New Rock Technologies, Inc.

OM Series IP Telephony System

Administrator Manual

OM20
OM50
OM80

http://www.newrocktech.com

Document Version: 201607

Amendment Records

Document Rev. 02 (July, 2016)

Document Rev. 01 (December, 2015)

Manual Description

This manual is applicable to OM20/50 IP-PBX ("OM" for short) Rev 2.1.5.103 and OM80 IP-PBX Rev 2.1.5.101.

The manual guides administrators in setting OM parameters on Web interfaces. Some parameters can be set by using a telephone. For details, see the *OM User Manual*.

Contents

Contents of Figure

Contents of Table

1 Overview

1.1 Introduction

The OM series delivers a multi-functional office-telephony system designed for small–to-medium enterprises. The series integrates functions such as IP-phone, fax, and voice recording, and is compatible with multiple service platforms, such as Cisco CallManager, Broadsoft, Huawei IMS, Asterisk, and many terminals. The products are highly reliable, easy-to-install-and-deploy, and offer a new user experience in mobile offices and communications.

OM supports local and remote management operations through Web GUI or Telnet/SSH, TR069/TR104/TR106-based centralized management schemes, and auto provisioning.

Maintenance tasks such as modifying configuration, upgrading software, collecting statistical data, downloading logs, and fault alarms can be performed.

In combination with the New Rock WeWei softphone APP and NeeHau Business Phone Assistant, OM delivers a full-featured IP telephony solution. By supporting intelligent communication functions such as mobile-phone extensions, instant multi-party conferences, call history, click-to-dial, and customer-information management, it not only facilitates seamless communication between enterprise employees and customers, but also provides a solid basis for enterprises to analyze core business data.

1.1.1 Models

OM supports multiple models with varying amounts of FXO ports and FXS ports, as shown in Table 1-1.

Table 1-1 Product models

Models		Interface Card	Number of Interface Card	Number of FXO Ports	Number of FXS Ports
OM20	**OM20-4S**	401A-4S	1	0	4
	OM20-4FXO	401A-4FXO	1	4	0
	OM20-2S/2	401A-4S	1	2	2
OM50	**OM50-12S**	401A-4S	3	0	12
	OM50-10S/2	401A-2S/2	1	2	10
		401A-4S	2		
	OM50-8S/4	401A-2S/2	2	4	8

		401A-4S	1		
OM80	**OM80-16S**	16FXS	1	0	16
	OM80-20S/4	16FXS	1	4	20
		4FXS/4	1		
	OM80-24S/8	16FXS	1	8	24
		8FXS/8	1		
	OM80-32S	16FXS	2	0	32
	OM80-32S/16	16FXS	1	16	32
		8FXS/8	2		
	OM80-40S/8	16FXS	2	8	40
		8FXS/8	1		
	OM80-48S	16FXS	3	0	48

1.1.2 Appearance

Figure 1-1 OM20 front panel

Figure 1-2 OM20 back panel

Figure 1-3 OM50 front panel

Figure 1-4 OM50 back panel

Figure 1-5 OM80 front panel

Figure 1-6 OM80 back panel

Table 1-2 OM20 indicator status

Indicator	Status	Description
PWR (green)	Blinking green	The device is starting
	Steady green	The device is running
	Off	The device is powered off or a power supply fault occurs.
STU (red, green)	Steady red	The WAN interface does not acquire the IP address. Possibly the WAN interface is not connected to a network cable, the WAN interface address fails to be acquired by using DHCP, the IP addresses are conflicted, and the PPPoE dialing fails.
	Blinking red	The device is starting or the Kupdate is upgrading.

Indicator	Status	Description
	Steady green	An IP address is obtained by WAN interface and the registration of SIP trunk is successful.
	Blinking alternatively between red and green	An IP address is obtained by WAN interface and the registration of SIP trunk is failed.
	Blinking green	An IP address is obtained by WAN interface and no SIP trunk is registered.
WAN (green)	Steady green	A WAN connection is established without any service flow.
	Blinking green	A WAN connection is established with service flows.
	Off	WAN interface is disconnected.
PC (green)	Steady green	A link is connected without any service flow.
	Blinking green	A service flow is being transmitted.
	Off	A link is not connected.
FXS/FXO (green)	Steady green	Off-hook or call established(analog extension/trunk)
	Blinking green	Ringing on incoming call(analog extension/trunk)
	off	Idle

Table 1-3 OM50 indicator status

Indicator	Status	Description
PWR (green)	Blinking green	The device is starting
	Steady green	The device is running
	Off	The device is powered off or a power supply fault occurs.
STU (red, green)	Steady red	The WAN interface does not acquire the IP address. Possibly the WAN interface is not connected to a network cable, the WAN interface address fails to be acquired by using DHCP, the IP addresses are conflicted, and the PPPoE dialing fails.
	Blinking red	The device is starting or the Kupdate is upgrading.
	Steady green	An IP address is obtained by WAN interface and the registration of SIP trunk is successful.
	Blinking alternatively between red and green	An IP address is obtained by WAN interface and the registration of SIP trunk is failed.
	Blinking green	An IP address is obtained by WAN interface and no SIP trunk is registered.
USB (green)	Steady green	The USB device inserted is properly recognized
	Blinking green	The Internet access via 3G/4G USB dongle is successful*
	Off	The USB device is not detected or the Internet access via 3G/4G USB dongle is failed or not performed*
WAN	Steady green	A WAN connection is established without any service flow.

Indicator	Status	Description
(green)	Blinking green	A WAN connection is established with service flows.
	Off	WAN interface is disconnected.
PC (green)	Steady green	A link is connected without any service flow.
	Blinking green	A service flow is being transmitted.
	Off	A link is not connected.
VOICE (Green-FXS, yellow-FXO)	Indicates line type and device status:	
	Blinking yellow	The device is starting and the port is an FXO port.
	Blinking green	The device is starting and the port is an FXS port.
	Off	No line is detected. Possibly the voice interface card is not inserted or the port is damaged.
	Indicates running status:	
	Steady yellow	Calling in or out via an analog trunk.
	Blinking yellow	Ringing of calling in for an analog trunk.
	Steady green	Picking up an analog extension or calling on.
	Blinking green	Ringing of a call coming for an analog extension.
	off	Idle
	Note: The device starts up for approximate 30 s to indicate line type, then indicates running status.	
Indicator of button:		
RST	To restore the device to factory default, press the RST for more than 3 seconds and release it when STU turn blinking red. This setting will be valid after rebooting the device.	

*The Internet access via 3G/4G USB dongle is currently not supported on the device.

Table 1-4 OM20/50 port description

Ports	Description
FXS	The FXS ports (RJ11) are used for connecting analog phones, fax machines or POS machines.
FXO	The FXO ports (RJ11) are used for connecting to the PSTN or another PBX.
PC/WAN	The PC port is used to connect a computer. The WAN port is used to connect the uplink network. Both are 10/100 Mbps Ethernet ports (RJ45). They share one IP address, which, by default, is obtained through DHCP. If no IP address is obtained, 192.168.2.218 is used by default, and you can change it on **Basic > Network** page.
USB	The USB port is used for connecting the USB device. Note: The device has 16 GB internal flash storage.

Ports	Description
CON	The console port is used for local management and testing. Note: The console port is used for local management and testing. A PC can be connected to device by linking the RS232 port to CON port. Connecting cables need to be produced or purchased. If the connection is established between the device and the mobile PC with no RS232 port, please use the cable together with a USB to an RS232 converter cable. Cables are shown below in Figure 1-7 and Figure 1-8. Generally, the console port is not used.
RST	The reset button restores factory default settings.
PWR	The power interface is used for connecting the power supply. Note: Please use the power adapter provided with the device.
Grounding terminal	The grounding terminal is used to connect the grounding cable.

Figure 1-7 RJ45 to RS232 serial cable

Figure 1-8 USB to RS232 converter cable

Table 1-5 OM80 port description

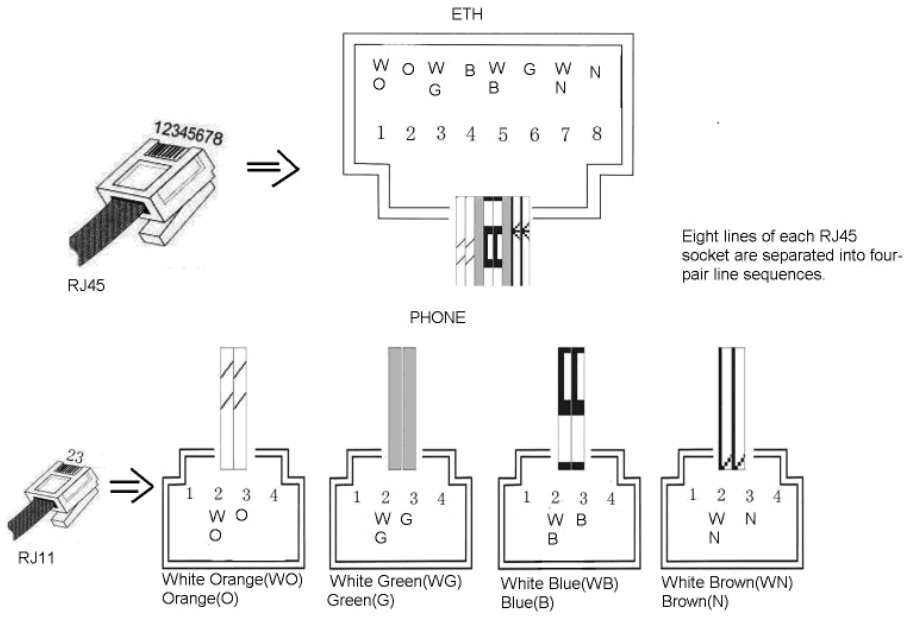
Ports	Description
Front panel	
RJ45 ports	Each RJ45 port corresponds with four pairs of analog lines. For corresponding relations, see Table 1-6.
Back panel	
ETHI/ETH2	Two 10/100 Mbps Ethernet ports (RJ45). By default, they share one IP address with the default value 192.168.2.240, and you can change it on **Basic > Network** page.
USB	USB port. Note: The OM80 contains an 8GB built-in SD card.
CON	The console port is used for local management and testing. Note: The console port is used for local management and testing. A PC can be connected to device by linking the RS232 port to CON port. Connecting cables need to be produced or purchased. If the connection is established between the device and the mobile PC with no RS232 port, please use the cable together with a USB to an RS232 converter cable. Cables are shown below in Figure 1-7 and Figure 1-8. Generally, the console port is not used.
Power socket	100-240 VAC voltage input or -48 V DC input.
Ground pole	Used to connect the ground.

Each RJ45 socket has 8 pins leading out 4 pairs of analog telephone or trunk lines in agreement with the pair specifications for Ethernet interfaces, whose corresponding relations can be seen in the table below. CAT-5 cables are used to connect the interface card and distribution panel in equipment installation. Standard RJ11 telephone lines can be used to plug in a RJ45 socket. The telephone/trunk lines are connected to the 3rd pair of pins for simple call test.

Table 1-6 Pin specifications for RJ45 socket port

RJ45 Pin Number	1	2	3	4	5	6	7	8
Analog line pair	1st Pair		2nd Pair	3rd Pair		2nd Pair	4th Pair	
	TIP1	RING1	TIP2	TIP3	RING3	RING2	TIP4	RING 4
Reference color	White Orange	Orange	White Green	Blue	White Blue	Green	White Brown	Brown

Figure 1-9 Schematic diagram of subscriber line connection



There is a 4 × 4 LED indicator matrixes on the left side of interface board. Each column of LED indicator matrixes matches four telephone lines on a RJ45. The first column on the left matches Line 1-4 respectively from top to bottom, the first column on the right matches Line 13-16 respectively from top to bottom, and the middle rows in the same manner.

LED indicators are used for multiple purposes as follows:

- Line status indication: this is the most common mode during normal use of equipment. In this mode, if a line is idle, the indicator corresponding to it goes off; if a line is in call or in use status (such as ringing, offhook) the indicator corresponding to it goes on.
- Line type indication: this is the mode for cable wiring check when installing the equipment. This mode can be entered by disconnecting Ethernet cables (Both WAN and LAN ports must be disconnected) at installation stage. After entering this mode, steady on LED indicates that the

corresponding line is equipped as analog subscriber line type, blinking LED indicates that the corresponding line is equipped as analog trunk line type, off LED indicates that the corresponding line is not equipped or not ready for use.

- System operation status indication: this is the mode for displaying information on system operation of equipment in specific conditions. Usually, this mode is entered when some prompts are required to give operator during equipment startup, diagnosis or operation. In this mode, LED flashes to display numbers, letters or other patterns in matrix. Please refer to Table 1-7.

Table 1-7 OM80 System Operation State

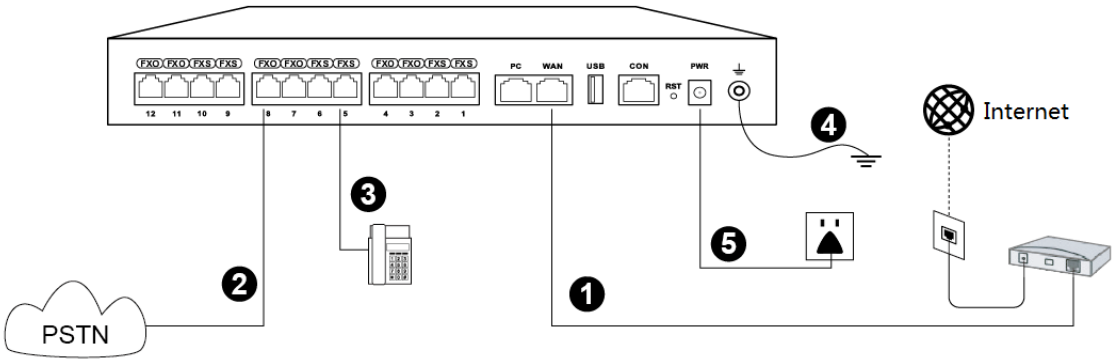
Glittery letter	Status meaning
C	The IP address of the device conflicts with that of other equipment in LAN. Please settle this problem before the gateway can be operated normally.
D	Internal failures have been encountered during the device start up procedure. Please contact your local distributor for further diagnosis.
P	The device is in progress of system software upgrade. Please guarantee stable power supply and do not conduct other operations during this period.
T	The application software of the device has been exited. If it cannot be restored by rebooting the system, please contact your local distributor for further diagnosis.

1.2 Accessing the Device

1.2.1 Connection

Place the device on an even surface, or secure it in a rack, and then follow these steps to connect (the diagram takes the OM50 as an example):

Figure 1-10 Diagram for proper connection



Step 1 Connect the WAN port (ETH1 or ETH2 for OM80) of the device to the Internet.

Step 2 Connect the FXO port of the device to the telephone line provided by a telecom operator or an extension line from another PBX.

Step 3 Connect the FXS port to an analog phone or a fax machine.

Note: For OM80, split the cable connected to FXO/FXS port (RJ45) to 4 pairs telephone lines for connecting. For details about the pin leading specification for the RJ45 socket, see Table 1-6.

Step 4 Connect the grounding cable: connect the end with a smaller diameter to the device, and connect the other end to a ground bar.

Step 5 Connect the power supply.

1.2.2 Log in to the Web GUI

Step 1 Use a CAT5 cable to connect the PC port (OM20/50) or ETH1/ETH2 (OM80) to a PC.

Step 2 Obtain the IP address of the device.

By default, the IP address of OM20/50 is automatically obtained by DHCP, the one of OM80 is 192.168.2.240. The default IP address of OM80 is 192.168.2.240. The IP address can be obtained by using these methods:

- FXS device and FXS + FXO device: dial "##" to obtain device IP address by an analog telephone connected to the FXS port after the equipment is powered on.
- FXO device: obtain device IP address via New Rock's Finder software.
  You can get the "Finder" software by visiting:
  http://website.newrocktech.com/ViewProduct_E.asp?id=68

Additional information:

(1) To assign a static IP address for your device, dial *90 and configure your network parameters as the following example on an analog phone:

192*168*2*218#255*255*0*0#192*168*2*1#0#

IP address Subnet mask Default gateway

(2) To obtain an IP address via DHCP, dial *90###1# and reboot the device after you hear "The feature is now activated".

Both configurations above take effect after a reboot.

Step 3 Make sure that the PC and the device are on the same network segment.

Step 4 Enter the device IP address in the browser address bar (e.g. 192.168.2.240);

Step 5 You can enter the login interface for device configuration by selecting your role and entering a password on the login interface. The default administrator password is **admin**.

Note

The device is only allowed to access using HTTPS. Since the factory default certificate is used, a prompt like "There is a problem with this website's security certificate" may occur. Click **Continue to this website** to access the login page.

Figure 1-11 Login interface

Table 1-8 Login parameters

Item	Description
Language	Select a language.
Role	The Web utility provides two authority levels: • An administrator is allowed to make changes to any configuration, such as login passwords. After login, "Welcome Admin" is displayed on the upper left corner. • An operator is allowed to navigate configuration pages and make limited changes to configurations. After login, "Operator" is displayed on the upper left side of the interface. The device allows multiple users to log in, in which case the first user can modify, while others can only browse. After login, "Welcome User" is displayed on the upper left side of the interface. **Note:** In the "Welcome user" mode, the operation only can browse certain pages. The pages that cannot be browsed include: **Advanced** > **Security**, **System tool** > **Change password**, **System tool** > **Software upgrade**, **System tool** > **Import data**, **System tool** > **Export data**.
Password	The default administrator password is admin. The default operator password is operator Please change the default password after the first time logging in to the Web utility to keep it secure. For details, see 2.9.3 Change Password.

1.3 Web GUI overview

The web management interface of the OM includes three areas: System button area, Menu bar, and Configuration area.

Figure 1-12 Web GUI layout

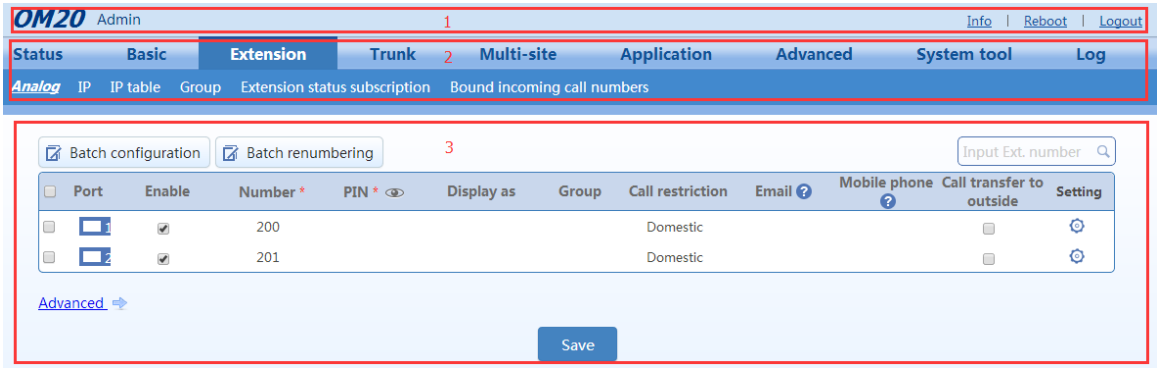


Table 1-9 Web management interface layout

Item	Description
1 System button area	Contains buttons such as Reboot, Logout, and Product information; and displays the identity of the current login user.
2 Menu bar	Displays submenus for your selection when the mouse pointer is moved onto a menu. The selection result is displayed in the configuration area.
3 Configuration area	View or modify or view configuration.

1.4 Network Configuration

1.4.1 Network Settings (OM20/50)

Go to **Basic** > **Network** to set IP address according to the installed network environment.

The IP address is shared by PC port and WAN port. By default, it is obtained through DHCP. If no IP address is obtained, 192.168.2.218 is used by default.

Figure 1-13 Network configuration interface

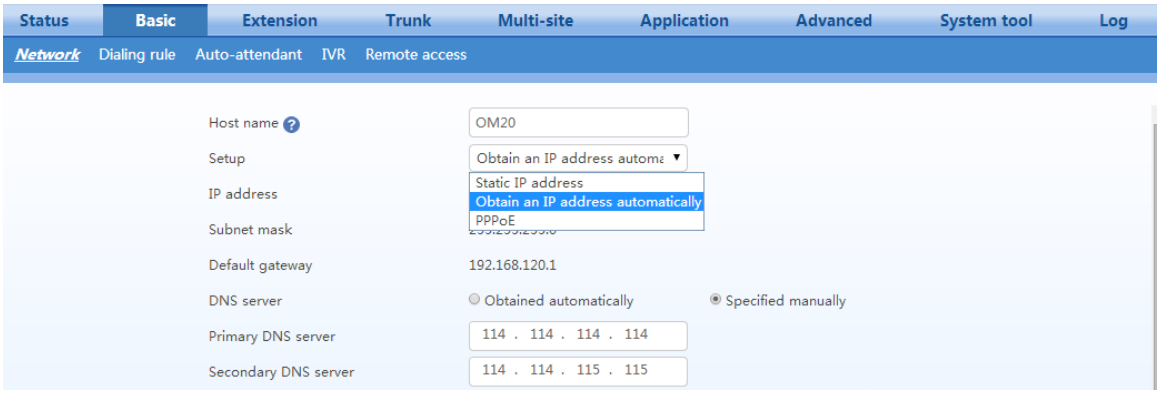


Table 1-10 Network parameters

Item	Description
Setup	Methods for obtaining an IP address. • Static IP address: static IP address is used. • Obtain an IP address automatically: use the dynamic host configuration protocol (DHCP) to obtain IP addresses and other network parameters. • PPPoE: use PPPoE to obtain IP addresses and other network parameters.
Username	Enter an authentication user name if PPPoE service is selected, and there is no default value.
Password	Enter an authentication password if PPPoE service is selected, and there is no default value.
IP address	If “Static IP” or “DHCP” is selected but an address fails to be obtained, the gateways will use the IP address filled in here. If the gateways obtain an IP address through DHCP, the system will display the current IP address automatically obtained from DHCP.
Subnet mask	The subnet mask is used with an IP address. When the gateway uses a static IP address, this parameter must be entered; when an IP address is automatically obtained through DHCP, the system will display the subnet mask automatically obtained by DHCP. It has no default value.
Default gateway	The IP address of the LAN gateway. When the gateway obtains an IP address through DHCP, the system will display the LAN gateway address automatically obtained through DHCP. It has no default value.

1.4.2 Network Parameters (OM80)

By default, network ports ETH1 and ETH2 of the OM80 are switch ports that share the same IP address configured for ETH1 on the **Basic** > **Network** page. The default IP address is 192.168.2.240.

For details about the ETH1 IP address, see Table 1-10.

The mode of the ETH2 can be changed. For details, see Table 1-11.

Figure 1-14 ETH2 configuration interface

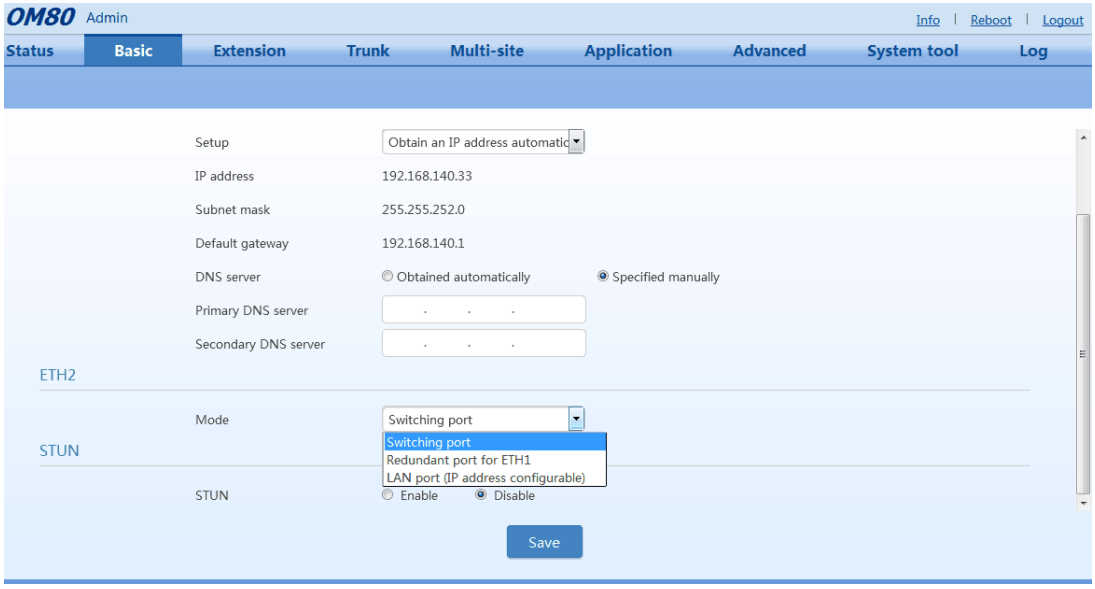


Table 1-11 ETH2 parameters

Item	Description
Mode	It can be configured as one of the following modes: ● Switch port: ETH1 and ETH2 are switch ports. The two ports share the IP address of ETH1 on the Web GUI. This mode is the factory default. ● Redundant port for ETH1: The port ETH2 is the redundant port for port ETH1. In this mode, both ETH1 and ETH2 are connected to the same LAN or WAN, and the two ports do not work simultaneously. ETH1 is used by priority. If ETH1 is damaged or offline, ETH2 automatically connects the network within 1.75 seconds to ensure network connection reliability. ● LAN port (IP address configurable): In this mode, ETH2 is used to connect to downlink voice devices such as an IP phone or voice gateway and it can be configured with an independent IP address. This mode is applicable when IP address resources of the uplink network are strained. Even when the uplink network can allocate only one IP address to the OM, the OM can still connect to other voice devices. The downlink voice device needs only an IP address in the same network segment as ETH2 to connect to the OM, without occupying IP address resources on the uplink network. The uplink network device load is thereby reduced, and communication between the OM and extensions is not affected by any faults in the uplink network device.
IP address	The IP address of ETH2. It is available only when the mode is set to LAN port. It is 192.168.2.2 by default.
Subnet mask	The subnet mask of ETH2. It is available only when the mode is set to LAN port. It is 255.255.255.0 by default.

1.4.3 DNS

When the device accesses a domain name, the device first requests the DNS server to translate the domain name to an IP address. The DNS server needs to be configured.

Step 1 Go to the **Basic** > **Network** to configure DNS server.

Figure 1-15 DNS server configuration interface

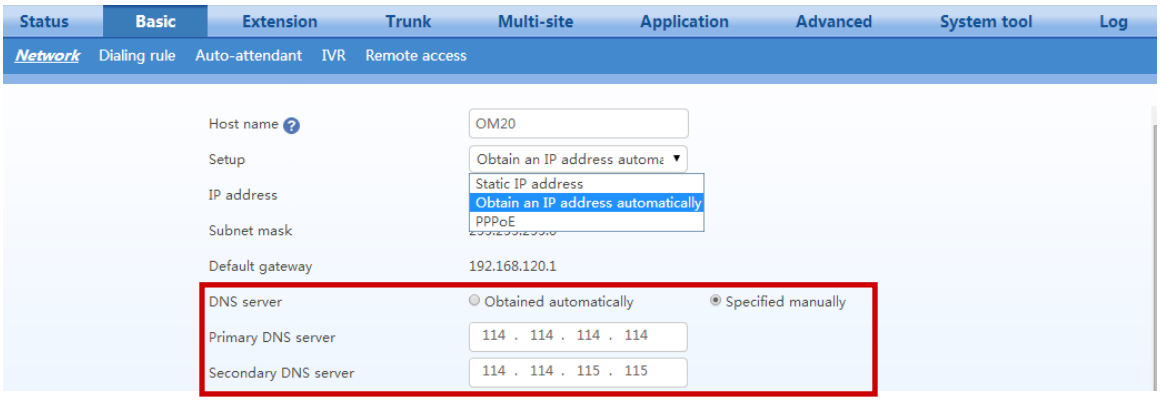


Table 1-12 DNS server parameters

Item	Description
Obtained automatically	The device automatically obtains the DNS server address by using DHCP or PPPoE. This option can be selected only when the network connection mode is set to **DHCP** or **PPPoE**.
Specified manually	Use the DNS server addresses specified manually. It is the default value.
Primary DNS Server	If **Specified manually** is selected, the network IP address of the **Primary DNS server** must be entered, and there is no default value. For OM20/50, it is 114.114.114.114 by default. For OM80, it is null by default.
Secondary DNS Server	If **Specified manually** is selected, the network IP address of the **Secondary DNS server** can be entered, and there is no default value. For OM20/50, it is 114.114.114.115 by default. For OM80, it is null by default.

1.4.4 STUN (RFC3489)

Go to **Basic** > **Network**, and set related parameters to obtain the public IP address of the front-end router by using the STUN function.

Figure 1-16 STUN configuration interface

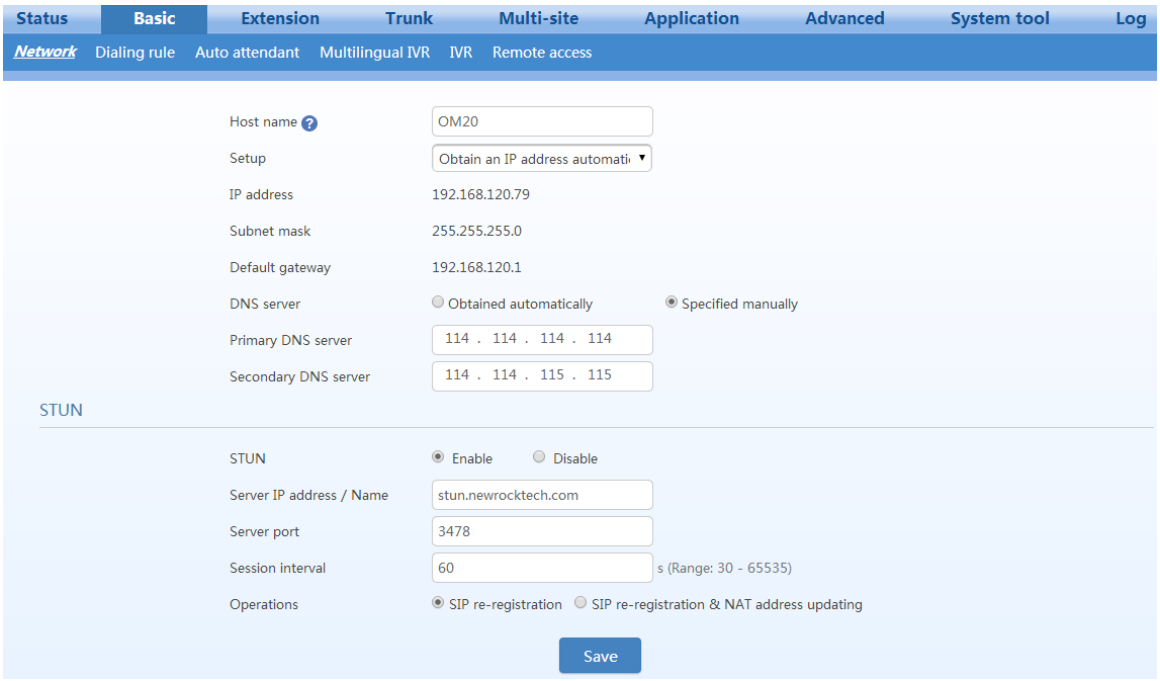


Table 1-13 STUN parameters

Item	Description
STUN	The device periodically sends a STUN request to the STUN server to obtain the public IP address for the front-end router. By default, it is enabled.
Server IP address / Name	Set the IP address or domain name of the STUN server. The default STUN server is the New Rock STUN server at stun.newrocktech.com.
Server port	Set the port of STUN server. It is 3478 by default.
Session interval	The interval at which the device sends a STUN request ranges from 30 to 3600 seconds.
operations	• **Trunk re-registration**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. Normally, the session interval of STUN request should be shorter than the registration period. Note: The IP address obtained through STUN is used only for re-registration with the SIP server and it is not used in SIP message fields such as Via and Contact and SDP C field. • **Trunk re-registration & NAT address updating**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. And the IP address obtained through STUN is used in SIP message fields such as Via and Contact and SDP C field.

1.4.5 Remote Access with NAT Traversal

When the OM is located in the intranet (the private network), if you register with the system from an external IP extension or if multi-site networking is used, it is necessary to configure remote-address information and configure port mapping on the Internet ingress router. This enables devices on external

networks to traverse NAT to get access to the OM.

Follow this procedure:

Step 1 Click **Basic** > **Remote access**, and set remote address.

Figure 1-17 Remote access configuration interface

Table 1-14 Remote access parameters

Item	Description
Build-in DDNS of the device	This option should be selected when the ingress router does not have a static IP address and nor DDNS support. The device will perform DDNS queries to determine its external IP address using the provided credentials. The domain name, user name, and password must be obtained from the DDNS service provider. The OM supports the following DDNS service providers: Dyndns.org, freedns.afraid.org, and www.no-ip.com.
External IP	This option should be selected when the ingress has a static IP address. In the **WAN IP address** field, enter the public IP address of the WAN port on the router.
External host name (DDNS on the router)	This option can be selected when the ingress of the external network does not have a static IP address. You need to enter the DDNS domain name of the WAN port on the ingress router.

Step 2 Click **Save**.

Step 3 Configure port mapping on the Internet ingress router. Take a New Rock WROC3000 as an example to show the ingress router configuration:

Figure 1-18 Port-mapping configuration interface

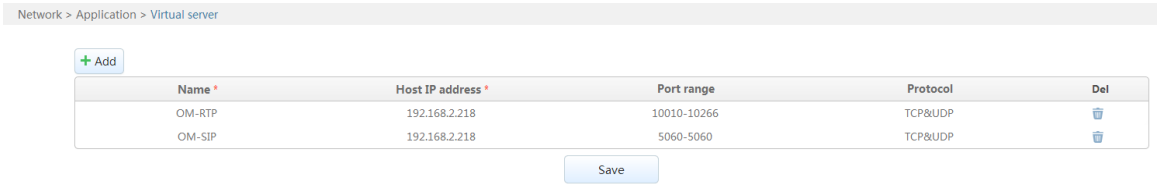


Table 1-15 Port mapping parameters

Item	Description
Host IP address	Enter the IP address of the OM. The current IP address of the device can be seen in the network part on the **Status** interface of the OM. Note: It is a must to set a static IP address which can be configured on **Basic** > **Network** page. For the OM80, it is the ETH1 IP address.
Port range	Enter the SIP signaling port and the RTP port range of the OM. You can go to **Trunk** >**IP trunk**> **Registrar OPTIONS** to view the SIP signaling port. You can view the maximum value and minimum value of the RTP port on the **Application**>**Media** interface. Note: Keep the mapping target port number the same as the port number of the OM.

Step 4 On the external IP extension, set the registrar address to the IP address or domain name configured on the **Basic** > **Remote Access** page.

2 Features

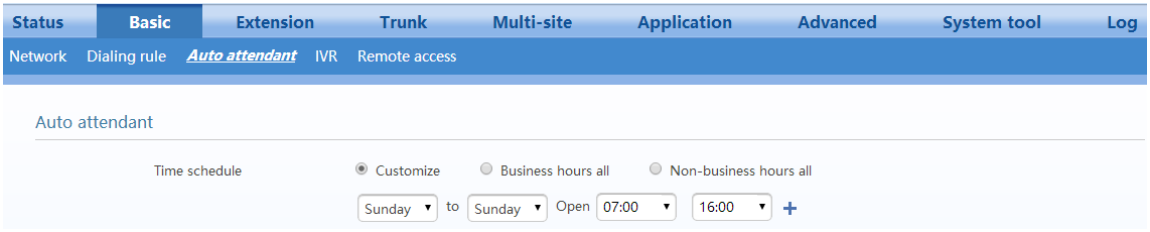
2.1 Auto Attendant

2.1.1 Auto Attendant

Incoming calls can be directed to auto attendants to provide immediate and professional service to callers. You can schedule different auto attendants to play, based on the time and day of the week. The greetings for business hours or non-business hours can be configured in **Greetings**.

Step 1 Go to **Basic** > **Auto attendant** to enter **Auto attendant configuration interface.**

Figure 2-1 Auto attendant configuration interface



Step 2 Assign time schedule. The default is business hours all.

Table 2-1 Auto attendant parameters

Item	Description
Customize	You can set the range of business hours in a week. The hours outside of business hours are non-business hours. You can click + to divide one day into up to three business-hour segments. The device will play corresponding greetings according to the preset business hours or non-business hours.
Business hours all	The device plays business-hour greetings at any time.
Non-business hours all	The device plays non-business-hour greetings at any time.

Step 3 Click **Save** to save the configuration.

2.1.2 Greetings

The device gives a greeting message to the caller when a call comes in.

Either of the two default greeting files can be used as shown in Table 2-2, or new greeting files can be made. For details, see **Generate new greeting files**.

Table 2-2 Default greeting files

Type	File name	Content
Business hours	welcome	Thank you for calling. If you know your party's extension, please dial it now. Or, to transfer to an operator, press zero.
Non-business hours	Off-hour	Thank you for calling. Our office is closed. If you know the extension, please dial it now.

Configuring auto-attendant greetings

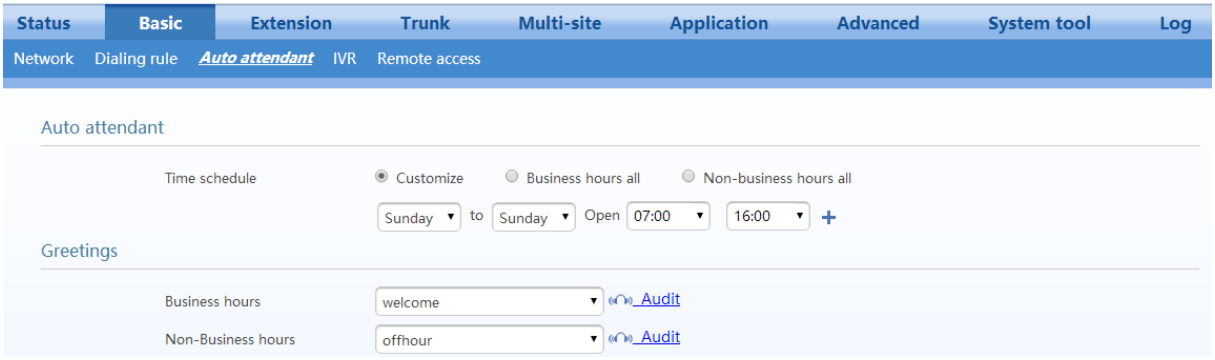
By default, every trunk uses auto attendant greetings which can be different for business and non-business hours.

Follow this procedure:

Step 1 Go to **Basic** > **Auto attendant** to select desired audio files for **Business hours** or **Non-business hours** greetings.

Either default greeting files or newly generated greeting files can be selected.

Figure 2-2 Interface to selecting greeting files



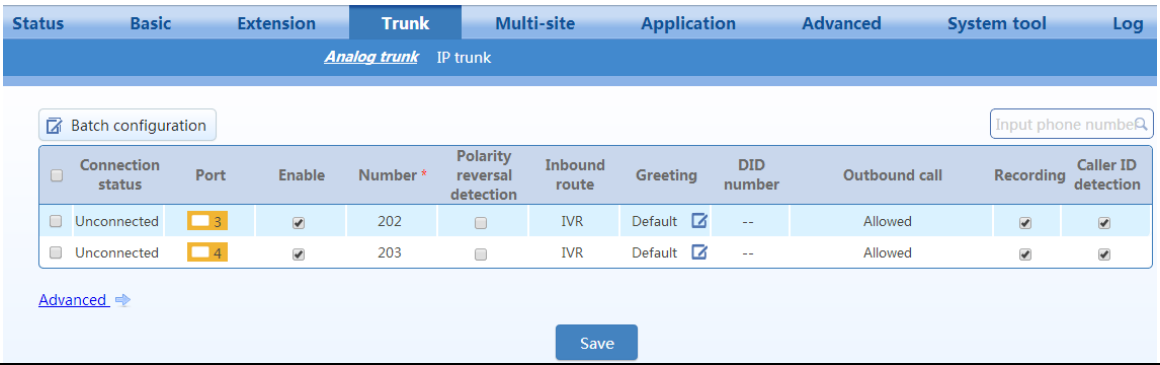
Step 2 Click **Save** to save the configuration.

