Grandstream Networks, Inc.

UCM630x Series - User Manual

UCM630x Series - User Manual

Thank you for purchasing the Grandstream UCM630X series IP PBX appliance. The UCM6300 series allows businesses to build powerful and scalable unified communication and collaboration solutions. This series of IP PBXs provide a platform that unifies all business communication on one centralized network, including voice, video calling, video conferencing, video surveillance, web meetings, data, analytics, mobility, facility access, intercoms, and more. The UCM6300 Series supports up to 3000 users and includes a built-in web meetings and video conferencing solution that allows employees to connect from the desktop, mobile, GVC series devices, and IP phones. It can be paired with the UCM6300 ecosystem to offer a hybrid platform that combines the control of an on-premises IP PBX with the remote access of a cloud solution. The UCM6300 ecosystem consists of the Wave app for desktop and mobile, which provides a hub for collaborating remotely, and UCM RemoteConnect, a cloud NAT traversal service for ensuring secure remote connections. The UCM6300 series also offers cloud setup and management through GDMS and an API for integration with third-party platforms. By offering a high-end unified communications and collaboration solution packed with a suite of mobility, security, meeting, and collaboration tools, the UCM6300 series provides a powerful platform for any organization.

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Please do not use a different power adaptor with the UCM630X as it may cause damage to the product and void the manufacturer warranty.

Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

PRODUCT OVERVIEW

Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings for the UCM630X series.

Interfaces	
Analog Telephone FXS Ports	UCM6301: 1 RJ11 port UCM6302: 2 RJ11 ports UCM6304: 4 RJ11 ports UCM6308: 8 RJ11 ports All ports have lifeline capability in case of a power outage; number of ports can be expanded by peering an FXS gateway
PSTN Line FXO Ports	UCM6301: 1 RJ11 port UCM6302: 2 RJ11 ports UCM6304: 4 RJ11 ports UCM6308: 8 RJ11 ports All ports have lifeline capability in case of a power outage; number of ports can be expanded by peering with an FXO gateway
Network Interfaces	Three self-adaptive Gigabit ports (switched, routed, or dual card mode) with PoE+
NAT Router	Yes (supports router mode and switch mode)
Peripheral Ports	UCM6301: 1x USB 3.0, and 1x SD card interface UCM6302: 1x USB 2.0, 1x USB 3.0, and 1x SD card interface UCM6304/6308: 2x USB 3.0 and 1x SD card interface
LED Indicators	UCM6301/UCM6302: None UCM6304/6308: Power 1/2, FXS, FXO, LAN, WAN, Heartbeat

LCD Display	UCM6301/UCM6302: 320*240 LCD with touch screen for Shortcut Keys and Scroll Bar UCM6304/6308: 128x32 dot matrix graphic LCD with DOWN and OK buttons
Reset Switch	Yes, long press for factory reset and short press for reboot
Voice/Video Capabilities	
Voice-over-PacketCapabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711, NetEQ, FEC 2.0, jitter resilience up to 50% audio packet loss
Voice and Fax Codecs	Opus, G.711 A-law/U-law, G.722, G722.1 G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38
Video Codecs	H.264, H.263, H263+, VP8
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Signaling and Control	
DTMF Methods	Inband, RFC4733, and SIP INFO
Provisioning Protocol andPlug-and-Play	Mass provisioning using AES encrypted XML configuration file, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66 multicast SIP SUBSCRIBE mDNS), eventlist between the local and remote trunk
Network Protocols	SIP, TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay (pending), IPv6, OpenVPN(R)
API	Full API available for third-party platform and application integration
Disconnect Methods	Busy/Congestion/Howl Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect
Security	
Media Encryption	SRTP, TLS1.2, HTTPS, SSH, 802.1x
Physical	
Universal Power Supply	UCM6301/6302: Input: 100 ~ 240VAC, 50/60Hz; Output: DC 12V, 1.5A UCM6304/6308: Input: 100~240VAC,50/60Hz; Output: DC 12V, 2A
Dimensions	UCM6301/6302: 270mm(L) x 175mm(W) x 36mm(H) UCM6304/6308: 485mm(L) x 187.2mm(W) x 46.2mm(H)
Temperature & Humidity	Operating: 32 - 113oF / 0 ~ 45oC, Humidity 10 - 90% (non-condensing) Storage: 14 - 140oF / -10 ~ 60oC, Humidity 10 - 90% (non-condensing)
Mounting	UCM6301/6302: Wall mount and desktop UCM6304/6308: Rack mount and desktop
Weight	UCM6301: Unit weight 715g, Package weight 1211g UCM6302: Unit weight 725g, Package weight 1221g UCM6304: Unit weight 2490g, Package weight 3260g UCM6308: Unit weight 2550g, Package weight 3320g
Additional Features	
Multi-language Support	Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech, Turkish Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Polish, Portuguese, Russian, Swedish, Turkish, Ukrainian, Hebrew, Arabic, Nederlands Customizable language pack to support any other languages
Caller ID	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 - BT, NTT
Polarity Reversal/ Wink	Yes, with enable/disable option upon call establishment and termination
Call Center	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/workload, in-queue announcement

Customizable Auto Attendant	Up to 5 layers of IVR (Interactive Voice Response) in multiple languages
Telephony Operating System	Based on Asterisk version 16
Maximum Call Capacity	UCM6301: Users: 500 Concurrent calls (G.711): 75 Max concurrent SRTP calls (G.711): 50 UCM6302: Users: 1000 Concurrent calls (G.711): 150 Max concurrent SRTP calls (G.711): 100 UCM6304: Users: 2000 Concurrent calls (G.711): 300 Max concurrent SRTP calls (G.711): 200 UCM6308: Users: 3000 Concurrent calls (G.711): 450 Max concurrent SRTP calls (G.711): 300
Maximum Attendees of Conference Bridges	UCM6301: Up to 4 simultaneous video conference rooms, up to 75 simultaneous participants in all rooms combined, up to 9 video feeds in all the conference rooms UCM6302: Up to 8 simultaneous video conference rooms, up to 150 simultaneous participants in all rooms combined, up to 9 video feeds in all conference rooms UCM6304: Up to 15 simultaneous video conference rooms, up to 200 simultaneous participants in all rooms combined, up to 9 video feeds in all conference rooms UCM6308: Up to 25 simultaneous video conference rooms, up to 300 simultaneous participants in all rooms combined, up to 9 video feeds in all conference rooms.
Call Features	Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, fax to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice conference, video conference, eventlist, feature codes, busy camp-on/ call completion, voice control, post-meeting reports, virtual fax sending/receiving, email to fax
Wave App	Free; Available for desktop (Windows 10+, Mac OS 10+), web (Firefox and Chrome Browsers) and mobile (Android & iOS), allows users to join UCM-hosted meetings, communicate with other users/solutions and make/receive calls using SIP accounts registered to a UCM6300 Audio series IP PBX
Firmware Upgrade	Supported by Grandstream Device Management System (GDMS), a zero-touch cloud provisioning and management system, It provides a centralized interface to provision, manage, monitor, and troubleshoot Grandstream products
Internet Protocol Standards	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028. RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 4582, RFC 4583, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550
Compliance	FCC: Part 15 (CFR 47) Class B, Part 68 CE: EN 55032, EN 55035, EN61000-3-2, EN61000-3-3, EN 62368.1, ES 203 021, ITU K.21 IC: ICES-003, CS-03 Part I Issue 9 RCM: AS/NZS CISPR 32, AS/NZS 62368.1, AS/CA S002, AS/CA S003.1/.2 Power adapter: UL 60950-1 or UL 62368-1

Technical Specifications

UCM630X FXS ports lifeline functionality: The UCM630X FXS interfaces are metallic through to the FXO interfaces. If there is a power outage, the FXS1 port will fail over to FXO 1 port, FXS 2 port will fail over to FXO 2 port. The user can still access the PSTN connected with the FXO interfaces from FXS interfaces.

INSTALLATION

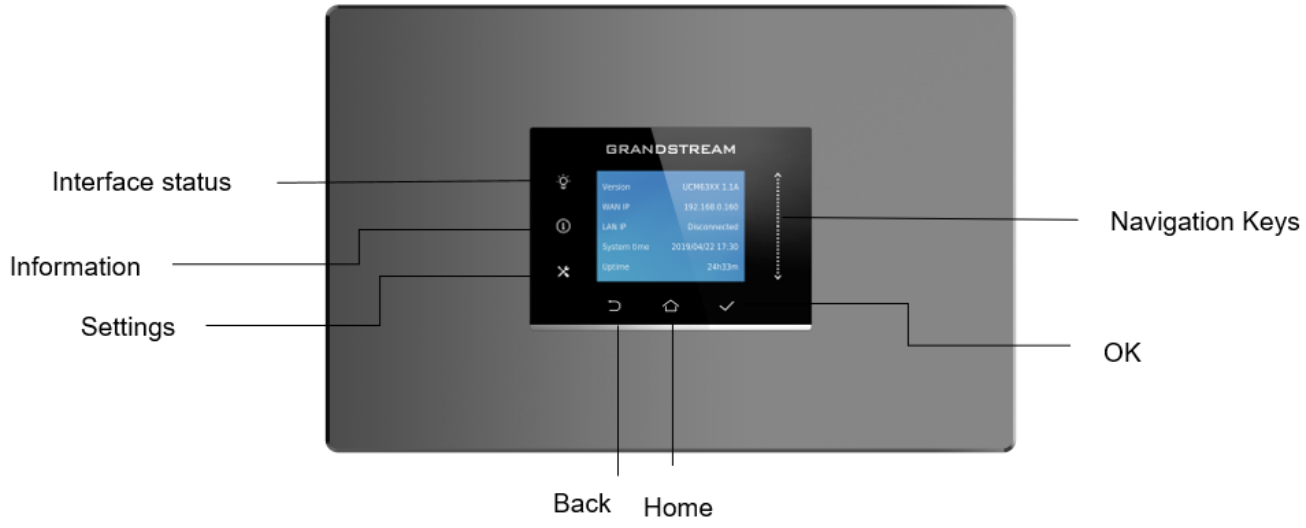
Before deploying and configuring the UCM630X series, the device needs to be properly powered up and connected to a network. This section describes detailed information on the installation, connection, and warranty policy of the UCM630X series.

Equipment Packaging

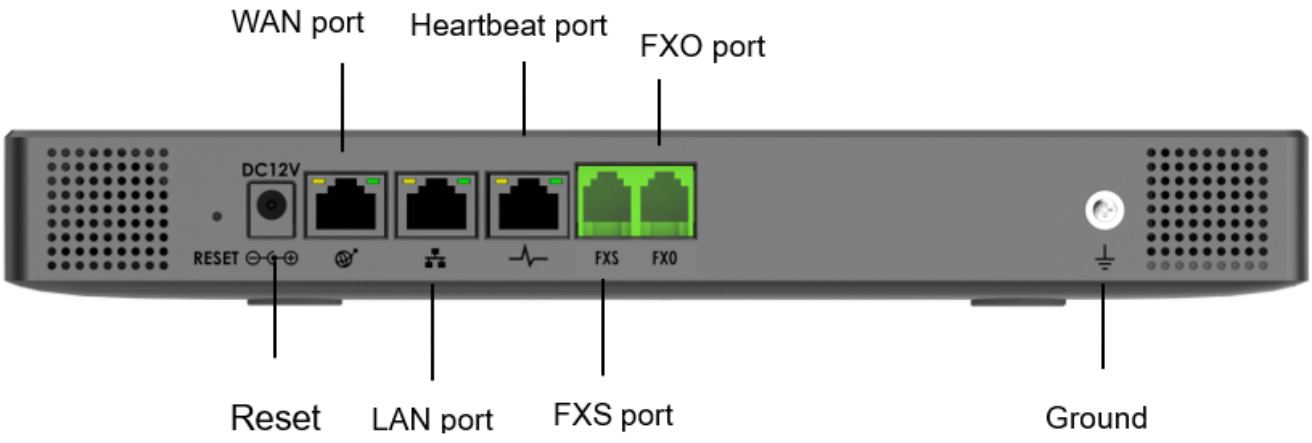
Main Case	1
Power Adaptor	1
Ethernet Cable	1
Quick Installation Guide	1

UCM630X Equipment Packaging

Connect Your UCM630X (UCM6301 as an example)



UCM6301 Top View



UCM6301 Back View



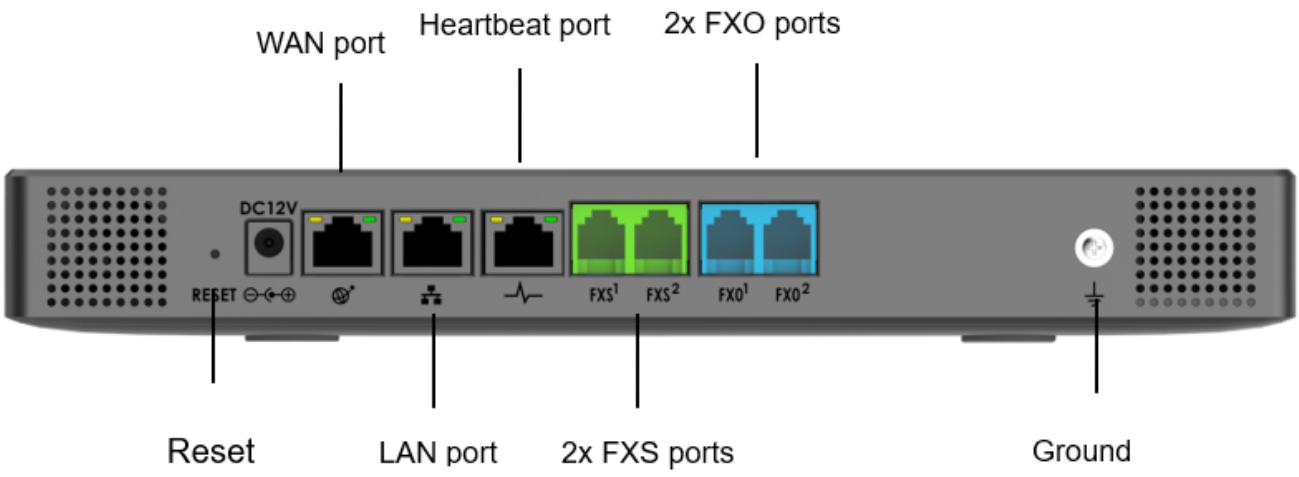
UCM6301 Front View

To set up the UCM6301, follow the steps below:

1. Connect one end of an RJ-45 Ethernet cable into the WAN port of the UCM6301.
2. Connect the other end of the Ethernet cable into the uplink port of an Ethernet switch/hub.
3. Connect the 12V DC power adapter into the 12V DC power jack on the back of the UCM6301. Insert the main plug of the power adapter into a surge-protected power outlet.
4. Wait for the UCM6301 to boot up. The LCD in the front will show the device hardware information when the boot process is done.
5. Once the UCM6301 is successfully connected to the network, press the Home button to display the IP address.
6. (Optional) Connect PSTN lines from the wall jack to the FXO ports; connect analog lines (phone and Fax) to the FXS ports.

- The ground screw needs to be connected.
- The same steps will be used to connect UCM6302/6304/6308.

UCM6302 front and back view

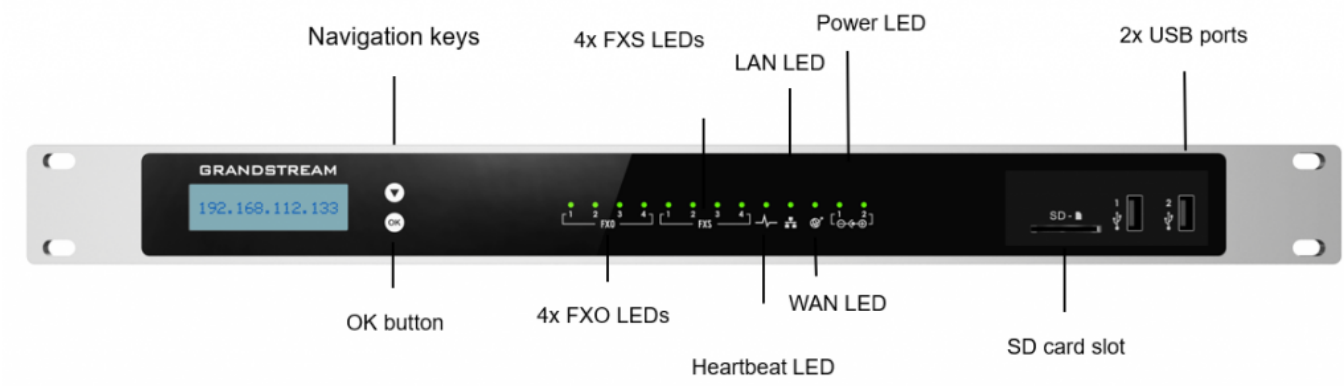


UCM6302 Back View

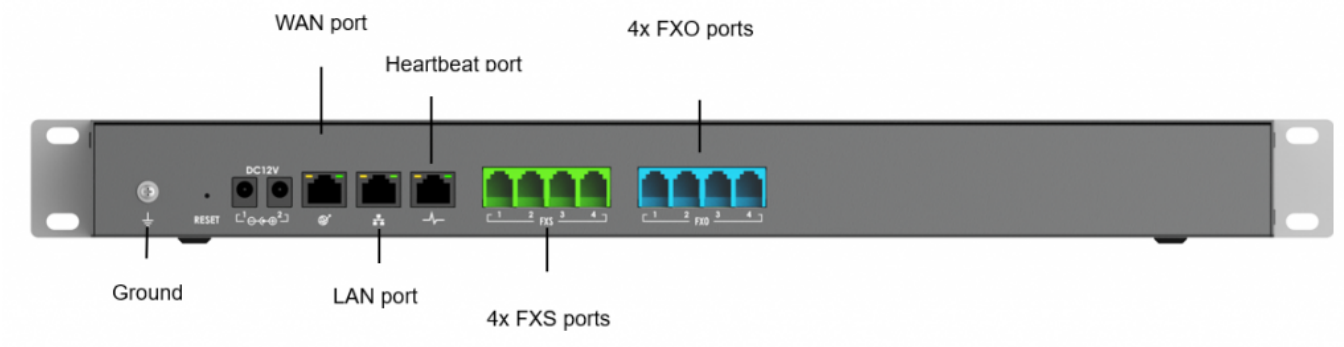


UCM6302 Front View

UCM6304 front and back view

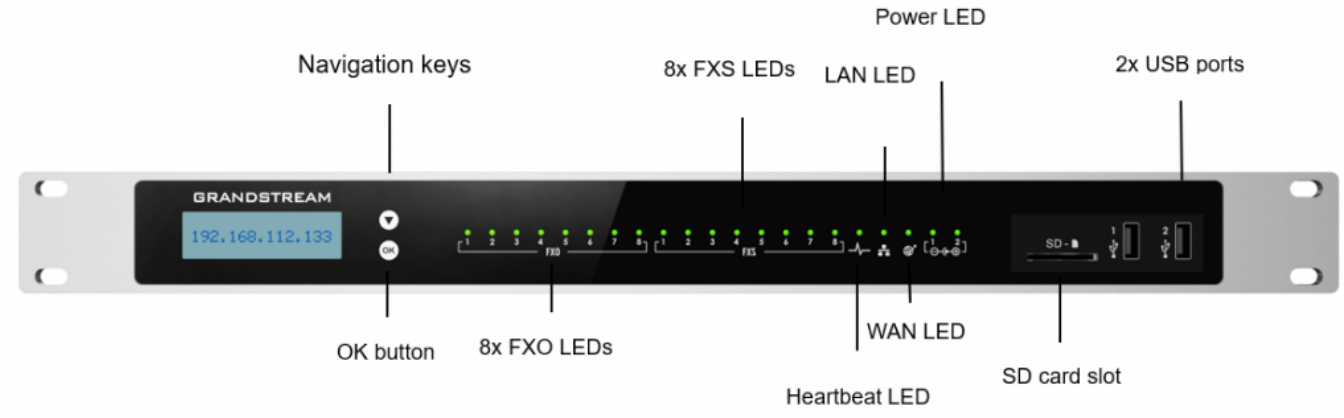


UCM6304 Front View

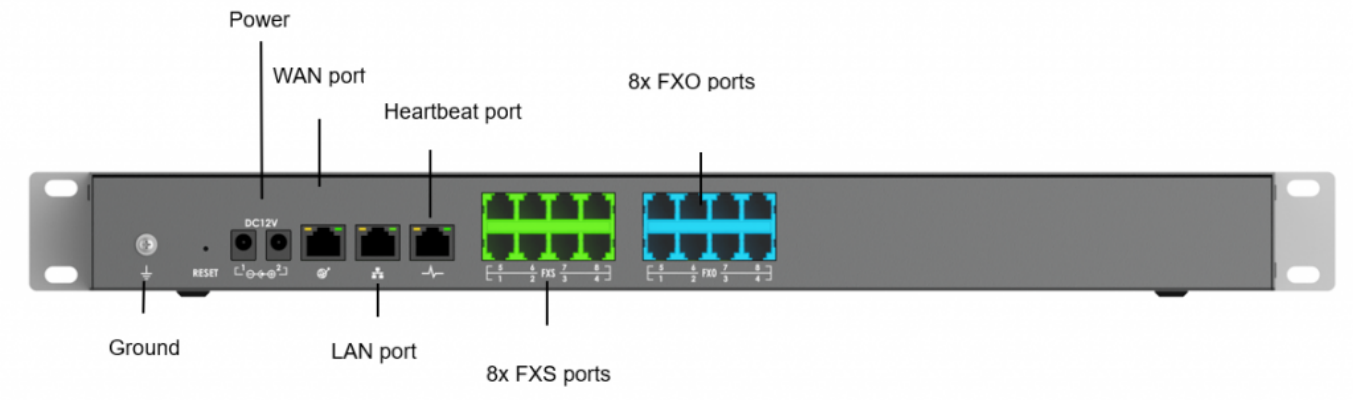


UCM6304 Back View

UCM6308 front and back view



UCM6308 Front View



UCM6308 Back View

The UCM630X series IP PBX complies with FCC/CE and various safety standards. The UCM630X power adapter is compliant with the UL standard. Use the universal power adapter provided with the UCM630X package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

If the UCM630X series IP PBX was purchased from a reseller, please contact the company where the device was purchased for replacement, repair, or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

Use the power adapter provided with the UCM630X series IP PBX. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.

GETTING STARTED

To get started with the UCM630X setup process, use the following available interfaces: LCD display, and web portal.

- The LCD display shows hardware, software, interface status, and network information and can be navigated via the Slide control and Touch keys. From here, users can configure basic network settings, run diagnostic tests, and factory reset.
- The web portal (may also be referred to as web UI in this guide) is the primary method of configuring the UCM.

This section will provide step-by-step instructions on how to use these interfaces to quickly set up the UCM and start making and receiving calls with it.

Use the LCD Menu

- **Idle Screen**

Once the device has booted up completely, the LCD will show the UCM model, hardware version, and IP address. Upon menu key press timeout (30 seconds), the screen will default back to this information.

- **Menu**

Pressing the Home button will show the main menu. All available menu options are found in [LCD Menu Options].

- **Menu Navigation**

Scrolling down using slide control through the menu options. Press the OK button to select an option.

- **Exit**

Selecting the Back option will return to the previous menu. For the Device Info, Network Info, and Web Info screens that have no Back option, pressing the OK button will return to the previous menu.

- **LCD Backlight**

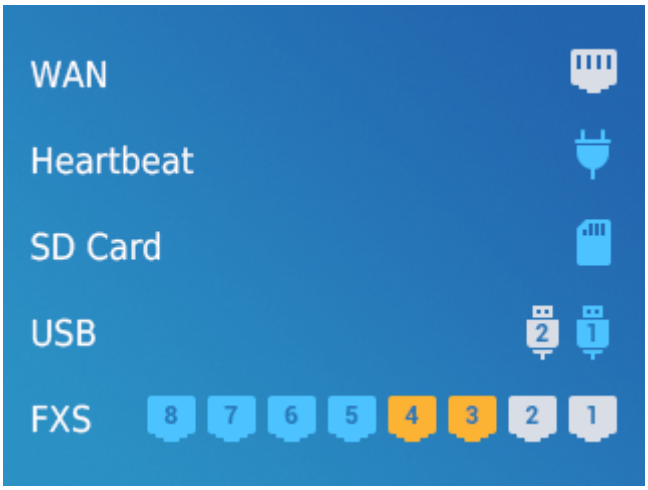
The LCD backlight will turn on upon button press and will go off when idle for 30 seconds.

The following table summarizes the layout of the LCD menu of UCM630x.

View Events	Critical Events Other Events
Device Info	Hardware: Hardware version number Software: Software version number P/N: Part number WAN MAC: WAN side MAC address LAN MAC: LAN side MAC address Uptime: System uptime
Network Info	WAN Mode: DHCP, Static IP, or PPPoE WAN IP: IP address WAN Subnet Mask LAN IP: IP address LAN Subnet Mask
Network Menu	WAN Mode: Select WAN mode as DHCP, Static IP, or PPPoE Static Route Reset: Select this to reset static route settings.
Factory Menu	Reboot Factory Reset LCD Test Patterns: Press DOWN and OK buttons to scroll through and select different LCD patterns to test. Once a test is done, press the OK button to return to the previous menu. Fan Mode: Select Auto or On. LED Test Patterns: All On, All Off, and Blinking are the available options. Selecting Back in the menu will revert the LED indicators to their actual status. RTC Test Patterns: Select either 2022-02-22 22:22 or 2011-01-11 11:11 to start the RTC (Real-Time Clock) test pattern. Check the system time from either the LCD idle screen or in the web portal System Status?System Information?General page. To revert to the correct time, manually reboot the device. Hardware Testing: Select Test SVIP to verify hardware connections within the device. The result will display on the LCD when the test is complete.
Web Info	Protocol: Web access protocol (HTTP/ HTTPS). HTTPS is used by default. Port: Web access port number, which is 8089 by default.
SSH Switch	Enable SSH Disable SSH SSH access is disabled by default

Use the LED Indicators

The UCM6301/6302 has LED indicators on the network port to display connection status and the following picture shows the other ports' status.



Ports Status

The UCM6304/6308 has LED indicators in the front to display the connection status. The following table shows the status definitions.

LED Indicator	LED Status
Power 1/Power 2 PoE LAN WAN USB SD FXS ports FXO ports	Solid: Connected Fast Blinking: Data Transferring Slow Blinking: Trying to connect OFF: Not Connected

UCM6304/6308 LED Indicators

Using the Web UI

Accessing the Web UI

The UCM's web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a web browser such as Microsoft IE (version 8+), Mozilla Firefox, Google Chrome, etc. To access the UCM's web portal, follow the steps below:



UCM6302 Web GUI Login Page

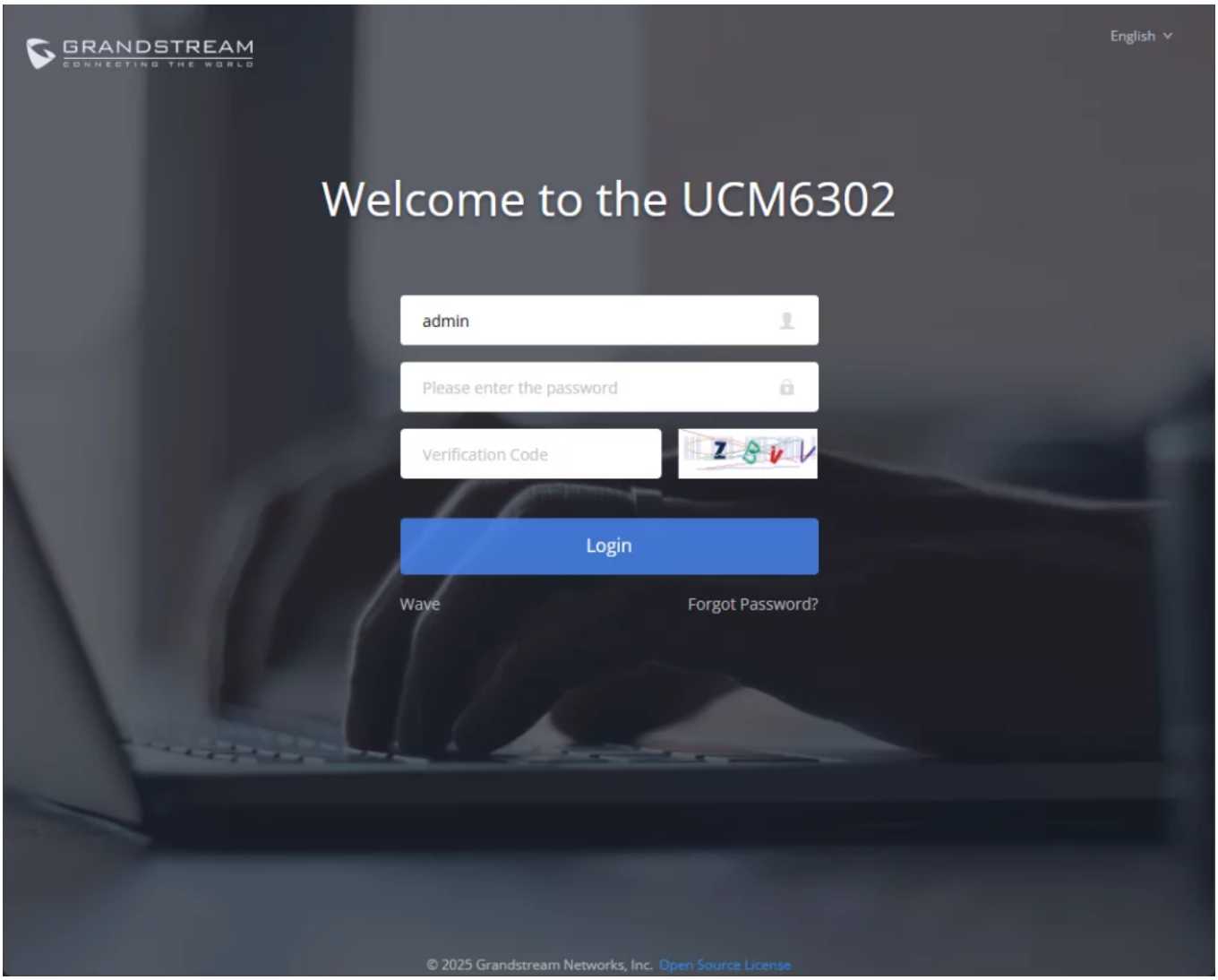
1. Make sure your computer is on the same network as the UCM.
2. Make sure that the UCM's IP address is displayed on its LCD.
3. Enter the UCM's IP address into a web browsers' address bar. The login page should appear (please see the above image).
4. Enter default administrator username "admin" and password can be found on the sticker at the back of the UCM.

By default, the UCM630X has **Redirect From Port 80** enabled. As such, if users type in the UCM630X IP address in the web browser, the web page will be automatically redirected to the page using HTTPS and port 8089. For example, if the LCD shows 192.168.40.167, and 192.168.40.167 is entered into the web browser, the web page will be redirected to: https://192.168.40.167:8089

The option **Redirect From Port 80** can be found under the UCM630X **System Settings** > **HTTP Server**.

Login Failed Attempt

If the user enters a wrong username or password, they will be prompted to resolve a captcha. To resolve the captcha, enter the characters shown in the image.



Captchas are not case sensitive, therefore, there is no need to consider whether the letters need to be upper case or lower case.

Setup Wizard

When you log in to the UCM Web GUI interface for the first time, the system will automatically start the setup wizard and expand the description of the instant messaging soft terminal supporting system (Wave). Click "Learn more" to open the Wave client download interface.



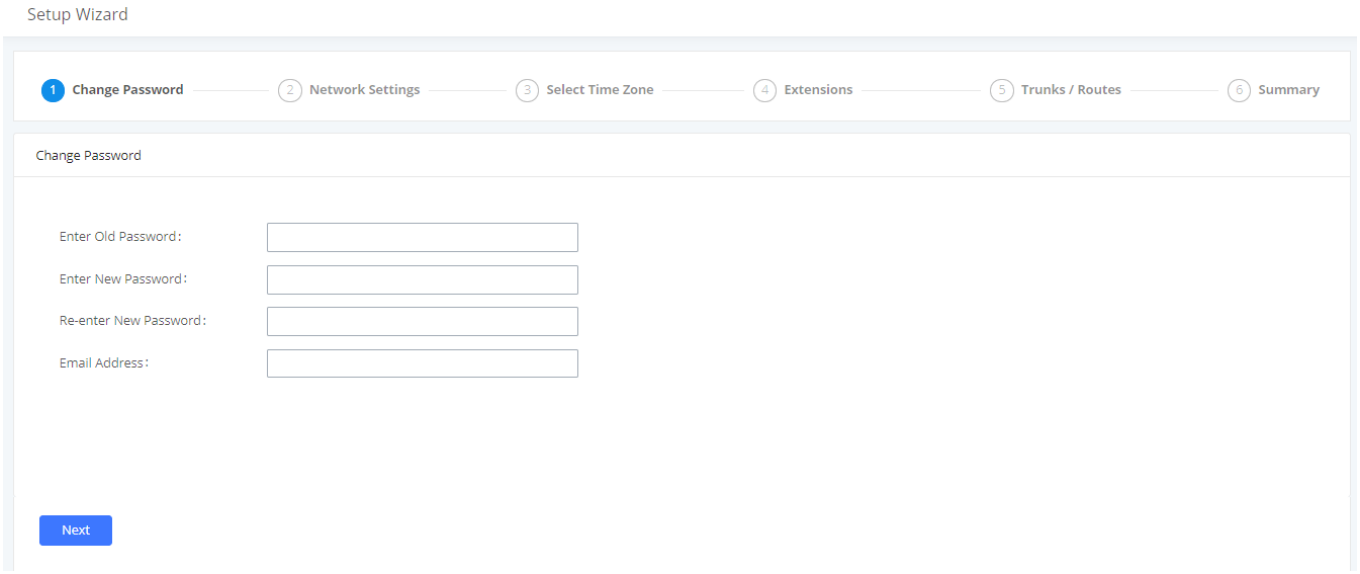
UCM has an instant messaging soft terminal supporting system called Wave, a unified communication application integrating chat/group chat, telephone, meeting and remote collaboration.

1. Use your phone number to log in to Wave.
2. Use the Wave app, use it at any time.
3. Instant messaging.
4. Point-to-point video/audio calls and multi-party meetings.
5. Resolve instant messaging within the enterprise.

Learn more

UCM630x Web GUI Wave guide interface

The setup wizard guides users to complete basic configuration, such as administrator password modification, network settings, time zone settings, extension settings, and routing rule configuration, etc.



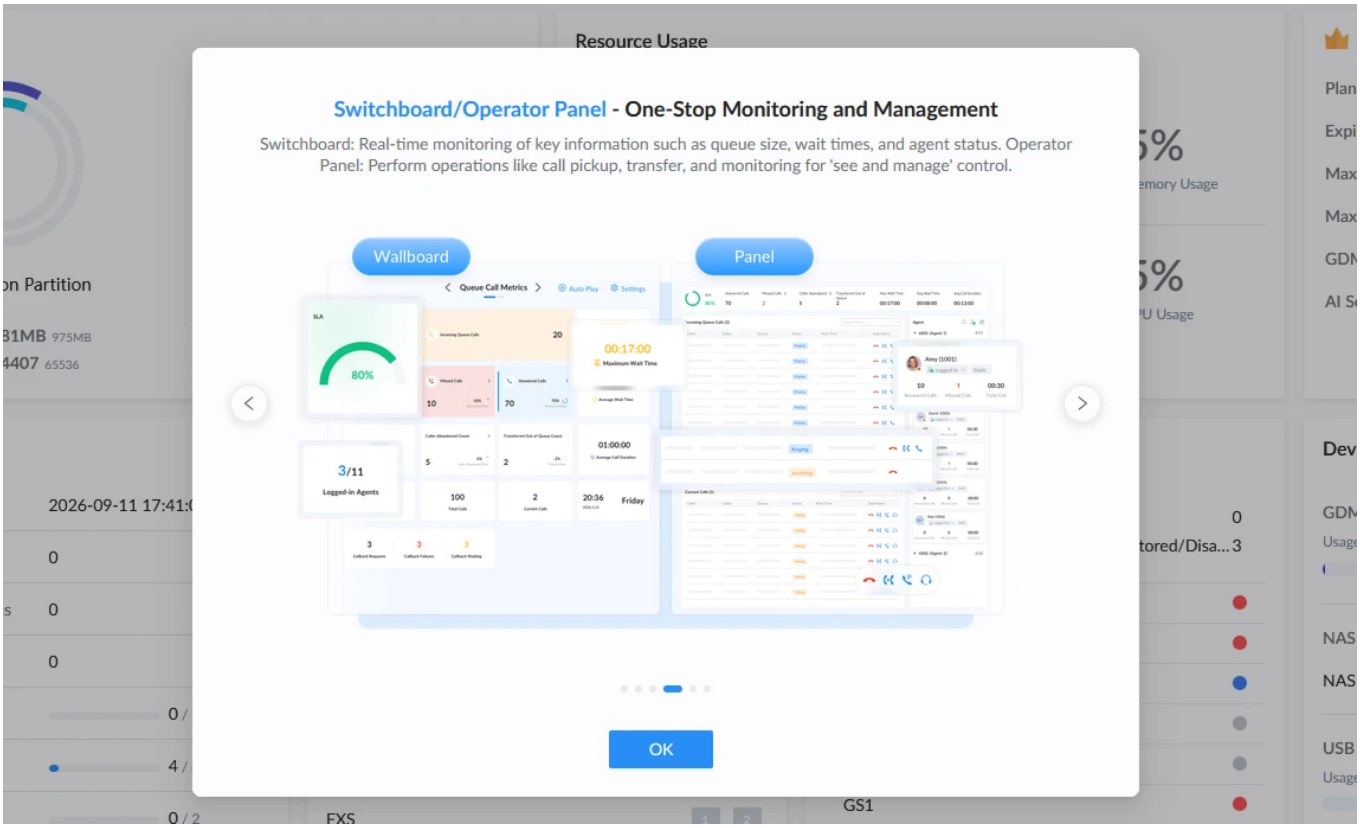
UCM630X Setup Wizard

The setup wizard can be closed and reopened at any time. At the end of the wizard, a summary of the pending configuration changes can be reviewed before applying them.

New Feature Guide

The UCM630X includes an interactive **New Feature Guide** to inform administrators of major platform

updates upon upgrading system firmware. When logging in for the first time following a firmware upgrade, an illustrated modal window automatically appears to highlight the key enhancements and value-added capabilities introduced in the new release.

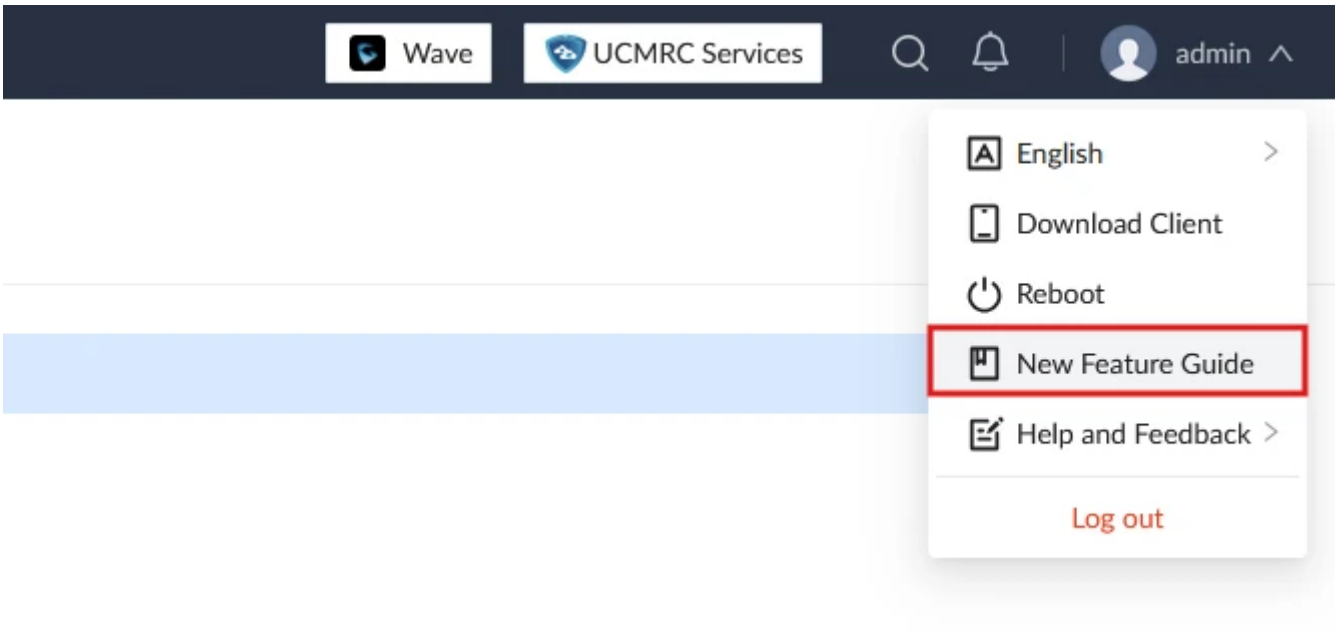


Interactive New Features Guide Modal

The interactive guide presents update highlights using visual card layouts with concise descriptions. Administrators can navigate through the card pages using the directional arrows or dismiss the dialog by clicking **OK**.

System restarts will not cause the initial welcome modal to re-appear.

Once closed, the guide remains permanently accessible from the Web GUI header bar. To revisit the guide at any time, click on your username in the upper-right corner and select **New Feature Guide** from the drop-down menu.



Accessing New Feature Guide via Top Header Menu

Main Settings

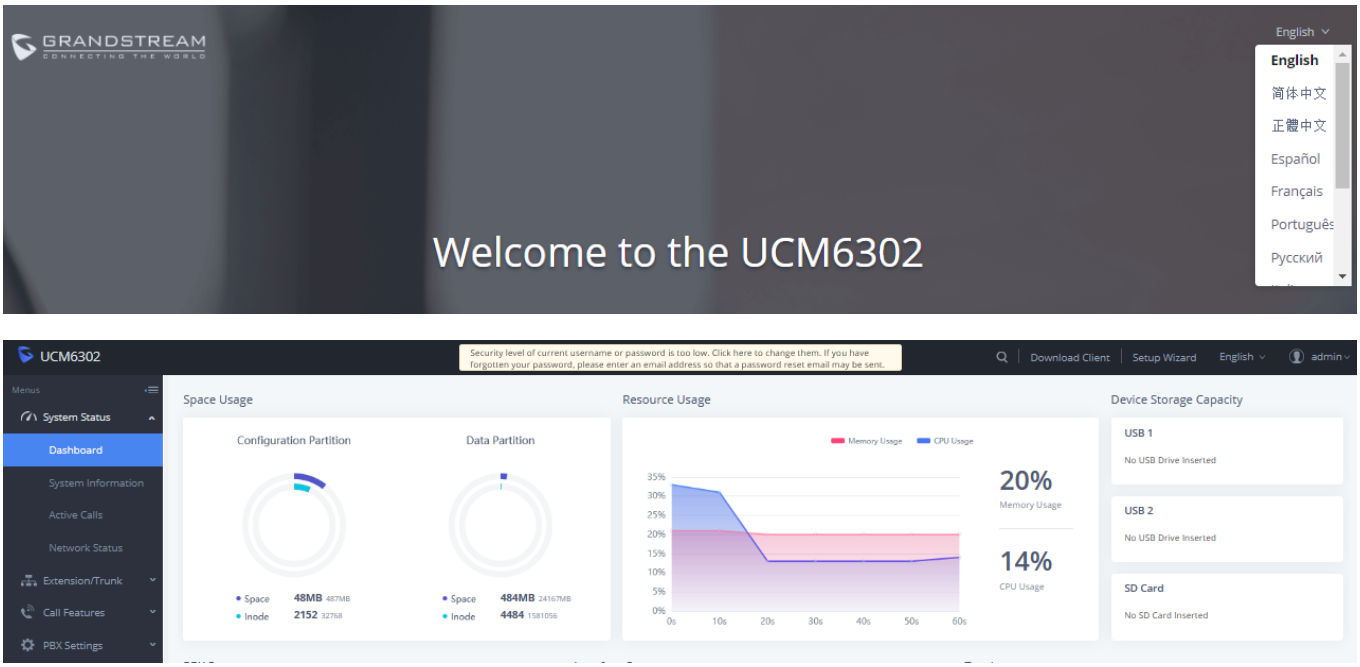
There are 12 main sections in the web portal to manage various features of the UCM.

- **System Status:** Displays the dashboard, system information, current active calls, and network status.
- **Extensions/Trunks:** Manages extensions, trunks, and routing rules.
- **Call Features:** Manages various features of the UCM such as the IVR and voicemail.
- **Messaging:** In this section the main settings for the methods of messaging which are offered by the UCM.
- **PBX Settings:** Manages the settings related to PBX functionality such as SIP settings and interface settings.
- **System Settings:** Manages the settings related to the UCM system itself such as network and security settings.
- **Contacts:** Manages all the type of contacts and departments in the UCM.
- **Device Management:** Manages cameras and Grandstream provisioning mechanism Zero Config.
- **Maintenance:** Manages settings and logs related to system management and maintenance such as user management, activity logs, backup settings, upgrade settings, and troubleshooting tools.
- **CDR:** Contains the call detail records, statistics, and audio recordings of calls processed by the UCM.
- **RemoteConnect:** the user can view the RemoteConnect purchased for the UCM. The user can also configure related settings from this section.
- **Integrations:** Manages the settings of features unrelated to core PBX functionality such as CRM/PMS integrations.

Web GUI Languages

Currently the UCM630X series Web GUI supports **English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, Russian, Italian, Polish, German, Turkish, and Czech.**

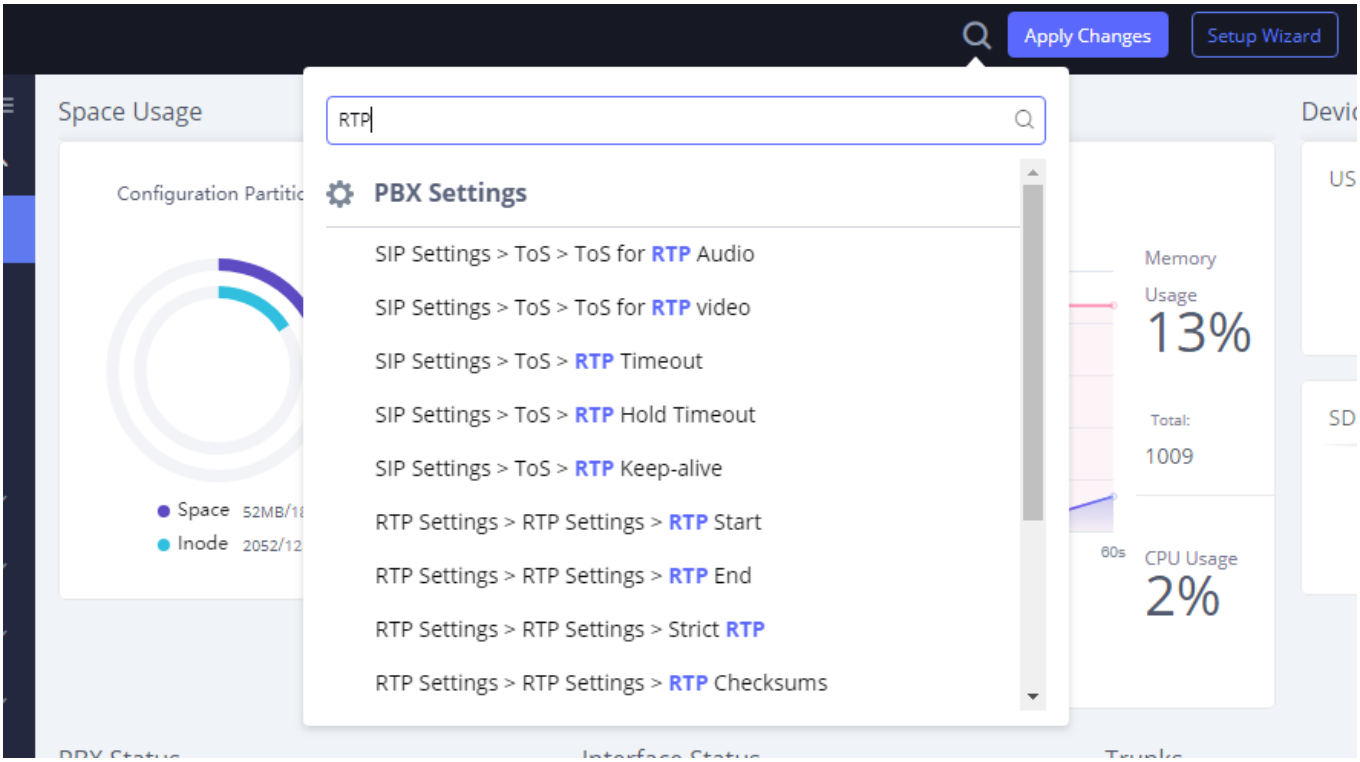
Users can select the UCM's web UI display language in the top-right corner of the page.



UCM630X Web GUI Language

Web GUI Search Bar

Users can search for options in the web portal with the search bar on the top right of the page.



