



New Rock Technologies, Inc.

OM Series IP Telephony System

Administrator Manual

OM20

OM50

<http://www.newrocktech.com>

Document Version: 201511



Amendment Records

Document Rev. 01 (December 26, 2015)

Copyright © 2016 New Rock Technologies, Inc. All Rights Reserved.

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

Manual Description

This manual is applicable to OM20/OM50 Internet-based office telephony systems (“OM” for short) Rev 2.1.5.91.

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](#).

Table of Contents

Amendment Records	2
Manual Description	3
Contents	4
Contents of Figure	7
Contents of Table	Error! Bookmark not defined.
1 Overview	2-1
1.1 Introduction	2-1
1.1.1 Model.....	2-1
1.1.2 Appearance	2-2
1.2 Accessing the Device.....	2-3
1.2.1 Connection	2-3
1.2.2 Log in to the Web GUI	2-4
1.3 Web GUI overview	2-6
1.4 Network Configuration	2-1
1.4.1 Network Settings	2-1
1.4.2 DNS.....	2-1
1.4.3 STUN.....	2-2
1.4.4 Remote Access	2-3
2 Features	3-6
2.1 Auto Attendant	3-6
2.1.1 Auto Attendant.....	3-6
2.1.2 Greetings	3-6
2.1.3 Operators/Receptionists	3-10
2.2 Trunk.....	3-12
2.2.1 Analog trunks.....	3-12
2.2.2 IP Trunk.....	3-14
2.2.3 Backup SIP Proxy Server Settings	3-19
2.2.4 IMS	3-20
2.3 Settings of Extensions	3-21
2.3.1 Analog extensions	3-21
2.3.2 IP Extensions.....	3-23
2.3.3 IP Trusted Authentication	3-24
2.4 Extension Features	3-25
2.4.1 Basic Functions	3-25
2.4.2 Making Outbound Calls	3-29
2.4.3 IP table	3-30
2.4.4 Hunting Group	3-31
2.4.5 Extension Status Subscription	3-32
2.4.6 Group Call Pickup.....	3-36

2.4.7 Call Pickup.....	3-36
2.4.8 Three-way Calling.....	3-37
2.4.9 Call Parking	3-37
2.4.10 DID	3-37
2.4.11 Feature Access Codes	3-37
2.5 Recording and Voicemail.....	3-38
2.5.1 Recording	3-38
2.5.2 Voicemail.....	3-42
2.6 FoIP	3-44
2.7 Multi-site	3-45
2.7.1 Assign the extension numbers on each site in a uniform way	3-45
2.7.2 Assign the extension numbers on each site individually.....	3-48
2.8 System Settings.....	3-54
2.8.1 Built-in Storage Management	3-54
2.8.2 CRBT.....	3-54
2.8.3 Music on Hold.....	3-55
2.8.4 Time.....	3-56
2.8.5 Encryption.....	3-57
2.8.6 Routing Table	3-58
2.8.7 Dialed Number Detection and Digit Map.....	3-60
2.8.8 Call Progress Tone	3-61
2.8.9 SIP Advanced Configuration.....	3-62
2.8.10 DTMF.....	3-63
2.8.11 Media.....	3-64
2.8.12 Call Detail Record.....	3-65
2.8.13 API.....	3-66
2.8.14 SIP Transmission Mode.....	3-67
2.8.15 Auto Provision	3-67
2.8.16 TR069.....	3-68
2.8.17 Ping Diagnosis.....	3-70
2.9 Security management	3-70
2.9.1 Whitelist.....	3-70
2.9.2 Outbound Call Screening.....	3-71
2.9.3 Change Password	3-72
2.9.4 Telnet & SSH.....	3-72
2.9.5 Ping	3-73
2.9.6 Web Management	3-73
2.9.7 Voice Security.....	3-74
2.10 Maintenance	3-75
2.10.1 Software Upgrading.....	3-75
2.10.2 Configuration Maintenance.....	3-76
2.10.3 Rebooting	3-76
2.10.4 Port Capture	3-77
2.10.5 Ethereal Capturing.....	3-78
2.10.6 Log Management.....	3-78
2.10.7 Runtime log	3-79
2.11 View Runtime Information.....	3-80
2.11.1 Running Status	3-80
2.11.2 Alarm	3-80

2.11.3 Product Information	3-81
2.11.4 Call Messages	3-82
2.12 Auxiliary Applications	3-83
3 FAQs	4-1
3.1 Incoming Call Number is Not Displayed.....	4-1
3.2 IP Trunk Registration Fails.....	4-1
3.3 IP Network Connection Fails.....	4-2
3.4 Analog Extension Does Not Ring.....	4-2
3.5 Incorrect Date is Displayed on the Phone.....	4-2
3.6 Low Volume on an Extension.....	4-3
3.7 Crosstalk on an Analog Extension	4-3
3.8 Can I Press the R Key on an Analog Extension?.....	4-4
3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?	4-4
Appendix: Registering a SIP Terminal to OM	4-1
SIP Phone.....	4-1
Softphone	4-2

Table of Figures

Figure 1-1 OM20 front panel.....	2-2
Figure 1-2 OM20 back panel	2-2
Figure 1-3 OM50 front panel.....	2-2
Figure 1-4 OM50 back panel	2-2
Figure 1-5 Diagram for proper connection	2-3
Figure 1-6 Login interface	2-5
Figure 1-7 Web GUI layout	2-6
Figure 1-8 Network setting interface	2-1
Figure 1-9 DNS server setting interface.....	2-2
Figure 1-10 STUN setting interface.....	2-3
Figure 1-11 Remote access setting interface.....	2-4
Figure 1-12 Port mapping setting interface	2-4
Figure 2-1 Auto attendant setting interface	3-6
Figure 2-2 Interface to selecting greeting files	3-7
Figure 2-3 Interface to select greeting files for trunk.....	3-7
Figure 2-4 Text-to-greeting conversion interface 1	3-8
Figure 2-5 Text-to-greeting conversion interface 2	3-9
Figure 2-6 IVR interface.....	3-9
Figure 2-7 Interface to upload greetings	3-10
Figure 2-8 Auto attendant setting interface	3-11
Figure 2-9 Analog trunk setting interface	3-12
Figure 2-10 Analog trunk advanced setting interface.....	3-13
Figure 2-11 IP trunk setting interface.....	3-15
Figure 2-12 IP trunk setting interface.....	3-17
Figure 2-13 IP trunk registration interface.....	3-18
Figure 2-14 Secondary SIP proxy server interface	3-19
Figure 2-15 IMS setting interface.....	3-20
Figure 2-16 Analog extension setting interface.....	3-21
Figure 2-17 Analog extension advance setting interface	3-23
Figure 2-18 IP extension setting interface.....	3-24
Figure 2-19 IP authentication setting interface.....	3-25
Figure 2-20 Interface of extension features	3-26
Figure 2-21 Outbound dialing rule interface.....	3-29
Figure 2-22 IP table setting interface	3-31
Figure 2-23 Hunting group setting interface.....	3-32
Figure 2-24 Extension status subscription interface.....	3-33
Figure 2-25 Figure 2-25 Selecting an extension model.....	3-34
Figure 2-26 Selecting extensions for subscription	3-35
Figure 2-27 Extension status subscription interface.....	3-35
Figure 2-28 Group setting interface	3-36
Figure 2-29 Group Interface.....	3-36
Figure 2-30 DID setting interface	3-37
Figure 2-31 Feature access codes interface.....	3-38

Figure 2-32 Remote recording setting interface	3-39
Figure 2-33 Extension recording setting interface.....	3-39
Figure 2-34 USB recording setting interface	3-40
Figure 2-35 Extension recording setting interface.....	3-41
Figure 2-36 Voicemail setting interface.....	3-42
Figure 2-37 FAX setting interface	3-44
Figure 2-38 Multi-site numbering scheme selection interface	3-46
Figure 2-39 Multi-site setting interface	3-46
Figure 2-40 Site adding interface	3-47
Figure 2-41 Domain name interface.....	3-48
Figure 2-42 Multi-site scenarios setting interface.....	3-49
Figure 2-43 Device multi-site role selection interface.....	3-49
Figure 2-44 Multi-site scenarios setting interface.....	3-49
Figure 2-45 Device list setting interface	3-50
Figure 2-46 Prefix setting interface	3-51
Figure 2-47 Trunk sharing setting interface	3-51
Figure 2-48 Domain name setting interface	3-52
Figure 2-49 Interface of multi-site scenarios 1	3-52
Figure 2-50 Interface for site roles	3-52
Figure 2-51 Managing site address interface.....	3-53
Figure 2-52 Multi-site networking status interface.....	3-53
Figure 2-53 Storage interface	3-54
Figure 2-54 CRBT file uploading setting interface	3-55
Figure 2-55 Music on hold setting interface	3-56
Figure 2-56 System time setting interface.....	3-56
Figure 2-57 Encryption interface.....	3-57
Figure 2-58 Dialing interface.....	3-60
Figure 2-59 Call progress tone setting interface	3-61
Figure 2-60 SIP related setting interface.....	3-62
Figure 2-61 DTMF interface.....	3-64
Figure 2-62 Media setting interface.....	3-65
Figure 2-63 CDR server setting interface.....	3-66
Figure 2-64 API setting interface.....	3-66
Figure 2-65 SIP transmission mode setting interface.....	3-67
Figure 2-66 Auto provision setting interface.....	3-68
Figure 2-67 TR069 setting interface.....	3-69
Figure 2-68 Ping diagnosis interface.....	3-70
Figure 2-69 Whitelist setting interface.....	3-71
Figure 2-70 Outbound call screening setting interface.....	3-72
Figure 2-71 Password changing interface.....	3-72
Figure 2-72 Telnet & SSH setting interface.....	3-73
Figure 2-73 Ping blocking/unblocking setting interface	3-73
Figure 2-74 Web management interface.....	3-74
Figure 2-75 Voice security setting interface	3-74
Figure 2-76 Software upgrade interface.....	3-75
Figure 2-77 Data importing interface.....	3-76
Figure 2-78 Data exporting interface.....	3-76
Figure 2-79 Restore Factory Settings interface	3-76

Figure 2-80 Rebooting interface	3-77
Figure 2-81 Port capturing interface.....	3-77
Figure 2-82 Ethereal capturing interface.....	3-78
Figure 2-83 Log management interface	3-78
Figure 2-84 Runtime Log Interface	3-79
Figure 2-85 Running status interface.....	3-80
Figure 2-86 Alarm interface	3-81
Figure 2-87 Product information interface.....	3-82
Figure 2-88 Call message interface	3-82
Figure 3-1 SIP Phone registration interface	4-1
Figure 3-2 X-Lite login interface.....	4-3
Figure 3-3 X-Lite registration interface.....	4-3

Table of Tables

Table 1-1 OM20 and OM50 product models	2-1
Table 1-2 Port description	2-3
Table 1-3 Login parameters	2-5
Table 1-4 Web management interface layout	2-6
Table 1-5 Network parameters	2-1
Table 1-6 DNS server parameters	2-2
Table 1-7 STUN setting parameters	2-3
Table 1-8 Remote access parameters	2-4
Table 1-9 Port mapping parameters	2-4
Table 2-1 Auto Attendant Setting Parameters	3-6
Table 2-2 Default greeting files	3-6
Table 2-3 Recording a greeting file by phone	3-9
Table 2-4 Auto attendant parameters	3-11
Table 2-5 Analog trunk parameters.....	3-12
Table 2-6 Analog trunk advanced setting parameters.....	3-13
Table 2-7 IP trunk registration parameters.....	3-15
Table 2-8 IP trunk parameters	3-17
Table 2-9 IP trunk registration parameters.....	3-18
Table 2-10 Secondary SIP proxy server parameters	3-19
Table 2-11 IMS setting parameters.....	3-21
Table 2-12 Analog extension parameters	3-21
Table 2-13 Analog extension advance setting parameters	3-23
Table 2-14 IP extension parameters	3-24
Table 2-15 Extension basic features.....	3-26
Table 2-16 Outbound dialing rule parameters.....	3-29
Table 2-17 IP table parameters	3-31
Table 2-18 Hunting group parameters	3-32
Table 2-19 Status of BLF indicators.....	3-33
Table 2-20 Managing recorded files.....	3-41
Table 2-21 Voice mailbox sending server parameters	3-43
Table 2-22 Managing message files	3-43
Table 2-23 FAX setting parameters	3-44
Table 2-24 Authentication policy parameters.....	3-46
Table 2-25 Configuring sites information	3-47
Table 2-26 Numbering scheme parameters.....	3-50
Table 2-27 Prefix setting parameters	3-51
Table 2-28 Trunk sharing setting parameters	3-51
Table 2-29 System time parameters	3-56
Table 2-30 Encryption parameters.....	3-57
Table 2-31 Description of a Digit map.....	3-60
Table 2-32 Call progress tone parameters.....	3-61
Table 2-33 Examples of Customized Tone	3-62
Table 2-34 SIP Related Configuration	3-63

Table 2-35 DTMF parameters.....	3-64
Table 2-36 Media parameters.....	3-65
Table 2-37 API setting parameters	3-66
Table 2-38 SIP transmission mode parameters.....	3-67
Table 2-39 Auto provision parameters.....	3-68
Table 2-40 TR069 parameters.....	3-69
Table 2-41 Whitelist parameters.....	3-71
Table 2-42 Web management parameters	3-74
Table 2-43 Voice security parameters	3-75
Table 2-44 System rebooting interface	3-77
Table 2-45 Log management parameters.....	3-79
Table 2-46 Running log parameters.....	3-80
Table 2-47 Classification of alarm messages	3-81
Table 2-48 List of Applications.....	3-83
Table 3-1 Solutions to IP trunk registration failures	4-1
Table 3-2 Solutions to low voice volume on an extension.....	4-3
Table 3-3 SIP Phone registration parameters.....	4-1
Table 3-4 SIP Phone registration parameters.....	4-4

2 Overview

2.1 Introduction

The OM20/OM50 series delivers a multi-functional officetelephony 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.

In combination with the New Rock WeWei softphone APP and NeeHau Business Phone Assistant, OM20/OM50 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.

2.1.1 Models

OM20/OM50 includes multiple models with varying amounts of FXO and FXS ports, as shown in Table 1-1.

Table 2-1 OM20 and OM50 product models

Model		Interface Card	Number of Interface Card	Number of FXO Ports	Number of FXS Ports
OM20	OM20-NA	NA	0	NA	NA
	OM20-4S	401A-4S	1	0	4
	OM20-4FXO	401A-4FXO	1	4	0
	OM20-2S/2	401A-4S	1	2	2
OM50	OM50-NA	NA	0	NA	NA
	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

Model	Interface Card	Number of Interface Card	Number of FXO Ports	Number of FXS Ports
	401A-4S	1		
OM50-8FXO	401A-4FXO	2	8	0

2.1.2 Appearance

Figure 2-1 OM20 front panel



Figure 2-2 OM20 back panel



Figure 2-3 OM50 front panel



Figure 2-4 OM50 back panel



Table 2-2 Port description

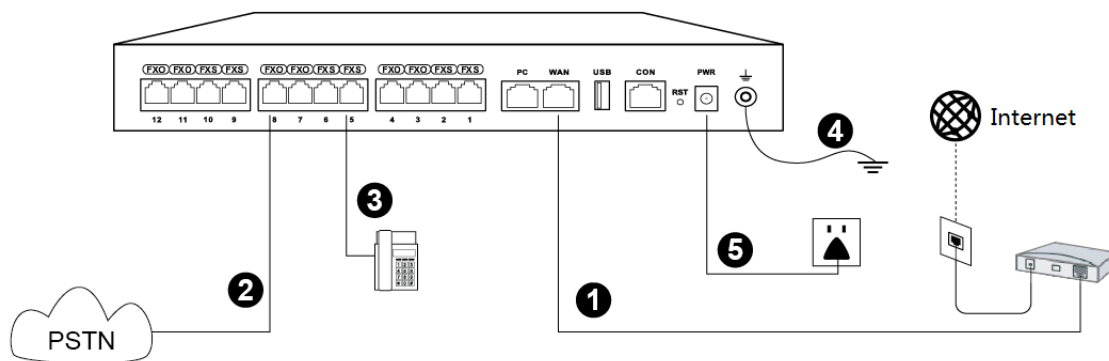
Ports	Description
FXS	The FXS ports are used for connecting analog phones, fax machines, or POS machines.
FXO	The FXO ports are used for connecting to the PSTN or another PBX.
PC	The PC port is used for connecting a PC or switch. Note: The OM will not assign the address automatically for these terminals. You must assign them to the same OM network/LAN segments.
WAN	The WAN port is used for Internet access.
USB	The USB port is used for connecting the USB device. Note: The device has 16 GB internal flash storage.
CON	The console port is used for local management and testing. Note: Generally, the console port is not used. If needed, use a serial line to connect it.
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.

2.2 Accessing the Device

2.2.1 Connection

Place the device on an even surface, or secure it in a rack, and then follow these steps to connect:

Figure 2-5 Diagram for proper connection



- Step 1** Connect the WAN port 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.
- 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.

2.2.2 Log in to the Web GUI

Step 1 Use a CAT5 cable to connect the device to the local network where the PC is connected, or connect the device directly to the PC.

Step 2 Obtain the IP address of the device. The default IP address is 192.168.2.218. 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#

The diagram shows the dial string 192*168*2*218#255*255*0*0#192*168*2*1#0# with three brackets underneath. The first bracket is under 192*168*2*218 and labeled 'IP address'. The second bracket is under 255*255*0*0 and labeled 'Subnet mask'. The third bracket is under 192*168*2*1 and labeled '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. 192.168.2.218);

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**.

Figure 2-6 Login interface



Table 2-3 Login parameters

Item	Description
Language	Select a language.
Role	<p>The Web utility provides two authority levels:</p> <ul style="list-style-type: none"> 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, “Welcome Operator” is displayed on the upper left side of the interface. <p>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.</p> <p>Note: The operation rights in the “Welcome user” mode are similar to those in the “Welcome operator” mode, where only certain pages can be browsed. 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.</p>
Password	<p>The default administrator password is admin.</p> <p>The default operator password is operator</p> <p>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.</p>

2.3 Web GUI overview

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

Figure 2-7 Web GUI layout

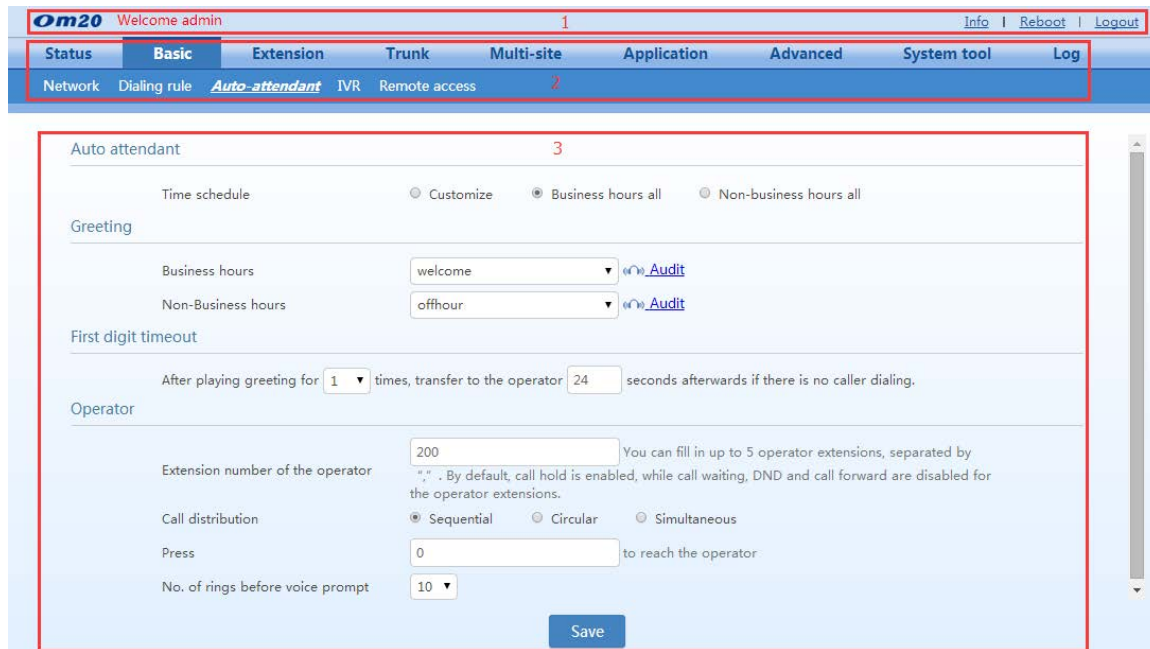


Table 2-4 Web management interface layout

Item	Description
1 System button area	Contains buttons such as Reboot, Logout, 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.

2.4 Network Configuration

2.4.1 Network Settings

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

Figure 2-8 Network setting interface



Table 2-5 Network parameters

Item	Description
Static IP address	The device uses a static IP address. This is the default setting. To obtain an IP address through DHCP, use a telephone connected to the FXS port and dial *90###1# . After you hear "The feature is now activated", restart the device.
Obtain an IP address automatically	Use the dynamic host configuration protocol (DHCP) to obtain IP addresses. To change the fixed IP address, use a telephone connected to the FXS port and dial *90+the fixed IP address+#subnet mask#IP address of the gateway#0# . The dots "." in the IP address need to be replaced with star keys "*".
PPPoE	Select PPPoE when an ADSL modem is connected to the device, and enter username and password obtained from the ISP.

2.4.2 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 2-9 DNS server setting interface



Table 2-6 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.
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.
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.

2.4.3 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.

(Note: New Rock maintains a stun server at stun.newrocktech.com.)

Figure 2-10 STUN interface

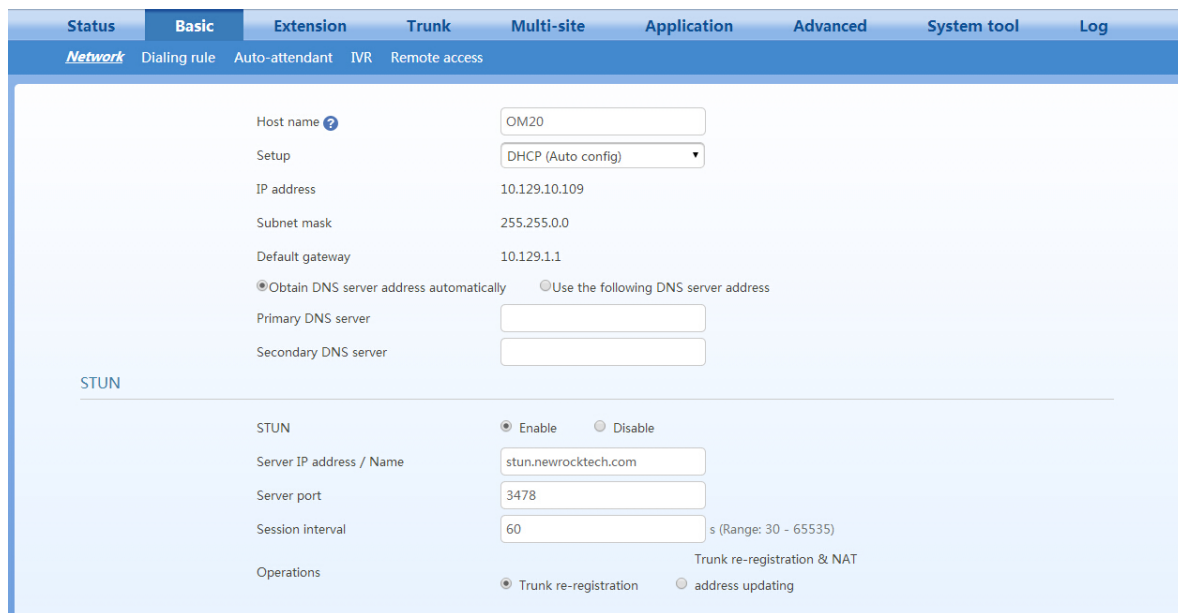


Table 2-7 STUN Configuration

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. It is disabled by default.
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	<ul style="list-style-type: none"> 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.