Configure greetings for each trunk

The device can associate a dedicated greeting to a specific trunk. The greeting file is available for both business hours and non-business hours. Follow this procedure:

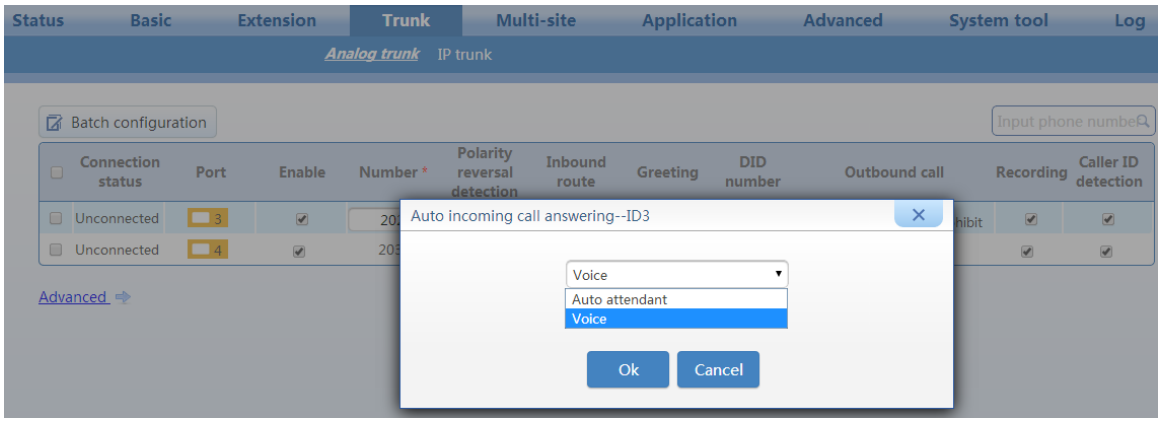
Step 1 Click **Trunk** > **Analog trunk / IP trunk** and click .

Figure 2-3 Interface to select greeting files for trunk (1)



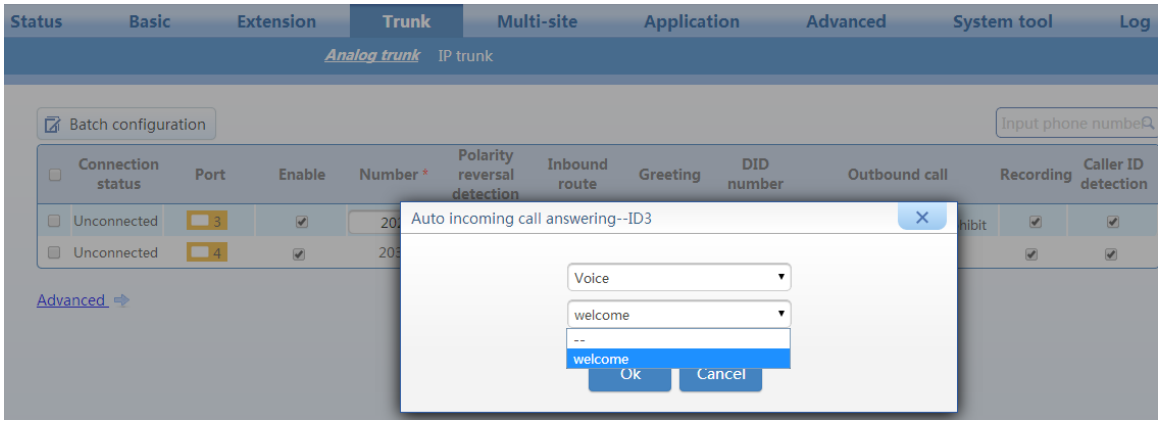
Step 2 Choose **Voice** in the dropdown list.

Figure 2-4 Interface to select greeting files for trunk (2)



Step 3 Choose the desired audio file.

Either default greeting files can be used, or new greeting files can be made. For details, see **Creating new greetings**.



Step 4 Click **Save** to save the configuration.

Creating new greetings

The following three methods can be selected:

- Text-to-greeting conversion
- Recording the greeting file on a phone
- Upload greetings

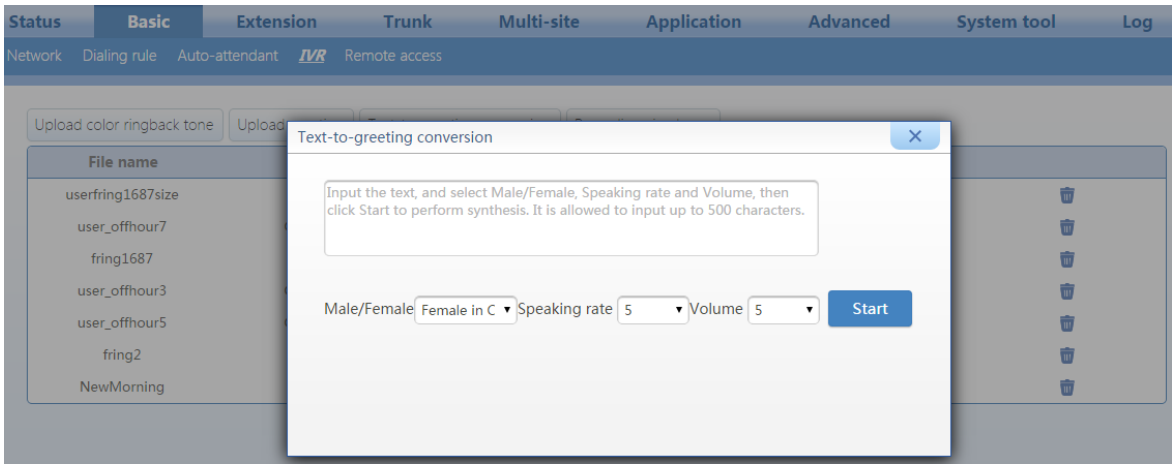
1) Text-to-greeting conversion

This is a simple way to customize the greetings in Chinese or English with high voice quality. The synthesizing service offered by New Rock Technologies, Inc. is powered by a speech-synthesis engine which is accessible on the Internet. To perform the synthesis, the device is required to be connected to the Internet. Follow this procedure:

Step 1 Go to **Basic** >**Network** page to configure DNS server. For details, see 1.4.3 DNS.

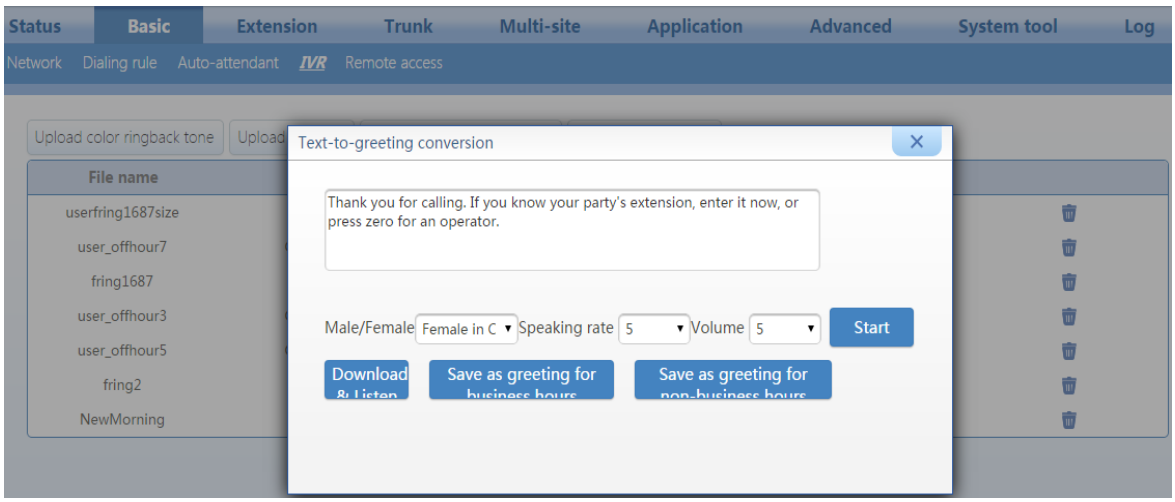
Step 2 Go to **Basic** > **IVR** > **Text-to-greeting conversion** page. Enter the greeting content in English and click **Start**.

Figure 2-5 Text-to-greeting conversion interface 1



Step 3 After synthesis, you can **Download & Listen** or save as a greeting for business hours or non-business hours.

Figure 2-6 Text-to-greeting conversion interface 2

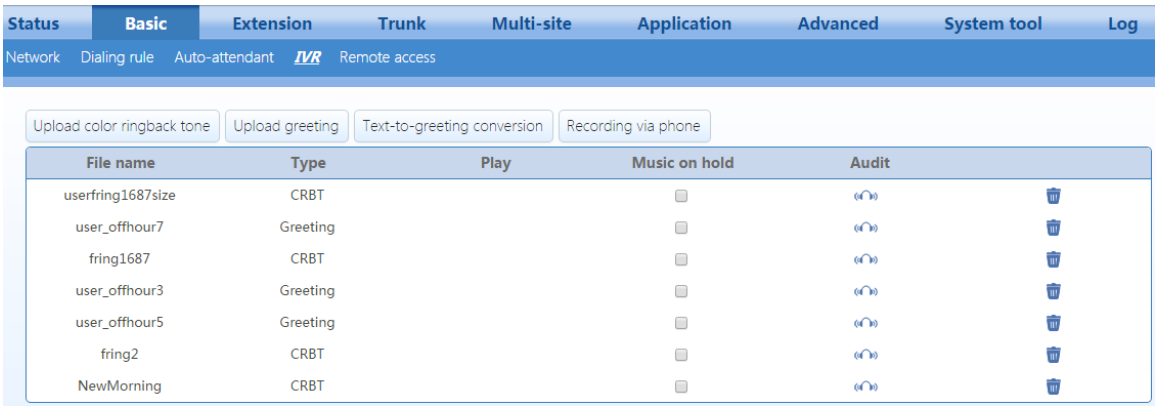


Note

Please ensure that the device can access the Internet before starting the text-to-greeting conversion.

Step 4 You can also audit or delete the saved greetings for business hours or non-business hours.

Figure 2-7 IVR interface



2) Recording by phone

The greeting file can be recorded directly on an IP or analog phone that is connected to the device. To ensure high quality, it is recommended to make the recording in a quiet environment.

Table 2-3 Recording a greeting file by phone

Item	Description
Recording	Pick up any phone connected to the device and press *81 to start the recording after the prompt, and hang up to finish the recording.
Listen	Press *8200 to listen to the voice recording
Save	• Press *8301 and hang up to replace the welcome file. • Press *8302 and hang up to replace the off-hours file.
Play the latest greeting file	• Press *8201 to listen to greetings; • Press *8202 to listen to off-hours greetings.
Recovery	Press *8300 to recover a replaced voice greeting file.

Note

Never restart your device during recording.

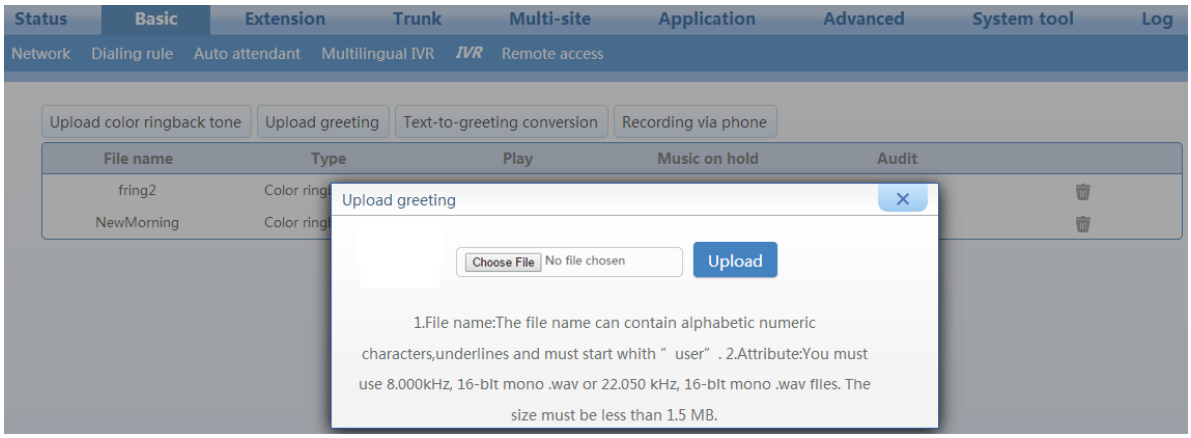
3) Upload greetings

Your customized greetings must be converted into an 8 kHz, 16-bit mono .wav file that can be used on device Telegreeting, an audio-file-conversion tool developed by New Rock. You can download the Telegreeting from

http://www.newrocktech.com/ViewProduct_E.asp?id=61.

Step 1 Go to **Basic** > **IVR** > **Uploading greeting**.

Figure 2-8 Interface to upload greetings



Step 2 Click **Choose File** to select the audio files for uploading.

Step 3 Click **Upload**.

Note

- The name of the audio file to be uploaded should begin with "user", and can contain letters, digits or underscores only. You must use a .wav file format.
- The sampling rate of the .wav file can only be 22.050 kHz or 8.000 kHz.

2.1.3 Operators/Receptionists

When the caller dials default-number 0, the call is transferred to an operator. By default, the first FXS port is reserved for the operator with the extension number 200. For devices without an FXS port (such as OM20-NA), no default operator is available.

But to add an operator or modify other related information, follow these procedures:

Step 1 Go to **Basic** > **Auto Attendant** to configure **First digit timeout** and **Operator** settings.

Figure 2-9 Auto attendant configuration interface

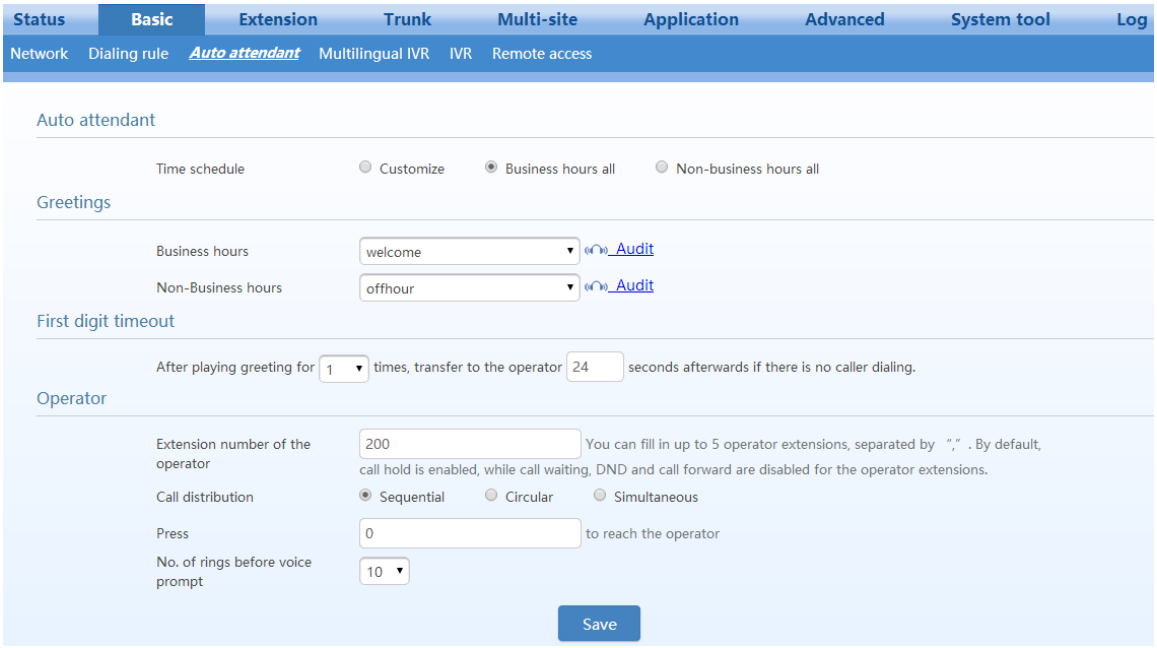


Table 2-4 Auto attendant parameters

Item	Description
First digit timeout	The device plays a greeting to incoming callers. The call will be transferred to the operator within the preset time after the greeting is played. After playing the greeting the first time, transfer it to the operator after 24 seconds if there is no caller dialing.
Operator	• **Extension number for the operator**: You can fill in up to five extension numbers, separated by a comma in this format: ",". The default extension number is 200. Call waiting and DND are disabled by default. The call transfer function for the receptionist's extension will function only during non-business hours. **Note**: No default extension number for an operator exists on a non-FXS device (e.g. OM20-NA, OM50-8FXO). • **Call Distribution**: Select a call distribution scheme below when there is more than one operator: - **Sequential**: Terminate the incoming call to the first available extension on the operator list starting from the first one. - **Circular**: Terminate the incoming call to extension in Round-robin order; - **Simultaneous**: Terminate incoming calls to all available extensions on the operator list simultaneously and the first one to pick up is connected. • **Press (number) to reach the operator**: The number to reach the operator. The default value is 0. **Note:** If the default value is changed, you must modify related greetings, such as "To transfer to an operator, press zero". • **No. of rings before voice prompt**: The device will play prompts when the number of rings reaches the value set here. The default value is 10.

Step 2 Click **Save** to save the configuration.

2.1.4 Multilingual IVR (OM20/50)

With the multilingual IVR function, caller of incoming call can press a button to choose a language based on the navigation menu.

Note: This interface is not be displayed if all voice prompt packages on the **System tool** > **Voice prompt packages** page are deleted (there are two voice prompt packages by default).

Step 1 Click **Basic** > **Multilingual IVR**.

Step 2 Enter the language description, such as “Chinese and English greetings”.

Step 3 Choose an audio file on the **Greeting file** list.

This file guides the caller to select a language for the following voice prompt, for example, “Welcome. For Chinese, press 0. For English, press 1.” For details on how to generate an audio file, see the section on **Generating new greeting files**.

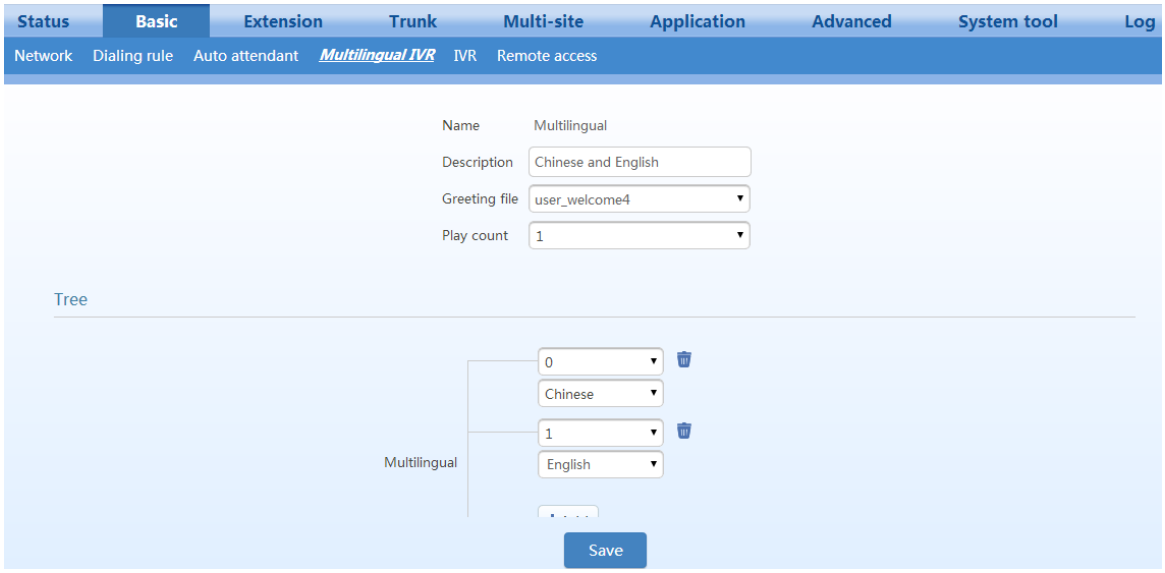
Step 4 Set the number of times the IVR will play on the **Play count** field. The default value is 1.

Step 5 Match the button with a language.

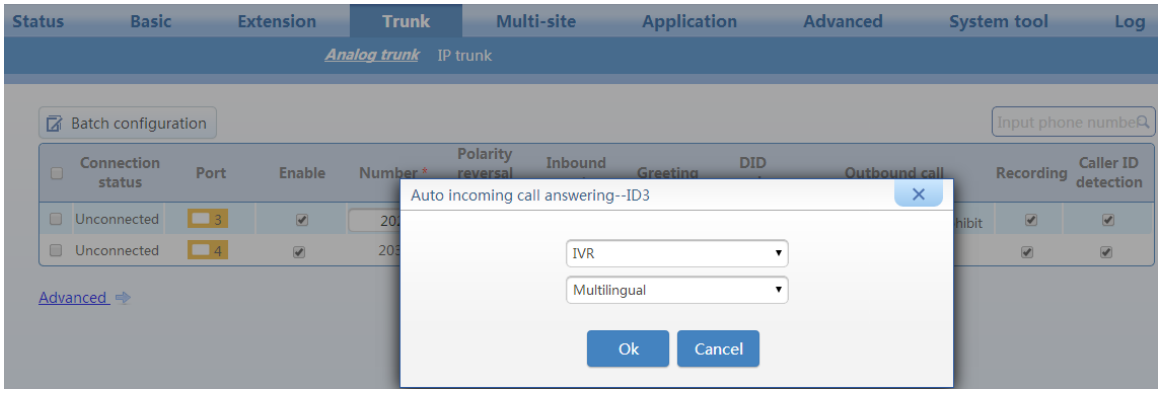
The settings must be consistent with the guidance of the audio file chosen in Step 3. For example, if the audio file asks the caller to press 0 for Chinese, match button 0 with the Chinese voice prompt package. After the caller presses 0, the system plays the “welcome” audio file of the “Chinese” voice prompt package. Please go to **System tool** > **Voice prompt packages** and upload “welcome” audio files for customizing greetings of different languages.

Step 6 Click **Save**.

Figure 2-10 Multilingual IVR navigation configuration interface



Step 7 Go to **Trunk > Analog trunk/IP trunk** page, select IVR for inbound route and click . In the displayed dialog box, choose **IVR** and **Multilingual**, and click **OK**.



2.1.5 Voice prompt packages (system voice prompt files) (OM20/50)

Each voice prompt package contains all system voice prompt files for a language. For details of the system voice files, see Table 2-5.

To upload a voice prompt package, follow this procedure:

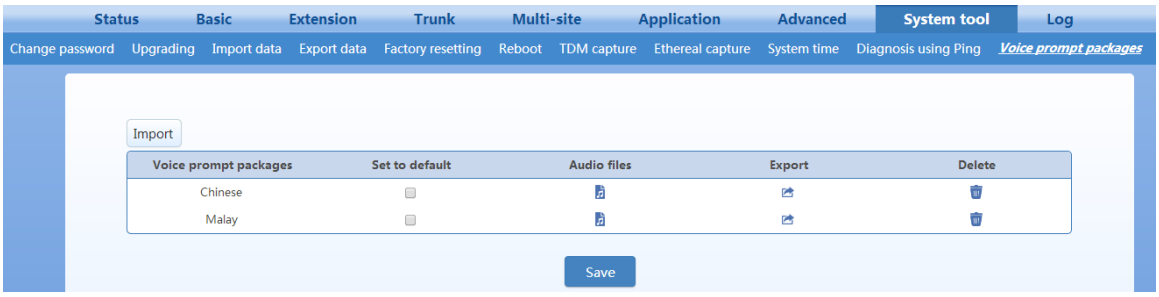
Step 1 Go to **System tool** > **Voice prompt packages**.

Step 2 Click **Import** to import the prepared voice prompt package.

Please use Telegreeting, an audio file conversion tool developed by New Rock Technologies, Inc., to prepare voice prompt package. For details, see *User Guide for Telegreeting*.

Step 3 Enable the **Set to default** checkbox to set a default language for system voice prompt.

Figure 2-11 Voice prompt packages interface



Step 4 If required, upload an audio file to replace the existing file.

Figure 2-12 Audio file configuration interface

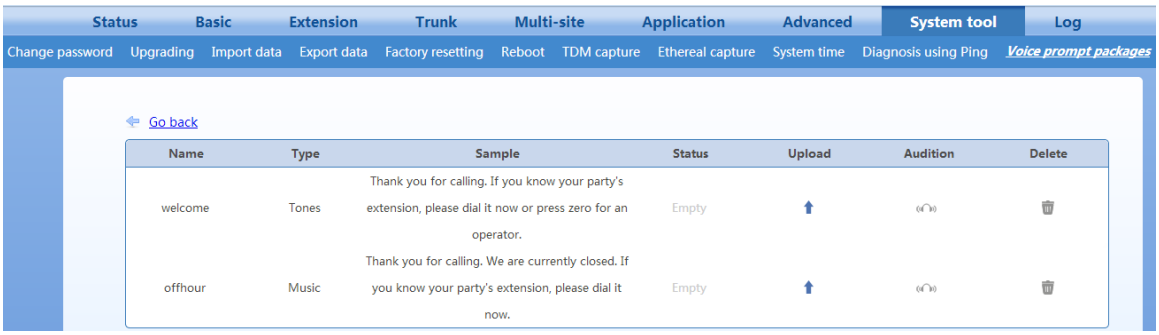


Table 2-5 System voice prompt files

File	Content
0_tip	Zero
1_tip	One
2_tip	Two
3_tip	Three
4_tip	Four
5_tip	Five
6_tip	Six
7_tip	Seven
8_tip	Eight
9_tip	Nine
account	Please enter the extension number, followed by the PIN.
block	You are not authorized to make this call. Please contact the administrator.
busy	That line is busy. Enter another number now, or hold for an operator.
callwaiting	Please hold. That line is busy, but your party has been notified of your call.
cancel	The feature is now deactivated.
confirm	The feature is now activated.
connect	Please hold while your call is transferred.
disable	Disable.
dnd	The extension you are trying to reach has do-not-disturb activated. Please hang up.
dot_tip	Dot.
enable	Enable.
gateway	Gateway.
groupbusy	Please hold. All lines are busy.
hangup	Your call is being disconnected. Thank you for calling.
hangup2	This call will be disconnected in one minute.
ip_tip	IP address.
IVR1	For call forward, press one. For voicemail, press two. Do not disturb: three. Call forking: four. Call waiting: five. Color ringback tone: six. For other extensions, press seven. To repeat this message, press nine.
IVR2	Enter the extension number, followed by the PIN then pound.
IVR3	Sorry, the feature cannot be activated.
IVR4	To obtain the current settings, press star; To return to the previous menu, press pound.
IVR5	The feature is now activated.
IVR6	Sorry, the feature cannot be activated.
wrong	Sorry, the feature cannot be activated.
IVR7	The feature is now deactivated.
IVR8	This is an invalid PIN, please enter a new PIN.
reenter	This is an invalid PIN, please enter a new PIN.

File	Content
IVR9	The current setting is___
setting	The current setting is___
IVR10	To activate do not disturb, press one. To deactivate, press zero.
IVR11	To disable voicemail, press zero. To forward all calls to voicemail, press one. To forward busy or no-answer calls to voicemail, press two.
IVR12	To listen to the color ringback tone, press star. To change, press two, To disable, press zero. To return to the previous menu, press pound.
IVR14	To set the target number, press one.
IVR14A	To disable call forking, press zero. To enable and set destination number, press one.
IVR15	Enter the extension number, followed by the PIN. When done, press pound.
IVR16	To disable call forward, press zero. To set the target number, press nine. To forward all calls, press one. To enable call forward busy or no answer, press two. To obtain the current settings, press star; To return to the previous menu, press pound.
IVR18	This is an invalid PIN, please enter a new PIN.
netmask	Netmask.
noanswer	There is no answer. Please enter another number, or hang up.
nocircuit	All circuits are busy. Please try your call again later.
nonumber	The number you have entered is not valid. Please check the number and enter again, or press zero for an operator.
offhour	Thank you for calling. We are currently closed. If you know your party's extension, enter it now.
operator	Please hold while your call is transferred to an operator.
operbusy	All operators are busy. Please enter another number or press star to hold.
port	Port.
record	Please record your message at the tone, and hang up when done.
tryagain	Your call cannot be completed, please try again later
version	Firmware version.
vm_all	Your call will be forwarded to voicemail. Leave your message at the tone and hang up when done.
vm_busy	That line is busy. Leave your message at the tone and hang up when done.
vm_fail	Your call cannot be completed, Leave your message at the tone and hang up when done.
vm_noans	Your party did not answer. Leave your message at the tone and hang up when done.
webport	Web access port
welcome	Thank you for calling. If you know your party's extension, enter it now, or press zero for an operator.

File	Content
vm_new	___ new voicemail messages.
vm_no	You have no voicemail messages.
vm_old	___ saved voicemail messages.
vm_pre	You have ___
vm_prompt	To repeat the message, press one. To delete, press two. To listen to the next message, press three.
wakeup	Hello, this is your scheduled notification.
btime	Sorry, you are not authorized to make calls at this time, please contact the administrator.
binternal	Sorry, you are not authorized to make outgoing call, please contact the administrator.
lock	Sorry, your extension is locked. Please unlock it.
bres	Sorry, you are not allowed to call this number.
bdomestic	Sorry, you are not authorized to make international calls, please contact the administrator.
blocal	Sorry, you are not authorized to make long distance calls, please contact the administrator.

2.2 Trunk

2.2.1 Analog trunks

Follow this procedure:

Step 1 Go to **Trunk** > **Analog trunk** to configure the analog trunk settings.

Figure 2-13 Analog trunk configuration interface

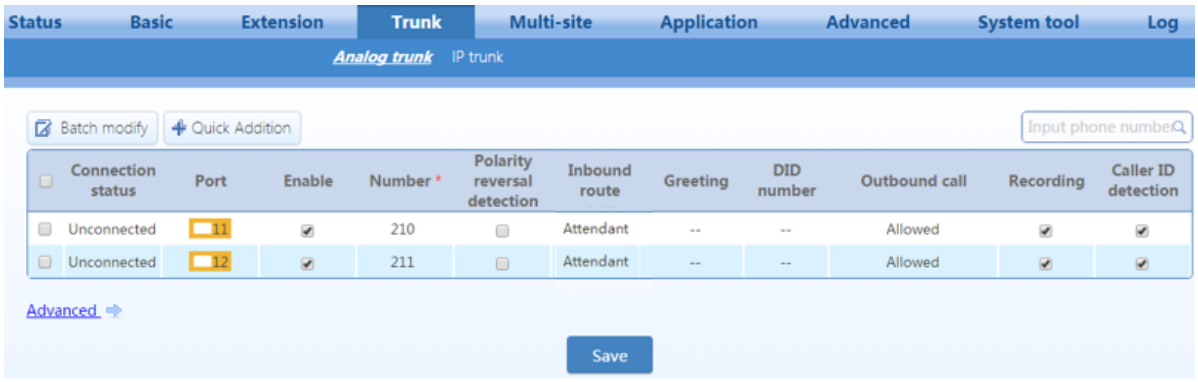


Table 2-6 Analog trunk parameters

Item	Description
Connection status	Displays whether the current port is connected to an analog trunk.
Port	FXO port number on the device.
Enable	Select to enable the line. By default, the trunk line is enabled.
Number	The trunk number will be displayed as the calling number when the incoming call number is not displayed or the caller ID is disabled, so it is recommended to use an actual trunk number. The number is 2xx by default.
Polarity Reversal Detection	Calls will be processed in the loop-start signaling mode if no polarity reversal signal is detected after the polarity reversal detection function is enabled.
Inbound route	Select the destination for an external number calling into device through an inbound route: • **Attendant:** Direct the received calls to auto attendant. • **DID:** Direct the received calls to the extension specified in **DID number** without passing through the auto attendant.
Greetings	Select the greeting for the trunk. By default, the greetings for the auto attendant are used the **Basic** > **Auto attendant** page). Different attendant greetings can be played for business hours and non-business hours. However, the greeting for a single trunk cannot be customized to the time. **Note**: When the **Inbound route** is set to **Attendant**, this item needs to be configured.
DID number	Enter the number of extension or hunting group that is bound to the trunk. **Note**: When the **Inbound route** is set to **DID**, this item needs to be configured.
Outbound call	When the **Inbound route** is configured as **Attendant**, there are two choice : • **Allowed:** Allowed to make outbound calls; • **Pickup prohibit:** Not allowed to make outbound calls. When the **Inbound route** is configured as **DID**, there are two choice : • **Share:** Other extensions are allowed to make outbound calls. • **DID only:** Only the extension or hunt group specified in **DID number** is allowed to make outbound calls through this trunk. And the bound extensions can only use this trunk to make outbound calls.

Item	Description
Recording	Enable recording for the trunk. **Note:** To enable the trunk recording, you need to enable the recording function on the **Application** > **Recording** page at first. For details, see 2.5.1 Recording.
Caller ID detection	Allow the extension to display the caller ID detected from a received call over the trunk. If no caller ID is detected or the caller ID is disabled, the trunk number will be displayed. **Note:** You need to enable the **caller ID delivery** for the extension.
Advanced	Configure advanced properties of an analog trunk.

Step 2 Click **Advanced** to enter the advanced settings of an analog trunk. The parameters relate to the volume, the caller ID detection, and busy tone detection of a trunk. There is no need to make changes to the default values, unless there is an issue with one of the functions.

Figure 2-14 Analog trunk advanced configuration interface

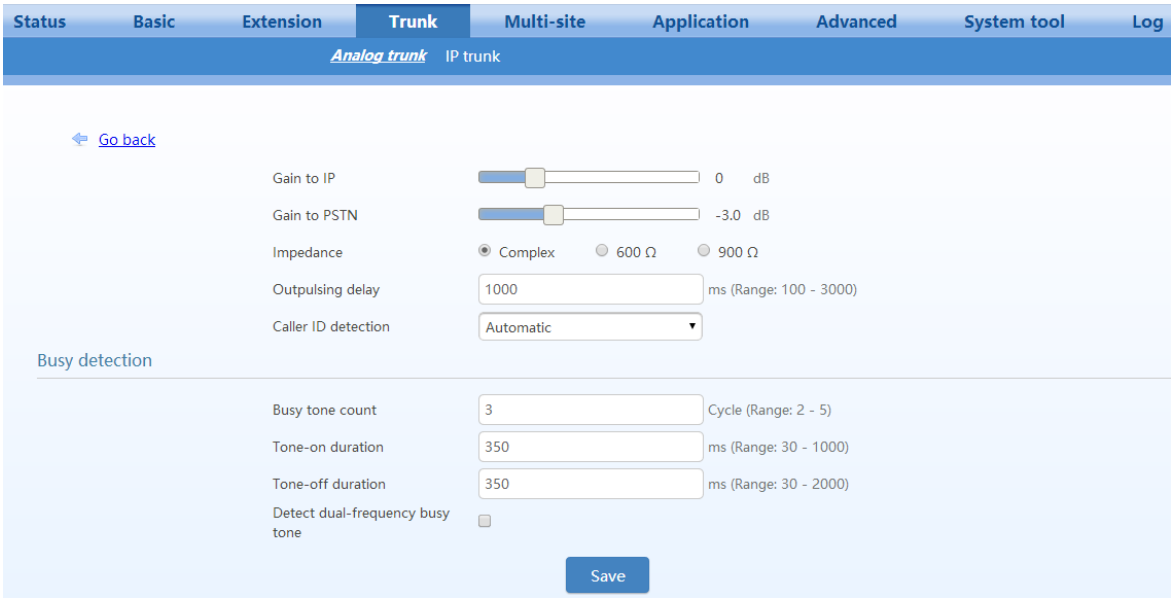


Table 2-7 Analog trunk advanced parameters

Item	Description
Gain to IP	Adjust the call volume received on the FXO port. Increase the value when the volume received by internal party is low. Range: -3.0 to +9.0 dBs.
Gain to PSTN	Adjust the call volume sent from the FXO port. Increase the value when the volume received by external party is low. Range: -6.0 to +3.0 dBs.
Impedance	If there is echo on the PSTN side, this parameter can be adjusted. Otherwise, accept the default value.
Outpulsing delay	The interval between FXO off-hook to sending the DTMF called number. If the value is too small, the peer device could miss a number; too large, it might increase the call connection time. Otherwise, accept the default value.
Caller ID detection	Select the caller ID detection mode according to the features of the peer switch. The default value is **Automatic**, which indicates the device detects **after ringing** or **before ringing** automatically.

Item	Description
Busy tone count	Compares the count of busy tones with the detection threshold. If the count is less than the detection threshold, the device will ignore the received signals. Range: 2 to 5.
Tone-on duration	The tone on period for the cadence on-off cycle of busy tone. The value is varied depending on the standard for your country/area. By default, the value is 350ms. For details, please see 2.8.8 Call Progress Tone.
Tone-off duration	The tone off period for the cadence on-off cycle of busy tone. The value is varied depending on your country or area. By default, the value is 350ms. For details, please see 2.8.8 Call Progress Tone.

2.2.2 IP Trunk

The OM supports standard SIP specifications and Skype Connect. Before setting the IP trunk, you need to obtain an account from your ITSP.

Follow this procedure:

Step 1 Go to **Trunk** > **IP trunk.**

Step 2 Click **Add**, enter the registration information.

Note: To register trunks to different SIP servers, go to **Trunk** > **IP trunk** > **Register OPTIONS** and enable **Permit to use multiple ITSPs** first.

Figure 2-15 IP trunk configuration interface

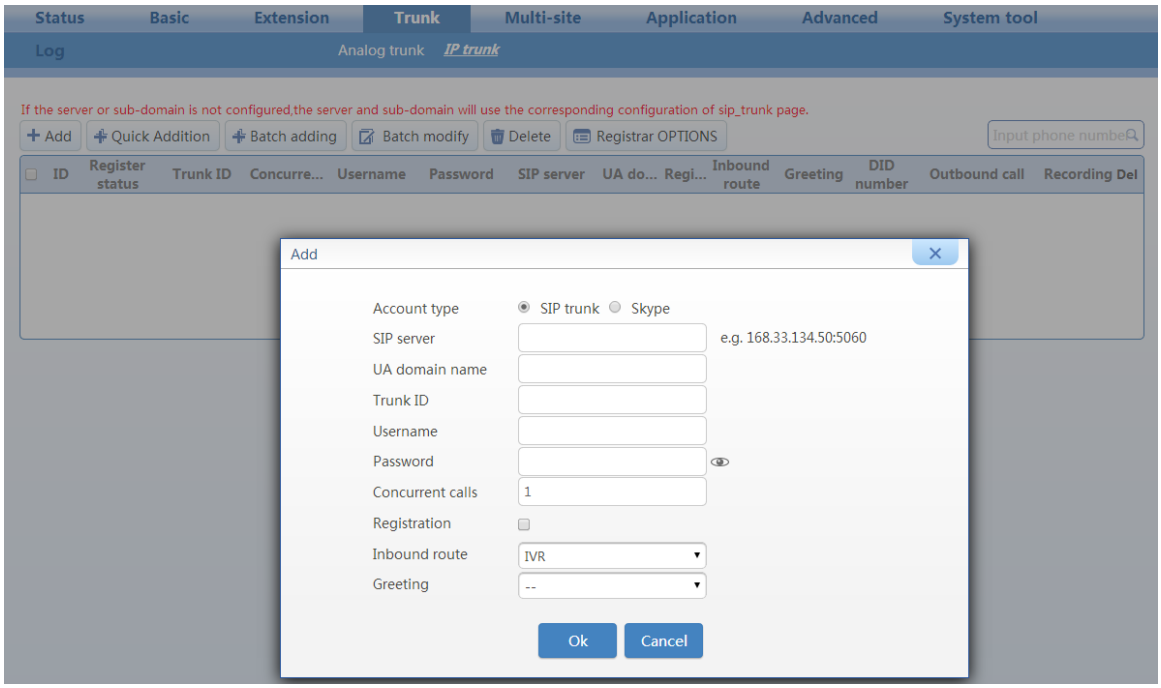


Table 2-8 IP trunk registration parameters

Account type	Item	Description
IP trunk	**SIP server**	Enter the server IP address and port provided by the ITSP.
	UA domain name	Provided by your ITSP, for example, salesdepart.abccompany.com.

Account type	Item	Description
	Trunk ID	Provided by your ITSP.
	Username	Provided by your ITSP. It is used for authentication when registering an IP trunk. If no username is entered, the trunk ID will be used for authentication.
	Password	Provided by your ITSP. The password is encrypted by default. Please contact your service provider if you forgot the password. The registration password can contain up to 16 characters if encryption is enabled (The password can contain up to 30 characters if encryption is disabled).
	Concurrent calls	The number of concurrent calls supported by the trunk. Note that the total number of all trunks must not exceed the maximum number for the device. The OM50 supports a maximum of 30 concurrent calls, and the OM20 supports a maximum of 24 concurrent calls.
	Registration	Select this to enable registration.
	Inbound route	Select the destination for an external number calling into device through an inbound route: • **Attendant:** Handles the incoming calls from this trunk using the auto attendant. • **DID:** Binds the trunk to an extension. When a call is received, the device directs the call to the specified extension without passing through the auto attendant.
	Greeting	Select the greeting for the trunk. By default, the greetings for the auto attendant are used the **Basic** > **Auto attendant** page). Different attendant greetings can be played for business hours and non-business hours. However, the greeting for a single trunk cannot be customized to the time. **Note:** When the **Inbound route** is set to **Attendant**, this must be configured.
	DID number	Enter the number of extension or hunt group that is bound to the trunk. **Note:** When the **Inbound route** is set to **DID**, this item needs to be configured.
	Outbound call	When the **Inbound route** is configured as **Attendant**, there are two choice : • **Allowed:** Allowed to make outbound calls; • **Pickup prohibit:** Not allowed to make outbound calls. When the **Inbound route** is configured as **DID**, there are two choice : • **Share:** Other extensions can make outbound calls over the trunk. • **DID only:** Only the extension specified in **DID number** can make outbound calls over the trunk.
Skype Note: Please go to **Trunk** > **IP trunk** > **Register OPTIONS** and	**SIP User**	Input the SIP user of the SIP profile created in Skype Manager. To obtain SIP profile's registration details, see the *Skype Connect User Guide*.
	Password	Input the password of the SIP profile created in Skype Manager. The password is displayed as cipher text. Click to display the password in plain text.