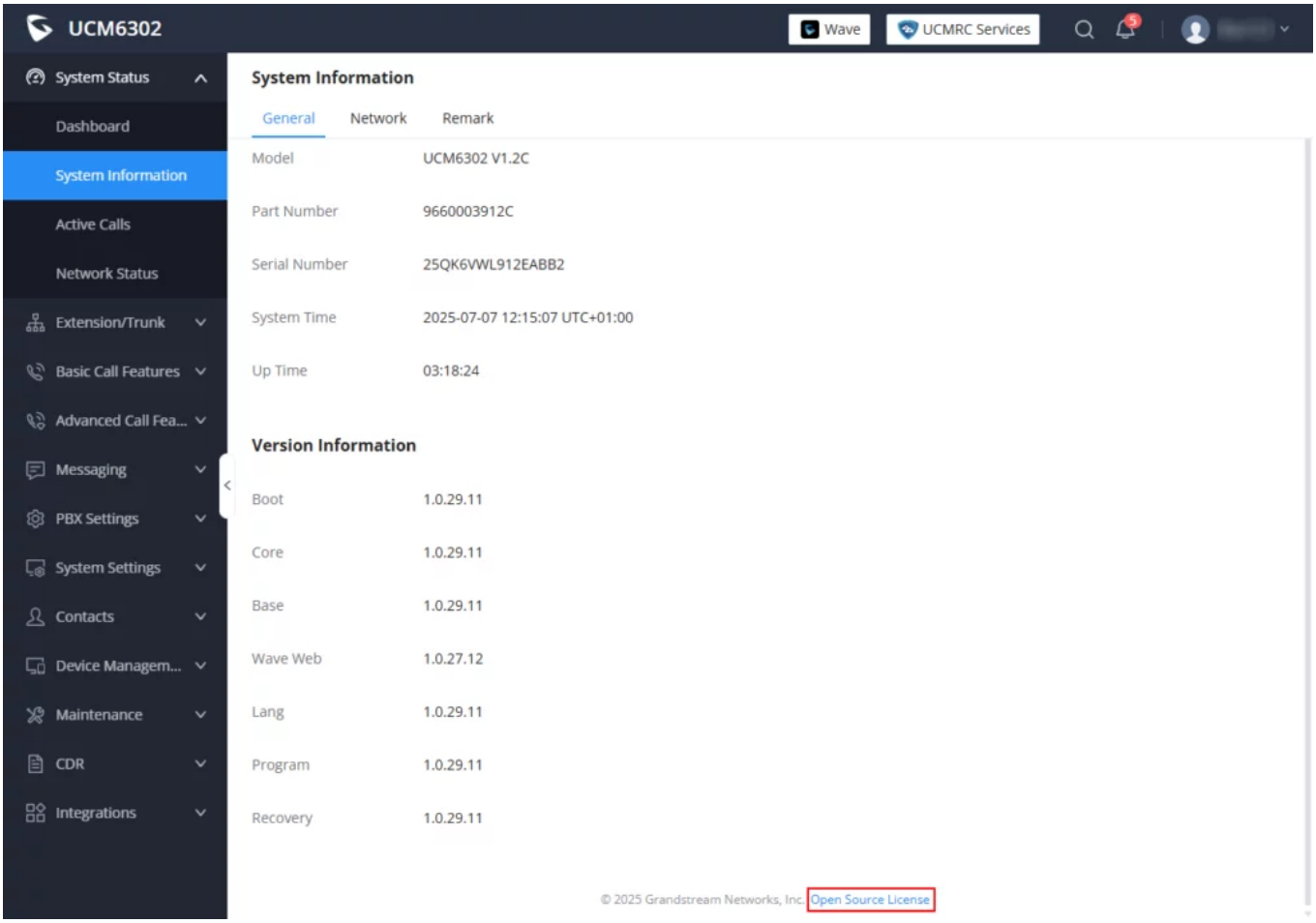
Web GUI Search Bar

Saving and Applying Changes

After making changes to a page, click on the "Save" button to save them and then the "Apply Changes" button that finalizes the changes. If a modification requires a reboot, a prompt will appear asking to reboot the device.

Open Source License

On the bottom of the page, as shown in the screenshot below, the user can access the open source license of the UCM6300 Series software.

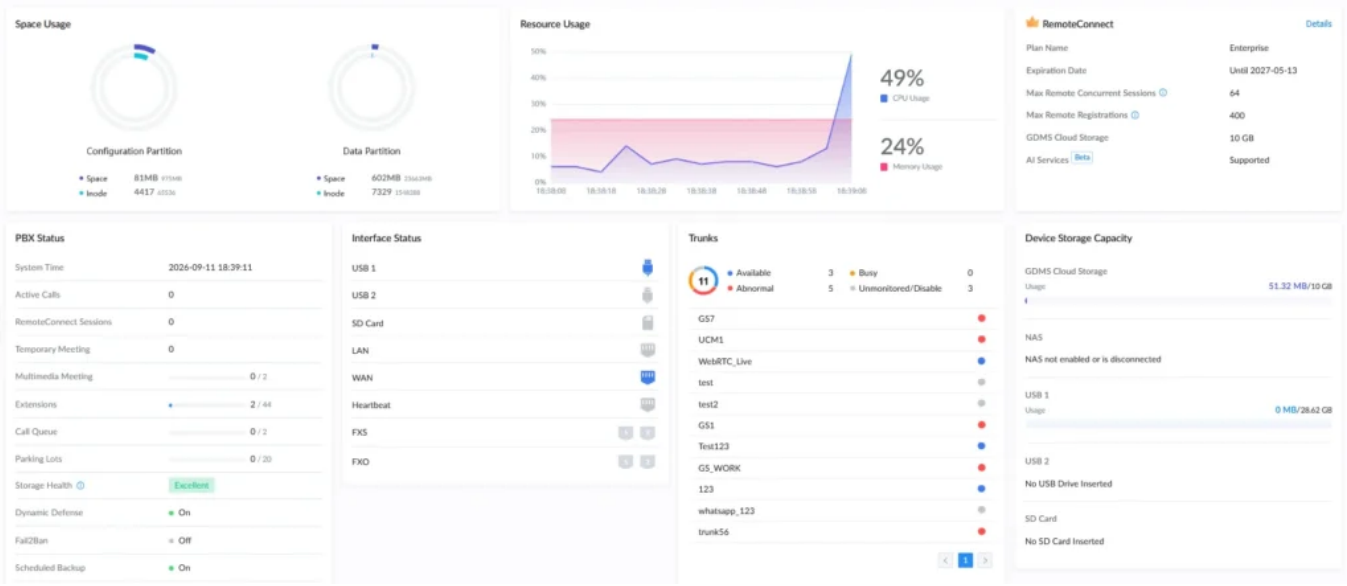


SYSTEM STATUS

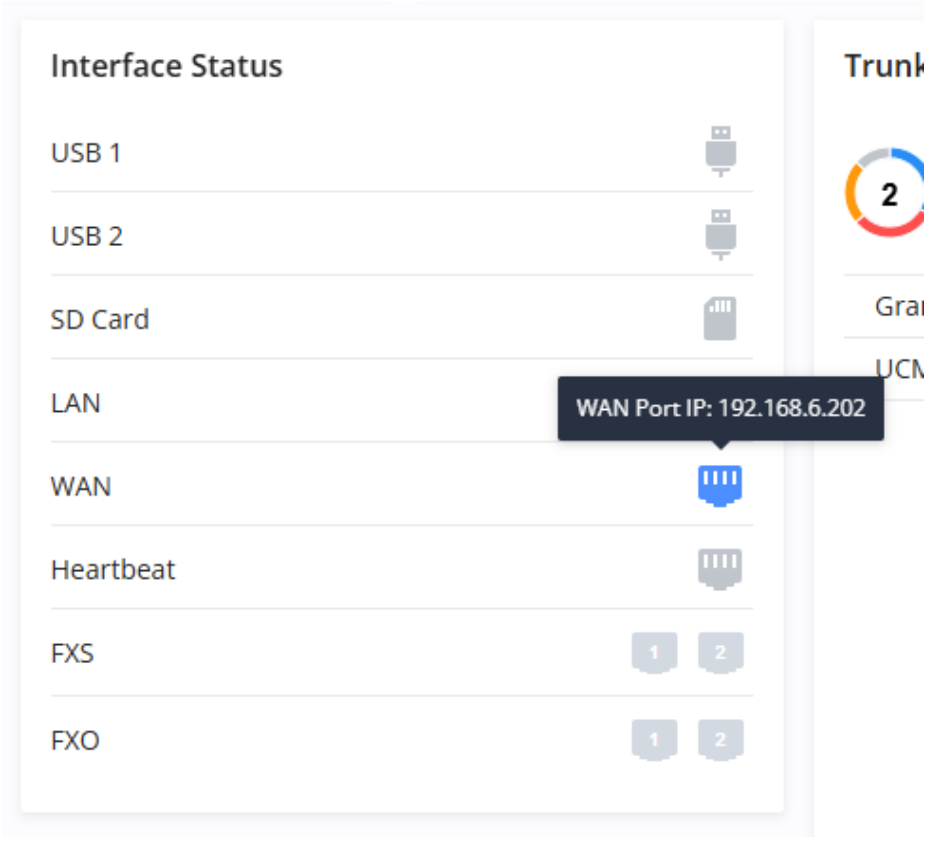
In this category, the user can view different information regarding the general operation of the IPPBX. Such as the dashboard, which displays the resources usage by the processes of the PBX, as well as the trunks created, the status of the different physical interfaces of the device, general statistics about the ongoing calls and meeting, and storage usage information.

Dashboard

- **Space Usage**
- **Resource Usage**
- **RemoteConnect**
- **PBX Status**
- **Interface Status**
- **Trunks**
- **Device Storage Capacity**

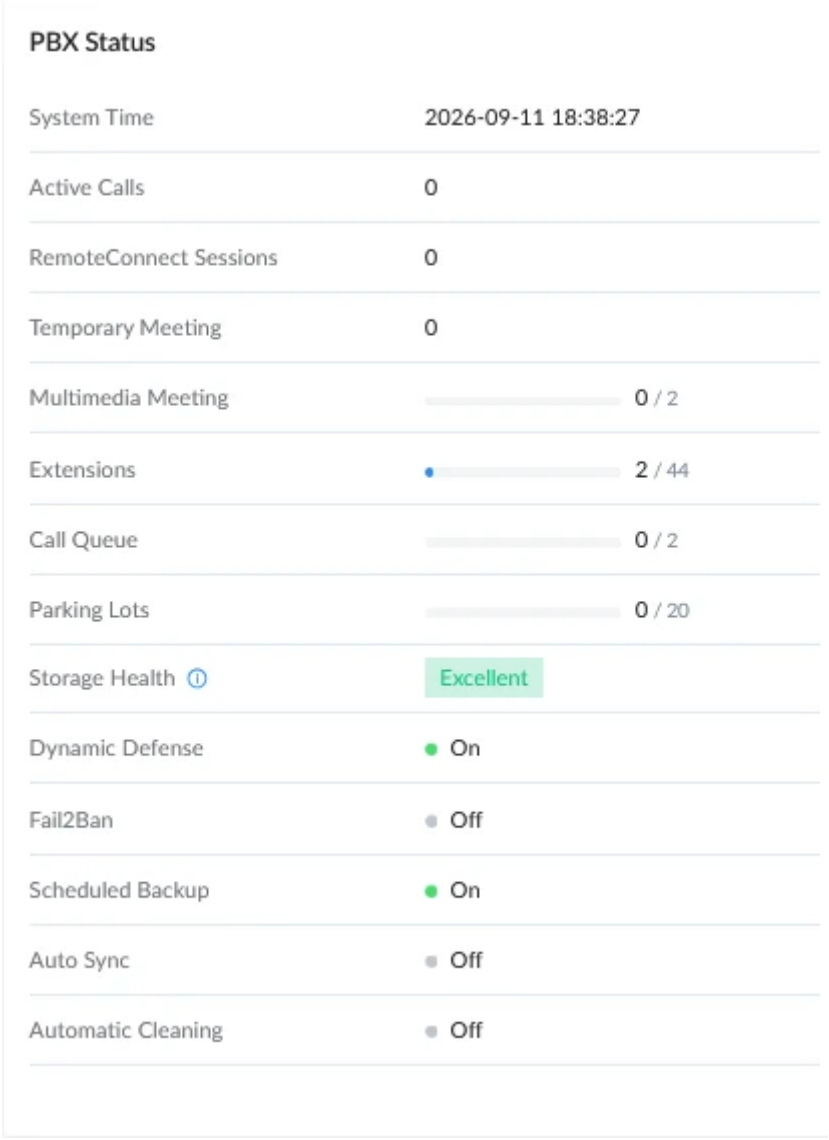


On the dashboard the user can view different statuses and place the cursor on the different sections to obtain more information about the UCM device. For example, the user can place the cursor on the port icon to view the IP address as shown in the screenshot below.



Interface Status

The administrator can also use the dashboard to view information about the different services of the UCM. Such as the number of multimedia meetings, the number of extensions (registered and unregistered), Storage Health status, active security modules (Dynamic Defense, Fail2Ban), scheduled system tasks, etc...

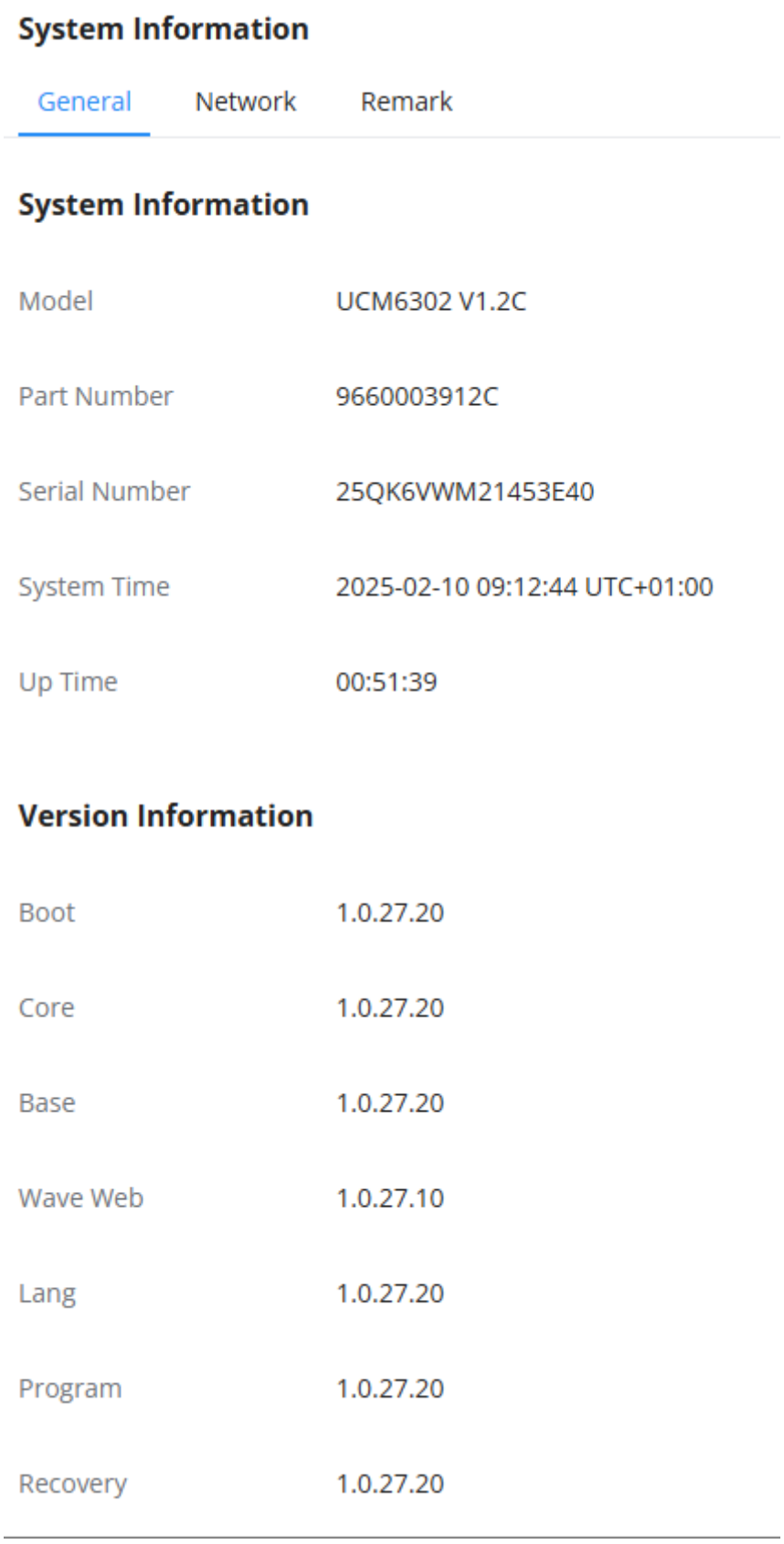


System Information

System Information page provides information regarding the hardware and software information of the UCM device, in addition to the network configuration. Remark tab allows the user to add additional information regarding the UCM device.

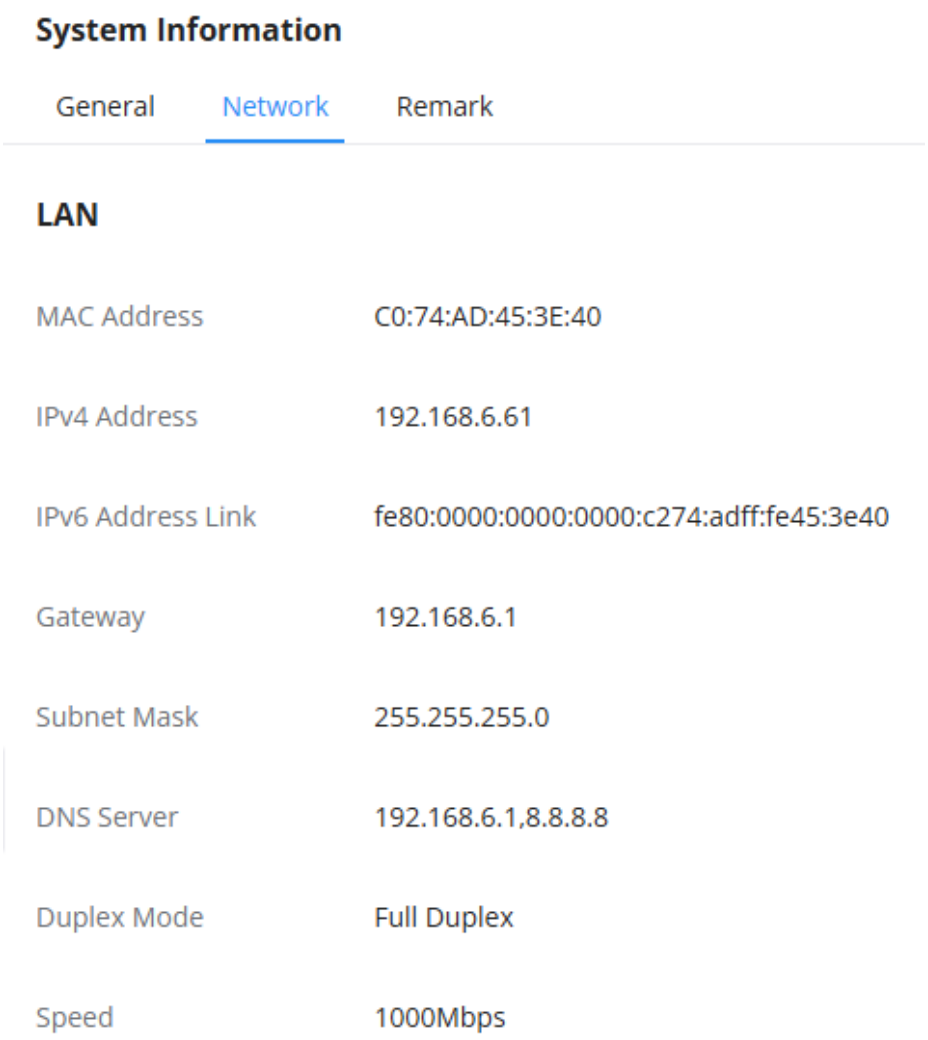
General

In **General** tab, the user can view the hardware and software information. Hardware information include model and part number. Software information include information about the version of the boot loader, the core software, and the PBX software. In addition to Wave Web version, language package version, and the recovery software version.



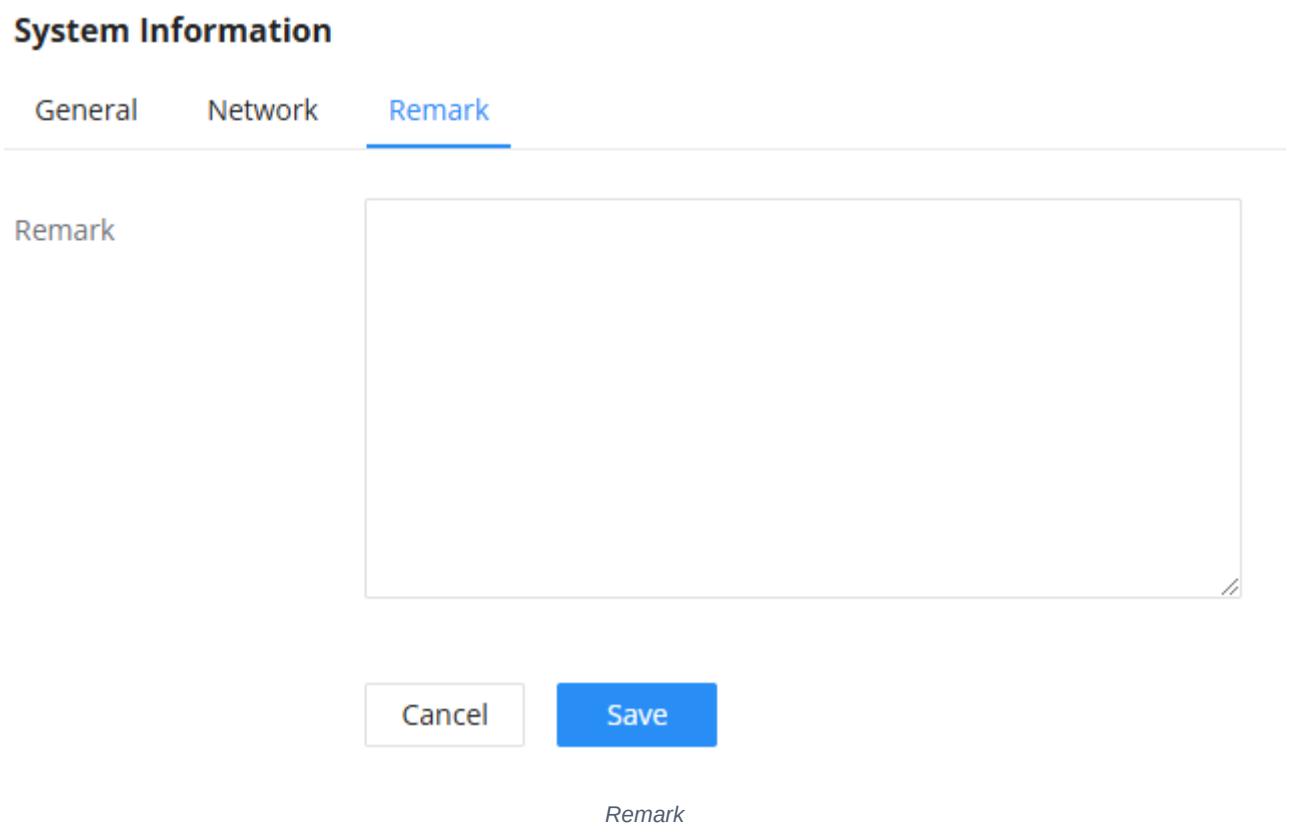
Network

Network page shows information related to the network interface of the UCM. This includes MAC Address, network configuration assigned by the DHCP server, link speed, and duplex mode.



Remark

In **Remark** tab, the user can add a note regarding the UCM device to easily identify the device when logged into the user manual.

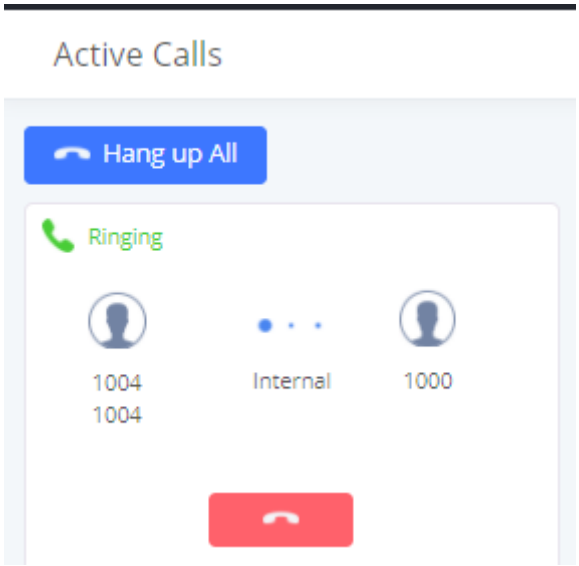


Remark

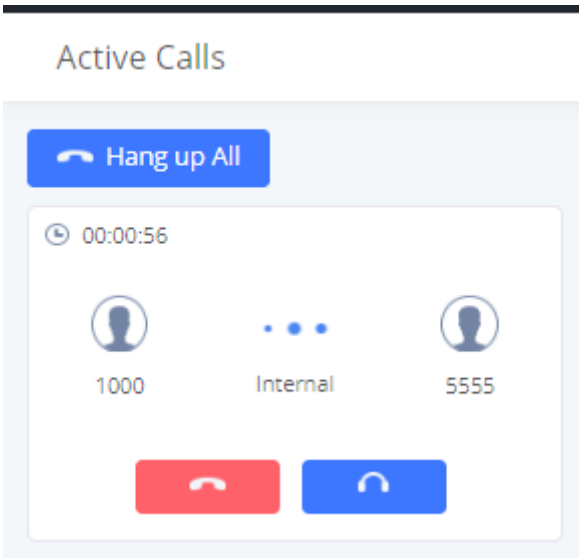
Active Calls

The active calls on the UCM6300 Series are displayed in the **System Status** -> **Active Calls** page. Users can monitor the status, hang up a call, and barge in the active calls in a real-time manner.

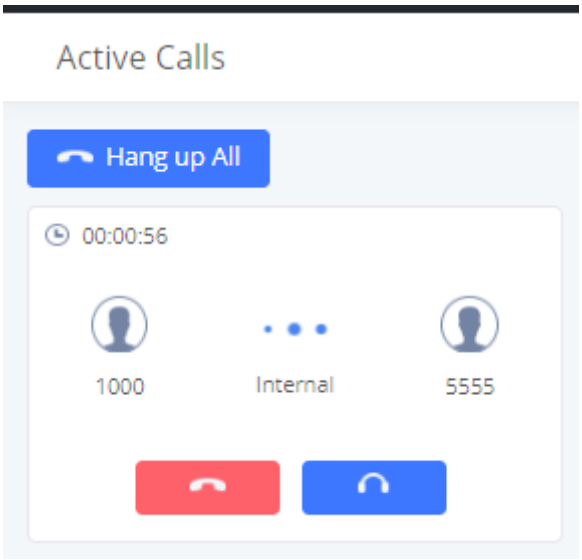
To view the status of active calls, navigate to **System Status** -> **Active Calls**. The following figure shows extension 1004 is calling 1000. 1000 is ringing.



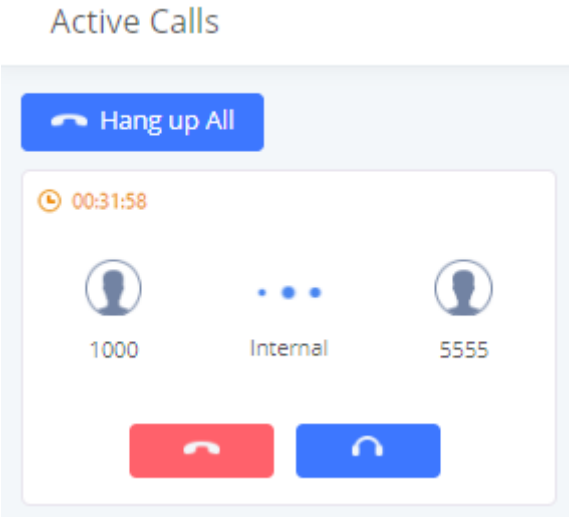
The following figure shows the call between 1000 and 5555 is established.



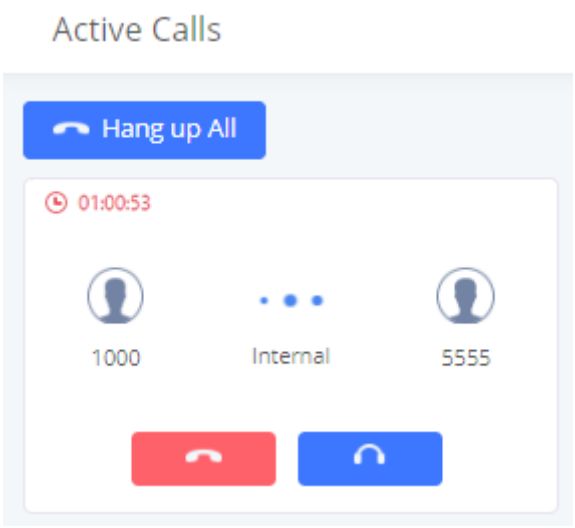
The gray color of the active call means the connection of call time is less than half an hour. It means this call is normal.



The orange color of the active call means the connection of call time is greater than half an hour but less than one hour. It means this call is a bit long.



The red color of the active call means the connection of call time is more than one hour. It means this call could be abnormal.

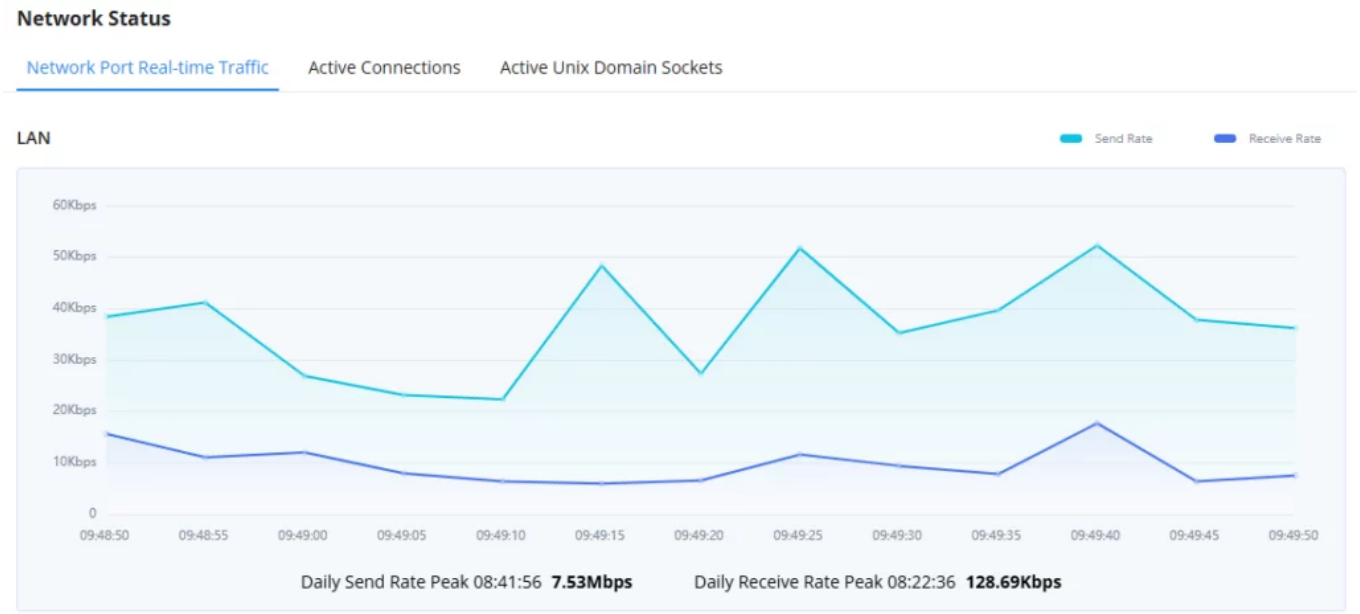


Network Status

In this category, the user can view real-time traffic, active connections, and active Unix Domain Sockets

Network Port Real-time Traffic

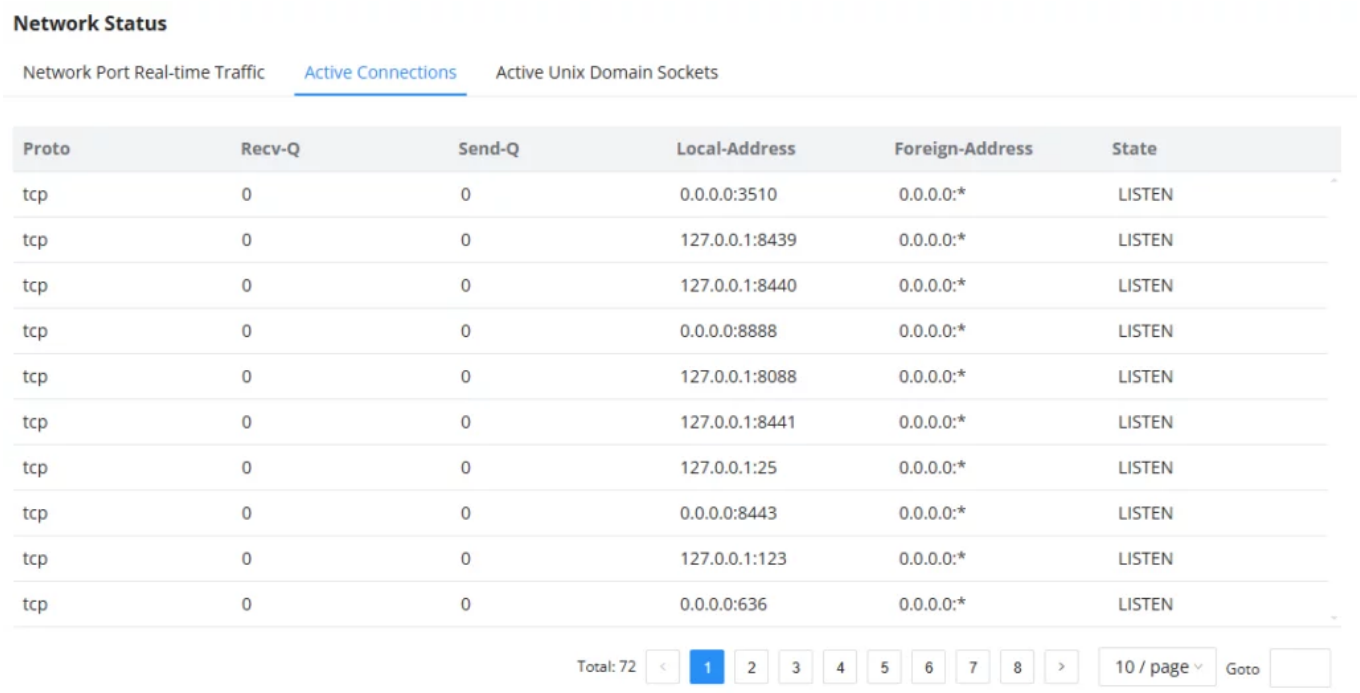
In this page, the user can view the rate of the data sent and received by the IPPBX. The graphs of the network activity is displayed for each interface.



Network Port Real-time Traffic

Active Connection

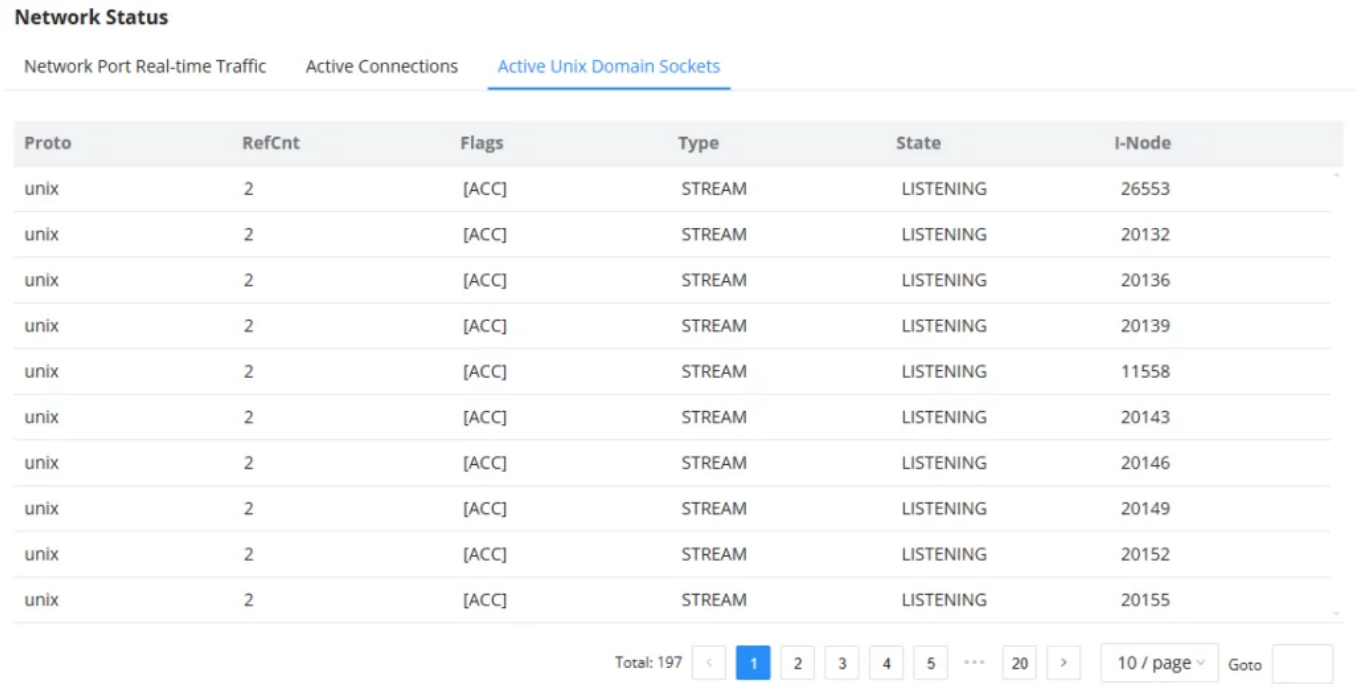
In this page, the user can view the network ports open and the established connections.



Active Connections

Active Unix Domain Sockets

In the page the user can view the active unix domain sockets.



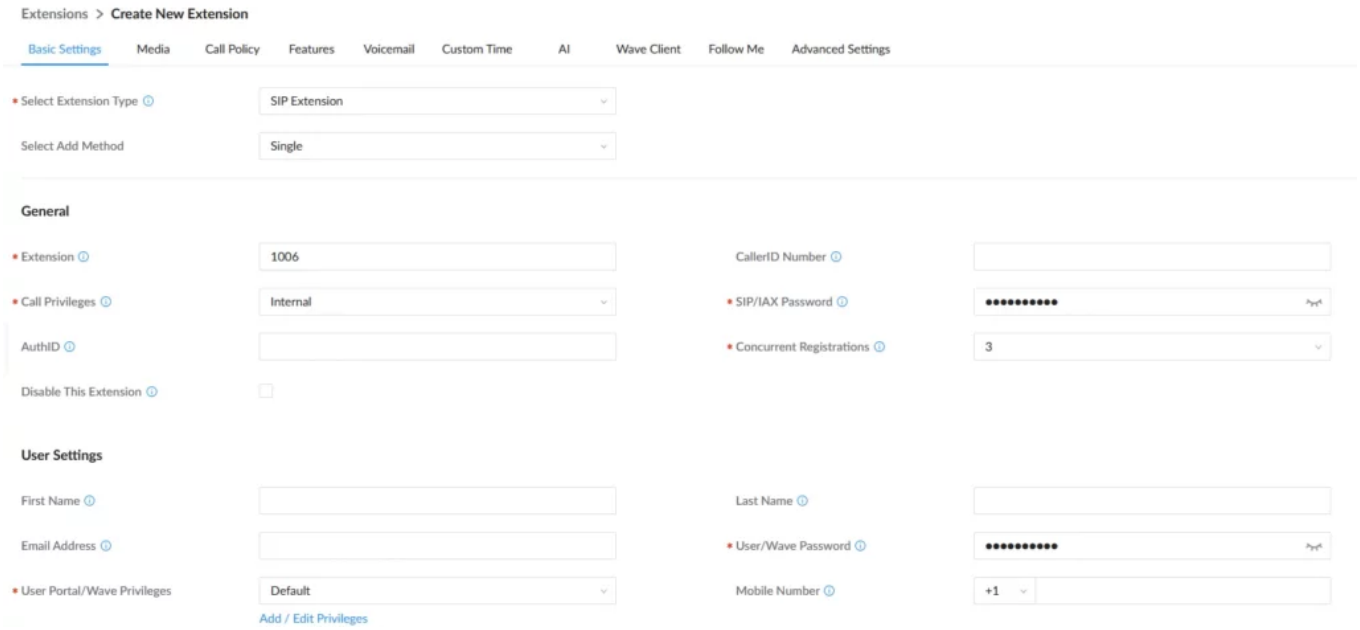
Active Unix Domain Sockets

EXTENSION/TRUNK

Extensions

Create New SIP Extension

To manually create a new SIP user, go to **Extension/Trunk->Extensions**. Click on "Add" and a new window will show for users to fill in the extension information.



Create a New SIP Extension

Extension options are divided into the following categories:

- **Basic Settings**
- **Media**
- **Call Policy**
- **Features**
- **Voicemail**
- **Custom Time**
- **AI**
- **Wave Client**
- **Follow me**
- **Advanced Settings**

Select first which type of extension: SIP Extension, IAX Extension, or FXS Extension. The configuration parameters are as follows.

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user.Note:The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Call Privileges	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.Note: The password should contain at least 10 characters, with at least one lower-case letter, one upper-case letter, one numeral, and one special character.The password must not contain an ascending or descending consecutive numeric sequence, or a consecutive sequence of the same number/letter.

Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
Concurrent Registrations	The maximum endpoints which can be registered to this extension. For security concerns, the default value is 3.Note: The user can configure up to 10 registrations per extensions.
Disable This Extension	Check this box to disable this extension.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User/Wave Password?	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.The password must respect the following criteria: At least one lower case letter At least one upper case letter At least one numeral At least one special character At least 10 total characters
User Portal/Wave Privileges	Change User Portal/Wave Privileges. Default: Setting this privilege will grant the standard Wave privileges. Wave Administrator: Setting this privilege will grant the user access to Management Portal on Wave.
Multi-Factor Authentication	When this option is enabled, the extension user will be prompted to configure multi-factor authentication on their account when they log in from the User Portal or Wave. The user can choose to use an OTP device or application, or they can use their email as a second factor of authentication. To ensure enabling Wave multi-factor authentication is successful, please refer to the minimum versions required below for Wave on each platform. Wave Web: 1.0.27.12 and later Wave Desktop: 1.27.10 and later Wave App for Android(TM): 1.0.27.18 and later Wave App for iOS(TM): 1.27.24 and later
Mobile Phone Number	Configure the phone number for the extension, user can type the related star code for the phone number followed by the extension number to directly call this number.For example, the user can type *881000 to call the mobile number associated with extension 1000.
Department	Configure the user's department. The department can be configured in User Management > Address Book Management > Department Management. Job Title: The user's department position.
Job Title	Configure the job title for this user.
Contact Privileges	
Same as Department Contact Privileges	When enabled, The extension will inherit the same privilege attributed to the department it belongs to.
Contact View Privileges	Select the privileges regarding the contact view in SIP endpoints and Wave.
Sync Contact	If enabled, this extension number will be displayed in the Wave contact, otherwise, it will not be displayed, and it cannot be found in the chat, but the user can still dial this number.

SIP Extension Configuration Parameters->Basic Settings

General	
NAT	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is a one-way audio issue, usually it is related to NAT configuration or the Firewall's support of SIP and RTP ports. The default setting is enabled.

Enable Direct Media	By default, the PBX will route the media streams from SIP endpoints through itself. If this option is enabled, the PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee.Note: It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing.
DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is "RFC4733". If "Info" is selected, the SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, RFC4733 will be used if offered, otherwise "Inband" will be used.Note: The default DTMF mode selected is RFC4733.
Alert-Info	When present in an INVITE request, the alert-Info header field specifies an alternative ring tone to the UAS.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
TURN Relay	Enable this option if the following are true:PBX is deployed on a private network.There are remote endpoints outside the PBX's network registering to it via its public IP address.The network's firewall is not configured for media port forwarding.Media NAT penetration is required.Once a TURN server is configured, media will be forwarded to it. This configuration does not affect endpoints that are registered via the PBX's RemoteConnect address.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G,726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.
QoS	
Jitter Buffer	Select the jitter buffer method.Disable: Jitter buffer will not be used.Fixed: Jitter buffer with a fixed size (equal to the value of "jitter buffer size")Adaptive: Jitter buffer with an adaptive size (no more than the value of "max jitter buffer").NetEQ: Dynamic jitter buffer via NetEQ.
Jitter Buffer Size (ms)	Configure the time (in ms) to buffer. This is the jitter buffer size used in "fixed" jitter buffer, or used as the initial time for "adaptive" jitter buffer.
Max Jitter Buffer (ms)	Configure the maximum time (in ms) to buffer for "adaptive" implementation.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission.NACKNACK+RTX(SSRC-GROUP)OFF
Video FEC	Check to enable Forward Error Correction (FEC) for Video.
Audio FEC	Check to enable Forward Error Correction (FEC) for Audio.
Silence Suppression	If enabled, the PBX will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the PBX will send DTX packets instead.
FECC	Configure to enable Remote Camera Management.
RTP Encryption	
SRTP	Enable SRTP for the call. The default setting is disabled.Disabled Enabled and Enforced: SRTP will be necessary to transmit media traffic. If the IP phone of this extension has SRTP disabled, calls cannot be established. Optional: The PBX will negotiate whether to use SRTP or not. If the SIP endpoint has SRTP enabled, SRTP will be used. If it is disabled, SRTP will not be used.
SRTP Crypto Suite	SRTP encryption suite used by the PBX for outbound calls. Priority is based on order of configuration.The following encryption alogrithms can be used to encrypt an RTP stream.AES_CM_128_HMAC_SHA1_80 (This is the default algorithm used)AES_256_CM_HMAC_SHA1_80AEAD_AES_128_GCMAEAD_AES_256_GCM
ZRTP Encryption Mode	ZRTP, also known as Media Path Key Agreement for Secure RTP, is an encryption protocol which allows negotiating the encryption key for RTP traffic. ZRTP uses Diffie-Hellman exchange to establish an encrypted and secure connection between the PBX and the SIP endpoint. If the SIP endpoint has both SRTP and ZRTP enabled, ZRTP will always be prioritized.

SIP Extension Configuration Parameters->Media

Presence Status	
Presence Status	Select which presence status to set for the extension and configure call forward conditions for each status. Six possible options are possible: "Available", "Away", "Chat", "Custom", "DND" and "Unavailable". More details at [PRESENCE]. Note: For supported Cisco endpoints (CP69xx/78xx/88xx series), enabling DND directly from the phone will synchronize with the PBX and update the extension presence status to DND on the UCM. DND synchronization may also function on other Cisco models, although compatibility is not explicitly guaranteed.
Enable Calendar Sync	Allow this extension's presence status to sync with Google Calender events.Note: This option requires to configure the Google Workspace Integration.
Call Transfer	
Call Forward Always	Enable and configure the Call Forward Unconditional target number. Available options for target number are:"None": Call forward deactivated."Extension": Select an extension from the dropdown list as CFU target."Custom Number": Enter a customer number as a target. For example: *97."Voicemail": Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension."Ring Group": Select a ring group from the dropdown list as CFU target."Queues": Select a queue from the dropdown list as CFU target."Voicemail Group": Select a voicemail group from the dropdown list as CFU target.Custom Prompt: The call will be forwarded to a custom prompt. The default setting is "None".
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.Notes:"Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. Available options for target number are:"None": Call forward deactivated."Extension": Select an extension from the dropdown list as CFN target."Custom Number": Enter a customer number as a target. For example: *97."Voicemail": Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension."Ring Group": Select a ring group from the dropdown list as CFN target."Queues": Select a queue from the dropdown list as CFN target."Voicemail Group": Select a voicemail group from the dropdown list as CFN target.Custom Prompt: The call will be forwarded to a custom prompt.The default setting is "None".
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.Notes:"Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. Available options for target number are:"None": Call forward deactivated."Extension": Select an extension from the dropdown list as CFB target."Custom Number": Enter a customer number as a target. For example: *97"Voicemail": Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension."Ring Group": Select a ring group from the dropdown list as CFB target."Queues": Select a queue from the dropdown list as CFB target."Voicemail Group": Select a voicemail group from dropdown list as CFB target.Custom Prompt: The default setting is "None".

CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
Forwarding Exemption List	Calls from users in the forward exemption list will not be forwarded. Multiple numbers are supported and must be separated by new lines.Pattern matching is supported.Z match any digit from 1-9,N match any digit from 2-9,X match any digit from 0-9.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
Time Condition	Select time condition for Do Not Disturb. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes:"Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
DND Allowlist	If DND is enabled, calls from the allowlisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.Z match any digit from 1-9.N match any digit from 2-9.X match any digit from 0-9.
Call Number Handling Policy	Call Number Handling Policy determines the destination of the calls received. The user can configure the destination based on the a matching pattern of the callee number.Call Number Matching Mode: Support input extension numbers and pattern matching rules: [12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 are allowed. N ... Any digit from 2-9. . ... Wildcard, matching one or more characters. ! ... Wildcard, matching zero or more characters immediately. X ... Any digit from 0-9. Z ... Any digit from 1-9. - ... Hyphens are used mainly to improve readability and are not involved in pattern matching. [] Contain special characters ([x], [n], [z]) represent letters x, n, z.Call Destination: Select the destination of the call. These are the destinations which can be set; Disconnect, Extensions, Voicemail, IVR, Hang up After Playing Background Sound, Call Accepted.