2.4.4 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 addressor if simple 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 2-11 Remote access configuration interface

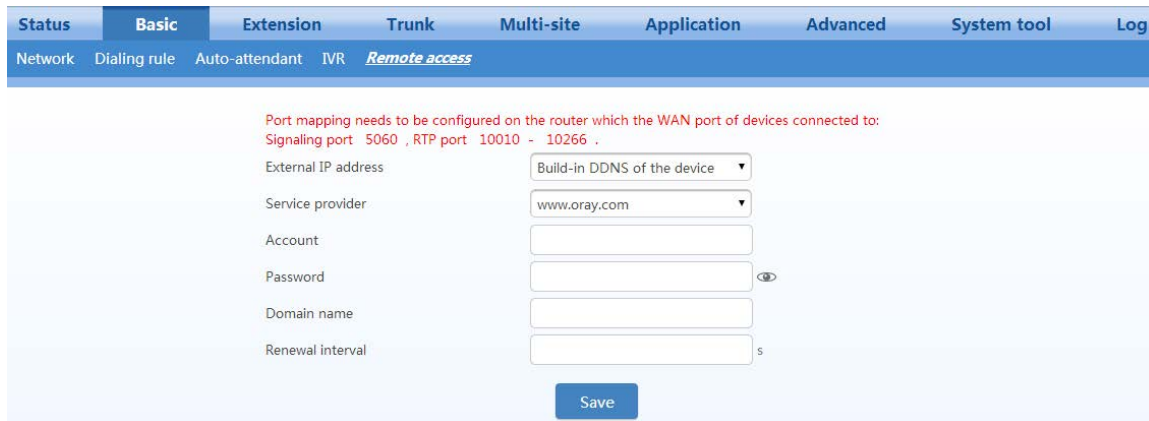


Table 2-8 Remote access parameters

Item	Description
OM-based DDNS	This option should be selected when the ingress router does not have a static IP address nor Dynamic DNS 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: Dyn dns.org, freedns.afraid.org, and www.no-ip.com.
Static 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 DDNS	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:

Figure 2-12 Port-mapping setting interface

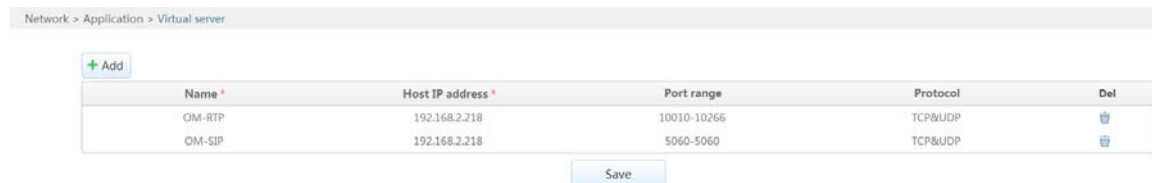


Table 2-9 Port mapping parameters

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.

Item	Description
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.

3 Features

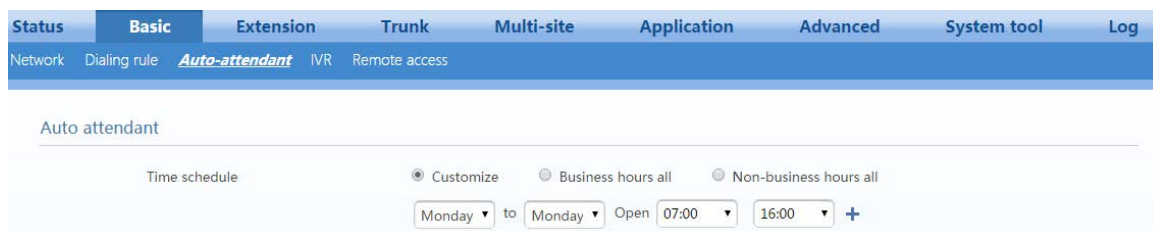
3.1 Auto Attendant

3.1.1 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 setting interface**.

Figure 3-1 Auto attendant setting interface



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

Table 3-1 Auto Attendant Setting 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.

3.1.2 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 3-2 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.

Type	File name	Content
Non-business hours	Off-hour	Thank you for calling. Our office is closed. If you know the extension, please dial it now.

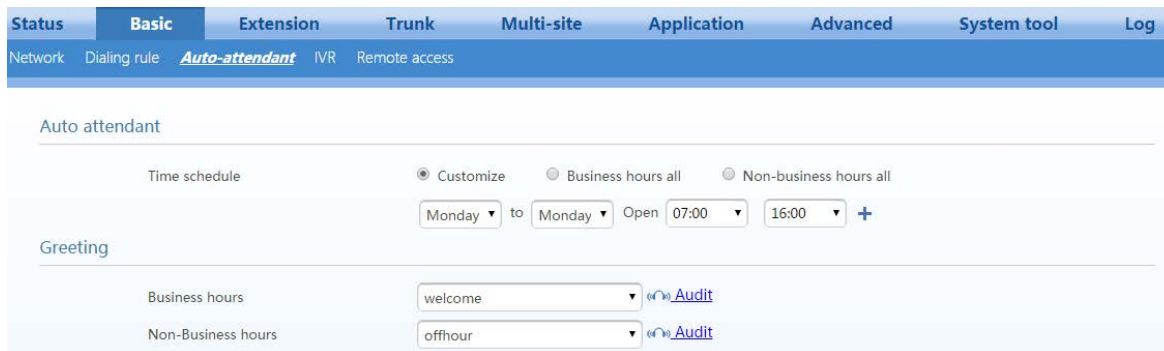
Configuring auto-attendant greetings

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 3-2 Interface to selecting greeting files



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

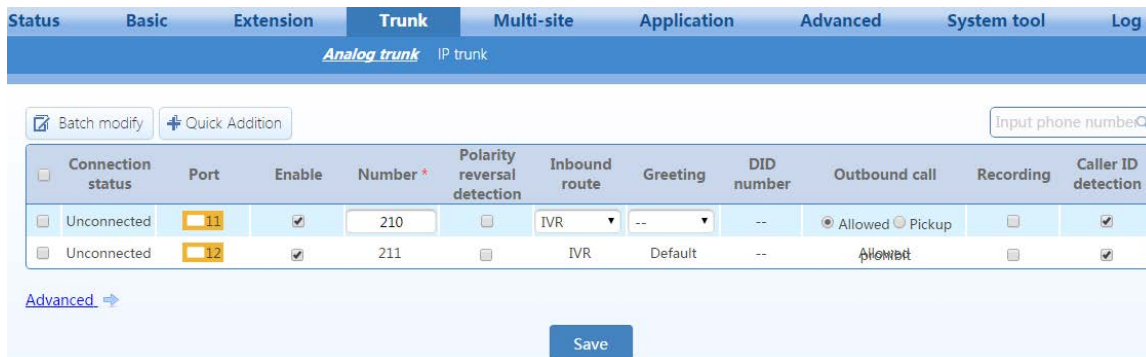
Configure greetings for each trunk

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

Step 1 Click **Trunk > Analog trunk / IP trunk** to select desired audio files.

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

Figure 3-3 Interface to select greeting files for trunk



Step 2 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

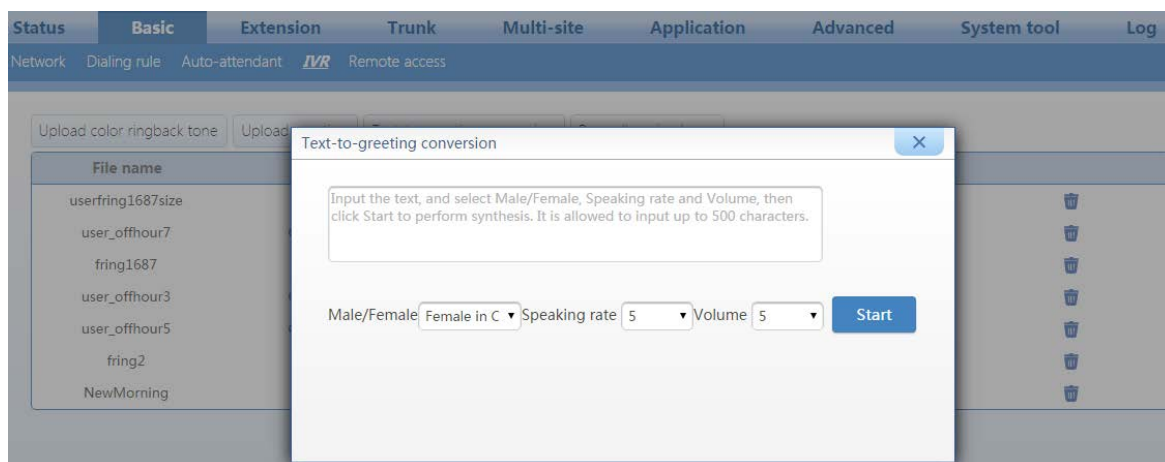
1) Text-to-greeting conversion

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 1.4.2 DNS.

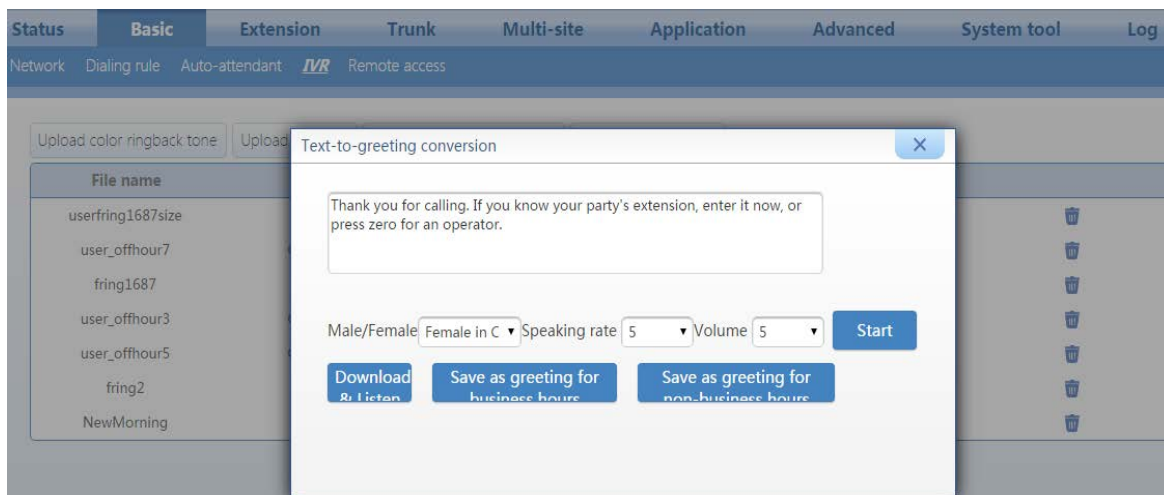
Step 2 Go to **Basic > IVR > Text-to-greeting conversion** page. Enter the greeting content in English and click **Start**.

Figure 3-4 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 3-5 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 3-6 IVR interface

File name	Type	Play	Music on hold	Audit
userfring1687size	CRBT		<input type="checkbox"/>	
user_offhour7	Greeting		<input type="checkbox"/>	
fring1687	CRBT		<input type="checkbox"/>	
user_offhour3	Greeting		<input type="checkbox"/>	
user_offhour5	Greeting		<input type="checkbox"/>	
fring2	CRBT		<input type="checkbox"/>	
NewMorning	CRBT		<input type="checkbox"/>	

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 3-3 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Press *8201 to listen to greetings; Press *8202 to listen to off-hours greetings.

Item	Description
Recovery	Press *8300 to recover a replaced voice greeting file.



Note

Never restart your device during recording.

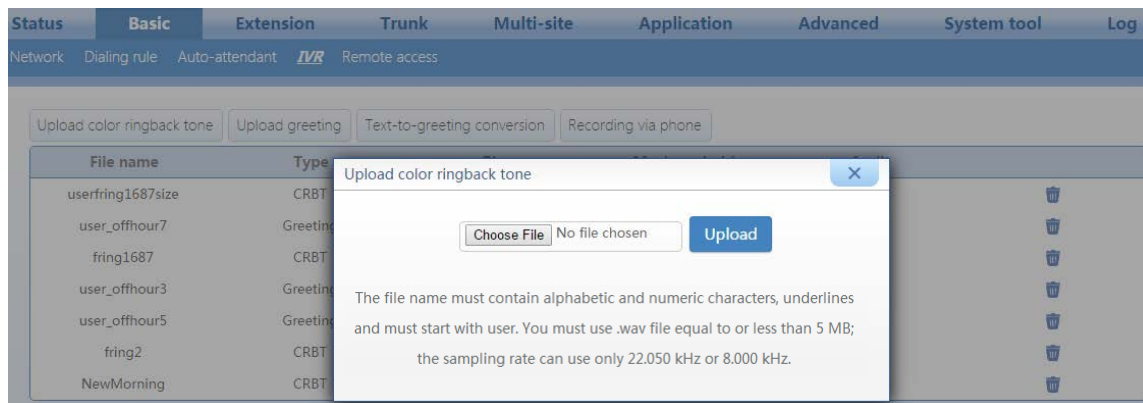
3) Upload greetings

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 3-7 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.

3.1.3 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 and OM50-8FXO), 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 3-8 Auto attendant setting interface

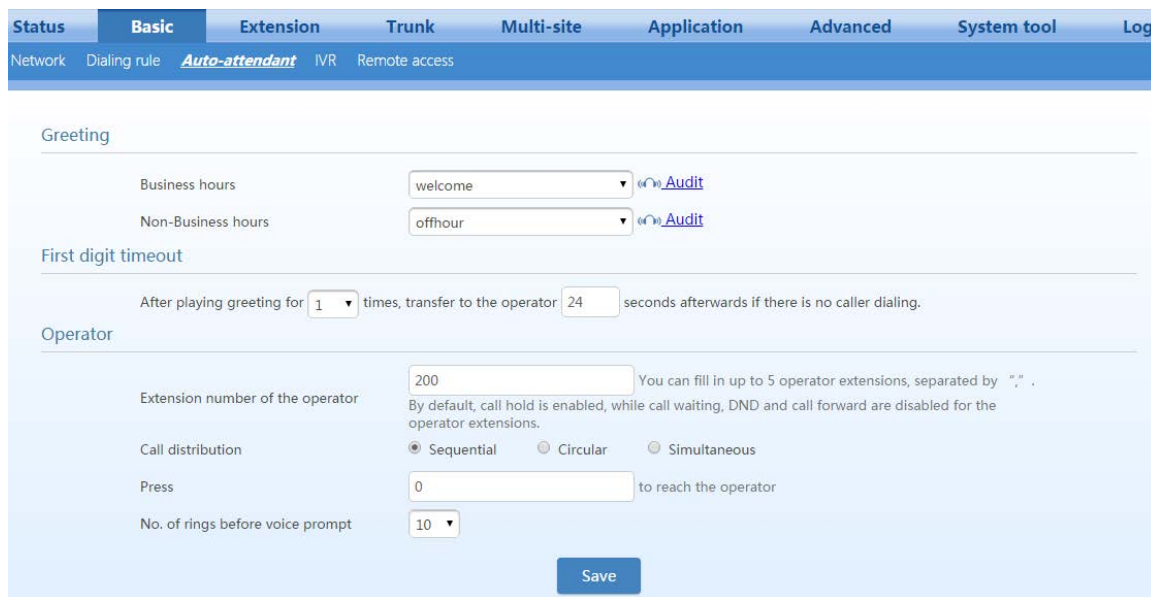


Table 3-4 Auto attendant parameters

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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ➢ 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”. ➢ Number of rings before voice prompt: The device will play prompts when the number of rings reaches the value set here. The default value is 5.

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

3.2 Trunk

3.2.1 Analog trunks

Follow this procedure:

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

Figure 3-9 Analog trunk setting interface



Table 3-5 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: <ul style="list-style-type: none"> • IVR: 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 (see 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 IVR , this must be configured.
DID number	Enter the number of extension or the hunt group that is bound to the trunk. Note: When the Inbound route is set to DID , this item must be configured.

Item	Description
Outbound call	<p>When the Inbound route is configured as IVR, there are two choices:</p> <ul style="list-style-type: none"> • Allowed: Allowed to make outbound calls; • Pickup prohibit: Not allowed to make outbound calls. <p>When the Inbound route is configured as DID, there are two choices:</p> <ul style="list-style-type: none"> • Share: Other extensions are allowed to make outbound calls. • DID only: Only the extension specified in the DID number is allowed to make outbound calls.
Recording	<p>Enable recording for the trunk.</p> <p>Note: To enable the trunk recording, you need to enable the recording function on the Application > Recording page first. For details, see 2.5.1 Recording.</p>
Caller ID detection	<p>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.</p> <p>Note: You must enable the caller ID delivery for the extension.</p>
Advanced	<p>Configure advanced properties of an analog trunk.</p>

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 3-10 Analog trunk advanced setting interface

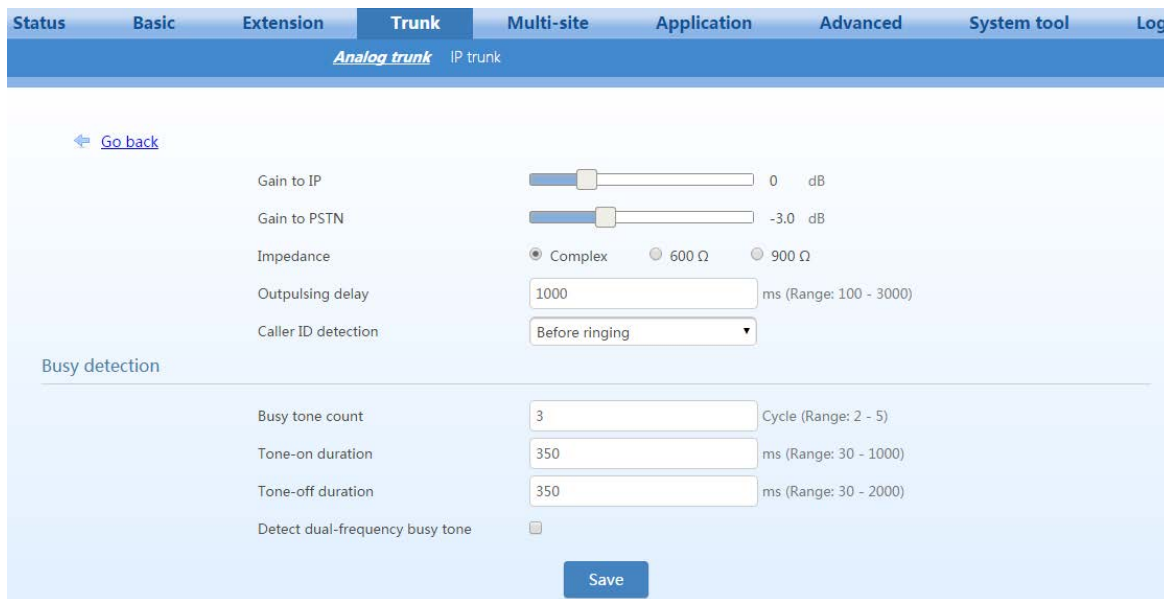


Table 3-6 Analog trunk advanced setting parameters

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 may be adjusted. Otherwise, accept the default value.

Item	Description
Outplusing 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. Note: This item needs to be configured only when the caller ID is not correctly displayed.
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 350-ms. For details, please see 2.8.8 Call Progress Tone.
Detect dual-frequency busy tone	To detect dual-frequency busy tones rather than using the on-off time of the busy tone.
Busy frequency	If Detect dual-frequency busy tones is enabled, you need to specify the frequency to be detected. Unit: Hz.

3.2.2 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, and select **IP trunk** or **Skype**.

Figure 3-11 IP trunk setting interface

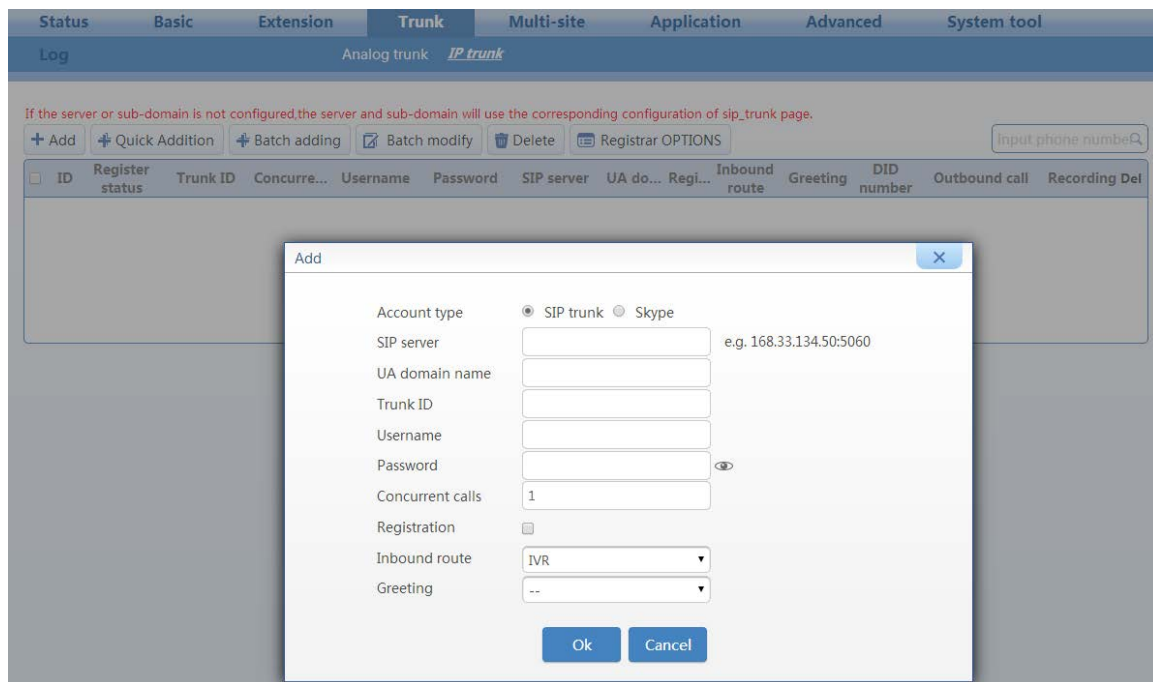




Table 3-7 IP-trunk registration parameters

Accoun	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.
	Trunk ID	Provided by your ITSP. (Also the assigned DID or extension number.)
	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. Click  to display the password in plaintext, and click it again to display the password as cipher text. Up to 30 characters is allowed.
	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: <ul style="list-style-type: none"> • IVR: 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 IVR , 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.	