Account type	Item	Description
enable **Permit to use multiple ITSPs** first.	**Skype Connect address**	Generally, it is **sip.skype.com**. It should be identical to the **Skype Connect address** of the SIP profile created in Skype Manager.
	UDP port	It is 5060 by default. It should be identical to the **UDP port** of the SIP profile created in Skype Manager.
	Registration	Select this to enable registration.
	Inbound route	Select the destination for an external number calling into device through an inbound route: • **Attendant:** Handles the incoming calls from this trunk using the auto attendant. • **DID:** Binds the trunk to an extension. When a call is received, the device directs the call to the bundled extension without passing through the auto attendant.
	Greeting	Select the greeting for the trunk. By default, the greetings for the auto attendant are used the **Basic** > **Auto attendant** page). Different attendant greetings can be played for business hours and non-business hours. However, the greeting for a single trunk cannot be customized to the time. **Note:** When the **Inbound route** is set to **Attendant**, this item needs to be configured.
	DID number	Enter the number of extension or hunting group that is bound to the trunk. **Note:** When the **Inbound route** is set to **DID**, this item needs to be configured.
	Outbound call	When the **Inbound route** is configured as **Attendant**, there are two choice : • **Allowed:** Allowed to make outbound calls; • **Pickup prohibit:** Not allowed to make outbound calls. When the **Inbound route** is configured as **DID**, there are two choice : • **Share:** Other extensions can make outbound calls over the trunk. • **DID only:** Only the extension specified in **DID number** can make outbound calls over the trunk.
	Add Skype Number	Skype number bound to the SIP account on the Skype website. For example: 13152880961.

Step 3 Click **OK** to return to the IP trunk setting interface, and view the registration status for the configured IP trunk.

Figure 2-16 IP trunk configuration interface

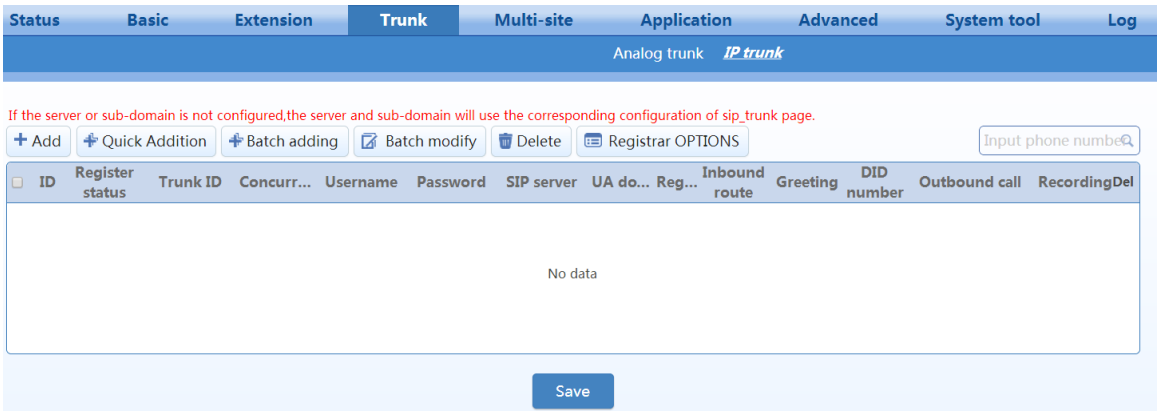


Table 2-9 IP trunk parameters

Item	Description
ID	Line number
Register status	Indicate the status of registration: • **Register success:** The IP trunk can be used. • **Register failure:** An error occurs during IP trunk registration and the IP trunk cannot be used. The issue can be determined according to the returned error code. • **Unregistered:** The registration option is not selected. • **Timeout:** The registration fails during the specified registration period and the IP trunk cannot be used. You need to check whether the account of the IP trunk is being used. • **DNS failure:** The registration of the IP trunk fails due to a failure in domain name resolution. You should go to the **Basic** > **Network** page to check whether the DNS server is correctly configured.
Trunk ID	See Table 2-8.
Concurrent calls	
Username	
Password	
SIP server	
UA domain name	
Registration	
Inbound route	
Greeting	
DID number	
Outbound calls	
Recording	Enable recording for the trunk. **Note:** To enable the trunk recording, you need to enable the recording function on the **Application** > **Recording** page at first. For details, see 2.5.1 Recording.
Delete	Deletes the current IP trunk.

Step 4 Click **Registrar OPTIONS**. You can modify information such as local signaling port and registration expiration. It is recommended to change the **Local signaling port** to prevent SIP attacks.

Figure 2-17 IP trunk registration interface

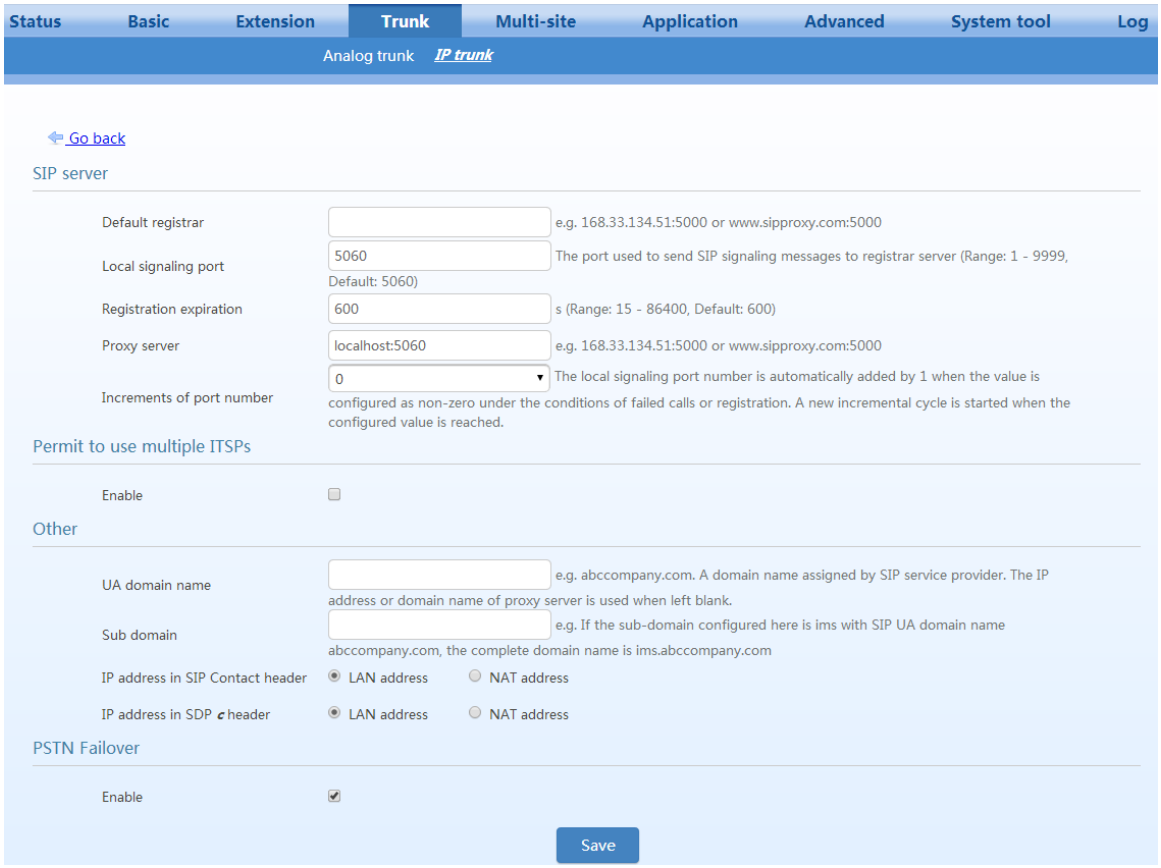


Table 2-10 IP trunk registration parameters

Item	Description
Default registrar	The address and port number of the default SIP registration server. The address and port number is separated by ":". It has no default value. The address can be an IP address or a domain name. e.g. 168.33.134.51:5000 or www.sipproxy.com:5000. When a domain name is used, DNS service must be activated and DNS server parameters configured on the **Basic** > **Network** page.
Local signaling port	The local SIP port used by the device to send SIP messages to the registrar server. It is 5060 by default and can be changed. It is recommended to change this port to prevent SIP attacks.
Registration expiration	Period for the device to register to the server. Range: 15 to 86400; default value: 600. It needs to be entered as required by the ITSP.

Item	Description
Proxy server	Generally, ensures that it is identical to the register server. If the ITSP provides a separate proxy server, it needs to be entered as required by the ITSP. When a domain name is used, a secondary IP address can be entered in **2.2.3** Backup SIP Proxy Server Settings. This enables the device to switch to this IP address when the domain name resolution service fails.
Increments of port number	The local signaling port number is automatically added by 1 when the value is configured as non-zero under the conditions of failed calls or registration. A new incremental cycle is started when the configured value is reached. **The times for Upon call or registration failure,**
Permit to use multiple ITSPs	To register trunks to different SIP servers, enable this function first. If disabled, the configured **Default registrar** will be used for the registration of each IP trunk.
UA domain name	A domain name assigned by the SIP service provider. For example: abccompany.com.
Sub domain	A sub domain name assigned by the SIP service provider. It works with the **SIP UA domain name**. If the domain name is set to **abccompany.com** and the sub domain name is set to **ims**, the full domain name is **ims.abccompany.com**.
IP address in SIP Contact Header	Set the IP address in the SIP Contact header field. If the device is used in an intranet (behind NAT) and one-way audio condition occurs during the outgoing call, you can try to rectify the one-way audio by adjusting this parameter. • **LAN IP address:** The LAN IP address configured by the device is used. • **NAT IP address:** The detected NAT IP address is used.
IP address in SDP c Header	Set the IP address in the Connect of SDP. If the device is used in an intranet (behind NAT) and one-way audio condition occurs during the outgoing call, you can try to rectify the one-way audio by adjusting this parameter. It is suggested to set as the same as the one for Contact header. • **LAN IP address:** The LAN IP address configured by the device is used. • **NAT IP address:** The detected NAT IP address is used.
PSTN Failover	Enables the failover function, so that when the IP trunk cannot be used due to a network failure, the call is made over analog trunk. Note: This function can be used only when the device has analog trunk port.

2.2.3 Backup SIP Proxy Server Settings

The second server is automatically used when the primary server of the IP trunk is unavailable.

Note: The primary server indicates the proxy server that is set in the **Trunk** > **IP trunk** > **Registrar OPTIONS** interface. If multi-platform is enabled, other SIP servers configured for SIP trunks do not support the backup mode.

Follow this procedure:

Step 1 Click **Trunk** > **IP trunk** > **Registrar OPTIONS**, and locate the **Second server**.

Figure 2-18 Secondary SIP proxy server interface

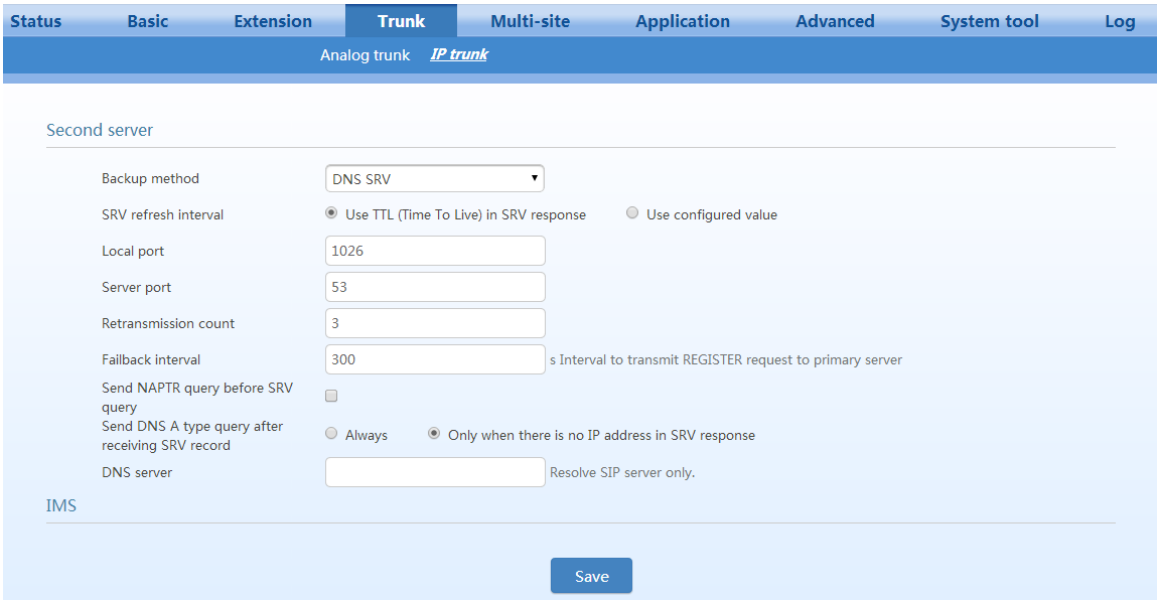


Table 2-11 Secondary SIP proxy server parameters

Parameters	Description
Backup methods	• **No backup:** Disable the second server configuration. When the primary server is unavailable, the secondary server will not be used for registration. • **Fixed:** Enable the second server configuration. The server IP address can be preset in the **Backup SIP proxy**. The IP address of the second server is provided by VoIP service provider. • **DNS SRV**: Enable the second server configuration. Multiple IP addresses can be obtained via DNS. The first IP address indicates the primary server, while the second indicates the second server.
SRV refresh interval	• **Use TTL (Time To Live) in SRV response:** Default configuration: • **Use configured value:** Customize the refreshing interval. The range is 1–65535s.
Local port	Used for sending DNS query requests. The default value is 1026.
Server port	The receiving port of the DNS server. The default value is 53.
Retransmission count	The times for the device to retransmit a DNS SRV query request to the DNS server when there is no response from DNS server. The default value is 3.
Failback interval	When the second server is used, the interval for the device to send a registration request to the primary server for failing back to the primary server can be set The default value is 300 s.
Send NAPTR query before SRV query	Configure whether to send a NAPTR query before a SRV query.
Send the DNS an A type query after receiving the SRV record	Set the conditions for sending an A type query, after a response to the SRV query request is returned. • **Always:** The A query request is always sent, regardless of the data type returned for the SRV query request. • **Only when there is no IP address in SRV response:** A query request is sent only when a domain name is returned for the SRV query request. This option is selected by default.
DNS server	It is only user to resolve SIP server.

Step 2 Choose **Backup method**.

Step 3 Click **Save** to save the configuration.

2.2.4 IMS

The OM can interwork with an IP Multimedia Subsystem (IMS) service network.

In addition to the configuration on the **Trunk** > **IP trunk** > **Add** interface, you must configure IMS information.

Follow this procedure to configure IMS information:

Step 1 Click **Trunk** > **IP trunk** > **Registrar OPTIONS**, and locate **IMS configuration**.

Figure 2-19 IMS configuration interface

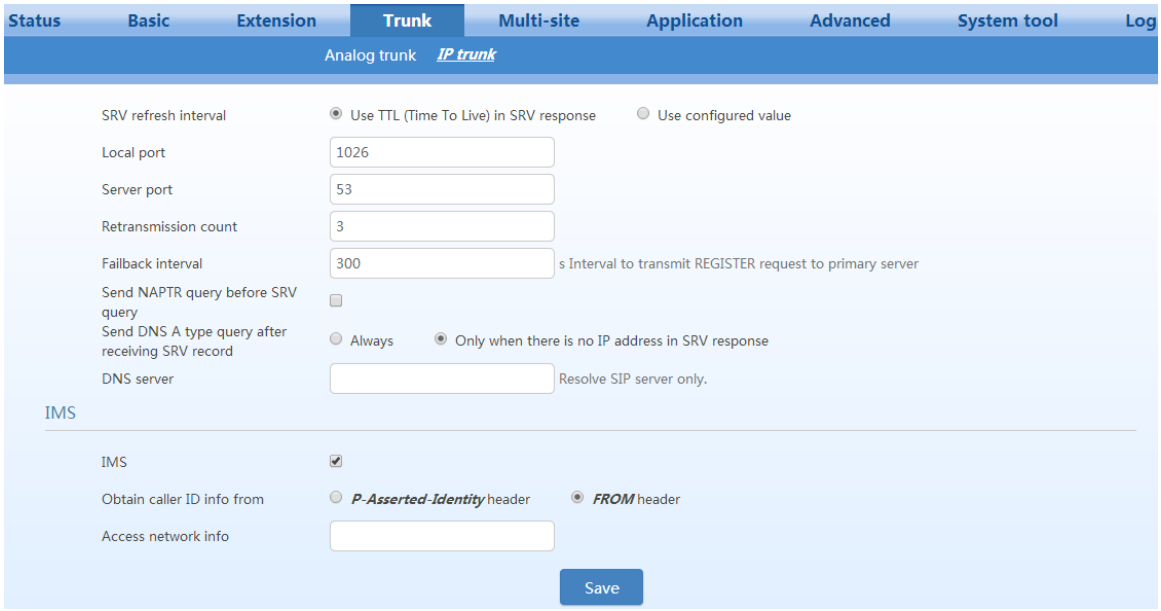


Table 2-12 IMS parameters

Item	Description
IMS	Enable interworking with IMS.
Obtain caller ID info from	For a received call of a SIP trunk, you can set to get the Caller ID from P-Asserted-Identity header or From header in the SIP message.
Access network info	The IP address and port number of the access network. For example: 192.168.100.200:5060. It is optional, input only when the IMS service provider requires.

Step 2 Check **IMS** and enter the **access network info**.

Step 3 Click **Save** to save the configuration.

2.3 Configuring Extensions

The OM supports analog and IP extensions, which are separately described below.

2.3.1 Analog extensions

Each FXS port corresponds to one analog extension. To configure an analog extension, follow this procedure:

Step 1 Go to **Extension** > **Analog** to configure analog extensions.

Figure 2-20 Analog extension configuration interface

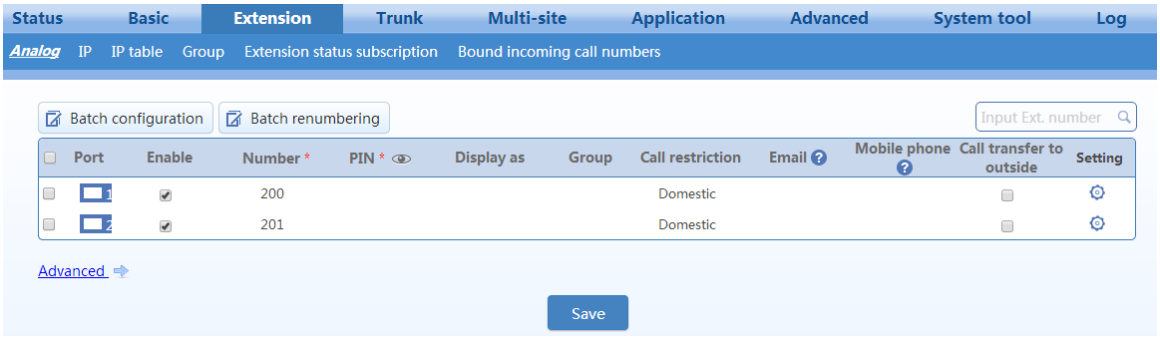


Table 2-13 Analog extension parameters

Item	Description
Batch configuration	Configure extensions in batch mode. Batch mode allows the configuration of multiple parameters for multiple extensions at once.
Batch renumbering	Modify extension numbers in batch.
Port	Analog extension port (FXS port) on the device.
Enable	Select to use this line. By default, the line is enabled.
Number	Number of the analog extension. The allocated numbers start from 200 by default.
PIN	Used for verification when operating via *33 and *99 navigation. **Note:** • The caller can perform the operations according to the *33 and *99 menus on analog phone. See the *OM User Manual*. • Both **DISA** and **Authorization with PIN** use this PIN, which is also used to set automatic downloading by an IP phone.
Display as	Set the display name of the analog or IP extension. This feature is only limited to calls between extensions, and it requires that the name display feature be supported at the called terminal. If display names are configured on both the OM and the IP extension, the display name configured on the OM prevails.
Group	Select a department for the extension. The extensions within the same department can use group call pickup. For details, see 2.4.6 Group Call Pickup..

Item	Description
Call restriction	Each extension has an assigned privilege for making outbound calls. When a user makes a call beyond its restriction, the device rejects the call with a voice announcement. If extension A is allowed only to make internal calls, when it tries to make outgoing call, the following announcement is heard, "Sorry, you are not authorized to make outgoing call, please contact the administrator." By default, the extension is allowed to make long distance calls. • **Internal:** Internal calls are allowed. • **Local:** Internal calls and local calls are allowed. • **Long distance:** Internal calls, local calls, and long distance calls are allowed. • **International:** Internal calls, local calls, long distance calls, and international calls are allowed. • **Prohibited:** The extension is only allowed to receive calls.
Email	Enter e-mail address to forward the call recording file or voicemail file to the user via email. For information on settings for voice mail, see 2.5.2 Voicemail.
Mobile phone	Instead of a PIN number a user's mobile phone number can be used for auto authentication of *33 and *99 for external access. If the **Authorization with *33 (Simplified-DISA)** function is selected, you can make outbound calls without dialing *33 for verification.
Call transfer to outside	An incoming call is allowed to be transferred to an external party. **Note 1**: Before using this function, the extension must have corresponding outbound rights. **Note 2:** During an outbound transfer, two lines are used.
Setting	Set multiple functions for the extension such as Authorization with PIN, Speed dialing, Call forking, Blocked numbers, Assistant, Block from being picked up, Call waiting, DND, Call hold, Call transfer, Call transfer to outside, and so on. For details, see 2.4.1 Basic Functions.
Advanced	Set advanced parameters of the analog extension.

Step 2 Click **Save** to save the configuration.

Step 3 Click **Advanced**, and set advanced properties of the extension such as Gain and Impedance. There is no need to make changes to the default values, unless there are issues when using the extension.

Figure 2-21 Analog extension advanced configuration interface

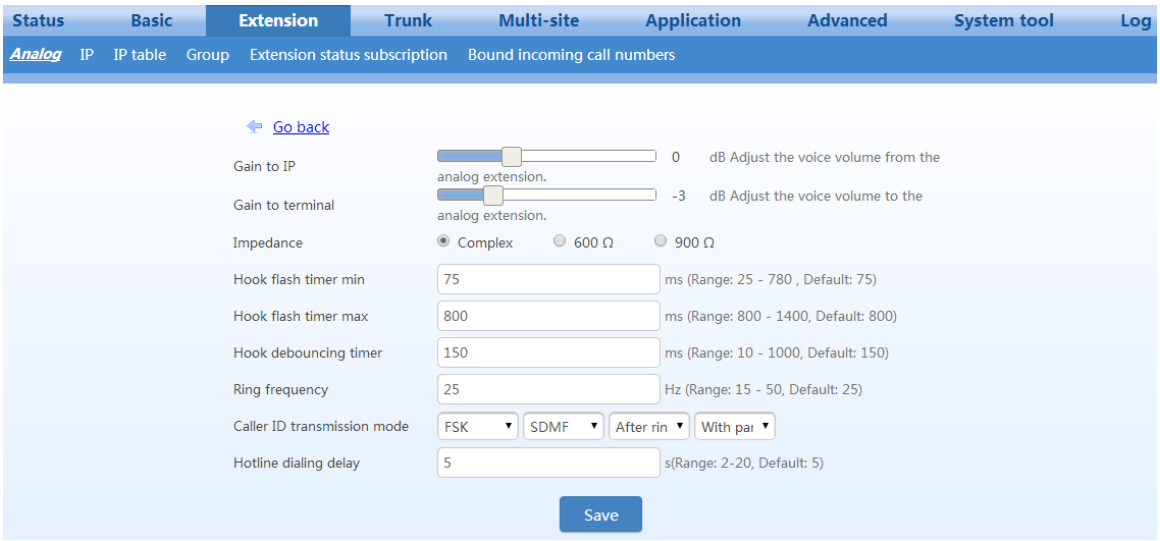


Table 2-14 Analog extension advanced parameters

Item	Description
Gain to IP	Adjust the call volume received on the FXS port. Increasing the value gives the internal party a louder voice. Range: -3.0 to +9.0 dBs.
Gain to terminal	Adjust the call volume sent from the FXO port. Increasing the value gives the external party a louder voice. Range: -6.0 to +3.0 dBs.
Impedance	Select the impedance of the FXS port. You can select Complex, 600 ohms, and 900 ohms. Complex is selected by default.
Hook flash time min	Used to detect hook flash, the default is 75 ms. The device will ignore any flash that shorter than the **Min. hook flash**. Generally, this value should not be less than 75 ms. You should adjust the parameter when the phone rings after an on-hook but no voice is heard after the off-hook.
Hook flash time max	Used to detect hook flash, the default is 800 ms. The device will regard the flash duration between **Min. hook flash** and **Max. hook flash** as effective flash. Any flash lasting over the longest time will be considered by the gateway as hang up. Generally, this value should not be less than 800 ms.
Hook debouncing timer	Used to avoid a phone status glitch. When the duration of on-hook/off-hook status changed is less than the value configured here, the device will consider the status to have not changed. The range is 10-to-1000 ms and the default value is 150 ms.
Ring frequency	The default is 25 Hz and the pattern is 1 second on, 4 seconds off. Generally, there's no need to change it. The range is 15 to 50 Hz.
Caller ID transmission mode	You need to adjust the parameter when the caller ID is displayed abnormally. Generally, there's no need to change it.
Hotline dialing relay	This parameter specifies the delay time before the preset hotline number is automatically dialed after hook-off. The default value is 5 seconds, and the value range is 2 to 20 seconds. This parameter works only if the delay mode is set for hotline function on **Extension** > **Analog** page. See Table 2-16.

2.3.2 IP Extensions

The IP phone or SIP softphone registered to the OM successfully can be used as an IP extension.

Before using an IP extension, you need to set the extension number and registration password on the OM. Follow this procedure:

Step 1 Go to **Extension** > **IP**.

Step 2 Click **Add**, and enter the IP extension number (for example, 208) and password (for example, 187986).

Figure 2-22 IP extension configuration interface

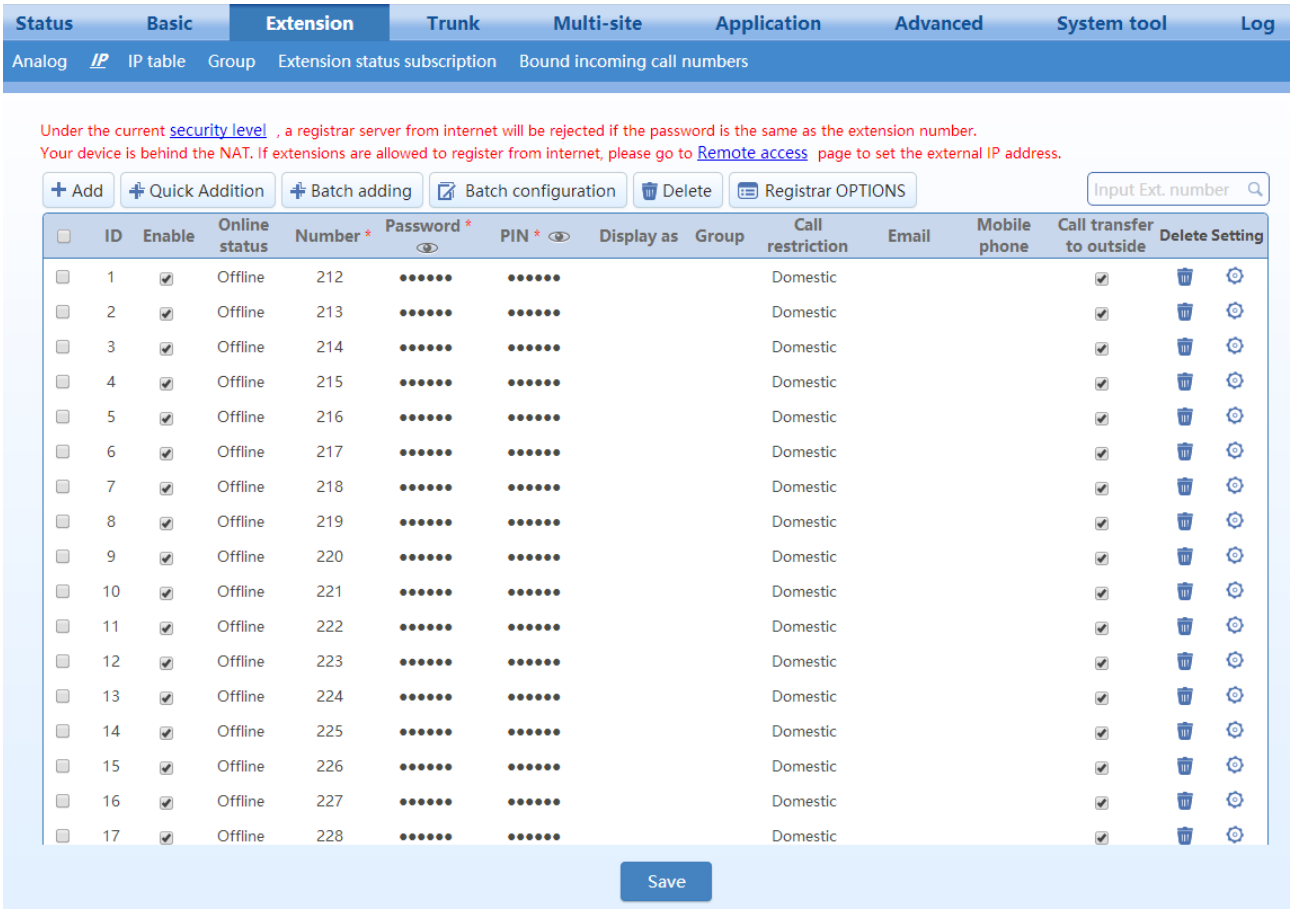


Table 2-15 IP extension parameters

Item	Description
Enable	Select to use this line. By default, the line is enabled.
Online status	Displays the current status of the IP extension.
Number	Phone number
Password	The password used for extension registration. The password is the same as PIN by default. After the password is changed, the PIN does not change.
PIN, **Group**, **display as**, **Call restriction**, **Email**, **Mobile phone**, **Call transfer to outside**, **Settings**	See Table 2-13.

Step 3 Click **Save** to save the configuration.

For details about registering an IP phone or SIP softphone to OM, see Appendix: Registering a SIP Terminal to OM.

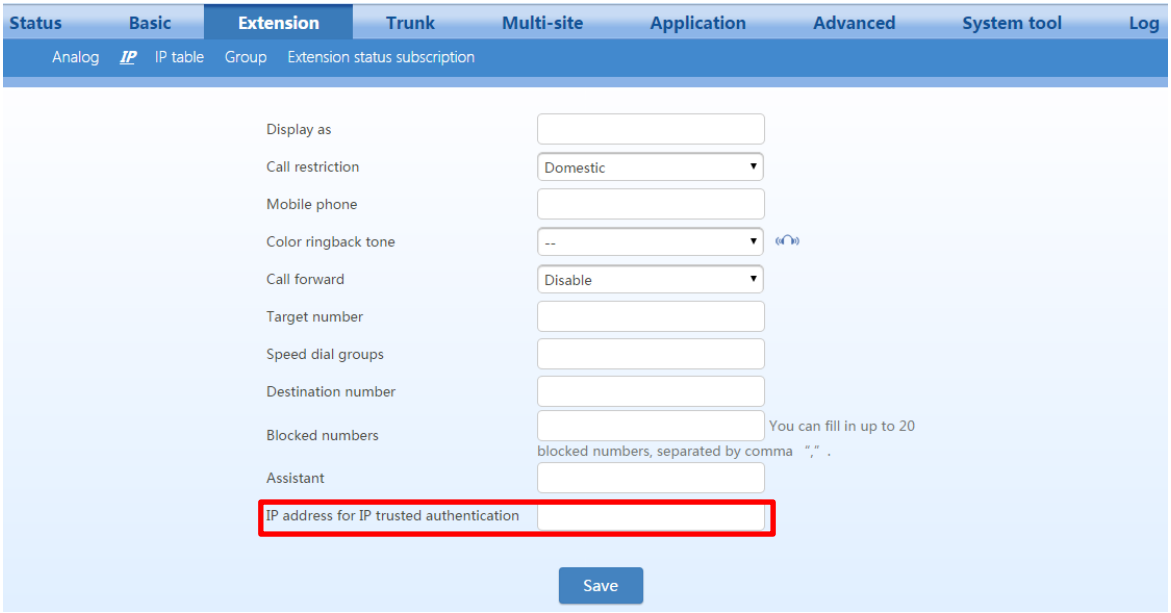
2.3.3 IP Trusted Authentication

To simplify the establishment of SIP sessions between OM and SIP terminals, you can define a trusted SIP terminal by entering its IP address here. For the trusted SIP terminal, there's no need to perform registration. It is recommended to use this function when OM works with voice gateway (for example MX60) in internal network.

Go to **Extension** > **IP**, click **Setting**, and enter the IP address of the SIP terminal works with the OM.

Note: On the voice gateway, you need to enter the IP address of the OM on the **Proxy server**. For details, see the *MX User Manual*.

Figure 2-23 IP authentication interface



2.4 Extension Features

2.4.1 Basic Functions

Go to **Extension** > **Analog/IP** > **Setting**, and set the basic functions for the extension.

Figure 2-24 Interface of extension features

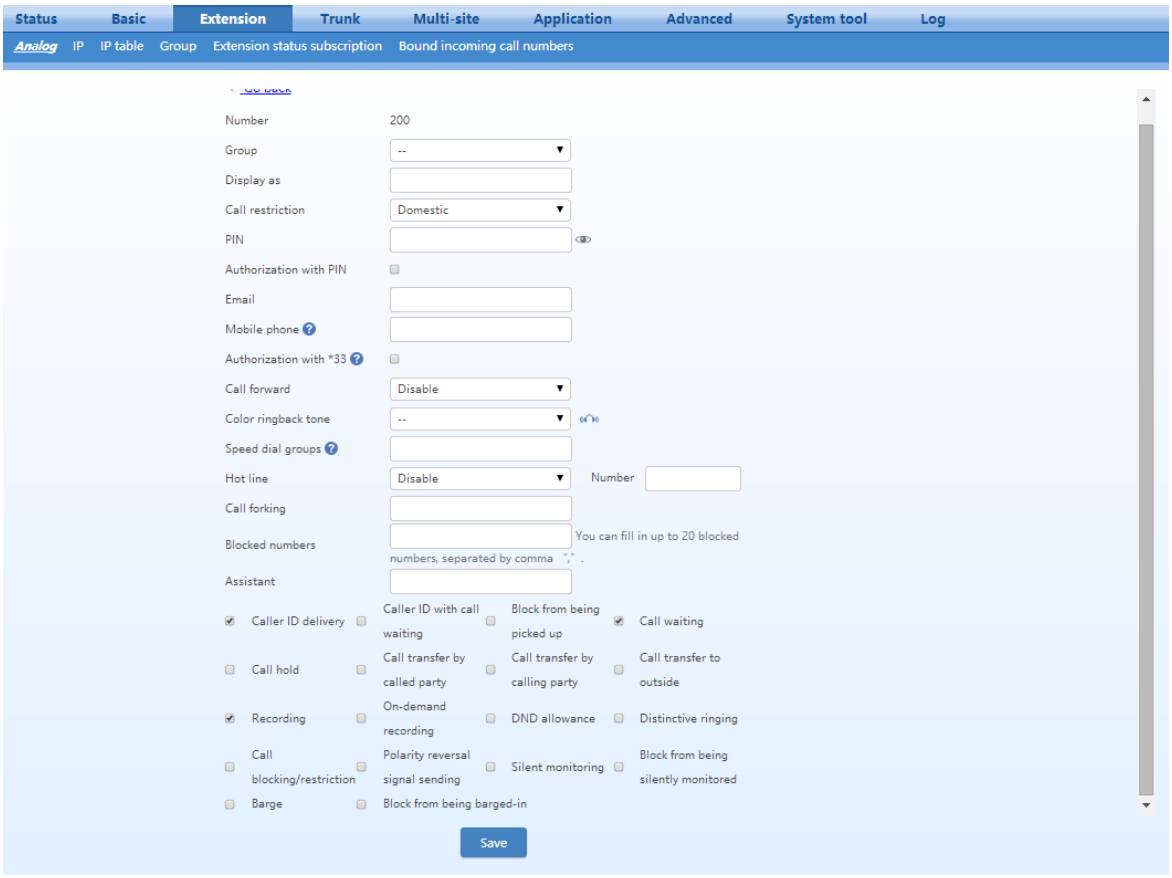


Table 2-16 Extension basic features

Item	Description
group	See Table 2-13.
Display as	
Call restriction	
Email	
Mobile phone	
PIN	
Authorization with PIN	Select it to lock the extension. The locked extension can only make an internal call. If an outbound call needs to be made, a PIN is required for authorization.
Authorization with *33 (Simplified-DISA)	The **Express-DISA** function allows the preset mobile phone to make outbound calls through trunks without entering a feature access code. ● If selected, the mobile phone number set in the **Mobile phone** field calls to the trunk, hears the dial tone, and directly dials the desired phone number to make an outbound call. ● If cleared, the mobile phone number calls to the trunk, must dials *33, hears the dial tone, and dials the desired phone number to make an outbound call. Note: *33 is the default feature access code, and it can be changed on the **Advanced** > **Feature access codes** interface.

Item	Description
Call forward	Forward incoming calls to the specified phone or voicemail. This function is disabled by default. • **CFA (phone)**: Forward all incoming calls to the specified phone. **Note:** This function cannot be enabled for an operator extension. • **CFB/CFNA (phone)**: Forward incoming calls to the specified phone when the extension is busy or does not answer. • **CFB (phone)**: Forward incoming calls to the specified phone when the extension is busy. • **CFNA (phone)**: Forward incoming calls to the specified phone when the extension does not answer. • **CFA (voicemail)**: Forward all incoming calls to voicemail For details on voicemail, see 2.5.2 Voicemail. • **CFB/CFNA (voicemail)**: Forward incoming calls to voicemail when the extension is busy or does not answer. Note: To set the ring duration before CFNA, go to **Advanced** > **System** > **Forward no answer ring counts**.
Different CFB / CFNA target number	If the call forwarding mode is **CFB/CFNA (phone)**, you can set a target phone number for CFB and a target number separately for CFNA.
Target number	Set the target phone number for **call forwarding**. The number can include extension number and external number (a mobile phone number or an external phone number). For external numbers, the extension should be allowed to make outgoing call. An outgoing call prefix and a comma are required to be input before you input the external number if the dialing prefix is required to make an outgoing call.
Color ringback tone	Select a CRBT file for the extension. For details on uploading and managing CRBT files, see 2.8.2 CRBT.
Speed dial groups	Allow users to dial the destination with a two-digit speed dial code preceded by **. The format for each group is “Speed dial code - Phone number”. Up to 30 speed dial groups are allowed, separated by comma “,”.The speed dial code must be in the range of 20–49. For example, speed dial group 20–13823218765 indicates 20 as the speed dial code for 13823218765.
Hot line	Outgoing calls are automatically routed to the preprogrammed telephone number when the user takes the telephone off-hook. • **Disable:** Disable hot line feature. • **Immediate:** Automatically dials out the preset number after off-hook. • **Delay mode**: Automatically dials out the preset number if the user does not dial any digit after off-hook for a certain period of time. The default value is 5s. This parameter is only applicable to analog extensions. For IP extensions, hot line configuration is set on the IP phones.
Number	Enter the hot line number.