SIP Extension Configuration Parameters->Call Policy

CC Settings	
Enable CC	If enabled, the PBX will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.
CC Mode	Two modes for Call Completion are supported: Normal: This extension is used as an ordinary extension.For Trunk: This extension is registered from a PBX.The default setting is "Normal".
Call Settings	
Call Duration Limit	Block calls for the configured duration.
Maximum Call Duration (s)	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).
The Maximum Number of Call Lines	The maximum number of simultaneous calls that the extension can have. 0 indicates no limit.
Outgoing Call Frequency Limit	If enabled, if the number of outbound calls exceed the configured threshold within the specified period, further outbound will be not be allowed.
Period (m)	The time window for the configured outbound call frequency limit. Supported value range is 1 to 120 minutes. Default value is 1.

Max Number of Calls	The maximum allowed number of outbound calls within the specified period. Supported value range is 1 to 20. Default value is 5.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. '-' is the connection character that will be ignored. This field accepts only letters, numbers, and special characters + = * #.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension based on this time condition.
Use callee DOD on FWD or RS	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
Monitor Privilege Control	
Allow being monitored	When disabled, this user's calls cannot be listened to by anyone. When enabled, this user's calls are allowed to be listened to through this extension or the opposite extension.
Call Monitoring Allowlist	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Allow Operator Panel Monitoring	Configure whether this extension can be monitored by the Operator Panel administrator.
Seamless Transfer Privilege Control	
Seamless Transfer Allowlist	Any extensions on the PBX can perform a seamless transfer. When using the Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform a seamless transfer to the edited extension.
PMS Remote Wakeup Whitelist	
Select the extensions that can set wakeup service for other extensions	Selected extensions can set a PMS wakeup service for this extension via feature code.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the PBX. The valid range is between 5 seconds and 600 seconds.Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under CDR > Recording Files.
Skip Trunk Auth	If set to "yes", users can skip entering the password when making outbound calls.If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering the password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via the trunk.
Support Hot-Desking Mode	Check to enable Hot-Desking Mode on the extension. Hot-Desking allows using the same endpoint device and logs in using extension/password combination. This feature is used in scenarios where different users need to use the same endpoint device during a different time of the day for instance. If enabled, SIP Password will accept only alphabet characters and digits. Auth ID will be changed to the same as Extension.

Enable LDAP	If enabled, the extension will be added to the LDAP Phonebook PBX list. Default is enabled.
Use MOH as IVR ringback tone	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
Music On Hold	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
Max Number of Calls	Set the maximum number of outgoing calls in a period. The valide tange is from 1 to 20. The default value is 5.
Enable Auto-Answer Support	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
Call Waiting	Allows calls to the extension even when it is already in a call. This only works if the caller is directly dialing the extension. If disabled, the CC service will take effect only for unanswered and timeout calls.
Stop Ringing	If enabled, when the extension has concurrent registrations on multiple devices, upon incoming call or meeting invite ringing, if one end device rejects the call, the rest of the devices will also stop ringing. By default, it's disabled.
Email Missed Call Log	If enabled, the log of missed calls will be sent to the extension's configured email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are:Default: All missed calls will be sent in email notifications.Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications.Missed External Call: Only missed calls from trunks will be sent in email notifications.
Enable SCA (Share Call Appearance)	If enabled, (1) Call Forward, Call Waiting and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Advanced Call Features > SCA page.
Emergency CID	CallerID name and number that will be used when making emergency calls and receiving direct callbacks. If ELIN subnet mapping has been configured, and the extension is registered to a device in a mapped subnet, the configured ELIN will be used for CID number instead.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used. If a language is selected, the voice prompt will be in the corresponding language when calling this specific extension.

SIP Extension Configuration Parameters->Features

Specific Time	
Time Condition	Click to add Time Condition to configure a specific time for this extension.

SIP Extension Configuration Parameters->Custom Time

AI Call Transcription and Summary	
Automatic Transcribing And Summarizing	Enables or disables automatic transcription and summarization for all calls associated with this extension. When enabled, calls for this extension are automatically transcribed and summarized without user action.
Language	Defines the language recognition behavior for call transcription on this extension. The options are: Follow Global Settings: Uses the language configuration defined under AI Settings.Automatic Recognition: Automatically detects the spoken language during the call. This is recommended when multiple languages are expected, though recognition accuracy may vary.Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy.Note: This setting controls only the transcription behavior for this extension. It does not enable or disable AI services at the system level.

AI Voicemail To Text	
Automatic Transcription	This section determines whether voicemail messages left for this extension are automatically converted from speech to text.
Language	Specifies the language recognition behavior used for voicemail transcription. The options are:Follow Global Settings: Uses the language configuration defined under AI Settings.Automatic Recognition: Automatically detects the spoken language during the call. This is recommended when multiple languages are expected, though recognition accuracy may vary.Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy.Note: This setting controls only the transcription behavior for this extension. It does not enable or disable AI services at the system level.

SIP Extension Configuration Parameters -> AI

General	
Enable Wave	Enable Wave for the specific extension.
Allow Simultaneous Logins from the Same Client Type	Enables/disables the ability to login to Wave from different sessions on the same type of client Notes: Concurrent Registrations limit for the SIP extension will still apply. When this option is enabled, Concurrent Registrations cannot be configured as "1 (Allowed to Seize)" This option is disabled by default.
Wave Welcome Email	Wave Welcome Email template.
Wave Permission Settings	Clicking the path will direct you to Wave Permission configuration.
Wave	
Download Link	https://fw.gdms.cloud/wave/download/

SIP Extension Configuration Parameters->Wave Client

Please note that the access to the QR code using the UCM6300 web UI using the admin account has been removed for security and confidentiality reasons.

Follow Me	
Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If the outbound calls need to check the password, we should enable this option or enable the option "Skip Trunk Auth" of the Extension. Otherwise, this Follow Me cannot call out.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Enable Destination	Configure to enable destination.
Default Destination	The call will be routed to this destination if no one in the Follow Me answers the call.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
Play Follow Me Prompt	If enabled, the Follow Me prompt tone will be played.
New Follow Me Number	Add a new Follow Me number which could be a "Local Extension" or an "External Number". The selected dial plan should have permissions to dial the defined external number.

Dialing Order	This is the order in which the Follow Me destinations will be dialed to reach the user.

SIP Extension Configuration Parameters->Follow Me

SIP Settings?	
Send PCPID Header	If enabled, this extension's SIP INVITE messages will contain the P-Called-Party-ID (PCPID) header if the callee is a SIP device.
Enable Auto-Answer	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
Enable Keep-alive	If enabled, the PBX will regularly send SIP OPTIONS to check if host device is online.
Keep-alive Frequency	Configure the keep-alive interval (in seconds) to check if the host is up.
TEL URI	If "Enabled" option is selected, TEL URI and Remove OBP from Route cannot be enabled at the same time. If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". A "User=Phone" parameter will then be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request.
ACL Policy	Access Control List manages the IP addresses that can register to this extension.Default: Follows Geo-IP Access ControlAllow Whitelist IP Address: Only whitelisted IP addresses in the configured network segments can register to this extension.Allow Whitelist IP Address + RemoteConnect: Registrations from whitelisted IP address network segments and RemoteConnect registrations to this extension will be allowed.
Fax	
Fax Mode	Configure fax mode. The following options are available:None: Disable fax support. This is the default option.Fax Detect: During a call, the fax signal from the user/trunk will be detected, and the received fax will be sent to the user's configured email address. If the destination does not have a configured email address, the fax will be sent to the Default Email Address configured in the Call Features > Fax/T.38 > Fax Settings page.
Fax to Email	If set to "Yes", the fax will be sent to the user-configured email address. If no user email address is found, the fax will be sent to the default email address configured in Fax/T.38 > Fax Settings.

SIP Extension Configuration Parameters->Advanced Settings

Create New IAX Extension

The UCM630X supports Inter-Asterisk eXchange (IAX) protocol. IAX is used for transporting VoIP telephony sessions between servers and terminal devices. Unlike SIP, IAX provides both the session opening and media packet transport. For more information, please refer to RFC 5456.

To manually create a new IAX user, go to Web GUI→**Extension/Trunk→Extensions**. Click on "Add" and a new dialog window will show for users which need to make sure first to select the extension type to be IAX Extension before proceeding to fill in the extension information. The configuration parameters are as follows.

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Privilege	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.

SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.
Voicemail	Configure Voicemail.There are three valid options, and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Skip Voicemail Password Verification	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Send Voicemail Email Notification	Configures whether to send emails to the extension's email address to notify of a new voicemail.
Attach Voicemail to Email	Configures whether to attach a voicemail audio file to the voicemail notification emails.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
Disable This Extension	If selected, this extension will be disabled on the UCM630X.Note: The disabled extension still exists on the PBX but cannot be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under Web GUI?PBX Settings?Voice Prompt?Language Settings. The dropdown list shows all the currently available voice prompt languages on the UCM630X. To add more languages to the list, please download the voice prompt package by selecting "Check Prompt List" under Web GUI?PBX Settings?Voice Prompt?Language Settings.
Mobile Phone Number	Configure the Mobile number of the user.

IAX Settings	
Max Number of Calls	Configure the maximum number of calls allowed for each remote IP address.
Require Call Token	Configure to enable/disable requiring call token. If set to "Auto", it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints. The default setting is "Yes".
SRTP	Enable SRTP for the call. The default setting is disabled.
ACL Policy	Access Control List manages the IP addresses that can register to this extension. Allow All: Any IP address can register to this extension. Local Network: Only IP addresses in the configured network segments can register to this extension.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G,726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.

Call Transfer	
Call Forward Always	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Allowlist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
Forwarding Exemption List	Calls from users in the forward whitelist will not be forwarded.Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. '-' is the connection character that will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension based on this time condition.
Use callee DOD on FWD or RS	Use the callee's DOD number as CallerID on Outgoing Forwarding or Ring Simultaneously calls.
Monitor Privilege Control	
Call Monitoring Allowlist	Members of the list can spy on this extension via feature codes.
Seamless Transfer Privilege Control	

Seamless Transfer Allowlist	Members of the list can seamlessly transfer via feature code.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM630X, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→Voice Prompt→Custom Prompt: General Preference. The valid range is between 5 seconds and 600 seconds.Note: If the endpoint also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.
Skip Trunk Auth	If set to "Yes", users can skip entering the password when making outbound calls. If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering the password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via the trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX lists.
Music On Hold	Configure the Music On Hold class to suggest to the bridged channel when putting them on hold.
Use MOH as IVR ringback tone	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
Call Duration Limit	Check to enable and set the call limit the duration.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
Email Missed Calls	Send a log of missed calls to the extension's email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are: Default: All missed calls will be sent in email notifications. Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications. Missed External Call: Only missed calls from trunks will be sent in email notifications.

IAX Extension Configuration Parameters→Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure a specific time for this extension.

Follow Me	
Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If the outbound calls need to check the password, we should enable this option or enable the option "Skip Trunk Auth" of the Extension. Otherwise, this Follow Me cannot call out.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Enable Destination	Configure to enable destination.

Default Destination	The call will be routed to this destination if no one in the Follow Me answers the call.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
Play Follow Me Prompt	If enabled, the Follow Me prompt tone will be played.
New Follow Me Number	Add a new Follow Me number which could be a "Local Extension" or an "External Number". The selected dial plan should have permissions to dial the defined external number.
Dialing Order	This is the order in which the Follow Me destinations will be dialed to reach the user.

Create New FXS Extension

The UCM630X supports Foreign eXchange Subscriber (FXS) interface. FXS is used when a user needs to connect analog phone lines or FAX machines to the UCM630X.

To manually create a new FXS user, go to Web GUI→**Extension/Trunk→Extensions**. Click on "Add" and a new dialog window will show for users which need to make sure first to select the extension type to be FXS Extension before proceeding to fill in the extension information. The configuration parameters are as follows.

General	
Extension	The extension number associated with the user.
Analog Station	Select the FXS port to be assigned for this extension.
Caller ID Number	Configure the CallerID Number that would be applied for outbound calls from this user.Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Privilege	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
Voicemail	Configure Voicemail.There are three valid options, and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Skip Voicemail Password Verification	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Send Voicemail Email Notification	Configures whether to send emails to the extension's email address to notify of a new voicemail.
Attach Voicemail to Email	Configures whether to attach a voicemail audio file to the voicemail notification emails.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
Emergency CID Name	CallerID name that will be used for emergency calls and callbacks.
Disable This Extension	If selected, this extension will be disabled on the UCM630X.Note: The disabled extension still exists on the PBX but cannot be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.

Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Mobile Phone Number	Configure the Mobile number of the user.
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under Web GUI?PBX Settings?Voice Prompt?Language Settings. The dropdown list shows all the currently available voice prompt languages on the UCM630X. To add more languages to the list, please download the voice prompt package by selecting "Check Prompt List" under Web GUI?PBX Settings?Voice Prompt?Language Settings.

Analog Settings	
Call Waiting	Configure to enable/disable call waiting feature. The default setting is "No".
User '#' as SEND	If configured, the # key can be used as SNED key after dialing the number on the analog phone. The default setting is "Yes".
RX Gain	Configure the RX gain for the receiving channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.
Min RX Flash	Configure the minimum period of time (in milliseconds) that the hook flash must remain unpressed for the PBX to consider the event as a valid flash event. The valid range is 30ms to 1000ms. The default setting is 200ms.
Max RX Flash	Configure the maximum period of time (in milliseconds) that the hook flash must remain unpressed for the PBX to consider the event as a valid flash event. The minimum period of time is 256ms and it cannot be modified. The default setting is 1250ms.
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as Hangup on a polarity reversal. The default setting is "Yes".
Echo Cancellation	Specify "ON", "OFF" or a value (the power of 2) from 32 to 1024 as the number of taps of cancellation.Note: When configuring the number of taps, the number 256 is not translated into 256ms of echo cancellation. Instead, 256 taps mean 256/8 = 32 ms. The default setting is "ON", which is 128 taps.
3-Way Calling	Configure to enable/disable the 3-way calling feature on the user. The default setting is enabled.
Send CallerID After	Configure the number of rings before sending CID. The default setting is 1.
Fax Mode	For the FXS extension, there are three options available in Fax Mode. The default setting is "None". None: Disable Fax. Fax Gateway: If selected, the UCM630X can support the conversation and processing of Fax data from T.30 to T.38 or T.38 to T.30. only for FXS ports. Fax Detection: During a call, the fax signal from the user/trunk will be detected, and the received fax will be sent to the email address configured for the user. If an email address has been configured for the user, the fax will be sent to the Default Email Address configured in Fax/T.38->Fax Settings.

Call Transfer	
Call Forward Always	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.

CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped.All call forward settings will be ignored.
Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Allowlist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
Forwarding Exemption List	Calls from users in the forward whitelist will not be forwarded.Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
CC Settings	
Enable CC	If enabled, UCM630X will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. '-' is the connection character that will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension based on this time condition.
Use callee DOD on FWD or RS	Use the callee's DOD number as CallerID on Outgoing Forwarding or Ring Simultaneously calls.
Hotline	
Enable Hotline	If enabled, a hotline dialing plan will be activated, a pre-configured number will be used according to the selected Hotline Type.

Hotline Number	Configure the Hotline Number
Hotline Type	Configure the Hotline Type: Immediate Hotline: When the phone is off-hook, UCM630X will immediately dial the preset number Delay Hotline: When the phone is off hook, if there is no dialing within 5 seconds, UCM630X will dial the preset number.
Monitor Privilege Control	
Allow being monitored	Enable/disable the monitor privilege control feature. This option is enabled by default.
Call Monitoring Allowlist	Members of the list can spy on this extension via feature codes.
Seamless Transfer Privilege Control	
Seamless Transfer Allowlist	Members of the list can seamlessly transfer via feature code.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM630X, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→Voice Prompt→Custom Prompt: General Preference. The valid range is between 5 seconds and 600 seconds.Note: If the endpoint also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.
Skip Trunk Auth	If set to "Yes", users can skip entering the password when making outbound calls. If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering a password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via the trunk.
Enable LDAP	If enabled, this extension will be added to the LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
Use MOH as IVR ringback tone	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
Music On Hold	Select which Music On Hold class to suggest to the extension when putting the active call on hold.
Call Duration Limit	Check to enable and set the call limit the duration.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
Email Missed Calls	Send a log of missed calls to the extension's email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are: Default: All missed calls will be sent in email notifications. Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications. Missed External Call: Only missed calls from trunks will be sent in email notifications.

Specific Time	
Time Condition	Click to add Time Condition to configure a specific time for this extension.

Follow Me	
Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If the outbound calls need to check the password, we should enable this option or enable the option "Skip Trunk Auth" of the Extension. Otherwise, this Follow Me cannot call out.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Enable Destination	Configure to enable destination.
Default Destination	The call will be routed to this destination if no one in the Follow Me answers the call.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
Play Follow Me Prompt	If enabled, the Follow Me prompt tone will be played.
New Follow Me Number	Add a new Follow Me number which could be a "Local Extension" or an "External Number". The selected dial plan should have permissions to dial the defined external number.
Dialing Order	This is the order in which the Follow Me destinations will be dialed to reach the user.

Batch Add Extensions

Batch creation allows administrators to generate multiple extension accounts quickly using standardized configurations.

Batch extension creation is supported only for **SIP** and **IAX** extensions.

Batch Add SIP Extensions

To create multiple SIP extensions at once, navigate to **Extension/Trunk -> Extensions**, click **Add**, set **Select Extension Type** to SIP Extension, and set **Select Add Method** to Batch.

- The **Custom Time** and **Follow Me** tabs are grayed out and unavailable during Batch SIP creation because their parameters require individual, per-user target numbers and time schedules. Configure these features on individual extension settings after batch creation if needed.
- All other available configuration tabs function identically to single extension setup and apply globally to all newly generated extensions.
- User-specific details (such as First Name, Last Name, and Email Address) are bypassed during batch creation and can be configured per extension post-creation.

Parameter	Description
Create Number	Specify the number of SIP extensions to generate (Default: 5).
Extension Incrementation	Select the step increment between successive extension numbers (e.g., an increment of 2 starting at 1000 generates 1000, 1002, 1004...).
Extension	The starting extension number for the generated batch.
CallerID Number	Configure the Caller ID number displayed for outbound calls. Enter a custom Caller ID number to apply to all extensions in the batch, or enter "e" to use each user's extension number as their Caller ID.

SIP/IAX Password	Enter a specific SIP password to apply to all extensions in the batch, or type "r" to generate a unique random password for each extension.
User/Wave Password	Enter a specific password for User Portal and Wave client access across all extensions in the batch, or type "r" to generate a unique random password for each extension user.
Voicemail Password	Enter a specific voicemail password across all extensions in the batch, or type "r" to generate a unique random password for each extension user.

Batch Add IAX Extensions

To create multiple IAX extensions at once, navigate to **Extension/Trunk -> Extensions**, click **Add**, set **Select Extension Type** to IAX Extension, and set **Select Add Method** to Batch.

- The **Custom Time** and **Follow Me** tabs are grayed out and unavailable during Batch IAX creation.
- Standard IAX parameters across the active tabs function identically to single IAX extension setup and apply globally to all newly generated batch extensions.
- Individual user details (such as First Name, Last Name, and Email Address) are bypassed during batch creation and can be configured per extension post-creation.

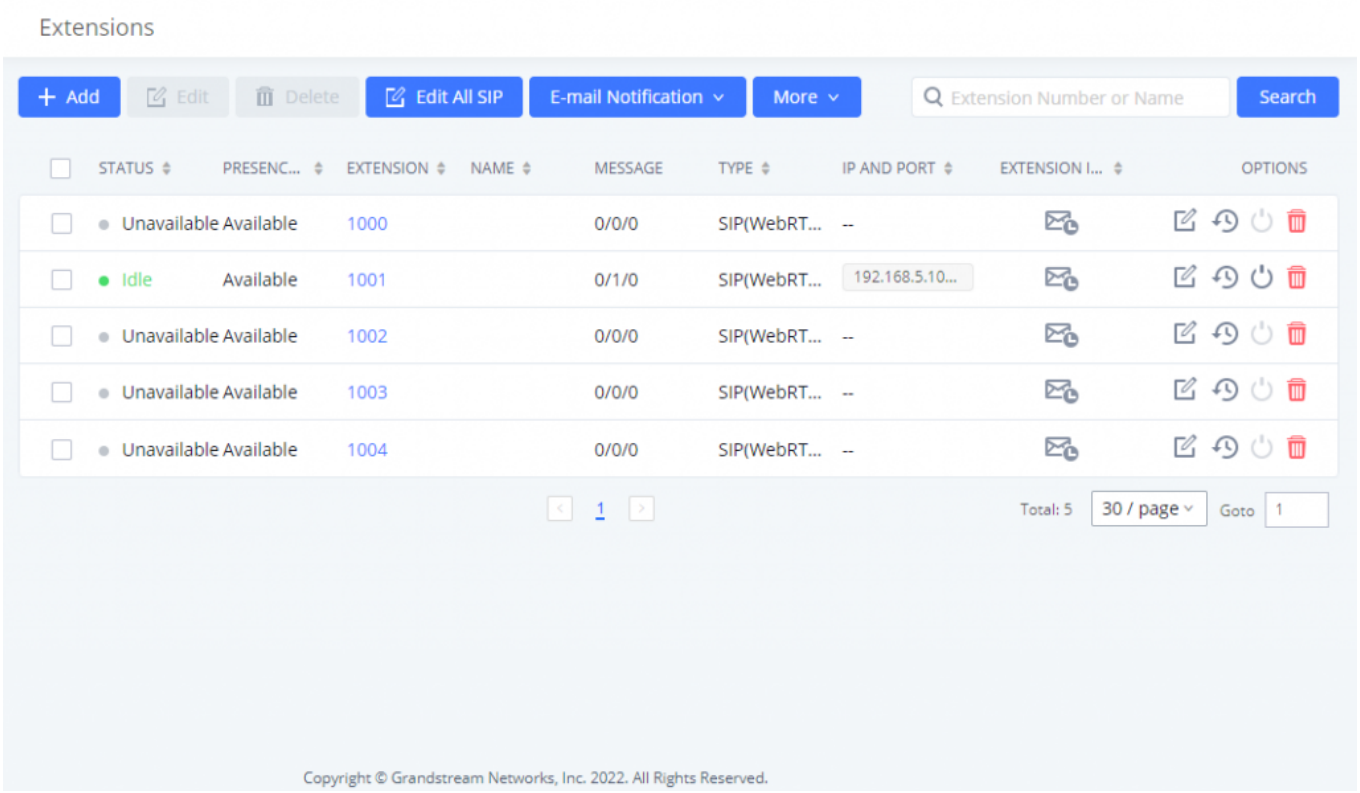
Parameter	Description
Create Number	Specify the number of IAX extensions to generate (Default: 5).
Extension Incrementation	Select the step increment between successive extension numbers (e.g., an increment of 1 generates sequential numbers).
Extension	The starting extension number for the generated batch.
CallerID Number	Configure the Caller ID number displayed for outbound calls. Enter a custom Caller ID number to apply across all extensions in the batch, or enter "e" to use each user's extension number as their Caller ID.
SIP/IAX Password	Enter a specific password to apply to all extensions in the batch, or type "r" to generate a unique random password for each extension.
User Password	Enter a specific password for User Portal access across all extensions in the batch, or type "r" to generate a unique random password for each extension user.

Batch Extension Resetting Functionality

Users can select multiple extensions and reset their settings to default by pressing the reset button and confirming the reset functionality. Once done, all settings on the Basic Settings page will be restored to default values except for Concurrent Registrations. User voicemail password will be reset to Random Password. User voicemail prompts and recordings will be deleted. User Management settings will also be restored to default except for usernames and custom privileges

Search and Edit Extension

All the UCM630X extensions are listed under Web GUI→**Extension/Trunk→Extensions**, with status, Extension, CallerID Name, Technology (SIP, IAX, and FXS), IP and Port. Each extension has a checkbox for users to "Edit" or "Delete". Also, options "Edit" , "Reboot" and "Delete" are available per extension. Users can search for an extension by specifying the extension number to find an extension quickly.



Manage Extensions

- **Status**

Users can see the following icon for each extension to indicate the SIP status.

Green: Idle

Blue: Ringing

Yellow: In Use

Grey: Unavailable (the extension is not registered or disabled on the PBX)

- **Edit single extension**

Click on

to start editing the extension parameters.

- **Reset single extension**

Click on

to reset the extension parameters to default (except concurrent registration).

Other settings will be restored to default in **Maintenance→User Management→User Information** except for username and permissions and delete the user voicemail prompt and voice messages.

This is the expected behavior when you reset an extension:

- All the data and configuration on the user side will be deleted. That includes user information, call history, call recordings, faxes, voice mails, meeting schedules and recordings, as well as chat history. However, the data related to the user will be kept on the UCM side.
- The extension will be removed from group chats and the messages sent previously by the extension will be kept. However, only other users can search through those messages while the new user of the extension cannot.
- If the extension was in a meeting schedule, the meeting will still be present. The extension will be removed from the meeting and will not be notified about the meeting.

- **Reboot the user**

Click on to send NOTIFY reboot event to the device which has a UCM630X extension already registered. To successfully reboot the user, "Zero Config" needs to be enabled on **Device Management > Zero Config > Zero Config Settings**.

- **Delete single extension**

Click on

to delete the extension. Or select the checkbox of the extension and then click on "Delete Selected Extensions".

This is the expected behavior when you delete an extension:

- The system will delete all the data of the extension except the CDR and meetings record. All the data on the user side will be erased.
- The extension will be removed from group chats and the messages sent previously by the extension will be kept. However, only other users can search through those messages while the new user of the extension cannot.

- If the extension was in a meeting schedule, the meeting will still be present. The extension will be removed from the meeting and will not be notified about the meeting.

- **Modify selected extensions**

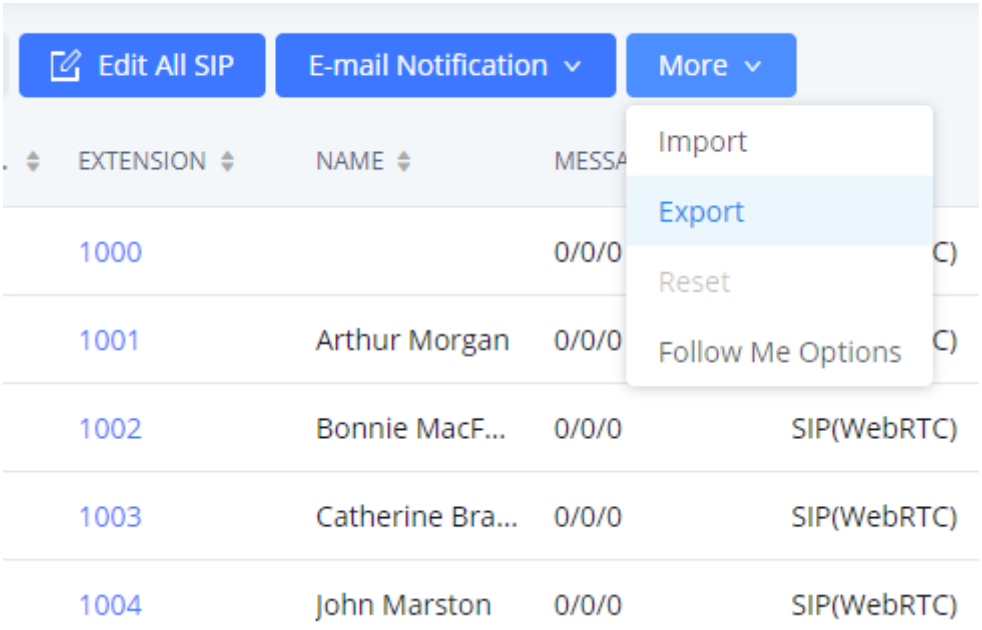
Select the checkbox for the extension(s). Then click on "Edit" to edit the extensions in a batch.

- **Delete selected extensions**

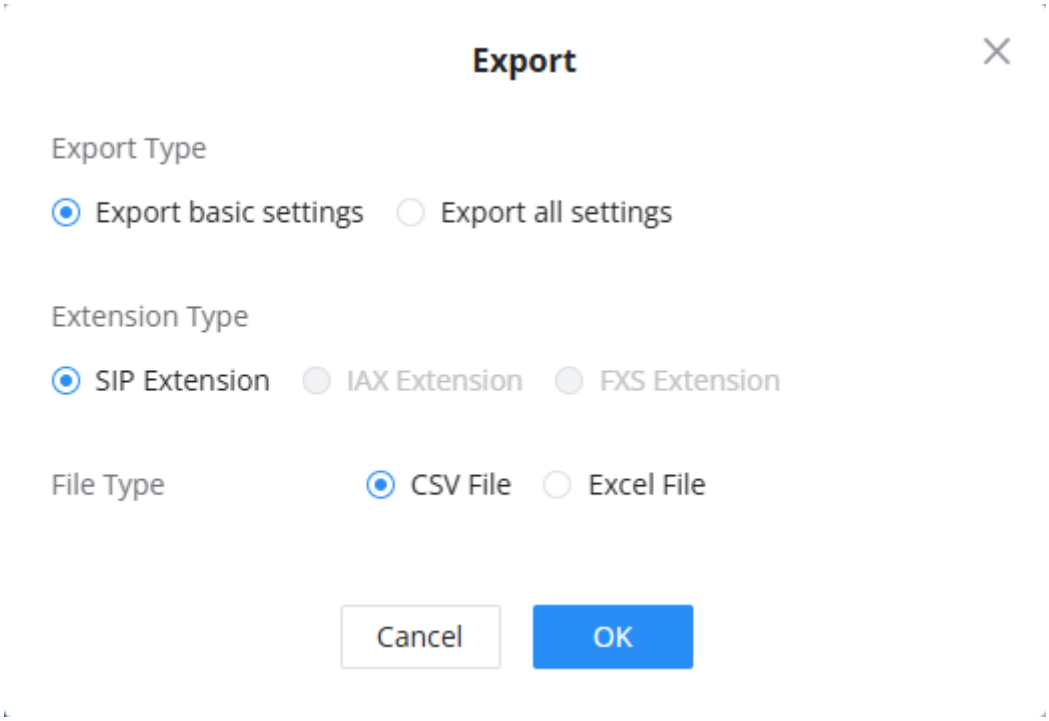
Select the checkbox for the extension(s). Then click on "Delete " to delete the extension(s).

Export Extensions

The extensions configured on the UCM630X can be exported to a CSV or XLSX format file with selected technology "SIP", "IAX" or "FXS". Click on the "Export Extensions" button and select technology in the prompt below.



Export Extensions



Export Basic Settings

Export Basic Information includes:

- Extension
- CallerID Number
- Privilege
- SIP/IAX Password
- AuthID
- Voicemail
- Voicemail Password
- Sync Contact
- First Name
- Last Name
- Email Address
- User/Wave Password

If importing extensions with no values for settings, the following will occur:

- If importing new extensions, or if **Replace** is selected as the duplicate import option, the default values for those settings will be used.
- If **Update** is selected as the duplicate import option, no changes will be made to the existing settings.

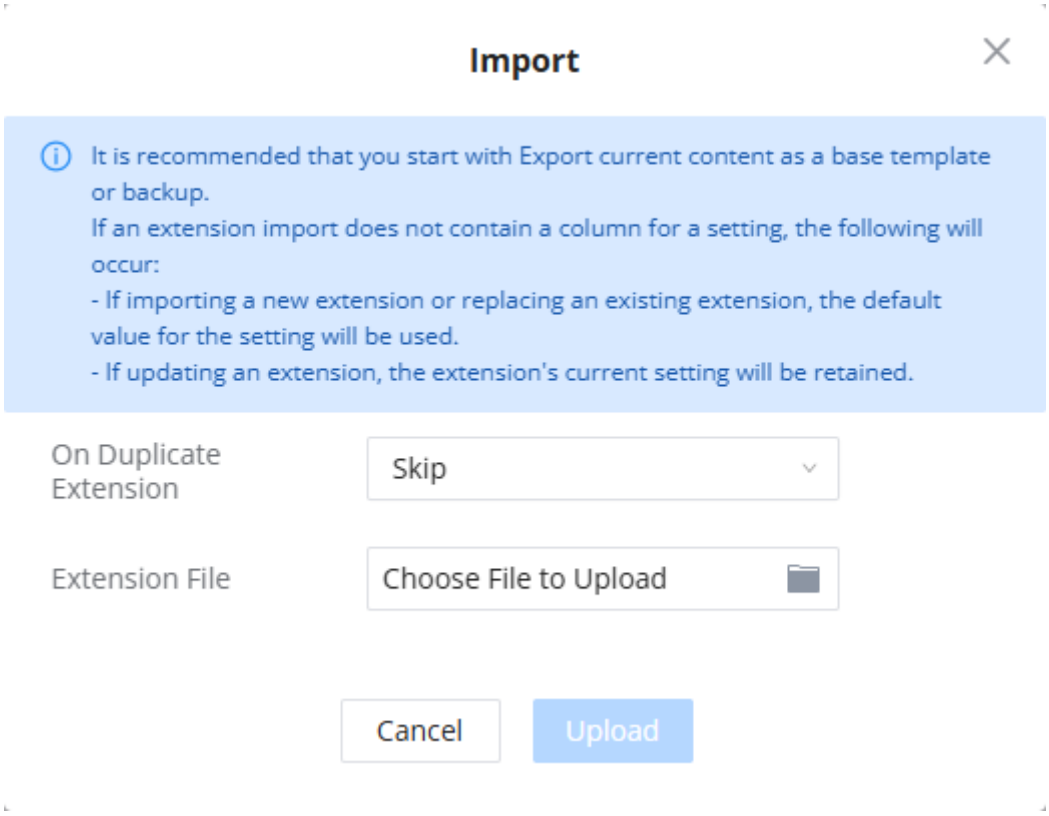
The exported file can serve as a template for users to fill in desired extension information to be imported to the UCM630X.

Import Extensions

The capability to import extensions to the UCM630X provides users the flexibility to batch add extensions with similar or different configurations quickly into the PBX system.

1. Export extension file from the UCM630X by clicking on the "Export Extensions" button.
2. Fill up the extension information you would like in the exported template.

3. Click on the "Import Extensions" button. The following dialog will be prompted.



Import Extensions

4. Select the option in "On Duplicate Extension" to define how the duplicate extension(s) in the imported file should be treated by the PBX.

- **Skip:** Duplicate extensions in the file will be skipped. The PBX will keep the current extension information as previously configured without change.

- **Delete and Recreate:** The current extension previously configured will be deleted and the duplicate extension in the file will be loaded to the PBX.

- **Update Information:** The current extension previously configured in the PBX will be kept. However, if the duplicate extension in the file has a different configuration for any options, it will override the configuration for those options in the extension.

5. Click on "Choose file to upload" to select a file from a local directory on the PC.
6. Click on "Apply Changes" to apply the imported file on the UCM630X.

Example of a file to import:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Extension	First Nam	Last Name	Technolog	Enable Vo	CallerID	SIP/IAX P	Voicemail	Skip Voic	Ring Time	Auto Reco	SRTP	Fax Mode	Strategy	Local Sub	Local Sub
2	1000			SIP(WebRT	yes		123456Adm	130270	no		off	no	None	Allow All		
3	1001			SIP(WebRT	no		123456Adm	2426	no		off	no	None	Allow All		
4	1002			SIP(WebRT	yes		123456Adm	771324	no		off	no	None	Allow All		
5	1003			SIP(WebRT	yes		123456Adm	398159	no		off	no	None	Allow All		
6	1004			SIP(WebRT	yes		123456Adm	89737	no		off	no	None	Allow All		

Import File

Field	Supported Values
Extension	Digits
Technology	SIP/SIP(WebRTC)
Enable Voicemail	yes/no/remote
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask
Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
NAT	yes/no
DTMF Mode	RFC4733/info/inband/auto
Insecure	Port
Enable Keep-alive	Yes/no
Keep-alive Frequency	Value from 1-3600
AuthID	Alphanumeric value without special characters
TEL URI	Disabled/user=phone/enabled
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Support Hot-Desking Mode	Yes/no
Dial Trunk Password	Digits
Disable This Extension	Yes/no

CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Enable T.38 UDPTL	Yes/no
Max Contacts	Values from 1-10
Enable Wave	Yes/no
Alert-Info	None/Ring 1/Ring2/Ring3/Ring 4/Ring 5/Ring 6/Ring 7/ Ring 8/Ring 9/Ring 10/bellcore-dr1/bellcore-dr2/ bellcore-dr3/ bellcore-dr4/ bellcore-dr5/custom
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Custom Auto answer	Yes/no
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.
Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits
Call-Barging Monitor	Extensions allowed to call barging
Seamless Transfer Members	Extensions allowed to seamless transfer

SIP extensions Imported File Example

Field	Supported Values

Extension	Digits
Technology	IAX
Enable Voicemail	yes/no
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask
Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
NAT	yes/no
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Require Call Token	Yes/no/auto
Max Number of Calls	Values from 1-512
Dial Trunk Password	Digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
Ring simultaneously	Yes/no
External Number	Digits

Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Limit Max time (s)	empty
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.
Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits
Call-Barging Monitor	Extensions allowed to call barging
Seamless Transfer Members	Extensions allowed to seamless transfer

IAX extensions Imported File Example

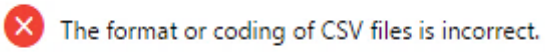
Field	Supported Values
Extension	Digits
Technology	FXS
Analog Station	FXS1/FXS2
Enable Voicemail	yes/no
CallerID Number	Digits
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
Auto Record	yes/no
Fax Mode	None/Fax Gateway/Fax Detection
Skip Trunk Auth	Yes/no/bytime
Permission	Internal/Local/National/International
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Call Waiting	Yes/no
Use # as SEND	Yes/no
RX Gain	Values from -30→6
TX Gain	Values from -30→6
MIN RX Flash	Values from: 30 - 1000

MAX RX Flash	Values from: 40 - 2000
Enable Polarity Reversal	Yes/no
Echo Cancellation	On/Off/32/64/128/256/512/1024
3-Way Calling	Yes/no
Send CallerID After	1/2
Dial Trunk Password	digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	
Enable LDAP	Yes/no
Enable Hotline	Yes/no
Hotline Type	Immediate hotline/delay hotline
Hotline Number	digits
Limit Max time (s)	empty
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.
Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits
Call-Barging Monitor	Extensions allowed to call barging

Seamless Transfer Members	Extensions allowed to seamless transfer

FXS Extensions Imported File Example

The file should contain all the above fields, if one of them is missing or empty, the UCM630X will display the following error message for missing fields.

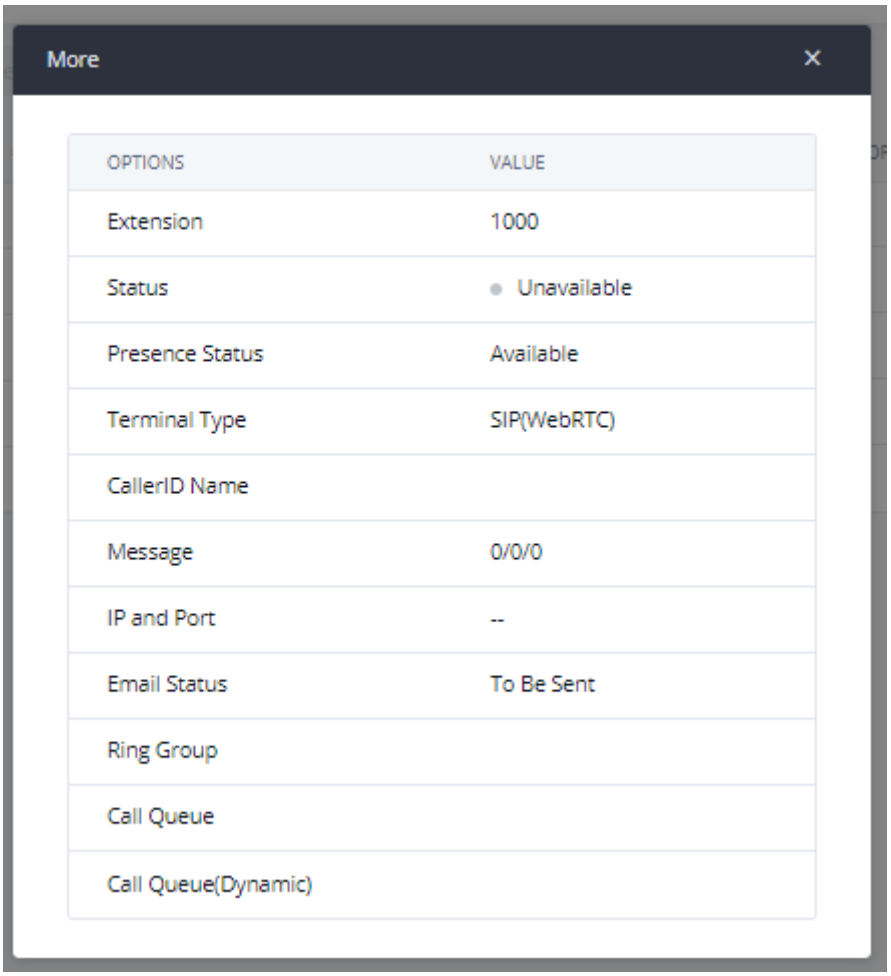


Import Error

Extension Details

Users can click on an extension number in the Extensions list page and quickly view information about it such as:

- **Extension**: This shows the Extension number.
- **Status**: This shows the status of the extension.
- **Presence status**: Indicates the Presence Status of this extension.
- **Terminal Type**: This shows the type of the terminal using this extension (SIP, FXS...etc.).
- **Caller ID Name**: Reveals the Caller ID Name configured on the extension.
- **Messages**: Shows the messages' stats.
- **IP and Port**: The IP address and the ports of the device using the extension.
- **Email status**: Show the Email status (sent, to be sent...etc.).
- **Ring Group**: Indicates the ring groups that this extension belongs to.
- **Call Queue**: Indicates the Cal Queues that this extension belongs to.
- **Call Queue (Dynamic)**: Indicates the Call Queues that this extension belongs to as a dynamic agent.

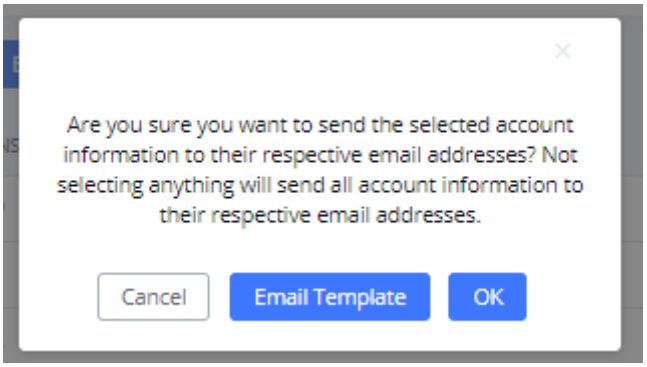


Extension Details

Email Notification

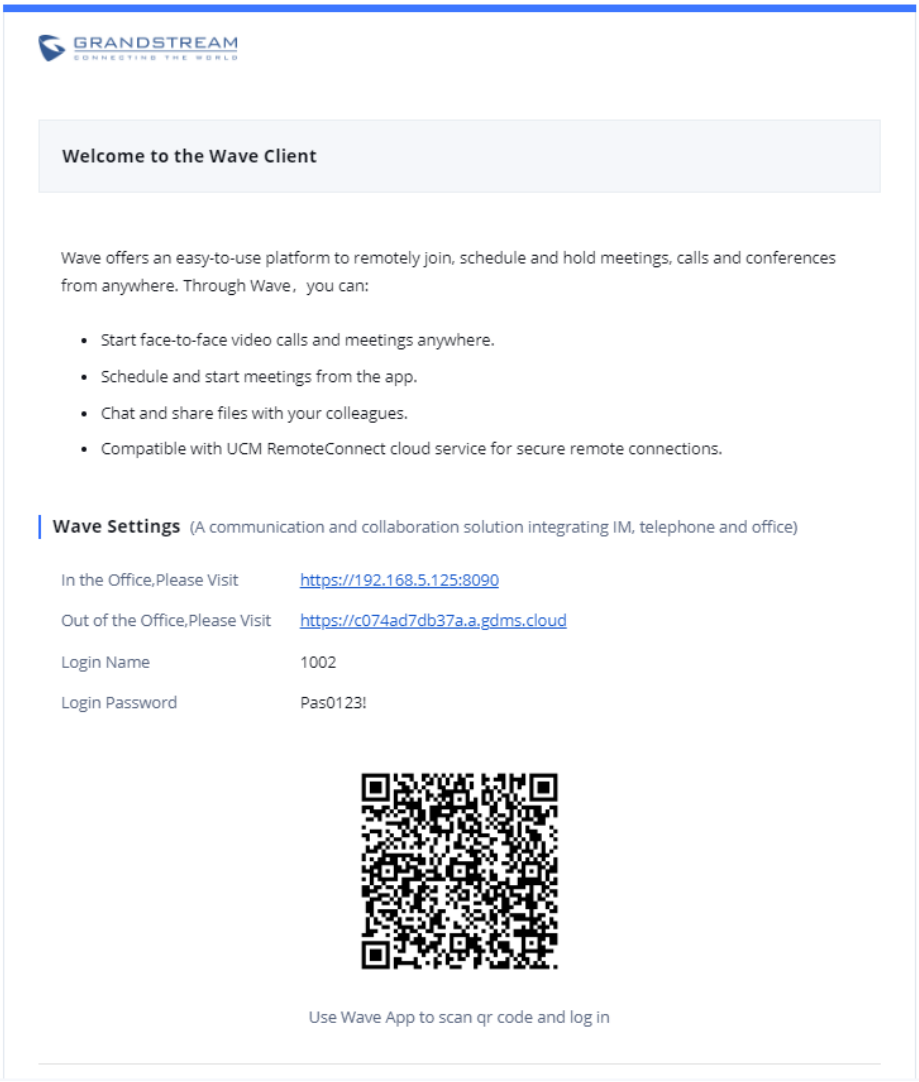
Once the extensions are created with Email addresses, the PBX administrator can click on the button "E-mail Notification" to send the account registration and configuration information to the user. Please make sure the Email setting under Web GUI→**System Settings→Email Settings** is properly configured and tested on the UCM630X before using "E-mail Notification".

When clicking on "More" > "E-mail Notification" button, the following message will be prompted on the web page. Click on OK to confirm sending the account information to all users' Email addresses.



E-mail Notification - Prompt Information

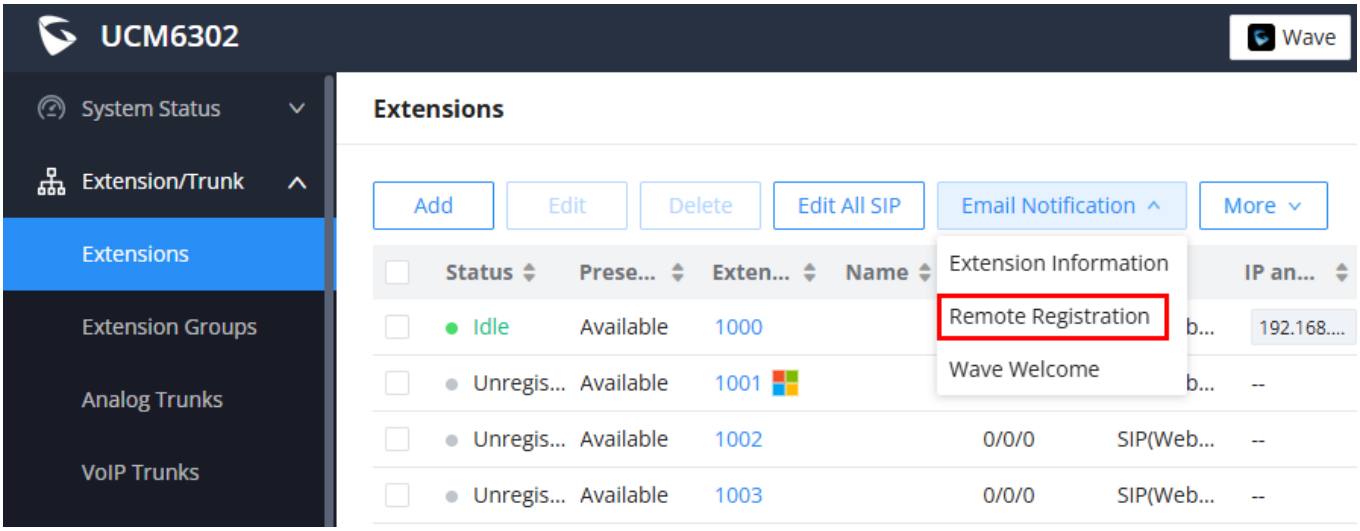
The user will receive an Email including account registration information as well as the Wave Settings with the QR code:



Wave Settings and QR Code

For security and confidentiality reasons, it is high advisable for the user to change the Wave login extension after the first time log in.