Account	Item	Description
	Outbound call	<p>When the Inbound route is set to DID, you can configure whether this trunk line can be used for other extensions or bundled extension / hunt group to make outbound calls:</p> <ul style="list-style-type: none"> • 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	SIP User	<p>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.</p>
	Password	<p>Input the password of the SIP profile created in Skype Manager. The password is displayed as ciphertext. Click  to display the password in plain text.</p>
	Skype Connect address	<p>Generally, it is sip.skype.com. It should be identical to the Skype Connect address of the SIP profile created in Skype Manager.</p>
	UDP port	<p>It is 5060 by default. It should be identical to the UDP port of the SIP profile created in Skype Manager.</p>
	Registration	<p>Select this to enable registration.</p>
	Inbound route	<p>Select the destination for an external number calling into device through an inbound route:</p> <ul style="list-style-type: none"> • IVR: 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	<p>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 IVR, this item needs to be configured.</p>
	DID number	<p>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.</p>
	Outbound call	<p>When the Inbound route is set to DID, you can configure whether this trunk line can be used for other extensions or bundled extension / hunt group to make outbound calls:</p> <ul style="list-style-type: none"> • 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	<p>Skype number bound to the SIP account on the Skype website. For example: 13152880961.</p>

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

Figure 3-12 IP trunk configuration interface

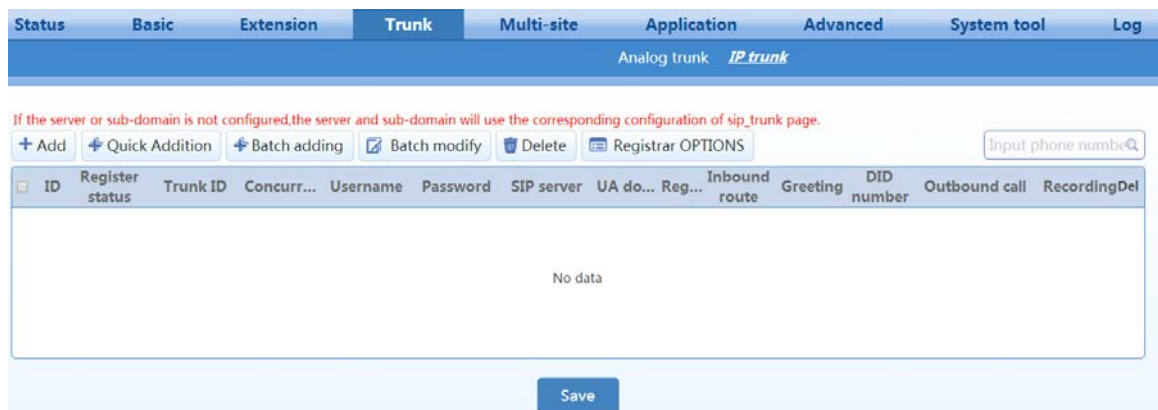


Table 3-8 IP trunk parameters

Item	Description
ID	Line number
Register status	<p>Indicate the status of registration:</p> <ul style="list-style-type: none"> • 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: If the registration of the IP trunk fails due to a failure in domain name resolution. Go to the Basic > Network page to check whether the DNS server is correctly configured.
Trunk ID	See Table 2-7.
Concurrent calls	
Username	
Password	
SIP server	
UA domain name	
Registration	
Inbound route	
Greeting	
DID number	
Outbound calls	
Recording	<p>Enable recording for the trunk.</p> <p>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.</p>
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 3-13 IP trunk registration interface

The screenshot shows a web interface for configuring IP trunk registration. At the top, there are tabs: Status, Basic, Extension, Trunk (selected), Multi-site, Application, Advanced, System tool, and Log. Below the tabs, there are sub-tabs: Analog trunk and IP trunk (selected). A 'Go back' link is visible. The main configuration area is divided into sections: Registrar server, Other, and PSTN Failover. The Registrar server section includes fields for SIP server, Local signaling port (5060), Registration expiration (600), Proxy server (localhost:5060), and Increments of port number (0). The Other section includes UA domain name, Sub domain, IP address in SIP Contact header (LAN or NAT), and IP address in SDP c header (LAN or NAT). The PSTN Failover section has an 'Enable' checkbox which is checked.

Table 3-9 IP trunk registration parameters

Item	Description
Default SIP server	This parameter will be applied when the SIP server address of a single trunk line is not entered. Configure the address and port number of the 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.
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,

Item	Description
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. <ul style="list-style-type: none"> 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.

3.2.3 Backup SIP Proxy Server Settings

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

Follow this procedure:

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

Figure 3-14 Secondary SIP proxy server interface

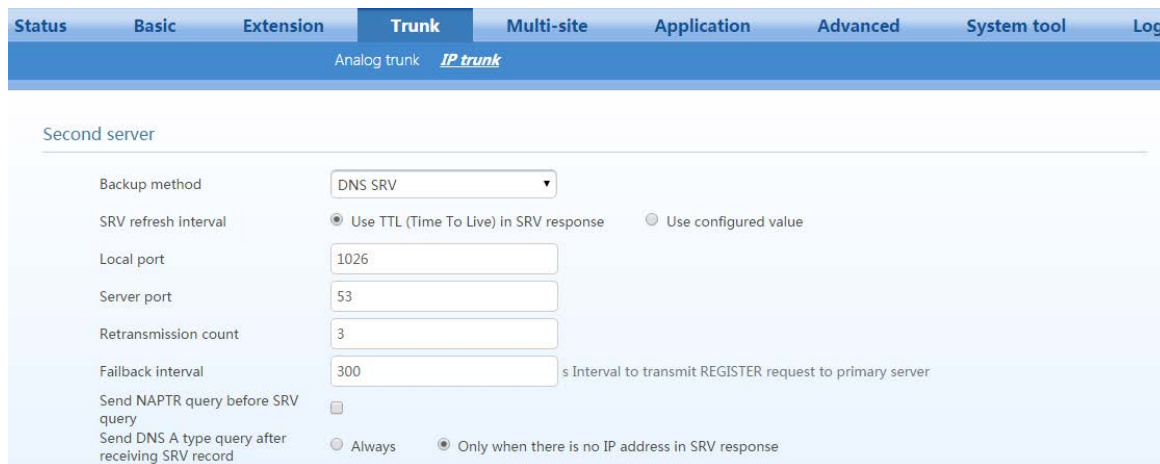


Table 3-10 Secondary SIP proxy server parameters

Parameters	Description
Backup methods	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Use TTL (Time To Live) in SRV response: Default configuration. Use configured value: Customize the refreshing interval. The range is 1–65535s.

Parameters	Description
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	<p>Set the conditions for sending an A type query, after a response to the SRV query request is returned.</p> <ul style="list-style-type: none"> 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.

Step 2 Choose **Backup method**.

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

3.2.4 IMS

The OM50/OM20 can interwork with an IP Multimedia Subsystem (IMS) service network. IMS is a service-network architecture developed by the 3GPP. Typically, an IMS provides services—announcements, for example—to a caller. However, an IMS service network can be used to provide services to clients/subscribers registered on an IP PBX. If this is your application, follow this procedure:

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

Figure 3-15 IMS configuration interface

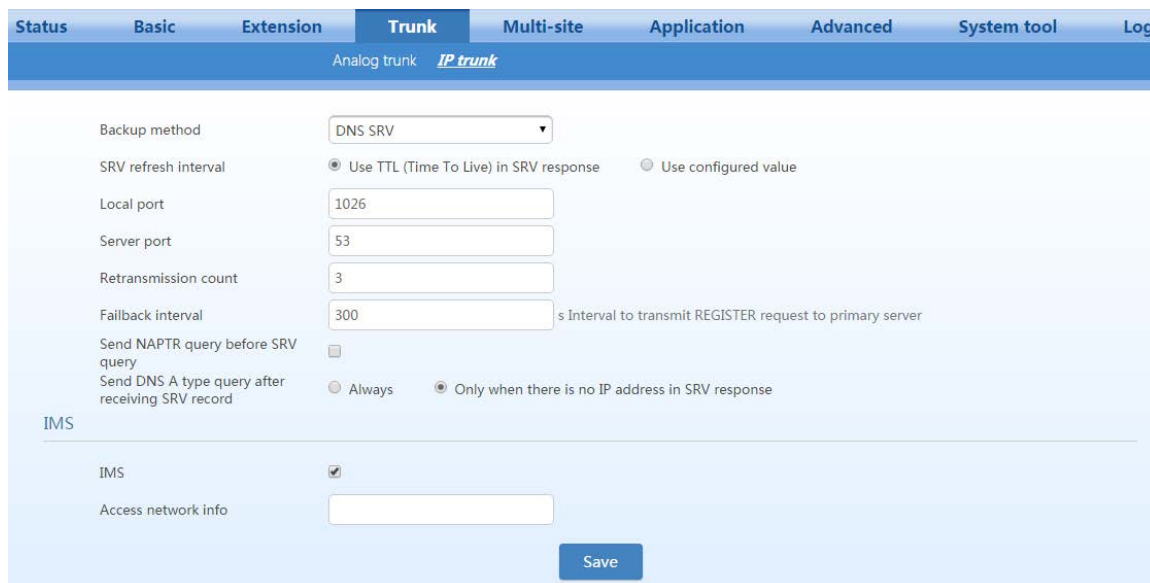


Table 3-11 IMS setting parameters

Item	Description
IMS	Enable interworking with IMS.
Access network info	The IP address and port number of the access network. For example: 192.168.100.200:5060.

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

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

3.3 Configuring Extensions

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

3.3.1 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 3-16 Analog extension setting interface

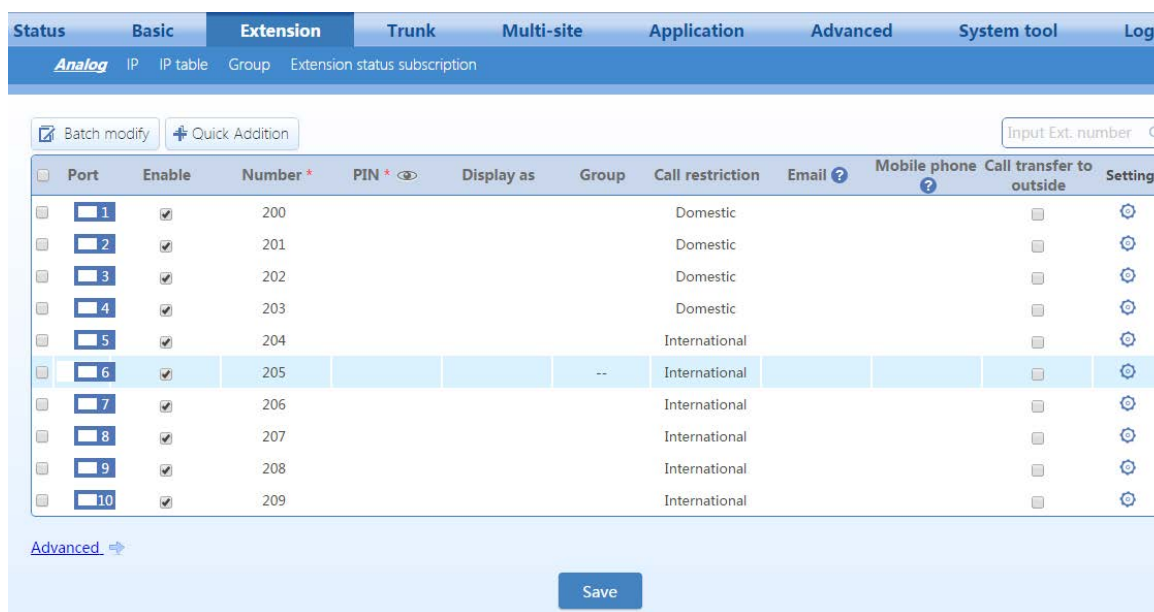


Table 3-12 Analog extension parameters

Item	Description
Batch modify	Configure extensions in batch mode. Batch modes allows the configuration of multiple parameters at once.
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.

Item	Description
PIN	Used for verification when operating via *33 and *99 navigation. Note: <ul style="list-style-type: none"> 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.
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. <ul style="list-style-type: none"> 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 express-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 3-17 Analog extension advanced configuration interface

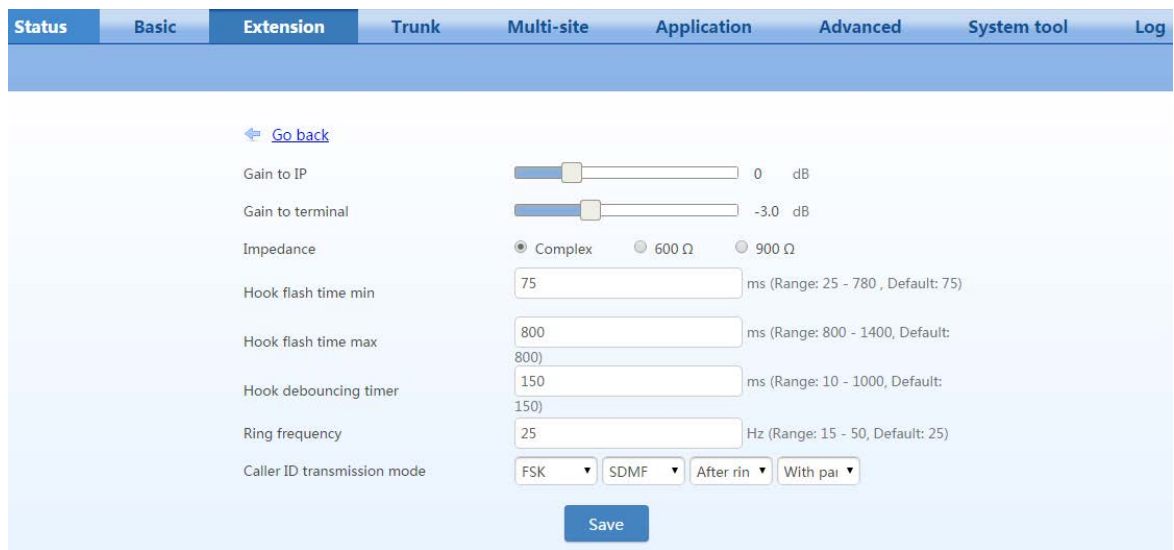


Table 3-13 Analog extension advance setting parameters

Item	Description
Gain to IP	Adjust the call volume received on the FXS port. Increase the value for a louder voice. Range: -3.0 to +9.0 dBs.
Gain to terminal	Adjust the call volume sent from the FXO port. Increase the value for 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 shorter than the min. Generally, this value should not be less than 75 ms. You should adjust the parameter when the phone rings after on-hook or no voice is heard after 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 change 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.

3.3.2 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 3-18 IP extension setting interface

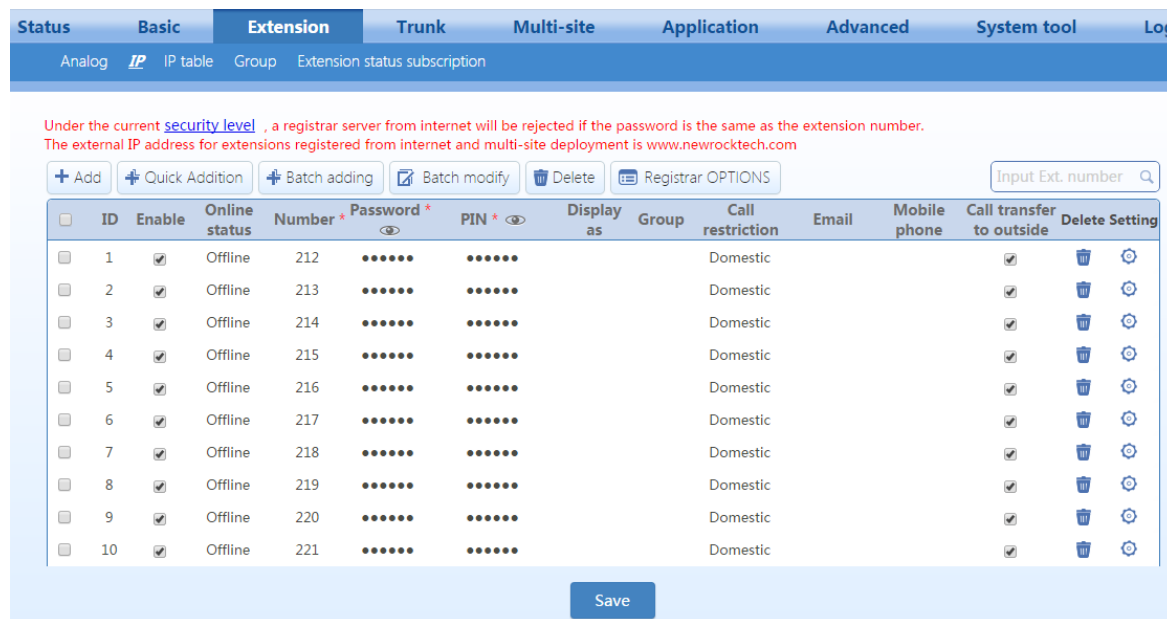


Table 3-14 IP extension parameters

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 2-12.

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.

3.3.3 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 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 3-19 IP authentication interface

The screenshot shows a web-based configuration interface for an extension. At the top, there is a navigation bar with tabs: Status, Basic, Extension (selected), Trunk, Multi-site, Application, Advanced, System tool, and Log. Below this is a sub-menu with options: Analog, IP (selected), IP table, Group, and Extension status subscription. The main content area contains several settings:

- Display as:
- Call restriction: Domestic (dropdown)
- Mobile phone:
- Color ringback tone: -- (dropdown) (r)
- Call forward: Disable (dropdown)
- Target number:
- Speed dial groups:
- Destination number:
- Blocked numbers: You can fill in up to 20 blocked numbers, separated by comma "," .
- Assistant:
- IP address for IP trusted authentication: (highlighted with a red box)

A Save button is located at the bottom center of the form.

3.4 Extension Features

3.4.1 Basic Functions

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

Figure 3-20 Interface of extension features

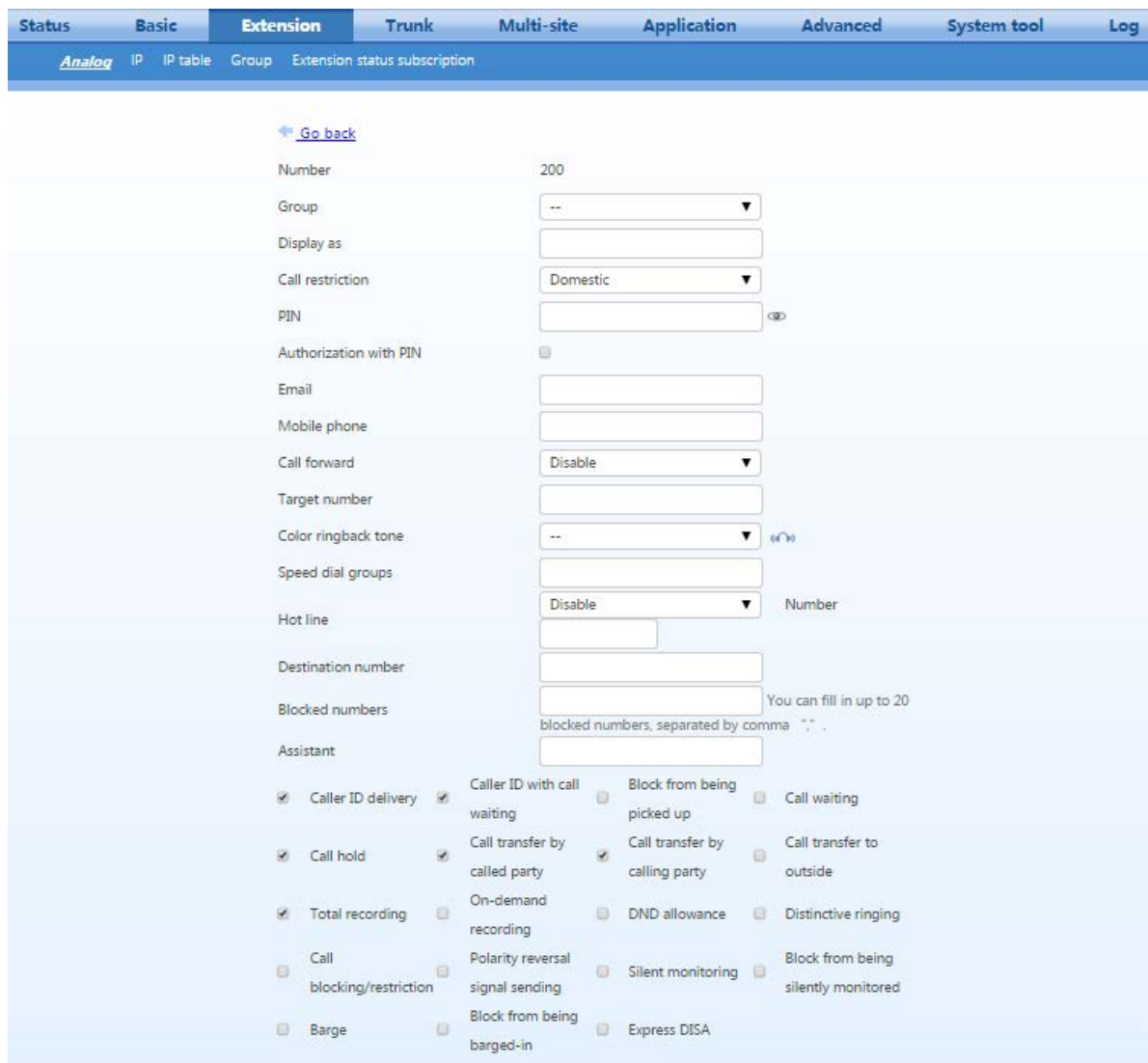


Table 3-15 Extension basic features

Item	Description
group	See Table 2-12.
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.

Item	Description
Call forward	<p>Forward incoming calls to the specified phone or voicemail. This function is disabled by default.</p> <ul style="list-style-type: none"> • CFA (phone): Forward all incoming calls to the specified phone. • Note: This function cannot be enabled for an extension of operator. • CFB/CFNA (phone): Forward incoming calls to the specified phone when the extension is busy or does not answer. • CFA (voicemail): Forward all incoming calls to the specified phone. For details on voicemail, see 2.5.2 Voicemail. • CFB/CFNA (voicemail): Forward incoming calls to the specified phone when the extension is busy or does not answer.
Target number	<p>Set the target phone number for CFA (phone) or CFB/CFNA (phone). 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 calls. 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.</p>
Color ringback tone	<p>Select a CRBT file for the extension. For details on uploading and managing CRBT files, see 2.8.2 CRBT.</p>
Speed-dial groups	<p>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.</p> <p>For example, speed dial group 20 – 13823218765 indicates 20 as the speed dial code for 13823218765..</p>
Hot line	<p>Outgoing calls are automatically routed to the preprogrammed telephone number when the user takes the telephone off-hook.</p> <ul style="list-style-type: none"> • 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. <p>This parameter is only applicable to analog extensions. For IP extensions, hot line configuration is set on the IP phones.</p>
Number	<p>Enter the hot-line number.</p>
Destination number (Call forking)	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> • 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	<p>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 ",".</p> <p>Note 1: An outbound call to the blocked numbers is allowed.</p> <p>Note 2: The blocked numbers configured here are applicable to an extension. To configure blocked numbers for all extensions, go to Extension > IP table.</p>
Assistant	<p>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 can then be transferred to the manager's extension by the assistant.</p> <p>Go to Application > Manager/Assistant, and then select the assistant mode as required.</p> <ul style="list-style-type: none"> • 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's phone. <p>You can dial *35 to enable or disable the assistant function.</p>
Caller ID delivery	<p>If enabled, the caller ID is delivered to the extension.</p>

Item	Description
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 transfers by called party	Transfers received calls to an external phone or other extension. To use the function, the extension should be allowed to transfer calls to outside. <ul style="list-style-type: none"> • 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 transfers 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. <ul style="list-style-type: none"> • 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 2-12.
Call waiting	When a new incoming call arrives while a call is in progress, the user will hear beeps and has three choices: <ul style="list-style-type: none"> • 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	The user can set DND to ensure the extension does not ring when incoming calls are received. The user can dial *72 to enable or disable DND.
Total 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Item	Description
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.
Express DISA	Operate DISA without dialing *33 for verification.