Item	Description
Call forking	The device forwards the call to both your extension and another receiving terminal (for example, a mobile phone) simultaneously. Enter the number you want to fork to. **Notes:** • The function does not work when DND, CFA, and assistant extension are enabled. • Call forking will be inactive when the incoming call is waiting. • When the call is forked to external terminal via analog trunk, the incoming call is routed to the external terminal when the ringing exceeds the **No. of rings before voice prompt** configured on **Auto-attendant** page.
Blocked numbers	Enter the incoming numbers you want to block for the extension. For an incoming call with a blocked number, the device will play busy tone. Up to 20 blocked numbers are allowed, separated by comma ",". Note 1: An outbound call to the blocked numbers is allowed. Note 2: The blocked numbers configured here are applicable to an extension. To configure blocked numbers for all extensions, go to **Extension** > **IP table**.
Assistant	An assistant's extension can be bundled with his or her manager's extension so that a call to the manager will be redirected to the assistant and then can be transferred to the manager's extension by the assistant. Go to **Application** >**Manager**/**Assistant**, and then select the assistant mode as required. • **External call:** Only external calls are forwarded to the assistant's phone. • **Forwarding all calls to the assistant:** All incoming calls are forwarded to the assistant' phone. You can dial *35 to enable or disable the assistant function.
Caller ID delivery	If enabled, the caller ID is delivered to the extension.
Block from being picked up	The incoming calls cannot be picked up by other extensions. Note: The local extension can pick up the calls of other extensions by default.
Call transfer by called party	Transfers received calls to an external phone or other extension. To transfer to an external phone, the extension should be allowed to transfer calls to outside. • **Blind transfer**: Transfers a call without consulting with the intended recipient (another internal extension). The number of the original caller is displayed on the recipient's phone. • **Consultation transfer**: Transfers a call after consulting with the intended recipient (an internal extension or an external phone). The number of the person who transfers the call is displayed on the recipient's phone. **Note:** Before using the call transfer function, ensure that **Call Hold** is enabled.
Call transfer by calling party	Transfers the current call to another extension or an external phone when the extension serves as the calling party. Transferring to an external requires the allowance to transfer calls to outside. • **Blind transfer:** Same as above. • **Consultation transfer:** Same as above. **Note:** Before using the call transfer function, ensure that **Call hold** and **Call forward** are enabled.
Call transfer to outside	See Table 2-13.

Item	Description
Call waiting	When a new incoming call arrives while a call is in progress, the user will hear beeps and has three choices: • **Ignore a new call**: No operation is required, and the current conversation continues. The beeps stop after the specified time. • **Answer a new call**: The user can press ** to suspend the current call and switch to the new incoming call. Meanwhile the suspended party hears call waiting music. • **Switch call**: The user can press ** to suspend the current call and switch back to the original call. **Note:** Before using this function, ensure that **call hold** is enabled.
Call hold	The user can suspend a current call and make a new call. Meanwhile the suspended party hears call waiting music.
DND allowance	When enabled, the user can set DND on phone set to ensure the extension does not ring when incoming calls are received. The user can dial *72 (or *99) to enable or disable DND. Note: After the device reboots, DND of the phone set is automatically disabled.
Recording	Record the whole conversation for each call. **Note:** To enable the total recording by the extension, you need to enable the recording on **Recording** page. For details, see 2.5.1 Recording.
On-demand recording	The user can start on-demand recording with one of the following methods: • Dial *# during the call • Dial *# before dialing phone number. For details on recording type, see 2.5.1 Recording.
Distinctive Ringing	The extension rings with different ringing pattern according to the type of the incoming call. • **Internal call:** “beep - beep - beep – beep - beep” • **External call:** “beep beep - beep beep beep” • **Speed dial call:** “beep beep beep beep beep - beep - beep”
Call blocking/restriction	Select whether to enable the call blocking or call restriction configured on **Application** > **Call barring** page. For details, see 2.9.2 Outbound Call Screening.
Polarity reversal signal sending	In the events of answers and disconnect at the remote end, the device sends polarity reversal signals to the local terminal as indication. Polarity reversal signals can be used on a phone with billing function. **Note**: This function is applicable only to analog extensions.
Silent monitoring	Monitor the call on other extensions. Note: If either of the two parties enables the **Block from being silently monitored**, the silent monitoring function does not work.
Block from being silently monitored	All the conversation with the extension cannot be monitored.
Barge	Bridge into a call on another extension and create a multi-party or conference call. If either of the two parties enables the **Block from being barged-in**, the barging function will not work.
Block from being barged-in	The conversation with the extension cannot be barged-in.

2.4.2 Making Outbound Calls

Go to **Basic** > **Dialing rule** > **Outbound** to configure outbound dialing rule**.**

Figure 2-25 Outbound dialing rule interface

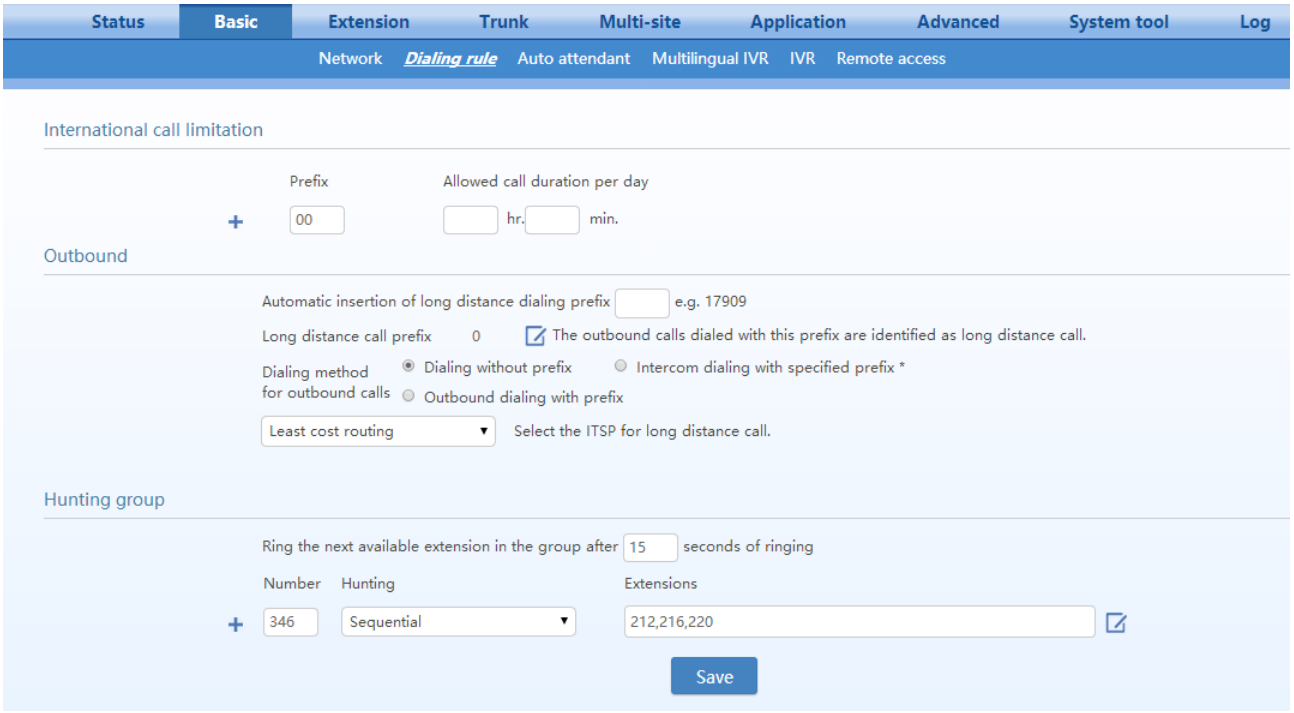


Table 2-17 Outbound dialing rule parameters

Item	Description
International call limitation	The outbound calls dialed with the prefix configured here are identified as international call. You can limit the international call time for every day. **Note:** If the Call restriction of the extension is configured as **Prohibited**, **Internal**, **local** or **long distance**, the number with the prefix configured here cannot be dialed.
Automatic insertion of long distance dialing prefix	When the user makes a long distance call using the analog trunk, the prefix set will be automatically added.
Long distance call prefix	The outbound calls dialed with the prefix configured here are identified as long distance call. The default value is 0. **Note:** If the **Call restriction** of the extension is configured as **Prohibited**, **Internal** or **local**, no long distance outbound call will be allowed.
Dialing method for outbound calls	• **Dialing without prefix**: Directly dial internal extension or external numbers. • **Intercom dialing with specified prefix***: Dial external numbers directly while dial internal numbers by adding prefix *. • **Outbound dialing with prefix**: Dial internal extension numbers directly while dial internal numbers with prefix.
Routing	When the device is configured with multiple trunks, a corresponding outbound call hunting method can be selected as required. The device provides six routes of outbound call for users to select. • **Sequential hunting for analog trunk:** Make the outgoing call through the first available analog trunk on the analog trunk list starting from the first one. • **Round-robin hunting for analog trunk:** Make the outgoing call through the

Item	Description
	analog trunk in Round-robin order. • **Sequential hunting for IP trunk:** Make the outgoing call through the first available IP trunk on the IP trunk list starting from the first one. • **Round-robin hunting for IP trunk:** Make the outgoing call through the IP trunk in Round-robin order. • **Least cost routing**: Analog trunks are selected for local calls, and IP trunks are selected for long distance/international calls. The device determines the long distance/international calls based on the prefix. For example: If the long distance call prefix is 0 and the international call prefix is 00, an IP trunk is selected for the calls made with the numbers starting with "0" or "00". An analog trunk is selected for local calls. If the IP trunk is not activated or a network failure occurs, an analog trunk is also selected for calls made with the numbers starting with "0" or "00". **Note:** If a long distance/international call is made with all IP trunks occupied, the following announcement will be played: All circuits are busy. Please try your call again later. • **Route:** The routing table rules are used to make the call to the PSTN. For details, see 2.8 System Settings.
Prefix	The user can make an outbound call with a routing method identified by the prefix configured here. For example, if the prefix for **Sequential hunting for IP trunk** is 9, the device will make sequential hunting over IP trunk when dialing the number starting with 9. **Note:** • The parameter can be configured only when the **Dialing method for outbound calls** is **Outbound dialing with prefix**. • To avoid collision, the prefix must be different from extension number, hunting group number, number to reach the operator, feature access code, and other outbound call prefixes.
Secondary dial tone	After the extension user dials the prefix, the device prompts the user to dial the called number with secondary dial tone. **Note:** Applicable only when the **Dialing method for outbound calls** is **Outbound dialing with prefix**.
Trunk	Specify the corresponding trunk numbers for the outbound group of analog trunks and IP trunks. Select the trunk numbers directly or enter them manually. The trunk numbers must be separated by ",".

2.4.3 IP table

Go to **Extension** > **IP Table**, and set rules for filtering inbound and outbound call numbers. For example: If 12345678 is set in **Blocked number**, the device will play a busy tone when a call dialed with this number arrives.

Figure 2-26 IP table configuration interface

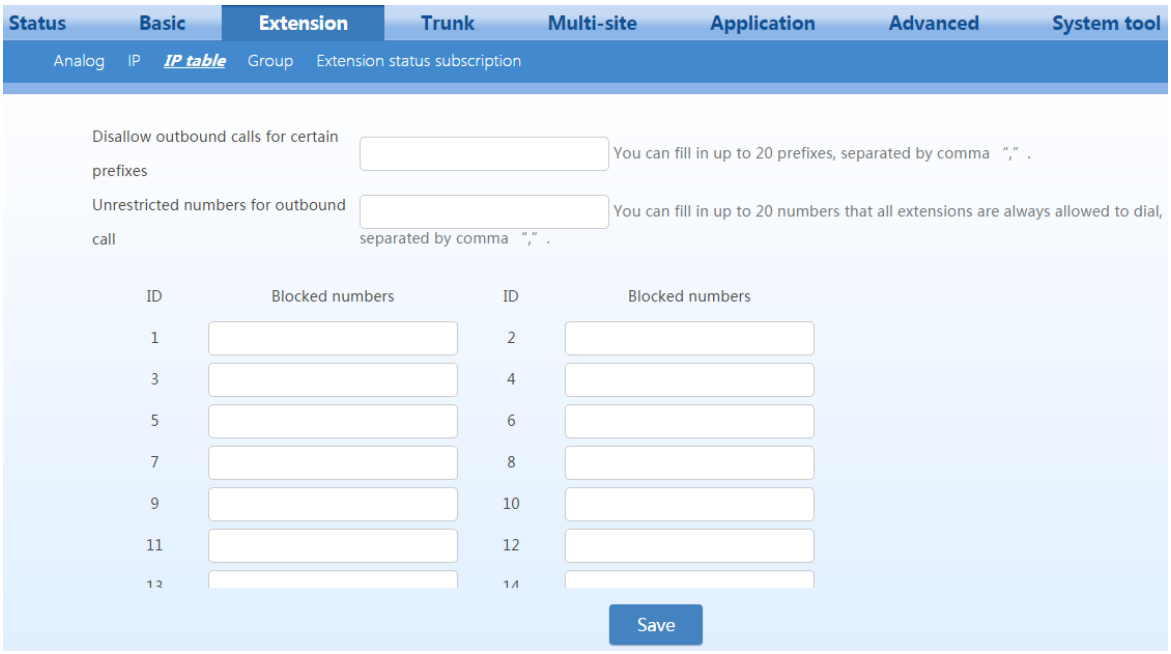


Table 2-18 IP table parameters

Item	Description
Disallow outbound calls for certain prefixes	The device prohibits the user from dialing numbers with the prefix configured here. When the number is dialed, the device plays a busy tone. You can fill in up to 20 prefixes, separated by comma ",". **Note:** The user can dial **Unrestricted numbers for outbound call** even if it is started with the prefix configured here.
Unrestricted numbers for outbound calls	The user can dial the number regardless of **Call restriction** and **Disallow outbound calls for certain prefixes**.
Blocked numbers	A table listed with up to 30 phone numbers, which are prohibited from calling in and busy tone will be played to reject the calls. **Note:** • Caller ID detection feature must be enabled for this feature to take effect. • The blocked numbers can be called from the device. • The blocked numbers configured here is applicable for all extensions. To configure blocked numbers for individual extension, see 2.4.1 Basic Functions.

2.4.4 Hunt Group

You can allocate multiple extensions to a hunt group of extensions. When a caller dials the hunt group number, the device will ring an idle extension in the group according to the preset allocation.

Go to **Basic** > **Dialing rule**, and set the hunting group. You can click + to add new groups.

Figure 2-27 Hunt group configuration interface

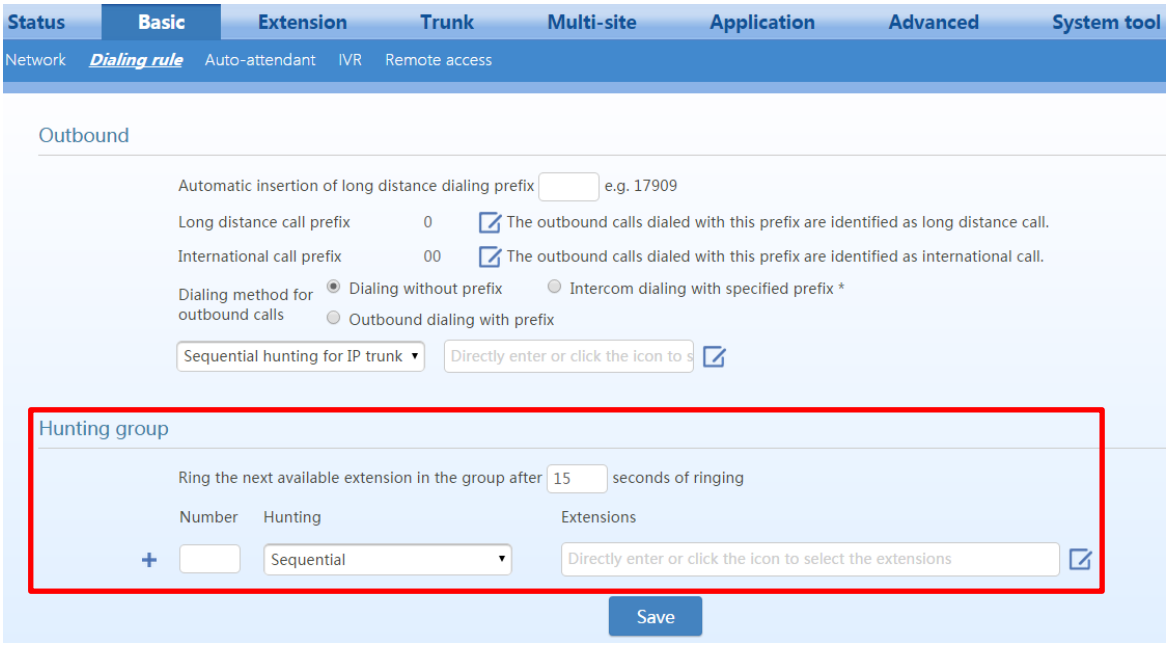


Table 2-19 Hunt group parameters

Item	Description
Ring the next available extension in the group after XX seconds of ringing	Ring timeout to select the next available extension in the group.
Numbers	Add extension numbers to the hunt group. **Note:** The numbers must be different from an outbound call prefix, a number forwarded to the auto attendant, an extension number, or a feature access code.
Hunting	Select a hunt group method: • **Sequential**: Terminate the incoming call to the first available extension on the extension list starting from the first one; • **Circular**: Terminate the incoming call to extension in Round-robin order • **Simultaneous:** Terminate incoming calls to all available extensions on the operator list simultaneously and the first one to pick up is connected. **Note:** If an extension configured with call forward is included in a sequential or circular hunt group, the incoming call will never re-route to the extension in the group after being forwarded to the call forward target number.
Extensions	Enter extension numbers included in a hunting group.

2.4.5 Extension Status Subscription

When you use the New Rock NRP1004 or NRP1012 IP phones as the extensions of OM, you can configure the extension–status-subscription feature for them. So you can see the status of other extensions through the indicators of BLF function keys.

Table 2-20 Status of BLF indicators

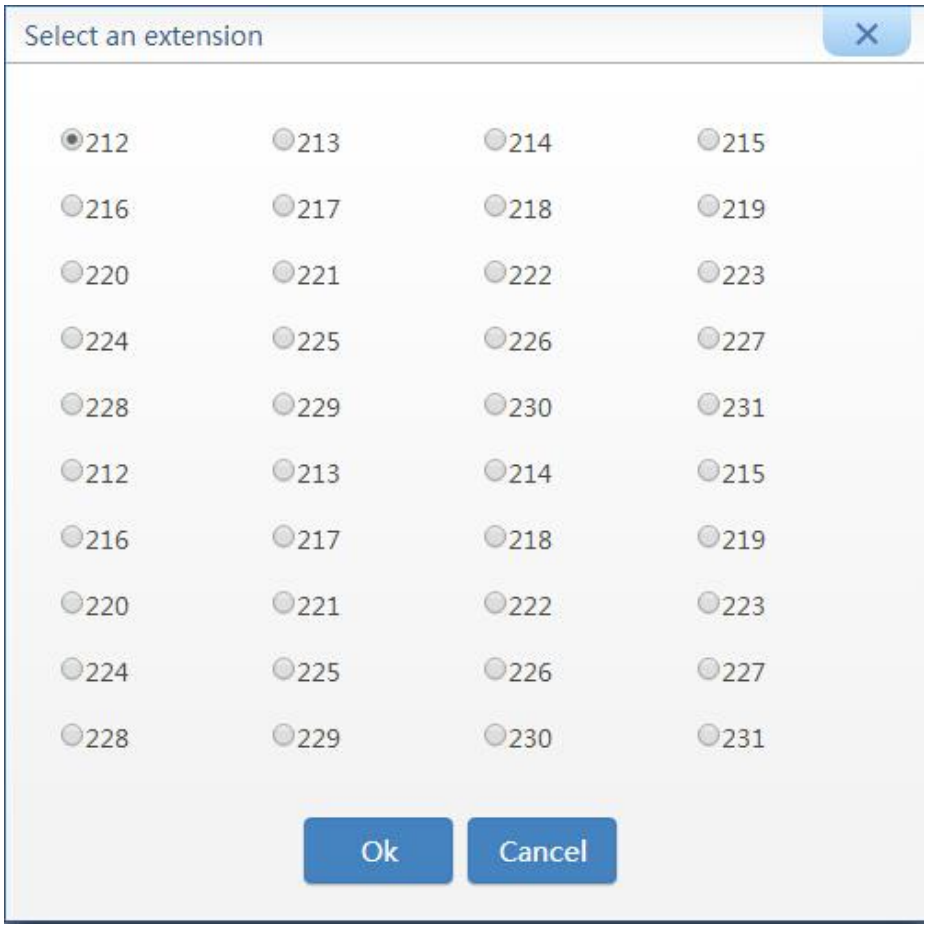
Indicator	Extension status
Steady green	Idle
Red flashing.	Ringing
Steady red	Talking or IP phone is offline

Follow this procedure:

Step 1 Go to **Extension** > **Extension status subscription**, and click **Add**.

Step 2 Select the desired extension.

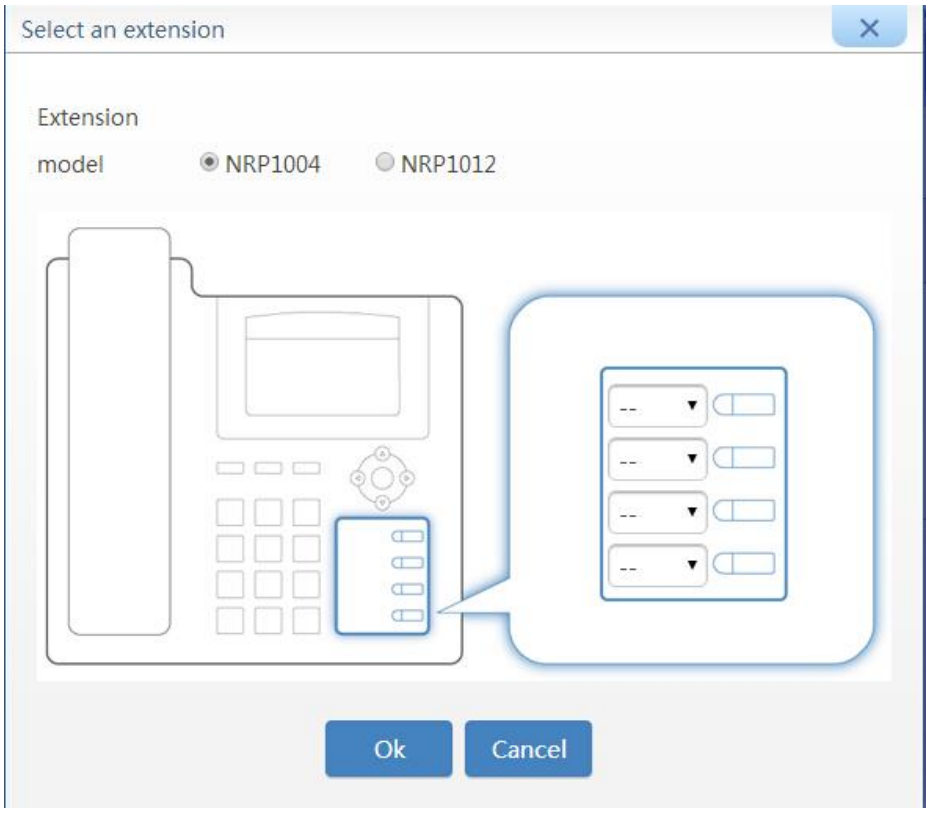
Figure 2-28 Extension status subscription interface



Step 3 Select the model of the extension. The NRP1004 provides four BLF function keys, while NRP1012 provides eight BLF function key

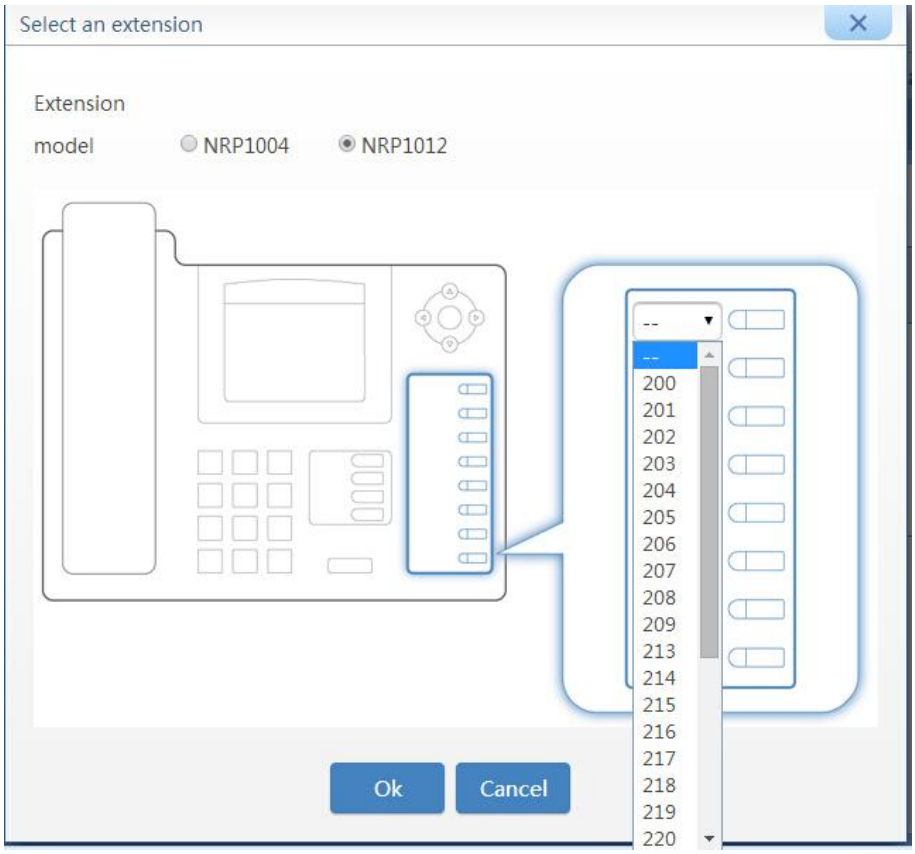
Note: The model of the extension must be correctly selected, otherwise the subscription will be invalid.

Figure 2-29 Selecting an extension model



Step 4 Select the extension number from the drop-down list next to the BLF function key.

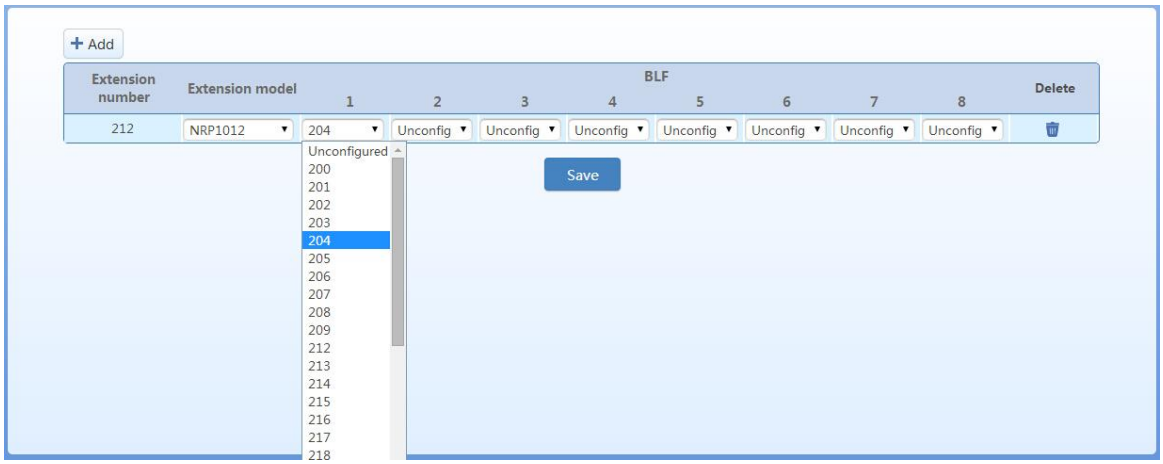
Figure 2-30 Selecting extensions for subscription



Step 5 Click **Save** to save the configuration.

After the configuration is completed, you can view, modify, or delete subscription information of the extension.

Figure 2-31 Extension status subscription interface



When the subscription period of the phone arrives or after the phone reboots, the phone will automatically download the subscription configuration from the device.

When the subscription period of the phone arrives or after the phone reboots, the phone will automatically download subscription configuration from the device. If the phone is not registered as the extension of the

OM, connect the phone to the device, power it on, and enter the PIN code for the extension in the PIN text box. After the download is completed and the phone reboots, the BLF function keys are enabled.

2.4.6 Group Call Pickup

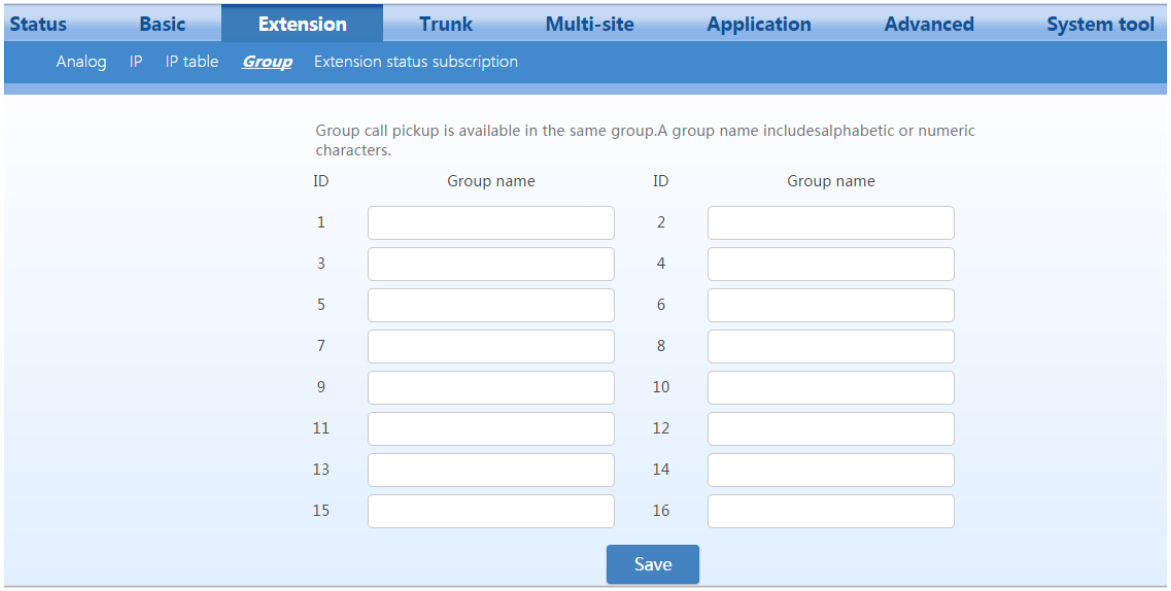
The group call pickup function allows users in the same group to pick up incoming calls for each other. To enable this function, you need to define groups and add member extensions to the groups.

To configure a department, follow this procedure:

Step 1 Go to **Extension** > **Group** to enter or change the group name. You can define up to 32 groups

Step 2 Click **Save** to save the configuration.

Figure 2-32 Group configuration interface



To distribute extensions to a specific group, follow this procedure:

Step 3 Go to **Extension** > **Analog/IP** > **Setting**, and enter the extension function configuration interface.

Step 4 Select the group you want to distribute the extension to from the **Group** drop-down list, and **save** the configuration.

Figure 2-33 Group interface

2.4.7 Call Pickup

The call pickup function allows another extension user to pick up an incoming call if the call is not answered. By default, the call pickup function is enabled. For details, see the *OM User Manual*.

2.4.8 Three-way Calling

The three-way calling function allows the extension user to invite a third party to attend the conversation for three-way calls. It also allows the extension user to communicate with one party while having the other party listening to the background music, and to switch between the parties. The drop of either of the other two parties from the three-way call will not affect the conversation. The extension user can hang up the phone to end the three-way calling. For details, see the *OM User Manual*.

Note: When **Call hold** is enabled, three-way calling is enabled by default. For details, see **Call hold**.

2.4.9 Call Parking

Call parking allows a user to put a call on hold at one extension and continue the conversation from any other extension. For details, see the *OM User Manual*.

Note: When **Call hold** is enabled, call parking is enabled by default. For details, see **Call hold**.

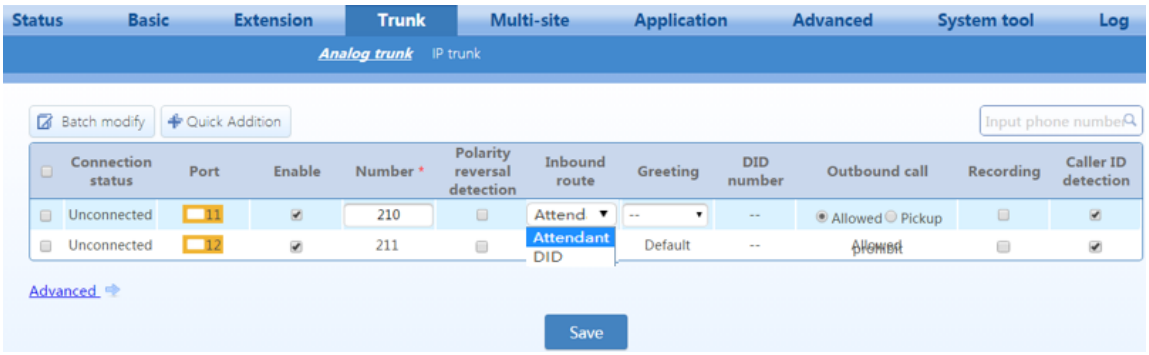
2.4.10 DID

With DID enabled, an incoming call can be directly routed to a specified extension or hunt group without passing through the auto attendant. The trunk can be used either by the specified extension/hunt group or other extensions/hunt groups depended on configuration.

Follow this procedure:

Step 1 Go to **Trunk** > **Analog trunk/IP trunk** to select bundled trunk for extension/hunting group, and select **DID** for **Inbound route**.

Figure 2-34 DID configuration interface



Step 2 Select drop-down list In the **DID number** field, enter and select the extension number or hunting group number that needs to be bundled.

Step 3 Select the **Outbound call** mode.

- **Share:** The trunk can be used by all extensions or hunt groups.
- **DID only**: The trunk can be used only by the specified extension or hunt group.

Step 4 Click **Save** to save the configuration.

2.4.11 Binding Incoming Call Numbers to an Extension

If an external call number is bound with an extension number, incoming calls go directly to the bound extension without greetings.

You can pick up the extension and dial *66 to bind the call number that you just hung up on (dial *67 to unbind the call number if required).

Binding relations can be checked or canceled on the **Extension** > **Bound incoming call numbers** page.

The NeeHau Business Phone Assistant can also be used to bind or unbind incoming call numbers and extensions (Go to **Application** > **API** to enable NeeHau first). For details, see *NeeHau User Guide*.

Figure 2-35 Incoming call number binding interface

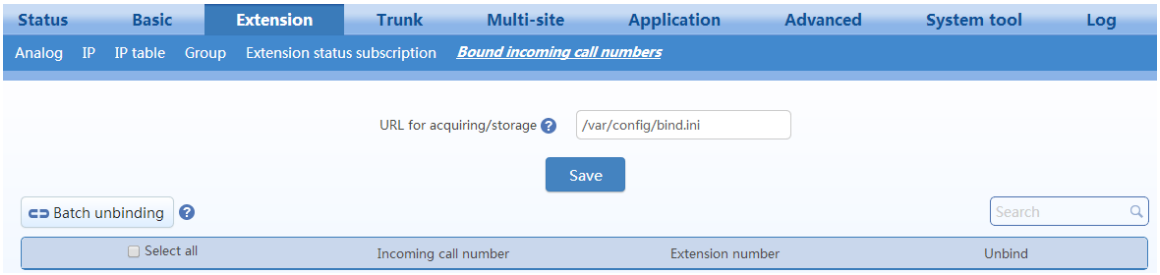


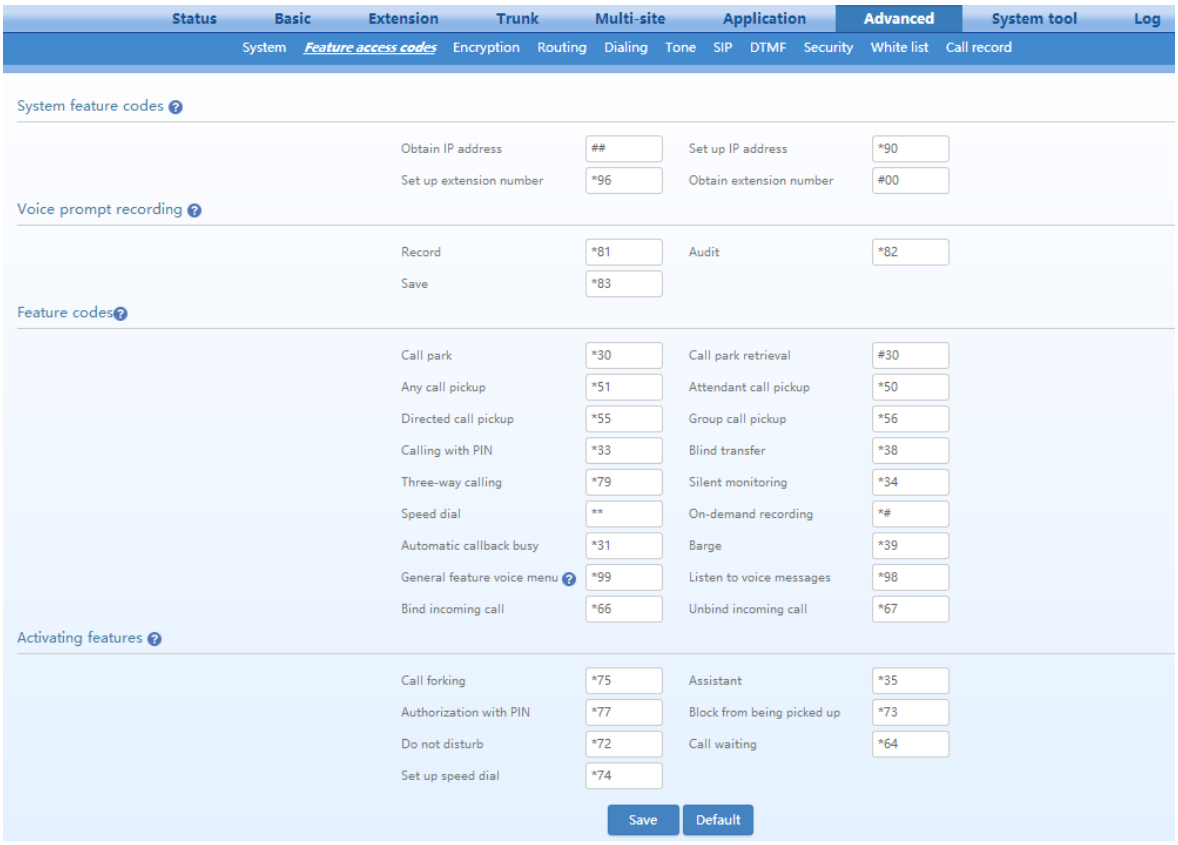
Table 2-21 Incoming call number binding parameters

Item	Description
URL for acquiring/storage	The path to store the binding relations. The default path is */var/config/bind.ini* and it can be changed. Note: This path is not displayed if you enable NeeHau on the **Application** > **API** interface.
Batch unbinding	Unbind incoming call numbers and extensions in batches. Note: This button is not displayed if you enable NeeHau on the **Application** > **API** interface. Please use NeeHau or extensions to unbind.
Search	Search for numbers. Fuzzy search is supported.
Incoming call number	The incoming call number to bind with the extension number. Note: This parameter cannot be configured on this interface.
Extension number	The extension number to bind with the incoming call number Note: This parameter cannot be configured on this interface.
Unbind	Unbind an incoming call number and an extension. Note: If you enable NeeHau on the **Application** > **API** interface, this function is disabled, please use NeeHau or extensions to unbind.

2.4.12 Feature Access Codes

Go to **Advanced**> **Feature access code** to query or customize feature access codes Click ? to view details about the feature access codes.

Figure 2-36 Feature access codes interface



Note

To avoid collision, the feature access code must be different from any extension number, hunt group number, number to reach the operator, outbound call prefix, and other feature access codes.

2.5 Recording and Voicemail

2.5.1 Recording

The OM supports remote recording and USB-device recordings, both for G.711 and G.729.

Remote recording

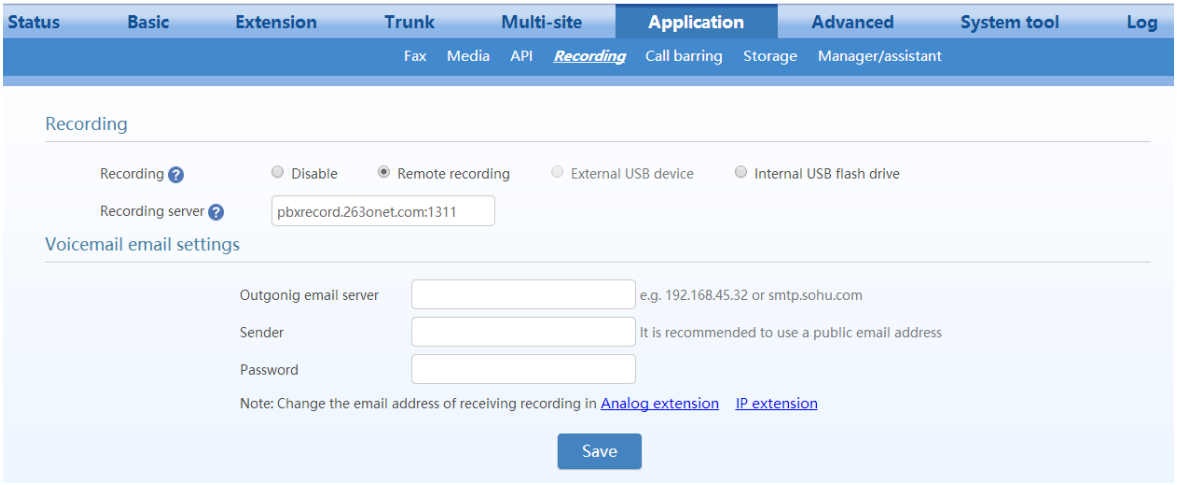
All the recorded files are stored in the external recording server. Before recording, an external recording server installed with New Rock Recording Agent is required. You can download the recording agent from:

http://www.newrocktech.com/ViewProduct_E.asp?id=64

Follow this procedure:

Step 1 Go to **Application**> **Recording**, and select **Remote recording**.