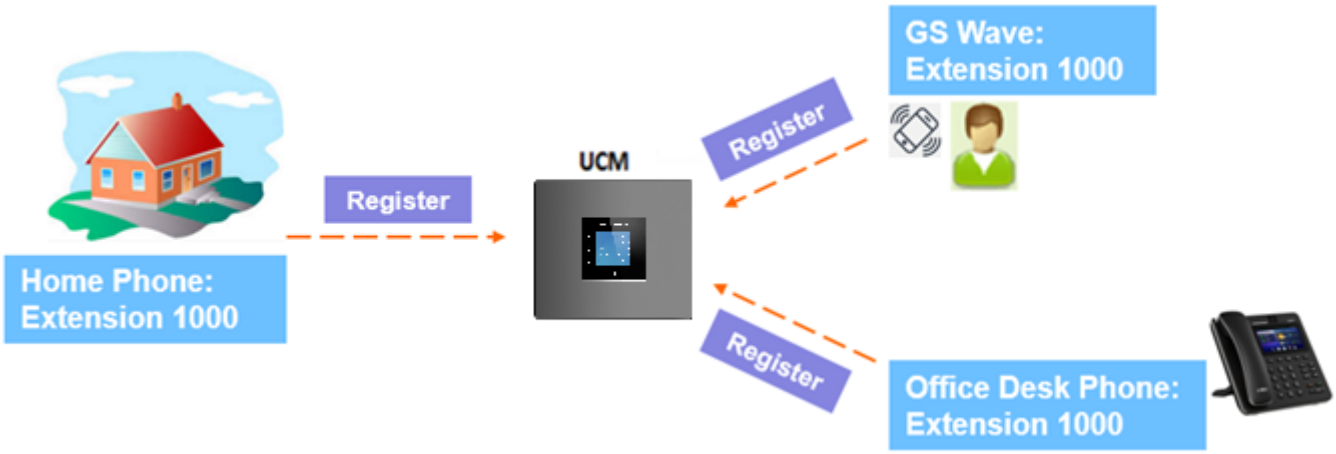
The UCM admin can also send "Remote Registration" and "Wave Welcome" as the figure below shows



Send Remote Registration Mail

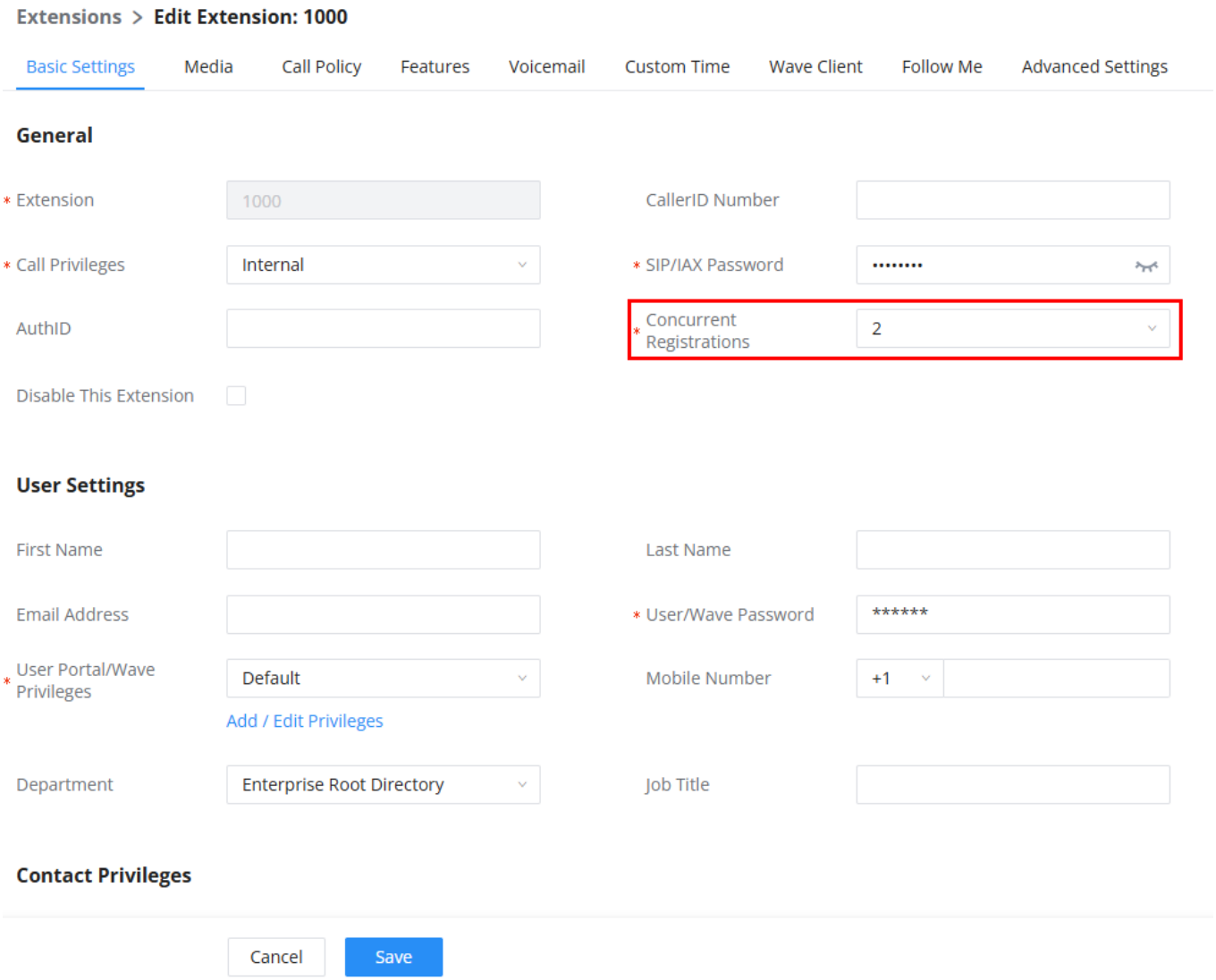
Multiple Registrations per Extension

UCM630X supports multiple registrations per extension so that users can use the same extension on devices in different locations.



Multiple Registrations per Extension

This feature can be enabled by configuring the option "Concurrent Registrations" under Web GUI **→Extension/Trunk→Edit Extension**. The default value is set to 3 registrations. The maximum is 10. When the option "1(allowed to seize) is selected, the UCM will allow newer registration attempts to seize the extension from a previously registered endpoint. To prevent this behaviour, please select the option 1.



Extension - Concurrent Registrations

SMS Message Support

The UCM630X provides built-in SIP SMS message support. For SIP end devices such as Grandstream GXP or GXV phones that support SIP message, after a UCM630X account is registered on the end device, the user can send and receive SMS messages. Please refer to the end device documentation on how to send and receive SMS messages.



Extension Groups

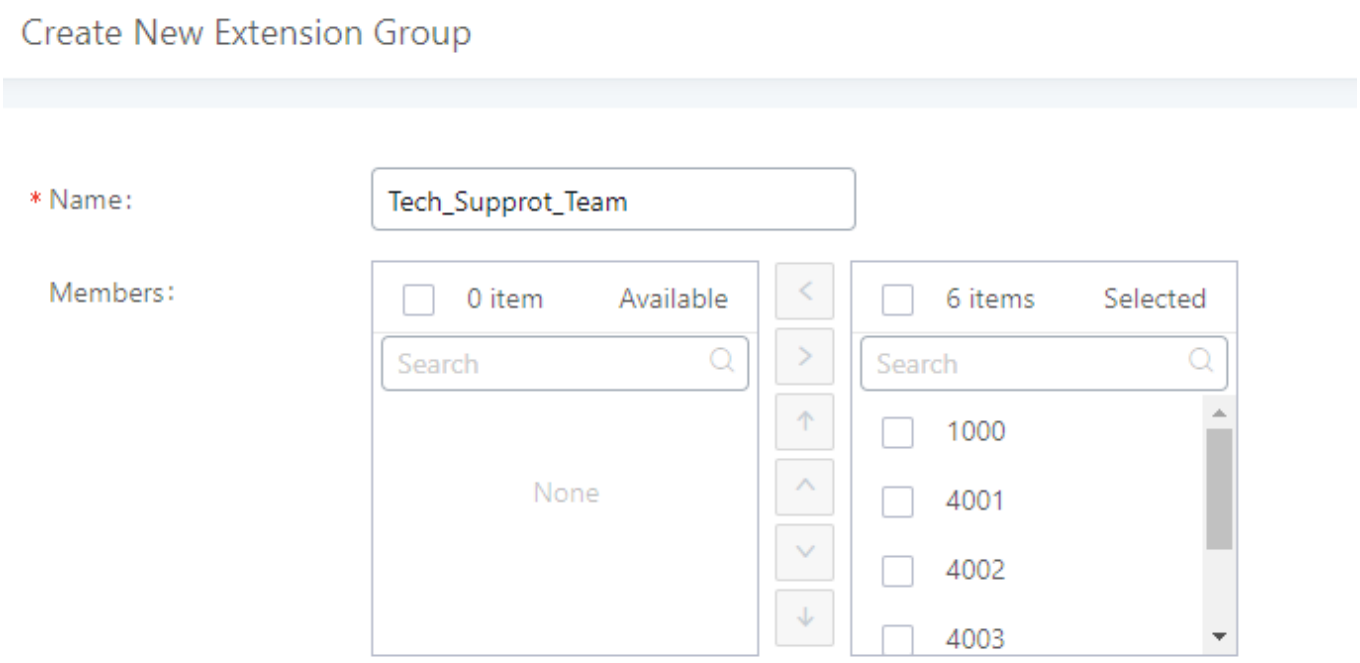
The UCM630X extension group feature allows users to assign and categorize extensions in different groups to better manage the configurations on the UCM630X. For example, when configuring "Enable Filter on Source Caller ID", users could select a group instead of each person's extension to assign. This feature simplifies the configuration process and helps manage and categorize the extensions for a business environment.

Configure Extension Groups

Extension groups can be configured via Web GUI -> **Extension/Trunk** -> **Extension Groups**.

- Click to create a new extension group.
- Click to edit the extension group.
- Click to delete the extension group.

Select extensions from the list on the left side to the right side.

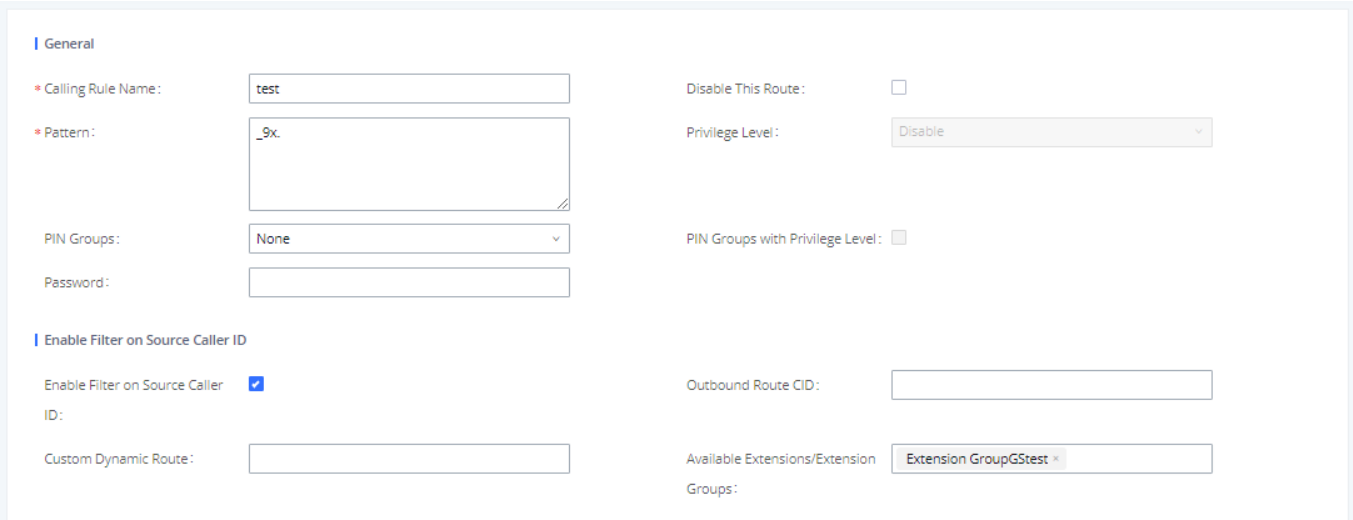


Edit Extension Group

Click on to change the ringing priority of the members selected on the group.

Using Extension Groups

Here is an example where the extension group can be used. Go to Web GUI→**Extension/Trunk**→ **Outbound Routes** and select "Enable Filter on Source Caller ID". Both single extensions and extension groups will show up for users to select.



Select Extension Group in Outbound Route

Analog Trunks

Go to Web GUI -> **Extension/Trunk** -> **Analog Trunks** to add and edit analog trunks.

- Click "Create New Analog Trunk" to add a new analog trunk.
- Click to edit the analog trunk.
- Click to delete the analog trunk.

Analog Trunk Configuration

The analog trunk options are listed in the table below.

Parameter	Description
FXO Port	Select the channel for the analog trunk. UCM6301: 1 channel UCM6302: 2 channels UCM6304: 4 channels UCM6308: 8 channels
Trunk Name	Specify a unique label to identify the trunk when listed in outbound rules, incoming rules, etc.
Advanced Options	
Disable This Trunk	If selected, the trunk will be disabled, and incoming/Outgoing calls via this trunk will not be possible.
SLA Mode	Enable this option to satisfy two primary use cases, which include emulating a simple key system and creating shared extensions on a PBX. Enable SLA Mode will disable polarity reversal.
Barge Allowed	The barge option specifies whether other stations can join a call in progress on this trunk. If enabled, the other stations can press the line button to join the call.The default setting is Yes.This option appears when SLA Mode is enabled.
Hold Access	The hold option specifies hold permissions for this trunk. If set to "Open", any station can place this trunk on hold and any other station is allowed to retrieve the call. If set to "Private", only the station that places the call on hold can retrieve the call.The default setting is Yes.
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as "Hangup" on a polarity reversal. The default setting is "No".

Polarity on Answer Delay (ms)	When the FXO port answers the call, FXS may send a Polarity Reversal. If this interval is shorter than the value of "Polarity on Answer Delay", the Polarity Reversal will be ignored. Otherwise, the FXO will On-hook to disconnect the call. The default setting is 600ms.
Current Disconnect Threshold (ms)	This is the periodic time (in ms) that the UCM630X will use to check on a voltage drop in the line. The default setting is 200. The valid range is 50 to 3000.
Ring Timeout (ms)	Configure the ring timeout (in ms). Trunk (FXO) devices must have a timeout to determine if there was a Hangup before the line is answered. This value can be used to configure how long it takes before the UCM630X considers a non-ringing line with Hangup activity. The default setting is 8000.
RX Gain	Configure the RX gain for the receiving channel of the analog FXO port. The valid range is from -13.5 (dB) to + 12.0 (dB). The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of the analog FXO port. The valid range is from -13.5 (dB) to + 12.0 (dB). The default setting is 0.
Use CallerID	Configure to enable CallerID detection.The default setting is "Yes".
Caller ID Scheme	Select the Caller ID scheme for this trunk. Bellcore/Telcordia ETSI-FSK During Ringing ETSI-FSK Prior to Ringing with DTAS ETSI-FSK Prior to Ringing with LR ETSI-FSK Prior to Ringing with RP ETSI-DTMF During Ringing ETSI-DTMF Prior to Ringing with DTAS ETSI-DTMF Prior to Ringing with LR ETSI-DTMF Prior to Ringing with RP SIN 227-BT NTT Japan Auto-Detect If you are not sure which scheme to choose, please select "Auto Detect". The default setting is "Bellcore/Telcordia".
Fax Mode	Configures how faxes to this extension will be handled. None: Faxes will not be processed. Fax Gateway: Faxes to this extension will be processed and converted from T.30 to T.38 or vice-versa. FXS/FXO ports only. The default setting is None.
FXO Dial Delay (ms)	Configure the time interval between off-hook and first dialed digit for outbound calls.
Auto Record	Enable automatic recording for the calls using this trunk. The default setting is disabled. The recording files can be accessed under Web GUI > CDR > Recording Files.
Speed Dial Out	If enabled, a # sign will be automatically added to the end of the called number for outgoing calls to improve dialing efficiency. If the FXS gateway does not support #, it may cause outgoing calls to fail. After activation, the SLA mode will be disabled.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them.For Example, User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option "Direct Callback" is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.
DAHDI Out Line Selection	This is to implement an analog trunk outbound line selection strategy.Three options are available: Ascend: When the call goes out from this analog trunk, it will always try to use the first idle FXO port. The port order that the call will use to go out if UCM6302 is used would be port 1?port 2?. Every time it will start with port 1 (if it is idle). Poll: When the call goes out from this analog trunk, it will use the port that is not used last time. And it will always use the port in the order of port 1??1??1??1??..., following the last port being used in case UCM6302, is used. Descend: When the call goes out from this analog trunk, it will always try to use the last idle FXO port. The port order that the call will use to go out if UCM6302 is used would be port 2?port 1. Every time it will start with port 2 (if it is idle). The default setting is "Ascend" mode.
Max Outgoing Calls	The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit.

Echo Cancellation Mode	The Non-Linear Processing (NLP) in echo cancellation helps to remove/suppress residual echo components that could not be removed by the LEC (Line Echo Canceller). Following modes are supported: Default: The NLP limits the signal level to the background noise level when active, and the background noise level adjustment is low. High Noise Level Adjustment: The NLP limits the signal level to the background noise level when active, and the background noise level adjustment is high. Noise Masking: The NLP sends sign noise when active, and the background noise level adjustment is high. White Noise Injection: The NLP injects white noise when active. The level corresponds to the background noise level at Sin, and the background noise level adjustment is high.
Max Incoming Calls	The max allowed number of concurrent incoming calls through the trunk. Default is 0 (no limit).
Noise Cancellation RX Frequency (Hz)	Prevents interference from low-frequency signals; when enabled, the RX frequency will only allow signals above this configured value to pass.These are the supported values: OFF 20 40 60 200 The default value is "OFF".
Noise Cancellation TX Frequency (Hz)	Prevents interference from low-frequency signals; when enabled, the TX frequency will only allow signals above this configured value to pass.These are the supported values: OFF 20 40 60 200 The default value is "OFF".
Enable Total Time Limit For Outbound Calls	If enabled, a limit will be placed on the cumulative duration of outbound calls within a specified period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.
Period	Configure the cumulative period for the total duration of outgoing calls. After reaching the next cycle, the accumulated time will be cleared, and it will start to accumulate again from 0. At the same time, the limit of the time-out trunk will be automatically lifted. If By Month is selected, the cycle will be one natural month, if Quarterly is selected, the cycle will be three months from the current month.
Total Time (m)	Configure the maximum allowed cumulative duration of outbound calls allowed by this trunk within the configured period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.
Tone Settings	
Busy Detection	Busy Detection is used to detect far-end Hangup or for detecting busy signal. The default setting is "Yes".
Busy Tone Count	If "Busy Detection" is enabled, users can specify the number of busy tones to be played before hanging up. The default setting is 2. Better results might be achieved if set to 4, 6, or even 8. Please note that the higher the number is, the more time is needed to Hangup the channel. However, this might lower the probability to get a random Hangup.
Congestion Detection	Congestion detection is used to detect far-end congestion signal. The default setting is "Yes".
Congestion Count	If "Congestion Detection" is enabled, users can specify the number of congestion tones to wait for. The default setting is 2.
Tone Country	Select the country for tone settings. If "Custom" is selected, users could manually configure the values for Busy Tone and Congestion Tone. The default setting is "United States of America (USA)".
Busy Tone	Syntax:f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]]; Frequencies are in Hz and cadence on and off are in ms.Frequencies Range: [0, 4000)Busy Level Range: (-300, 0)Cadence Range: [0, 16383].Select Tone Country "Custom" to manually configure Busy Tone value.Default value:f1=480@-50,f2=620@-50,c=500/500
Congestion Tone	Syntax:f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]]; Frequencies are in Hz and cadence on and off are in ms. Frequencies Range: [0, 4000) Busy Level Range: (-300, 0) Cadence Range: [0, 16383]. Select Tone Country "Custom" to manually configure Busy Tone value.Default value:f1=480@-50,f2=620@-50,c=250/250

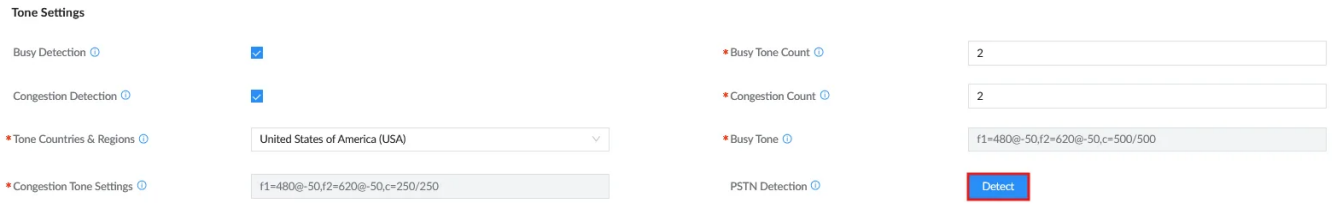
PSTN Detection	Click on "Detect" to detect the busy tone, Polarity Reversal, and Current Disconnect by PSTN. Before the detection, please make sure there is more than one channel configured and working properly. If the detection has a busy tone, the "Tone Country" option will be set as "Custom".

PSTN Detection

The UCM630X provides a PSTN detection function to help users detect the busy tone, Polarity Reversal, and Current Disconnect by making a call from the PSTN line to another destination. The detecting call will be answered and up for about 1 minute. Once done, the detecting result will show and can be used for the UCM630X settings.

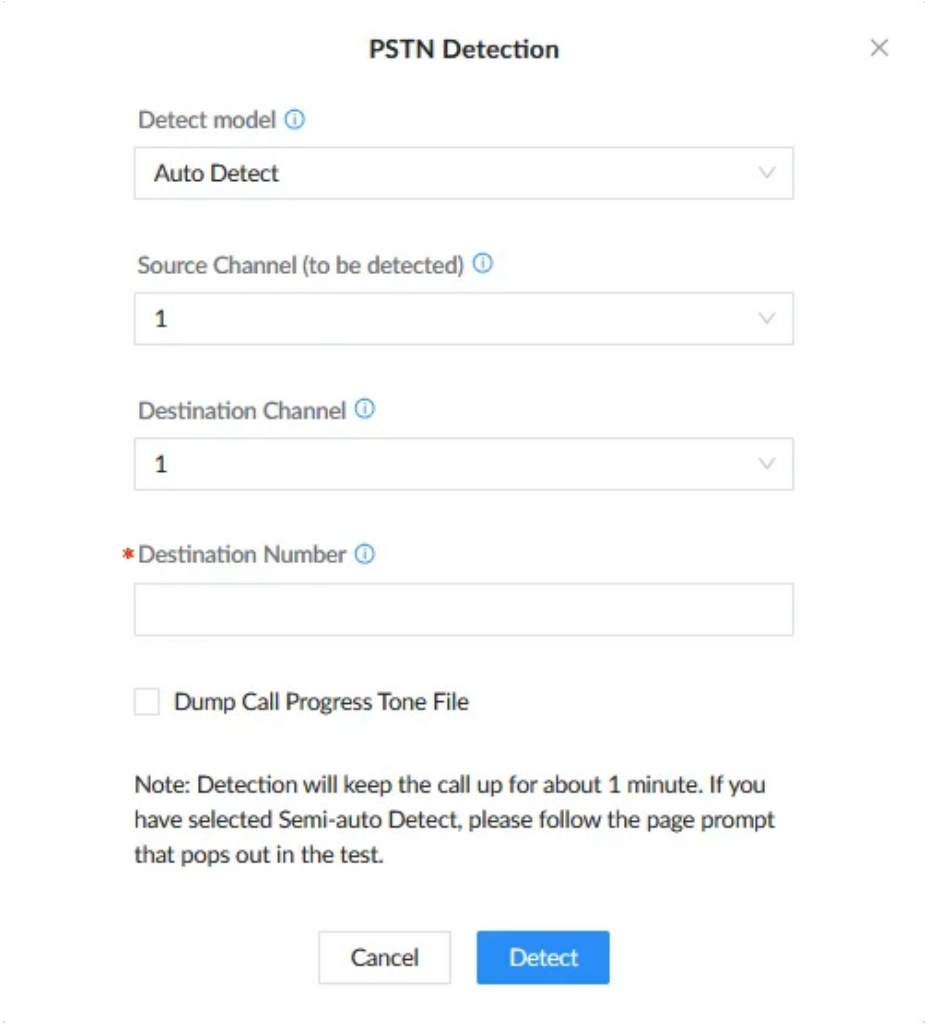
1. Go to UCM630X Web GUI -> **Extension/Trunk** -> **Analog Trunks** page.
2. Click to edit the analog trunk created for the FXO port.
3. In the window to edit the analog trunk, go to the "Tone Settings" section and there are two methods to set the busy tone.

- Tone Country. The default setting is "United States of America (USA)".
- PSTN Detection.



UCM630X FXO Tone Settings

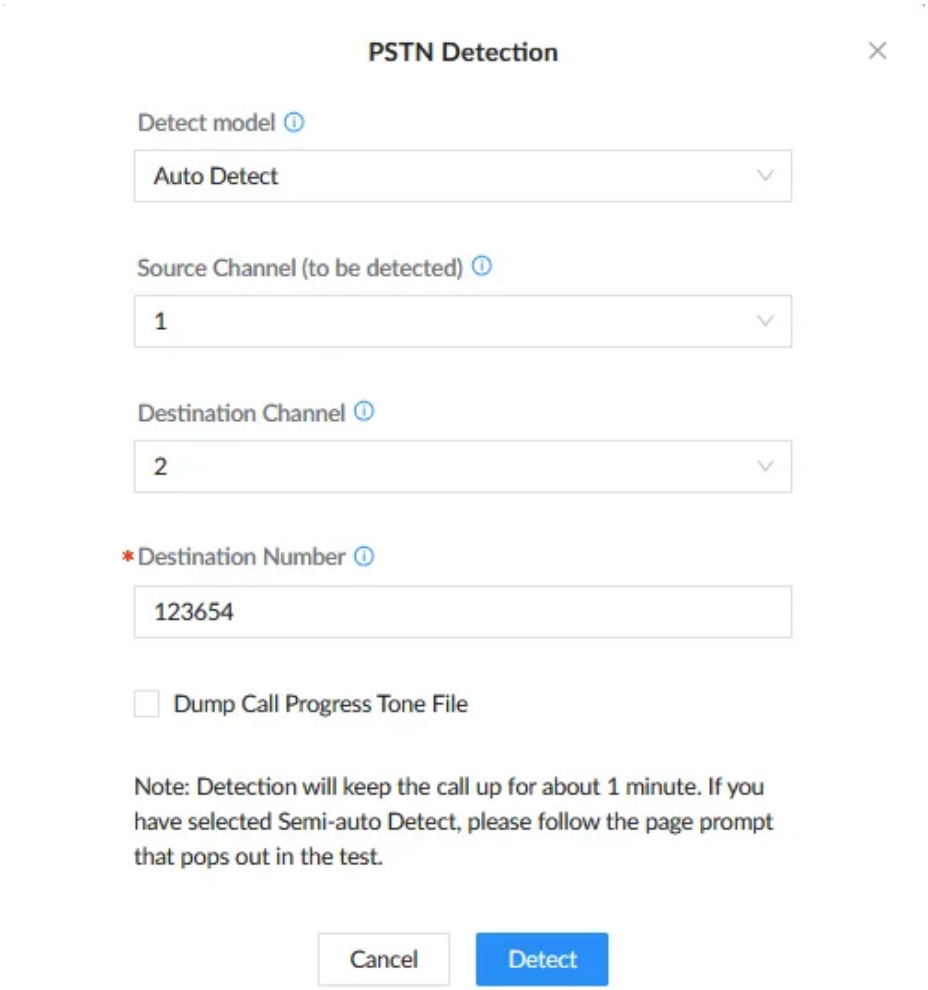
4. Click on "Detect" to start PSTN detection.



UCM630X PSTN Detection

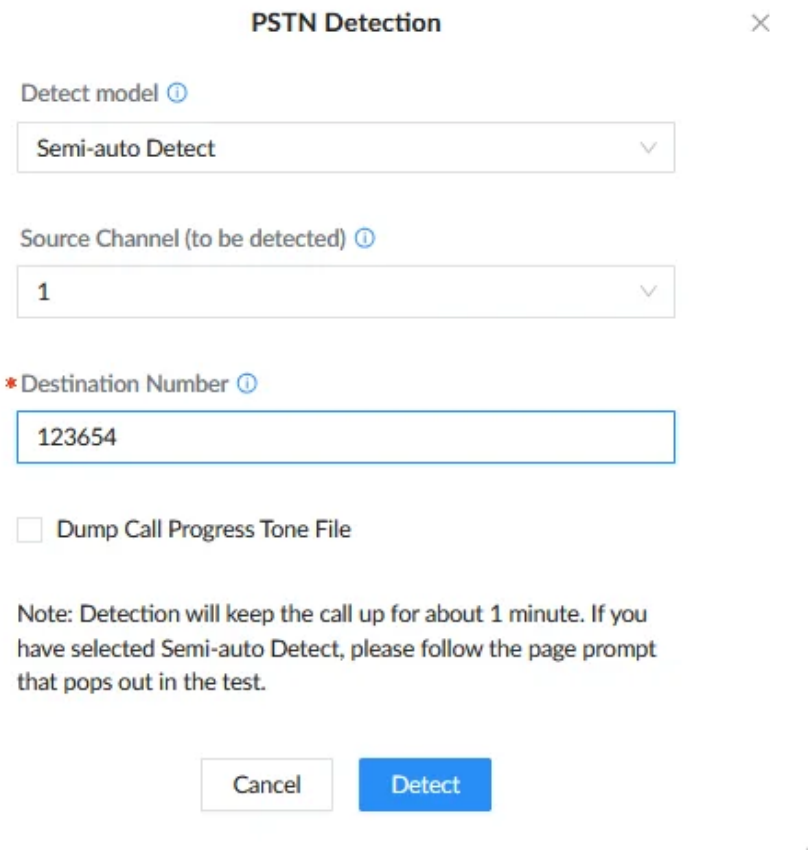
If there are two FXO ports connected to PSTN lines, use the following settings for auto-detection.

- **Detect Model**: Auto Detect.
- **Source Channel**: The source channel to be detected.
- **Destination Channel**: The channel to help detect. For example, the second FXO port.
- **Destination Number**: The number to be dialed for detecting. This number must be the actual PSTN number for the FXO port used as the destination channel.



UCM630X PSTN Detection: Auto-Detect

If there is only one FXO port connected to the PSTN line, use the following settings for auto-detection.



UCM630X PSTN Detection: Semi-Auto Detect

- **Detect Model**: Semi-auto Detect.
- **Source Channel**: The source channel to be detected.
- **Destination Number**: The number to be dialed for detecting. This number could be a cell phone number or another PSTN number that can be reached from the source channel PSTN number.

5. Click "Detect" to start detecting. The source channel will initiate a call to the destination number. For "Auto Detect", the call will be automatically answered. For "Semi-auto Detect", the UCM630X Web GUI will display a prompt to notify the user to answer or hang up the call to finish the detecting process.
6. Once done, the detected result will show. Users could save the detecting result as the current UCM630X settings.

Detect Model	Select "Auto Detect" or "Semi-auto Detect" for PSTN detection. Auto-Detect: Please make sure two or more channels are connected to the UCM630X and in idle status before starting the detection. During the detection, one channel will be used as the caller (Source Channel) and another channel will be used as a callee (Destination Channel). The UCM630X will control the call to be established and hang up between caller and callee to finish the detection. Semi-auto Detect: Semi-auto detection requires answering or hanging up the call manually. Please make sure one channel is connected to the UCM630X and in idle status before starting the detection. During the detection, the source-channel will be used as a caller and send the call to the configured Destination Number. Users will then need to follow the prompts in Web GUI to help finish the detection. The default setting is "Auto Detect".
Source Channel (to be detected)	Select the channel to be detected.
Destination Channel	Select the channel to help detect when "Auto Detect" is used.
Destination Number	Configure the number to be called to help the detection.
Dump Call Progress Tone File	Choose whether to save the calling tone file, it is not checked by default.

- The PSTN detection process will keep the call up for about 1 minute.
- If "Semi-auto Detect' is used, please pick up the call only after being informed from the Web GUI prompt.
- Once the detection is successful, the detected parameters "Busy Tone", "Polarity Reversal" and "Current Disconnect by PSTN" will be filled into the corresponding fields in the analog trunk configuration.

VoIP Trunks

Peer SIP Trunk

Peer trunk allows to create a peer-to-peer connection between two PBXs over the internet or in an internal network. This allows the calls to be exchanged between the PBXs.

Option	Description
Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send an UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
Type	Select the trunk type (e.g., Peer SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.
Auto Record	Enable automatic recording for calls using this trunk (SIP trunk only). The default setting is disabled. Recordings can be accessed under Web GUI -> CDR -> Recording Files.
Keep Original CID	Configures CID handling for forwarded outgoing calls. The default setting is "No". Yes: Keep the CID from the inbound call when dialing out. This setting overrides "Keep Trunk CID". Ensure the peer PBX supports matching user entries using the username field from the authentication line. No: Do not keep the original incoming CID. DOD: Checks if the originating extension has a DOD assigned. If assigned, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, set to "User=Phone" to attach a "User=Phone" parameter to the Request-Line and TO header in the SIP request. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. Default setting is disabled.

CallerID Number	Configure the default Caller ID number sent when making calls through this trunk. Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: CID from inbound call (Keep Original CID Enabled) -> Trunk Username/CallerID (Keep Trunk CID Enabled) -> DOD -> Extension CallerID Number -> Trunk Username/CallerID (Keep Trunk CID Disabled) -> Global Outbound CID.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them. For Example: User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option "Direct Callback" is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.
RemoteConnect Mode	If enabled, RemoteConnect parameters are set synchronously. Ensure the trunk host is allocated by GDMS or supports TLS.
Monitor Concurrent Calls	If enabled, the "Trunk Concurrent Calls" system event monitors the number of concurrent calls on this trunk and generates an alert if the threshold is exceeded. Turn on the alert for "Trunk Concurrent Calls" first.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	Enables setting a cumulative total outbound call duration limit for this SIP trunk across a specified time period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three calendar months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Media	
Codec Preference	Select the audio codec for the VoIP trunk (PCMU, PCMA, GSM, G.726, G.729, iLBC, G.722, G.722.1, G.722.1C, G.723.1, H.263, H.263p, H.264, H.265, VP8, etc.).
Packet Loss Retransmission	Configure Packet Loss Retransmission.
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure Forward Error Correction (FEC) for video.
Media Traversal Method	Select the NAT traversal method for media packets: None: No NAT traversal mechanism will be used by the UCM. ICE Support: STUN will be used as a NAT traversal mechanism. TURN Relay: TURN relay will be used to relay the media packets.
FECC	Configure to enable Far-end Camera Control.
Silence Suppression	If enabled, the UCM will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the UCM will send DTX packets instead.
SRTP	Enable SRTP for the VoIP trunk. Default setting is "No".

SRTP Crypto Suite	SRTP encryption suite priority order used by UCM for outbound calls. Priority is based on order of configuration.
ZRTP Encryption Mode	If disabled, ZRTP encryption is not supported. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.
IPVT Mode	Configures the UCM to be used exclusively for IPVT. Warning: This will lock out certain UCM features.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. May cause incompatibility when interconnecting with certain devices.
Features	
Send PPI Header	If checked, the invite message sent to trunks will contain PPI (P-Preferred-Identity) Header.
Send PAI Header	If checked, the INVITE, 18x and 200 SIP messages sent to trunks will contain P-Asserted-Identity (PAI) header. It is not possible to send both PPI and PAI headers.
PAI Header	If "Send PAI Header" is enabled and "PAI Header" is configured, the PAI header in the SIP message sent from the UCM will contain the configured value. If empty, the PAI header will contain the original CID.
Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the UCM.
Send PANI Header	If checked, the INVITE sent to the trunk will contain P-Access-Network-Info header.
Access Network Info	Access network information carried in the P-Access-Network-Info header.
Send Diversion Header	Configure whether or not send Diversion header on the trunk call. Diversion header indicates that the call has been forwarded, it includes information about the call before the forwarding like the original callee and the type of forwarding: Yes: Include the Diversion header. No Deflection: Do not include Diversion header if the diversion reason is "deflection". No: Do not include the Diversion header.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). No Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call.
Send Anonymous	If checked, the "From" header in outgoing INVITE message will be set to anonymous.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	Configure the default DTMF mode when sending DTMF on this trunk: Default: Uses global ToS SIP settings. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO message. Inband: Send DTMF using inband audio. Auto: Send DTMF using RFC4733 if offered; otherwise, inband is used.
Enable Heartbeat Detection	If enabled, the UCM630xA will regularly send SIP OPTIONS to the device to check if the device is still online. Default setting is "No".
Heartbeat Frequency (s)	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. Default setting is 60 seconds.
Max Outgoing Calls	The number of concurrent outgoing calls over the trunk at the same time. The default value 0 means no limit.
Max Incoming Calls	The max allowed number of concurrent incoming calls through the trunk.

Max Concurrent Calls	The maximum allowed number of concurrent incoming and outgoing calls going through the SIP trunk. Default value is 0 (no limit).
Response to Blocked Call	Set the response code to the caller when the concurrent calls has reached the upper limit: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
Sync LDAP Enable	Automatically sync local LDAP phonebooks to a remote peer (SIP peer trunk only). To ensure successful syncing, the remote peer must also enable this service and set the same password as the local UCM. Port 873 is used by default.
Sync LDAP Password	Password used for LDAP phonebook encryption and decryption. The password must be the same for both peers to ensure successful syncing.
LDAP Outbound Rule	Specify an outbound rule. The PBX system will automatically modify the remote contacts by adding prefix parsed from this rule.
LDAP Dialed Prefix	System will automatically modify the remote contacts by adding this prefix.
LDAP Sync Method	Specifies the sync method of the UCM. When an LDAP sync request is received, the UCM will send the phonebook data via the specified method.
LDAP Last Sync Date	Displays the timestamp of the last successful sync.
STIR/SHAKEN	Configure this feature to prevent call spoofing, robocalls and spam calls: Disabled Outgoing Attest: The UCM will only authenticate the caller ID. Incoming Verify: The UCM will only verify if the caller ID is authenticated. Both: The UCM will authenticate outgoing calls as well as verify if incoming calls are authenticated.
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. Minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. Minimum value is 1.

Register SIP Trunk

This type of SIP trunk allows registering the trunk to an account SIP trunk, which allows exchanging the calls between two PBXs. This deployment is often found when connecting the UCM to an ITSP service line.

Option	Description
Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send an UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
Type	Select the trunk type (e.g., Register SIP Trunk or Peer SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.

Auto Record	Enable automatic recording for calls using this trunk (SIP trunk only). The default setting is disabled. Recordings can be accessed under Web GUI -> CDR -> Recording Files.
Keep Original CID	Configures CID handling for forwarded outgoing calls. The default setting is "No". Yes: Keep the CID from the inbound call when dialing out. This setting overrides "Keep Trunk CID". Ensure the peer PBX supports matching user entries using the username field from the authentication line. No: Do not keep the original incoming CID. DOD: Checks if the originating extension has a DOD assigned. If assigned, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, set to "User=Phone" to attach a "User=Phone" parameter to the Request-Line and TO header in the SIP request. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. Default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when the "Register SIP Trunk" type is selected. Default setting is No.
Allow outgoing calls if registration fails	If enabled, outgoing calls can still go through even if registration to this trunk fails. Note: Unchecking "Need Registration" causes this option to be ignored.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
From User	Configure the actual username of the extension to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for the "Register SIP Trunk" type.
Verify Inbound Requests	If enabled, incoming SIP requests will be verified against authentication credentials or trunk parameters.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them.
Monitor Concurrent Calls	If enabled, the "Trunk Concurrent Calls" system event monitors the number of concurrent calls on this trunk and generates an alert if the threshold is exceeded. Turn on the alert for "Trunk Concurrent Calls" first.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	Enables setting a cumulative total outbound call duration limit for this SIP trunk across a specified time period.

Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Advanced Settings	
Codec Preference	Select the audio codec for the VoIP trunk (PCMU, PCMA, GSM, G.726, G.729, iLBC, G.722, G.722.1, G.722.1C, G.723.1, H.263, H.263p, etc.).
Packet Loss Retransmission	Configure Packet Loss Retransmission: NACK NACK+RTX(SSRC-GROUP) OFF
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure Forward Error Correction (FEC) for video.
Media Traversal Method	Configures the media traversal method (e.g., None, STUN, TURN) used for NAT traversal.
FECC	Remote Camera Management.
Silence Suppression	Enables silence suppression to save bandwidth during periods of silence.
SRTP	Enable SRTP for the call (Default: Disabled): Disabled Enabled and Enforced: SRTP is required to transmit media traffic. Optional: Negotiates whether to use SRTP based on endpoint capability.
SRTP Crypto Suite	SRTP encryption suite priority order used by UCM for outbound calls: AES_CM_128_HMAC_SHA1_80 (Default) AES_256_CM_HMAC_SHA1_80 AEAD_AES_128_GCM AEAD_AES_256_GCM
ZRTP Encryption Mode	If disabled, ZRTP encryption is not supported. Otherwise, ZRTP will be supported and prioritized over SRTP if the endpoint supports both.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. May cause incompatibility when interconnecting with certain devices.
Send PPI Header	If enabled, outgoing SIP INVITE messages contain a PPI (P-Preferred-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.
Send PAI Header	If enabled, outgoing SIP INVITE messages contain a PAI (P-Asserted-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.
DOD as From Name	If enabled, uses the extension's assigned DOD name as the "From" display name in outgoing SIP headers.
DOD as Contact User	If enabled, uses the extension's assigned DOD number as the user portion of the SIP Contact header.
Passthrough PAI Header	If checked and "Send PAI Header" is disabled, the PAI header is passed through from one side to the other.
Send PANI Header	If checked, INVITE and REGISTER messages sent to the trunk contain the P-Access-Network-Info header.
Send Diversion Header	Configure whether to send a Diversion header on trunk calls to indicate call forwarding details.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). Not Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call.
Send Anonymous	If checked, the "From" header in outgoing INVITE messages is set to anonymous.

Outbound Proxy Support	Enables outbound proxy support for this trunk. Default setting is "No".
DID Mode	Configure whether to extract the incoming call destination ID from the SIP Request-line or To-header. Default is "Request-line".
GIN Registration	If enabled, the UCM sends a GIN REGISTER to generate implicit numbers.
DTMF Mode	Configures DTMF transmission mode: Default: Uses global ToS SIP settings. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO messages. Inband: Send DTMF using inband audio (requires PCMU or PCMA). Auto: Uses RFC4733 if offered; falls back to inband.
Enable Heartbeat Detection	If enabled, regularly sends SIP OPTIONS to monitor device availability. Default setting is "No".
Max Outgoing Calls	Configures maximum concurrent outgoing calls over the trunk (Default: 0 / unlimited).
Max Incoming Calls	Configures maximum concurrent incoming calls through the trunk (Default: 0 / unlimited).
Max Concurrent Calls	Configures maximum simultaneous incoming and outgoing calls going through the SIP trunk (Default: 0 / unlimited).
Response to Blocked Call	Configures the SIP response code returned when concurrent call limits are reached: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
STIR/SHAKEN	Configures STIR/SHAKEN authentication to prevent call spoofing, robocalls, and spam: Disabled Outgoing Attest: Authenticates outgoing caller IDs. Incoming Verify: Verifies incoming caller ID authentication. Both: Authenticates outgoing calls and verifies incoming calls.
CC Settings	
Enable CC	If enabled, automatically alerts the user when a previously busy or unavailable called party becomes available.

Account SIP Trunk

This type of SIP trunk allows devices such as ATAsand gateways to trunk directly with the UCM6300 to handle and route calls.

This is especially useful when the devices do not have a static IP address for peering or if they cannot register to a UCM extension due to call handling and routing complications.

Option	Description
Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled.
Type	Select the trunk type (e.g., Account SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.
Auto Record	Enable automatic recording for calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under Web GUI -> CDR -> Recording Files.

Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports matching user entries using the "username" field from the authentication line. Yes: Keep original CID. No: Do not keep original CID. DOD: Checks if the originating extension has a DOD assigned. If it does, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
CallerID Number	Number that the trunk will try to use when making outbound calls. This field is required if "Keep Trunk CID" is enabled. CID priority from highest to lowest is as follows: From User -> Inbound Call CID (if Keep Original CID is enabled and the call is originally from another trunk) -> Trunk CID / Username (Keep Trunk CID enabled) -> DOD CID -> Extension CID -> Trunk CID / Username (Keep Trunk CID disabled) -> Global Outbound CID. Note 1: Certain providers may ignore this CID. Note 2: If this CID contains an asterisk (*), call recordings from this trunk may be lost when saving them to NAS storage.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from. This can be used to override the "From" Header.
Username	Configure the SIP account username provided by your ITSP/VoIP service provider to authenticate outgoing calls or register incoming requests on this account trunk.
Password	Configure the password associated with the SIP account username for authentication with the VoIP provider.
AuthID	Enter the Authentication ID provided by your VoIP service provider if required for SIP authentication.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them. For Example: User 2002 has dialed external number 061234575, but they were not reachable; once they have received a missed call notification on their phone, they would mostly call back the number. If the option "Direct Callback" is enabled, they will be directly bridged to user 2002 regardless of the configured inbound destination.
Monitor Concurrent Calls	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	If enabled, a limit will be placed on the cumulative duration of outbound calls within a specified period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.

Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three calendar months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Media	
Codec Preference	Select the audio codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.722.1, G.722.1C, G.723.1, G.729, iLBC, ADPCM, H.264, H.263, H.263p and H.265.
Packet Loss Retransmission	Configure Packet Loss Retransmission: NACK NACK+RTX(SSRC-GROUP) OFF
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure to enable Forward Error Correction (FEC) for video.
Media Traversal Method	Select the NAT traversal method for media packets (e.g., None, STUN/ICE, TURN Relay).
FECC	Remote Camera Management.
Silence Suppression	If enabled, the UCM will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the UCM will send DTX packets instead.
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
SRTP Crypto Suite	SRTP encryption suite used by UCM for outbound calls. Priority is based on order of configuration.
ZRTP Encryption Mode	If disabled, UCM will not support ZRTP encryption. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. These attributes may cause incompatibility when interconnecting with other devices.
Features	
Send PPI Header	If enabled, the SIP INVITE message sent to the trunk will contain a PPI (P-Preferred-Identity) header. The default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled at the same time. Only one of the two headers can be contained in the SIP INVITE message.
Send PAI Header	If enabled, the SIP INVITE message sent to the trunk will contain a PAI (P-Asserted-Identity) header including configured PAI Header. The default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled at the same time. Only one of the two headers can be contained in the SIP INVITE message.
PAI Header	If "Send PAI Header" is enabled and "PAI Header" is configured as "123456" for instance, the PAI header in the SIP message sent from the UCM will contain "123456". If "Send PAI Header" is enabled and "PAI Header" is configured as "empty", the PAI header in the SIP message sent from the UCM will contain the original CID.
Passthrough PAI Header	If checked and the option "Send PAI Header" is not checked, the PAI header will be passthrough from one side to the other side.
Send PANI Header	If checked, the INVITE and REGISTER sent to the trunk will contain the P-Access-Network-Info header.
Access Network Info	The access network information in the P-Access-Network-Info header.

Send Diversion Header	Configure whether or not send Diversion header on the trunk call. Diversion header indicates that the call has been forwarded, it includes information about the call before the forwarding like the original callee and the type of forwarding. Yes: Include the Diversion header. No Deflection: Do not include Diversion header if the diversion reason is "deflection". "Deflection" is used as a diversion reason when calls are rerouted to an external number, either through Follow Me or on the inbound route level. No: Do not include the Diversion header.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). Not Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call. This prevents upstream carrier metadata or internal routing info from passing through to external destinations.
Send Anonymous	If checked, the "From" header in the outgoing INVITE message will be set to anonymous.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	Configure the default DTMF mode when sending DTMF on this trunk. Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under Web GUI -> PBX Settings -> SIP Settings -> ToS. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO message. Inband: Send DTMF using inband audio. This requires a 64-bit codec, i.e., PCMU and PCMA. Auto: Send DTMF using RFC4733 if offered; otherwise, inband is used.
Enable Heartbeat Detection	If enabled, the UCM630X will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency (s)	When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Max Outgoing Calls	The number of concurrent outgoing calls over the trunk at the same time. The default value is 0, which indicates that no limit is set.
Max Incoming Calls	The maximum allowed number of concurrent incoming calls through the trunk. Default is 0 (no limit).
Max Concurrent Calls	The maximum allowed number of concurrent incoming and outgoing calls going through the SIP trunk. Default value is 0 (no limit).
Response to Blocked Call	Set the response code to the caller when the concurrent calls has reached the upper limit: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
STIR/SHAKEN	Configure this feature to prevent call spoofing, robocalls, and spam calls. Disabled Outgoing Attest: The UCM will only authenticate the caller ID. Incoming Verify: The UCM will only verify if the caller ID is authenticated. Both: The UCM will authenticate outgoing calls as well as verify if incoming calls are authenticated.
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

IAX Trunk Configuration

Type	Select the VoIP trunk type. Peer IAX Trunk Register IAX Trunk
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
Username	Enter the username to register to the trunk from the provider when the "Register IAX Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when the "Register IAX Trunk" type is selected.
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID Number	The number that the trunk will try to use when making outbound calls. CID priority from highest to lowest is as follows: From User (register trunk only) >>> Inbound Call CID (if Keep Original CID is enabled and the call is originally from another trunk) >>> Trunk CID (Keep Trunk CID enabled) >>> DOD CID >>> Extension CID >>> Register Trunk Username (Keep Trunk CID disabled) >>> Global Outbound CID.Note 1: Certain providers may ignore this CID. Note 2: If this CID contains an asterisk (*), call recordings from this trunk might be lost when saving them to NAS storage.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.

