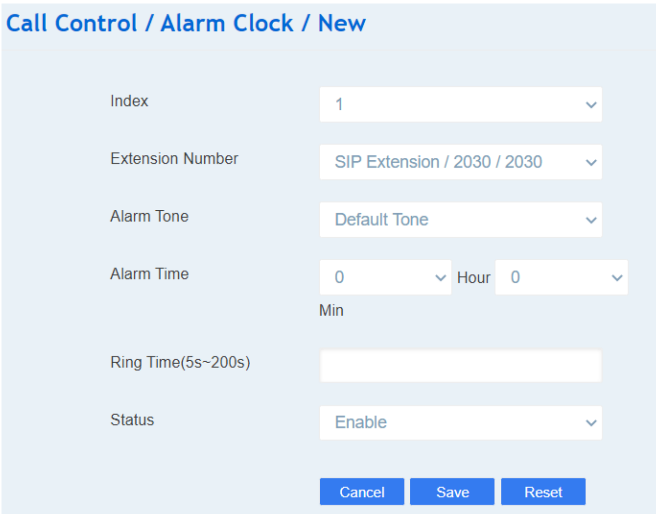


Figure 5.8.10 Create a new alarm clock

Table 5.8.10 Explanation of parameters

Index	Can be selected arbitrarily, the only non-repeatable, that is, after the selection of a new item does not include the selected item.
Extension Number	Select the extension where you want to turn on the alarm.
Alarm Tone	Users can choose to customize the uploaded waiting music or use the default music. The phone rings when the set alarm time is reached. Music will play automatically when off-hook.
Alarm Time	Customized alarm clock ringing time.

Ring Time(5s~200s)	Alarm clock to the set time phone ringing time.
Status	This feature is only available when enabled.

- After saving the application, check whether the extension number is ringing at the configured time.

Use scenario: Hotel wake-up call service, timed phone ringing, automatic play of wake-up call service music after taking off the phone.

5.8.11 Diagnostics

In case that call cannot be connected or voice has quality problem, users can enter the **Call Control -> Diagnostics** interface to collect fault information and then send it to technical support for diagnosis.

Operation Procedures:

- Select the module that needs to be traced. For example, if a call from SIP to trunk has voice problems, users can select SIP message and voice, and then click the **Start** button.
- Make a call, and come back to the **Call Control -> Diagnostics** interface after the call ends. Then click stop and download the tracing file.
- In order to locate faults more quickly, users need to enter into **System -> Service Log** interface, click export, and then send this exported file and the tracing file to technical support.

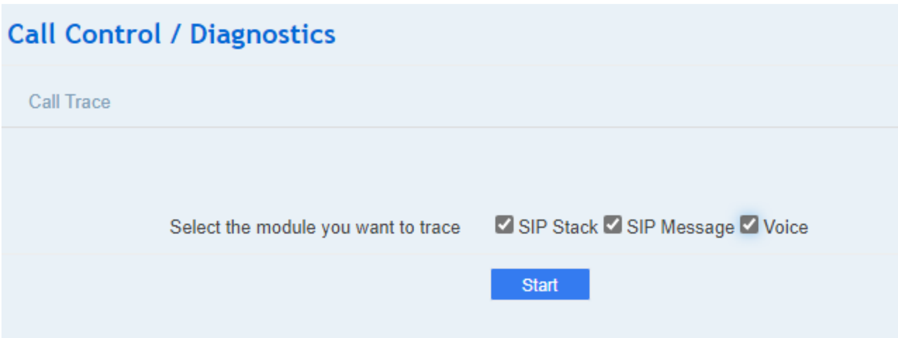


Figure 5.8.11 Call Tracing for Diagnostics

6 Appendix

Abbreviation	Explanation
ARP	Address Resolution Protocol
CID	Caller Identity
DNS	Domain Name System
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DND	Do NOT Disturb
DTMF	DTMF: Dual Tone Multi Frequency
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
PPTP	Point-to-Point Tunneling Protocol
MAC Address	Media Access Control Address
NAT	Network Address Translation
Ping	Packet Internet Grope
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

RTP	Real Time Protocol
PPPOE	Point-to-point Protocol over Ethernet
QoS	Quality of Service
UPnP	Universal Plug and Play
VLAN	Virtual Local Area Network
NTP	Network Time Protocol
STUN	Simple Traversal of UDP over NAT
PSTN	Public Switched Telephone Network
WLAN	Wireless Local Area Network
HA	High Availability