Figure 2-37 Remote recording configuration interface



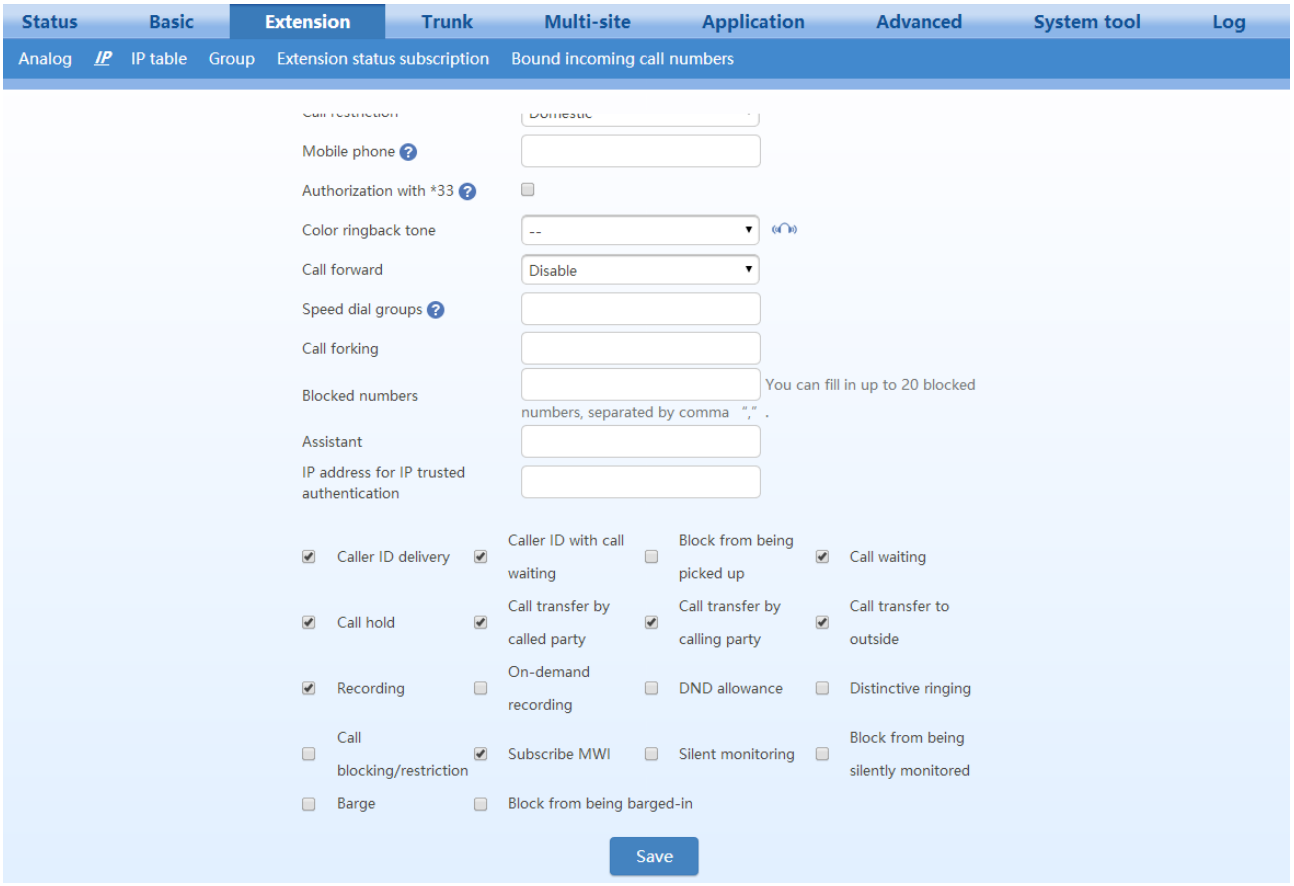
Step 2 Enter the IP address and port number of the recording server. The default port number is 1311.

Step 3 Click **Save** to save the configuration.

Step 4 Go to **Extension** > **Analog/IP**, select the desired extension, and click **Setting**.

Step 5 Select **Recording**.

Figure 2-38 Extension recording configuration interface



Step 6 Click **Save** to save the configuration.

For details about managing recording files on the recording server, please refer to OM Recording Agent User Guide. You can acquire the document from:

http://www.newrocktech.com/ViewProduct_E.asp?id=64

USB device recording

All the recording files are stored in the internal USB flash drive or external USB device. The storage space allocated for the internal USB flash drive is 10240 MB by default. You can modify it on **Application** > **Storage** page.

Step 1 Go to **System tools**> **System time** to check that the current time of the device is correct. For details of time setting, see 2.8.4 Time.

Note: Please make sure the system time is correct because the recording files are named using the system time.

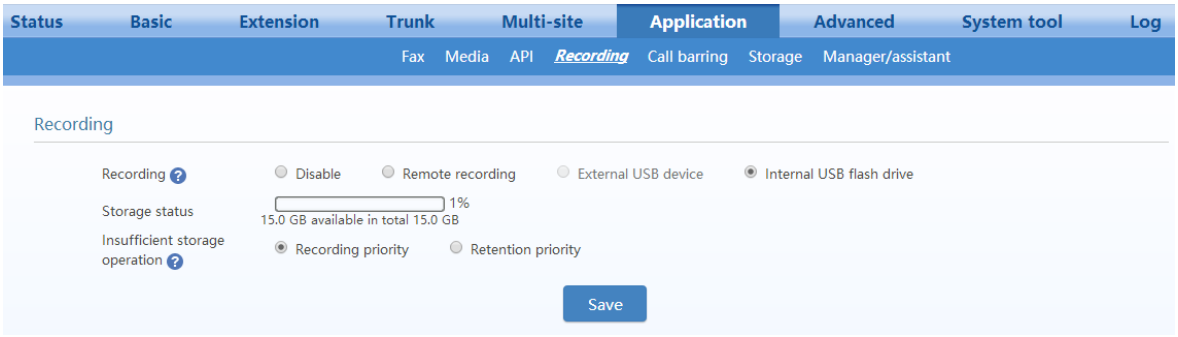
Step 2 Go to **Application** > **Recording**, and select the storage mode. Before selecting **Recording through external USB device**, you need to connect the external USB device.

Step 3 Choose the operation when the available space is insufficient.

Recording priority: The new recording will overwrite the existing recording. When the available storage space is less than 500MB, recoding files for the earliest day or the earliest 100 recording files are overwritten.

Retention priority: The new recording will be stopped.

Figure 2-39 USB recording configuration interface

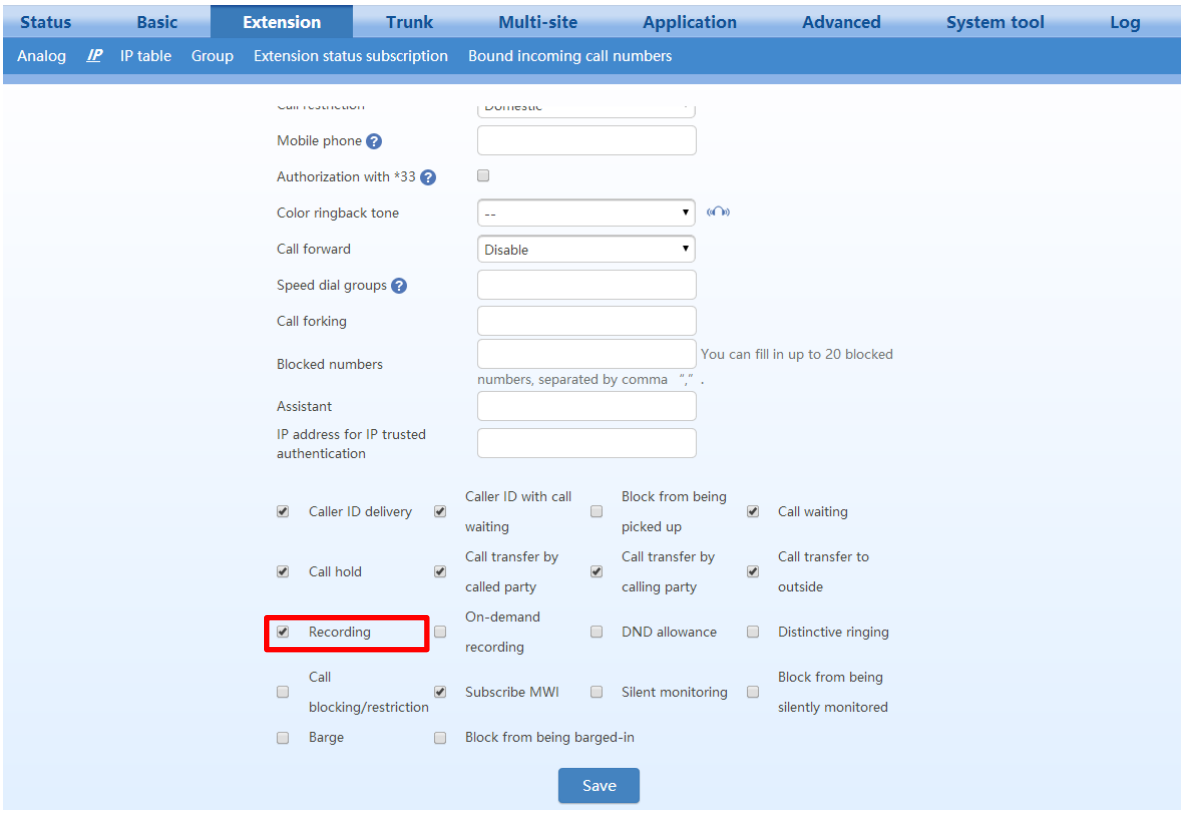


Step 4 Click **Save** to save the configuration.

Step 5 Go to **Extension** > **Analog/IP**, select the desired extension, and click **Set**.

Step 6 Select **Recording**.

Figure 2-40 Extension recording interface



Step 7 Click **Save** to save the configuration.

Managing recorded files

Table 2-22 Managing recorded files

Format	Calling party_Called party_Date_Time_Random code_cg.wav Calling party_Called party_Date_Time_Random code_cd.wav cg.wav indicates a recorded file that is generated when the extension serves as the calling party. cd.wav indicates a recorded file that is generated when the extension serves as the called party. For example: 200_80001_20121130_180028_a00a_cg.wav indicates that the recorded file is generated at 18:00:28 on November 30, 2012 when the extension 200 calls 80001.
View recorded files	• Go to **Application** > **Storage** to get the access path and view the recorded files in the browser. Click **builtin** to view the files recorded through internal USB flash drive, and **usb** to view the files recorded through external USB device. The typical example of the storage path is: sda1/Recorder/20140930. • If recorded files are stored in an external USB device, you can remove the USB device from the OM and connect it to your PC, then view the recorded files. The typical example of the storage path is: G:/Recorder/20140930.
Listen to recorded files	You can listen to the recorded files with either of the following methods: • Locate and download the recorded files, and play it; • Play the recordings on the Call log page of NeeHau Business Phone Assistant.
Backup and clear recorded files	• Internal USB flash drive: Go to **Application** > **Storage**, click **Backup** to store the **Recorder** folder to the root directory of the external USB device.

	When the backup is completed, click **clear** to delete the remaining recorded files from the internal USB flash drive. • External USB device: Remove the USB storage device and connect it to your PC, and then back up or clear the recorded files.

2.5.2 Voicemail

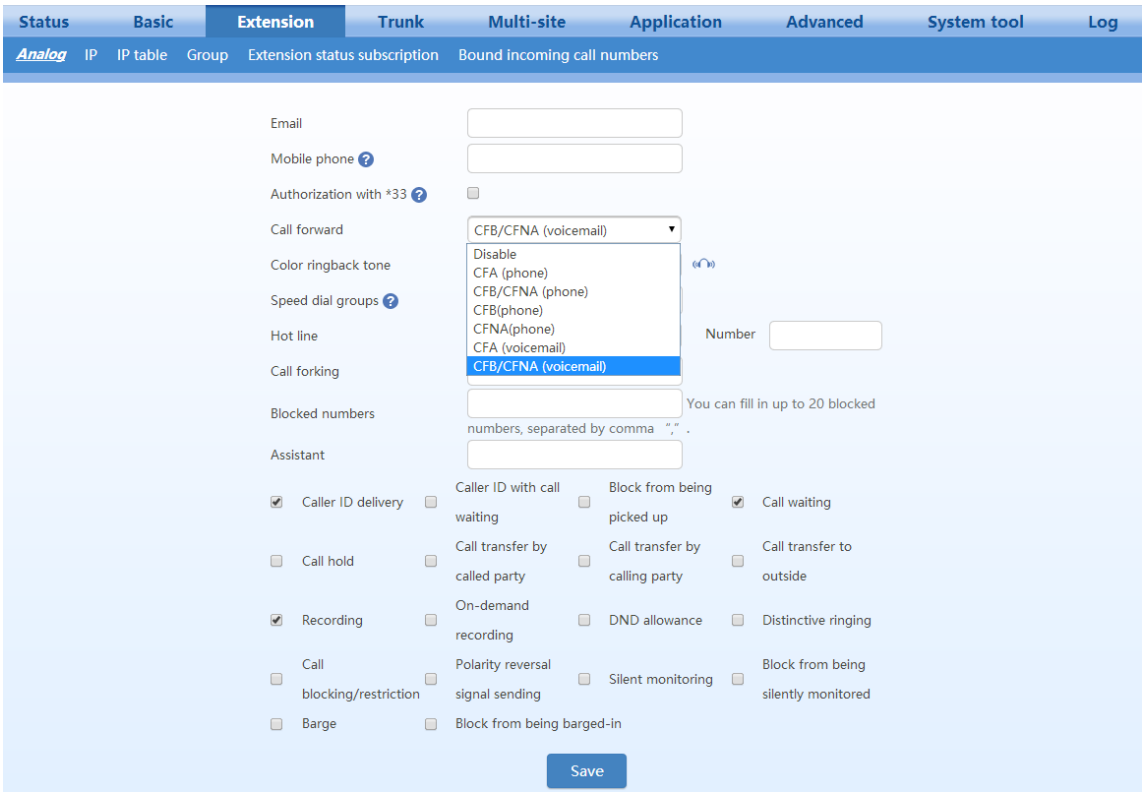
When the extension user cannot receive the incoming call, the calling party can leave a message after the prompt.

Step 1 Go to **Application** > **Recording**, and enable the recording. For details, see 2.5.1 Recording.

The storage path of recorded files is varied depending on the recording mode, for example, if **Internal USB flash drive** is selected, the voicemail messages will be stored in the internal USB flash drive.

Step 2 Go to **Extension** > **Analog/IP** > **Setting**, and set the **Call Forward** to **CFA (voicemail)** or **CFB/CFNA (voicemail)**.

Figure 2-41 Voicemail configuration interface



Step 3 Click **Save** to save the configuration.

When the recording mode is **Remote recording**, the voicemail messages can be sent to the mailbox of the extension user. To configure it, follow this procedure:

Step 1 Select **Remote recording** on the **Recording** page and configure the **Recording server** and **Outgoing email server**.

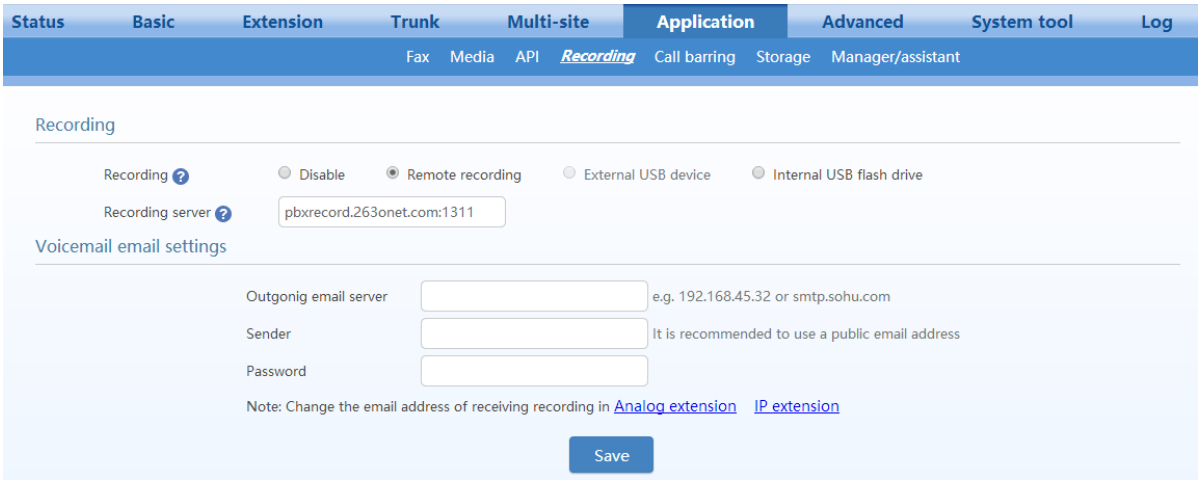


Table 2-23 Voice mailbox sending server parameters

Item	Description
Outgoing email server	Enter the IP address or domain name of the mail server. The device supports Sina mailbox and Sohu mailbox.
Sender	Enter the mailbox address of the sender.
Password	Enter the mailbox password of the sender.

Step 2 Click **Save**.

Step 3 Go to **Extension** > **Analog/IP** > **Setting**, and configure **Email**. The mailbox will serve as the mailbox for receiving voicemail messages.

Step 4 Click **Save**.

Managing voicemail message files

Table 2-24 Managing message files

Format	The name of a voicemail message file is in this format: vm_Called party-Calling party-Random code.pcm. For example: vm_200-6033432345-946685192.pcm. If the user presses **Replay** or **Next** when listening to a voicemail message or the voicemail message is played, the message will be identified with the file name become **old**vm_200-6033432345-946685192.pcm. **Note:** The filename extensions are varied depending on the codec of the voicemail message: • G.711μ: The file extension is .pcm. • G.711a: The file extension is .pcma. • G.729: The file extension is .dat.
View the voicemail message files	• Go to **Application** > **Storage** to get the access path and view the voicemail message files in the browser. Click **builtin** to view the files recorded through internal USB flash drive, and **usb** to view the files recorded through external USB device. The typical example of the storage path is: Recorder/voicemail. • If recorded files are stored in an external USB device, you can remove the USB device from the OM and connect it to your PC, then view the recorded files. The typical example of the storage path is: G:\Recorder\ voicemail.

Listen to the voicemail message files	• **Analog phone:** Press *98 and listen to the voicemail messages. You may hear: "You have no voicemail messages". "You have n new/saved voicemail messages" After the voicemail message is played, you may hear: "To repeat the message, press one. To delete, press two. To listen to the next message, press three". • **IP phone:** Configure the feature access code for listening to the voice messages by MWI function key and memory key. For details about the configuration on New Rock's IP phone, see *NRP User Manual*.
Backup and clear voicemail message files	Same as Table 2-22.

2.6 FoIP

A fax machine can be connected to either FXS port on the OM or the FXS port of the gateway registered to OM. To send a fax message, dial the fax number just like making an outbound call. For details, see 2.4.2 Making Outbound Calls.

Go to **Application** > **Fax**, and set the fax parameters.

Figure 2-42 FAX configuration interface

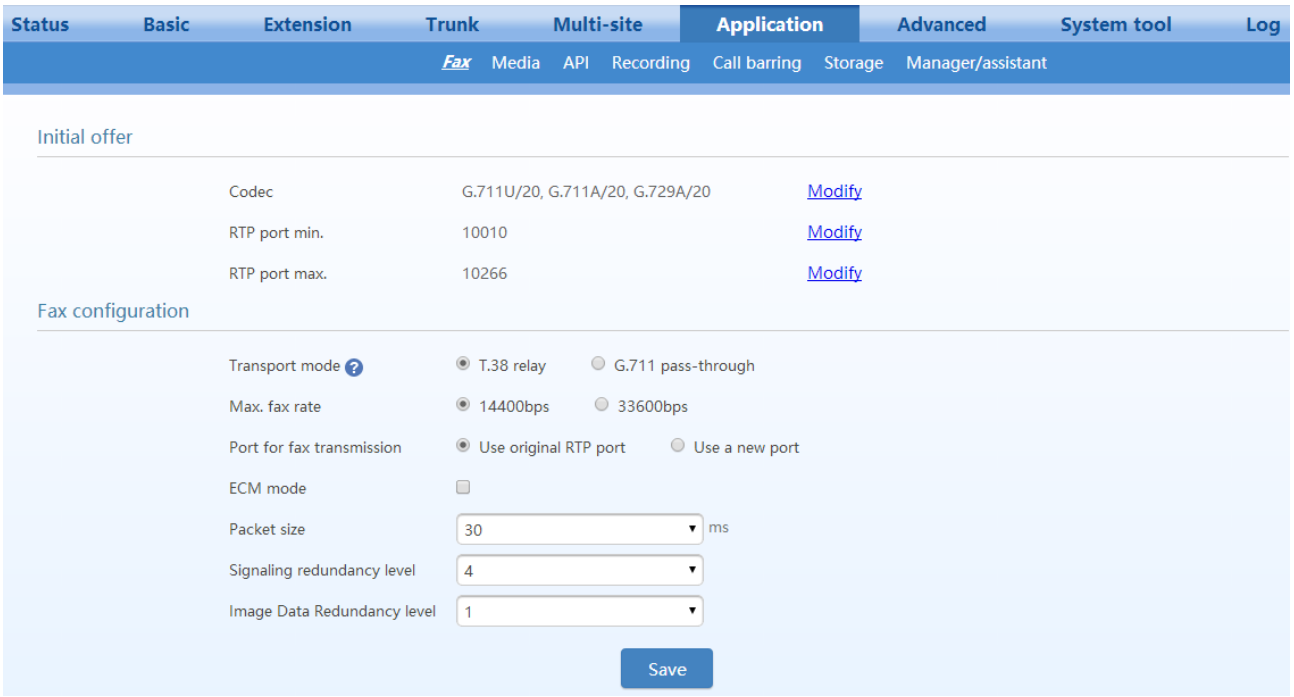


Table 2-25 FAX parameters

Item	Description
Initial offer	To configure codecs in the range of RTP ports for fax transmission, click **Modify** to go to **Media** page for modification. For details, see Table 2-38. **Note:** For G.711 pass-through mode, be sure to select G.711U/20 or G.711A/20 as initial codecs to ensure a successful fax relay.
Transport mode	The device supports two fax transport modes: **T.38 relay** and **G.711 pass-through**. The fax transport modes should be selected based on the service provider's requirement. • **Transport via analog trunk:** Select **G.711 pass-through** • **Transport via SIP trunk:** Select the fax transport mode based on the service provider's capabilities. If the SIP trunk provider supports both **T.38 relay** and **G.711 pass-through**, it is recommended to select T.38 relay for more reliable transport.
Max. fax rate	Select the fax maximum transmission rate. The fax messages can be sent at either the higher speed of 33,600 bps or the lower speed of 14,400 bps. Note: the service provider's gateways must support T.38 version 3 with V.34 for the fax to actually be sent at 33,600bps, otherwise, it will fall back to V.17 speeds (14,400bps).
Port for fax transmission	Set whether to use a new RTP port when the gateway switches to the T.38 mode. The default value is **Use original RTP port**. • **Use original RTP port:** The original RTP port established during the call is used. • **Use a new port:** A new RTP port is used.
ECM mode	The error correction mode (ECM) for the fax feature. The default setting is varied depending on the fax transport mode. • **T.38 relay:** ECM is not checked by default for T38 mode. • **G.711 pass-through:** ECM is checked by default.
Packet size	Set the T.38 data packet interval for T.38. The options include 30 ms and 40 ms. The default value is 30 ms.
Signaling redundancy level	Set the number of signaling redundant frames in T.38 data packets. The range is 0 to 6 frames, and the default value is 4 frames.
Image Data Redundancy level	Set the number of image data frames in T.38 data packets. The range is 0 to 2 frames, and the default value is 1 frames.
Allow opposite terminal to switch to T.38	When the device serves as a fax sending terminal with **G.711 pass-through**, the fax transport mode will automatically switch to **T.38 relay** if the T.38 negotiation request is sent from the opposite terminal.

Note

It is recommended to assign a DID trunk for the extension used for fax transmission. For details, see 2.4.10 DID.

2.7 Multi-site

Two multi-site numbering schemes can be selected:

• Globally assigned: Assign the extension numbers on each site in a uniform way (numbers are unique across all sites).

• Assigned by site: Assign the extension numbers on each site individually.

The two numbering schemes differ in dialing rules for extension number assignment.

2.7.1 Assign the extension numbers globally

With extension numbers assigned in a uniform way, you can make intersite calling without dialing a prefix. As a simple and straightforward numbering scheme, it can be used for expanding port capacity with multiple devices or forming a private network of headquarter and its branch offices. To establish a large scale intersite network in a hierarchical management mode, you need to select **Assigned by site**.

Before configuration, you need to carefully design the numbering scheme for each device to avoid potential number conflicts.

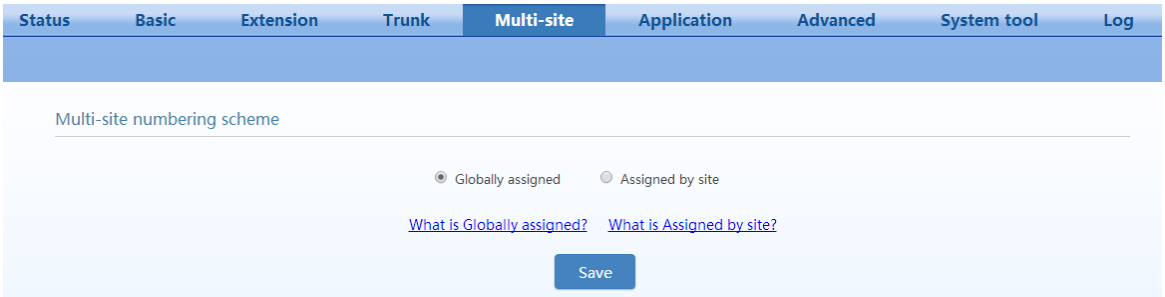
You must configure a management site with several common sites. The management site obtains updated information from each common site and distributes the information to all common sites.

For details, see the description below.

Management site

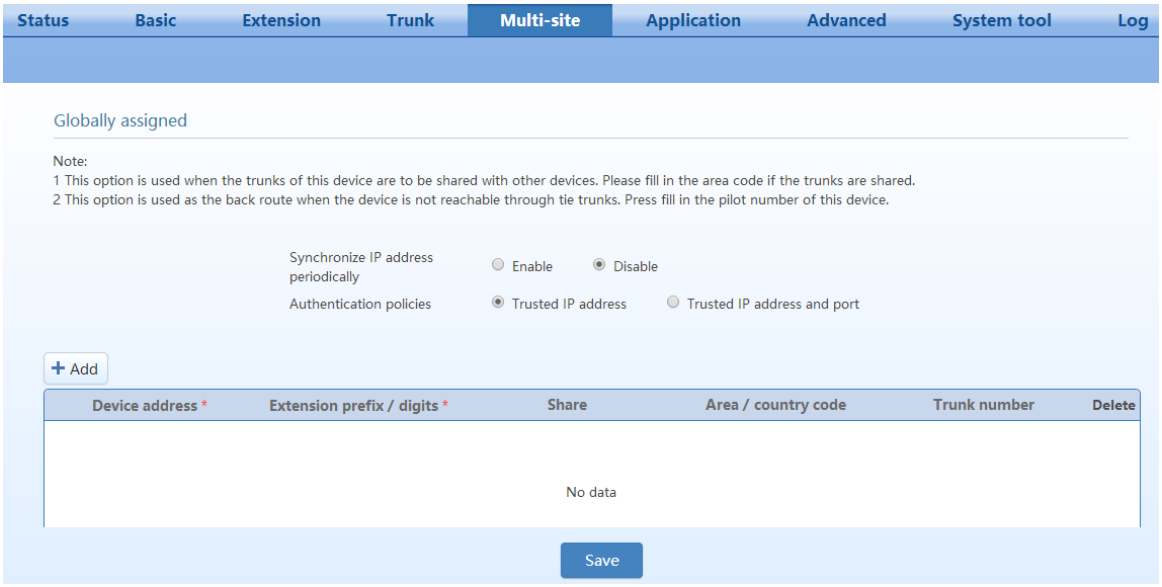
Step 1 Click **Multi-site**, select **Globally assigned**, and click **Save** to display the configuration options.

Figure 2-43 Multi-site numbering scheme selection interface



Step 2 Enable **Synchronize IP address periodically**.

Figure 2-44 Multi-site configuration interface



Step 3 Select authentication policies.

Table 2-26 Authentication policy parameters

Item	Description
Trusted IP address	Authenticates the IP address of the other device in the multi-site network. The message sender whose IP address matches the setting in the site configuration list is considered as a trustworthy device and its message will be processed. Otherwise, the received message will be ignored. This policy is applicable when other devices in the multi-site network communicate from behind a NAT device, for their port numbers will be random.
Trusted IP address and port	Authenticates the IP address and SIP port number of the other device in the multi-site network. The message sender whose IP address and SIP port number both match the setting in the site configuration list is considered as a trustworthy device and its message will be processed. Otherwise, the received message will be ignored.

Step 4 Click **Add**, and configure the managing site.

Figure 2-45 Site adding interface

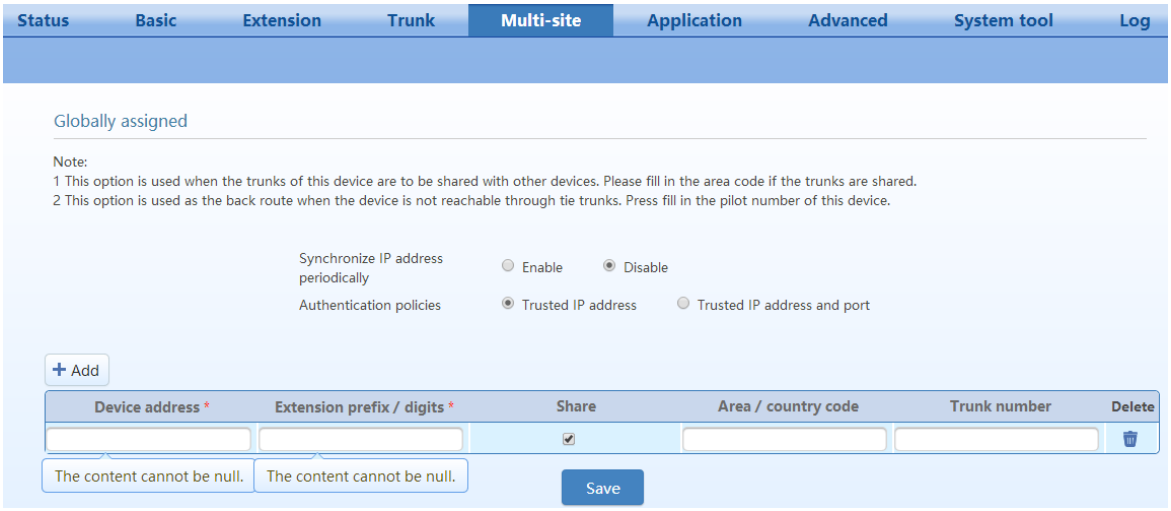


Table 2-27 Configuring sites information

Item	Description
Device address	Enter the device IP address and port number of devices participating in the multi-site setup. For example: 202.56.209.63:8888. If no port number is entered, 5060 is used by default. Important, the first entry must be the management site, while the others are common sites. The IP address of the management site must be fixed. If the IP address of a common site is dynamic, enter the domain name of the common site device, which is the same as the one configured in the Remote Access page. **Note:** If the device is in a private network, port mapping needs to be performed on the front-end router. For details, see Remote Access.
Extension prefix/ digit	The expression of the extension numbers of the device. For example: 2/3 expresses a 3-digit number starting with 2. **Note:** The numbering plans of devices involved in the network must be carefully examined to avoid potential number conflicts. For example: if the prefixes of device A and device B are respectively 2/3 and 21/3, and the two devices have extension 210, the user of device A cannot call extension 210 of device B. All calls to 210 will be connected to extension 210 of device A.

Item	Description
Share	Configure the device trunk to be used by other devices.
Area/country code	Fill in the area/country code of the device. A call to the region covered by the area codes could be routed via the trunk of the device. For example: Suppose the area/country code of site A is set to 8, the trunk of site A is shared with other sites in the network. In this case, if other sites can make calls through the trunk of the site A. For example, they dial 861202777 (61202700 is the called party number), then the call will be terminated to 61202700 through the trunk of site A. **Note:** The area/country code must be different from local numbers of other sites. For example: Area code "021" conflicts with the default number 0 to reach the operator (this conflict exists only when an outbound call prefix is configured in the dialing rules of other sites).
Trunk number	When the network is disconnected, the devices in the network can call an extension of other device by calling "Area code + trunk number" through the PSTN.

Step 5 Add other devices to the list.

Click **Add**, and configure all common sites. For the parameter specifications, see Table 2-27.

Step 6 Obtain the latest device list from the management site.

The managing site, which is on the top of the list, will send the latest device list to other devices in the network.

Click **Save** to save the configuration, and restart the device. The managing site (which is on the top of the list) will send the latest device list to other devices in the network.

Note

- If the IP address of a common site is dynamic, the managing site needs to be configured with a fixed IP address, while the device IP address of the common site needs to be domain name.
- If the DNS fails, no IP address can be obtained. It is recommended to disable the DNS.

Common Site

Step 1 Click **Multi-site**, select **Globally assigned**, and click **Save** to display the configuration options.

Step 2 Enable **Synchronize IP address periodically**.

Step 3 Select authentication policies.

Step 4 Click **Add** to configure the management site.

Step 5 Click **Add** to configure this device.

Step 6 Obtain the latest device list from the management site.

Click **Save** to save the configuration. The management site, which is on the top of the list, will send the latest device list to other devices in the network.

2.7.2 Assign the extension numbers for each site individually

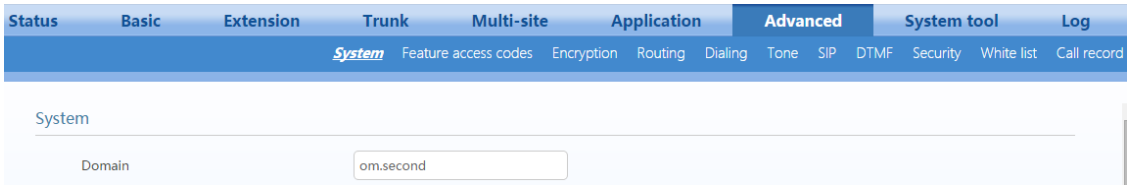
When extensions call each other, a prefix needs to be added to prevent number conflict and ensure that the extension numbers under different sites can be reused with per-site numbering. With this form, a large-scale multi-site telephony network can be built up, in which the numbering plan of each device can be managed independently.

Management Device Configuration

The management device is one of the devices in the multi-site telephone network. The procedure of configuring the managing device is illustrated below.

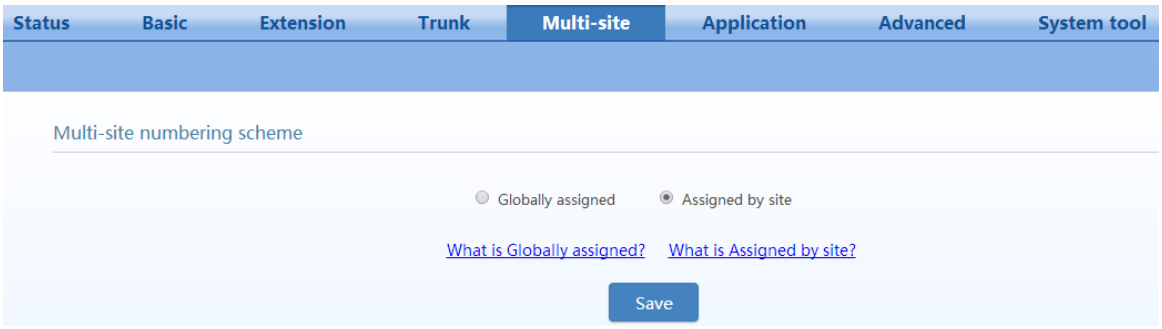
Step1 Go to **Advanced** > **System**, and enter the IP address or domain name of the device in the **Domain** input box, and click **Save**.

Figure 2-46 Domain name interface



Step2 Click **Multi-site**, select **Assigned by site**, and click **Save** to display the configuration options.

Figure 2-47 Multi-site scenarios configuration interface



Step3 Select **Managing site** as the role of the device and click **Save**.

Figure 2-48 Device multi-site role selection interface

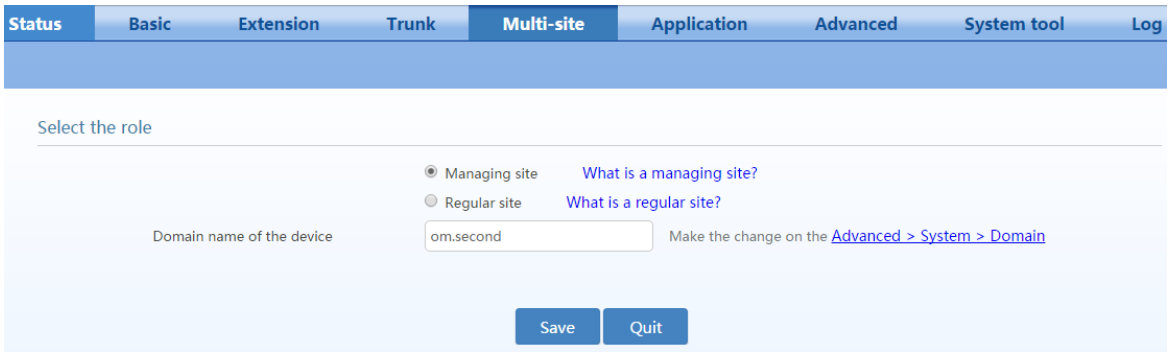
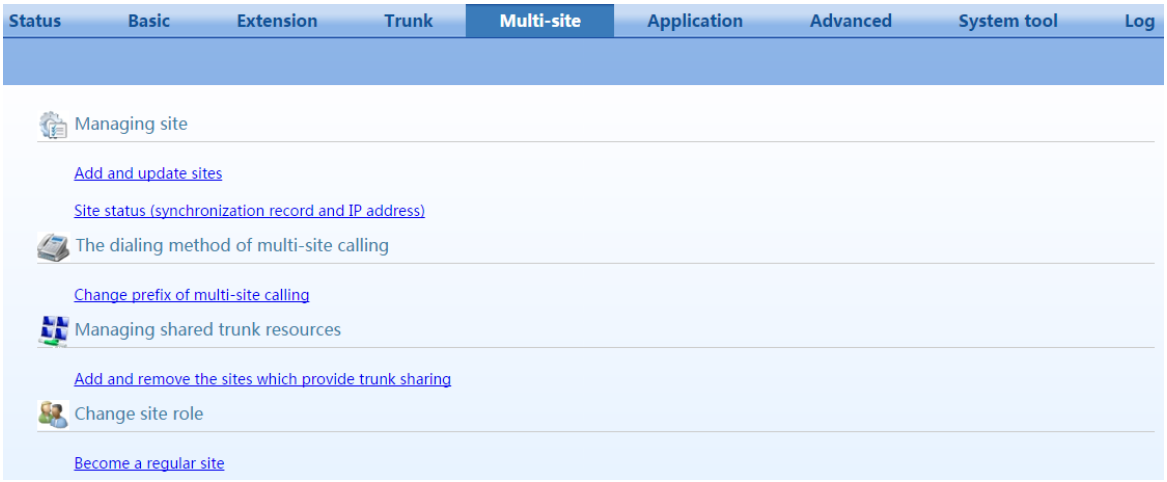


Figure 2-49 Multi-site scenarios configuration interface



Step4 Click **Add and update sites** under **Managing site**, and then click **Add**.