3.4.2 Making Outbound Calls

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

Figure 3-21 Outbound dialing rule interface

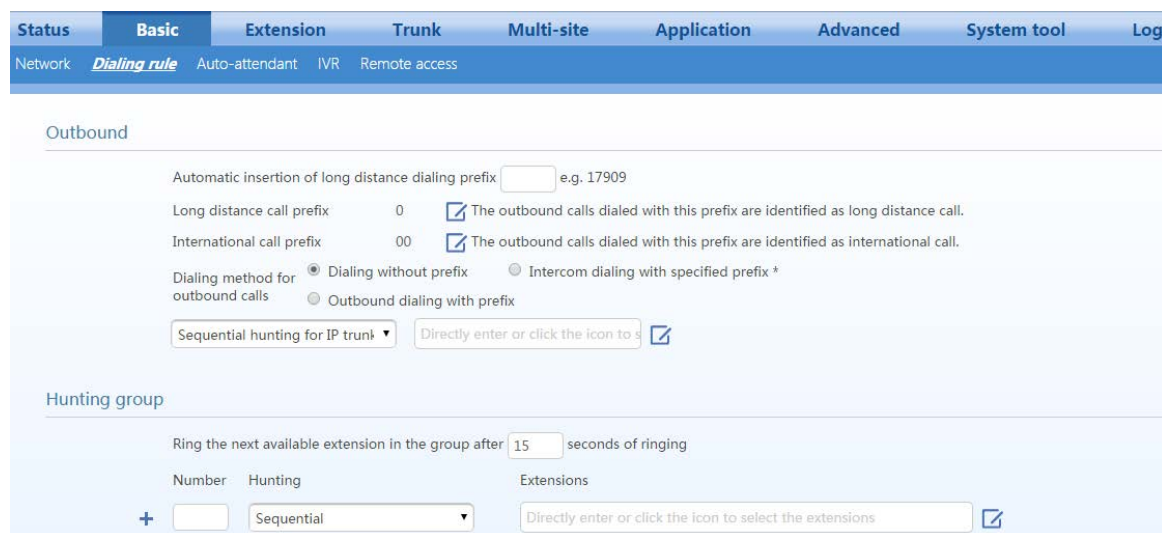


Table 3-16 Outbound dialing rule parameters

Item	Description
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.
International call prefix	The outbound calls dialed with the prefix configured here are identified as international call. The default value is 00. 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.

Item	Description
Dialing method for outbound calls	<ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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 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". <p>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.</p> <ul style="list-style-type: none"> • Route: The routing table rules are used to make the call to the PSTN. For details, see 2.8 System Settings.
Prefix	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> • 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	<p>After the extension user dials the prefix, the device prompts the user to dial the called number with secondary dial tone.</p> <p>Note: Applicable only when the Dialing method for outbound calls is Outbound dialing with prefix.</p>
Trunk	<p>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 ",".</p> <p>Note: Applicable only when the Dialing method for outbound calls is Outbound dialing with prefix.</p>

3.4.3 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 3-22 IP table setting interface

Table 3-17 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 20 phone numbers, separated by comma “,”, which are prohibited from calling in and busy tone will be played to reject the calls. Note: <ul style="list-style-type: none"> • 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.

3.4.4 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 3-23 Hunt-group configuration interface

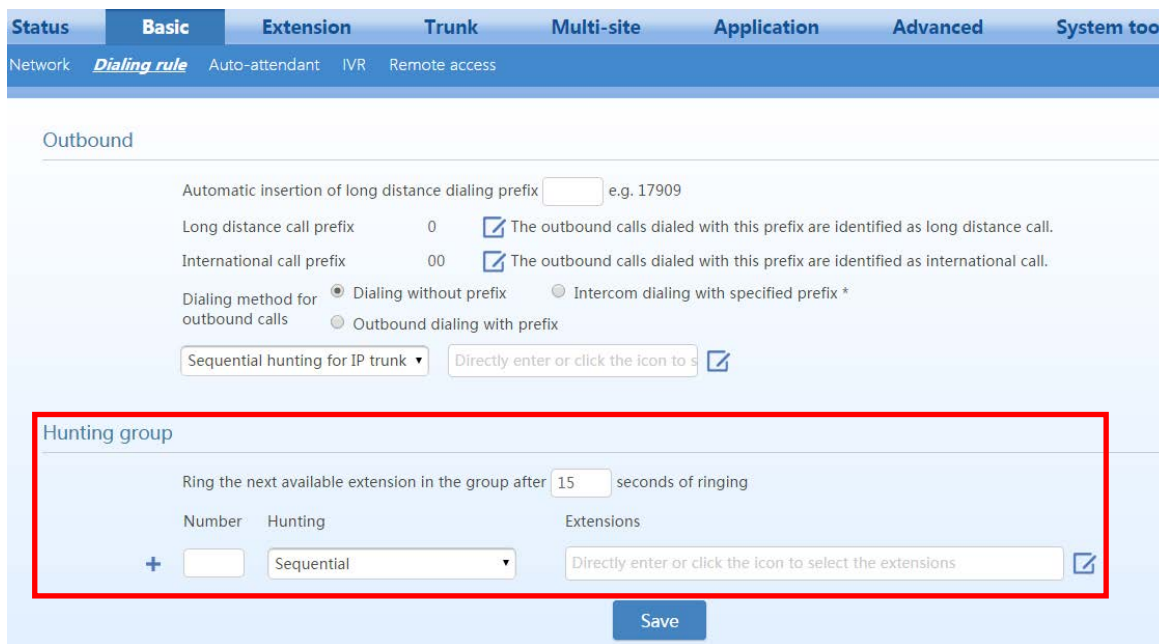


Table 3-18 Hunt-group parameters

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.
Hunt	Select a hunt-group method: <ul style="list-style-type: none"> • 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.

3.4.5 Extension Status Subscription

When you use the New Rock NRP1004 or NRP1012 IP phones as OM voice stations, 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 3-19 Status of BLF indicators

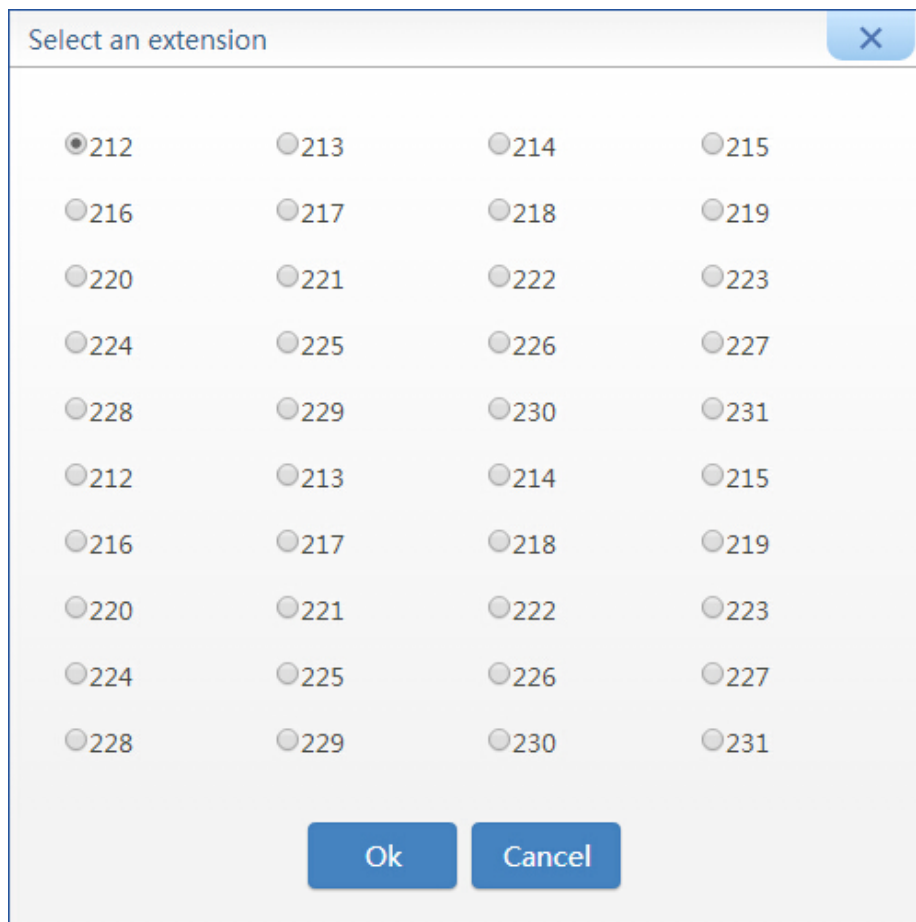
Indicator	Extension status
Steady green	Idle
Red flashing.	Ringing
Steady red	Talking or IP phone is offline

Follow this procedure:

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

Step 2 Select the desired extension.

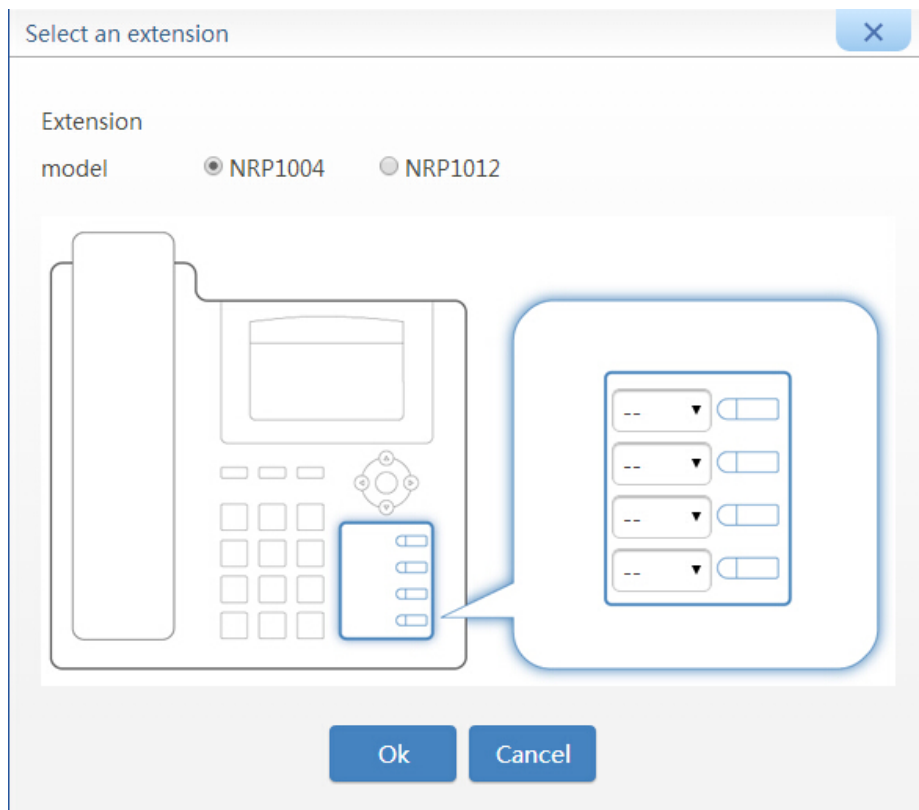
Figure 3-24 Extension status subscription interface



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

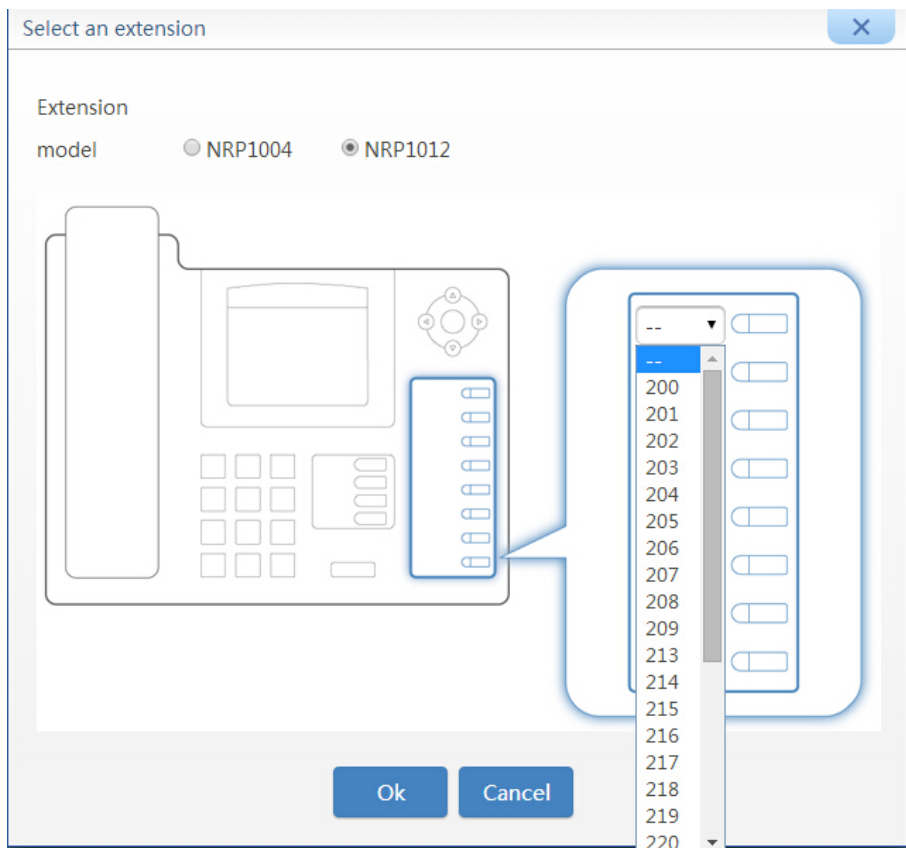
Note: The model of the extension must be correctly selected, otherwise the subscription will be invalid.

Figure 3-25 Figure 2-25 Selecting an extension model



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

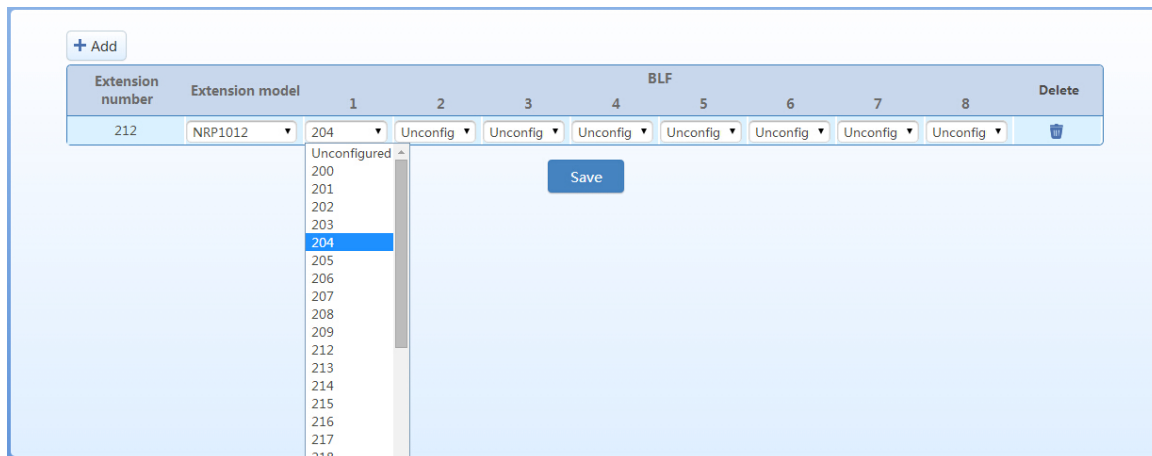
Figure 3-26 Selecting extensions for subscription



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 3-27 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. After the download is completed and the phone reboots, the BLF function keys are enabled.

3.4.6 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 3-28 Group setting interface

The screenshot shows a web interface with a top navigation bar containing tabs: Status, Basic, Extension, Trunk, Multi-site, Application, Advanced, and System tool. Below the tabs is a sub-menu bar with options: Analog, IP, IP table, Group (highlighted), Extension status, and subscription. The main content area has a heading: "Group call pickup is available in the same group. A group name includes alphabetic or numeric characters." Below this is a table with two columns: "ID" and "Group name". The table contains 16 rows, each with an ID (1-16) and an empty text input field for the group name. At the bottom right of the table area is a blue "Save" button.

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

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

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

Figure 3-29 Group Interface

The screenshot shows a web interface with a top navigation bar containing tabs: Status, Basic, Extension, Trunk, Multi-site, Application, Advanced, System tool, and Log. Below the tabs is a sub-menu bar with options: Analog, IP, IP table, Group (highlighted), Extension status, and subscription. The main content area has a heading: "Go back" with a left-pointing arrow. Below this is a form with a "Number" field containing "200" and a "Group" dropdown menu. The "Group" dropdown menu is highlighted with a red rectangular box.

3.4.7 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](#).

3.4.8 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](#).

3.4.9 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](#).

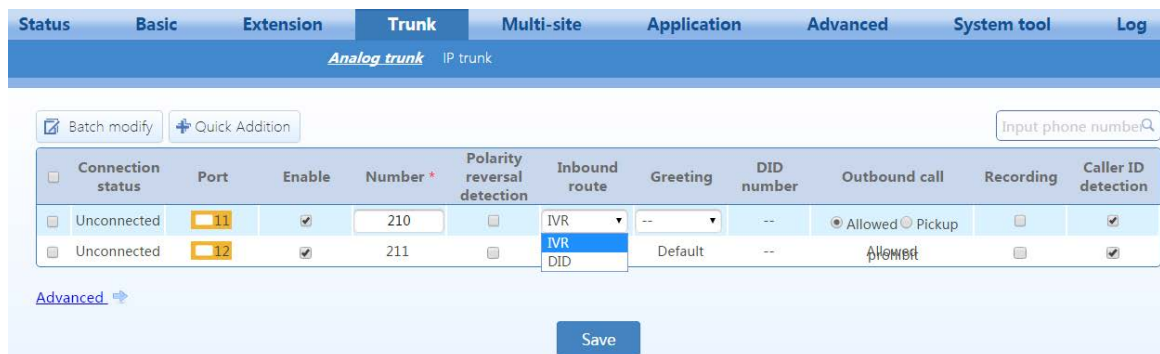
3.4.10 DID

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.

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 3-30 DID setting 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.

3.4.11 Feature Access Codes

Feature Access Codes are special patterns of characters that are dialed from a phone keypad to invoke particular features.

Go to **Advanced > Feature access code** to query or customize feature access codes Click [?](#) to view

details about the feature-access codes.

Figure 3-31 Feature access codes interface

The screenshot shows a web interface for configuring feature access codes. It has a top navigation bar with tabs: Status, Basic, Extension, Trunk, Multi-site, Application, **Advanced**, System tool, and Log. Below the tabs is a sub-menu with links: System, Feature access codes, Encryption, Routing, Dialing, Tone, SIP, DTMF, Security, White list, and Call record.

The main content area is divided into four sections:

- System feature codes**:
 - Obtain IP address: ##
 - Set up IP address: *90
 - Set up extension number: *96
 - Obtain extension number: #00
- Voice prompt recording**:
 - Record: *81
 - Audit: *82
 - Save: *83
- Feature codes**:
 - Call park: *30
 - Call park retrieval: #30
 - Call pickup: *51
 - Attendant call pickup: *50
 - Directed call pickup: *55
 - Group pickup: *56
 - Calling with PIN: *33
 - Blind transfer: *38
 - Three-way calling: *79
 - Silent monitoring: *34
 - Speed dial: **
 - On-demand recording: *#
 - Automatic callback busy: *31
 - Barge: *39
 - Listen to voice messages: *98
- Activating features**:
 - Call forking: *75
 - Assistant: *35
 - Authorization with PIN: *77
 - Block from being picked up: *73
 - Do not disturb: *72
 - Call waiting: *64
 - Set up speed dial: *74

At the bottom of the form are two buttons: **Save** and **Default**.



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.

3.5 Recording and Voicemail

3.5.1 Recording

The OM series supports remote recording and USB-device recordings.

Remote recording

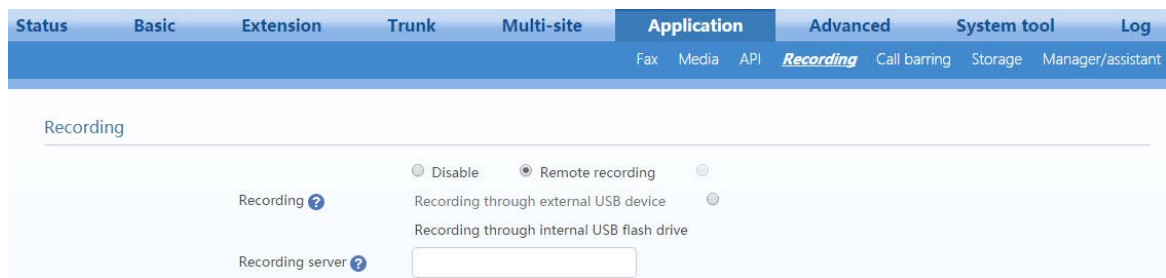
All the recorded files are stored in the external recording server. Before recording, an external recording server installed with New Rock Recording Agent is required. You can download the recording agent from:

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

Follow this procedure:

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

Figure 3-32 Remote recording configuration interface



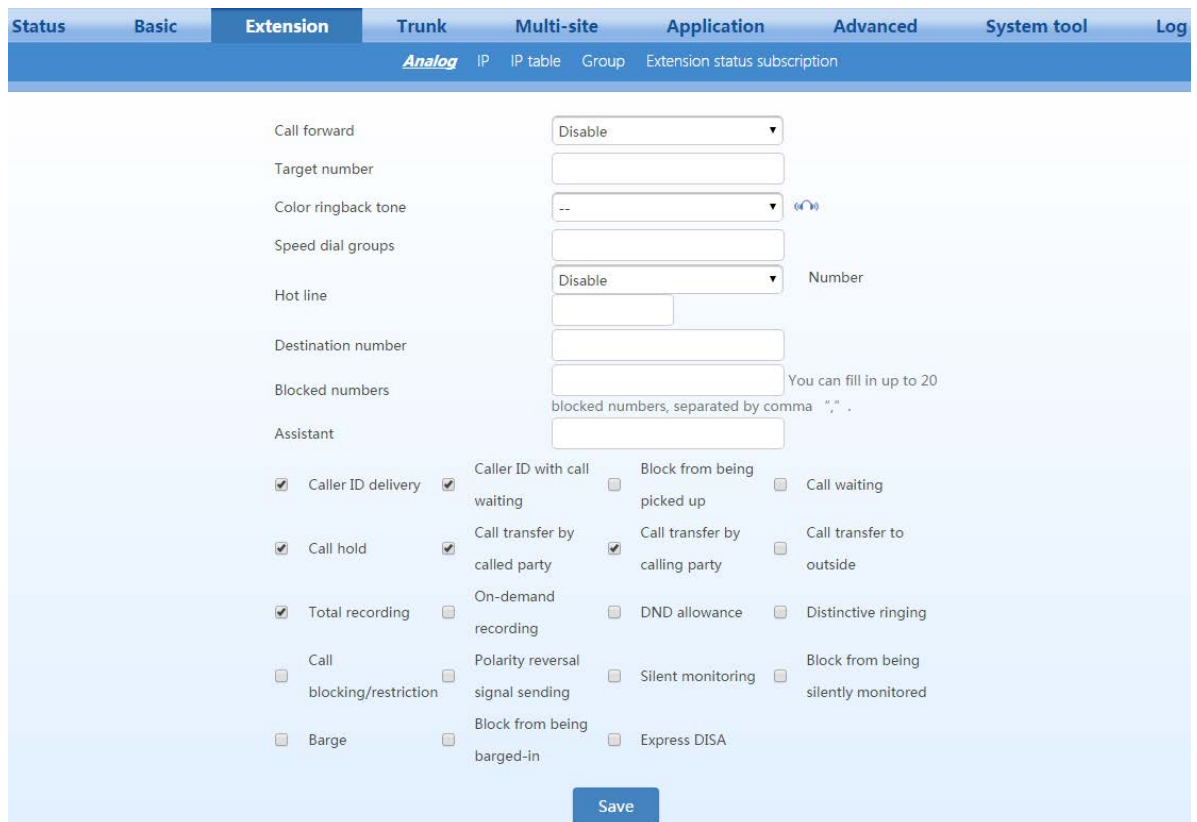
Step 2 Enter the IP address and port number of the recording server. The default port number is 1311.

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 **Total recording**.

Figure 3-33 Extension recording 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.

Note: When there is 500 MB of free space left, a warning will be displayed on the **Status** page and the recording is stopped, allowing you to free some storage space.