Create New IAX Trunk

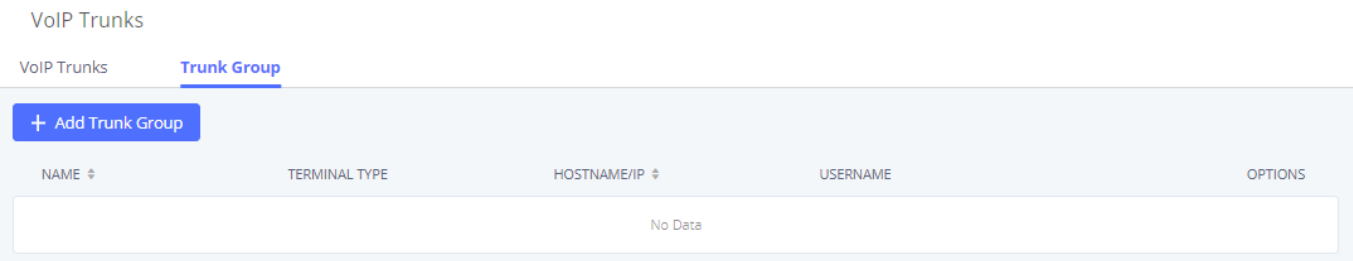
Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call.From the user (Register Trunk Only) ? CID from inbound call (Keep Original CID Enabled) ? Trunk Username/CallerID (Keep Trunk CID Enabled) ? DOD ? Extension CallerID Number ? Trunk Username/CallerID (Keep Trunk CID Disabled) ? Global Outbound CID.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Username	Enter the username to register to the trunk from the provider.
Password	Enter the password to register to the trunk from the provider.
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p and VP8.
Enable Heartbeat Detection	If enabled, the UCM630X will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".

Heartbeat Frequency	When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default setting is 0, which means no limit.

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call.CID from inbound call (Keep Original CID Enabled) ? Trunk Username/CallerID (Keep Trunk CID Enabled) ? DOD ? Extension CallerID Number ? Trunk Username/CallerID (Keep Trunk CID Disabled) ? Global Outbound CID..
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p and VP8.
Enable Heartbeat Detection	If enabled, the UCM630X will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default setting is 0, which means no limit.

Trunk Groups

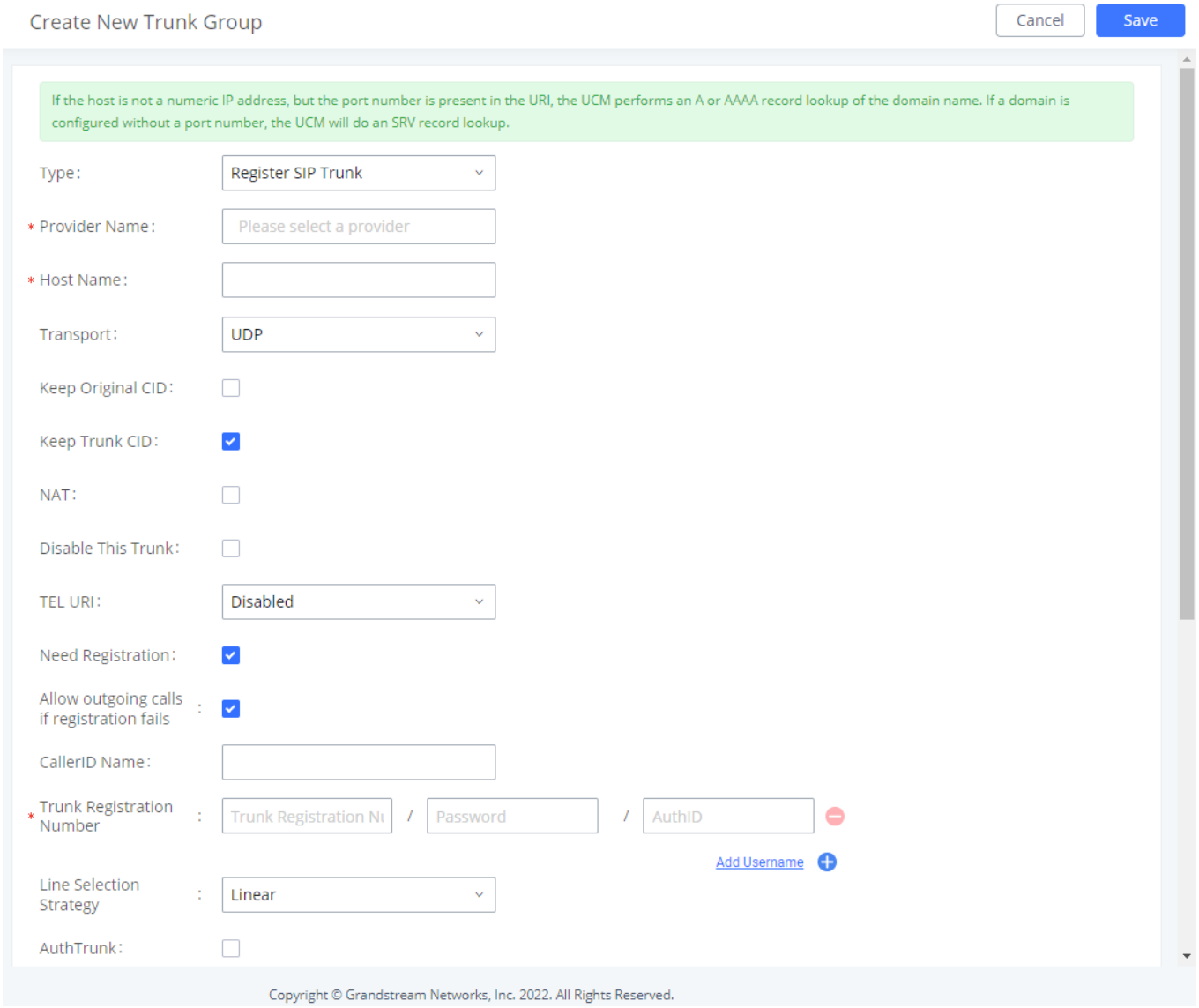
Users can create VoIP Trunk Groups to register and easily apply the same settings on multiple accounts within the same SIP server. This can drastically reduce the amount of time needed to manage accounts for the same server and improve the overall cleanliness of the web UI.



Trunk Group

Once creating the new trunk group and configuring the SIP settings, users can add multiple accounts within the configured SIP server by pressing the button and configuring the username, password, and

authentication ID fields.



Trunk Group Configuration

Trunk Name	Create a unique label to easily identify the trunk for inbound route configuration.
Disable This Trunk	Check this box to disable this trunk.
Auto Record	If enabled, calls handled with this extension/trunk will automatically be recorded.
Monitor Concurrent Calls	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
WebRTC Inbound Link Address	This link can be embedded onto a web page. Clicking the link will connect to a pre-configured WebRTC trunk destination. You can also enter this link in the browser address bar to directly access and test WebRTC calls.

Direct Outward Dialing (DOD)

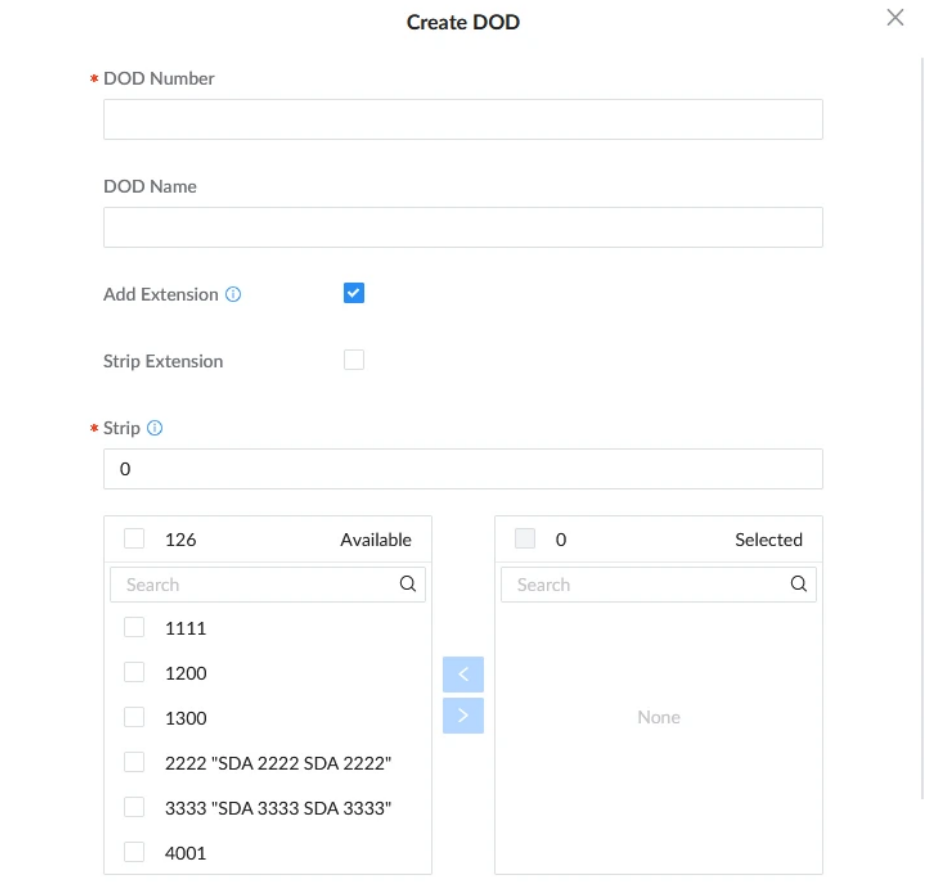
The UCM630X provides Direct Outward Dialing (DOD), which is a service of a local phone company (or local exchange carrier) that allows subscribers within a company's PBX system to connect to outside lines directly.

Example of how DOD is used:

Company ABC has a SIP trunk. This SIP trunk has 4 DIDs associated with it. The main number of the office is routed to an auto attendant. The other three numbers are direct lines to specific users of the company. Now when a user makes an outbound call their caller ID shows up as the main office number. This poses a problem, as the CEO would like their calls to come from their direct line. This can be accomplished by configuring DOD for the CEO's extension.

Steps to configure DOD on the UCM630X:

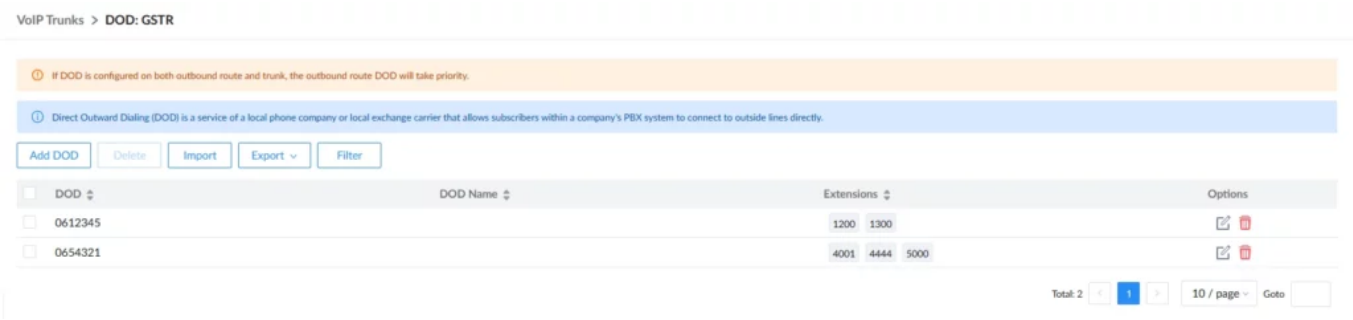
1. To setup DOD go to UCM630X Web GUI→**Extension/Trunk→VoIP Trunks** page.
2. Click on the "DOD" icon to access the DOD options for the selected SIP Trunk.
3. Click "Add DOD" to begin your DOD setup
4. Enter a SIP trunk DID number in the "DOD number" field. In this example, ABC company has a total of 4 DID numbers. Enter the phone number used by the CEO here.
5. When adding extensions, you can choose whether to "Enable Strip" according to your needs. If it is enabled, you can configure the number (0-64) that will be stripped from the extension number before being added to the DOD number. For example, if the entered digit is 2, and the DOD number for extension 4002 is 1122, then dialing out from 4002, 112202 will be used as the caller ID (DOD).
6. Select an extension from the "Available Extensions" list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO's extension. After making the selection, click on the button to move the extension(s) to the "Selected Extensions" list.



DOD Extension Selection

7. Click "Save" at the bottom.

Once completed, the user will return to the **EDIT DOD** page that shows all the extensions that are associated with a particular DOD.



Edit DOD

From this page users can:

- Add Direct Outward Dialing (DOD) entries manually.
- Import DOD entries from CSV or XLSX files.
- Export DOD entries to CSV or XLSX files.
- Filter DOD entries by number or name.
- Select multiple DOD entries for bulk operations.
- Delete one or multiple selected DOD entries in batch.

For DOD importing, please refer to the screenshot below for the template used.

	A	B	C	D	E	F	G
1	DOD Number	DOD Name	Add Extension	Local Members	Ldap Members	Enable Strip	Strip Number
2	2.12555E+11	DOD1	no	1,002,100,310,051,000		no	0
3							
4							
5							
6							
7							

DOD CSV file Template

If the user imports a DOD number that had already been added. The UCM will prompt to skip, replace, or update the DOD which is already added.

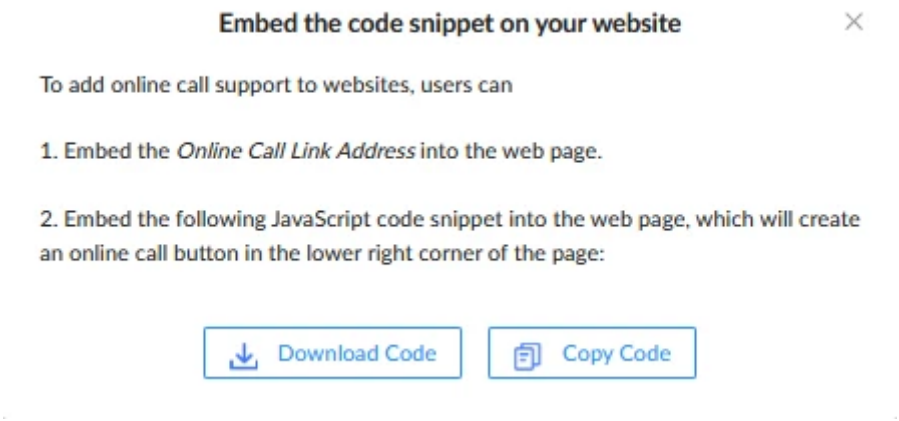
WebRTC Trunks

WebRTC (Web Real-Time Communication) is a real-time framework that enables audio and video communication directly through web browsers. The UCM63xx series supports creating WebRTC trunks to connect web applications with the PBX, allowing visitors or customers to initiate calls or join meetings directly from a website.



For a detailed step-by-step walkthrough on setting up and integrating WebRTC trunks, please refer to the WebRTC Trunk Guide.

Administrators can configure parameter settings for each WebRTC trunk and easily integrate call options into their web pages using the generated link addresses or script code snippets.



Below is a table that describes the options to configure when setting up this feature:

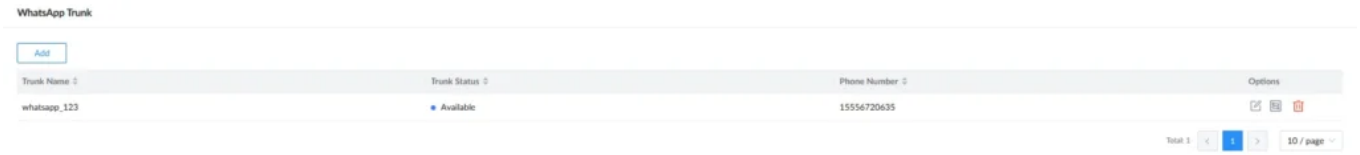
Parameter	Description
Basic Settings	
Trunk Name	Create a unique label to easily identify the trunk for inbound route configuration.
Disable This Trunk	Check this box to disable this trunk.
Auto Record	If enabled, calls handled with this trunk will automatically be recorded.
Allow Video Calling	Enables video call support for WebRTC connections established over this trunk.
One-Click Dialing	If enabled, calls are initiated immediately upon clicking the web link without requiring secondary confirmation or user prompts.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) to optimize audio packet handling and stability over web networks.
Monitor Concurrent Calls	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured threshold.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
WebRTC Inbound Link Address	Displays the unique URL generated for this trunk. This link can be embedded into a web page or entered directly in a browser address bar to initiate calls.
Advanced Settings	
Packet Loss Retransmission	Configures packet loss recovery methods (e.g., NACK+RTX) to maintain call quality during network congestion.
Codec Preference	Specifies and prioritizes the supported audio and video codecs (e.g., PCMU, PCMA, Opus, G.722, H.264) used for WebRTC trunk calls.

Please note that in order to use WebRTC Trunk feature, the UCM must have a paid RemoteConnect plan. For more information, please refer to the following link: https://ucmrc.gdms.cloud/plans

WhatsApp Trunk

The WhatsApp Trunk feature allows the UCM Series to integrate directly with Meta WhatsApp Business

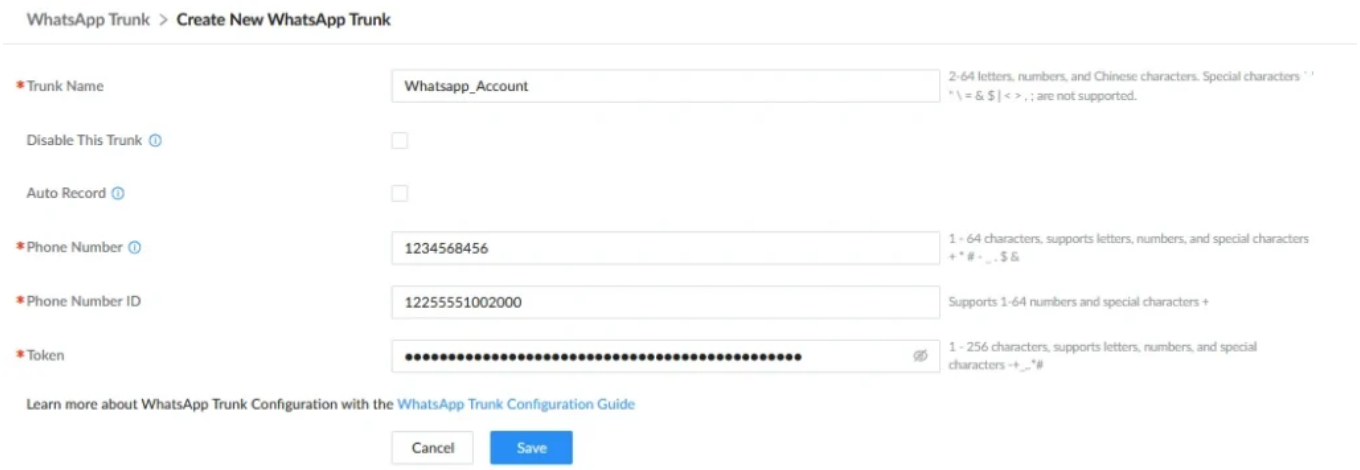
accounts as a specialized SIP trunk. Once configured, businesses can handle incoming voice calls initiated by customers from WhatsApp, as well as make outbound WhatsApp voice calls directly to authorized clients through Wave applications or registered endpoints.



To use the WhatsApp Trunk feature, the UCM must have a supported RemoteConnect plan.

For detailed step-by-step instructions on obtaining API credentials, setting up Meta WhatsApp Business developer accounts, and configuring webhook integrations, please refer to the dedicated WhatsApp Trunk Configuration Guide.

To create a new WhatsApp Trunk, go to **Extension/Trunk-> WhatsApp Trunk** and click on **Add**.



Configure the parameters as described in the table below:

Parameter	Description
Trunk Name	Enter a unique label to identify the WhatsApp Trunk across inbound routes and reporting. Supports 2-64 alphanumeric characters, Chinese characters, and spaces. Special characters ` ' " \ = & $ | < > , ; are not supported.
Disable This Trunk	If selected, the trunk will be disabled. Inbound and outbound WhatsApp calls passing through this trunk will be blocked.
Auto Record	If enabled, all calls handled by this WhatsApp Trunk will automatically be recorded. Recordings can be accessed under CDR -> Recording Files.
Phone Number	Enter the business WhatsApp phone number associated with the account. Supports 1-64 characters including digits, letters, and special characters + * # - _ . $ &.
Phone Number ID	Enter the unique Phone Number ID assigned to the business number in the Meta WhatsApp Business API console. Supports 1-64 characters including numbers and the + symbol.
Token	Enter the Meta WhatsApp API authentication Token. Supports 1-256 characters including letters, numbers, and special characters - + _ . * #.

Inbound and Outbound Whatsapp Routing

Inbound Routing (Manual)

Because inbound call matching is strictly tied to the trunk's unique phone number, each WhatsApp Trunk supports exactly one dedicated Inbound Route and must be configured manually:

1. Navigate to **Extension/Trunk->Inbound Routes**.
2. In the top-right trunk selection dropdown, choose the target **WhatsApp Trunk**.
3. Click **Add**.
4. Enter an **Inbound Rule Name** and select the desired **Default Destination**.
5. Click **Save** and **Apply Changes**.

Incoming calls arriving via a WhatsApp Trunk are automatically tagged in CDR logs as WhatsApp call types.

Outbound Routing (Automatic Provisioning)

When a WhatsApp Trunk is created on the UCM, the system automatically creates a default outbound route bound to the trunk's unique phone number.

Manual outbound route configuration is not required. When a Wave user initiates an outbound call to an authorized WhatsApp client number, Wave attaches a SIP header containing the trunk number.

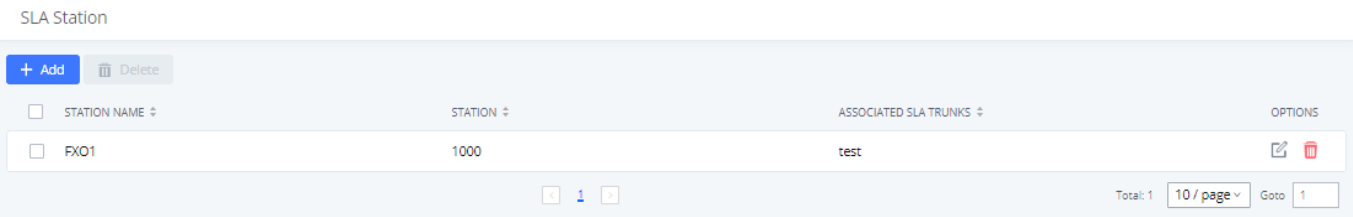
The UCM automatically matches the request header to the default outbound route associated with that WhatsApp Trunk and places the call.

SLA Station

The UCM630X supports SLA (Shared Line Appearance) that allows mapping the key with LED on a multi-line phone to different external lines. When there is an incoming call and the phone starts to ring, the LED on the key will flash in red and the call can be picked up by pressing this key. This allows users to know if the line is occupied or not. The SLA function on the UCM630X is like BLF but SLA is used to monitor external lines, i.e., analog trunk on the UCM630X. Users could configure the phone with BLF mode on the MPK to monitor the analog trunk status or press the line key pick-up call from the analog trunk on the UCM630X.

Create/Edit Shared Line Appearance Station

Shared Line Appearance Station can be configured on Web GUI→**Extension/Trunk→SLA Station.**



SLA Station

- Click on to add an Shared Line Appearance Station.
- Click on to edit the Shared Line Appearance Station. The following table shows the SLA Station configuration parameters.
- Click on to delete the Shared Line Appearance Station.

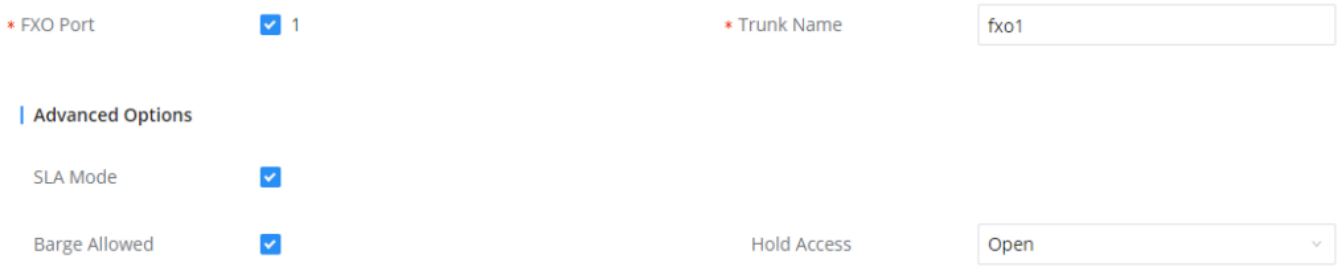
Station Name	Configure a name to identify the SLA Station.
Station	Specify a SIP extension as a station that will be using SLA.

Available SLA Trunks	Existing Analog Trunks with SLA Mode enabled will be listed here.
Associated SLA Trunks	 Select a trunk for this SLA from the Available SLA Trunks list. Click on to arrange the order. If there are multiple trunks selected, when there are calls on those trunks at the same time, pressing the LINE key on the phone will pick up the call on the first trunk here.
SLA Station Options	
Ring Timeout	Configure the time (in seconds) to ring the station before the call is considered unanswered. No timeout is set by default. If set to 0, there will be no timeout.
Ring Delay	Configure the time (in seconds) for a delay before ringing the station when a call first comes in on the shared line. No delay is set by default. If set to 0, there will be no delay.
Hold Access	This option defines the competence of the hold action for one particular trunk. If set to "open", any station could hold a call on that trunk or resume one held session; if set to "private", only the station that places the trunk call on hold could resume the session. The default setting is "open".

SLA Station Configuration Parameters

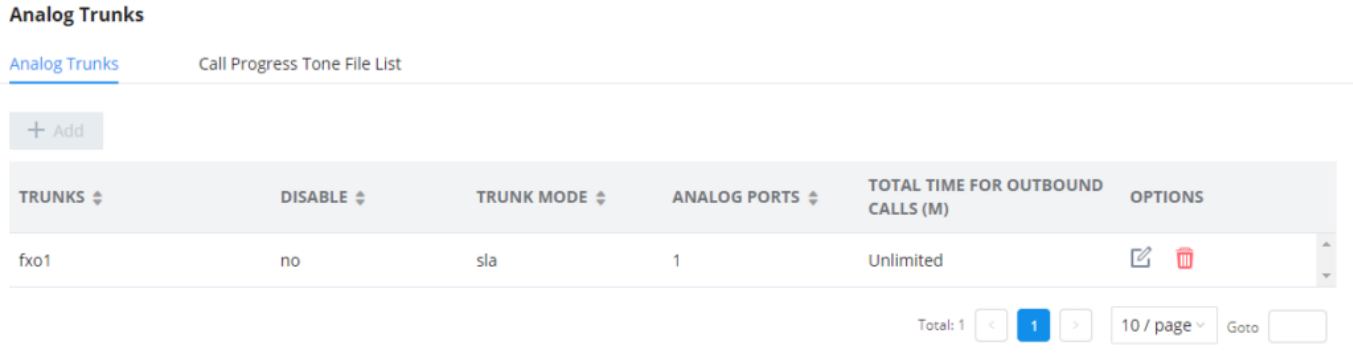
Sample Configuration

1. On the UCM630X, go to Web GUI→**Extension/Trunk→Analog Trunks** page. Create an analog trunk or edit the existing analog trunk. Make sure "SLA Mode" is enabled for the analog trunk. Once enabled, this analog trunk will be only available for the SLA stations created under Web GUI→**Extension/Trunk→SLA Station** page.



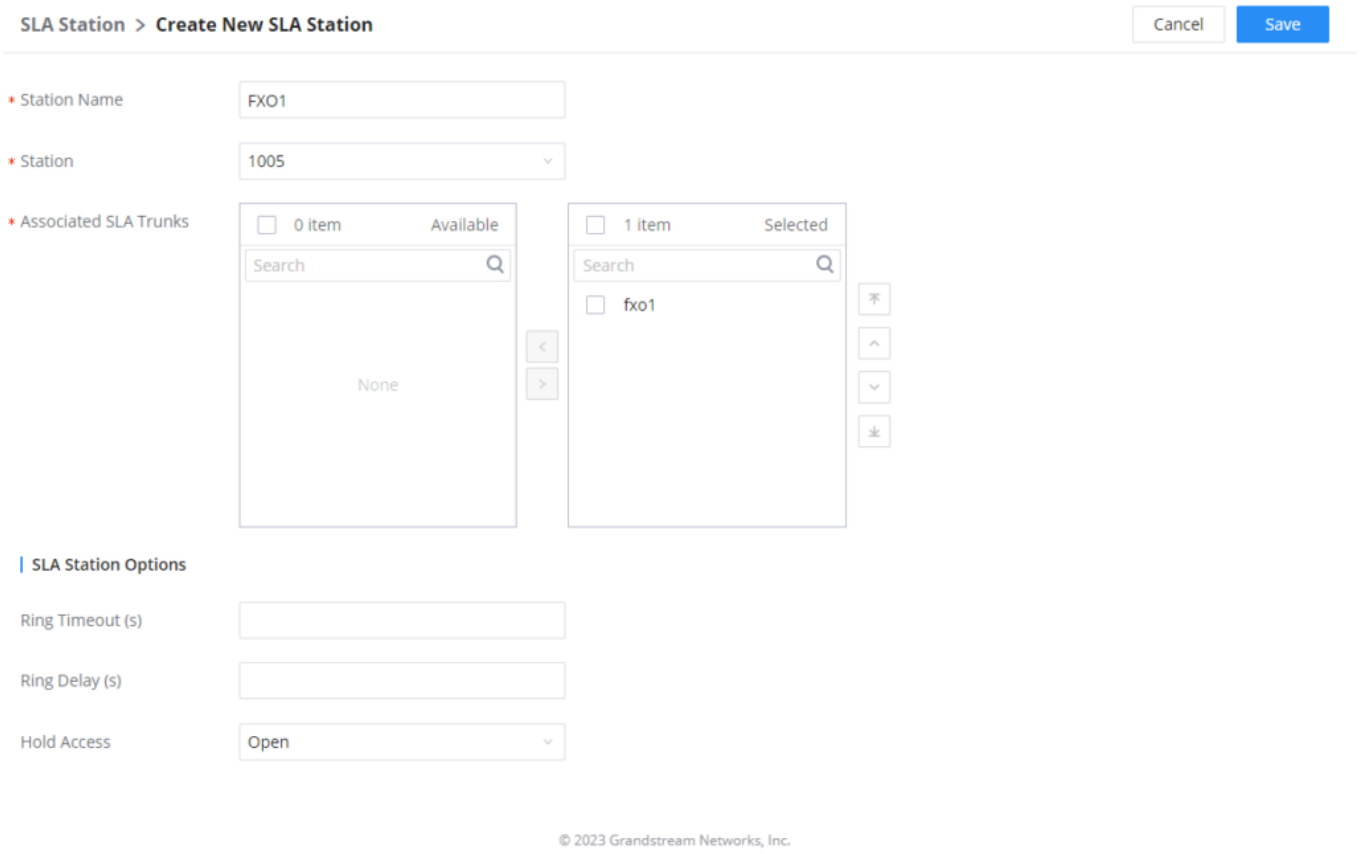
Enable SLA Mode for Analog Trunk

2. Click on "Save". The analog trunk will be listed with trunk mode "SLA".

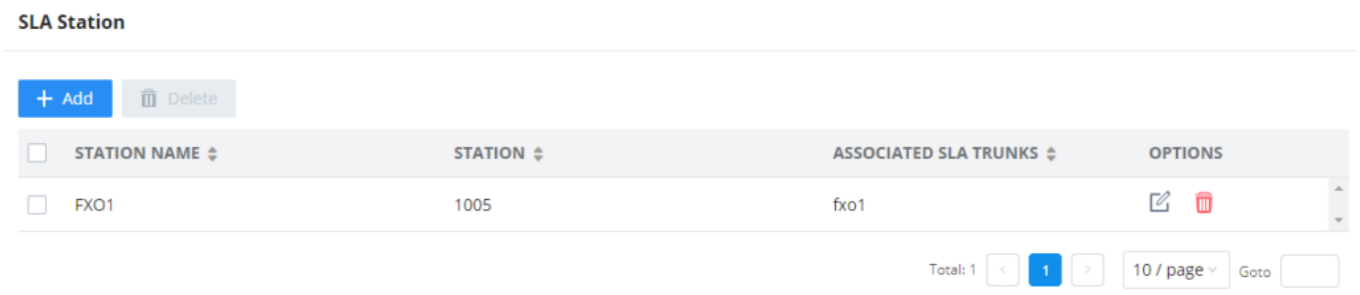


Analog Trunk with SLA Mode Enabled

3. On the UCM630X, go to Web GUI→**Extension/Trunk→SLA Station** page, click on "Add". Please refer to section **[Create/Edit SLA Station]** for the configuration parameters. Users can create one or more SLA stations to monitor the analog trunk. The following figure shows station 1005 associated with FXO1 trunk.

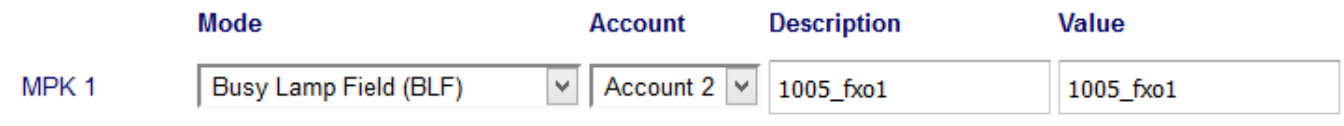


SLA Example - SLA Station



SLA Example -SLA Created

4. On the SIP phone 2, configure to register UCM630X extension 1005. Configure the MPK as BLF mode and the value must be set to "extension_trunkname", which is 1005_fxo1 in this case.



SLA Example - MPK Configuration

Now the SLA station is ready to use. The following functions can be achieved by this configuration.

- **Making an outbound call from the station/extension, using LINE key**

When the extension is in an idle state, press the line key for this extension on the phone to off-hook. Then dial the station's extension number, for example, dial 1002 on phone 1 (or dial 1005 on phone 2), to hear the

dial tone. Then the users could dial an external number for the outbound call.

- **Making an outbound call from the station/extension, using the BLF key**

When the extension is in an idle state (BLF is lit in green), press the MPK and users could dial external numbers directly.

- **Answering call using LINE key**

When the station is ringing (BLF is blinking in red), press the LINE key to answer the incoming call.

- **Barging-in active call using BLF key**

When there is an active call between an SLA station and an external number using the SLA trunk, other SLA stations monitoring the same trunk could join the call by pressing the BLF key if "Barge Allowed" is enabled for the analog trunk.

- **Hold/UnHold using BLF key**

If the external line is previously put on hold by an SLA station, another station that monitors the same SLA trunk could UnHold the call by pressing the BLF key if "Hold Access" is set to "open" on the analog trunk and the SLA station.

Outbound Routes

This section explains how to configure and manage outbound routes on the UCM630X. Outbound routes control all external outgoing calls initiated by the UCM, regardless of trunk type (SIP, Analog, or Digital).

Configuring Outbound Routes

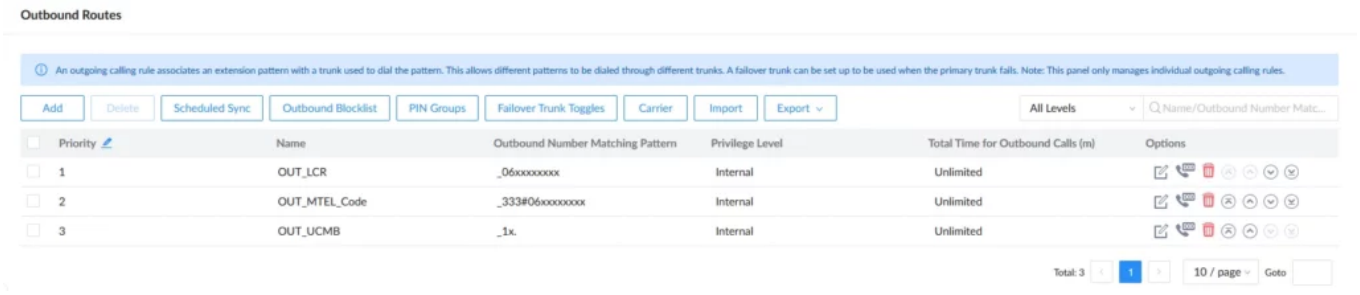
An outbound route in the UCM630X links a dial pattern to a trunk, allowing different call types to use different trunks. For example:

- **Local calls (7 digits)** -> FXO trunk
- **Long-distance calls (10 digits)** -> low-cost SIP trunk

Users can also configure a failover trunk to handle calls if the primary trunk is unavailable.

To manage outbound routes:

1. Go to **Web GUI->Extension/Trunk->Outbound Routes**.



Outbound Routes Overview Page

2. Click the **Add** button to create a new outbound route.
3. Click **Import** to upload routes in CSV or XLSX format.
4. Click **Export** to download routes in CSV or XLSX format.
5. Click the **Edit** icon to modify a route.
6. Click the **Delete** icon to remove a single route, or use the selection feature to delete multiple outbound

routes at once.

On the UCM630X, route selection is determined by the Outgoing Routing Priority feature, which can prioritize routes by either list order or pattern accuracy. For detailed configuration, see the Outgoing Routing Priority section in this guide.

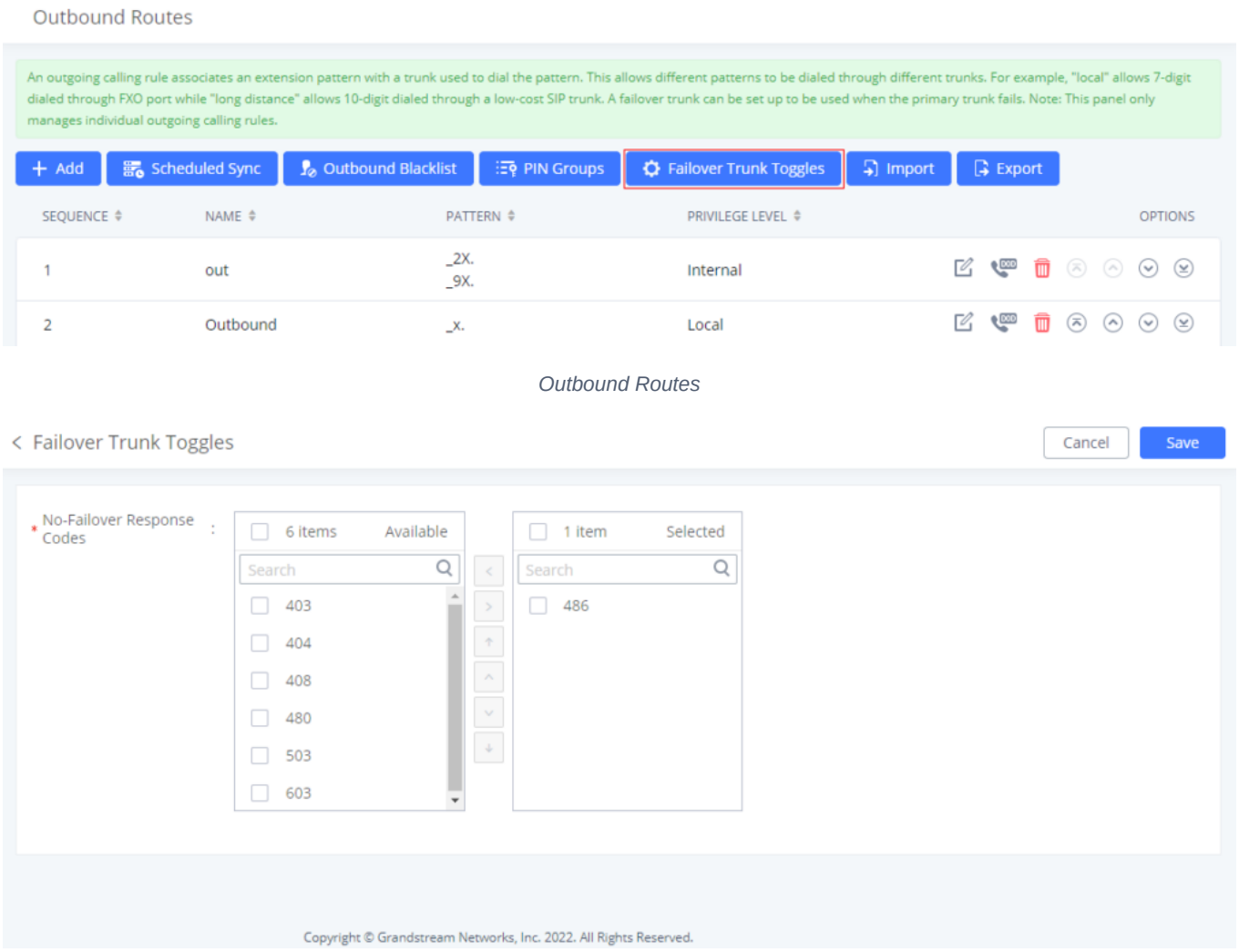
When creating an outbound route, users can configure the parameters described in the table below:

Option	Description
General	
Outbound Rule Name	Configure the name of the calling rule (e.g., local, long_distance, etc.). Letters, digits, _ and - are allowed.
Outbound Number Matching Pattern	All patterns are prefixed by the "_" character, but please do not enter more than one "_" at the beginning. All patterns can add comments, such as "_pattern /* comment */". In patterns, some characters have special meanings: [12345-9]: Any digit in the brackets (1,2,3,4,5,6,7,8,9 allowed). N: Any digit from 2-9. .: Wildcard, matching one or more characters. !: Wildcard, matching zero or more characters immediately. X: Any digit from 0-9. Z: Any digit from 1-9. -: Hyphen connects characters and is ignored. []: Containing special characters ([x], [n], [z]) represent letters x, n, z.
Auto Record	If enabled, calls using this route will automatically be recorded.
Local Country Code	If your local country code is affected by the outbound blacklist, enter it here to bypass the blacklist.
Outbound Route CID	Sets the Caller ID for this outbound route. Format must be "name<number>", "<number>", or "number". This CID is ignored if a DOD is configured. Note: This field does not apply to analog trunks.
Caller ID Manipulation	Enables Caller ID manipulation for this outbound rule. When enabled, the UCM applies the configured Strip/Prepend rules to calls using this route. The transformation is applied to both the SIP From header and the Remote-Party-ID (RPID) header. Example: A forwarded caller ID of 0123456789 with a strip of 1 and prepend of +972 results in +972123456789 in both From and RPID headers.
Caller ID Mode	Determines which Caller ID numbers the transformation applies to: Original CID: Transform only the forwarded caller's number. The UCM must have "Keep Original CID" enabled on the trunk for forwarded calls. All: Apply transformations to every outbound number on this route. Default: "Original CID".
Strip	Specifies the number of leading characters to remove from the Caller ID before sending the call out. Only numeric values (0-2) are allowed.
Prepend	Defines characters to add in front of the Caller ID after stripping. Supports 0-20 characters (Digits, Letters, + - * # only).
Diversion ID Manipulation	Enables transformation rules (strip and prepend) specifically applied to the SIP Diversion header number without altering the main Outbound Caller ID.
Strip	Specifies the number of leading characters to remove from the Diversion header number (0-2 characters, digits only).
Prepend	Defines characters to add in front of the Diversion header number after stripping (0-20 characters, allows digits, letters, and + - * #).
Don't Call Me Blocklist	If enabled, outgoing calls will first be checked against the "Don't Call Me" database. If the called number is in the database, the call will be blocked.
Disable This Route	Disables the outbound route. When disabled, the route will not take effect, but its settings remain stored in the UCM.
Outbound Permission	
Password Settings	Configures the authentication method for this outbound route: Password: The configured password will be used. PIN Groups: The PIN number related to the configured PIN Group will be used. Default: "Password".

Password	Configure the password for users to use this rule when making outbound calls.
PIN Groups	Select a PIN Group.
PIN Groups with Privilege Level	If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied.
Privilege Level	Select the privilege level for the outbound rule: Internal: The lowest level required. All users can use this rule. Local: Users with Local, National, or International levels can use this rule. National: Users with National or International levels can use this rule. International: The highest level required. Only users with the international level can use this rule. Disable: Default setting. Only the matched source caller ID will be allowed to use this outbound route. Note: Please be aware of potential security risks when using the "Internal" level.
Enable Source Caller ID Allowlist	When enabled, users can specify extensions allowed to use this outbound route. "Privilege Level" is automatically disabled if enabled. Select available extensions/extension groups from the list. Custom Dynamic Route: Define the pattern for the source caller ID (prefixed with "_", using pattern characters X, Z, N, ., !).
Call Duration Limit	Enable to configure the maximum duration for calls using this outbound route.
Per-Call Duration Limit	Enable to configure the maximum duration of each individual call using this outbound route. Once reached, the call is terminated.
Maximum Call Duration (s)	Configure the maximum duration of the call (in seconds). Default is 0 (no limit).
Warning Time (s)	Configure the warning time before call termination. A warning tone is played when x seconds remain.
Warning Repeat Interval (s)	Configure the repeat interval for the warning tone after the first warning.
Total Call Duration Limit	Enables setting a maximum cumulative call duration for this outbound route within a specified period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three months. Default: "Monthly".
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Main Trunk	
Trunk	Select the main trunk for this outbound rule.
Strip	Specify the number of digits to strip from the beginning of the dialed string before placing the call.
Prepend	Specify digits to prepend to the dialed number after stripping.
Failover Trunk	
Failover Trunk	Configures alternate trunks (up to 10) to route calls when the primary trunk is busy or down.
Strip	Specify the number of digits to strip from the dialed string for the failover trunk.
Prepend	Specify digits to prepend before placing the call via the failover trunk.
Time Condition	
Time Condition Mode	Selects the trunk routing behavior during time conditions: Use Main Trunk or Failover Trunk: Use the main trunk during configured time conditions; fall back to failover trunk if unavailable. Use Specific Trunks: Use specific trunks during configured time conditions using main trunk strip/prepend rules.

Failover Trunk Toggles

This option controls whether failover trunks will be used if receiving specific responses to outgoing calls.



Outbound Routes

Failover Trunk Toggles

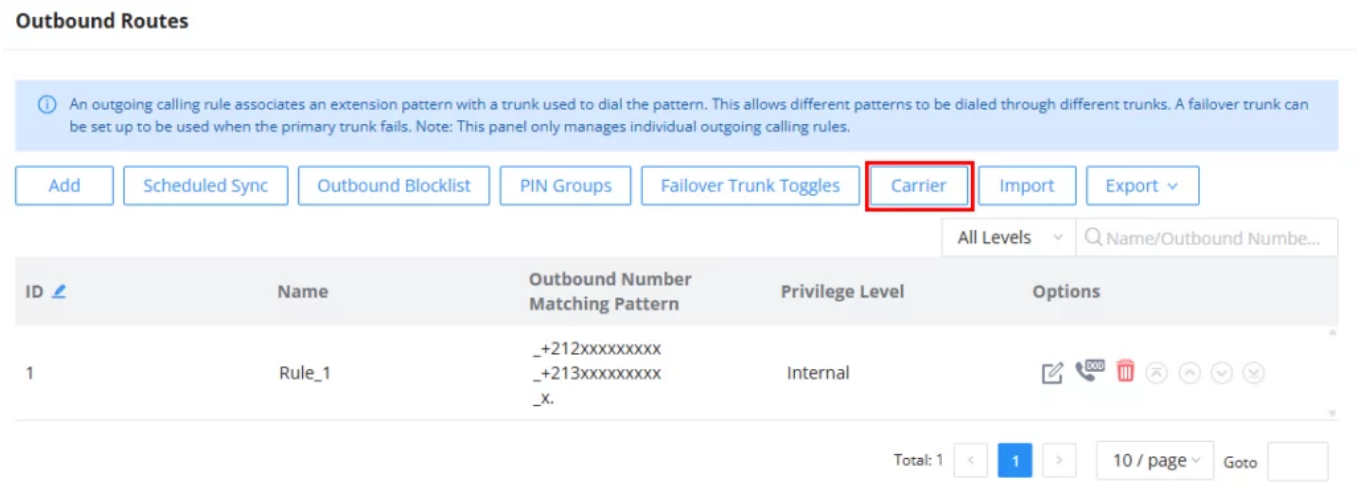
If a call receives the selected response codes, the UCM will not be redirect it to the call route's failover trunk.

Due to the addition of this option, the **Enable 486 to Failover Trunks** option under PBX Settings→General Settings page has been removed.