Figure 2-50 Device list configuration interface

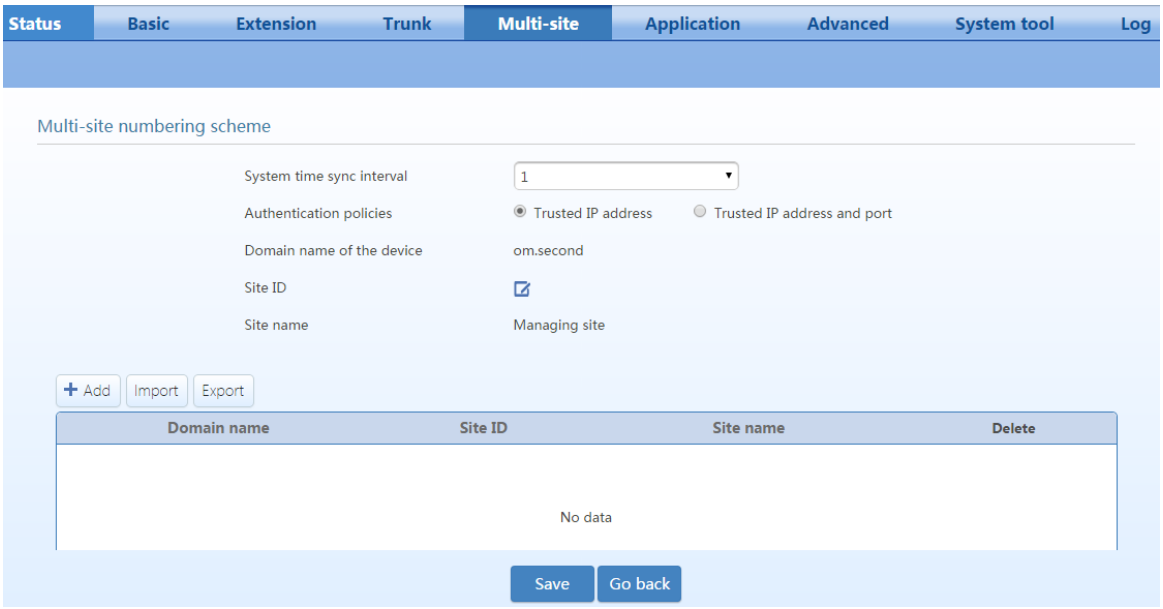


Table 2-28 Numbering scheme parameters

Item	Description
System time sync interval	Interval for synchronization with common sites.
Authentication policies	• **Trusted IP address:** Only IP address of the device needs to be authenticated. • **Trusted IP address and port**: Both the device IP address and the SIP port number need to be authenticated. For details, see Table 2-26.
Domain name of the device	The IP address or domain name of the device. It can be modified in **Advanced** > **System** > **Device domain name**.

Item	Description
Site ID	Enter the site number of the management site, which is used to distinguish between calls of different site devices. The site number can be any value but must be unique.
Site name	Customize the name/role of the site.
Add	
Domain name	Add the domain name of the common site, which must be the same as the domain name configured on the common site. If the port number is not entered, port 5060 is used as default. When the Authentication policy is **Trusted IP address and port**, the port number must be correct. Go to **Trunk** > **IP trunk** > **Registrar OPTIONS**, and you can change the **Local signaling port**.
Site ID	Enter the site number of the common site, which is used to distinguish between calls of different site devices. The site number can be any value but must be unique.
Site name	Customize the role of site. For example: **Common site**.
Delete	Delete the current site.

Step5 **Go back** to the managing site configuration interface, click **Change prefix of multi-site calling** under **The dialing method of multi-site calling**, and then set the dialup prefix.

Figure 2-51 Prefix configuration interface

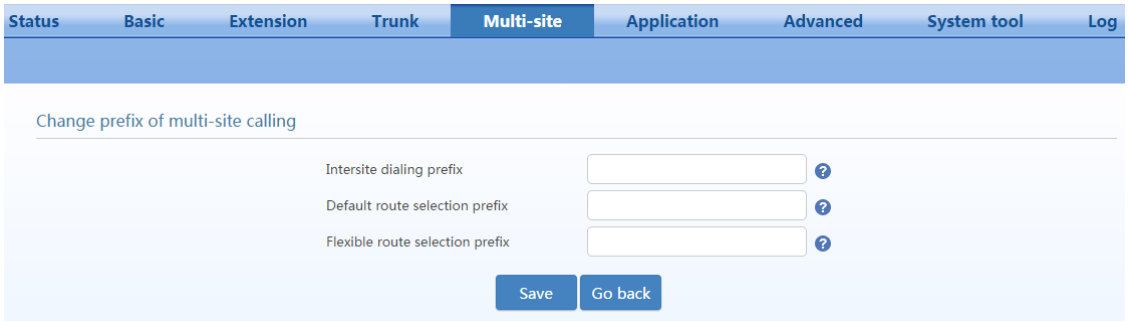


Table 2-29 Prefix setting parameters

Item	Description
Inter-site dialing prefix	Dial to make internal calls between sites. The dial format is: # + Intersite dialing prefix + Site ID +Peer extension number.
Default route selection prefix	Dial to make external calls. The dial format is: #+ Default route selection prefix + Called party number.
Flexible route selection prefix	Added when making external calls. The typical format is: #+ Flexible route selection prefix + Site ID + Called party number.

Step6 **Go back** to the managing site configuration interface, click **Add and remove the sites which provide trunk sharing** under **Managing shared trunk resources**, and configure outbound trunks.

Figure 2-52 Trunk sharing configuration interface

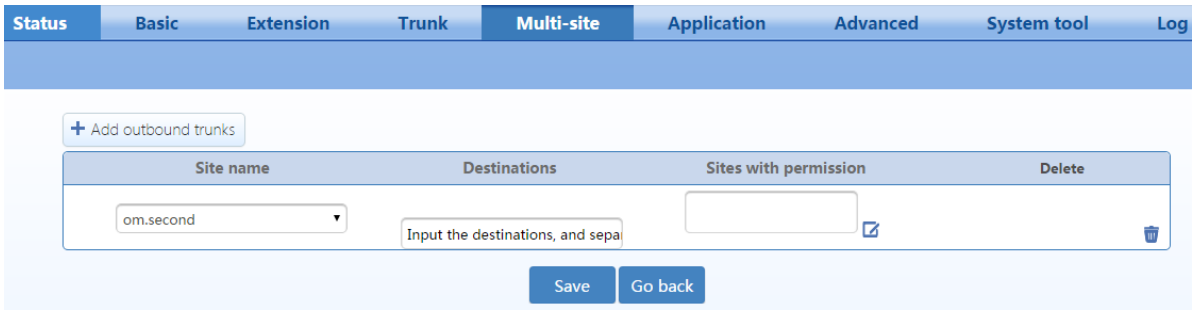


Table 2-30 Trunk sharing setting parameters

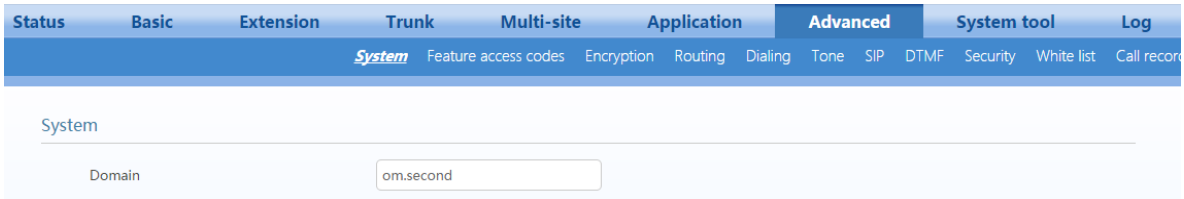
Item	Description
Site name	A site that provides trunk sharing. An outgoing line is provided for the trunk according to the default first rule on the **Outbound dialing rule** interface.
Destinations	Area/country codes that are allowed to call. Multiple area/country codes must be separated by ",".
Sites with permission	Select a site that can use the trunk.

Regular Site

Enter the device domain name.

Step1 On the **Advanced** > **System** interface, enter the domain name of common sites, and click **Save**.

Figure 2-53 Domain name configuration interface

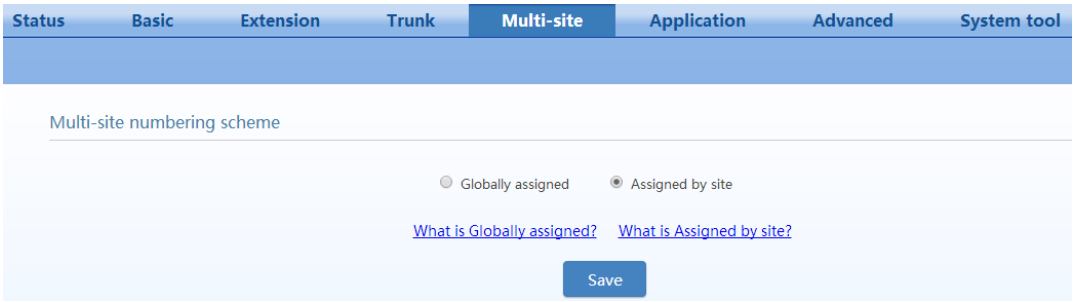


Note

- If the domain name of the device is already set, you can proceed to step 2 directly.
- The device domain name and port number of the common site needs to be reported to the managing site.

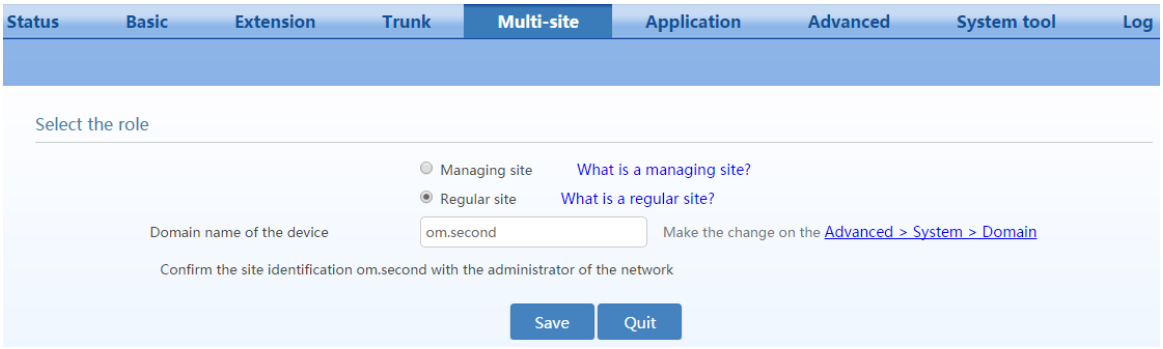
Step2 Click **Multi-site**, select **Assigned by site**, and click **Save** to display the configuration options.

Figure 2-54 Interface of multi-site scenarios 1



Step3 Select **Regular site**, and click **Save**.

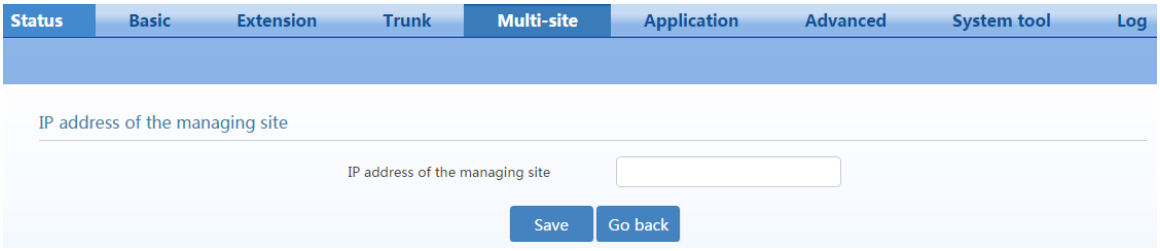
Figure 2-55 Interface for site roles



Step4 Enter the IP address of managing site.

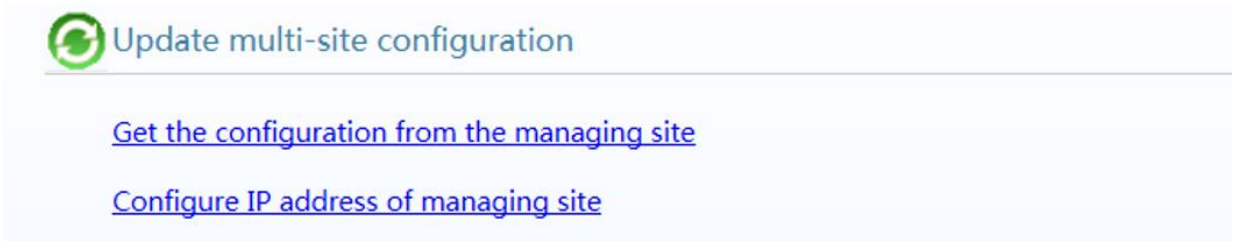
On the **Managing site address** interface, enter **IP address of the managing site**.

Figure 2-56 Managing site address interface



When configuration is successful, the icon turns green.

Figure 2-57 Multi-site networking status interface



2.8 System Settings

2.8.1 Built-in Storage Management (OM20/50)

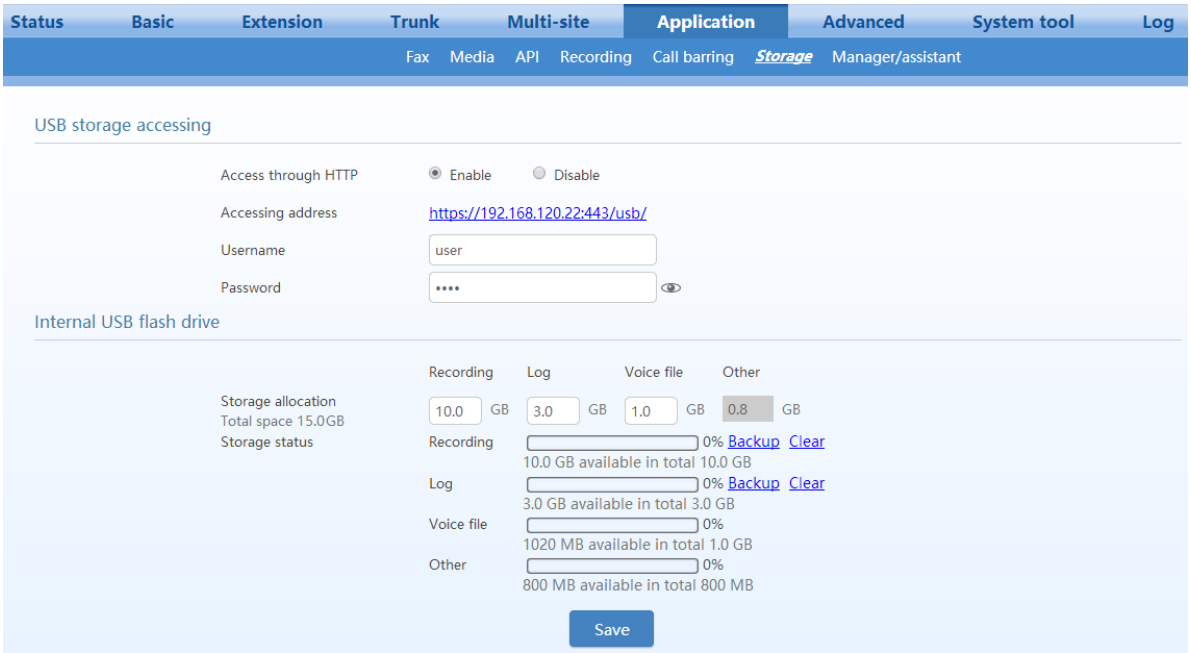
The OM20/50 have an internal USB flash drive of 16GB for storing recording files, log, audio files, etc.

Go to **Application** > **Storage** to manage the internal USB flash drive. Storage space is allocated by default as follows:

Item	Space
Recording	10,240MB
Log	3072MB
Audio file	1024MB
Others	800MB

To expand the storage space, connect an external storage device to the USB port on the device. You can click **Backup** to back up recording files to the external storage device, and then click **Clear** to delete files from the internal USB flash drive. Before backing up files, ensure that sufficient free space is available in the external storage device.

Figure 2-58 Storage interface



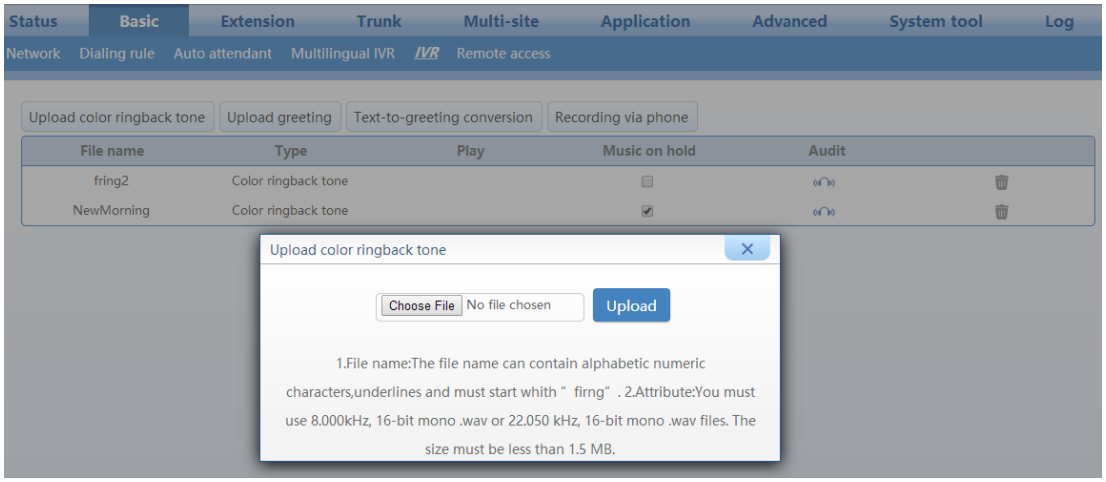
2.8.2 CRBT

Step 1 Go to **Basic** > **IVR**, click **Upload color ringback tone**, and locate and then upload a CRBT file. If the name of the uploaded CRBT file is the same as that of an existing CRBT file, the existing RBT file will be overwritten.

The name of the uploaded audio file must be "fring+number", for example, fring1; the format must be .wav; and the size must not exceed 1.5 MB. The uploaded file is stored in the built-in storage unit (the path is **/media/sda1/ann**). The number of audio files is only limited by the amount of space available on the built-in storage unit.

The audio file conversion tool of New Rock Technologies Inc. can be used to convert an MP3 or WAV file into a CRBT file supported by the OM. For details on how to use the tool, see the *User Guide for Telegreeting*.

Figure 2-59 CRBT file uploading interface



Step 2 Click on the **Extension**>**Analog/IP ext.** page to set the sequence number of the CRBT file to be used for your extension.

Click to play the CRBT file.

Step 3 Click **Save** to save the configuration.

CRBT files can be used to set background music. For details, see 2.8.3 Music on Hold.

2.8.3 Music on Hold

Background music will be played for the party that is placed on hold. Two background music files are available by default: fring2 and NewMorning. You can customize and upload audio files.

CRBT audio files and background music audio files can be shared by the OM50/OM20. For information about uploading a customized audio file, see 2.8.2 CRBT.

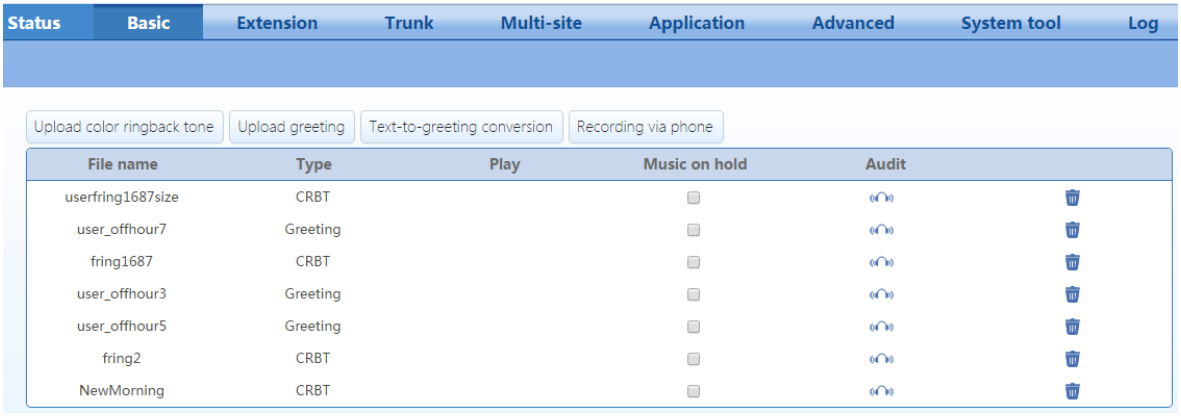
After uploading an audio file, follow this procedure to set background music:

Step 1 Go to **Basic** > **IVR**, select the check box of the desired audio file below **Music on hold**, and then click **OK**.

To play the audio file, click .

To delete an audio file, click .

Figure 2-60 Music on hold configuration interface



2.8.4 Time

The device gets its time from a time server in the network. The device provides a cell for the clock system to ensure normal running of the system in case of a power failure.

Click **System tools**> **System time**, and configure the time server.

Figure 2-61 System time configuration interface

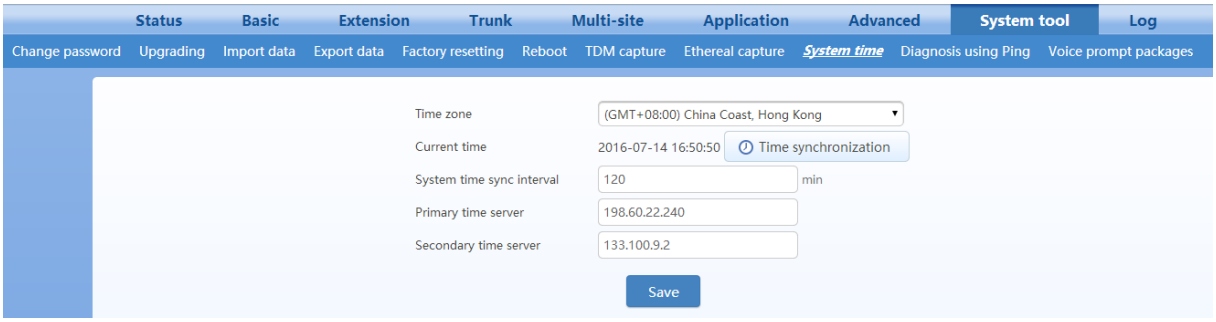


Table 2-31 System time parameters

Item	Description
Time Zone	Select the time zone according to the region where the device is located.
Current time	Displays the current time of the device. You can click **Time synchronization** to calibrate the time.
System time sync interval	Interval for the device to synchronize with the time server. The default value is 120 minutes.
Primary time server	Enter the IP address of primary time server here. It has no default value.
Secondary time server	Enter the IP address of Secondary time server here. It has no default value.

Note

If the device cannot synchronize with a time server, you can click **Time synchronization** to set the time of your PC as the system time of the device.

2.8.5 Encryption

Go to **Advanced** > **Encryption**.

Figure 2-62 Encryption interface

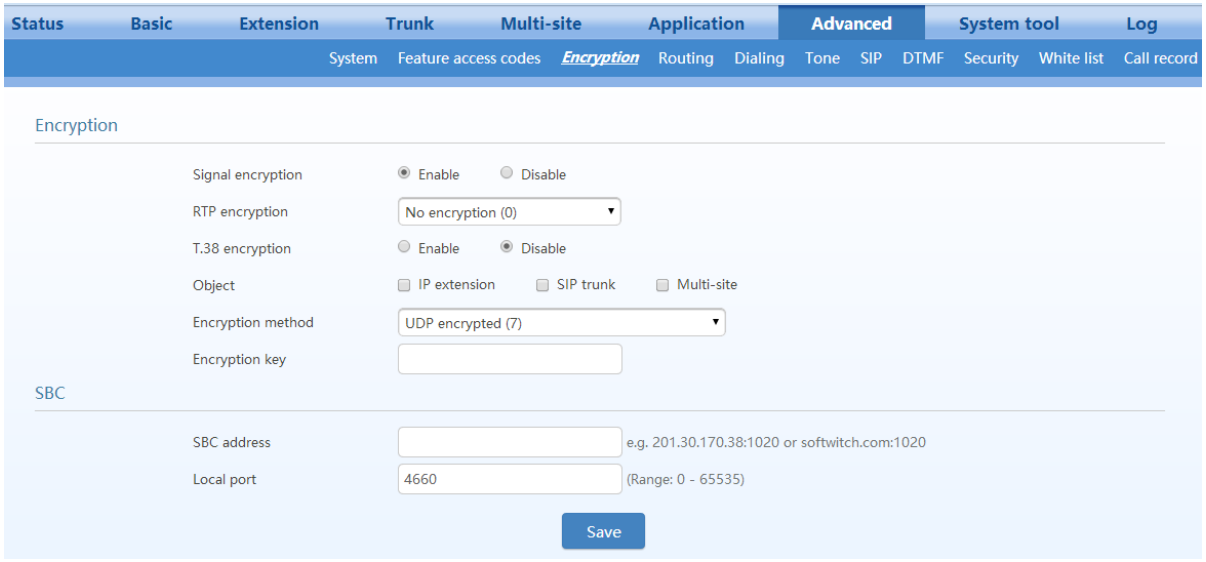


Table 2-32 Encryption parameters

Item	Description
Signal encryption	Enable or disable signaling encryption. It is disabled by default.
RTP encryption	Choose whether to encrypt RTP voice pack, the default is 0. • 0: no encryption • 1: entire message • 2: header only 3: the data body only
T.38 encryption	Choose whether to encrypt the T.38 fax media stream pack. This is not selected by default.
object	• Select an encryption object. • If **IP extension** or **Multi-site** is checked, the terminal needs to support encryption. Otherwise, the terminal cannot be used. • Check **SIP trunk** if SIP server requires encryption.

Item	Description
Encryption method	Set the gateway encryption method, the default value is 7. The optional parameters are: • 2: TCP not encrypted • 3: TCP encrypted • 6: UDP not encrypted • 7:UDP encrypted • 8: Using keyword • 10: RC4 • 14: Encrypt14 • 16: Word reverse(263) • 17: Word reverse(263) • 18: Word reverse(263) • 19: Word reverse(263) • 20:VOS An encryption method can be selected according to the softswitch platform.
Encryption key	Can be obtained from your service provider
SBC	Encryption methods (2), (3), (6), and (7) need to work with New Rock SBC products.
SBC address	Set the IP address and port number of session border proxy server. The characters ":" must be used between the IP address and port number. Server address could be set into the IP address or domain name. Example: 201.30.170.38:1020 or sbc.com:1020. When a domain name is used, it is required to configure the DNS server on the "**Basic**>**Network**" page. Example: 201.30.170.38:1020 or softswitch.com:1020.
Local port	Local port number used for interconnection between the device and the border proxy server. It is 4660 by default. Signaling port number may be set at will, but cannot conflict with other device ports (e.g. 5060).
VOS encryption key	When the encryption method VOS (20) is used, corresponding user names and passwords must be entered.
Username	User name used for encryption. It must be entered when the encryption method VOS (20) is used.
Password	Password used for encryption. It must be entered when the encryption method VOS (20) is used.

2.8.6 Routing Table

A routing table is used to implement number replacement and route allocation. A routing table can contain up to 100 routing rules, which are applied in the order they appear in the table.

Go to **Advanced** > **Routing table**, and add routing rules. The routing rules are described below.

Number Transformation

Format: **Trunk type** *called number prefix* **ADD** *added prefix*

This rule is used to add the *added prefix* to a called number matching the *called number prefix* for an outbound call.

Note: Trunk types include FXS and FXO. FXS indicates that the IP trunk is used to make outbound

calls; FXO indicates that the analog trunk is used to make inbound calls

Examples:

- When an analog trunk is used to make an outbound call, the prefix 17909 is added to the number of the called party:

  FXO *x* **ADD** *17909*

- When an analog trunk is used to make a national toll call (for example: begins with 0), the prefix 17909 is added to the number of the called party:

  FXO *0* **ADD** *17909*

- When an analog trunk is used to make an international toll call (for example: begins with 00), the prefix 17909 is added to the number of the called party:

  FXO *00* **ADD** *17909*

- When a specified analog trunk is used to call a specified called party (for example, analog trunk 1, 2, 3, 4, or 6 is used to call a called number starting with 9), the prefix 17909 is added to the number of the called party:

  FXO[1-4,6] *9* **ADD** *17909*

- When an IP trunk is used to make an outbound call, the prefix 17909 is added to the number of the called party:

  FXS *x* **ADD** *17909*

- When an IP trunk is used to call a called number starting with 10, the prefix 17909 is added to the number of the called party:

  FXS *10* **ADD** *17909*

Call Duration Restriction

Format: **FXS** *Called number prefix* **TIME** *Duration*

This rule restricts the call duration of an outbound call whose called number matches the *called number prefix*.

Note: The call duration restriction rule starts with “FXS” no matter the outbound call is made by an analog extension or an IP extension.

Examples:

- When a call is made to a specified called number (for example, a number starting with 00 when an international toll call is made), the call duration is restricted to 10 minutes:

  FXS *00* **TIME** *10*

Directional Route

Format: **FXS** *called number prefix* **ROUTE** *destination*

This rule is used to direct an outbound call whose called number matches the *called number prefix* to a

specified destination.

Note: No matter the outbound call is made by an analog extension or an IP extension, the directional routing rule starts with “FXS”. The destination can be FXO (analog trunk), IPT (IP trunk), or IP (IP address).

Examples:

- Called-party-number-based routing to an outbound analog trunk. In this example, calls to destination numbers starting with 6120 are routed to FXO port 1 or port 2 in sequential fashion

  FXS *6120* **ROUTE** *FXO 1-2*

- Called-party-number based routing to an outbound SIP trunk. In this example, calls to destination numbers starting with 6120 are routed to SIP trunk with ID 1 to 6 in sequential fashion:

  FXS *6120* **ROUTE** *IPT 1–6*

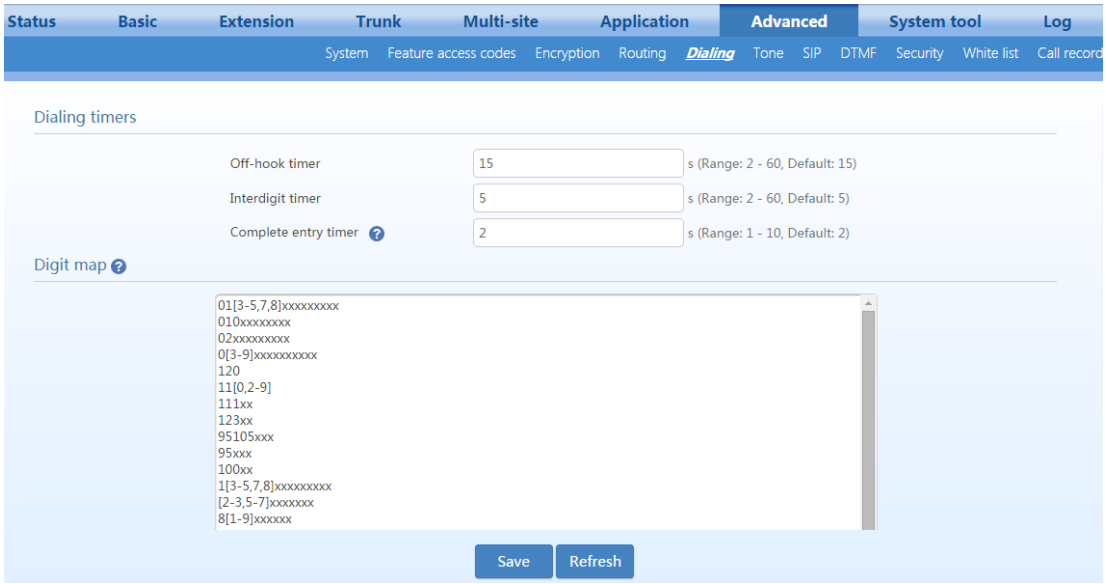
- Called party number based routing to an IP address. **FXS** *6120* **ROUTE** *IP 192.168.2.218*

2.8.7 Dialed Number Detection and Digit Map

During the process of collecting DTMF digits, the device matches the receiving digit string with the rules in the digit map. The receiving process is completed when a matching pattern is encountered. A well-defined digit map helps to speed up the time it takes to dial a number.

Click **Advanced**>**Dialing**, and set digit map rules.

Figure 2-63 Dialing interface



A digit map in the device is composed of up to 100 rules, each with up to 50 digits. The total length of a digit map is limited to 4,500 digits. The default digit map only contains system function rules. If you want set your own digit map, please choose the country in **Advanced** > **Tones** and input the rules you want to the text box. The following provides descriptions of typical rules:

Table 2-33 Description of a digit map

Character	Description
Off-hook timer	If an analog phone hasn't dialed any number within a specified time by this parameter after being offhook, the device will consider that the analog phone has given up the call and prompt them to hang up with a busy tone. The default value is 15s.
Interdigit timer	If an analog phone hasn't dialed the next number key from the time of dialing the last number key to the time set by this parameter, the device will consider that the dialed number is complete and outdial the dialed number. The default value is 5s.
Complete entry timer	It works with the "XXXXXXXXXX.T" rule in the digit map. The default value is 2s.
0-9, *, #	Matches a specific a DTMF digit.
x	Matches any single digit. For example, x can match 1 or 2 or 3...
.	Matches any string of DTMF digits. For example: "1." can match any DTMF numbers starting with "1".
T	End of collecting DTMF digits after the timeout waiting for the next digit. For example, x.T means matching a string (a DTMF string) with any length. The ending is triggered by the timeout for waiting for the next digit.
[ ]	Matches to a set of DTMF digits. For example: [1-3,5,7-9] means the set of 1, 2, 3, 5, 7, 8 and 9.
xxxxxxxxxx.T	For a number with 10 digits, or less than 10 digits, the device terminates receiving digits and sends detected numbers if the duration of no dialing period exceeded the value of the **Interdigit timer** parameter. For a number with more than 10 digits, the device terminates receiving digits and sends detected numbers if the duration of no dialing period exceeded the value of the **Complete entry timer** parameter.
x.#	If "#" is received after any digit is received, the device terminates receiving digits.
[2-8]xxxxxxx	The device terminates receiving digits after receiving eight digits starting with any digits between 2 and 8.
02xxxxxxxxx	The device terminates receiving digits after receiving 11 digits starting with 02.
013xxxxxxxxx	The device terminates receiving digits after receiving 12 digits starting with 013.
13xxxxxxxxx	The device terminates receiving digits after receiving 11 digits starting with 13.
11x	The device terminates receiving digits after receiving three digits starting with 11.
9xxxx	The device terminates receiving digits after receiving five digits starting with 9.

2.8.8 Call Progress Tone

Go to **Advanced**> **tone**, and set or customize prompt tones according to the country or region, such as set dial tone, busy tone, and ring back tone.

Figure 2-64 Call progress tone interface

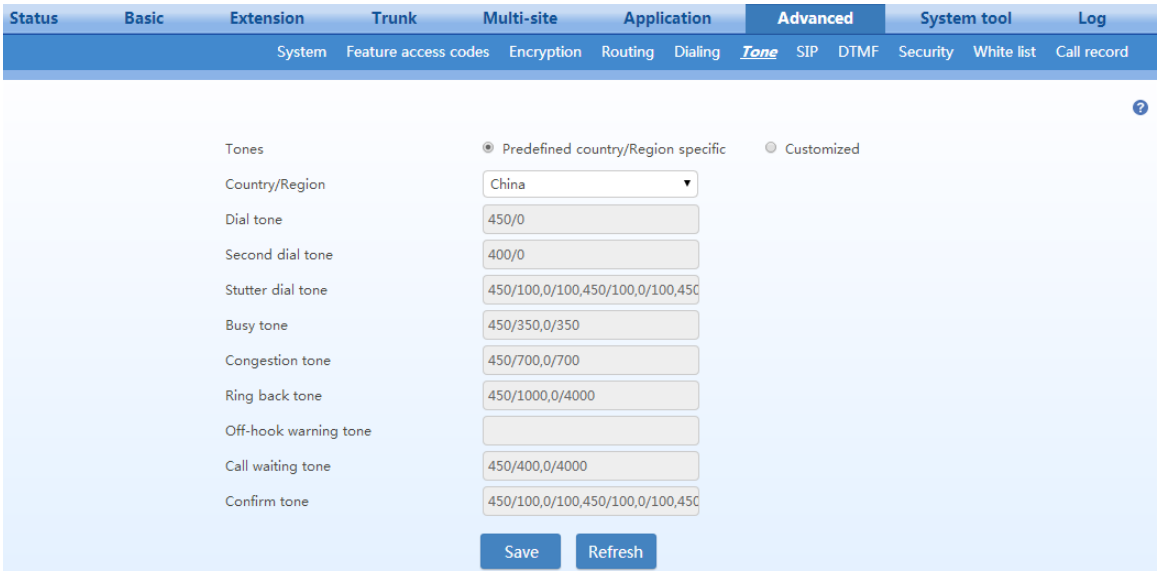


Table 2-34 Call progress tone parameters

Item	Description
Tones	Customized: you can customize the following call prompt tones.
Country/Region	There are call progress tone plans for several countries and regions that are pre-programmed in the device. Users can also specify the tone plan according to the national standard. The device provides tone plans for the following countries and regions: China, the United States, Singapore, Israel, Malaysia, Indonesia, United Arab Emirates, Zimbabwe, Australia, France, Italy, Germany, Mexico, Chile, Russia, Japan, South Korea, Hong Kong, Taiwan, India, Sudan, Iran, Algeria, Pakistan, Philippines, and Kazakhstan.
Dial tone	Prompt tone for off-hook dial tone.
Second dial tone	Used for the second stage dial tone.
Stutter dial tone	Used to notify the following conditions: 1. DND or unconditional call forwarding is activated, or there is new voice message arrived.
Busy tone	Used to notify the caller of a busy line condition.
Congestion tone/reorder tone	Used for notification of call set up failure due to resource limit.
Ring back tone	The tone sent to caller when ringing is on.
Off-hook warning tone	Used to notify the off-hook and no dial activity status of the analog phone.
Call waiting tone	Used to notify the subscriber who is engaged on a call that another caller is attempting to call.
Confirmation tone	Used to confirm feature access codes being entered.

Table 2-35 Examples of customized tone

Examples	Description
350+440 (dial tone)	Indicates the dual–frequency tone consisting of 350 and 440 Hz

Examples	Description
480+620/500,0/500 (busy)	Indicates the dual–frequency tone consisting of 480 and 620 Hz, repeated playing with 500 ms on and 500 ms off. Note: 0/500 indicates 500 ms mute.
440/300,0/10000,440/300,0/10000	Indicates 440 Hz single frequency tone, repeated twice, with 300 ms on and 10s off.
950/333,1400/333,1800/333,0/1000	Indicates repeated playing of 333 ms of 950 Hz, 333 ms of 1400 Hz, 333 ms of 1800 Hz, and mute of 1 second.

2.8.9 SIP Advanced Configuration

Go to **Advanced**> **SIP**, and set SIP compatibility information.

Figure 2-65 SIP related configuration interface

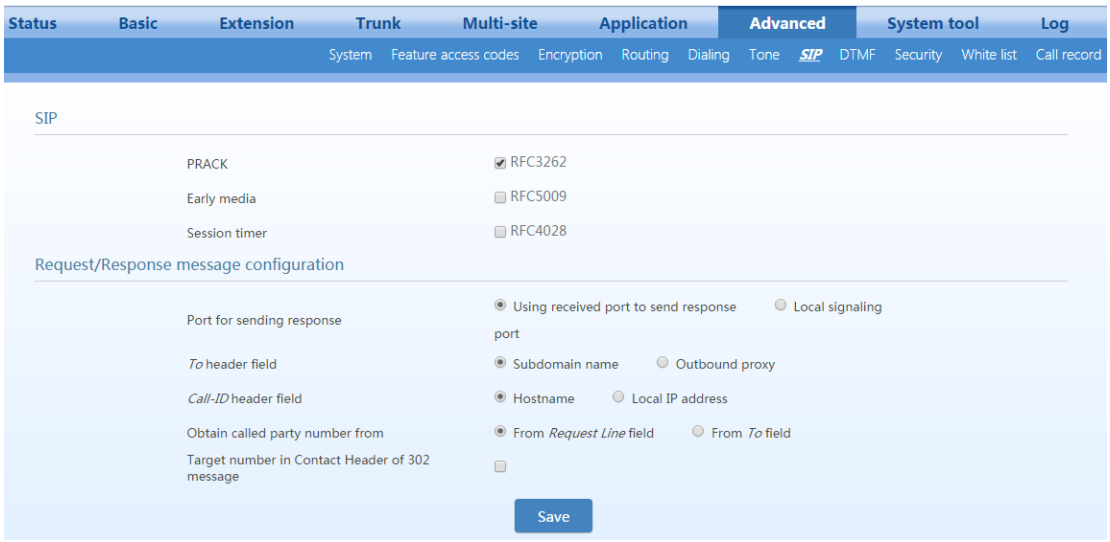


Table 2-36 SIP related parameters

Item	Description
PRACK	Determine whether to activate Provisional Response ACKnowledgement (PRACK). (RFC 3262) It is not selected by default.
Early media	Enable RFC5009. It is not enabled by default.
Media direction attribute	Set parameter values of the P-Early-Media header field: • Supported • Sendrecv • Sendonly • recvonly • Inactive The fields vary according to the type of SIP message. They should be set as required by the peer end. Note: This parameter can be configured after **Early media** is selected.