Figure 3-34 USB recording setting interface

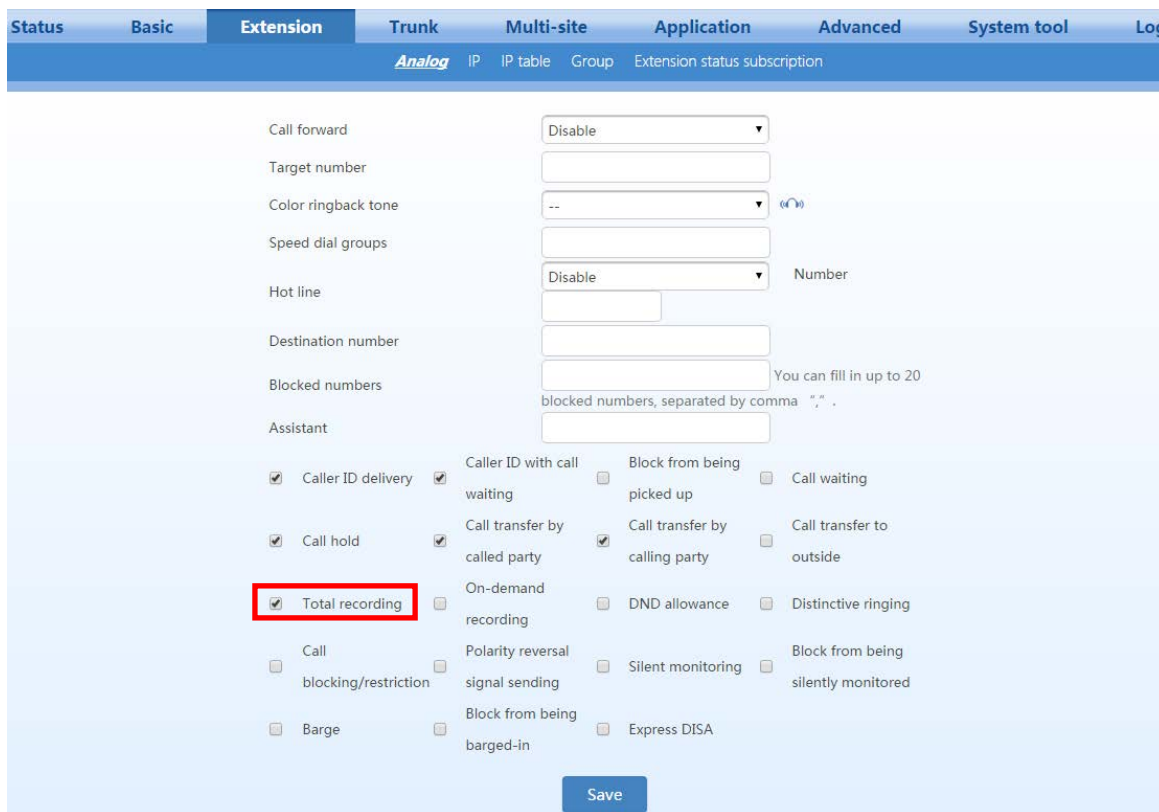


Step 3 Click **Save** to save the configuration.

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

Step 5 Select **Total recording**.

Figure 3-35 Extension recording interface



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

Managing recorded files

Table 3-20 Managing recorded files

<p>Format</p>	<p>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.</p>
<p>View recorded files</p>	<ul style="list-style-type: none"> 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.
<p>Listen to recorded files</p>	<p>You can listen to the recorded files with either of the following methods:</p> <ul style="list-style-type: none"> Locate and download the recorded files, and play it; Play the recordings on the Call log page of NeeHau Business Phone Assistant.
<p>Backup and clear recorded files</p>	<ul style="list-style-type: none"> 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.
--	--

3.5.2 Voicemail

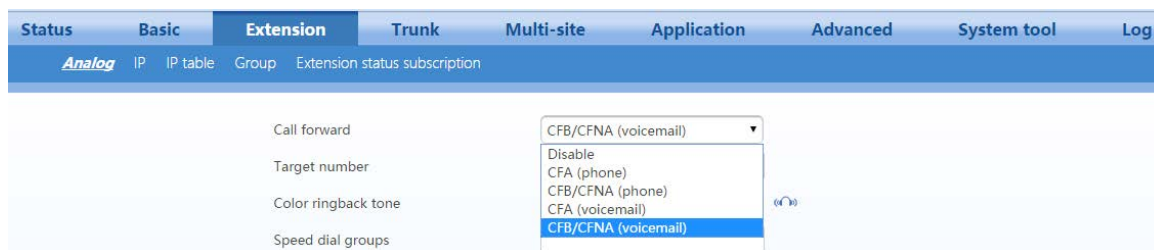
When the extension user cannot receive the incoming call, the calling party can leave a message after the prompt.

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 **Recording through 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 3-36 Voicemail setting 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 **Mail server**.

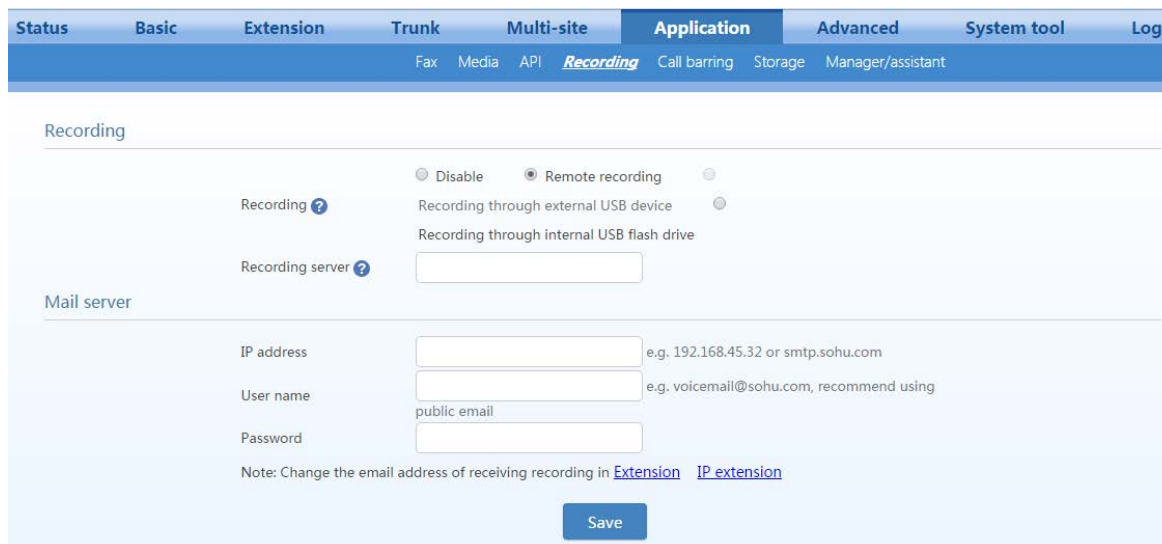


Table 3-21 Voice mailbox sending server parameters

Item	Description
IP address	Enter the IP address or domain name of the mail server. The device supports Sina and Soho mailboxes.
User name	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 3-22 Managing message files

Format	<p>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 oldvm_200-6033432345-946685192.pcm.</p> <p>Note: The filename extensions are varied depending on the codec of the voicemail message:</p> <ul style="list-style-type: none"> • G.711μ: The file extension is .pcmu. • G.711a: The file extension is .pcma. • G.729: The file extension is .dat.
View the voicemail message files	<ul style="list-style-type: none"> • 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: sda1/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	<ul style="list-style-type: none"> • Analog phone: Press *98 and listen to the voicemail messages. You may hear: <ul style="list-style-type: none"> “You have no voicemail messages”. “You have n new/saved voicemail messages“ After the voicemail message is played, you may hear: <ul style="list-style-type: none"> “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	<p>Same as Table 2-20 Managing recorded files.</p>

3.6 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 3-37 FAX configuration interface

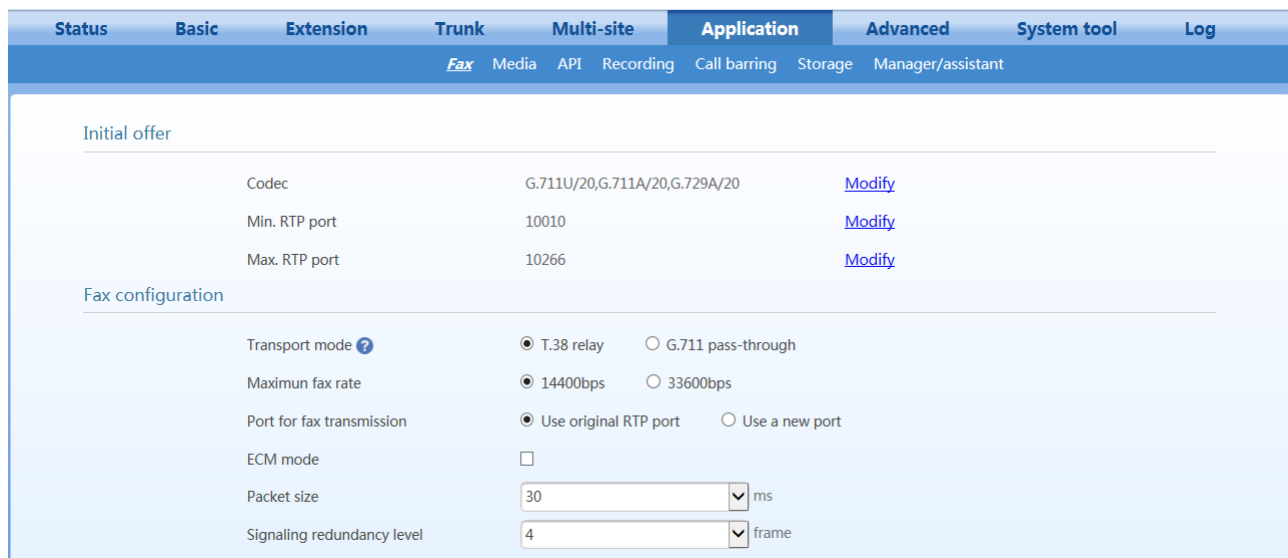


Table 3-23 FAX parameters

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 2-36 Media parameters. 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.
Fax 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. <ul style="list-style-type: none"> • Transport via analog trunk: Select G.711 pass-through • Transport via SIP trunk: Select the fax transport mode based on the service provier’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.
Maximum 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 33,600-bps, 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 . <ul style="list-style-type: none"> • Use a new port: A new RTP port is used. • Use original RTP port: The original RTP port established during the call is used.

Item	Description
ECM mode	The error-correction mode (ECM) for the fax feature. The default setting is varied depending on the fax transport mode. <ul style="list-style-type: none"> • G.711 pass-through: ECM is checked by default • T.38 relay: ECM is not checked .by default for T38 mode, which is turned off 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.
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.

3.7 Multi-site

Two multi-site numbering schemes can be selected:

- Assign the extension numbers on each site in a uniform way (e.g. numbers are unique across all sites.);
- Assign the extension numbers on each site individually.

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

3.7.1 Assign the extension numbers on each site in a uniform way

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 headquarters and its branch offices. To establish a large-scale intersite network in a hierarchical management mode, you need to select **Assigned by each site**.

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

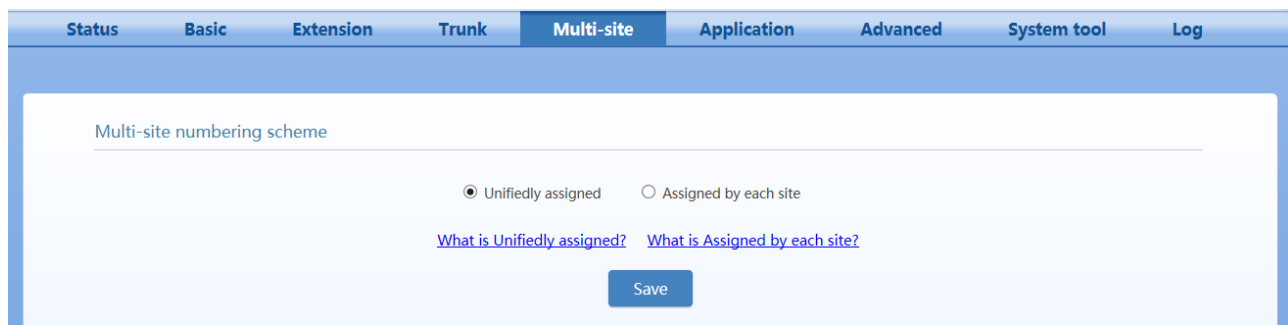
You must configure a management site with several common sites. The management site obtains updated information from each common site and distributes the information to all common sites.

For details, see the description below.

Management site

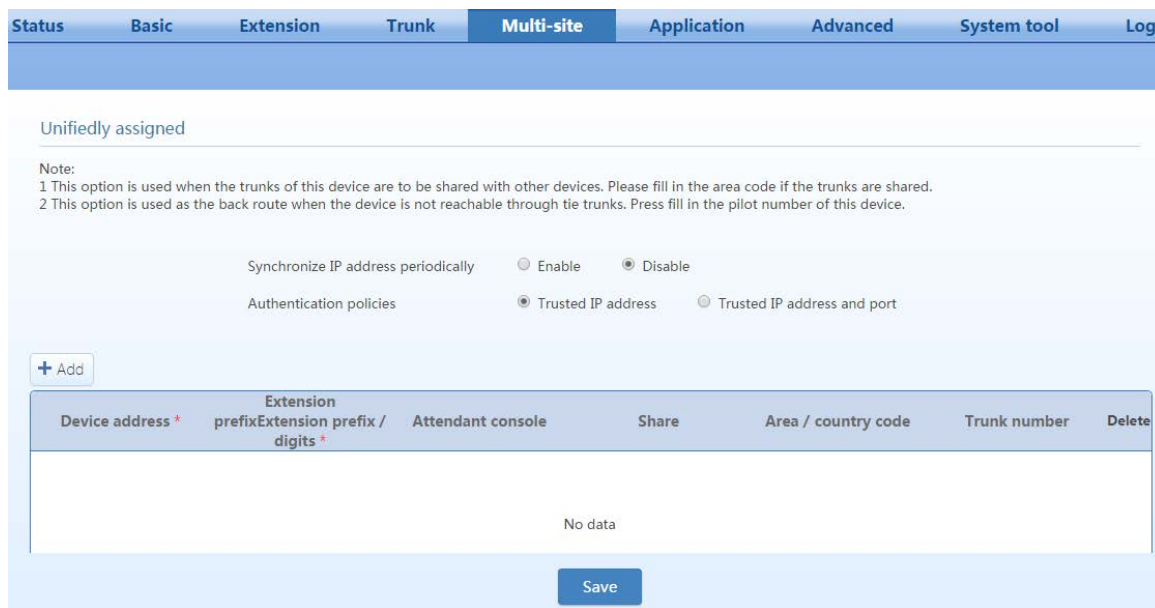
Step 1 Click **Multi-site**, select **Unifiedly assigned**, and click **Save** to display the configuration options.

Figure 3-38 Multi-site numbering scheme selection interface



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

Figure 3-39 Multi-site configuration interface



Step 3 Select authentication policies.

Table 3-24 Authentication policy parameters

Item	Description
Trusted IP address	Authenticates the IP address of the site device. The IP address of the message sender should conform to the setting in the site configuration list to ensure that the device is trustworthy and the message sent by the sender should be processed. When other devices in the multi-site network communicate from behind a NAT device, the port numbers used will be random. Site identity authentication must then be selected for the device.
Trusted IP address and port	Authenticates IP address and SIP port number of the site. The IP address and SIP port of the message sender must match an entry in the list of multi-site peers to ensure that the device is trustworthy. Otherwise, the received call may be ignored.

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

Figure 3-40 Site adding interface

Table 3-25 Configuring per-site 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 as 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 (NATed), 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.
Attendant console	For extensions in a same group of devices, their call status can be monitored by the auto-attendant monitoring software.
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 2-25.

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 **Uniform**, 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.

3.7.2 Assign the extension numbers for each site individually (per-site)

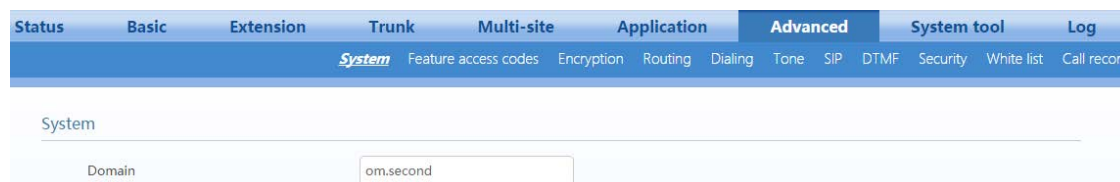
When extensions call each other, a prefix needs to be added to prevent number conflict and ensure that the extension numbers under different sites can be reused with per-site numbering. With this form, a large-scale multi-site telephony network can be built up, in which the numbering plan of each device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

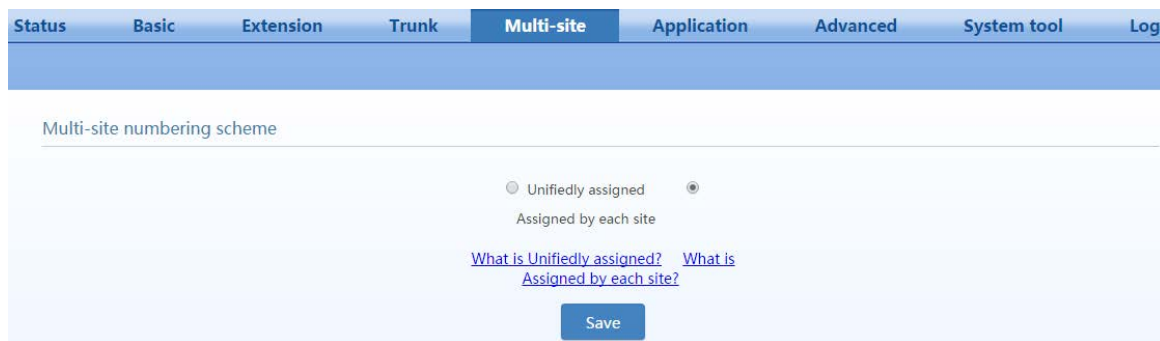
Step1 Go to **Advanced > System**, and enter the IP address or domain name of the device in the **Domain** input box, and click **Save**.

Figure 3-41 Domain name interface



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

Figure 3-42 Multi-site scenarios configuration interface



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

Figure 3-43 Device multi-site role selection interface

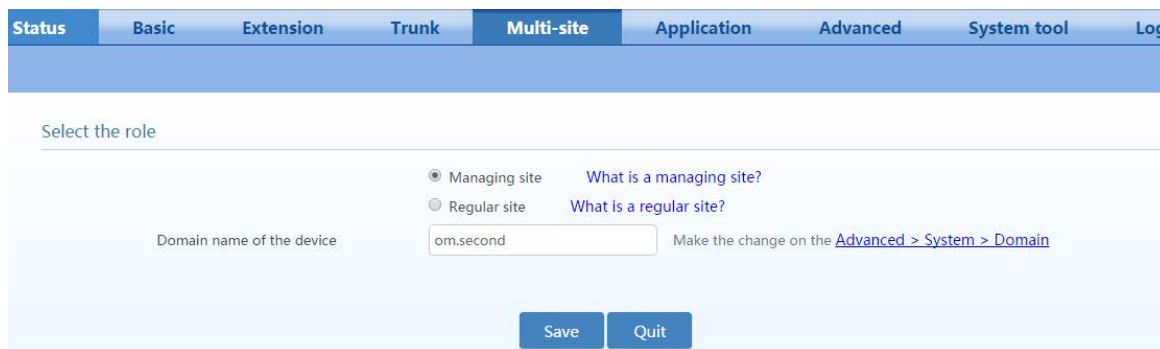
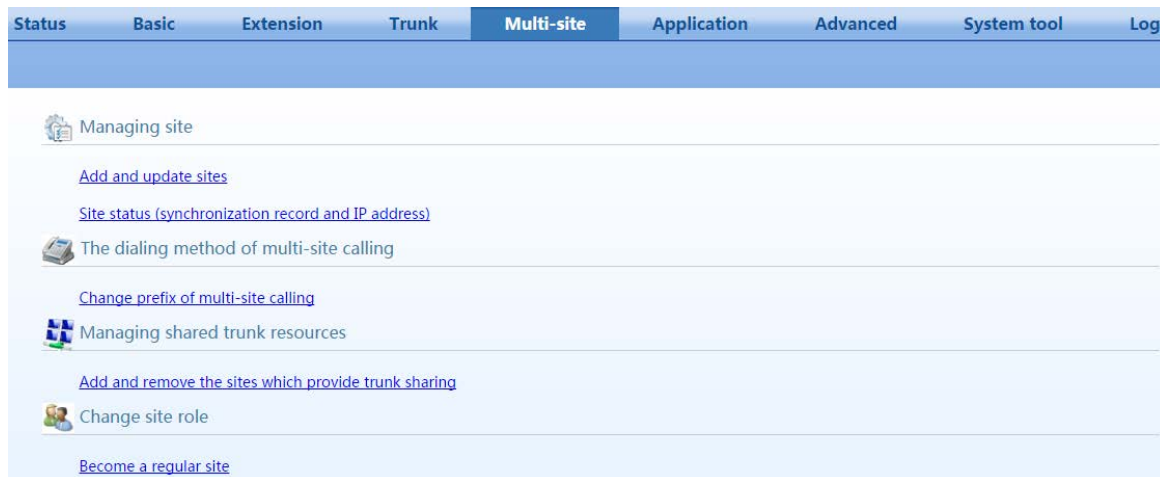


Figure 3-44 Multi-site scenarios configuration interface



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

Figure 3-45 Device list configuration interface

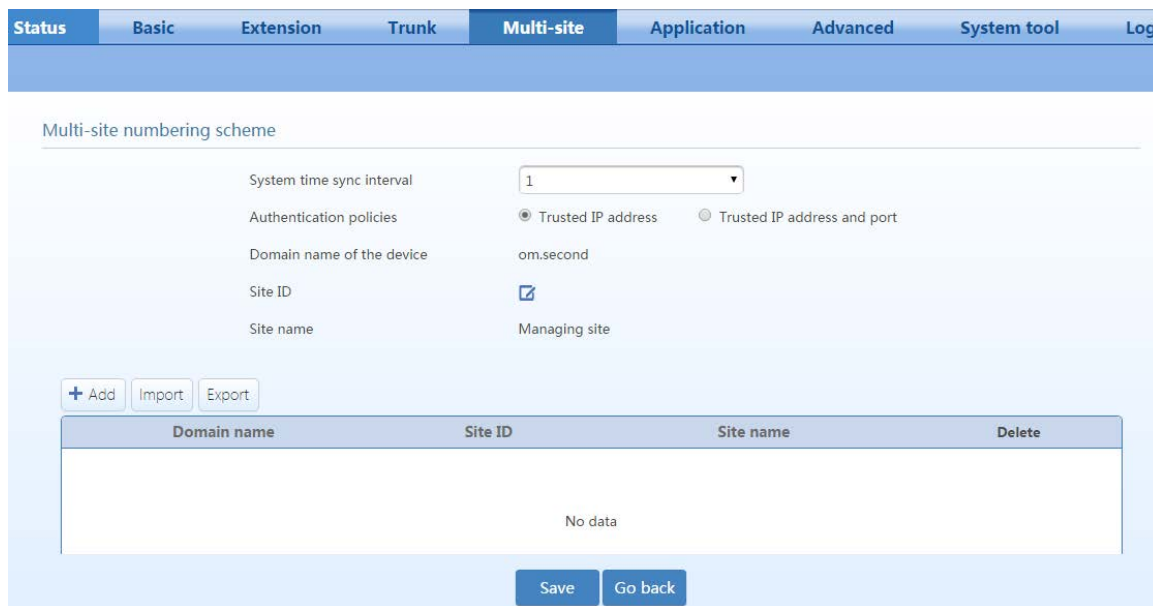


Table 3-26 Numbering scheme parameters

Item	Description
System time sync interval	Interval for synchronization with common sites.
Authentication policies	<ul style="list-style-type: none"> • 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 2-24.
Domain name of the device	The IP address or domain name of the device. It can be modified in Advanced > System > Device domain name .
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 setting interface, click **Change prefix of multi-site calling** under **The dialing method of multi-site calling**, and then set the dialup prefix.