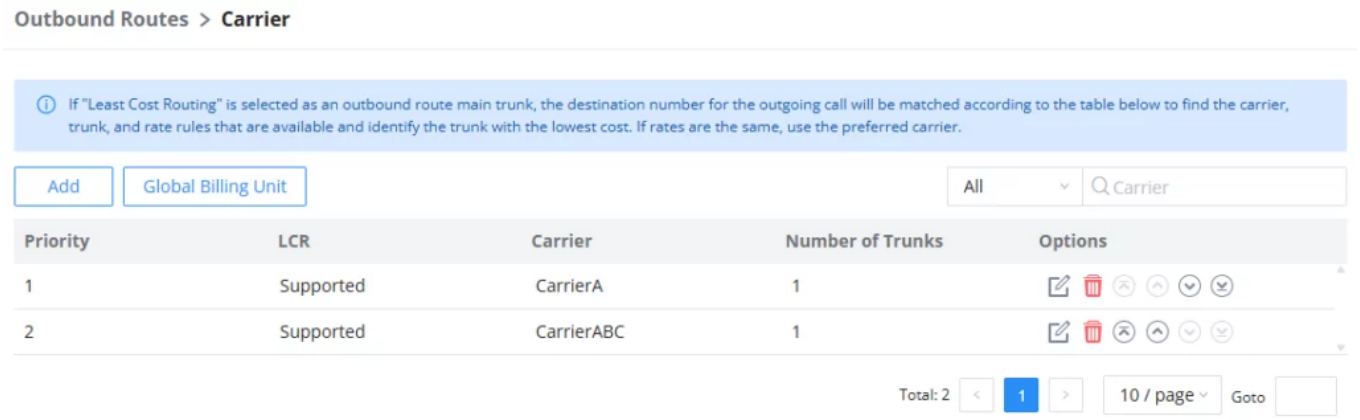
Carrier

In Carrier page, the user can configure LCR, Least Cost Routing, which is a mechanism where the user can set the priority for the trunks to use when emitting a call. Typically for Least Cost Routing, the user can set higher priority for the trunks which have a lower call rate. This is an effective approach to use the trunks which have a lower cost, and in the case when they cannot be used, like when they are down or many concurrent calls, the next trunk in the list will be used.

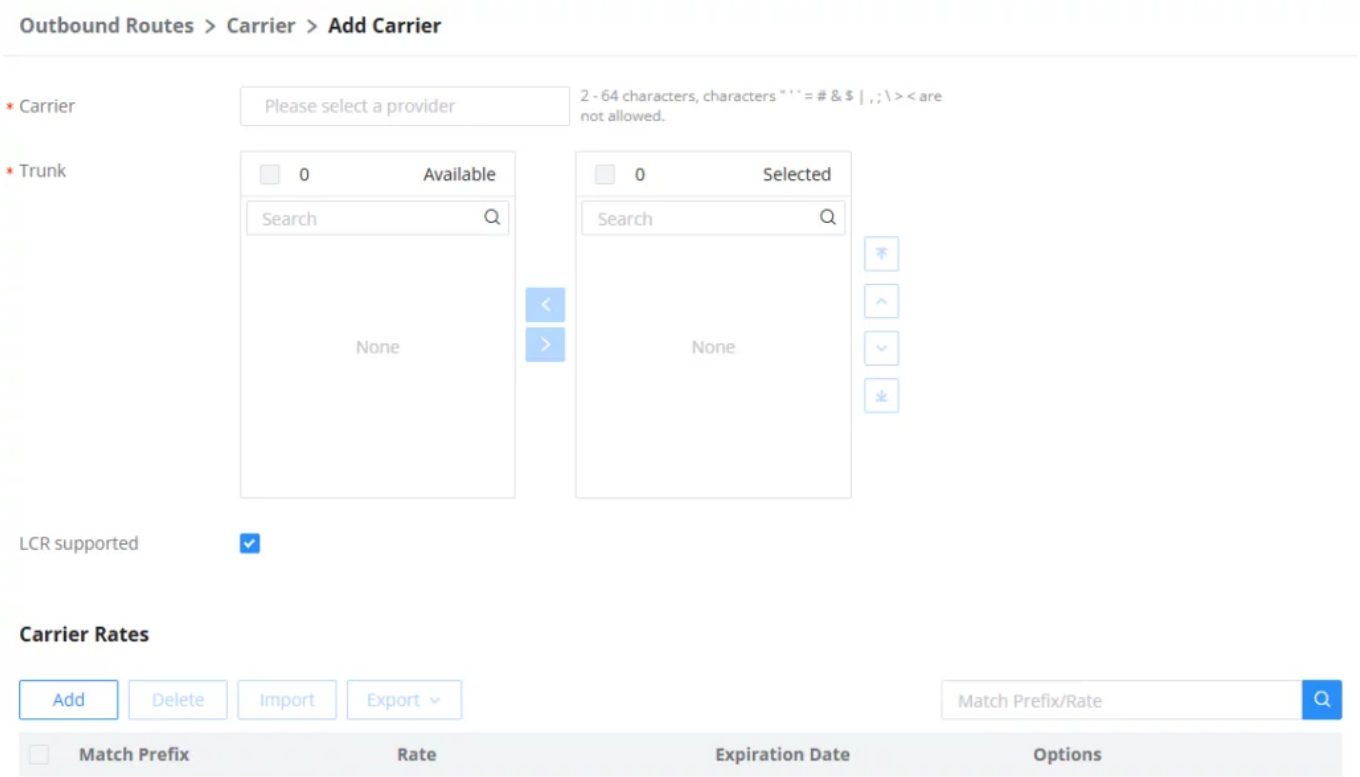
To configure this option, navigate to **Extension/Trunk > Outbound Routes** and click on Carrier.



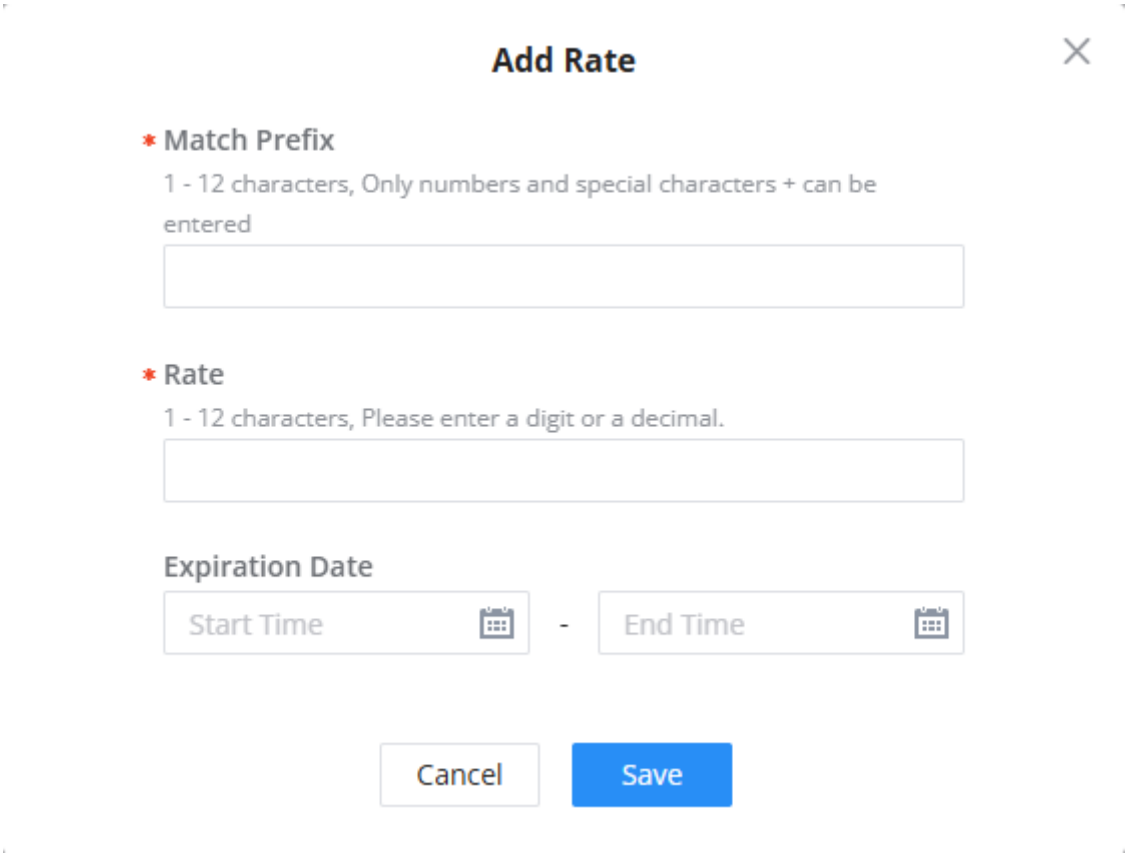
On the list of carriers, please click on "Add".



Select the trunks to apply the rates on, the add the rate in **Carrier Rates** section.



Click on "Add" button under **Carrier Rates** section.



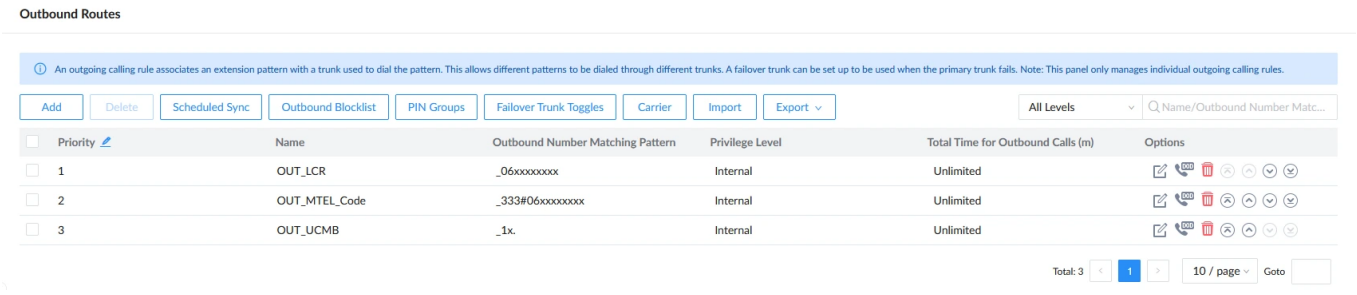
Add Call Rate

Parameter Name	Description
Match Prefix	If the prefix entered is matched, this rate will apply to this call.
Rate	Enter the rate of the call.
Expiration Date	Select the expiraton date and time

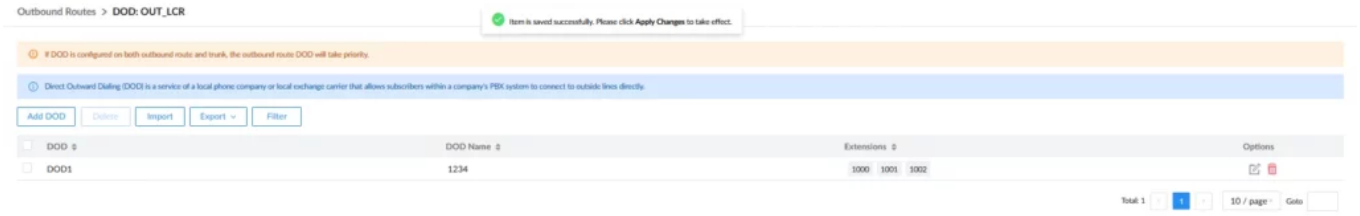
To learn more about configuring the LCR feature and how it operates on the UCM6300 series, please refer to the Grandstream Billing System Guide.

Outbound Routes DOD

It is possible to specify DOD number based on Outbound Route, as displayed on the screenshot below. For each outbound route.



Outbound Routes Page



DOD for First Outbound Route

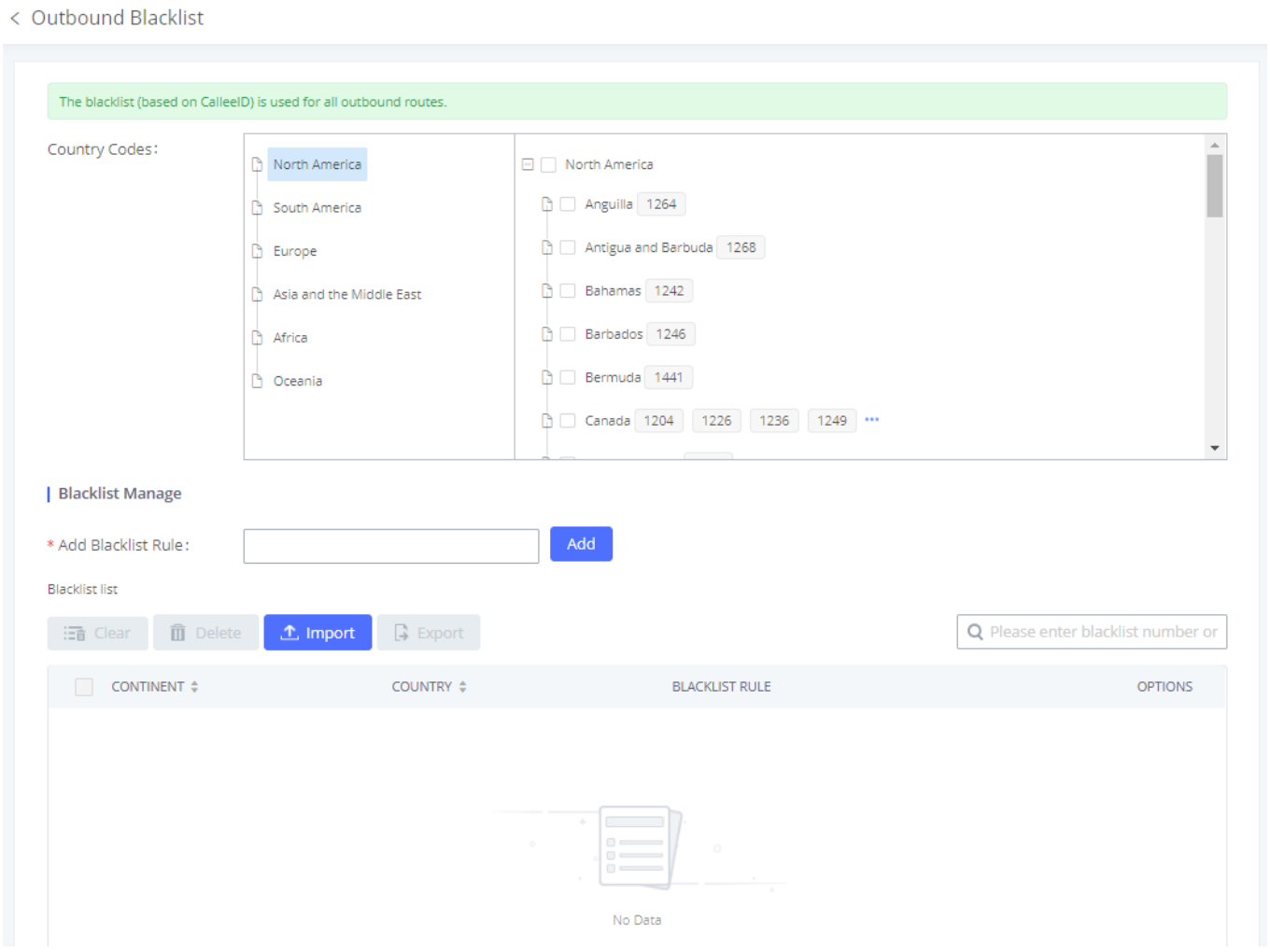


DOD for Second Outbound Route

Outbound Blacklist

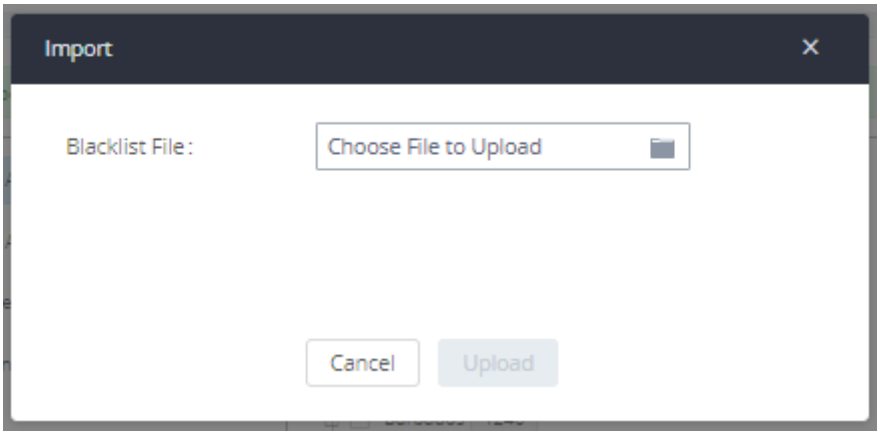
The UCM630X allows users to configure a blacklist for outbound routes. If the dialing number matches the blacklist numbers or patterns, the outbound call will not be allowed. The outbound blacklist can be configured under UCM Web GUI→**Extension/Trunk→Outbound Routes**: Outbound Blacklist.

Users can configure numbers, patterns or select country code to add to the blacklist. Please note that the blacklist settings apply to all outbound routes.



Country Codes

Users can export outbound route blacklists and delete all blacklist entries. Additionally, users can also import blacklists for outbound routes.

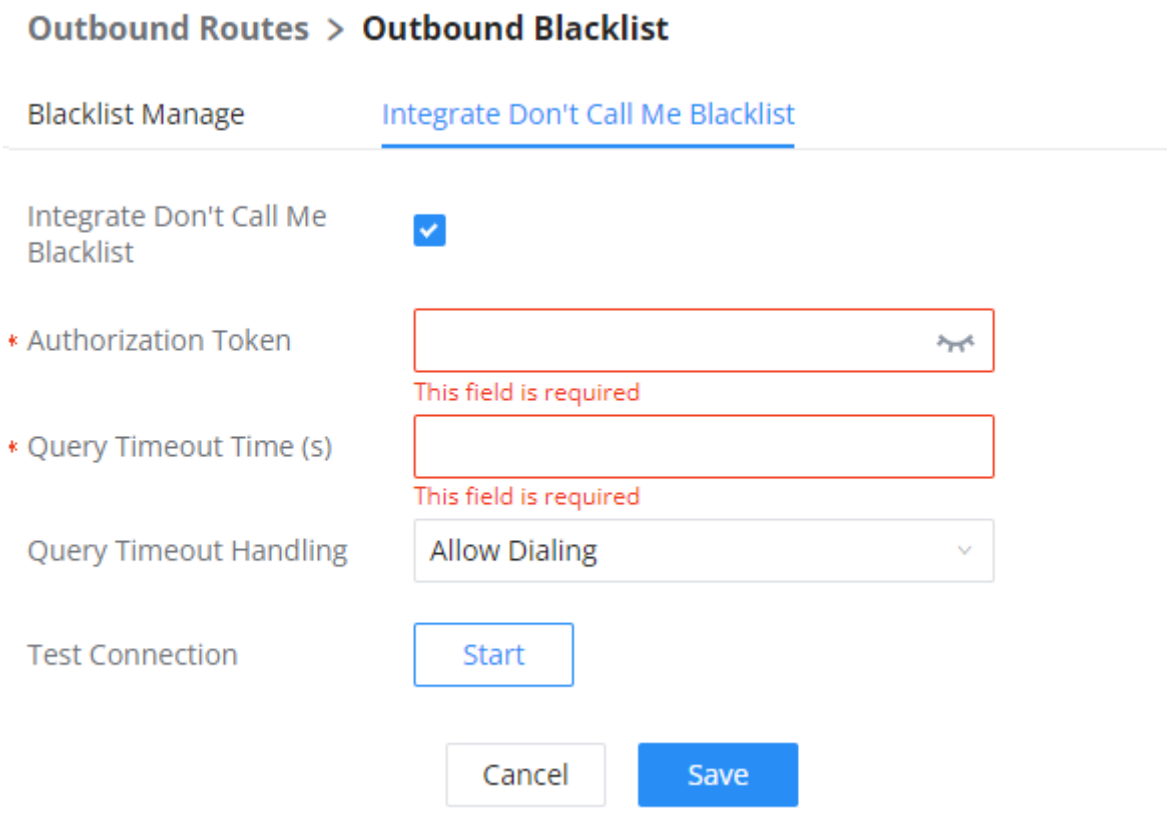


Blacklist Import/Export

Don't Call Me Blacklist Integration

UCM now supports integration with Vercel's Don't Call Me, a large public database containing numbers that have been registered and opted to not receive unsolicited telemarketing calls. This allows UCM to query dialed numbers via API and deny outgoing calls if they are found in database to comply with some countries' laws.

To access the integration page, please navigate to **Extension/Trunk > Outbound Routes,** then click on "Outbound Blacklist" button and click on **Integrate Don't Call Me Blacklist**.



Don't Call Me Database Integration

Parameter	Description
Integrate Don't Call Me Blacklist	Enable or disable Don't Call Me integration

Authorization Token	Enter the authorization token generated by the Don't Call Me database.
Query Timeout (s)	Enter the duration after which the query is considered timed out.
Query Timeout Handling	Select the action to perform after the query timeout. Allow Dialing: If the query times out, the call will be allowed. Prohibit Dialing: If the query times out, the call will be prohibited.
Test Connection	Click on this button to test that the integration is working as intended. Note: If the database or Internet access is momentarily down, this test will fail.

Scheduled Sync

The UCM630X allows users to synchronize the outbound routes, this feature can be found on the Web GUI→ **Extension/Trunk→Outbound Routes→ Scheduled Sync.**

Scheduled Sync	Enable the Scheduled Sync feature
Server Address	Enter the TFTP server address. For example, "192.168.1.2:69".
File Name	Specify the file name
Sync Time	Enter the sync time (24hr format). The valid range is 0-23.
Sync Frequency	Create new sync every x day(s). The valid range is 1 to 30.

Outbound Routes/Scheduled Sync

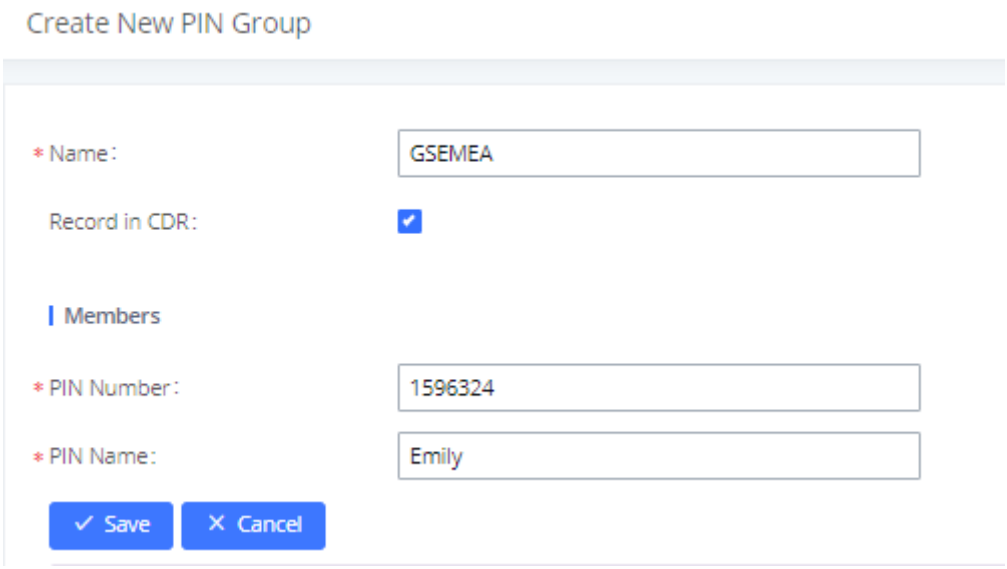
PIN Groups

The UCM630X supports the pin group. Once this feature is configured, users can apply pin groups to specific outbound routes. When placing a call on pin-protected outbound routes, the caller will be asked to input the group pin number, this feature can be found on the Web GUI→**Extension/Trunk→Outbound Routes→PIN Groups.**

Name	Specify the name of the group
Record In CDR	Specify whether to enable/disable record in CDR
PIN Number	Specify the code that will be asked once dialing via a trunk
PIN Name	Specify the name of the PIN

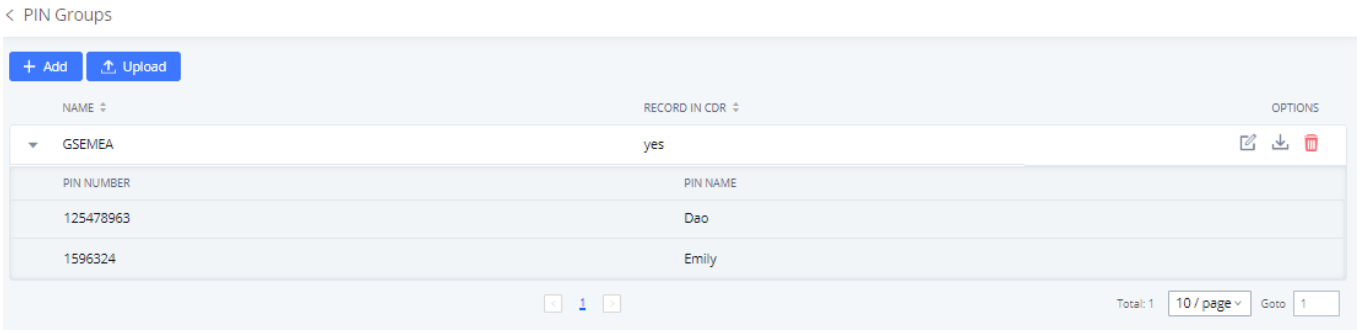
Outbound Routes/PIN Group

Once the user clicks , the following figure shows to configure the new PIN.



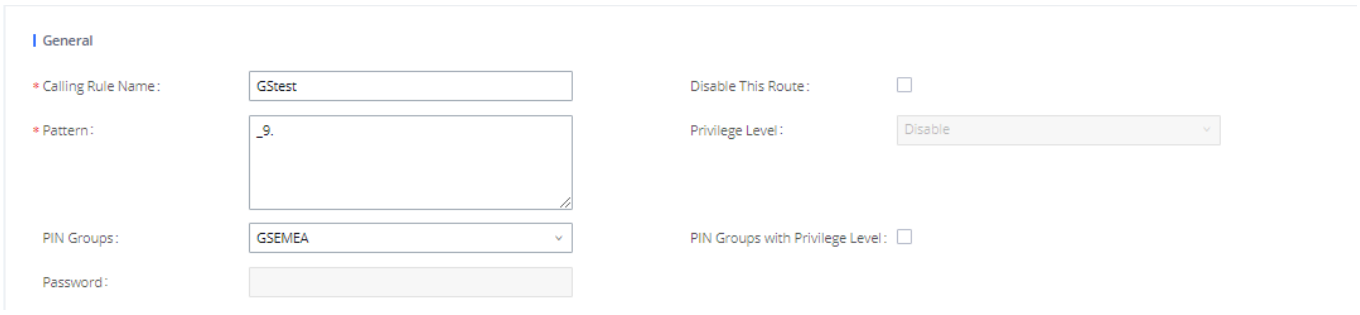
Create New PIN Group

The following screenshot shows an example of created PIN Groups and members:



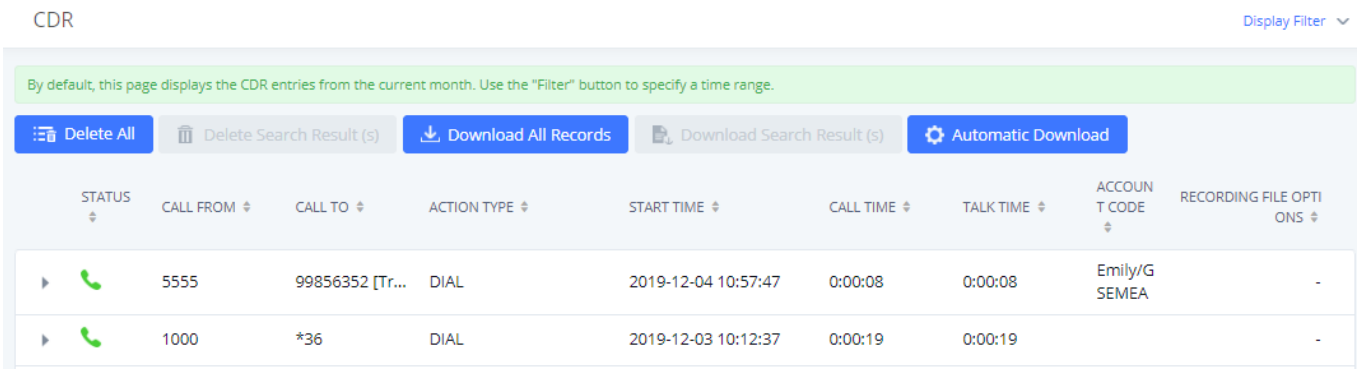
PIN Members

If PIN group is enabled on outbound route level, password, privilege level and enable the filter on source caller ID will be disabled, unless if you check the option "PIN Groups with Privilege Level" where you can use the PIN Groups and Privilege Level or PIN Groups and Enable Filter on Source Caller ID.



Outbound PIN

If PIN group CDR is enabled, the call with PIN group information will be displayed as part of CDR under the Account Code field.

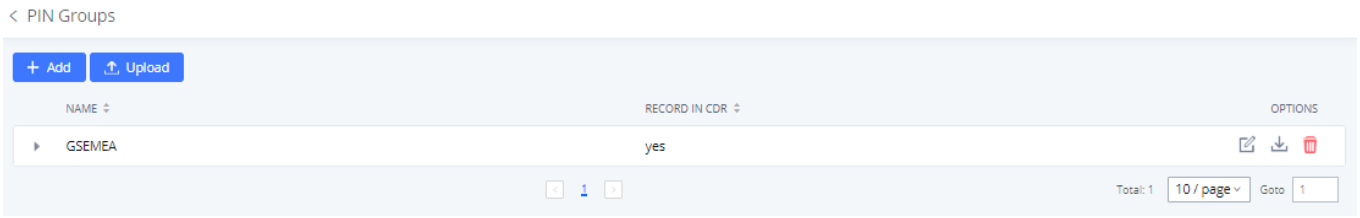


CDR Record

- **Importing PIN Groups:**

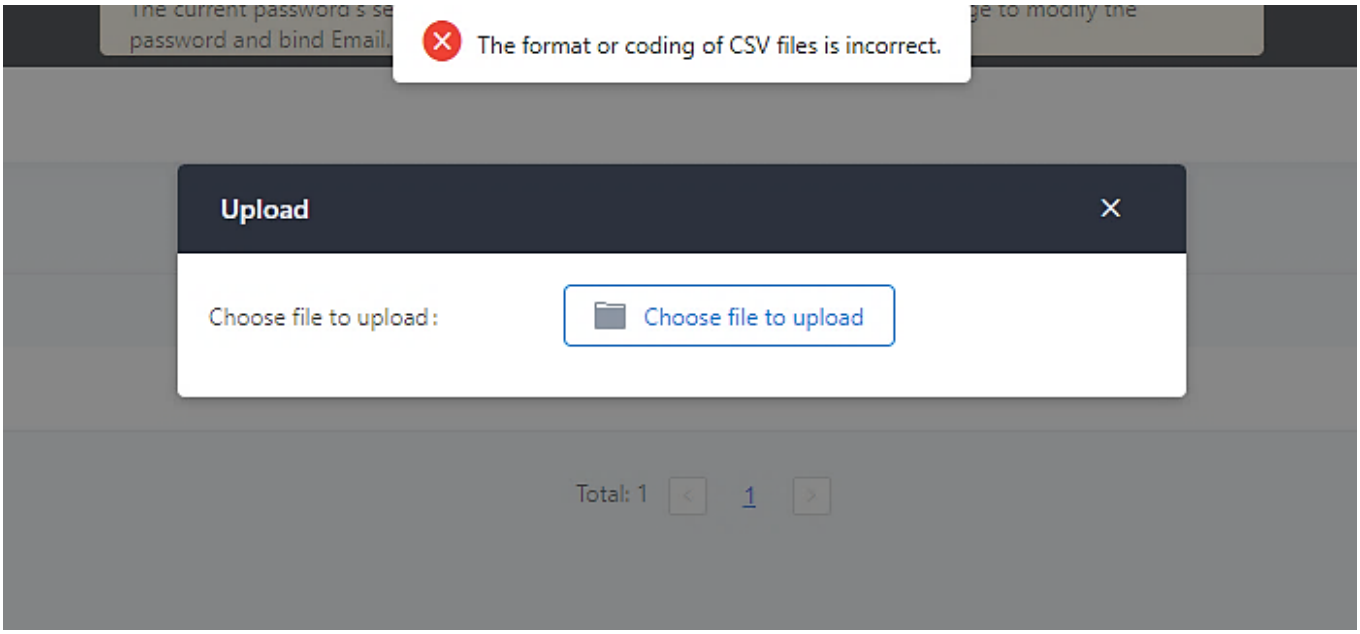
Users can also import PIN Groups by uploading csv or xlsx files for each group. To do this:

1. Navigate to **Extension/Trunk→Outbound Routes→PIN Groups** and click on the "Upload" button.



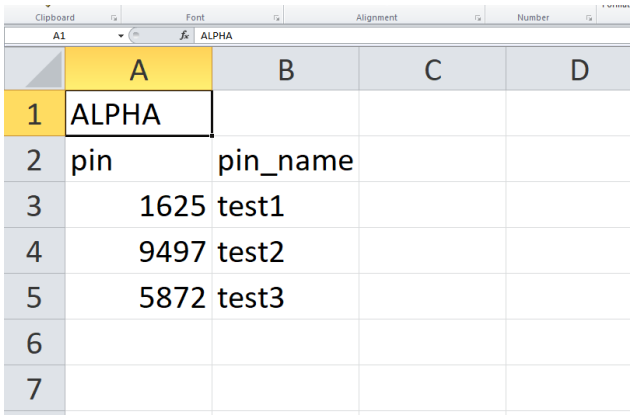
Importing PIN Groups

2. Select the CSV file to upload. Incorrect file formats and improperly formatted files will result in error messages such as the one below:



Incorrect CSV File

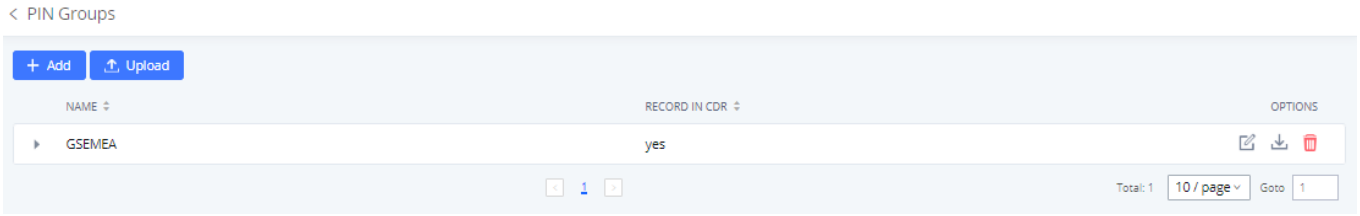
3. To ensure a successful import, please follow the format in the sample image below



	A	B	C	D
1	ALPHA			
2	pin	pin_name		
3	1625	test1		
4	9497	test2		
5	5872	test3		
6				
7				

CSV File Format

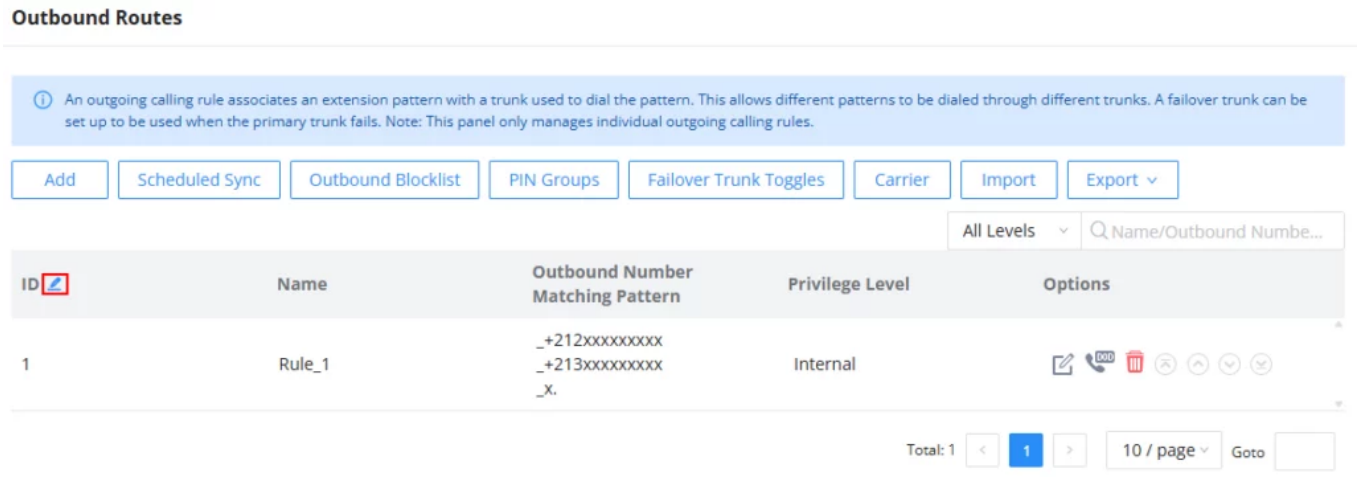
- The top-left value (A1) is the PIN Group name. In this case, it is "ALPHA".
- Row 2 contains the labels for the modifiable fields: pin and pin_name. These values should not be changed and will cause an upload error otherwise.
- Rows 3+ contain the user-defined values with Column A holding the PINs and Column B holding the PIN names. PIN values must consist of at least four digits.
- Once the file is successfully uploaded, the entry will be added to the list of PIN Groups.

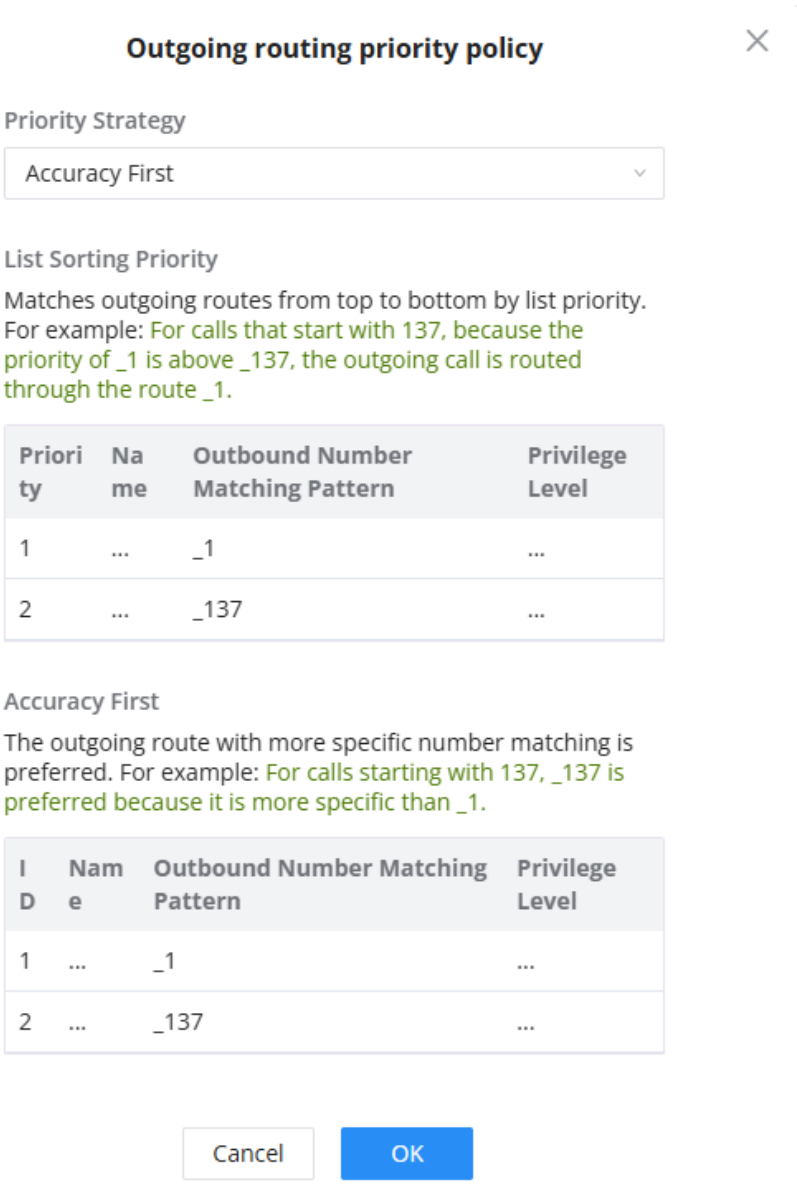


Outgoing Routing Priority

Outgoing Routing Priority Policy feature allows defining the priority approach for the outbound routes. Using this feature, the administrator can select either the accuracy of the dial pattern, or the position of the outbound route in the list to determine the route of the call.

To configure this feature, please click on the following button on the Outbound Routes page.





Selecting one of the policies will result in the following behaviour.

- **List Sorting Priority**: Selecting this option will result in taking the sorting order of the list of outbound routes as a matching criteria for the dial pattern. The route with the first matching dial plan will be used to route the call. Any routes further down the list with a more resembling dial pattern will not be taken into consideration.
- **Accuracy First**: Selecting this option will result in choosing the route with the most resembling dial pattern. In contrast with List Sorting Priority, the position of the route in the list is irrelevant and will not be taken into consideration.

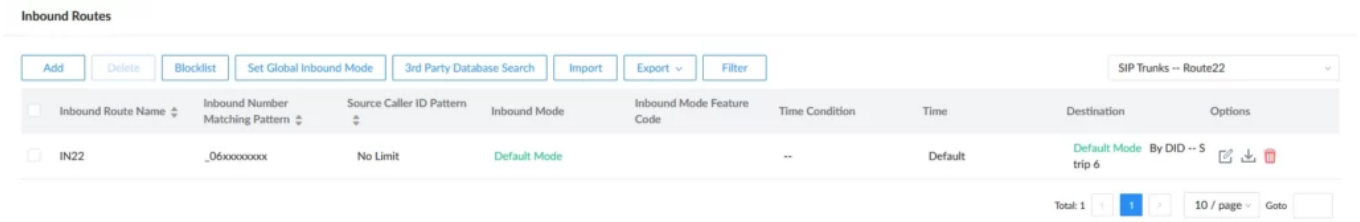
Inbound Routes

Inbound routes allow the UCM630X to control and forward incoming external calls to specific destinations based on defined criteria. These criteria can include source caller ID, destination number, and other route-level settings. A default destination can also be set to handle calls that do not match any specific criteria.

Configuring Inbound Routes

To manage inbound routes:

1. Go to **Web GUI->Extension/Trunk->Inbound Routes**.



Inbound Routes Overview Page

2. Click the **Add** button to create a new inbound route.
3. Click **Blocklist** to configure numbers or patterns that should be blocked on all inbound routes.
4. Click **Import** to upload routes in CSV or XLSX format.
5. Click **Export** to download routes in CSV or XLSX format.
6. Click the **Edit** icon to modify an existing inbound route.
7. Click the **Filter** button to search in the list inbound routes using specific filters.
8. Click the **Delete** icon to remove a single route, or use the selection feature to delete multiple routes at once.

When creating an inbound route, users can configure the parameters described in the table below:

Trunks	Select the trunk to configure the inbound rule.
Inbound Route Name	Configure the name of the Inbound Route. For example, "Local", "LongDistance" etc.
Inbound Number Matching Pattern	All patterns are prefixed with the "_". Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9.Notes: Multiple patterns can be used. Each pattern should be entered in a new line. Example: _X. _ NNXXNXXXXX /* 10-digit long distance */
Disable This Route	After creating the inbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in the PBX. Users can enable it again when it is needed.
CID Source	Configures the source of the CID to match with the configured CallerID Pattern. None: CID is not obtained from any source. Only applicable if no CallerID Pattern is configured. DiversionID: CID is obtained from the Diversion header. Only applicable to SIP trunks. CallerID: If the call is from a SIP trunk, the CID is obtained from the From header. Otherwise, the CID will be obtained from other related signaling.
Seamless Transfer Whitelist	Allows the selected extension to use this function. If an extension is busy, and a mobile phone is bound to that extension, the mobile phone can pick up calls to that extension.
Call Settings	
Ringback tone	Choose the custom ringback tone to play when the caller reaches the route.
Auto Record	If enabled, calls using this route will automatically be recorded.
Block Collect Call	If enabled, collect calls will be blocked.Note: Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call".
Alert-Info	Configure the Alert-Info, when the PBX receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.
Fax Detection	If enabled, fax signals from the trunk during a call will be detected.

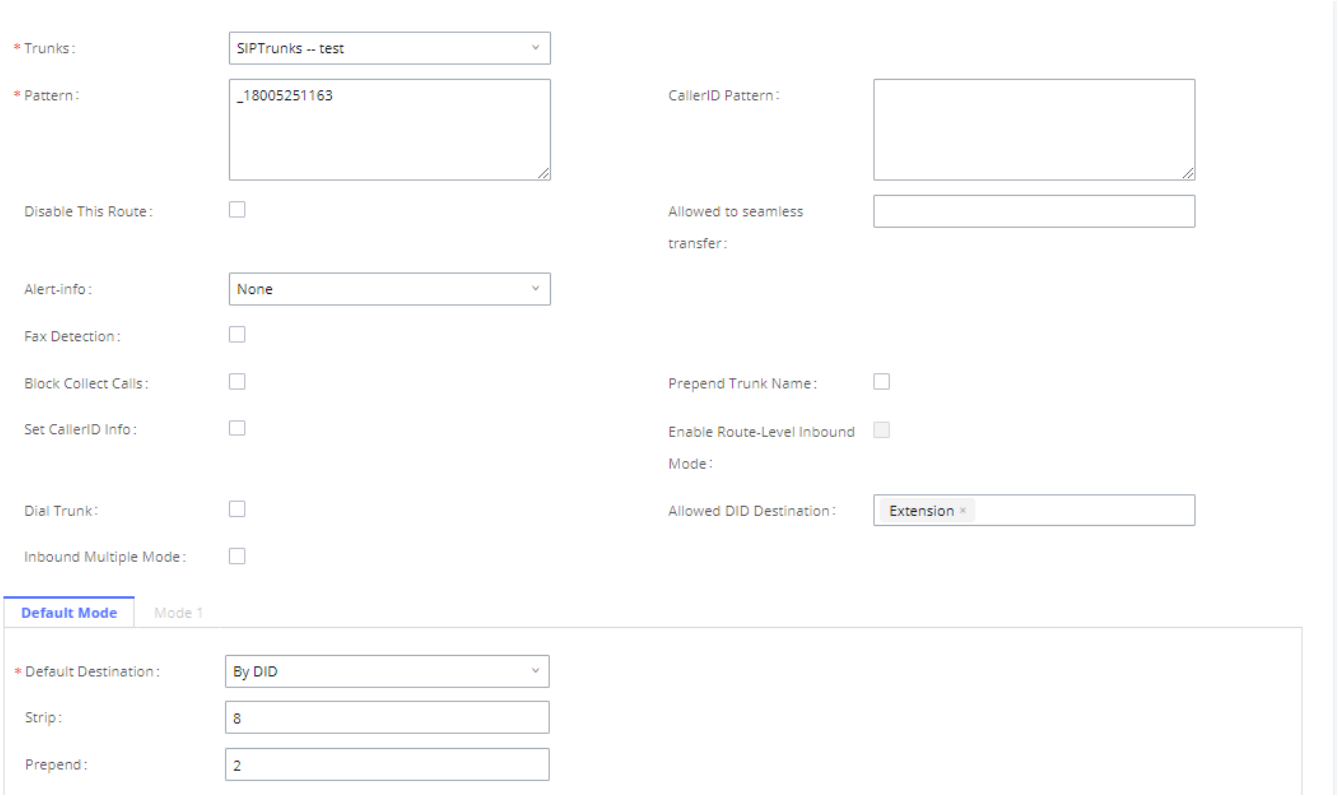
Fax Destination	Configures the destination of faxes. Extension: send the fax to the designated FXS/SIP extension (fax machine) or a FAX extension. Fax to Email: send the fax as an email attachment to the designated extension's email address. If the selected extension does not have an associated email address, it will be sent to the default email address configured in the Call Features->Fax/T.38->Fax Settings page. Note: please make sure the sending email address is correctly configured in System Settings->Email Settings.
Auto Answer	If enabled, the PBX will automatically answer calls and receive faxes through the inbound route. If disabled, the PBX will not receive a fax until after the call has been answered. Enabling this option will slow down the answering of non-fax calls on the inbound route. The alert tone heard during the detection period can be customized.
Block Collect Calls	If enabled, collect calls will be blocked. Note: Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call". Note: This is affected by Block Set Calls on the SIP Settings -> General Settings page.
Prepend Trunk Name	If enabled, the trunk name will be added to the caller id name as the displayed caller id name.
Set Caller ID Info	Manipulates Caller ID (CID) name and/or number within the call flow to help identify who is calling. When enabled two fields will show allowing to manipulate the CalleID Number and the Caller ID Name.
CallerID Number	Configure the pattern-matching format to manipulate the numbers of incoming callers or to set a fixed CallerID number for calls that go through this inbound route. ${CALLERID(num)}: Default value which indicates the number of an incoming caller (CID). The CID will not be modified. ${CALLERID(num):n}: Skips the first n characters of a CID number, where n is a number. ${CALLERID(num):-n}: Takes the last n characters of a CID number, where n is a number. ${CALLERID(num):s:n}: Takes n characters of a CID number starting from s+1, where n is a number and s is a character position (e.g. ${CALLERID(num):2:7} takes 7 characters after the second character of a CID number). n${CALLERID(num)}: Prepends n to a CID number, where n is a number.
CallerID Name	The default string is ${CALLERID(name)},which means the name of an incoming caller, it is a pattern-matching syntax format. A${CALLERID(name)}B means Prepend a character 'A' and suffix a character 'B' to ${CALLERID(name)}.Not using pattern-matching syntax means setting a fixed name to the incoming caller.
Enable Route-Level Inbound Mode	Gives uses the ability to configure inbound mode per individual route. When enabled two fields will show allowing to set the Inbound mode and the Inbound mode Suffix.Note: Global inbound mode must be enabled before users can configure route-level inbound mode.
Inbound Mode	Choose the inbound mode for this route.Note: Toggling the global inbound mode will not affect routes that have Route-level Inbound Mode enabled. If all routes have the option enabled, toggling the global inbound mode via BLF will trigger a voice prompt indicating that none of the routes will be affected by the global inbound mode change.
Inbound Mode Suffix	Dial "Global Inbound Mode feature code + Inbound Mode Suffix" or a route's assigned suffix to toggle the route's inbound mode.The BLF subscribed to the inbound mode suffix can monitor the current inbound mode.
Inbound Multiple Mode	Multiple mode allows users to switch between destinations of the inbound rule by feature codes. Configure related feature codes as described in [Inbound Route: Multiple Mode]. If this option is enabled, the user can use feature code to switch between different modes/destinations.
CallerID Name Lookup	If enabled, the callerID will be resolved to a name through local LDAP. Note, if a matched name is found, the original callerID name will be replaced. The name lookup is performed before other callerID or callerID name modifiers (e.g., Inbound Route's Set CallerID Info or Prepend Trunk Name). Note: Name lookup may impact system performance.