Item	Description
Session timer	UAs send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The interval for the session refresh requests is determined through negotiation between UAs. If a session refresh request is not received before the interval passes, the session is considered terminated. Both UAs are supposed to send a BYE, and call stateful proxies can remove any state for the call. The refresher and refresh interval are determined based on the negotiation among related parties in the session (including the two parties in the session and the traversing proxies). The refresh interval (carried by the header field of Session-Expires) cannot be less than the **Minimum timer** (carried by the header field of Min-SE). The session refresh function is disabled by default. It is advisable to enable it if the resource release mechanism is incomplete for session-related parties (for example, if there is no RTP stream detection or BYE request timeout detection). After session refresh is enabled: If the device is the calling party, it sends INVITE requests that contain session refresh header field. If the device is the called party, it inserts the final session refresh interval and recommended refresher into the 200 OK message to finish the negotiation.
Session interval	The session refresh interval is the value contained in the Session-Expires header field of INVITE or UPDATE requests. The value range is 30s to 65535s, and the default value is 1800s.
Minimum timer	The minimum session refresh interval allowed by the device. The value range is 30s to 65535s, and the default value is 1800s. The final session refresh interval cannot be less than this value.
Selecting the receiving port for response	Use the receiving port of proxy or use the sending port of proxy. Using received port to send response as default. Use the proxy receiving port or the proxy sending port. The received port is used to send a response as default.
***To* header field**	Choose whether to apply a Sub domain name or an Outbound proxy to the "To" header field. The default is **Sub domain name**.
***Call-ID* header field**	Choose whether to fill Call ID field with the Host name or Local IP address. The default is **Local IP address.**
Called party number	Choose whether the gateway acquires the called number from Request Line header field or the "To" header field. The default is **From Request line field**.
Target number in Contact Header of 302 message	In case of call forwarding, this parameter is used to specify whether the prefix added in the routing rules is included in the target number in the Contact header field of the 302 message sent by the device. This parameter works only when all the following conditions are met: • **FT_FAT_X=on** is set for the IP trunk. • DID to an extension is set for the IP trunk. • Call forwarding to an external target number (e.g. 13812345678) is set for the corresponding DID extension. • A routing rule is configured in which a prefix is added for outbound calls to the target number through an IP trunk (e.g. for routing rule FXS 138 ADD 9). • If this parameter is selected, the target number in the Contact header field of the 302 message sent by the device includes the prefix 9 set in the routing rule, for example 913812345678. Otherwise, the target number in the Contact will be 13812345678.

2.8.10 DTMF

Go to **Advanced** > **DTMF**, and configure DTMF information.

Figure 2-66 DTMF interface

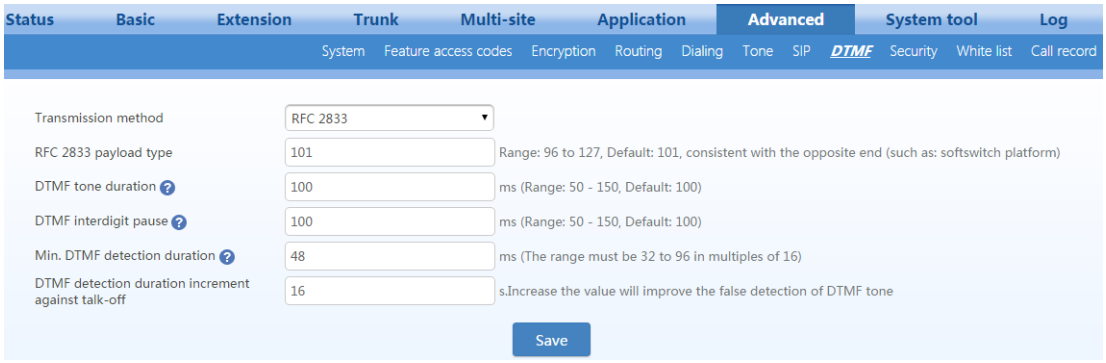


Table 2-37 DTMF parameters

Item	Description
Transmission method	Transmission modes for the DTMF signal supported by the device include RFC 2833, Audio and SIP INFO. The default value is RFC 2833. • **RFC 2833:** Separate the DTMF signal from the media stream and transmit it to the platform through an RTP data package in the format of RFC2833. • **Audio:** The DTMF signal is transmitted to the platform in-band. • **SIP INFO:** Separate the DTMF signal from the media stream and transmit it to the platform in the SIP INFO message format.
RFC 2833 payload type	Used with "RFC 2833" in the DTMF transmission modes. The default value of 2833 payload type is 101. The effective range available is 96 - 127. This parameter should match the setting of a far-end device (e.g. a platform).
DTMF Tone duration	This parameter sets the on time (in ms) of the DTMF signal sent from the FXO port. The default value is 100 ms. The duration time range is 80 - 150 ms.
DTMF Inderdigit pause	This parameter sets the off time (ms) of the DTMF signal sent from the FXO port. The default value is 100 ms. The duration time range is 80 – 150 ms.
Min. DTMF detection duration	Minimum duration time of effective DTMF signal. The valid value ranges from 32 to 96 ms in multiples of 16 ms. The default value is 48 ms. The greater the value is set, the more stringent the detection is.
DTMF detection duration increment against talk-off	The valid values are 16, 32, and 48 ms. Increasing the value can prevent false detection of DTMF signal.

2.8.11 Media

Go to **Application** > **Media**, and set IP media parameters.

Figure 2-67 Media configuration interface

Table 2-38 Media parameters

Item	Description
Codec	Support G729A/20, PCMU/20 and PCMA/20. Multiple codec types can be set separated by a comma, and in this case the device will sequentially negotiate a codec with the peer SIP device.
RTP port Min.	The lower boundary of RTP transmission and the receiving port. The value range is 3000 to 65535 and the default value is 10010. It is recommended that the value be greater than or equal to 10000. Note: Each phone call will occupy RTP and RTCP ports. If the device is equipped with 4 subscriber lines (or trunk line), then 8 UDP ports are needed.
RTP port Max.	The upper boundary of RTP transmission and the receiving port. The value range is 3020 to 65535, and the default value is 10266. The configured value must be greater than or equal to "2 X number of lines + min. RPT port".
TOS/DSCP	Set the service level quality as a guarantee for different priorities. The default value is 0x0c. This parameter specifies the priorities of media streaming.
Max. Jitter buffer	The RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This parameter specifies the maximum number of RTP packets that can be stored in the buffer area. The value range is 0 to 30 frames, and the default value is 2 frames.
Min. Jitter buffer	RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This parameter specifies the minimum number of RTP packets that need to be stored in the buffer area. The value range is 10 to 250 frames, and the default value is 50 frames.
RTP drop SID	If it is selected, the received RTP SID voice packets will be discarded. By default, this is not selected. Note: RTP SID packets should be dropped only when they do not conform to the specifications. Nonstandard RTP SID data could generate noise in calls.
Obtain Media Address From	• **SDP global address**: obtain the media destination IP address from the global connection entry in received SDPs; • **SDP media address**: Obtain the media destination IP address from the first media description in received SDPs. If the first media descriptor in a received SDP does not contain an IP address, the global connection address is used.

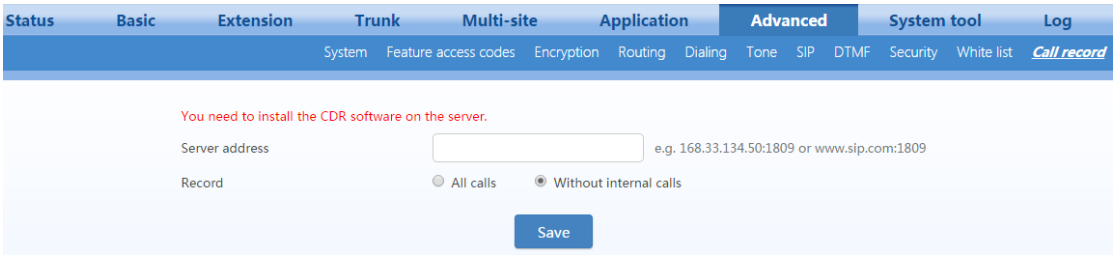
2.8.12 Call Detail Record (CDR)

The device is capable of outputting a detailed record for each call to an external storage server. The information of a CDR includes (among many details), the calling party number, called party number, and the starting and ending timestamps of a call.

The detailed call records are output to a storage server after the completion of a call, and they can be read, searched, saved and deleted through a pre-installed software "CDR software". For details about using the CDR software, see the *CDR Software User Guide*.

Go to **Advanced**> **Call record**, and set the IP address and port number of the CDR server. The default port number is 1809.

Figure 2-68 CDR server configuration interface



2.8.13 API

API is an application programming interface of the "RESTful" style that allows external applications to perform operations on the OM, such as call control, call status monitoring, and configuration. Moreover, with the API, the device can push reports such as events and call records to the external applications.

To use the API, configure the API on the device by following this procedure:

Step 1 Go to **Application** >**API**, and enter the application server address.

Figure 2-69 API configuration interface

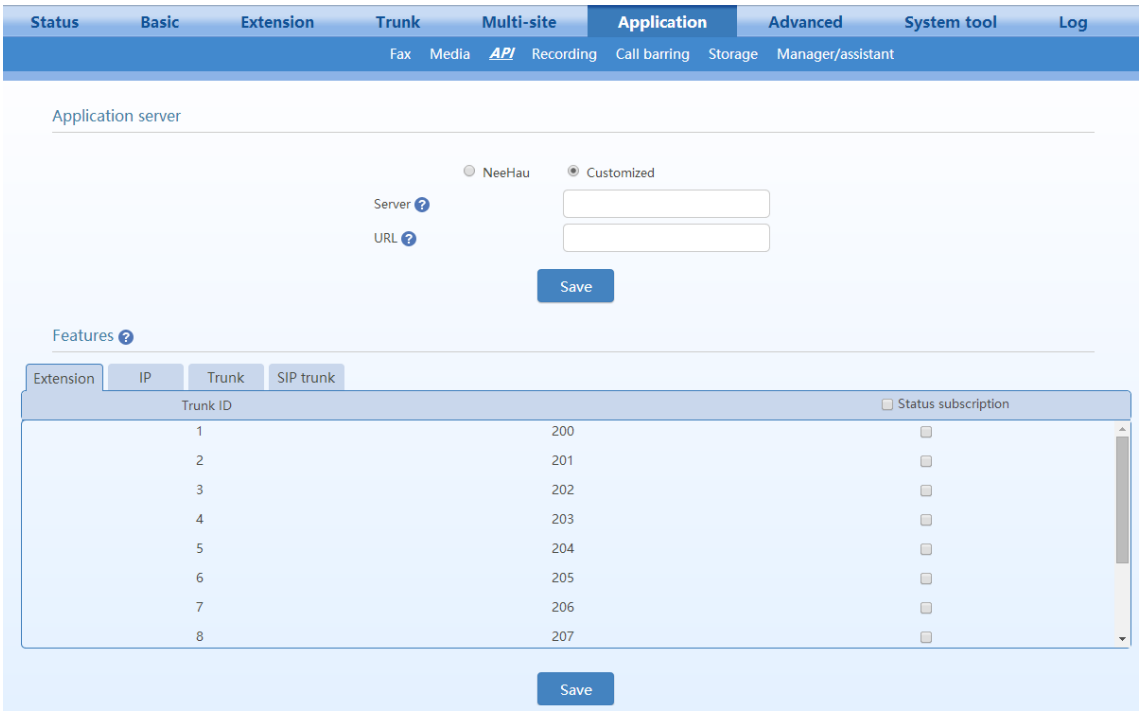


Table 2-39 API parameters

Item	Description
NeeHau	When enabled, the NeeHau Business Phone Assistant is used as the application server. Other application servers are not supported.
Server	Enter the IP address and port number of the third party application server. If no port is specified, port 80 is used. The OM only accepts API request messages that are sent from this IP address. When the OM needs to push API report messages to the application server, it also uses this IP address. Note: To configure this parameter, first disable the NeeHau.
URL	Enter the web page address (relative path) used by the application server to receive messages from the device.

Step 2 Enable API function for the extension/trunk.

Step 3 Click **Save** to save the configuration, and restart the device.

2.8.14 SIP Transmission Mode

Go to **Advanced** > **System**, and set SIP transmission mode.

Figure 2-70 SIP transmission mode configuration interface

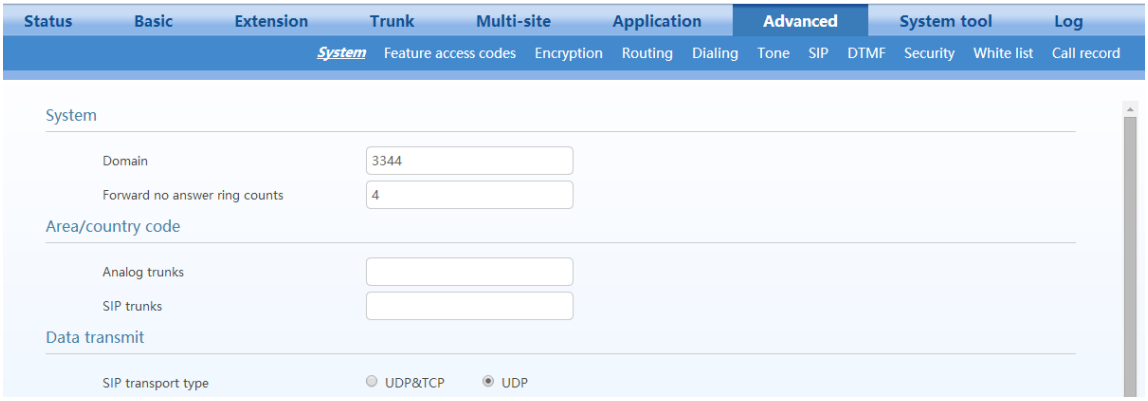


Table 2-40 SIP transmission mode parameters

Item	Description
SIP transport type	Select either UDP&TCP or UDP for SIP messages, and the default is UDP. Both sides must select the same transmission protocol.
SIP TCP local port	Local SIP port used when TCP is used.

2.8.15 Auto Provisioning

The auto provision function allows you to centrally manage software and configuration files for the device by using an auto provisioning server (ACS).

Go to **Advanced** > **System**.

Figure 2-71 Auto provision interface

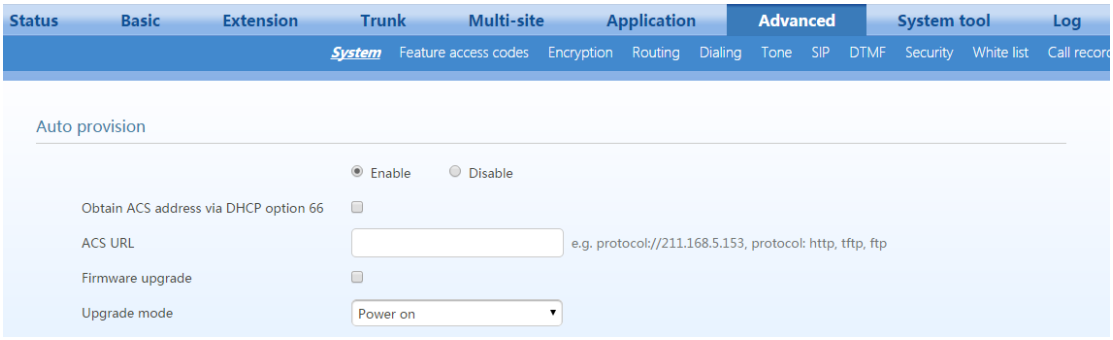


Table 2-41 Auto provision parameters

Item	Description
Obtain ACS address via DHCP option 66	ACS (TFTP/HTTP/HTTPS) address is obtained by using option 66 of the DHCP

Item	Description
ACS URL	Manually configure the ACS address, which can be a TFTP, FTP, or HTTP server. • tftp://ACS address • ftp:// ACS address • http:// ACS address • https://ACS address
User name	Input a user name for accessing the ACS. Note: If the ACS is a TFTP server, the username and the password are not displayed.
Password	Input a password for accessing the ACS.
Firmware upgrade	Download the firmware upgrade package from the firmware upgrade package address set in the configuration file. The device will automatically upgrade the firmware. Note: For the OM20/50, the firmware can be a **tar.gz** file or an **img** file. For the OM80, the firmware is always a **tar.gz** file.
Update mode	• Power on: The device detects whether there are configurations and firmware to be updated when the device is powered on. • Power on + Periodic: When the device is powered on, the gateway first checks whether there are configurations and firmware to be updated, and then periodically performs checking based on the set times.
Upgrade period	When **Power on + Period** is set, this parameter specifies the interval for periodic automatic upgrades. The default is 3600s. The value range is 5 to 86400 second.

2.8.16 TR069

Go to **Advanced** > **System**.

Figure 2-72 TR069 interface

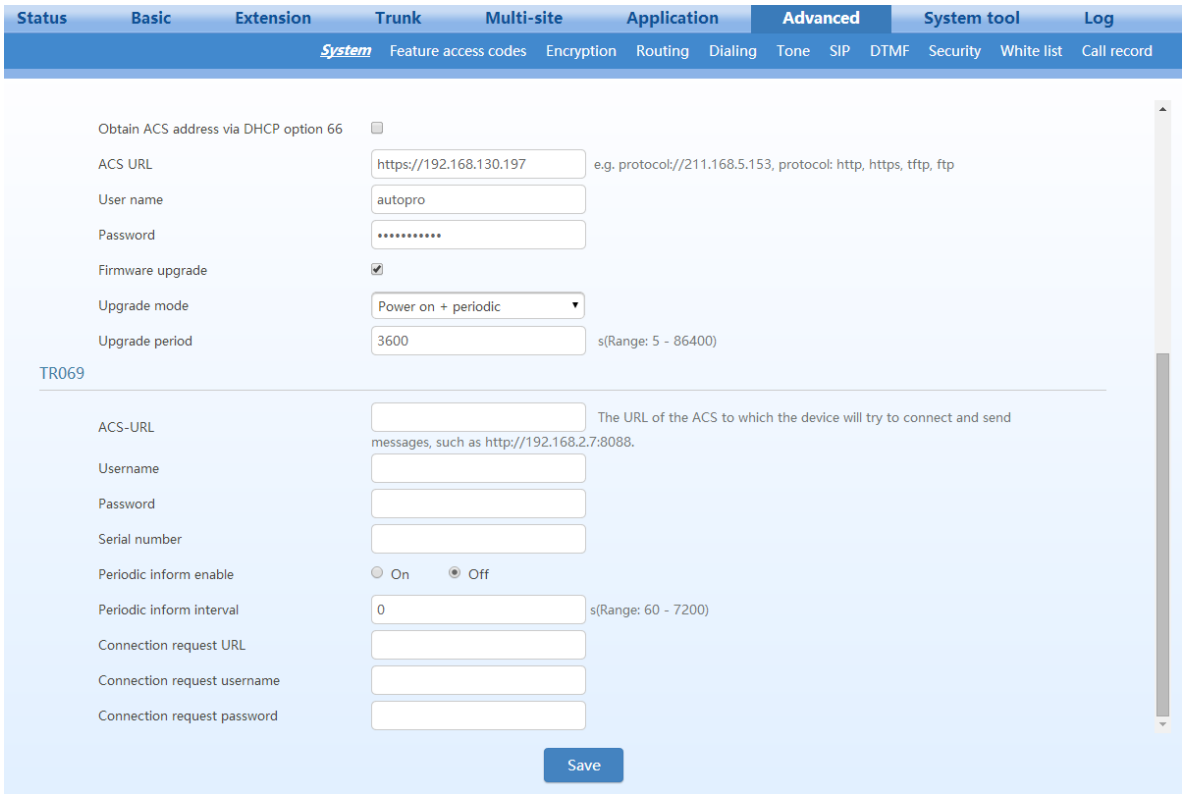


Table 2-42 TR069 parameters

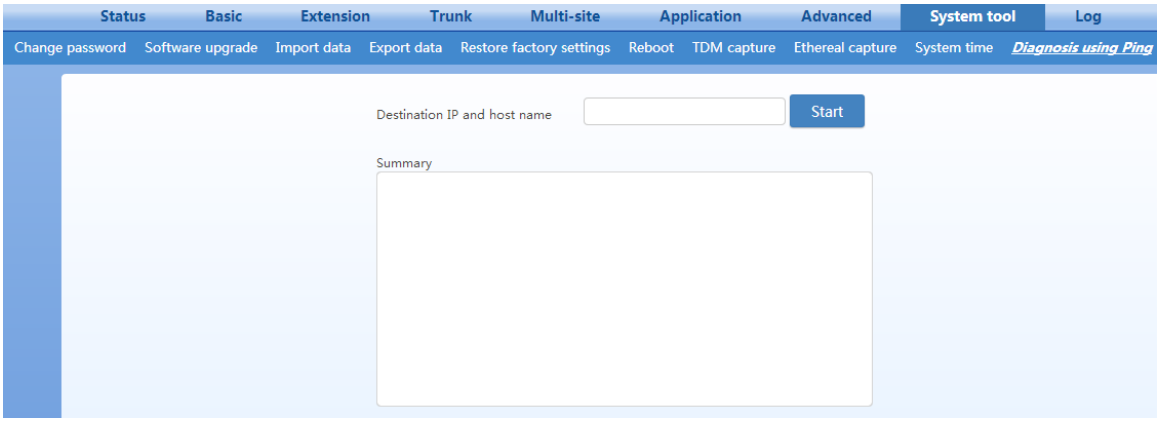
Item	Description
ACS-URL	Specify the URL of the ACS.
User name	Specify the user name to be used by the device to authenticate with the ACS.
Password	Specify the password to be used by the device to authenticate with the file server
Serial number	Serial number of the product. By default, it is the MAC address provided by New Rock. When the device is connected to the operator's network management server, the serial number provided by the operator can be entered.
Periodic inform enable	A switch used to specify whether to periodically report to the ACS.
Periodic inform interval	The interval for reporting to the ACS.
Connection request URL	The address used for the ACS to connect back to the device. Generally, it is automatically generated. You can also enter the address of the device manually.
Connection request username	The account used for the ACS to connect back to the device. For example: admin.
Connection request password	The password used for the network management server to connect back to the device.

2.8.17 Ping Diagnosis

This tool is used to check the connectivity of the network.

Go to **System tools**>**Diagnosis using ping**, enter the IP address or host name, and start diagnosis. The diagnosis details can be seen in the **Summary** box.

Figure 2-73 Ping diagnosis interface



2.9 Security management

2.9.1 Whitelist

Go to the **Advanced**>**Whitelist** page to enter the IP addresses that are allowed to access the web or Telnet/SSH service on the device.

After the Whitelist function is enabled, only IP addresses in the Whitelist are allowed to access the web or Telnet service on the OM. The OM also provides an embedded white-listed address 192.168.2.100 upon factory delivery, in addition to the customized Whitelist.

Follow this procedure:

Step1 Go to **Advanced** > **Whitelist**, click **Add**, and enter an address. A maximum of 20 addresses can be added.

Figure 2-74 Whitelist interface

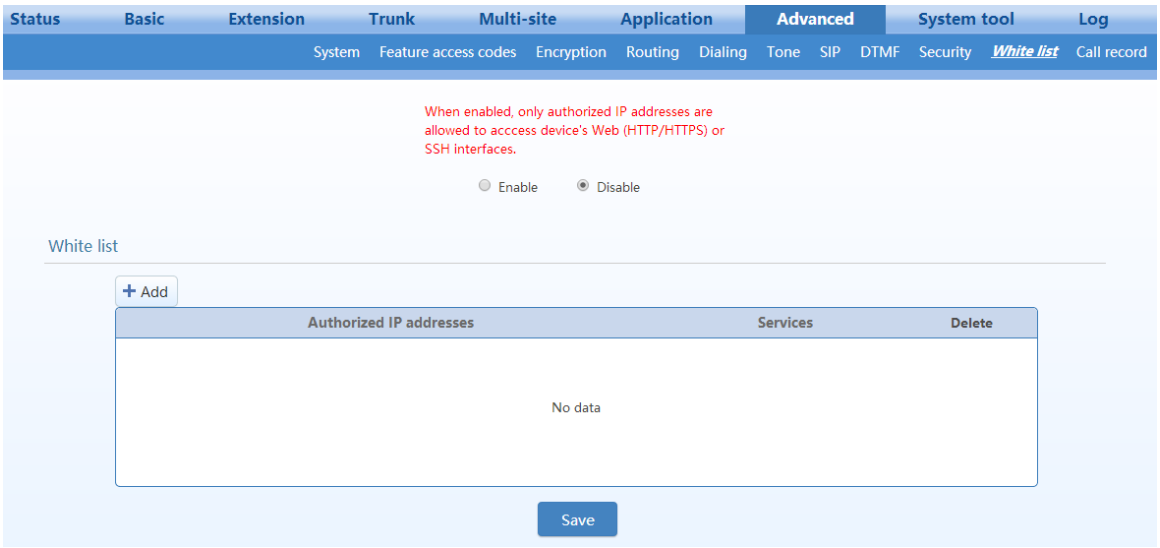


Table 2-43 Whitelist parameters

Item	Description
Authorized IP addresses	Click **Add**, enter the IP address allowed to access the OM.
Service	Select services that can be accessed, such as Telnet, SSH, HTTP and HTTPS.
Delete	Delete the current entry from the Whitelist.

Step2 Click **Save** to save the configuration.

Step3 **Enable** Whitelist.

Note

- To access the device by using a Telnet/SSH session, you also need to enable the Telnet/SSH service on the **Advanced**> **Security** interface.
- If you forgot the white-listed address previously set and cannot access the device it can be recovered. For details, see 3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?

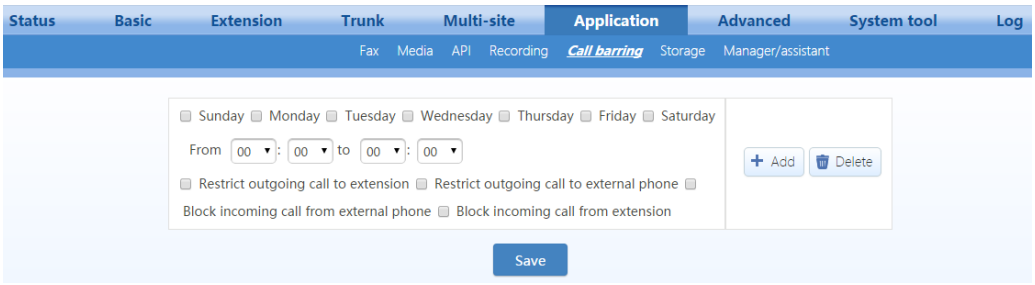
2.9.2 Outbound Call Screening

The device can restrict the outbound and inbound call functions of an extension based on time segment according to preset time and function templates.

Follow this procedure:

Step 1 Go to **Application** > **Call Barring**, set the time when the restriction becomes valid, and set the inbound call restriction and outbound call restriction of the extension. For example: You can prevent inbound calls made from 00:00 to 08:00. Click **Add** to add call restriction conditions.

Figure 2-75 Outbound call screening interface



Step 2 Click **Save**.

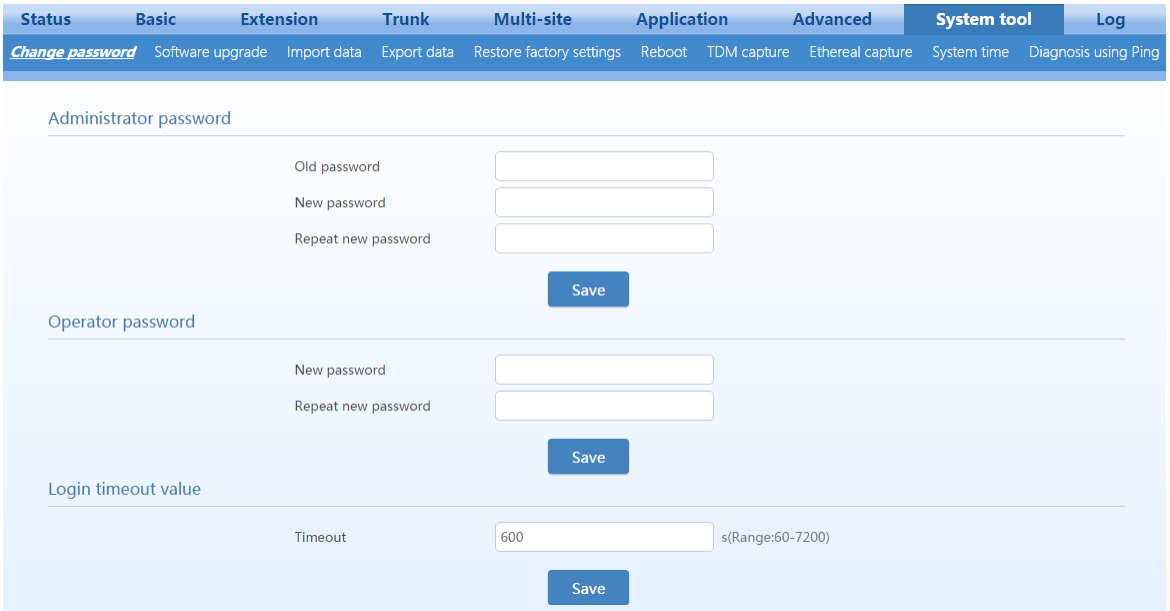
Step 3 Go to **Extension** > **Analog/IP** > **Set**, and select the **Call restriction** function of the extension.

Step 4 Click **Save**.

2.9.3 Change Password

Go to **System tools** > **Change password**, change administrator password or operator password, and set a login timer. Only an administrator is allowed to change passwords.

Figure 2-76 Password interface

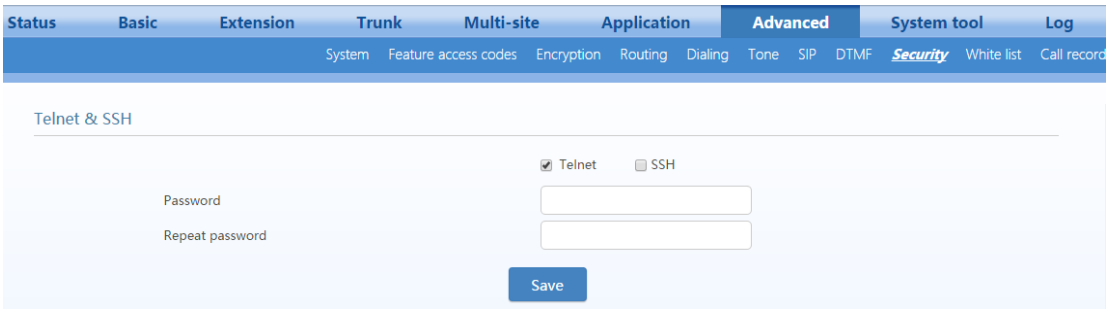


2.9.4 Telnet&SSH

By default, Telnet/SSH is disabled on the device. Generally, it is recommended that the Telnet/SSH be disabled.

To enable Telnet or SSH, go to **Advanced** > **Security**. When both Telnet and SSH are enabled, their passwords are the same.

Figure 2-77 Telnet&SSH configuration interface

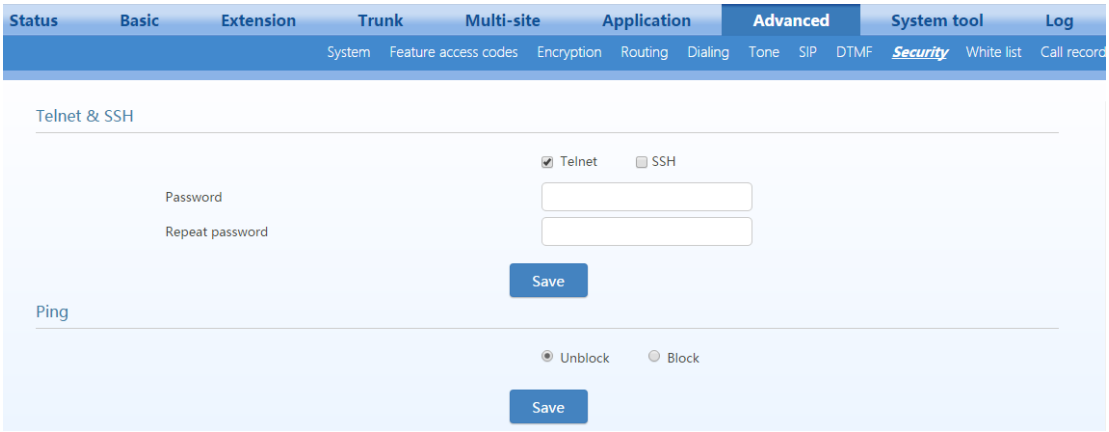


2.9.5 Ping Blocking

If **Block** is chosen, the device will not respond to any Ping requests, which helps prevent malicious attacks.

Go to **Advanced** > **Security** to block or unblock the Ping requests.

Figure 2-78 Ping blocking/unblocking interface



2.9.6 Web Management

The device supports access to the Web GUI by using HTTP or HTTPS.

Go to **Advanced** > **Security**, and configure an HTTPS or HTTP port. The settings take effect after the OM is restarted.

Figure 2-79 Web management interface

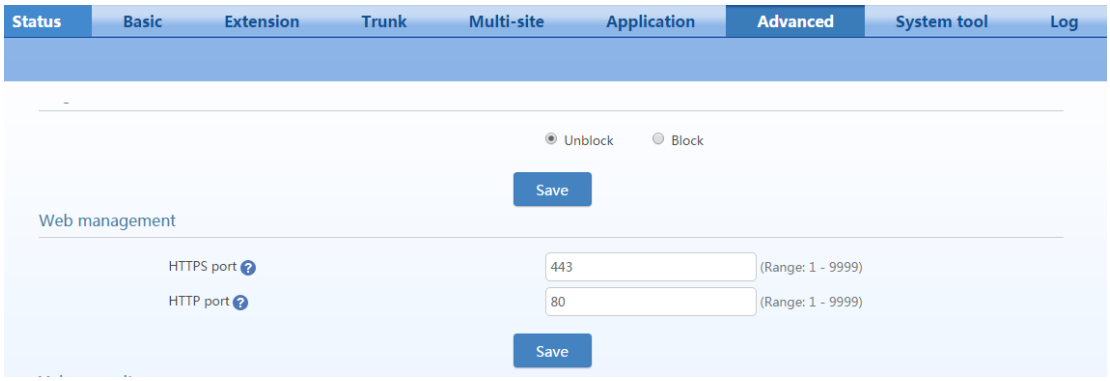


Table 2-44 Web management parameters

Item	Description
HTTPS port	Set the port used to access the device with HTTPS. The value range is 1 to 9999, and the default value is 443. Note: HTTPS port cannot be set for the OM80.
HTTP port	Set the port used to access the device with HTTP. The value range is 1 to 9999, and the default value is 80.

2.9.7 Voice Security

Go to **Advanced** > **Security**, and configure voice security related functions.

Figure 2-80 Voice security interface

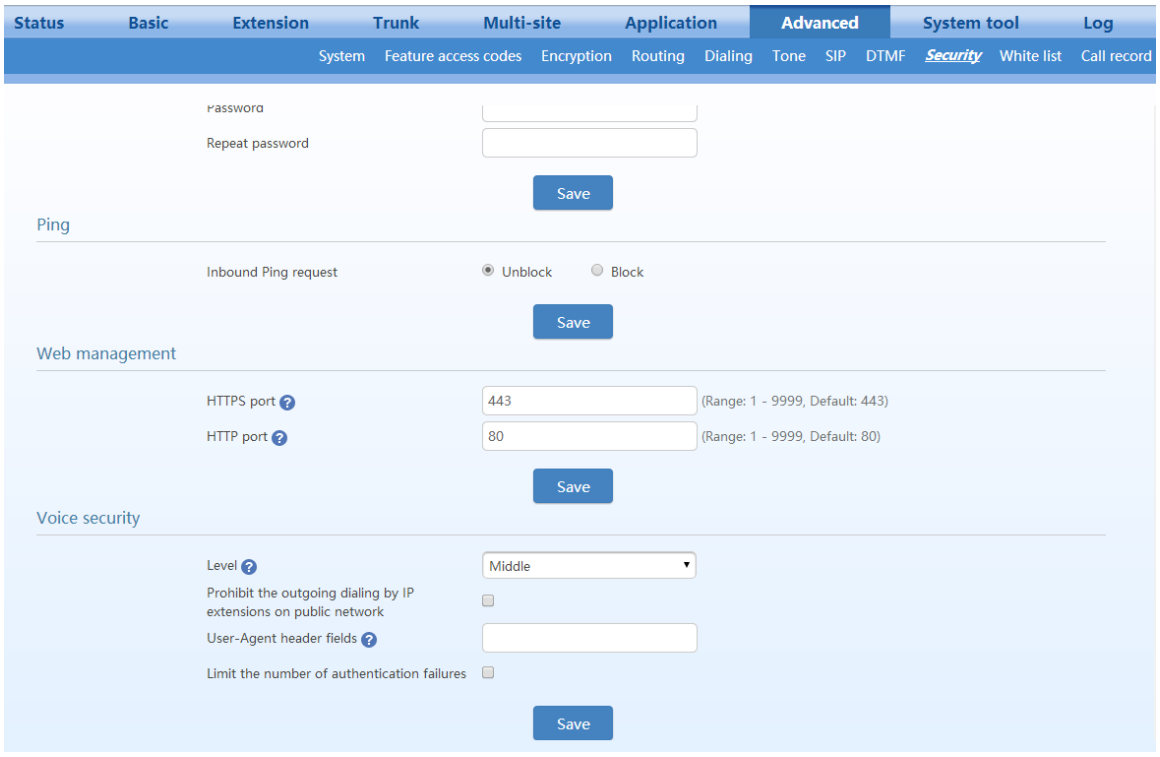


Table 2-45 Voice security parameters

Item	Description
Level	The security levels are described as follows: • **High security level: For an IP extension** in an internal network, if the SIP signaling port is greater than 10000 and if the registration password and number are the same, registration is not allowed. For an IP extension in an external network, if the registration password and number are the same, registration is not allowed. A terminal in an external network is not allowed to access the Web GUI. • **Medium security level:** Similar to the above restrictions, except that a terminal in an external network is allowed to access the Web GUI. • **Low security level:** The preceding restrictions are not imposed.
Prohibit the outgoing dialing by IP extensions on public network	An IP extension in an external network is only allowed to call extensions.
User-Agent header fields	Input the User-Agent header field of the clients that are allowed to register with the device. If there are multiples of client fields, each of them must be separated by ",". If this parameter is set when registering with the device, the IP extension must carry the same User-Agent header field, otherwise registration fails.
Limit the number of authentication failures	When the number of authentication failures of the IP extension exceeds the specified threshold, the device will reject the registration request by the IP extension. The IP extension is allowed to register with the device only after the IP address of the extension is changed or the OM is restarted.

2.10 Maintenance

2.10.1 Upgrading

Upgrading by .tar.gz file

Before upgrading software, go to **System tool** > **Export data**, and export the current configuration for backup.

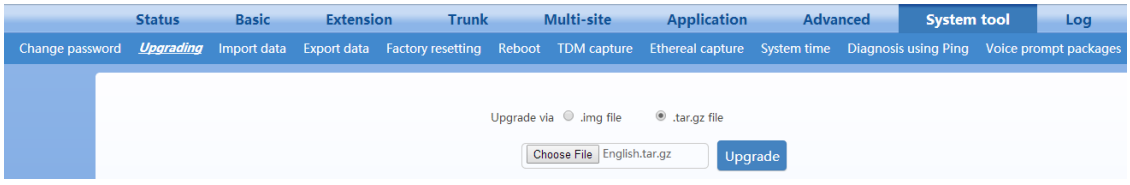
Step 1 Go to **System tool** > **Upgrading**.

Step 2 If the kernel version is not required to upgrade, choose the **.tzr.gz file** and upload the upgrade file (the upgrade file can be directly uploaded without being decompressed).

Step 3 Click **Upgrade** and follow the upgrade instructions.

Note: Please contact the supplier to obtain the latest firmware release.