Figure 3-46 Prefix setting interface

Table 3-27 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 setting interface, click **Add and remove the sites which provide trunk sharing** under **Managing shared trunk resources**, and configure outbound trunks.

Figure 3-47 Trunk sharing setting interface

Table 3-28 Trunk sharing setting parameters

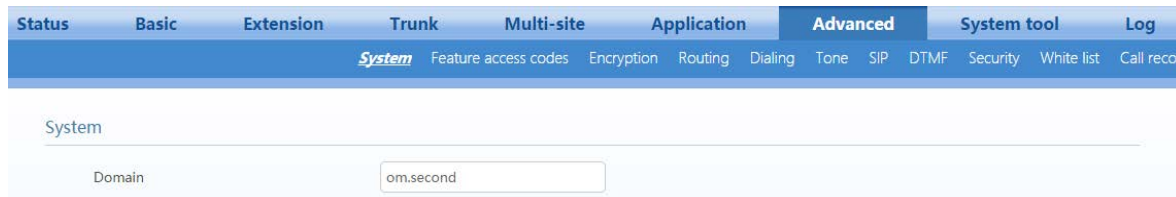
Item	Description
Site name	A site that provides trunk sharing. An outgoing line is provided for the trunk according to the default first rule on the Outbound dialing rule interface.
Destinations	Area/country codes that are allowed to call. Multiple area/country codes must be separated by ",".
Sites with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

Common Site

Enter the device domain name.

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

Figure 3-48 Domain name setting interface

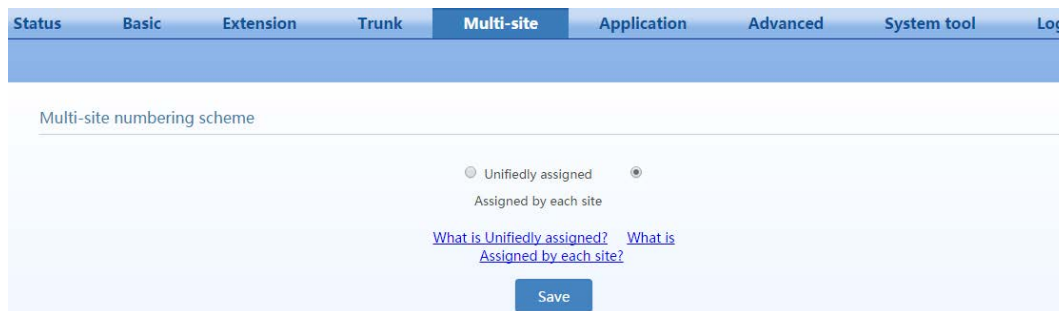


Note

- 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.

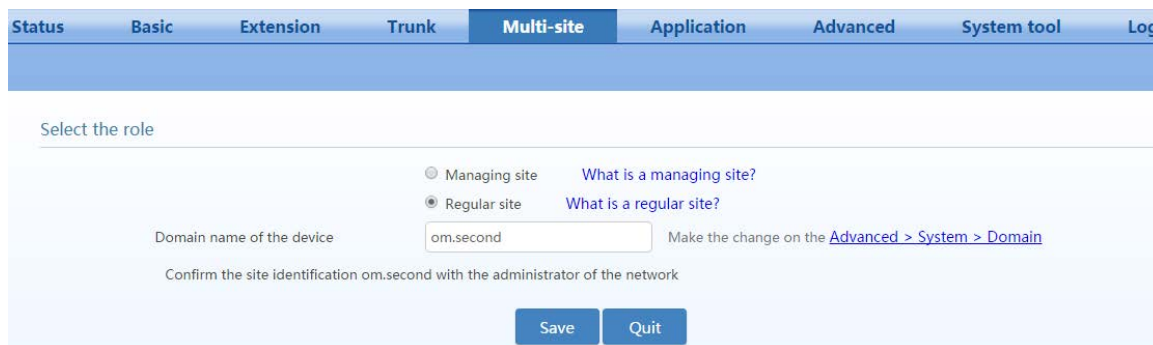
Step2 Click **Multi-site**, select **Assigned by each site**, and click **Save** to display the configuration options.

Figure 3-49 Interface of multi-site scenarios 1



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

Figure 3-50 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 3-51 Managing site address interface

The screenshot shows a web interface with a navigation menu at the top containing the following items: Status, Basic, Extension, Trunk, Multi-site (highlighted), Application, Advanced, System tool, and Log. Below the menu, there is a section titled "IP address of the managing site" with a corresponding input field. The label "IP address of the managing site" is positioned above the input field. Below the input field are two buttons: "Save" and "Go back".

When configuration is successful, the icon turns green.

Figure 3-52 Multi-site networking status interface

The screenshot displays a status interface with a green refresh icon on the left. To the right of the icon is the text "Update multi-site configuration". Below this, there are two blue underlined links: "Get the configuration from the managing site" and "Configure IP address of managing site".

3.8 System Settings

3.8.1 Built-in Storage Management

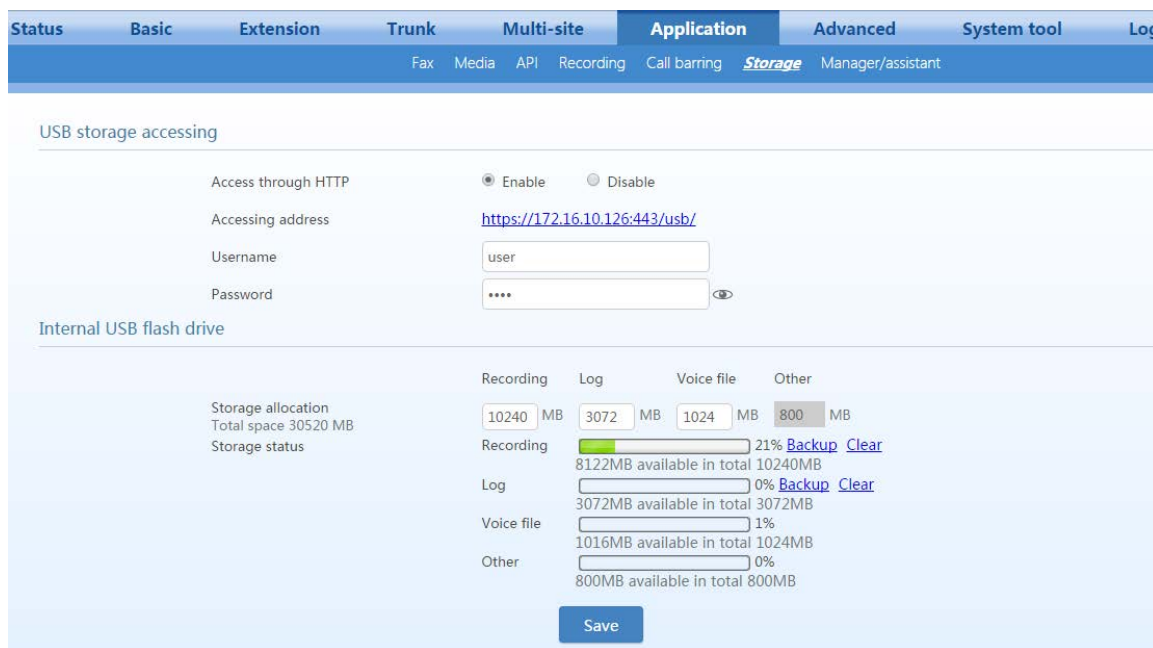
The OM50/OM20 have an internal USB flash drive of 16GB for storing recording files, log, audio files, etc.

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	30,72MB
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 3-53 Storage interface



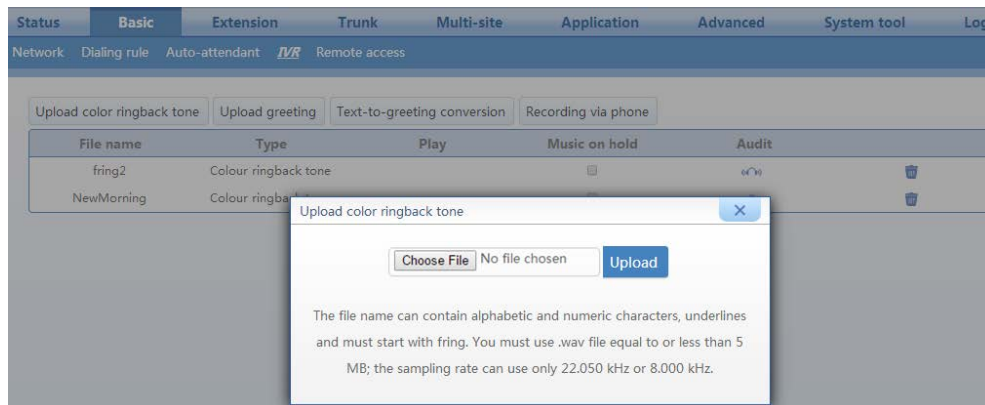
3.8.2 CRBT

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 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 3-54 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.

3.8.3 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 .


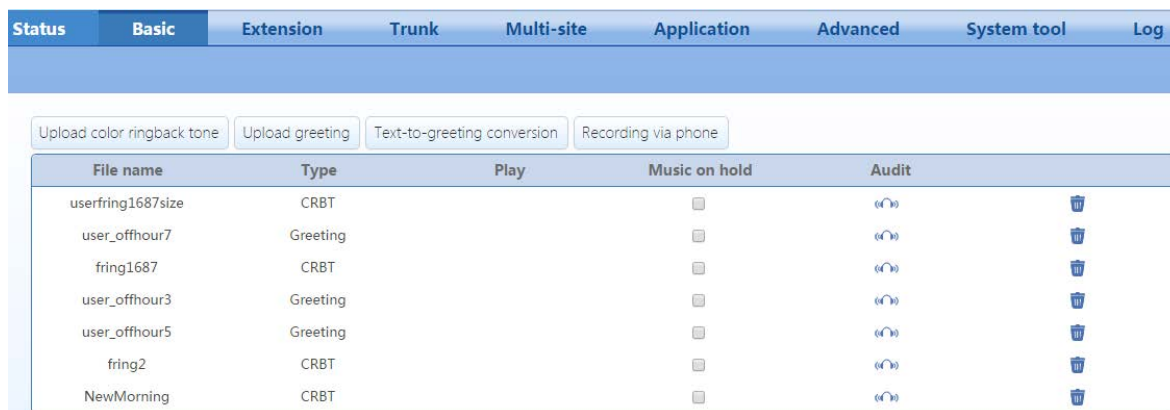
To delete an audio file, click .

Figure 3-55 Music on hold setting interface



3.8.4 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 3-56 System time setting interface

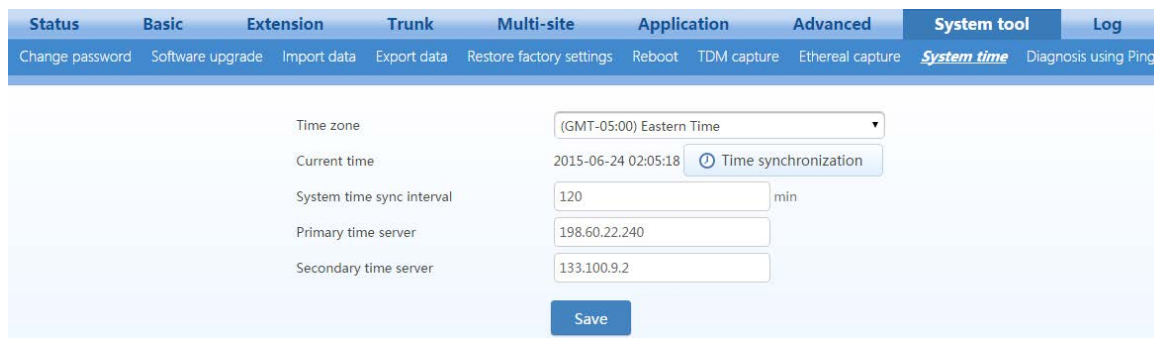


Table 3-29 System time parameters

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.

3.8.5 Encryption

Go to **Advanced > Encryption**.

Figure 3-57 Encryption interface

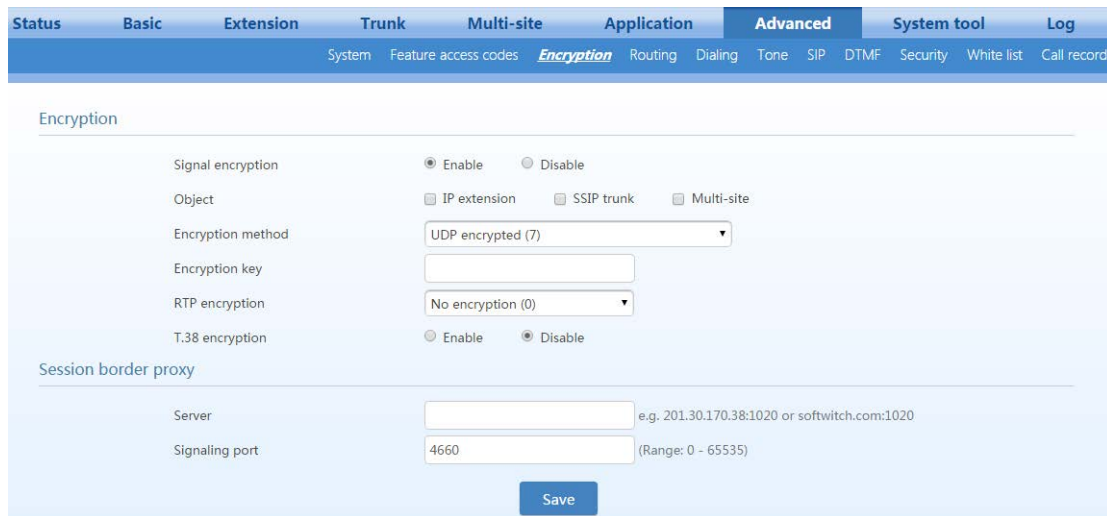


Table 3-30 Encryption parameters

Item	Description
Signal encryption	Enable or disable signaling encryption. It is disabled by default.
object	<ul style="list-style-type: none"> 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.
Encryption method	<p>Set the gateway encryption method, the default value is 7. The optional parameters are:</p> <ul style="list-style-type: none"> 2:TCP not encrypted 3: TCP encrypted 7: UDP not encrypted 7:TCP not 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 <p>An encryption method can be selected according to the softswitch platform.</p>
Encryption key	Can be obtained from your service provider
RTP encryption	<p>Choose whether to encrypt RTP voice pack, the default is 0.</p> <ul style="list-style-type: none"> 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.
Session Border Proxy	Encryption methods (2), (3), (6), and (7) need to work with New Rock SBC products.

Item	Description
Server	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.
Signaling 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.

3.8.6 Routing Table

A routing table is used to implement number replacement and route allocation/specification. 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.

Dialed-Number Transformation (analog trunks)

Format: **Trunk type** *called number prefix (to match)* **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 type include FXS and FXO. FXS indicates that the IP trunk is used to make the outbound call; FXO indicates that the IP trunk receives the inbound call which is then routed to the FXO trunk.

Examples:

- When an analog trunk/FXO 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 (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, the prefix 17909 is added to the number of the called party:
FXO 011 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 make a 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 011 when an international toll call is made), the call duration is restricted to 10 minutes:

FXS 011 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

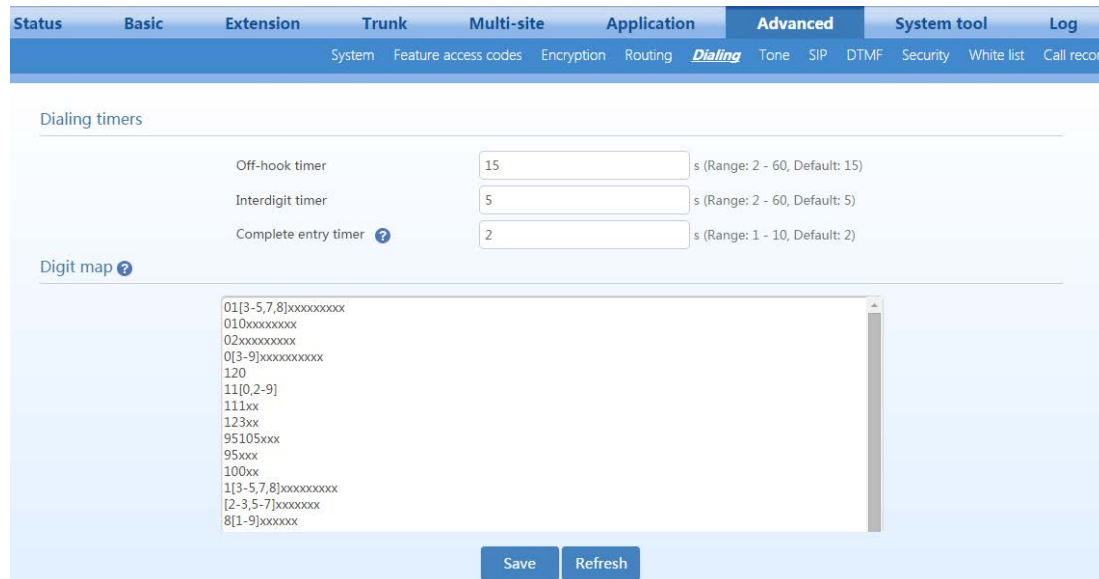
- Called party number based routing to an IP address. **FXS 6120 ROUTE IP 192.168.2.218**

3.8.7 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 3-58 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 3-31 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.. E.g., x can be matched to 1 or 2.
.	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 e.g. 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.

Character	Description
xxxxxxxx.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.
02xxxxxxxx	The device terminates receiving digits after receiving 11 digits starting with 02.
013xxxxxxxx	The device terminates receiving digits after receiving 12 digits starting with 013.
13xxxxxxxx	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.

3.8.8 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 3-59 Call-progress tone interface

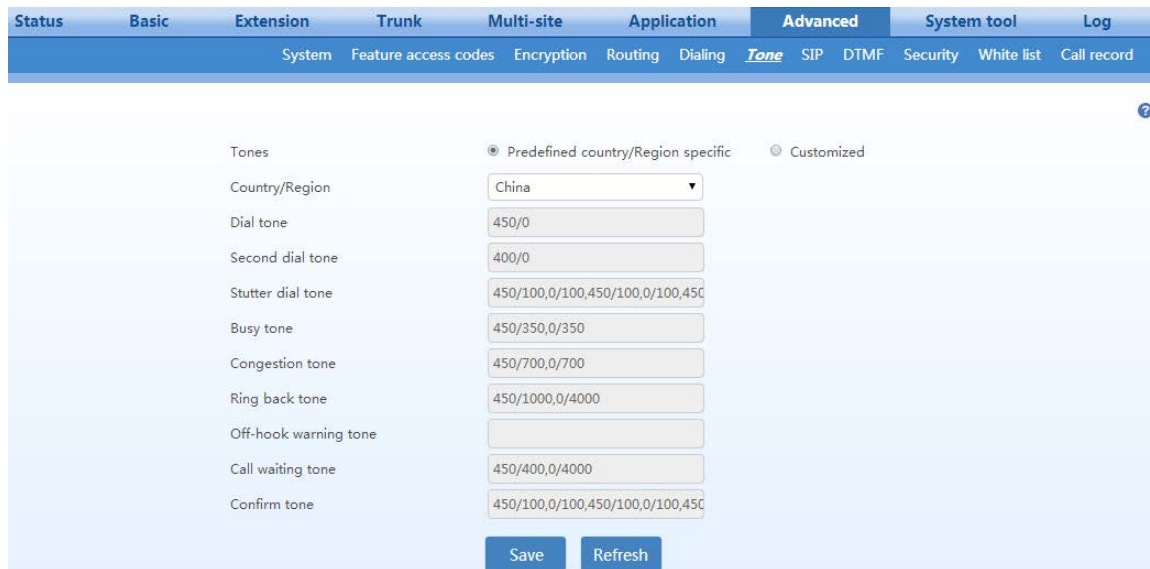


Table 3-32 Call progress tone parameters

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.

Item	Description
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/re-order tone	Used for notification of call set-up failure due to resource limit.
Ringback 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 3-33 Examples of Customized Tone

Examples	Description
350+440 (dial tone)	Indicates the dual-frequency tone consisting of 350- and 440-Hz
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 30- ms on and 10-s off.
950/333,1400/333,1800/333,0/1000	Indicates repeated playing of 33- ms of 950-Hz, 333 ms of 1400-Hz, 333 ms of 1800-Hz, and mute of 1 second.

3.8.9 SIP Advanced Configuration

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

Figure 3-60 SIP related setting interface

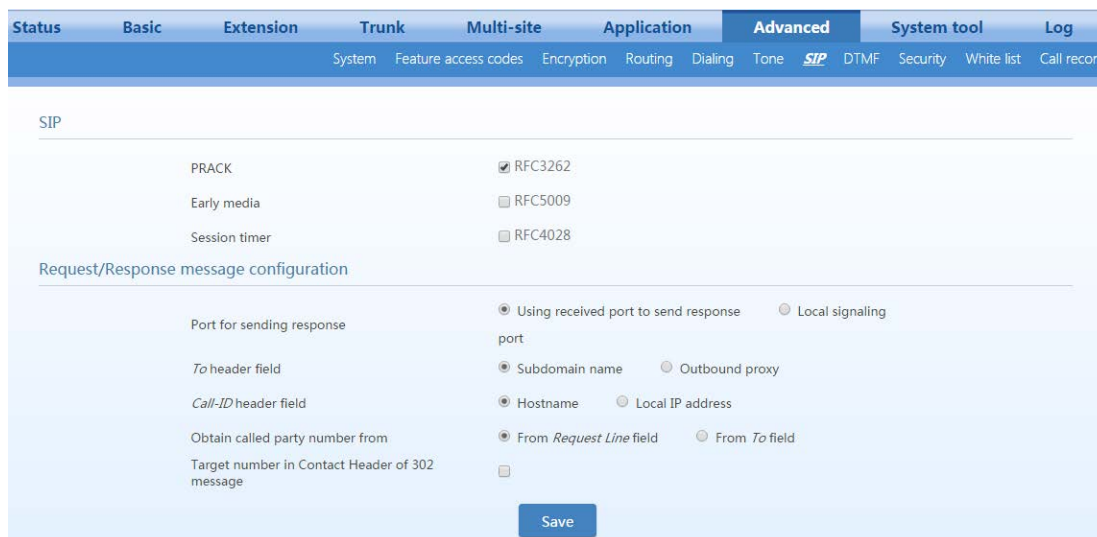


Table 3-34 SIP Related Configuration

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: <ul style="list-style-type: none"> • 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.
Session timer	Choose to activate session refresh (RFC 4028). The session timer is not activated or selected by default.
Session interval	Set the session refresh interval, the device will enclose the value of Session-Expires into INVITE or UPDATE messages. The value range is 30 to 65535 second, and the default value is 1800s.
Minimum timer	Minimum interval for receiving session refresh requests. The value range is 30 to 65535 second, and the default value is 1800s.
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: <ul style="list-style-type: none"> • 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. Otherwiase, the target number in the Contact will be 13812345678.

3.8.10 DTMF

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

Figure 3-61 DTMF interface

The screenshot shows a web-based configuration interface for DTMF. At the top, there are navigation tabs: Status, Basic, Extension, Trunk, Multi-site, Application, **Advanced**, System tool, and Log. Under the 'Advanced' tab, there are sub-tabs: System, Feature access codes, Encryption, Routing, Dialing, Tone, SIP, **DTMF**, Security, White list, and Call record. The main configuration area contains the following fields:

- Transmission method: RFC 2833 (dropdown menu)
- RFC 2833 payload type: 101 (text input). Range: 96 to 127, Default: 101, consistent with the opposite end (such as: softswitch platform)
- DTMF tone duration: 100 (text input). ms (Range: 50 - 150, Default: 100)
- DTMF interdigit pause: 100 (text input). ms (Range: 50 - 150, Default: 100)
- Min. DTMF detection duration: 48 (text input). ms (The range must be 32 to 96 in multiples of 16)
- DTMF detection duration increment against talk-off: 16 (text input). s. Increase the value will improve the false detection of DTMF tone

A 'Save' button is located at the bottom right of the configuration area.