Dial Trunk	This option shows up only when "By DID" is selected. If enabled, the external users dialing into the trunk via this inbound route can dial outbound calls using the PBX's trunk.
Privilege Level	This option shows up only when "By DID" is selected. Disable: Only the selected Extensions or Extension Groups are allowed to use this rule when enabled Filter on Source Caller ID. Internal: The lowest level required. All users are allowed to use this rule, checking this level might be risky for security purposes. Local: Users with Local level, National or International level are allowed to use this rule. National: Users with National or International Level are allowed to use this rule. International: The highest level required. Only users with an international level are allowed to use this rule.
Allowed DID Destination	This option shows up only when "By DID" is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination is: Extension Conference Call Queue Ring Group Paging/Intercom Groups IVR Voicemail Groups Dial By Name All
	Extension Voicemail Conference Room Call Queue Ring Group Paging/Intercom Voicemail Group DISA IVR External Number By DID When "By DID" is used, the PBX will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through. Dial By Name Callback
	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
	Select the start time "hour:minute" for the trunk to use the inbound rule.
End Time	Select the end time "hour:minute" for the trunk to use the inbound rule.
Date	Select "By Week" or "By Day" and specify the date for the trunk to use the inbound rule.
Week	Select the day in the week to use the inbound rule.
Destination	Select the destination for the inbound call under the defined time condition. Extension Voicemail Conference Room Call Queue Ring Group Paging/Intercom Voicemail Group DISA IVR By DID When "By DID" is used, the PBX will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through.Configure the number of digits to be stripped in the "Strip" option. Dial By Name External Number Callback

Inbound Route: Prepend

UCM630X allows users to prepend digits to an inbound DID pattern, with strip taking precedence over prepend. With the ability to prepend digits in the inbound route DID pattern, the user no longer needs to create multiple routes for the same trunk to route calls to different extensions. The following example demonstrates the process:

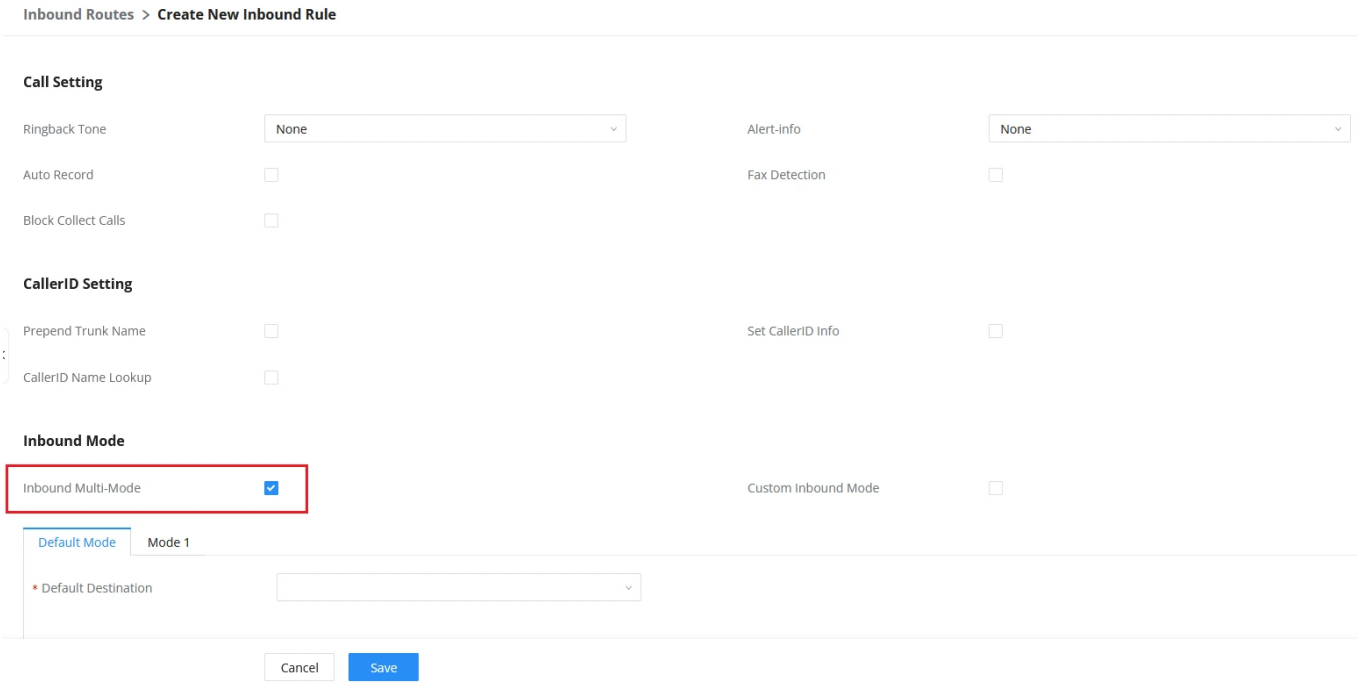
1. If Trunk provides a DID pattern of 18005251163.
2. If **Strip** is set to 8, UCM630X will strip the first 8 digits.
3. If **Prepend** is set to 2, UCM630X will then prepend a 2 to the stripped number, now the number becomes 2163.
4. UCM630X will now forward the incoming call to extension 2163.



Inbound Route feature: Prepend

Inbound Route: Multiple Mode

The UCM630X allows configuring an inbound route to enable multiple mode to switch between different destinations. The inbound multiple mode can be enabled under Inbound Route settings.



Inbound Route - Inbound Multi-Mode

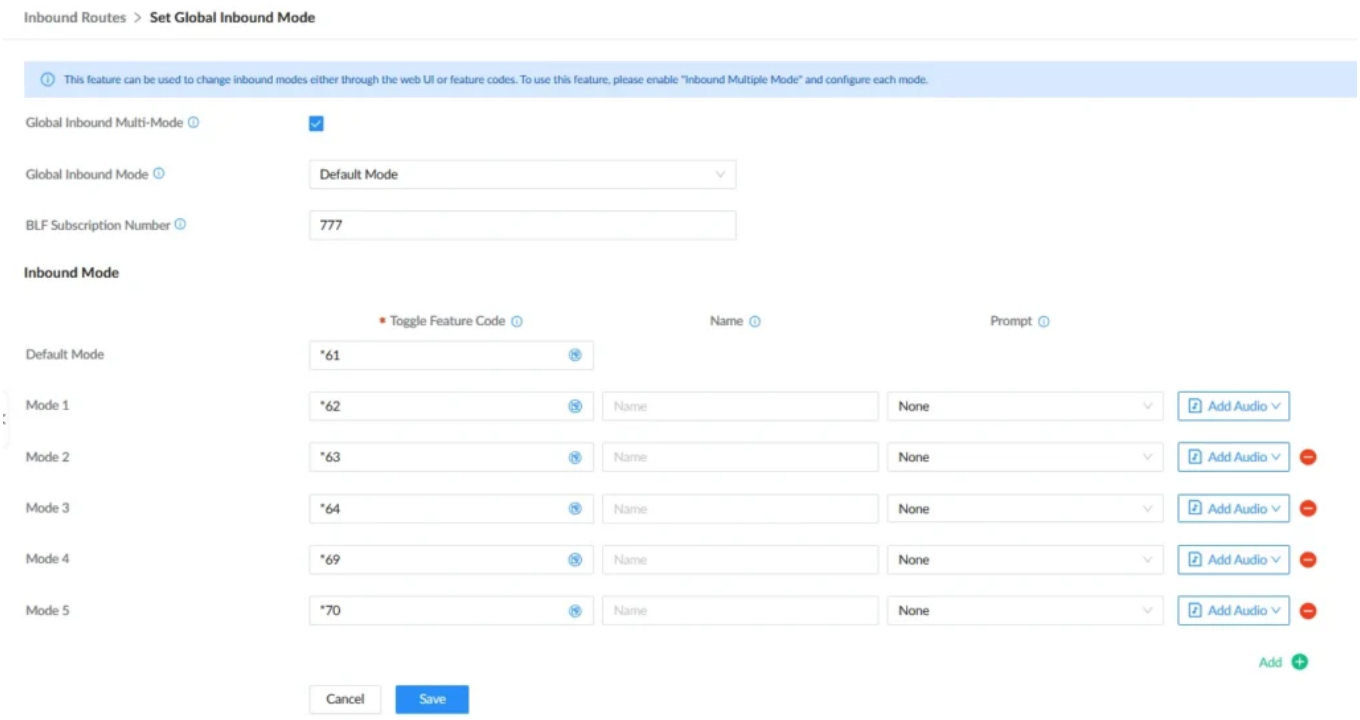
When Multiple Mode is enabled for the inbound route, the user can configure a "Default Destination" and up to 9 destination modes for all routes (Mode 1, Mode 2, etc). By default, calls coming into the inbound routes will be routed to the default destination.

SIP end devices registered on the UCM630X can dial feature codes (e.g., *62) to switch to "Mode 1" and dial

feature code *61 to switch back to "Default Destination". These feature codes can be customized under **Extension/Trunk -> Inbound Routes -> Set Global Inbound Mode** (ensure they do not conflict with other configured feature codes). Switching modes can be easily performed via phone keypads without logging into the Web GUI.

If a customer service hotline destination needs to switch to a specific night-service IVR after 7 PM, the administrator or authorized user can dial *62 to switch to "Mode 1" before leaving for the day.

To configure Global Inbound Multi-Modes, navigate to **Extension/Trunk -> Inbound Routes**, click on **Set Global Inbound Mode**, and check the **Global Inbound Multi-Mode** option.

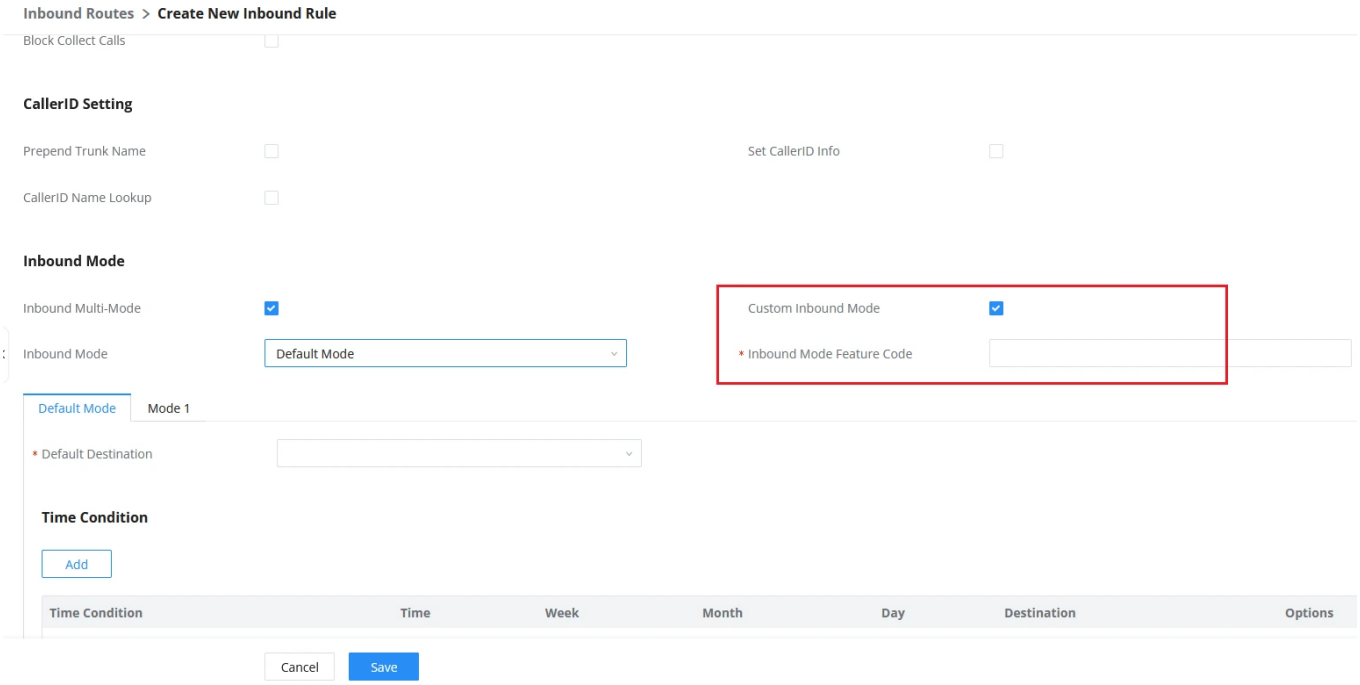


The following options are available under the Inbound Mode configuration list:

Option	Description
Global Inbound Multi-Mode	Enables or disables system-wide multi-mode inbound destination switching.
Global Inbound Mode	Selects the default global inbound mode (e.g., Default Mode, Mode 1, Mode 2, etc.).
BLF Subscription Number	Configures a BLF extension number (e.g., 777) that users can subscribe to on SIP endpoints to monitor the active inbound mode.
Toggle Feature Code	Configures the feature code dialed to activate the corresponding inbound mode (Default: *61 for Default Mode, *62 for Mode 1, etc.).
Name	Configures a custom descriptive label for the inbound mode (e.g., "Day Service", "Night Service", or "Holiday Mode") to easily identify mode purposes.
Prompt	Select, upload, or AI generate a custom audio prompt for the inbound mode. Note: This audio confirmation prompt is played strictly to the administrator or extension user who dials the Feature Code when executing a mode switch.
Add Mode	Click the Add button to create new inbound modes. The system supports up to 9 custom modes in addition to the Default Mode.

Inbound Route: Custom Inbound Mode

In the UCM630X, users can enable Custom Inbound Mode to switch between different destinations for each specific inbound route. The Custom Inbound Mode can be enabled under Inbound Route settings.



Inbound Route - Custom Inbound Mode

The global inbound mode must be enabled before configuring Route-Level Inbound Mode. Additionally, other modes must be configured as well.

When Custom Inbound Mode is enabled, the user can configure a "Default Destination" and or a "Mode X" destination for each specific route. This Inbound route will use the inbound mode specified in this page's **Inbound Mode** setting instead of the configured **Global Inbound Mode**.

Users can toggle the route's inbound mode by dialing "Global Inbound Mode feature code + Inbound Mode Feature Code" and the current inbound route can be monitored by subscribing a BLF to the Inbound Mode Suffix.

For example, the Inbound Default Mode feature code is set to *61 and the Inbound Mode Feature Code for route 1 is set to 1010. To switch the mode of route 1 to Default Mode, users can dial *611010.

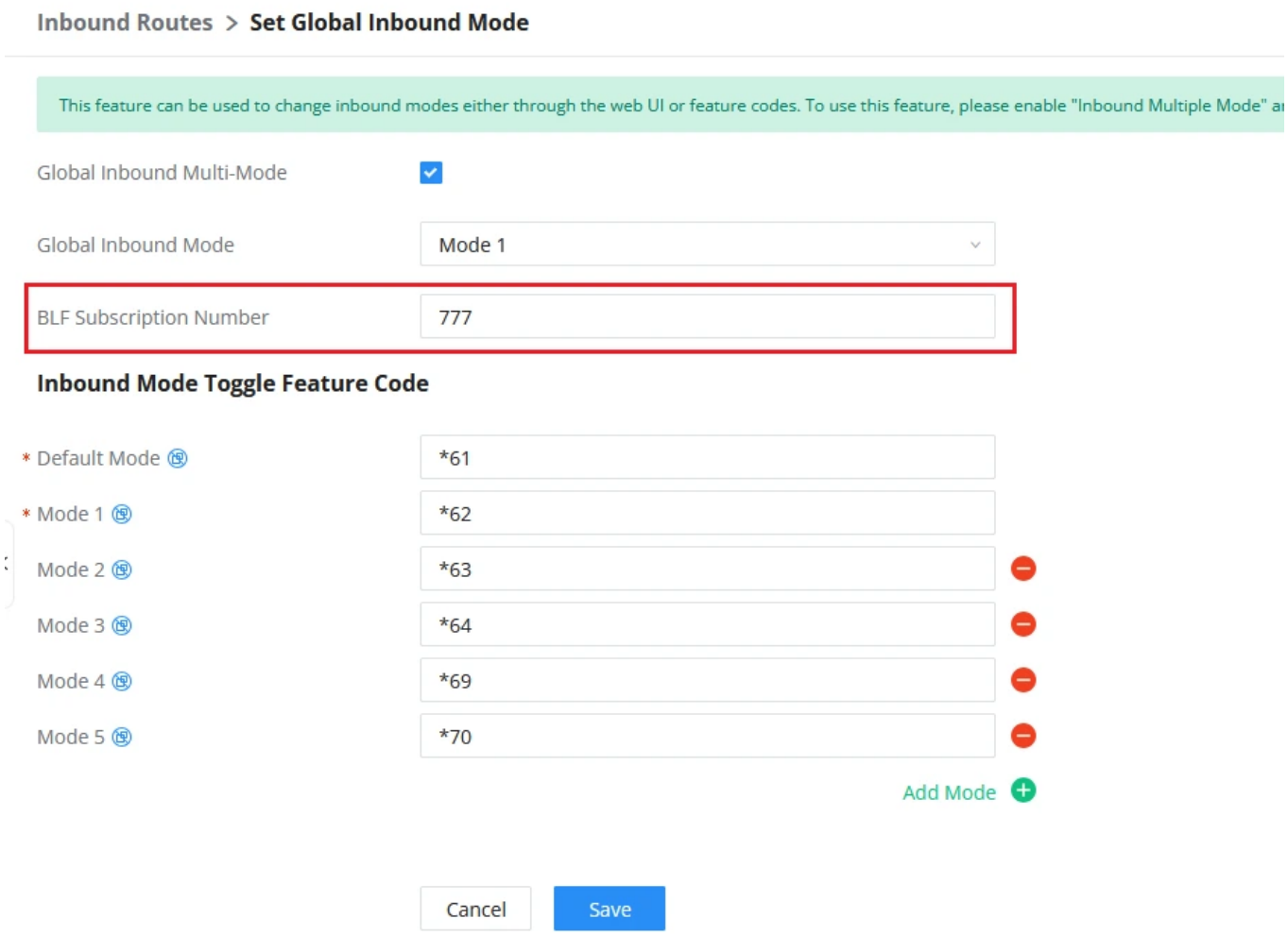
Note: Toggling the global inbound mode will not affect routes that have Custom Inbound Mode enabled. If all routes have the option enabled, toggling the global inbound mode via BLF will trigger a voice prompt indicating that none of the routes will be affected by the global inbound mode change.

Inbound Route: Set Global Inbound Mode (Inbound Mode BLF Monitoring)

Users can assign MPKs and VPKs to monitor and toggle the current global inbound mode of the UCM.

To do this, please refer to the following steps:

1. Access the UCM web GUI and navigate to Extension/Trunk→Inbound Routes.
2. Click on the button and enable Global Inbound Multi-Mode.
3. Edit the subscribe number field to the desired BLF value.



Global Inbound Mode - BLF Subscription Number

4. Configure the BLF value on a phone's MPK/VPK. As an example, a GXP2140 with the BLF configured will show the Inbound Mode status on its screen once configured. The 777 BLF is lit green, indicating that the current inbound mode is "Default Mode".



Inbound Mode - Default Mode

5. Pressing the key will toggle the inbound mode to "Mode 1", and the button's color will change to red.

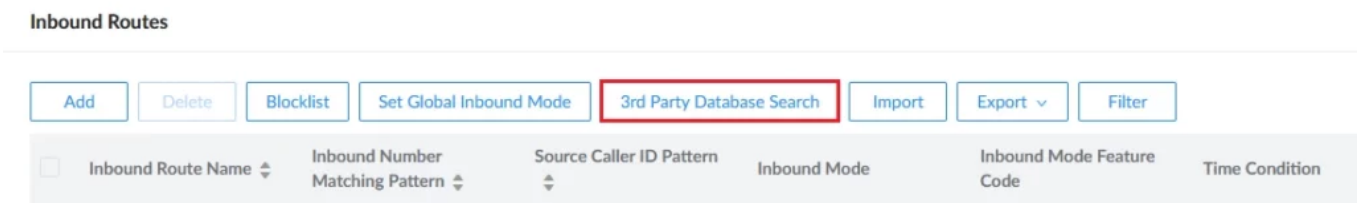


Inbound Mode - Mode 1

Inbound Routes: 3rd Party Database Search

This feature allows the UCM to perform a real-time lookup using an external database when an inbound call is received. If the incoming caller number matches a record in the external database, the corresponding name is retrieved and displayed as the caller ID.

To access this feature, navigate to **Extension/Trunk->Inbound Routes** and click on the "3rd Party Database Search" button.



Inbound Routes Page

Database connection parameters (database type, server address, and credentials) are configured globally under 3rd Party Database Integration. This page only specifies the query keys used to construct the lookup statement for inbound routes.

On this page, users can enable or disable third-party database lookup for inbound routes by enabling or disabling the **3rd Party Database Search** option.

This page also allows users to specify the database objects used by the UCM to construct the SQL query for inbound caller name lookup. The parameters configured here must exactly match the corresponding table and column names in the external database.



3rd Party Database Search Feature for Inbound Routes

The following table describes the parameters used by the UCM to generate the SQL lookup query for inbound caller name resolution.

Field	Description

Table	Specifies the name of the database table that contains caller information. This table is queried when an inbound call is received. Note: The table name must exist in the configured database and be accessible by the database user defined under 3rd Party Database Integration.
Caller Name	Specifies the column in the selected table that stores the caller's display name. When a matching record is found, the value from this column is used as the inbound caller ID name.
Number	Specifies the column in the selected table that stores the phone number. The UCM compares the inbound caller number against this column to determine whether a matching record exists.

Based on the configured query keys, the UCM automatically generates and executes a SQL query in the following format:

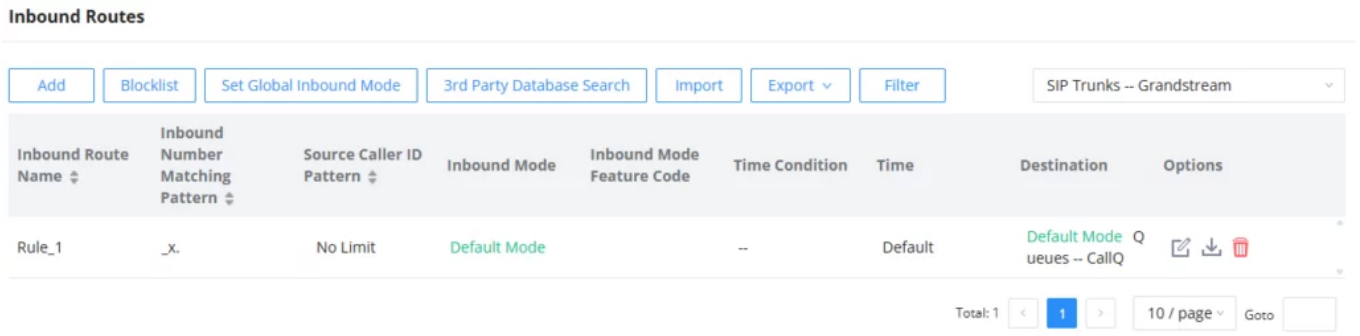
```
SELECT <Caller Name Column>
FROM <Table>
WHERE <Number Column> LIKE '%[INBOUND_NUMBER]%';
```

The inbound caller number is dynamically substituted at call time.

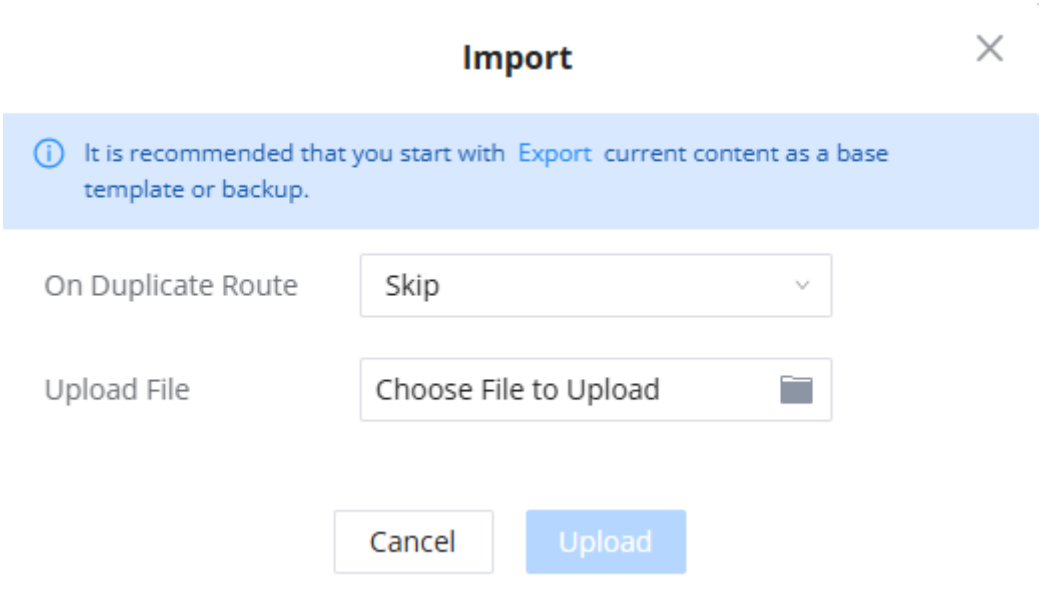
Inbound Route: Import/Export Inbound Route

Users can now import and export inbound routes to quickly set up inbound routing on a UCM or to back up an existing configuration. An exported inbound route configuration can be directly imported without needing any manual modifications.

To import inbound routes, click on "Import".



Import/Export Inbound Route



When uploading the file, the user can choose to either skip or overwrite the existing inbound route by selecting "Skip" or "Update" in On Duplicate Route, respectively.

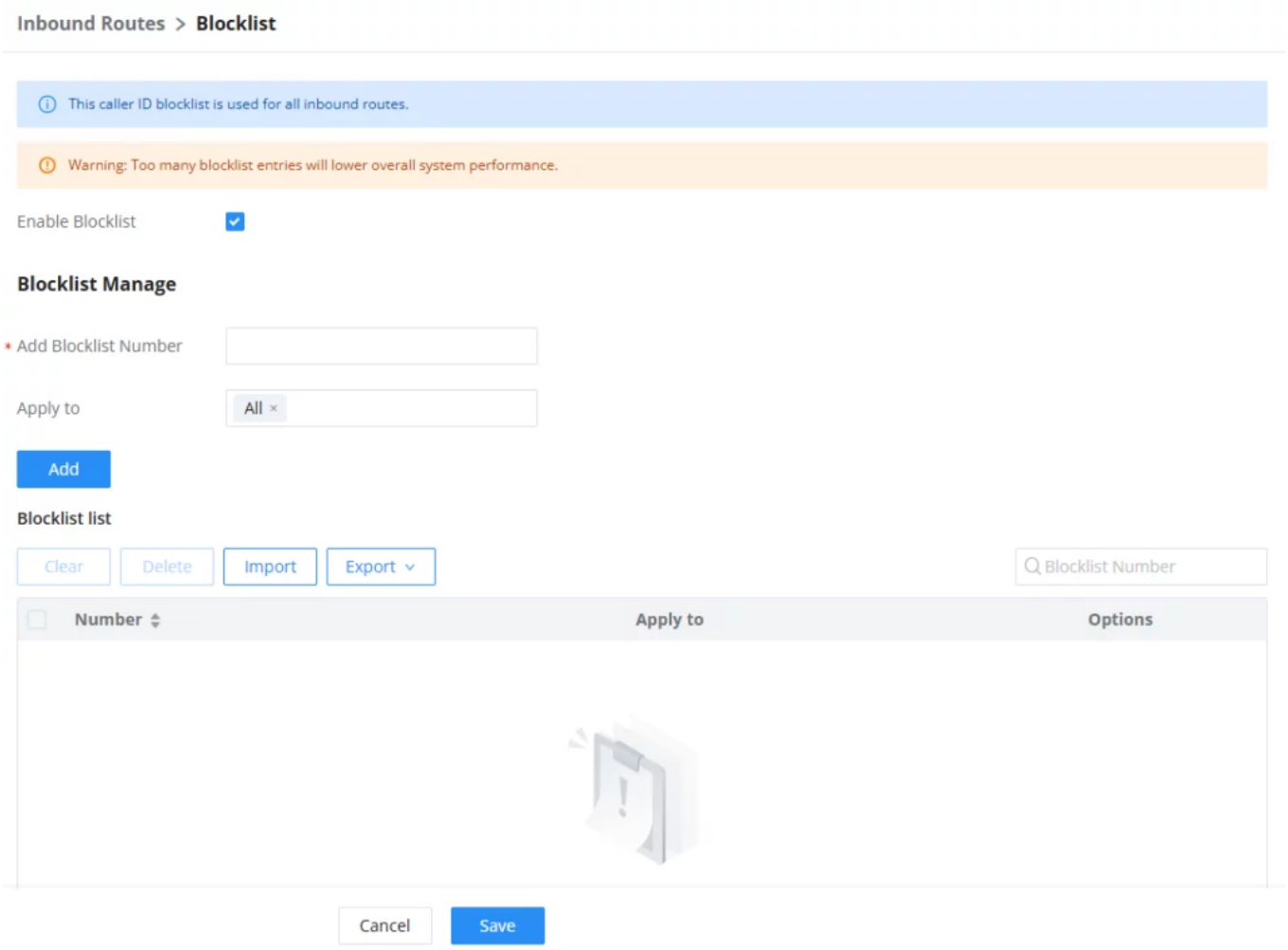
The imported file should be in csv or xlsx format and using UTF-8 encoding, the imported file should contain below columns, and each column should be separated by a comma (It is recommended to use Notepad++ for the imported file creation):

- Disable This Route: Yes/No.
- Pattern: Always prefixed with _
- CallerID Pattern: Always prefixed with _
- Prepend Trunk Name: Yes/No.
- Prepend User Defined Name Enable: Yes/No.
- Prepend User Defined Name: A string.
- Alert-info: None, Ring 1, Ring 2... User should enter an Alert-info string following the values we have in the Inbound route Alert-Info list.
- Allowed to seamless transfer: [Extension_number]
- Inbound Multiple Mode: Yes/No.
- Default Destination: By DID, Extension, Voicemail... Users should enter a Default Destination string following the values we have in the Inbound route Default Destination list.
- Destination: An Extension number, Ring Group Extension...
- Default Time Condition.
- Mode 1: By DID, Extension, Voicemail... Users should enter a Default Destination string following the values we have in the mode 1 Default Destination list.
- Mode 1 Destination: An Extension number, Ring Group Extension...
- Mode 1 Time Condition.

Blocklist Configurations

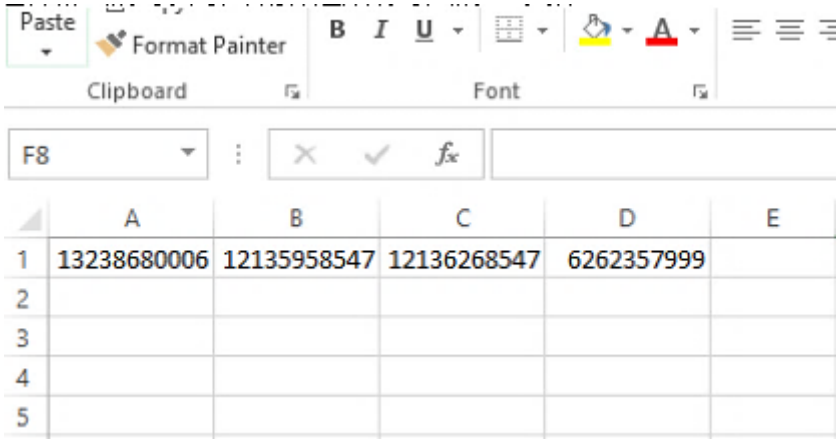
In the UCM630X, blocklist is supported for all inbound routes. Users could enable the blocklistfeature and manage the Blacklist by clicking on "Blacklist".

- Select the checkbox for "Blacklist Enable" to turn on the Blacklist feature for all inbound routes. Blacklist is disabled by default.
- Enter a number in the "Add Blacklist Number" field and then click "Add" to add to the list. Anonymous can also be added as a Blacklist Number by typing "Anonymous" in Add Blacklist Number field.
- To remove a number from the Blacklist, select the number in the "Blacklist list" and click on or click on the" Clear" button to remove all the numbers on the blacklist.
- Users can also export the inbound route blacklist by pressing the button.



Blacklist Configuration Parameters

- To add blacklisted numbers in batch, click on "Import" to upload the blacklist file in csv or xlsx format.



Blacklist CSV File

Users could also add a number to the Blacklist or remove a number from the Blacklist by dialing the feature code for "Blacklist Add' (default: *40) and "Blacklist Remove" (default: *41) from an extension. The feature code can be configured under Web GUI **Basic Call Features > Feature Codes**.

BASIC CALL FEATURES

Multimedia Meeting

The UCM630X supports multimedia meeting room allowing multiple rooms used at the same time.

The multimedia meeting room configurations can be accessed under Web GUI **Basic Call Features > Multimedia Meeting**. In this page, users could create, edit, view, invite, manage the participants, and delete multimedia meeting rooms. The multimedia meeting room status and meeting call recordings (if recording is enabled) will be displayed in this web page as well.

For video meeting, which is based on WebRTC, participants can join the meeting from PC without installing extra plug-in or software.

The UCM admin can create multiple multimedia meeting rooms for users to dial in.

Model	Number of Public Meeting Rooms	Number of Meeting Room Members
UCM6301	4	75
UCM6302	8	150
UCM6304	15	200
UCM6308	25	300

Meeting room specifications affect user participation to a certain extent. UCM supports forecasting of meeting resources. There will be corresponding judgments and adjustments in the following scenarios:

1. When meeting resources are used up, scheduled meeting members cannot join the meeting in advance.
2. When a point-to-point call is transferred to a conference, the conference resources are used up.
3. When meeting resources are used up, do not join a group IM chat when you initiate a meeting.
4. When meeting resources are used up, do not join an instant meeting.
5. Close other instant meetings or scheduled meetings that have timed out to ensure that invited members can join the scheduled meeting.
6. In an ongoing meeting, if the number of invited members exceeds the upper limit, members cannot be invited to join the meeting.
7. Enable flow control for videos and presentations in the conference room.

The multimedia meeting room supports up to 4 video calls and one video presentation.

- The administrator can set the number of videos to 9 parties. The increase in the number of videos will take up more system resources and affect the overall performance of the UCM system. Please set it according to your needs.
- During a meeting, when the system detects that another scheduled meeting is about to be held, it will remind the meeting members that the subsequent meeting room has been reserved, please end the meeting in advance.
- The use of video in the meeting will take up system resources and may cause performance problems when used.
- The maximum meeting duration is 12 hours. If it exceeds 12 hours, the system will remind the current meeting and the host can continue to extend the meeting.

Multimedia Room Configurations

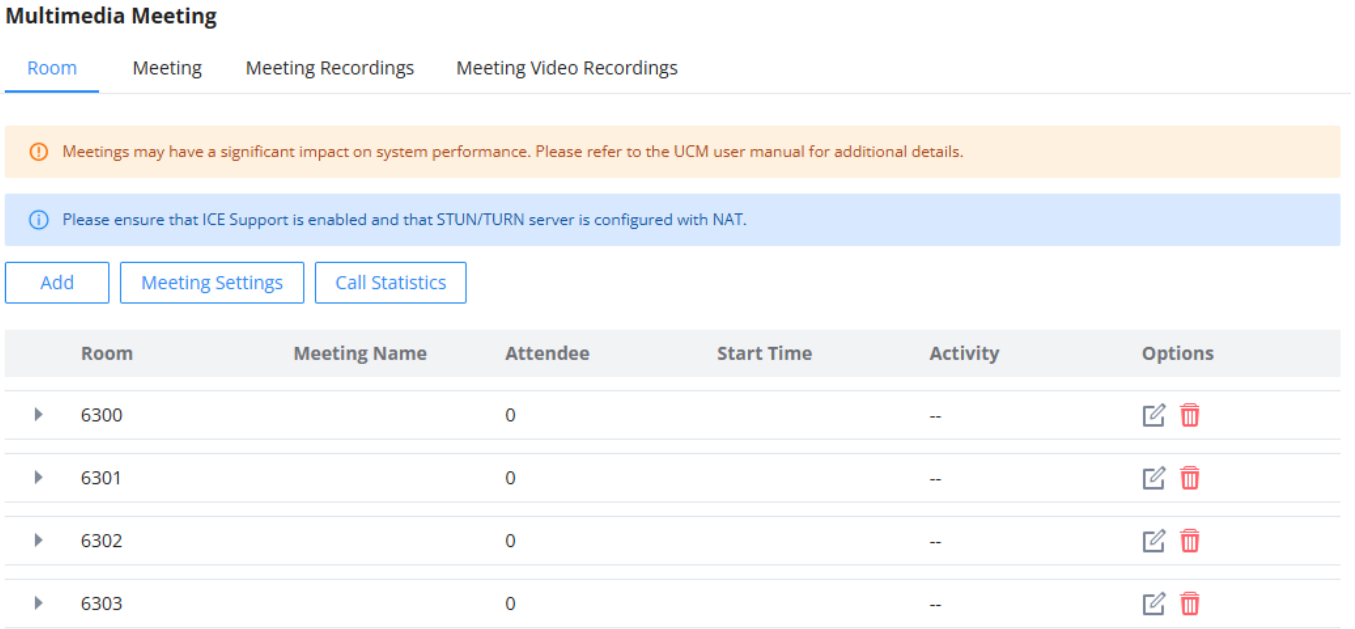
- Click on "Add" to add a new meeting room.

- Click on to edit the meeting room.
- Click on to delete the meeting room.

Meeting Settings contains the following options:

Extension	The number to dial to reach the meeting room.
Meeting Name	Meeting Name
Privilege	Please select the permission for outgoing calls.
Allow User Invite	If enabled, participants will be able to invite other to the meeting by pressing 1 on their keypad or by clicking the Participants -> Invite option on the Wave bottom bar.
Allowed to Override Most Mute	Allowed to Override Host Mute
Auto Record	Meeting audio and video can be automatically recorded. These recordings can be found under the Meeting Recording or Meeting Video Recordings Page. Record Audio: Record only the meeting Audio. Record video: Record the meeting audio and all video feeds. When there is a shared source (shared screen/shared whiteboard/shared document) or focus, only the shared or focus screen is recorded, and when both are present, the shared screen will b recorded. Record video (Focus Mode): Record the focus screen and all audio of the meeting. When a shared source is present in the meeting, only the shared screen is recorded.
Room Password	If meeting room password is configured, meeting participants will need to enter a password to enter the room. Scheduling meetings will not be supported for this room.

Log in to the UCM Web GUI and open the **Basic Call Features > Multimedia Meeting** page to manage the conference room. Users can create, edit, view, invite, manage meeting members, and delete meeting rooms. The conference room status and conference call recording (if recording function is enabled) will be displayed on the page. The meeting rooms in the list include public meeting rooms and random meeting rooms. For temporary meeting room administrators, only the "batch kicking people" function is supported. The temporary meeting room has no meeting password and host code. The member who initiates the group meeting is the host, and ordinary members have the right to invite.



Multimedia Meeting

Meeting Settings

To edit the general settings of the meeting rooms created in the UCM, the user can click on the **Meeting**

Settings button under the **Room** tab under **Basic Call Features -> Multimedia Meeting**.

The table below describes the available parameters in Meeting Settings:

Option	Description
Meeting Max Concurrent Audio	Configures the maximum number of concurrent audio streams allowed in a meeting session.
Meeting Voice Indicator Sensitivity	Adjusts the voice indicator sensitivity level (e.g., Low, Medium, High) to detect active speakers during meetings.
Meeting Audio Quality	Configures the default meeting audio quality and sample rate (e.g., Opus Fullband 48 kHz).
Meeting Recording Prompt	Enables or disables playing an audio prompt informing participants that the meeting is being recorded.
Allow New Participants To View Chat History	When enabled, late-joining participants can view chat messages sent prior to their entry into the meeting.
Meeting AGC	Enables Automatic Gain Control (AGC) for audio processing during meetings.
Auto End Meeting	Configures the system to automatically end meeting rooms when no active participants remain.
Silence Suppression	Enables silence suppression to save bandwidth by not transmitting audio packets during periods of silence.
Use Station ID as Prefix	If enabled, the UCM's configured Station ID will be prepended as a prefix to randomly generated conference room numbers. Note: This allows users on remote UCM extension nodes to directly dial into randomly created meeting rooms across multi-PBX networks via outbound routes. Station ID can be configured under PBX Settings > General Settings > General Preferences.
Add Contact Number to Email	Enables including a contact phone number in automated meeting email invitations.
Contact Number	Selects or specifies the contact phone number (e.g., Enterprise Contact Number) included in meeting invitation emails.
Enable Talk Detection	Enables DSP talk detection to dynamically track and highlight active speakers.
DSP Talking Threshold (ms)	Configures the time duration threshold (in ms) for the DSP to identify continuous speech before declaring a participant as talking. Default is 200 ms.
DSP Silence Threshold (ms)	Configures the time duration threshold (in ms) of continuous silence before the DSP determines a speaker has stopped talking. Default is 2500 ms.
Max Number of Video Feeds	Configures the maximum number of simultaneous video feeds displayed in meeting sessions.
Audio Codec Preference	Specifies and prioritizes supported audio codecs (e.g., Opus, PCMU, PCMA, GSM, G.726, G.722) for meeting connections.
Packet Loss Retransmission	Configures packet loss retransmission protocols (e.g., NACK+RTX) to ensure audio/video quality over lossy networks.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.

Multimedia Meeting Call Operations

Join a Meeting Call

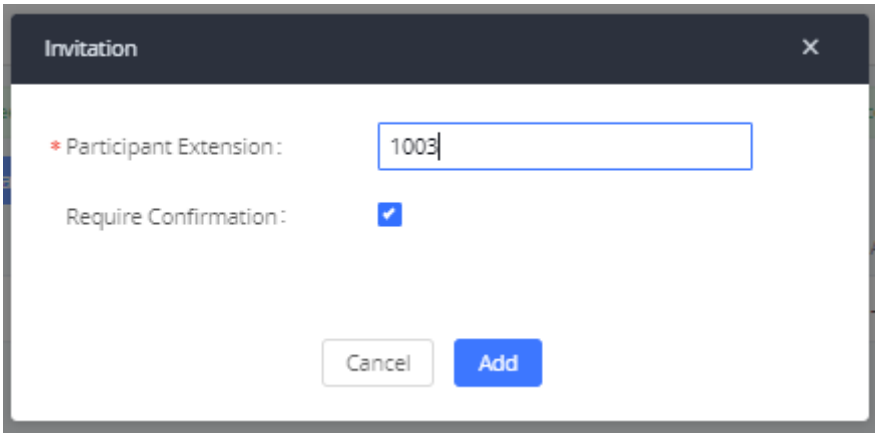
Users could dial the meeting room extension to join the meeting. If password is required, enter the password to join the meeting as a normal user, or enter the admin password to join the meeting as administrator.

Invite Other Parties to Join Meeting

When using the UCM630X meeting room., there are two ways to invite other parties to join the meeting.

- **Invite from Web GUI.**

For each meeting room in UCM630X Web GUI **Basic Call Features > Multimedia Meeting**, there is an icon for option "Invite a participant". Click on it and enter the number of the party you would like to invite. Then click on "Add". A call will be sent to this number to join it into the conference.



Meeting Invitation from Web GUI

- **Invite by dialing 0 or 1 during conference call.**

A meeting participant can invite other parties to the meeting by dialing from the phone during the meeting call. Please make sure option "Enable User Invite" is turned on for the meeting room first. Enter 0 or 1 during the meeting call. Follow the voice prompt to input the number of the party you would like to invite. A call will be sent to this number to join it into the meeting.

0: If 0 is entered to invite other party, once the invited party picks up the invitation call, a permission will be asked to "accept" or "reject" the invitation before joining the conference.

1: If 1 is entered to invite other party, no permission will be required from the invited party.

Conference administrator can always invite other parties from the phone during the call by entering 0 or 1. To join a conference room as administrator, enter the admin password when joining the conference. A conference room can have multiple administrators.

During The Meeting

During the meeting call, users can manage the conference from Web GUI or IVR.

- **Manage the meeting call from Web GUI.**

Log in UCM630X Web GUI during the meeting call, the participants in each meeting room will be listed.

1. Click on to kick a participant from the meeting.
2. Click on to mute the participant.
3. Click on to lock this meeting room so that other users cannot join it anymore.
4. Click on to invite other users into the meeting room.
5. Click on to Invite meeting rooms or invite contact groups.

- **Manage the meeting call from IVR.**

Please see options listed in the table below.

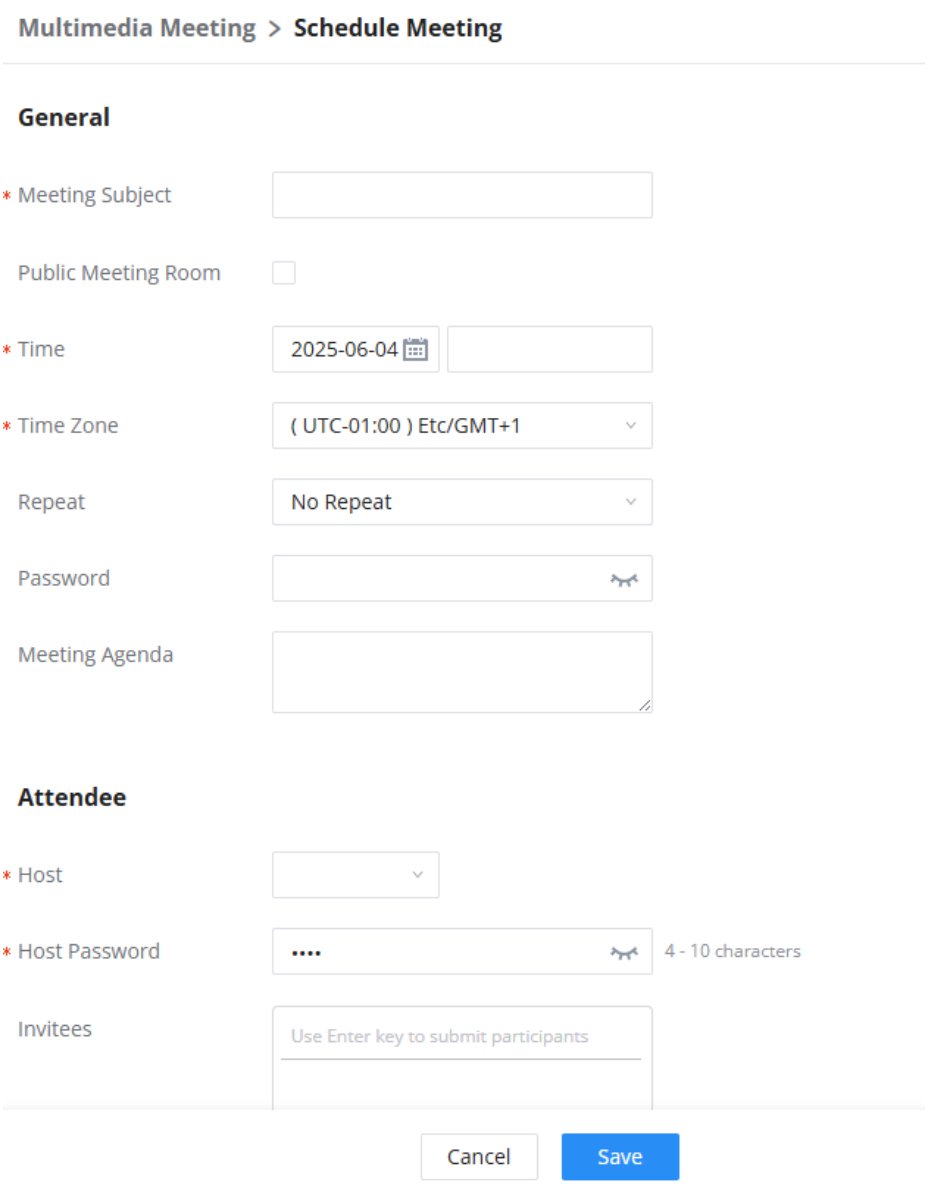
Meeting Administrator IVR Menu	
1	Mute/unmute yourself.
2	Lock/unlock the conference room.
3	Kick the last joined user from the conference.
4	Decrease the volume of the conference call.
5	Decrease your volume.
6	Increase the volume of the conference call.
7	Increase your volume.
8	More options. 1: List all users currently in the conference call. 2: Kick all non-Administrator participants from the conference call. 3: Mute/Unmute all non-Administrator participants from the conference call. 4: Record the conference call. 8: Exit the caller menu and return to the conference.
Meeting User IVR Menu	
1	Mute/unmute yourself.
4	Decrease the volume of the conference call.
5	Decrease your volume.
6	Increase the volume of the conference call.
7	Increase your volume.
8	Exit the caller menu and return to the conference.