Figure 2-81 Upgrading interface by .tar.gz file



Upgrading by .img file

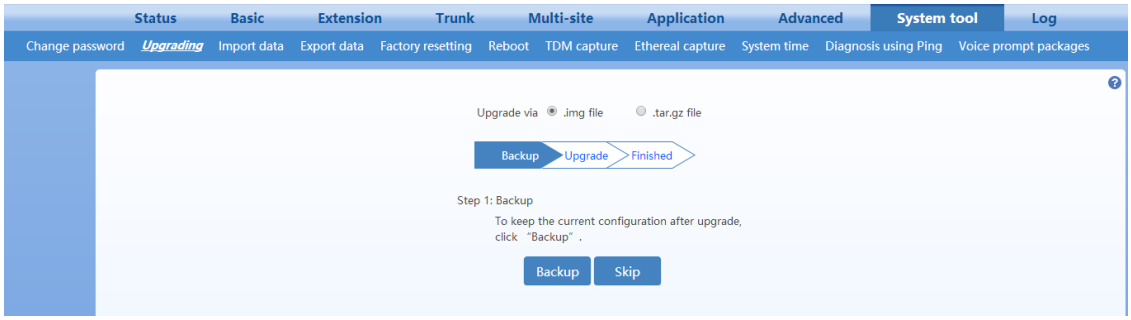
If the kernel version is required to upgrade, choose the **.img file**.

Step 1 Click **Backup** to save the current configuration.

Step 2 Click **Upgrade** and follow the upgrade instructions.

Note: Please contact the supplier to obtain the latest firmware release.

Figure 2-82 Upgrading interface by .img file



Note

- The upgrade takes several minutes. It is not advisable to upgrade software when network traffic is heavy.
- During the upgrade, do not power off, restart the device, or disconnect the device from the Internet, otherwise the system will be corrupted, and the device cannot be started. When the upgrade succeeds, the device will restart automatically.

2.10.2 Configuration Maintenance

Go to **System tool** > **Import data/ Export data/Factory resetting** to import/export configuration files for the device or restore the device to factory settings.

Figure 2-83 Data importing interface

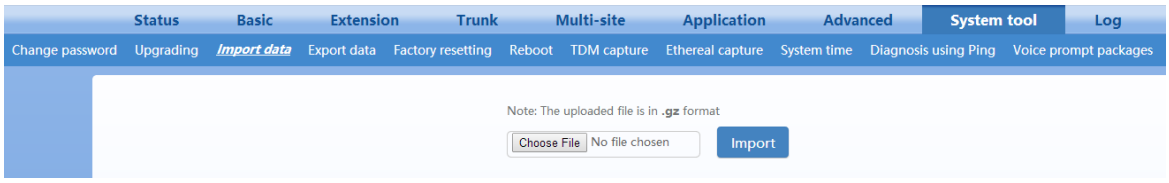


Figure 2-84 Data-export interface

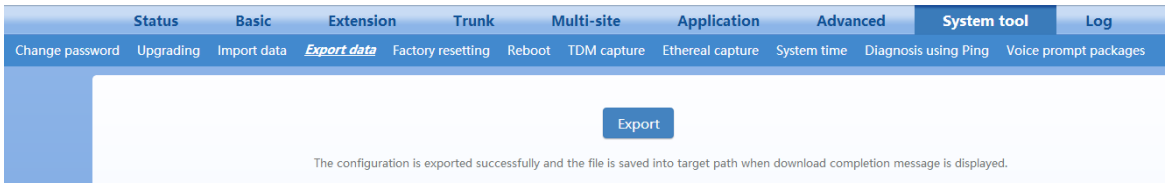
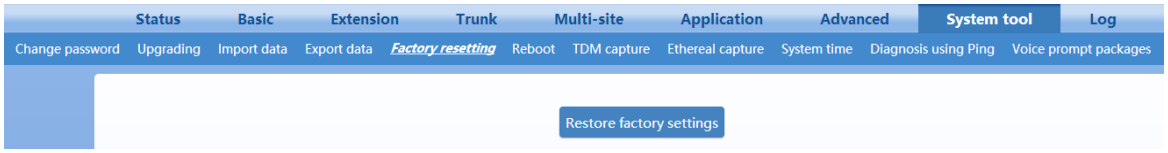


Figure 2-85 Restore factory settings interface



Note

- Don't operate the device during this period. When the configuration is imported successfully, the device will restart automatically.
- The speed at which configuration files are imported or exported is affected by the network. Please be patient.

2.10.3 Rebooting

To restart the device on the Web interface, go to **System tool** > **Reboot**.

Figure 2-86 Rebooting interface

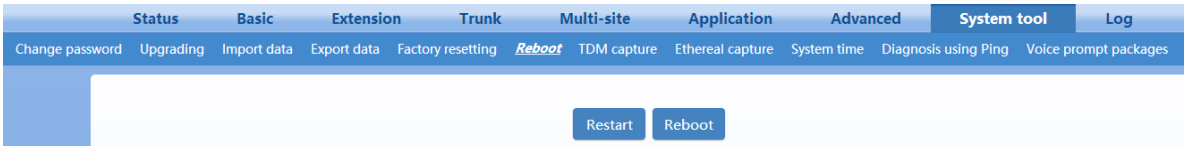


Table 2-46 System-reboot interface

Item	Description
Restart	Restart software.
Reboot	Reboot system (both hardware and software) takes longer time than a software restart. Note: Generally, it's sufficient to only restart software when the device requires a reset; the system reboot will be required only when network settings of the device are changed. A system reboot is not required when the OM20/50 IP address is changed.

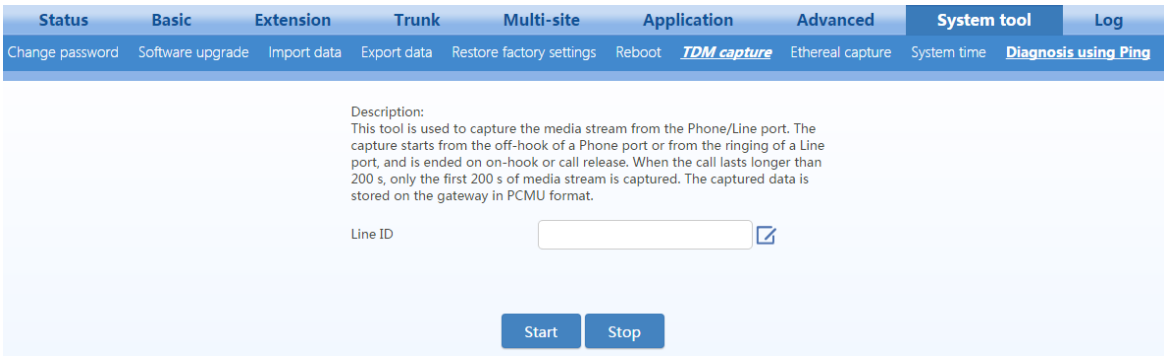
2.10.4 Port Capture

This feature is used for troubleshooting media-related issues, such as CID detection failure or busy tone detection failure .Port capture records the media stream from the analog line. The capturing starts from the off-hook of a phone interface or from the ringing of a line interface, and it is ended upon on-hook. Only the first 200 seconds of a media stream is captured and data captured afterwards will be discarded. The captured data will be saved on OM as PCMU format file.

Step 1 Go to **System tool** > **TDM capture**, select the desired port, and then click **OK**.

To ensure the capture of an entire call, it must be completed in 200 seconds.

Figure 2-87 Port-capture interface



Step 2 Click **Start** to initiate the capture procedure.

Step 3 Make the test call (Outbound call for FXS port, inbound call for FXO port).

Step 4 Click **Stop** to finish the capture procedure. A download-request window will pop up to allow you to download the captured data to your PC.

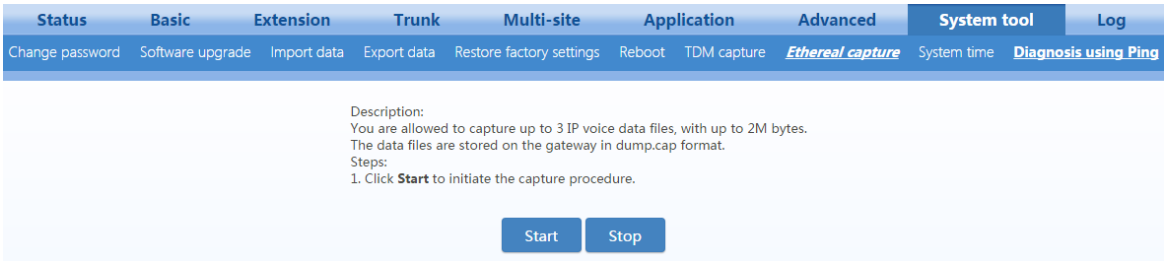
Send the captured file or related issue description to gs@newrocktech.com. Our technicians will help you to analyze and solve the issue.

2.10.5 Ethereal Capture

This feature is used for troubleshooting IP-packet-related issues, such as one-way voice, noise or echo. Up to three files each with max. 2MB in size can be captured. Files will be saved as dump.cap in OM and click STOP to finish the capturing and download these files. The file will not be stored in OM after downloading.

Step 1 Go to **System** > **Ethereal capture**, and click Start.

Figure 2-88 Ethereal interface



Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Stop** to finish the capture procedure. A download request window will pop up to allow you to download the captured packets to your PC.

Step 4 If you need help with problem analysis, you can send the captured file to gs@newrocktech.com. You can open the file by using Wireshark.

2.10.6 Log Management

Log files contain the status change information of the device, which are helpful for troubleshooting and understanding the network conditions.

By default, the OM20/50 stores log files in the internal storage device (by default, there is 3GB space is used to store log file, the log storage space can be changed on the **Application** > **Storage** interface). The

OM80 stores log files on the RAM and backed up in the built-in SD card. The storage devices store only the latest log information.

To collect all logs, you need to use an external log server and configure the log server with the following procedure:

Step 1 Go to **Log** > **Log download**, select a log level, and configure the log server.

Figure 2-89 Log-management interface

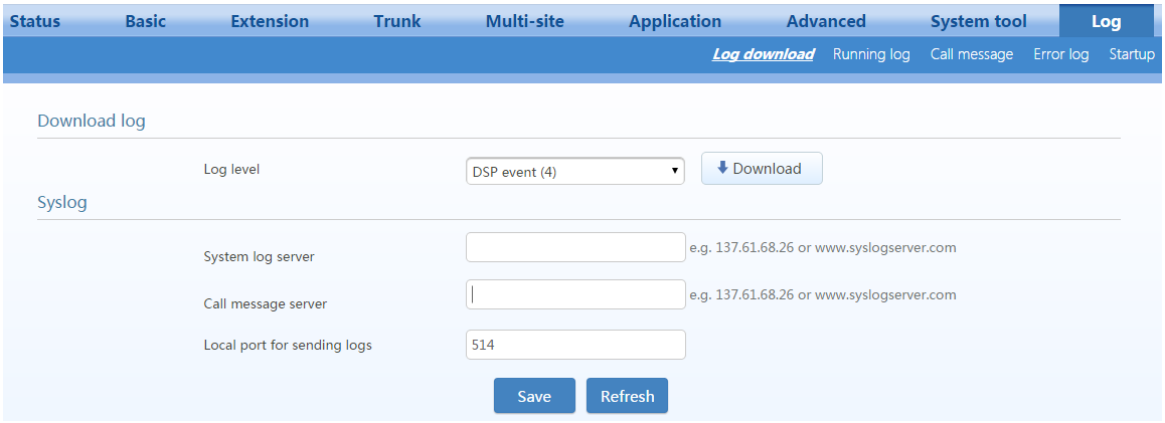


Table 2-47 Log-management parameters

Item	Description
Log level	By default, the log level is 4. Select a log level as required. Note: Whenever the device restarts, the default log level is restored.
System log server	• Enter the IP address or domain name of the log server (Syslog). If a port number is required, separate it from the IP address by using ":". For example: 192.168.1.100:518. • After this parameter is set, log files of the system will be sent to the log server instead of the local device.
Call Message server	• It is used for interworking with the Syslog server. Enter the IP address or domain name of the Syslog server. If a port number is required, separate it from the IP address with a ":". For example: 192.168.1.100:518. • After this parameter is set, call messages for the system will be sent to the log server instead of the local device.
Local port for sending logs	• Local port for sending log files. It is used for interworking with the Syslog server. The default value is 514. Generally, this value does not need to be changed.

Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Stop**. When the device instructs you to download the log file and select a path, select a folder for saving them.

Step 4 If you need help with problem analysis, you can send the captured file to gs@newrocktech.com.

2.10.7 Runtime log

The runtime log provides device's runtime status and events.

Go to **Log** > **Running log**, and then click **Refresh** to view the currently running information of the system.

Figure 2-90 Runtime log interface

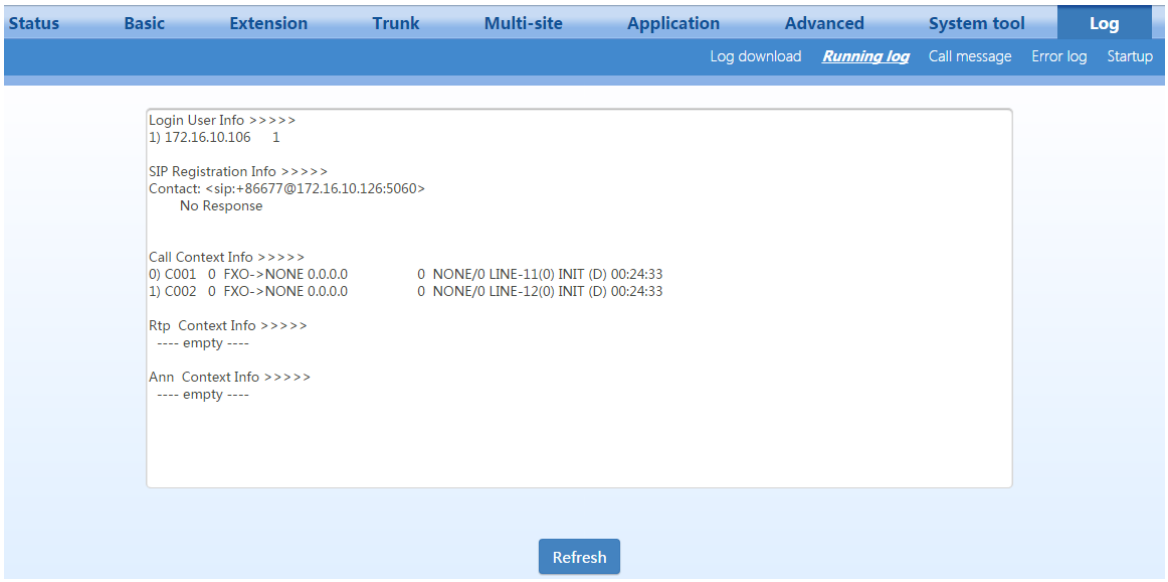


Table 2-48 Runtime log parameters

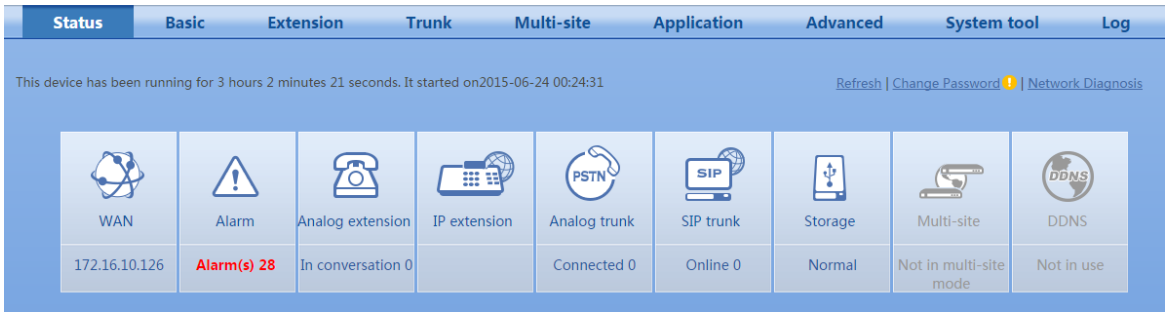
Item	Description
Login User Info	Displays the IP address that currently accesses the Web GUI and its operation privilege: • **1**: administrator • **2**: operator • **3**: Read only
SIP Registration Info	Displays registration information of the device. • **Not enabled:** The registration server's address is not entered yet. • **Latest response:** The latest response message for the registration. 200 means registered successfully. • **No response:** No response from the registration server. The IP network fails, or the registration server is unreachable.
Call Context Info	• Shows the call status.
RTP Context Info	• Shows the voice channel related to the calls.
Ann Context Info	• Displays IVR file resources.

2.11 View Runtime Information

2.11.1 Running Status

Open the **Status** interface. Device information such as network parameters, alarms, extension and trunk statuses, storage usage, tie trunk (for multi-site application), and the dynamic domain name is displayed.

Figure 2-91 Running status interface



2.11.2 Alarm

After opening the **Status** interface, move the mouse pointer to the **Alarm** icon to view alarm messages of the device.

In terms of severity level, the alarm messages are classified respectively into security alerts, orange alarms, and red alarms.

Figure 2-92 Alarm interface

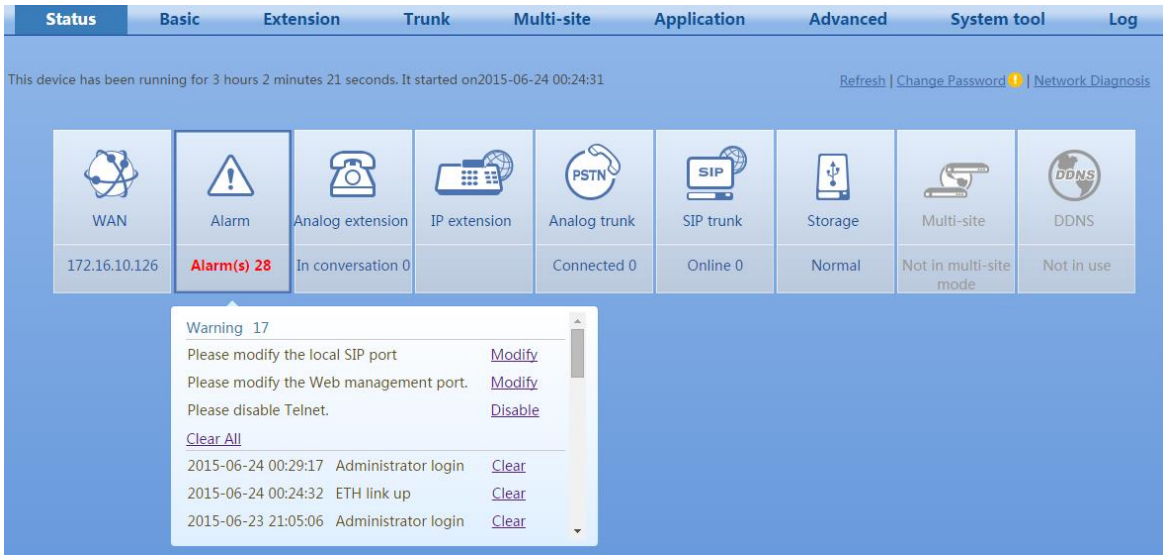


Table 2-49 Classification of alarm messages

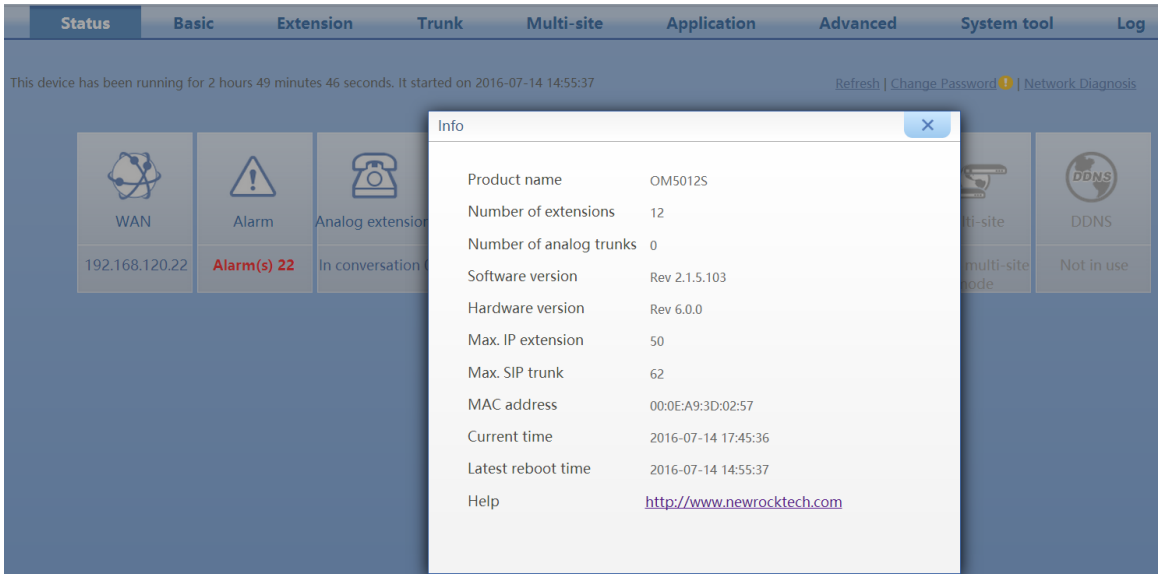
Type	Description
Security alerts	Registration of IP trunk succeeded.
	Please modify the local SIP port.
	The WAN is connected.
	The operator has logged on.
	The administrator has logged on.
	The IP address has changed.
	The FXO port is connected.
	The FXO port is not connected.
Orange alarms	The administrator password was changed.

Type	Description
	A logon password was incorrect.
	The operator password was changed.
Red alarms	The device restarts.
	Software reboot
	Registration of IP trunk failed.
	An IP extension registration failed.
	A DNS resolution failed.
	The network port connection is malfunctioning.
	SIP attack has or is occurring.

2.11.3 Product Information

Click **Info** in the right upper part to view information such as device model, version, number of extensions, and MAC address.

Figure 2-93 Product information interface

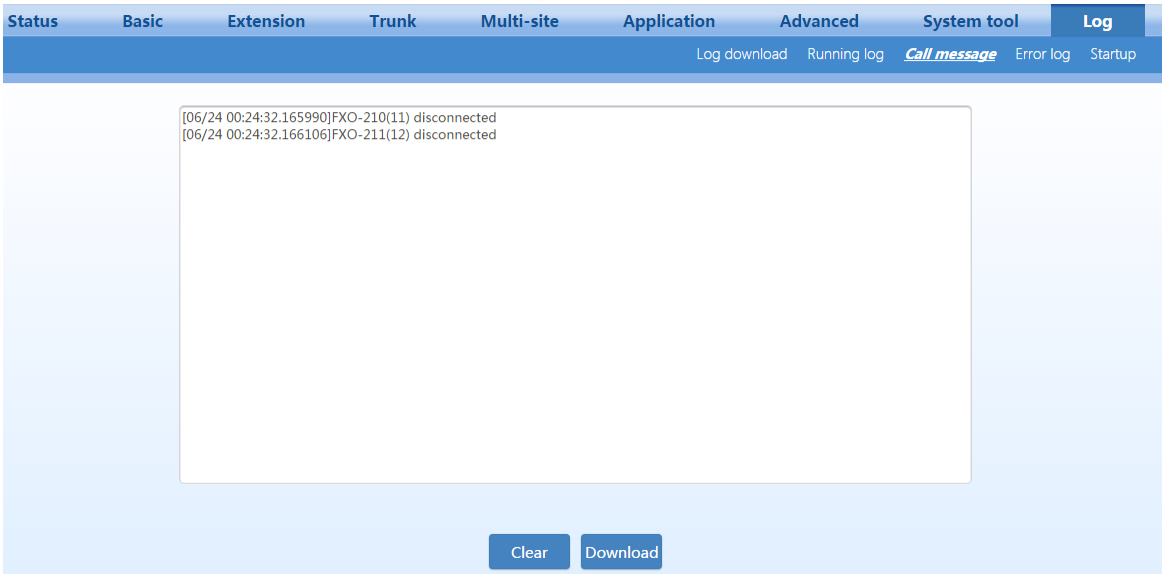


2.11.4 Call Messages

You can use call messages to locate a call problem.

Step 1 Go to **Log** >**Call message**, and click **Clear** to delete the current call messages.

Figure 2-94 Call message interface



Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Download** to save the call message file.

Step 4 Send the captured file to gs@newrocktech.com to get help with problem analysis.

2.12 Auxiliary Applications

The table below lists the applications that work with the OM. To use NeeHau Business Phone Assistant and DockPMS, ensure that device APIs are enabled. For details, see 2.8.13 API.

Table 2-50 List of applications

Item	Description
NeeHau Business Phone Assistant	Provides functions, such as screen pop-up, click to dial, call history, call recording, notes, and alarm clock reminders.
WeWei Softphone App	A smart-phone application running on Android/iOS. It delivers reliable business-telephone communication by combining the SIP extension feature with the legacy DISA (Direct Inward System Access) feature. As a mobile extension, WeWei allows users to communicate with customers and colleagues over either the Internet or PSTN, taking advantage of the accessibility and the reliability of both networks.
DockPMS	Use DockPMS, the OM can work with a hotel management system to provide functions such as guest call history, wake-up call, and controlling privilege of outbound call.
Zibo accounting software	Provides functions such as call accounting, toll settings, real-time call details record queries, and report printing.

3 FAQs

3.1 Incoming Call Number is Not Displayed

Symptom: For an incoming call from the analog trunk (FXO), the Line port number instead of the calling number is displayed on the phone.

Solution:

1. **Check the line**

   Connect the phone to the telephone line directly to check whether the Calling Number Identification Presentation (CLIP) function is enabled on the line by the provider. If the phone does not show the correct calling number, contact the provider. If the correct calling number is displayed, check whether the calling number is displayed before the first ring or displayed after one or two rings.

2. **Check the device configuration**

   Go to the **System** > **Analog trunk** page to check whether the CLIP function is enabled and whether the value of Call ID detection mode (before ringing or after ringing) matches the line.

3.2 IP Trunk Registration Fails

Symptom: When an outbound call is made with the IP trunk, there is a dial tone, but the call cannot be connected.

Solution:

Go to the **Logs** > **System Status** page to check the IP trunk registration status. See the table below for details.

Table 3-1 Solutions to IP trunk registration failures

Displayed Content	Registration Status	Solution
SIP Registration Info >>>>> Contact:<sip:61208000@192.168.250.5:5060> response: **200**	Registration is successful.	Check the network configuration and wiring, and analyze call SIP signaling.

Displayed Content	Registration Status	Solution
SIP Registration Info >>>>> Contact: <sip:61208000@192.168.250.5:5060> **No Response**	There is no response to the registration request.	Contact the VoIP service provider to confirm whether the address of the IP trunk registration server is correct, and test whether the network communications from the device to the registration platform are normal.
SIP Registration Info >>>>> Contact: <sip:61202000@192.168.250.5:5060> response:**404**	IP trunk registration number is incorrect.	Contact the VoIP service provider to confirm whether the IP trunk registration number is correct.
SIP Registration Info >>>>> Contact: <sip:61208000@192.168.250.5:5060> response: **403**	Registration password is incorrect.	Contact the VoIP service provider to confirm whether the IP trunk registration password is correct.

3.3 IP Network Connection Fails

Symptom: Unable to log on to the web administrator's interface.

Solution:

1. Connect your phone to the FXS port on the device, pick up the phone, and press ## to listen and check whether the network parameters of the device are correct.
2. Check the LAN where the device is located.
3. Check the connection between the LAN and the device.

3.4 Analog Extension Does Not Ring

Symptom: The analog extension does not ring for an incoming call.

Solution:

1. Replace the phone to determine whether the ringing function of the original phone is normal.
2. Go to **Extension** > **Analog** > **Advanced**, change Caller ID transmission mode, and dial the extension until the caller ID display modes supported by the device and the phone are the same and the ringing function becomes normal.
3. Go to **Extension** > **Analog** > **Advanced**, and change the ring frequency to different values to test whether the extension rings. Recommended test values include 15, 20, 30, 40, and 50.

3.5 Incorrect Date is Displayed on the Phone

Symptom: The date and time displayed with the calling number on the phone is inconsistent with those

on the device.

Solution:

1. Check whether time information can be obtained from a time server on the Internet.
2. If the device cannot access the time server on the Internet, select a PC in the LAN to serve as the time server. If the operating system is Windows Vista, Windows 7, or Windows server 2008, manually start the Windows time service.
3. Check whether the firewall of the Windows operating system is enabled on the PC. If the firewall is enabled, perform the following steps to enable the port through which the device accesses the time server on the firewall.
   a) Open the firewall window, and choose **Exceptions** > **Add Port**.
   b) Add port 1 Name the port ntp-tcp, specify the port number as 123, and select the TCP mode.
   c) Add port 2 Name the port ntp-udp, specify the port number as 123, and select the UDP mode.
   d) Go to the **Control Panel** > **Administrative Tools** > **Services page**, and confirm that the Windows time service has been enabled.
4. Call extension B from any extension A. Extension B shows the same time information as that on the device.

3.6 Low Volume on an Extension

Symptom: The other party's voice is too low on a call.

Solution:

Table 3-2 Solutions to low voice volume on an extension

Extension Type	Solution
Volume is too low on an analog extension	Go to **Extension** > **Analog** > **Advanced**, and increase the value of **Gain to terminal**.
Volume is too low on an IP extension called by an analog extension	Go to **Extension** > **Analog** > **Advanced**, and increase the value of Gain to **IP**.

3.7 Crosstalk on an Analog Extension

Symptom: Conversation on another extension is heard during a call.

Solution:

Generally, crosstalk is caused by telephone line short-circuits. Check the connection line of the FXS port and remove the line fault.

3.8 Can I Press the R Key on an Analog Extension?

Pressing the R key after off-hook is equivalent to hook-flash. However, because R keys on different phones may follow different design specifications, pressing the R key on an extension is not always reliable. It is recommended that you press ** for functions such as three-way calling, call transfer, and call parking.

3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?

The OM provides the embedded white-listed address of 192.168.2.100 upon factory delivery. When the Whitelist function is enabled, if you forget the whitelisted IP address previously set, the following steps can be performed for recovery.

Step 1 Connect a PC directly to the OM through a network cable.

Step 2 Press *90 to set the IP address of the OM to one that is located in the same network segment as the embedded white-listed address, such as 192.168.2.101. To do so, continuously dial *90192*168*2*101#255*255*255*0#192*168*2*1#0# after off-hook, and then hook on after hearing the successful service registration announcement.

Step 3 Restart the OM.

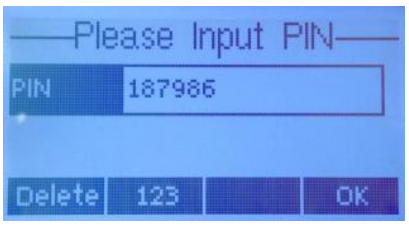
Step 4 Set the IP address of the PC to 192.168.2.100.

Step 5 Enter the new IP address of the OM on the Internet Explorer or the Telnet client of the PC to access the OM.

Appendix: Registering a SIP Terminal to OM

SIP Phone

- If a New Rock NRP phone is used, it can be registered with the device as follows: Connect the phone to the network where the device is located, and enter the corresponding PIN of the IP extension on the device.



- For a phone that is not a New Rock NRP phone, registration information must be entered. The following describes the registration information using the NRP1000 as an example.

Step 1 Open the Web management interface of the IP phone, click **VOIP** > **SIP**, select the desired SIP line, and then enter the registration information in **Basic setting**.

Figure 3-1 SIP Phone registration interface

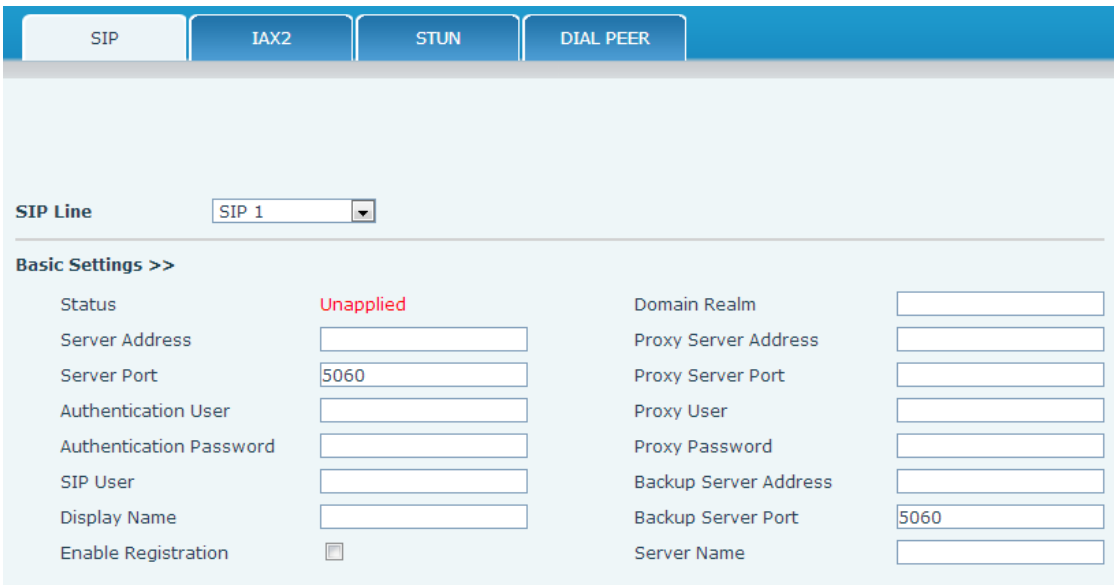


Table 3-3 SIP Phone registration parameters

Item	Description
Server Address	Enter the IP address or dynamic domain name of the OM. When the extension needs to register with the OM from an external network, the external access address of the device needs to be entered. Go to **Basic** > **Remote access** to view the IP address of the device.

Item	Description
Server port	Enter the SIP listening port of the OM. The default port is 5060. **Note:** By default, the SIP listening port of the device and the SIP trunk share a port, that is, port 5060. You can set a different registration port on the **Extension** > **IP**> **Registrar OPTIONS**.
Authentication User	Enter the number of the IP extension that is set in the OM. For example: 208.
Authentication Password	Enter the password corresponding to the number of the extension. For example: the password corresponding to the number 208 is 187986.
SIP user	Enter the number of the IP extension that is set on the OM. For example: 208.
Display name	The name to be displayed on the other party's phone. The name of the extension user can be set. If it is not set, the **Authentication User** will be displayed on the other party's phone. For example: 208.

Step 2 Select **Enable registration**, and click **Apply**.

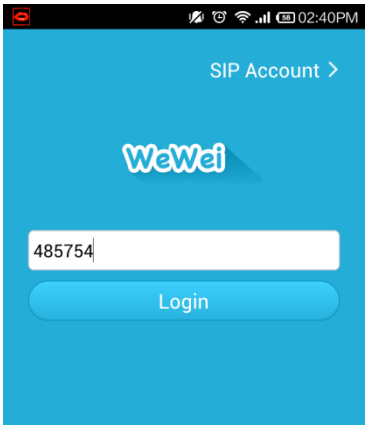
Step 3 On the web interface of the OM, go to **Extension** > **IP** to view the registration status of the IP extension.

Note

For an IP phone, it is recommended that G.729 codec standard be selected, and that the DTMF processing mode be the same as that on the device.

Softphone

- If the New Rock WeWei softphone is used, it can be registered with the device as follows: Connect the phone to the network where the device is located, and enter the corresponding PIN of the IP extension on the softphone.



- If another softphone is used, registration information must be entered. The following describes the specific registration information using the X-Lite as an example.

Step 1 Register X-Lite: Enter the SIP configuration page. Click the button “Add” which pops up the interface for Properties of Account.

Figure 3-2 X-Lite login interface

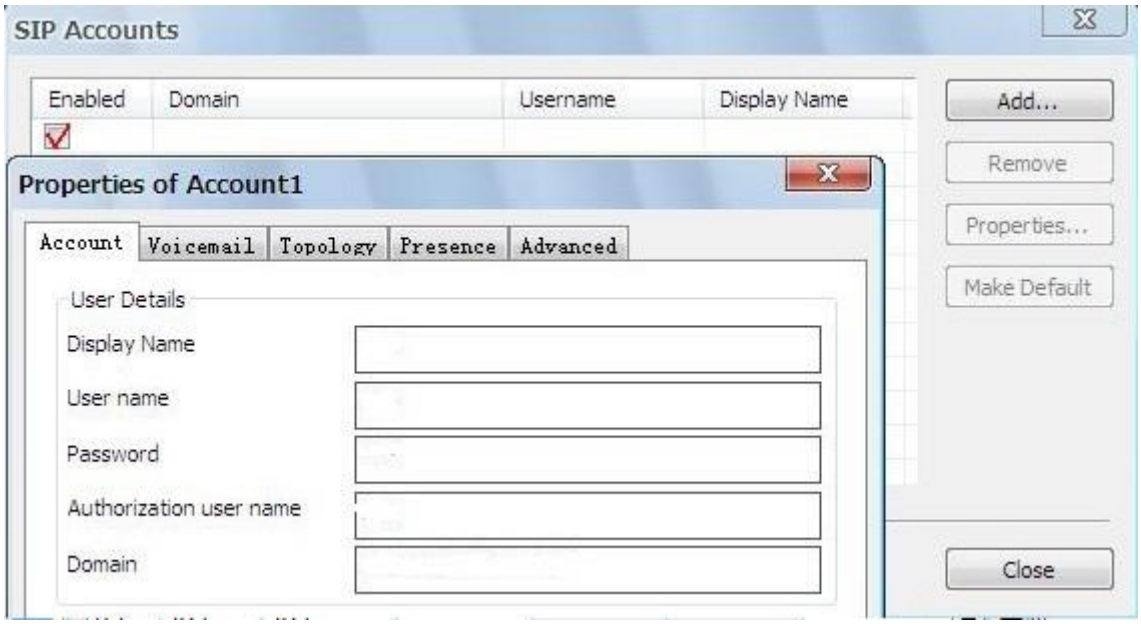


Figure 3-3 X-Lite registration interface

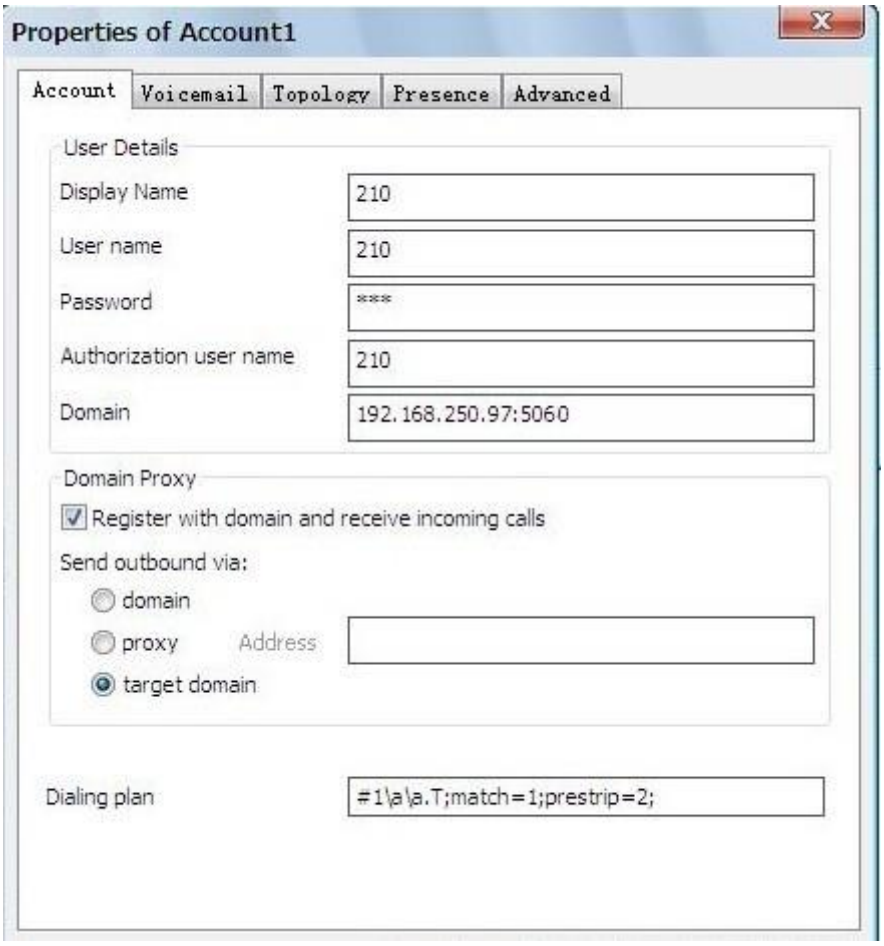


Table 3-4 SIP Phone registration parameters

Item	Description
Display name	The name to be displayed on the other party's phone. The name of the extension user can be set. If it is not set, the **User Name** will be displayed on the other party's phone. For example: 208.
User name	Enter the number of the IP extension that is set on the OM. For example: 208.
Password	Enter the password corresponding to the number of the extension. For example: the password corresponding to the number 208 is 187986.
Authorization user name	Enter the number of the IP extension that is set on the OM. For example: 208.
Domain	Enter the IP address or dynamic domain name of the OM. When the extension needs to register with the OM from an external network, the external access address of the device needs to be entered. Go to **Basic** > **Remote access** to view the IP address of the device.