Table 3-35 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. <ul style="list-style-type: none"> • 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 100. 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.

3.8.11 Media

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

Figure 3-62 Media setting interface

Table 3-36 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 Remote Media Address From	<ul style="list-style-type: none"> SDP Global Connection: Obtain the media destination IP address from the global connection entry in received SDPs; SDP Media Connection (default value): Obtain the media destination IP address from the first media descriptor in received SDPs. If the first media descriptor in a received SDP does not contain an IP address, the global connection address is used.

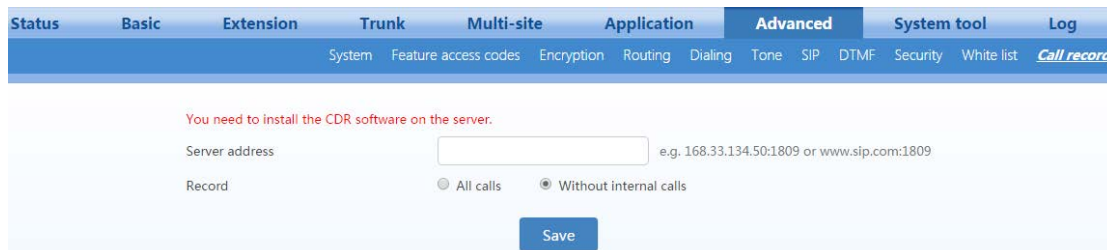
3.8.12 Call-Detail Record (CDR)

The OM20/50 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 CDRs 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 3-63 CDR server interface



3.8.13 API

The OM20/50 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 3-64 API configuration interface

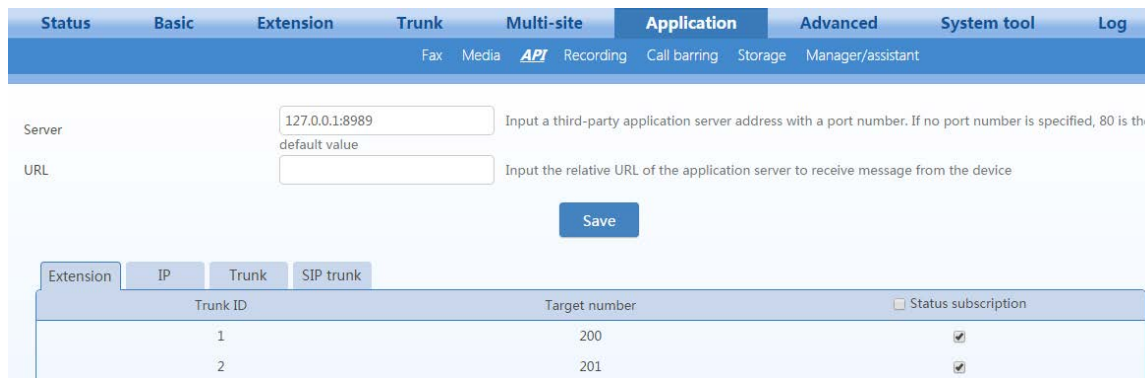


Table 3-37 API parameters

Item	Description
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.
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.

3.8.14 SIP Transmission Mode

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

Figure 3-65 SIP transmission mode setting interface

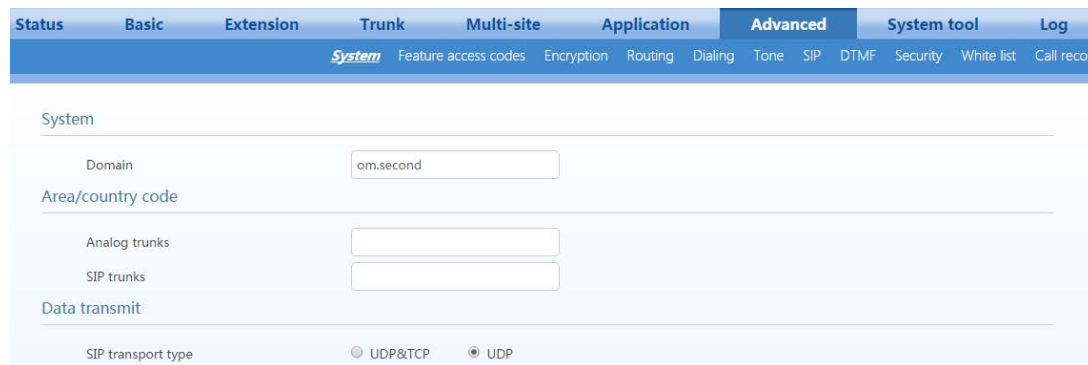


Table 3-38 SIP transmission mode parameters

Item	Description
SIP transmission type	Select either UDP or TCP for SIP messages. The default is UDP. Both sides must select the same transmission protocol.
TCP-based local SIP port	Local SIP port used when TCP is used.

3.8.15 Auto Provision

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 3-66 Auto provision interface

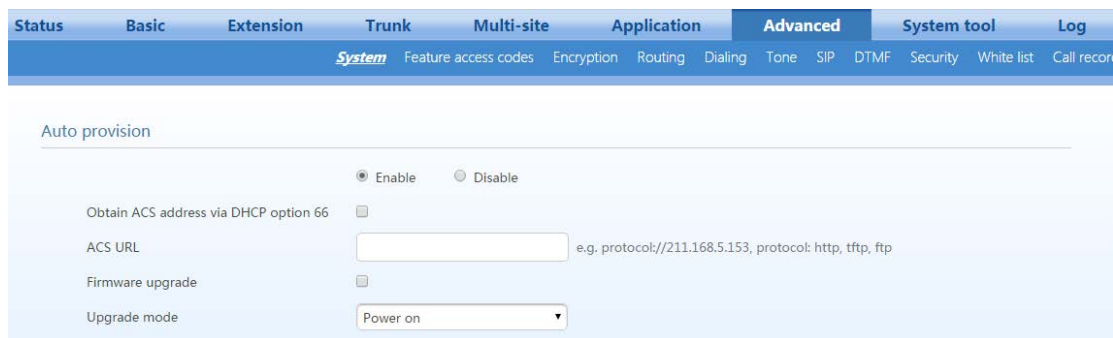


Table 3-39 Auto provision parameters

Item	Description
Obtain ACS address via DHCP option 66	ACS (Auto Provisioning Server) address is obtained by using option 66 of the DHCP
ACS URL	Manually configure the ACS address, which can be an TFTP, FTP, or HTTP server. <ul style="list-style-type: none"> • tftp://ACS address • ftp:// ACS address • http:// ACS address
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.
Update mode	<ul style="list-style-type: none"> • Power on: The device detects whether there are configurations and firmware to be updated when the device is powered on. • Power on + Periodically: 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.

3.8.16 TR069

From Wikipedia, the free encyclopedia

TR-069 (Technical Report 069) is a technical specification that defines an [application-layer](#) protocol for remote management of end-user devices. It was published by the [Broadband Forum](#) and entitled [CPE WAN-Management Protocol](#) (CWMP).

As a bidirectional [SOAP/HTTP](#)-based protocol, it provides the communication between [customer-premises equipment](#) (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE-management functions within an integrated framework. The protocol addresses the growing number of different [Internet-access](#) devices, such as [modems](#), [routers](#), and [gateways](#), as well as end-user devices that connect to the Internet, such as [set-top boxes](#) and [VoIP-phones](#). The TR-069 standard was developed for automatic configuration and management of these devices by Auto Configuration Servers (ACS). The technical specifications are managed and published by the [Broadband Forum](#). TR-069 was first published in May 2004, with amendments in 2006, 2007, 2010, July 2011 to version 1.3, and November 2013 to version 1.4.

Other forums, such as the [Home Gateway Initiative](#) (HGI), [Digital Video Broadcasting](#) (DVB) and [WiMAX Forum](#), endorsed CWMP as the protocol for remote management of home-network devices and terminals (such as the DVB-IPTV set-top box). There is a growing trend to add TR-069 management functionality to home networking devices behind the gateway, as well as many other access devices like M2M, FTTH CPE/ONTs, WIMAX CPE and other carrier-access equipment.

Go to **Advanced > System**.

Figure 3-67 TR069 interface

Table 3-40 TR069 parameters

Item	Description
server	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.

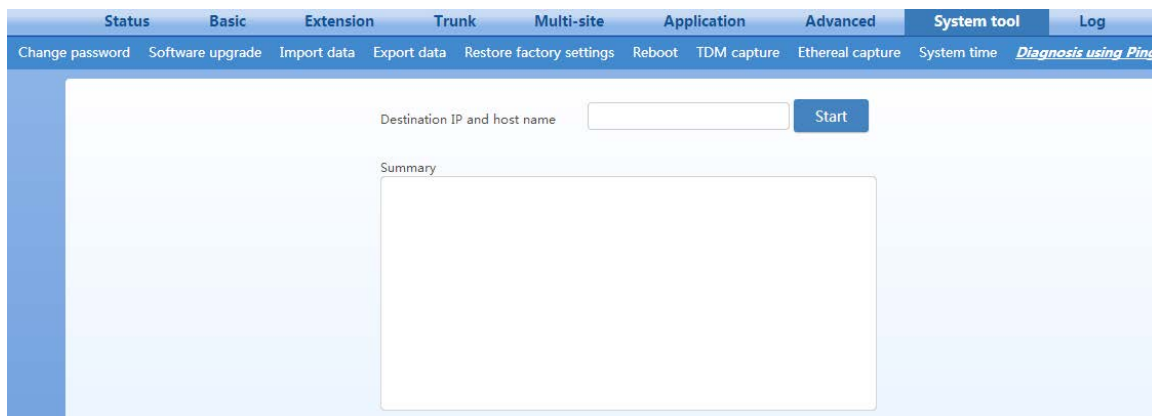
Item	Description
Connection request password	The password used for the network-management server to connect back to the device.

3.8.17 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 3-68 Ping diagnosis interface



3.9 Security management

3.9.1 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 3-69 Whitelist interface

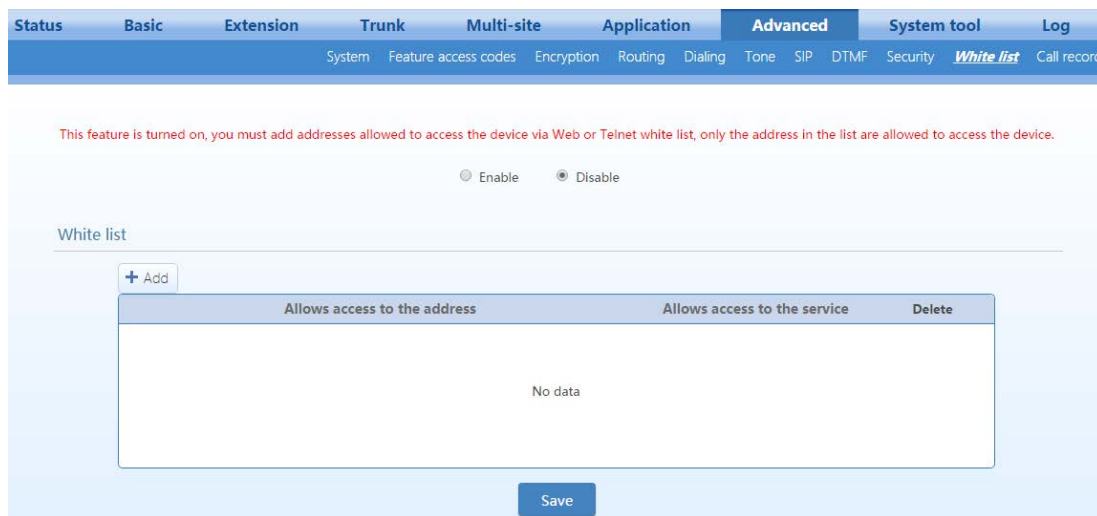


Table 3-41 Whitelist parameters

Item	Description
Allows access to the address	Enter the IP address allowed to access the OM in the “Allows access to the address” text box.
Allows access to the service	Select services that can be accessed, such as Telnet, SSH, and HTTP.
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?

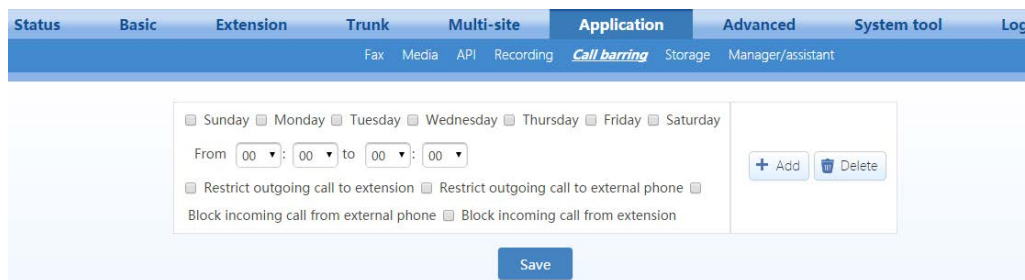
3.9.2 Outbound Call Screening

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 3-70 Outbound call screening interface



Step 2 Click **Save**.

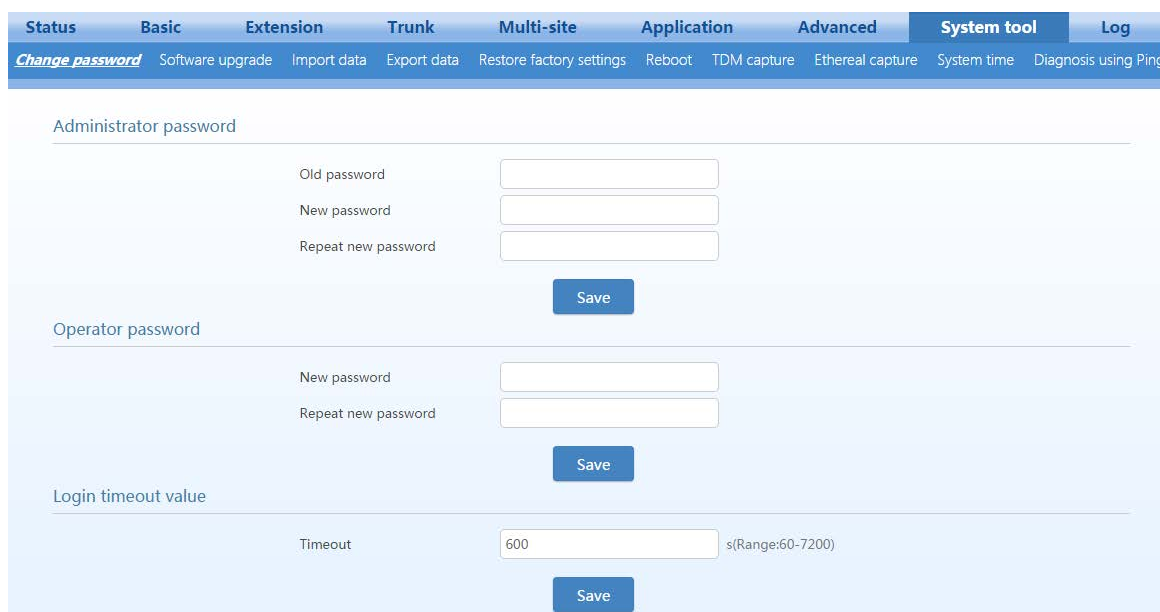
Step 3 Go to **Extension > Analog/IP > Set**, and select the **Call restriction** function of the extension.

Step 4 Click **Save**.

3.9.3 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 3-71 Password interface

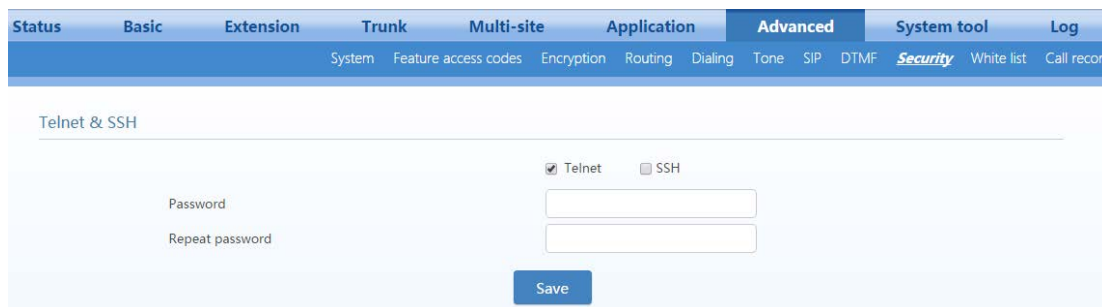


3.9.4 Telnet & SSH

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 3-72 Telnet & SSH setting interface

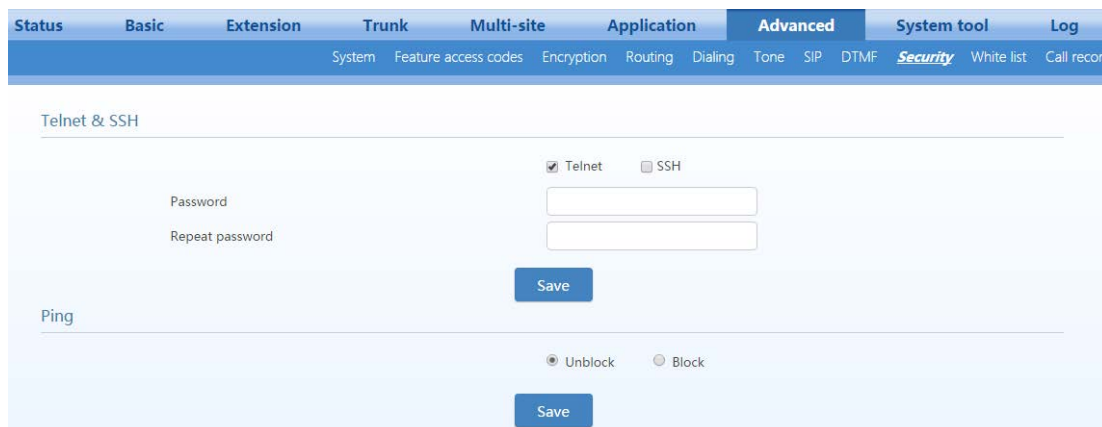


3.9.5 Ping Blocking

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 3-73 Ping blocking/unblocking interface



3.9.6 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 3-74 Web-management interface

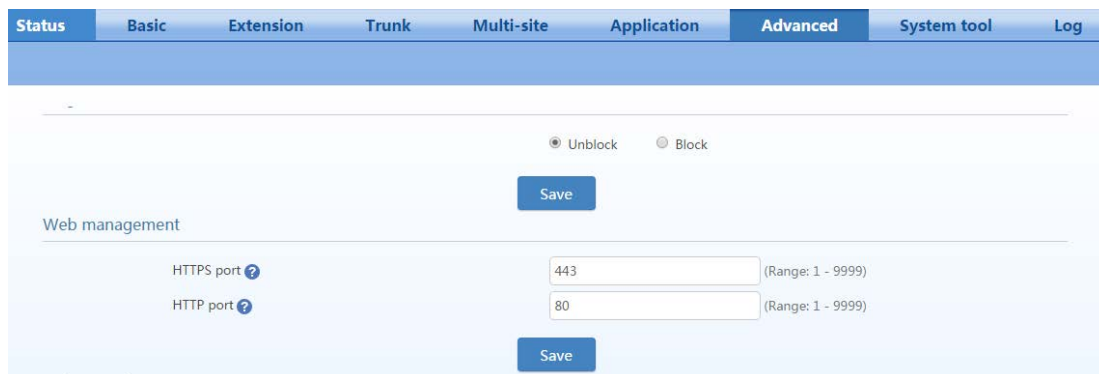


Table 3-42 Web-management parameters

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.
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.

3.9.7 Voice Security

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

Figure 3-75 Voice security interface

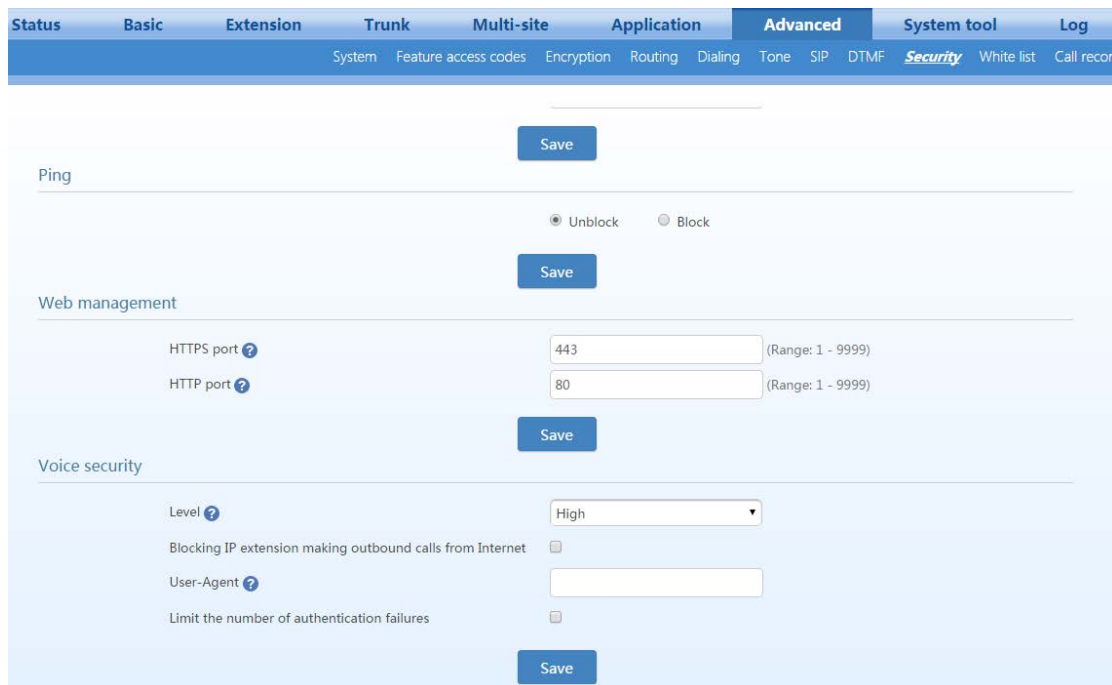


Table 3-43 Voice security parameters

Item	Description
Level	<p>The security levels are described as follows:</p> <ul style="list-style-type: none"> • 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.
Blocking IP extension making outboard calls from Internet	An IP extension in an external network is only allowed to call extensions.
User-Agent header	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.
Block the registrar after	Set the threshold for the authentication failures of an IP extension. The value is 1 to 99, and the default value is 5. Note: This parameter can be set only when Limit the number of authentication failures is selected.

3.10 Maintenance

3.10.1 Software Upgrading

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

Step 1 Go to **System tool > Software upgrade**, and locate and upload the upgrade file (the upgrade file can be directly uploaded without being decompressed).

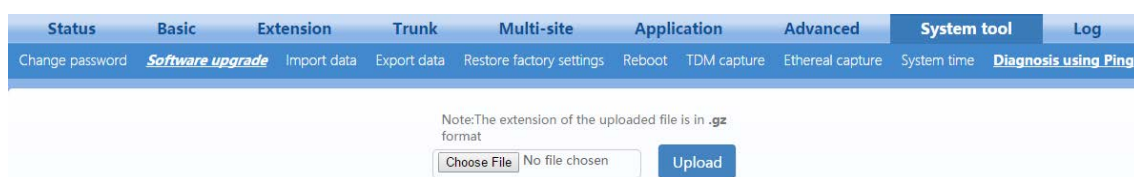
Step 2 Click **Browse** to select the upgrade package.

Step 3 Click **Upload** to upload the package to the system.

Step 4 After the upgrade package is uploaded, follow the upgrade instructions.

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

Figure 3-76 Software upgrade interface





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.

3.10.2 Configuration Maintenance

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

Figure 3-77 Data importing interface

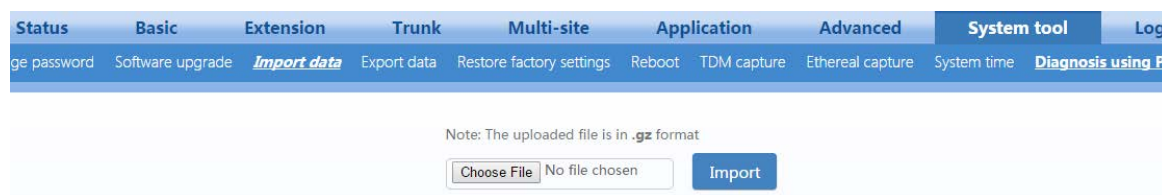


Figure 3-78 Data-export interface

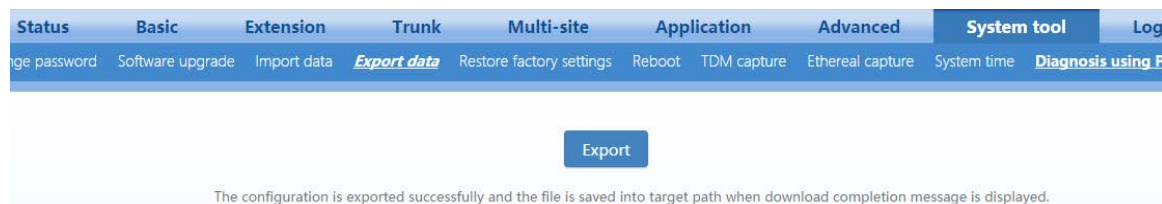


Figure 3-79 Restore Factory Settings interface



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.

3.10.3 Rebooting

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

Figure 3-80 Rebooting interface

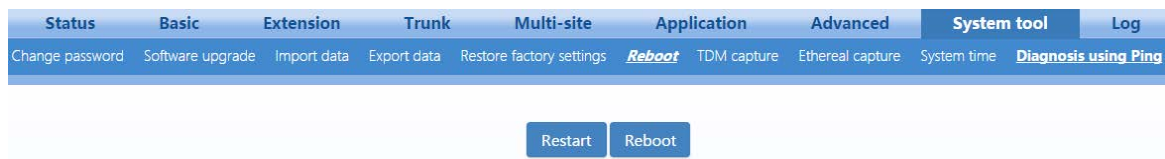


Table 3-44 System-reboot interface

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.

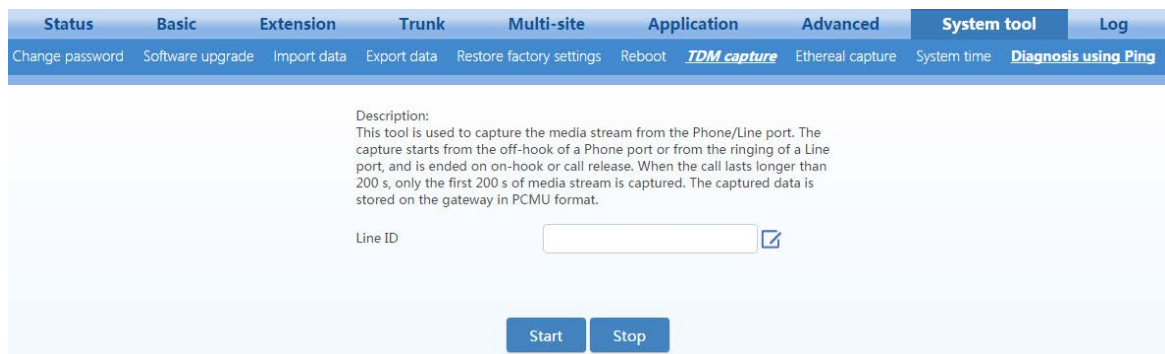
3.10.4 Port Capture

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 WROC2000 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 3-81 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.

3.10.5 Ethereal Captures

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. 2-MB in size can be captured. Files will be saved as dump.cap in WROC2000 and click STOP to finish the capturing and download these files. The file will not be stored in WROC after downloading.

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

Figure 3-82 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.

3.10.6 Log Management

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

Log files stored inside the device contain only the latest log information. To collect an entire log you may need to use an external log server.

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

Figure 3-83 Log-management interface

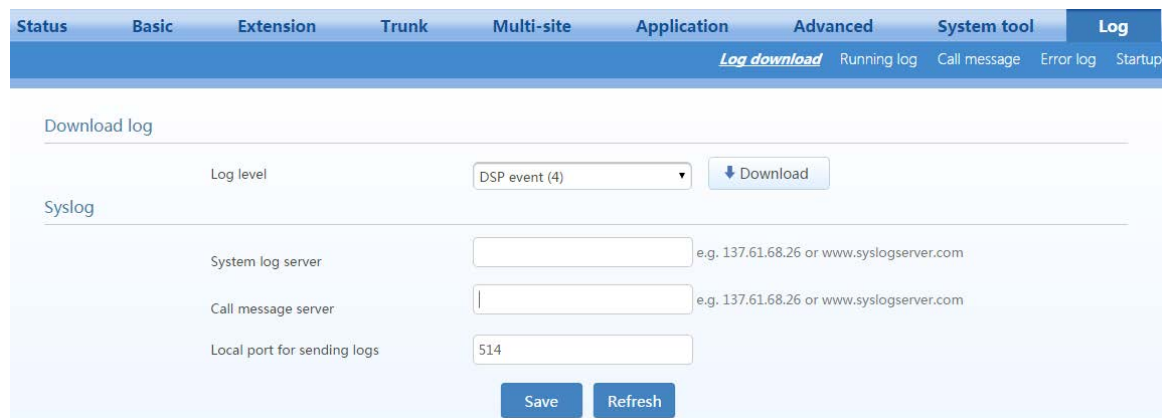


Table 3-45 Log-management parameters

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 support@NetGenCommunications.com or attach it to your trouble ticket at dev.NetGenCommunications.com.

3.10.7 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 3-84 Runtime Log Interface

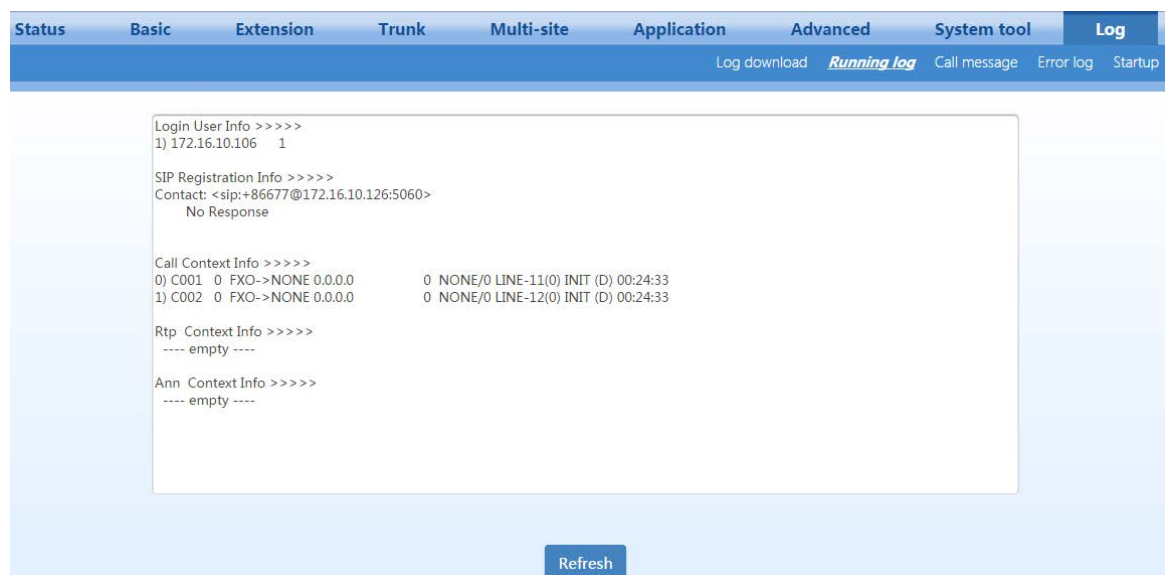


Table 3-46 Runtime log parameters

Item	Description
Login User Info	Displays the IP address that currently accesses the Web GUI and its operation privilege: <ul style="list-style-type: none"> • 1: administrator • 2: operator • 3: Read only
SIP Registration Info	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Shows the call status.
RTP Context Info	<ul style="list-style-type: none"> • Shows the voice channel related to the calls.
Ann Context Info	<ul style="list-style-type: none"> • Displays IVR file resources.

3.11 View Runtime Information

3.11.1 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 3-85 Running status interface



3.11.2 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 3-86 Alarm interface

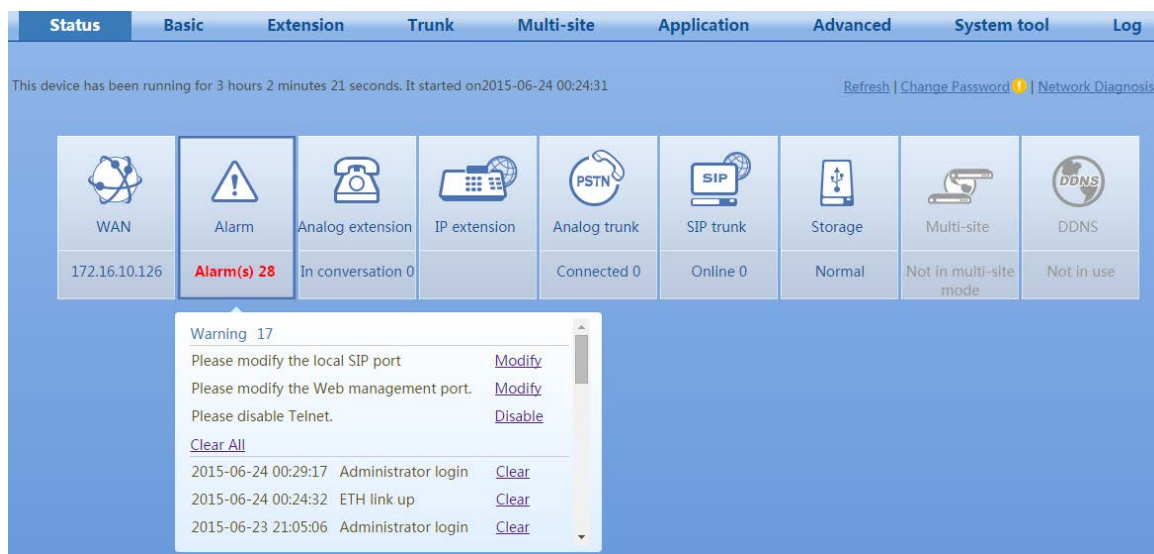


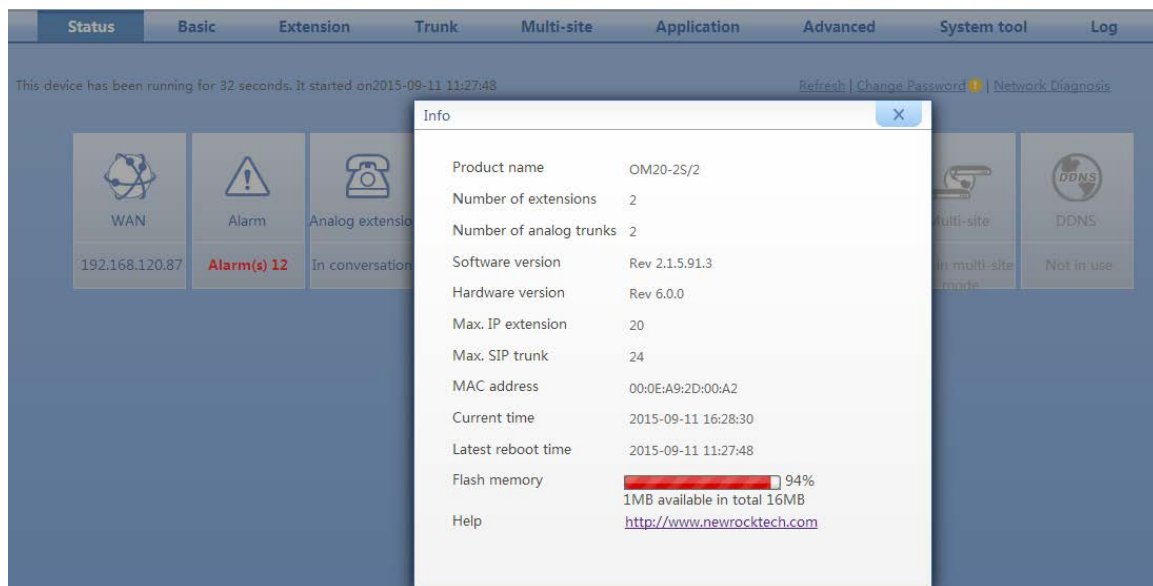
Table 3-47 Classification of alarm messages

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

3.11.3 Product Information

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

Figure 3-87 Product information interface

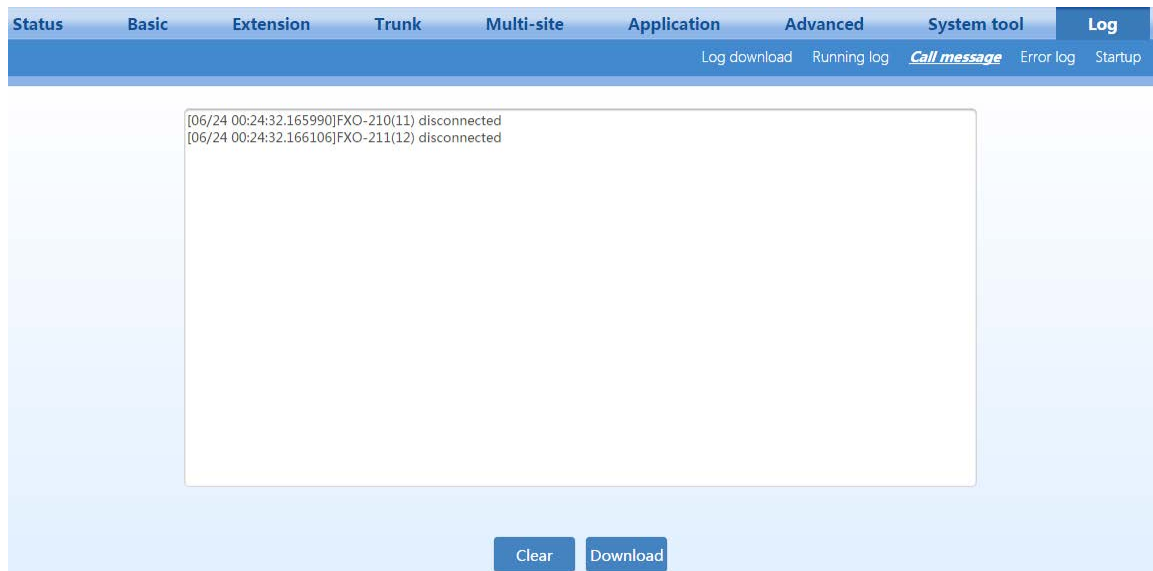


3.11.4 Call Messages

You can use call messages to locate a call problem. A call message is...

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

Figure 3-88 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 support@NetGenCommunications.com or attach it to your trouble ticket at dev.NetGenCommunications.com

3.12 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 3-48 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 calls.
Zibo accounting software	Provides functions such as call accounting, toll settings, real-time call details record queries, and report printing.

4 FAQs

4.1 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.

4.2 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 4-1 Solutions to IP trunk registration failures

Displayed Content	Registration Status	Solution
SIP Registration Info >>>>> Contact:< sip:61208000@192.168.250.5:50 60 > 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.

4.3 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.

4.4 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.

4.5 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.

4.6 Low Volume on an Extension

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

Solution:

Table 4-2 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 .

4.7 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.

4.8 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.

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

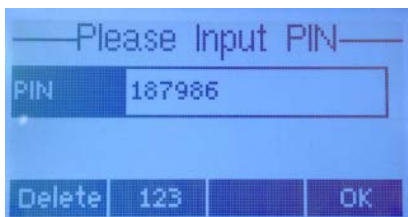
The OM provides the embedded white-listed address of 192.168.2.100 upon factory delivery. When the Whitelist function is enabled, if you forget the whitelisted IP address previously set, the following steps can be performed for recovery.

- 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 4-1 SIP Phone registration interface

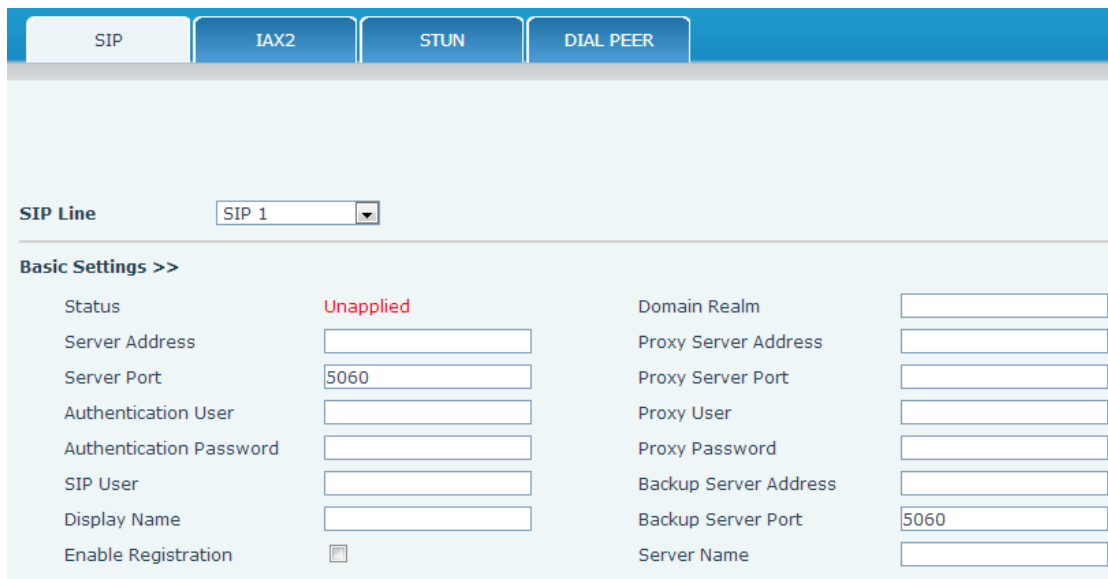


Table 4-3 SIP Phone registration parameters

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.

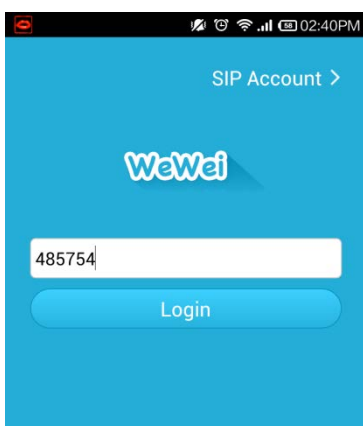


Note

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 4-2 X-Lite login interface

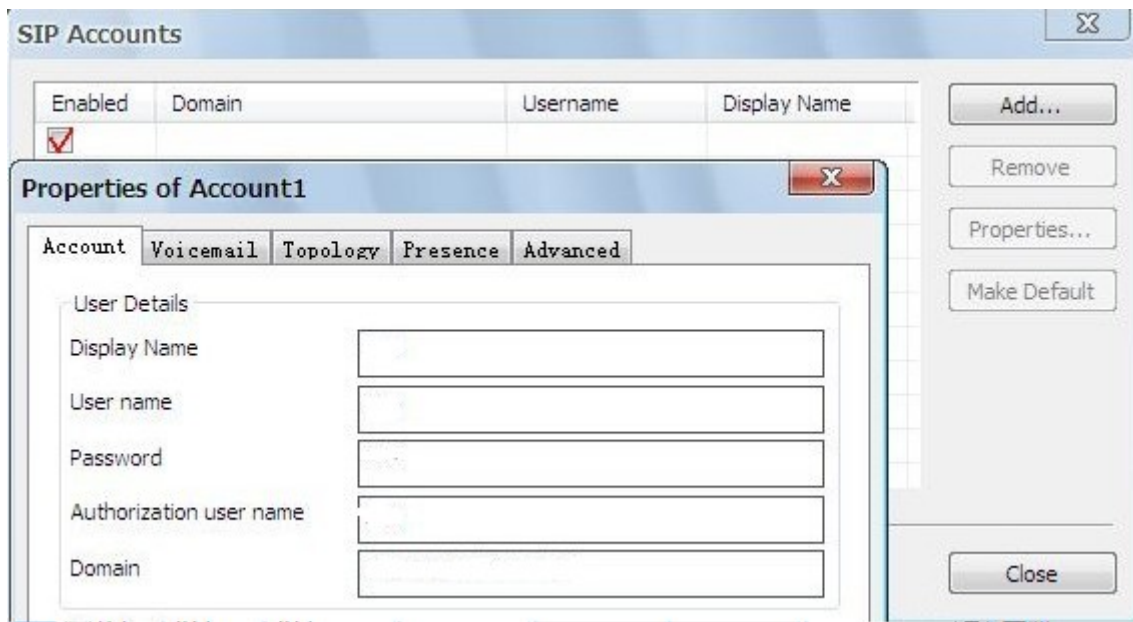


Figure 4-3 X-Lite registration interface

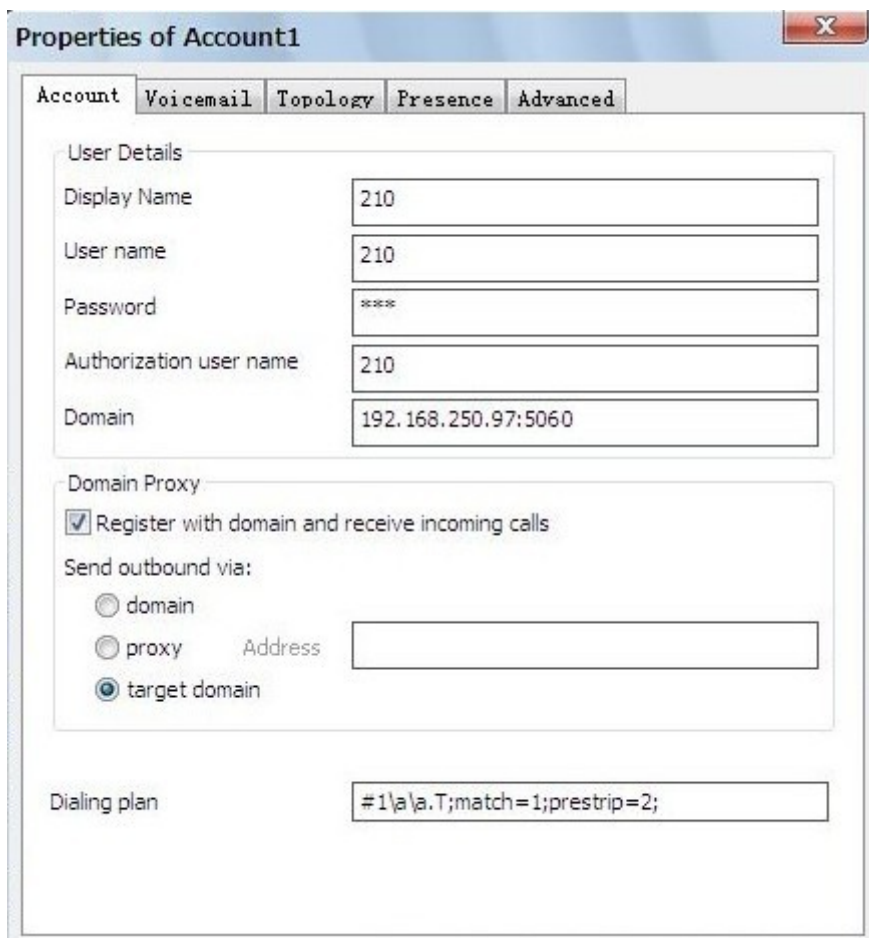


Table 4-4 SIP Phone registration parameters

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.