When there is participant in the meeting, the meeting room configuration cannot be modified.

Schedule Meeting

Log in to the UCM Web GUI, open the **Basic Call Features > Mutimedia Meeting > Meeting Schedule** page, and you can manage the reservation management of the meeting room. Users can create, edit, view, and delete conference room reservation records. The following is a set meeting room reservation, which shows the ongoing and pending reservations. Once the conference room is reserved, all users will be removed from the conference room at the start time, and extensions will no longer be allowed to enter the conference room. At the scheduled meeting time, UCM will send invitations to the extensions that have been selected to participate in the meeting. At the same time, it supports users to enter the meeting 10 minutes in advance. If the current meeting is occupied, enter the waiting room and wait (members joining the meeting in advance occupy global member resources, but it will be released after the scheduled meeting starts); otherwise, you can join the meeting directly and the meeting will be held in advance. After the meeting ends, the reservation record is transferred to meeting history list. Meeting history displays the information of the ended and expired meetings.

- Click the button "Schedule Meeting" to edit the meeting room reservation.

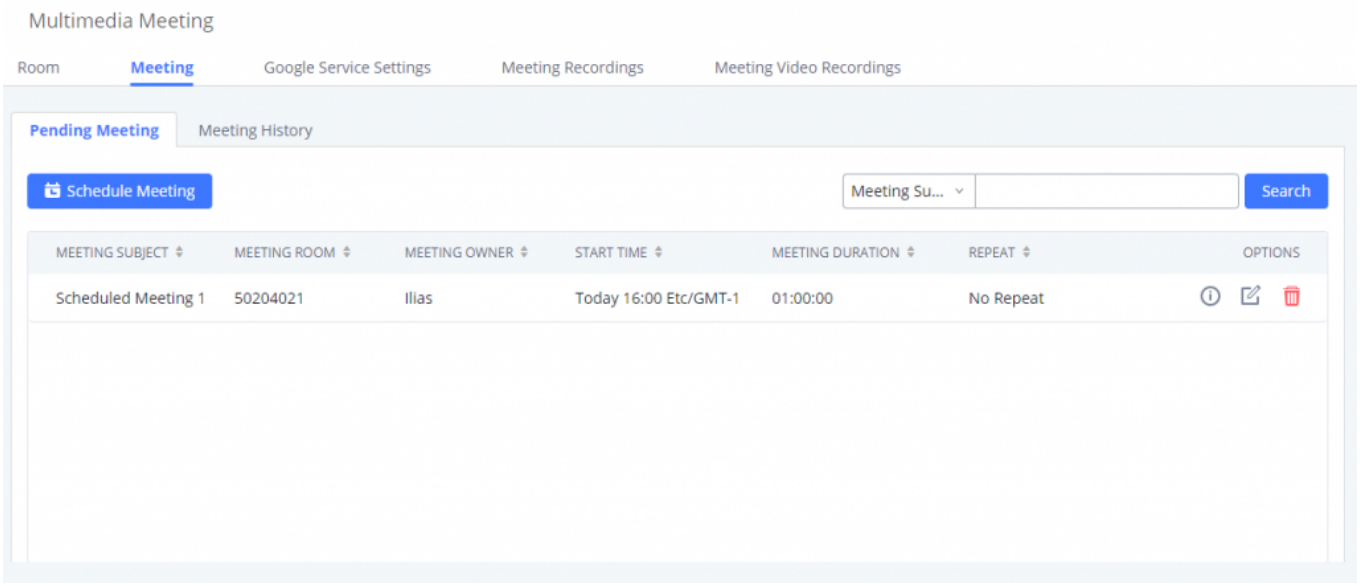


Schedule meeting Interface

General	
Meeting Subject	Configure the name of the scheduled meeting. Letters, digits, some special characters are also supported. The characters ` % # ? < > @ $ ^ ~ | are not allowed.
Public Meeting Room	Choose which room to have this scheduled meeting.
Time	Configure the meeting date and time.
Time Zone	Select the meeting time zone.
Repeat	Choose when to repeat a scheduled meeting. No Repeat Every Day Weekly Monthly Custom: it specifies how often the meeting is repeated per days/weeks. E.g., every 3 days/weeks.
End Repeat	This option appears when a reccurrent schedule is configured. Configure the date when the recurrence stops.
Password	Configure the meeting's login password.
Meeting Agenda	The description of this scheduled meeting.
Attendee	
Host	Configure Host.

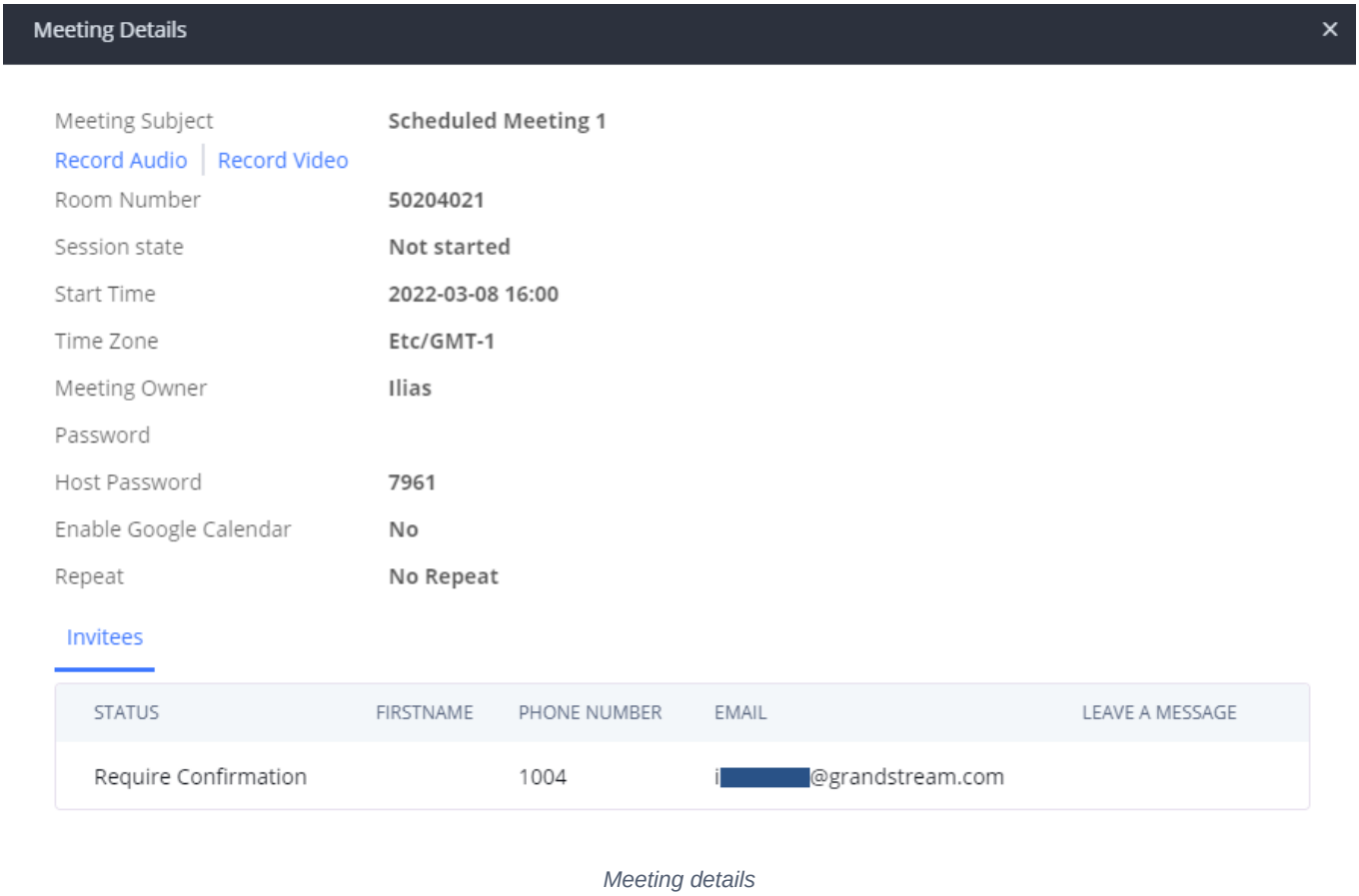
Host Password	Configure the Host Password. Note: It is randomly generated when first creating a new meeting Schedule.
Invitees	Local extensions, remote extensions, and special extensions are supported.
Allow User Invite	If enabled, participants will be able to invite others to the meeting by pressing 1 on their keypad or by clicking the Participants->Invite option.
Advanced	
Email Reminder (m)	Check to enable scheduled meeting email reminder. Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-120. 60 is the default value. Note: After editing the time of a single recurrence of a scheduled meeting, a cancellation email will be sent out followed by a meeting update email.
Call Participant	If enabled, the invited participants will be called upon meeting start time.
Allowed to Override Host Mute	If enabled, participants will be able to unmute themselves if they have been muted by the host.
Play Joining/Leaving Meeting Announcement	Configure whether the join/leave meeting prompt is played when participants join or leave.
Auto Record	Meeting audio and video can be automatically recorded. These recordings can be found under the Meeting Recordings or Meeting Video Recordings page. Record Audio: Record only the meeting audio. Record Video: Record the meeting audio and all video feeds. When there is a shared source (shared screen/shared whiteboard/shared document) or focus, only the shared or focus screen is recorded, and when both are present, the shared screen is recorded. Record Video (Focus Mode): Record the focus screen and all audio of the meeting. When a shared source is present in the meeting, only the shared screen is recorded. Note: Please note that UCM63XX Audio Series doesn't support Screen Sharing, Whiteboard, or PDF file sharing.
Sync Google Calendar	Select this option to sync scheduled meeting with Google Calendar. Note: Google Service Setting OAuth2.0 must be configured on the IPPBX. Please refer to section [Google Service Settings Support].
Support AI transcription	Choose whether to support AI transcription for the scheduled meeting. This parameter cannot be controlled if the AI meeting transcription and summary is disabled in the general AI Settings.
Language	Specifies the language recognition behavior used for AI transcription. The options are: Automatic Recognition: Automatically detects the spoken language during the meeting. This is recommended when multiple languages are expected, though recognition accuracy may vary. Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy. Note: This setting controls only the transcription language for this scheduled meeting. It does not apply to the general AI Conference Transcription and Summary feature.
Automatic AI Transcription	Once enabled, meeting audio will be automatically transcribed in real time once the meeting starts. A summary will also be generated after the meeting.
Allow Participants to View Summary	When enabled, meeting summaries generated by AI are made accessible to all attendees via meeting reports, rather than restricting access exclusively to the host or organizer.

Once the Meeting Schedule is configured, scheduled meeting will be displayed as below figure.



Meetings Schedule

- Click the button to view the meeting details in the Meeting room. The meeting details of Meeting History include actual participant information.

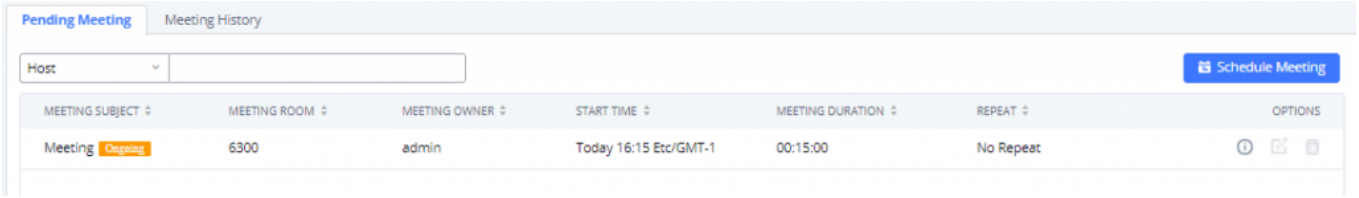


Meeting details

- Click on to edit the Meeting Schedule.
- Click on to delete the Meeting Schedule.

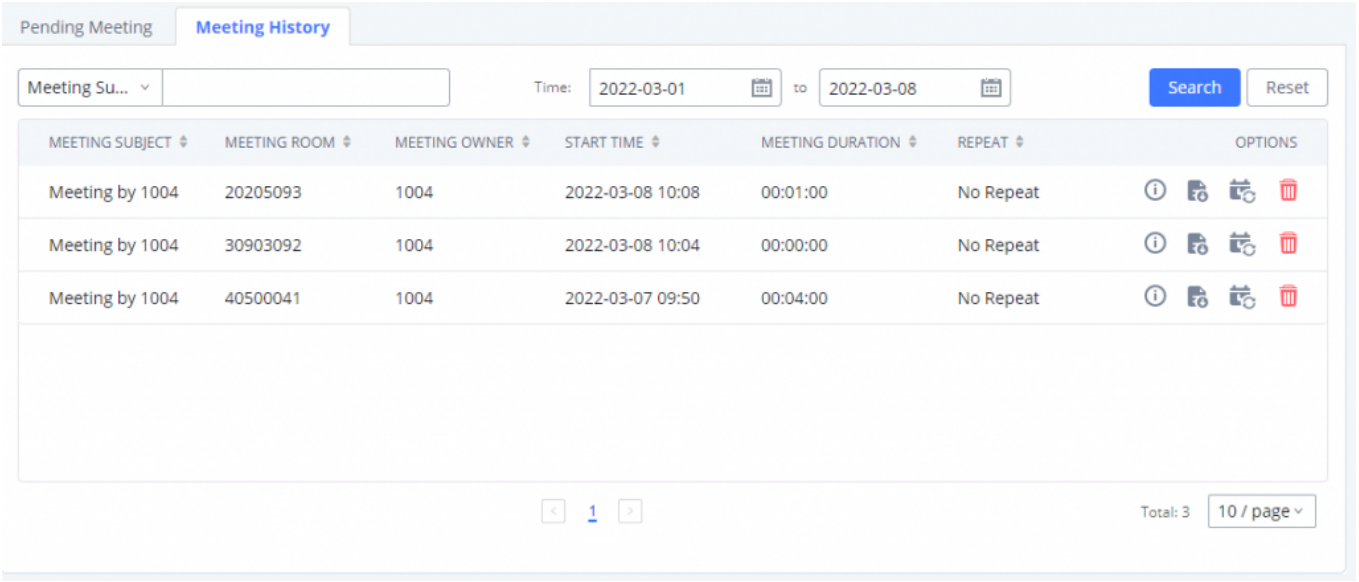
At the scheduled meeting time, UCM630X will send INVITE to the extensions that have been selected for conference.

Once the meeting starts, it will be displayed under **Pending Meeting** with an "Ongoing" status, as displayed below:



Meeting Scheduled - Ongoing

Once the conference is finished, the conference will be displayed under Meeting History as shown below:

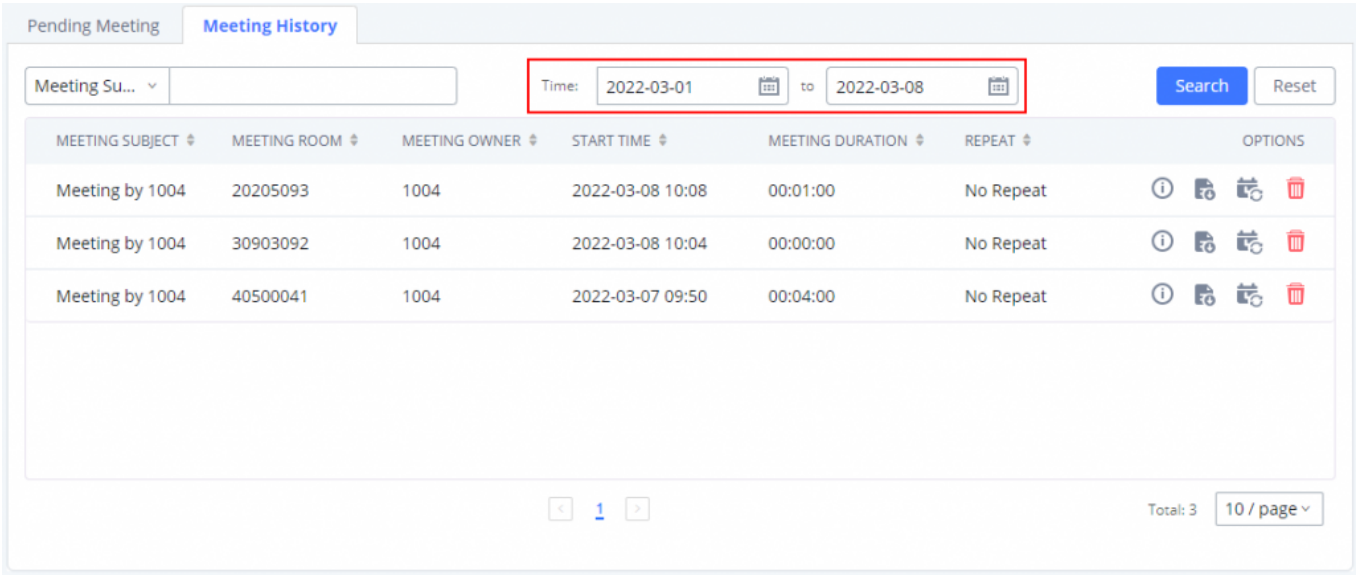


Meeting Schedule - Completed

- Click the button to download the Meeting Report of the meeting.
- Click the button to reschedule the Meeting.

In addition, once the meeting ends, the system will send a meeting report email to the host including PDF file where he/she can view the meeting, participant information, device type and trend graph of participant levels.

You can also choose to display the meetings that took place in a specific timeframe. Please see the screenshot below:



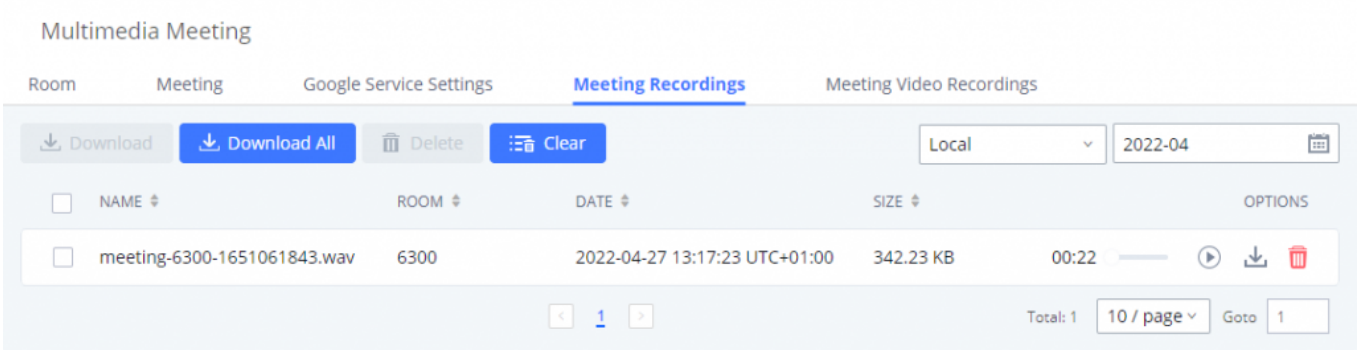
Please make sure that outbound route is properly configured for remote extensions to join the meeting.

Meeting Recordings

The UCM630X allows users to record the audio of the meeting call and retrieve the recording from Web GUI→**Basic Call Features > Multimedia Meeting > Meeting Recordings**.

To record the Meeting call, when the meeting room is in idle, enable "Auto Record" from the meeting room configuration dialog. Save the setting and apply the change. When the meeting call starts, the call will be automatically recorded in .wav format.

The recording files will be listed as below once available. Users could click on to download the recording or click on to delete the recording. Users could also delete all recording files by clicking on "Delete All Recording Files" or delete multiple recording files at once by clicking on "Delete" after selecting the recording files.



Meeting Recordings

Meeting Video Recordings

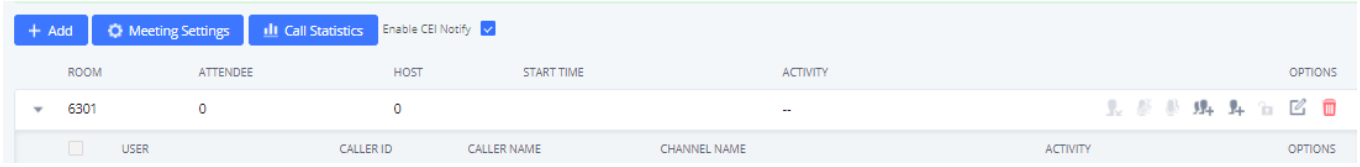
The UCM630X allows users to record the audio and video of the meeting call and retrieve the recording from Web GUI **Basic Call Features > Multimedia Meeting > Meeting Recordings**.

To record the Meeting call, when the meeting room is in idle, enable "Auto Record" from the meeting room configuration dialog. Save the setting and apply the change. When the meeting call starts, the call will be automatically recorded in .mkv format.

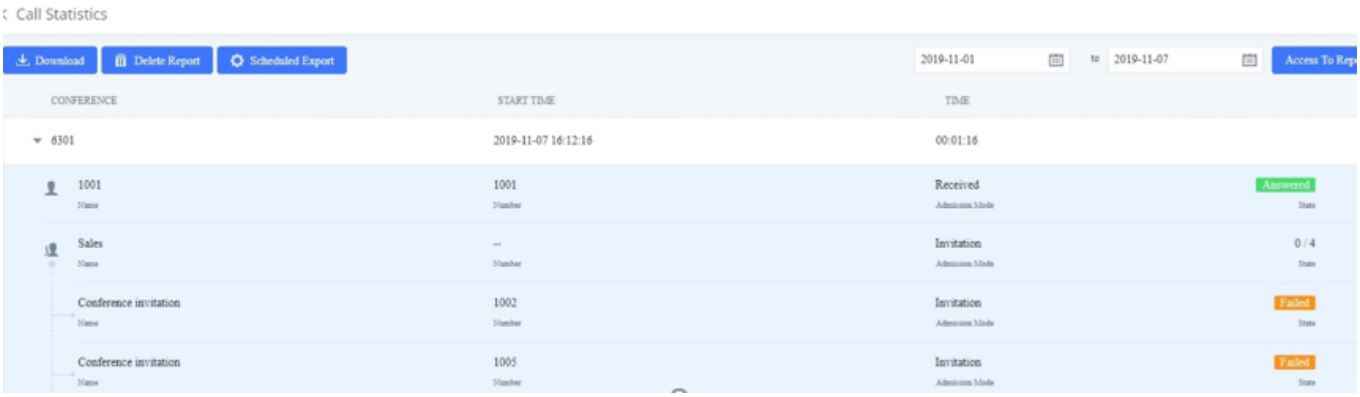
The recording files will be listed as below once available. Users could click on to download the recording or click on to delete the recording. Users could also delete all recording files by clicking on "Delete All Recording Files" or delete multiple recording files at once by clicking on "Delete" after selecting the recording files.

Call Statistics

Meeting reports will now be generated after every conference. These reports can be exported to a csv or xlsx file for offline viewing. The conference report page can be accessed by clicking on the Call Statistics button on the main Conference page.



Meeting Call Statistics



Meeting Report on Web

	A	B	C	D	E	F	G
1	Room	Start Time	Duration Time				
2	6301	11/7/2019 16:12	0:01:16				
3	Contact Number	Name	Way	Status	Contact Group Name		
4	1002	Conference invitatio	INVITE	FAILURE	Sales		
5	1005	Conference invitatio	INVITE	FAILURE	Sales		
6	1004	Conference invitatio	INVITE	FAILURE	Sales		
7	1003	Conference invitatio	INVITE	FAILURE	Sales		
8	1001	1001	CALLIN	ANSWER			

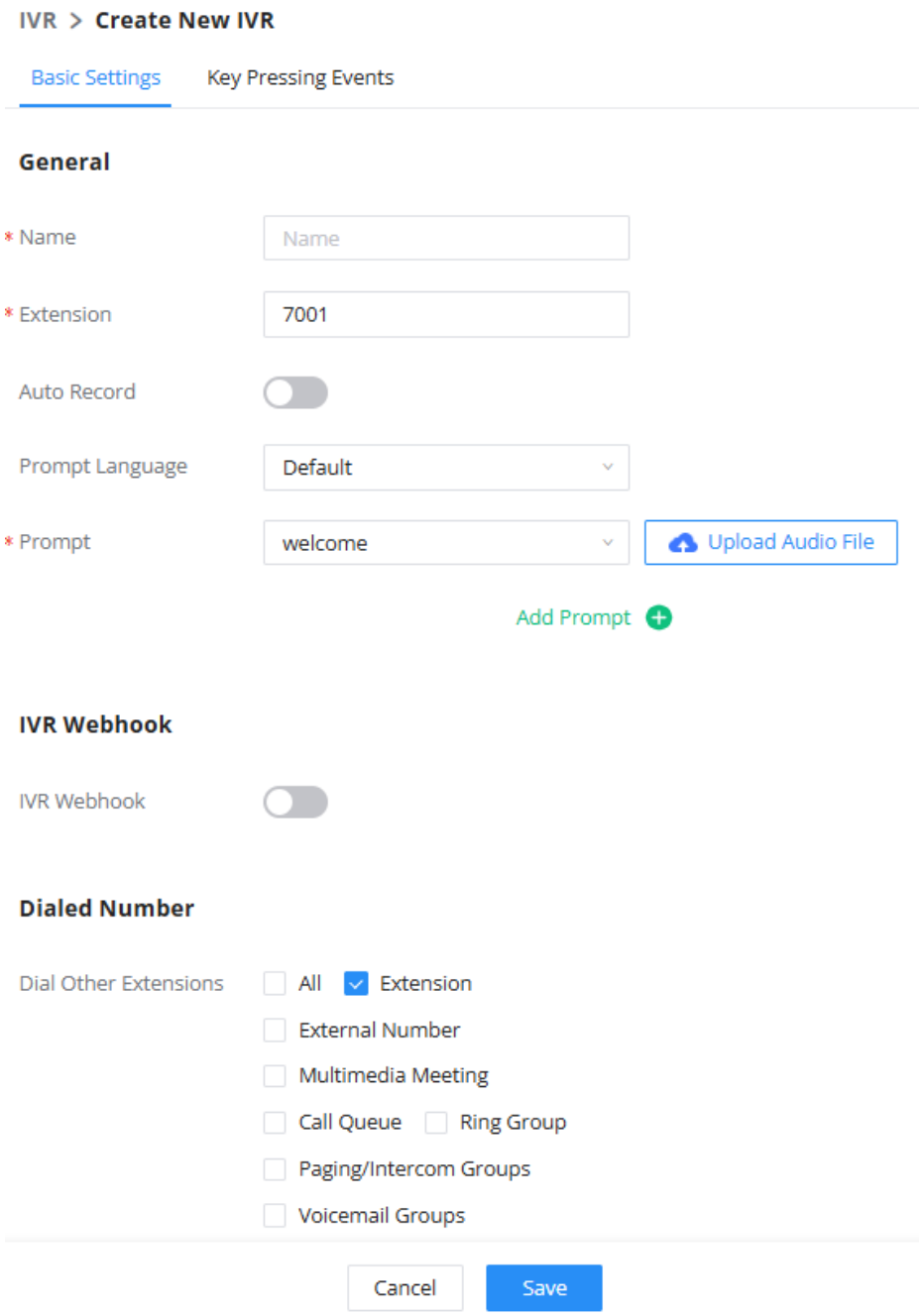
Meeting Report on CSV

IVR

Configure IVR

IVR configurations can be accessed under the UCM630X Web GUI **Basic Call Features > IVR**. Users could create, edit, view, and delete an IVR.

- Click on "Add" to add a new IVR.
- Click on to edit the IVR configuration.
- Click on to delete the IVR.

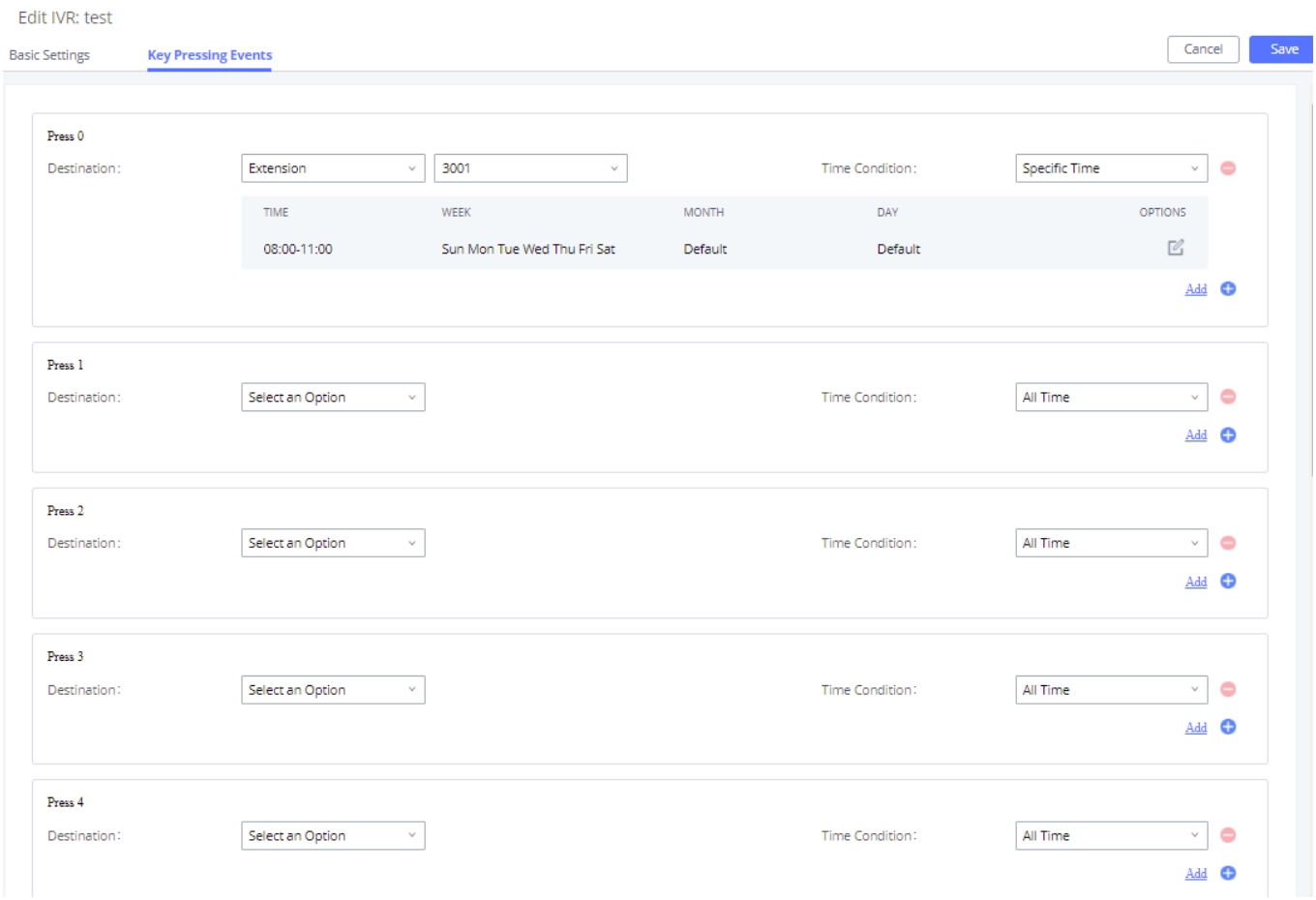


Create New IVR

General	
Name	Configure the name of the IVR. Letters, digits, _ and - are allowed.
Extension	Enter the extension number for users to access the IVR.
Auto Record	If enabled, calls to this IVR will automatically be recorded.
Prompt Language	Select voice prompt language for this extension. If set to "Default", the global setting for Voice Prompt will be used.?This configuration only applies to the system prompt, and does not affect the language of custom prompt.
Prompt	Initial tone that plays when the user enters the IVR.
IVR Webhook	
IVR Webhook	If enabled, call event notification and call control can be achieved via URL. Using webhooks, the user can send requests to a specific server to perform actions through DTMF.

Target URL	Target URL address for receiving notification commands as well as sending operation commands. It needs to be the full URL of the web server, static parameters and pages can be included.?
Username	Enter the username used to connect to the target URL.
Password	Enter the password used to connect to the target URL.
Call Event	Select the call events to notify the IVR about.AllNotify IVR of Incoming CallsNotify IVR of AnswerNotify IVR of DTMF EventsNotify IVR of End
Call Control	If enabled, the predefined IVR flow for the destination URL will be followed. Configurations related to the original IVR flow such as dialed numbers, key events, etc. will be disabled.
Timeout Time (s)	Configure the timeout time for receiving call control, default 2 seconds, the system tries up to three times after the timeout.
Timeout/Invalid Settings	
Digit Timeout (s)	Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, the UCM630X will consider the entries complete. The default timeout is 3s.
Response Timeout (s)	After playing the prompts in the IVR, the UCM630X will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout prompt will be played. The default setting is 10 seconds.
Response Timeout Prompt	Select the prompt message to be played when timeout occurs.
Response Timeout Prompt Repeats	Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3.
Invalid Input Prompt	Select the prompt message to be played when an invalid extension is pressed.
Invalid Input Prompt Repeats	Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3.
PMS Wake-Up Call Service Mode	
PMS Wake-Up Call Service	If enabled, this IVR can be used with Wakeup Service to send notifications to specified destinations based on caller key presses.If enabled, key events will only be supported in standard mode. Time conditions will not be supported.
Other Settings	
Replace Display Name	If enabled, the UCM will replace the caller display name with IVR name.
Return IVR Menu	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
Alert-info	When present in an INVITE request, the Alert-info header field specifies an alternative ringtone to the UAS.
IVR Black/Whitelist	If enabled only numbers inside of the Whitelist or outside of the Blacklist can be called from IVR.
Internal Black/Whitelist	Contain numbers, either of Blacklist or Whitelist.
External Black/Whitelist	This feature can be used only when Dial Trunk is enabled, it contains external numbers allowed or denied calling from the IVR, the allowed format is the following: Number1, number2, number3...
Replace Display Name	If enabled, the UCM will replace the caller display name with IVR name.
Return to IVR Menu	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
Alert Info	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.

Timeout	When exceeding the number of defined answer timeout, IVR will enter the configured event when timeout. If not configured, then it will Hangup.
Invalid	Configure the destination when the Invalid Repeat Loop is done.
Time Condition	Configure the time condition for each key press event, so that it goes to the corresponding destination within a specified time.



Key Pressing Events

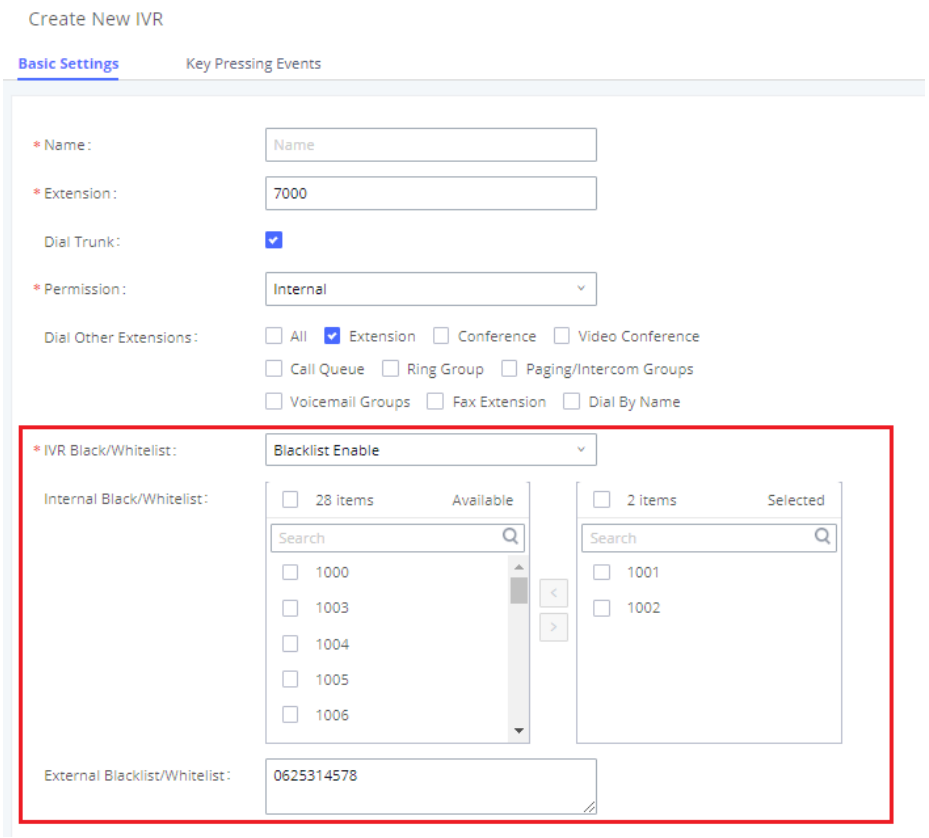
Blocklist/Allowlist in IVR

In some scenarios, the IPPBX administrator needs to restrict the extensions that can be reached from IVR. For example, the company CEO and directors prefer only receiving calls transferred by the secretary, some special extensions are used on IP surveillance end points which should not be reached from external calls via IVR for privacy reason. UCM has now added blacklist and whitelist in IVR settings for users to manage this.

Up to 500 extensions are allowed on the blocklist/allowlist.

To use this feature, log in UCM Web GUI and navigate to **Basic Call Features** > **IVR** > Create/Edit IVR: IVR Black/Whitelist.

- If the user selects "Blocklist Enable" and adds extension in the list, the extensions in the list will not be allowed to be reached via IVR.
- If the user selects "Allowlist Enable" and adds extension in the list, only the extensions in the list can be allowed to be reached via IVR.



Black/Whitelist

Create Custom Prompt

To record new IVR prompt or upload IVR prompt to be used in IVR, click on "Upload Audio File" next to the "Welcome Prompt" option and the users will be redirected to Custom Prompt page. Or users could go to Web GUI→**PBX Settings→Voice Prompt→Custom Prompt** page directly.



Click on Prompt to Create IVR Prompt

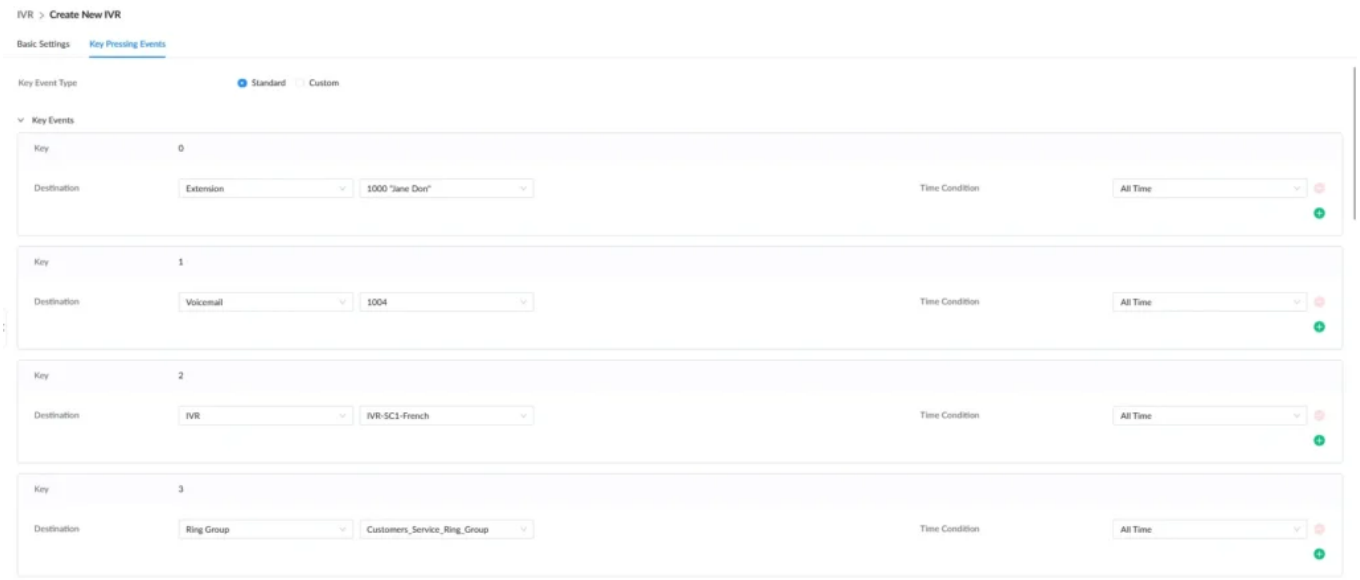
Once the IVR prompt file is successfully added to the UCM630X, it will be added into the prompt list options for users to select in different IVR scenarios.

Key Pressing Events

Standard Key Event

UCM supports adding time conditions for different key events, so that each key event of the IVR goes to the corresponding destination within a specified time.

Each key event supports up to five time conditions, the options available are: All time, Office Time, Out of Office Time, Holiday, Out of Holiday, Out of Office Time or Holiday, Office Time and Out Of Holiday, Specific time.



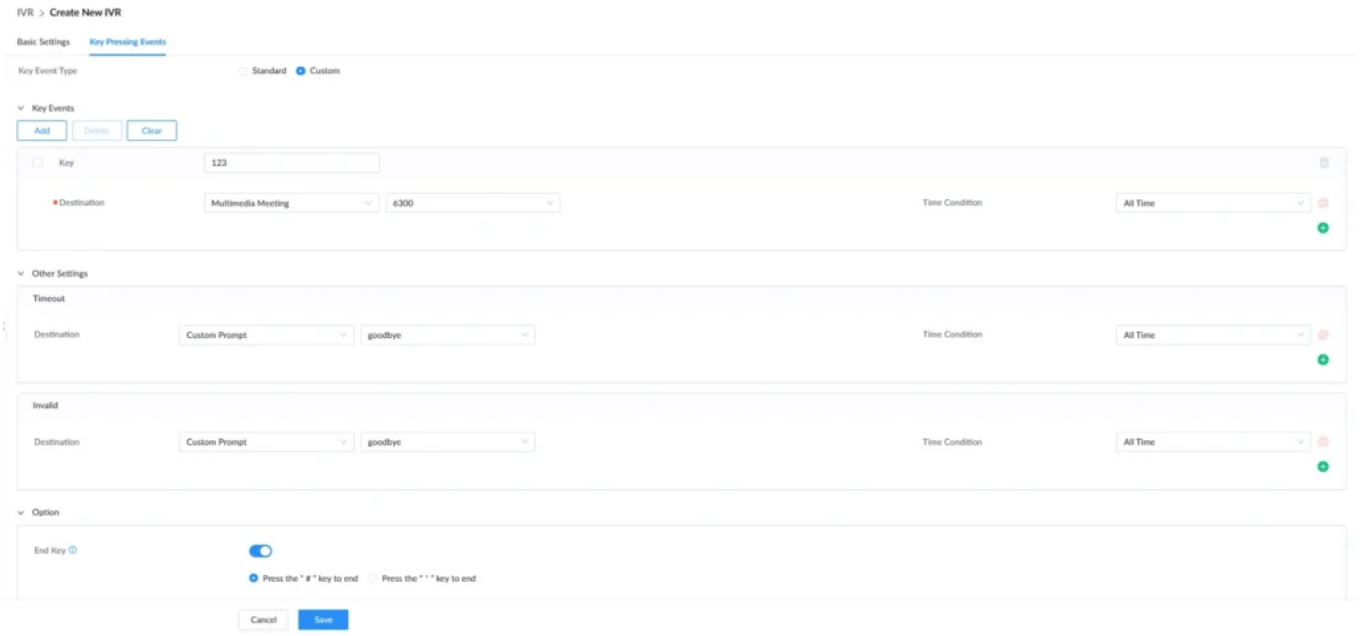
If you select "Specific time", you need to select the start time and the end time. The frequency supports two options: By week and By Month. By default, the specific time does not include holidays.

The following table describes available options that can be assigned for Standard Key Pressing Events:

Option	Description
Key Event Type	Select Standard to configure single-key DTMF events (0-9, *, #). This mode supports time-based routing per key.
Key (0-9, *, #)	Each section corresponds to a specific DTMF key. Configuration under a key defines how calls are routed when that key is pressed.
Destination	Select the destination type and target for the key event. Supported destinations include: Extension Meeting Voicemail Voicemail Group IVR (Maximum 64 nested IVRs) Ring Group Queues Paging/Intercom Group Fax Custom Prompt Hang-up DISA Dial By Name External Number Callback Announcement SMS (Sends a pre-configured automated SMS template to the caller) Time Condition Routing
Time Condition	Assign a time condition to each destination entry. The IVR evaluates time conditions in order and routes the call to the first matching rule. Common options include All Time, Office Time, Out of Office Time, Holiday, and Specific Time. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for the same key, or the (-) icon to remove an existing rule.
Timeout	Configures the destination when the Timeout Repeat Loop is done. Note: Multiple destination entries with different time conditions (up to five) can be configured for this option.
Invalid	Configures the destination when the Invalid Repeat Loop is done. Note: Multiple destination entries with different time conditions (up to five) can be configured for this option.
End Key	Configures whether the caller can press a designated End Key to complete their DTMF input immediately and be directed to the target destination. Options: Press the "#" key to end Press the "*" key to end Note: The configured End Key value must not conflict with key values defined in key pressing events to avoid recognition failure.

Custom Key Event

Users can create custom IVR key press events, vastly increasing the options a business can provide to its customers and improving customer relations and accessibility.



This feature supports the following:

- Up to 100 custom key press events
- Each key combination can contain up to 8 characters (numbers, star (*), and pound (#) depending on End Key settings)
- Supports Time Conditions
- Different custom keys can have the same Destination and Time Condition

IVR option **Dial Other Extensions** is supported when using custom IVR keys, provided there are no digit sequence conflicts with defined custom key combinations.

The following options are available for Custom Key Pressing Events:

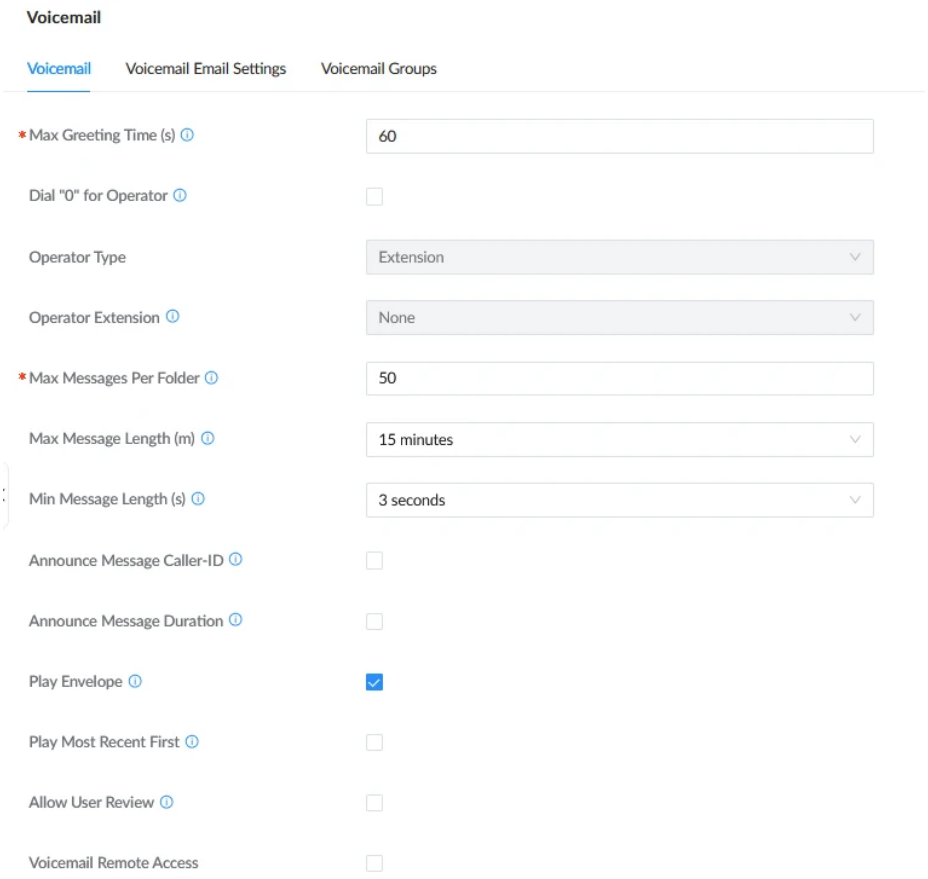
Option	Description
Key Event Type	Select Custom to configure multi-digit DTMF key combinations. This mode supports time-based routing and advanced IVR logic.
Key	Defines the DTMF key combination that triggers the event. Notes: Each key combination can contain up to 8 characters. Supported characters: 0-9, *, and #. Up to 100 custom key events are supported per IVR. The configured End Key value should not be included in your custom key settings to prevent recognition failure.
Destination	Select the destination type and target for the custom key event. Supported destinations include: Extension Meeting Voicemail Voicemail Group IVR (Maximum 64 nested IVRs) Ring Group Queues Paging/Intercom Group Fax Custom Prompt Hang-up DISA Dial By Name External Number Callback Announcement SMS (Sends an automated SMS template to the caller) Time Condition Routing
Time Condition	Assign a time condition to each destination entry. The IVR evaluates the time conditions in order and routes the call to the first matching rule. Common options include All Time, Office Time, Out of Office Time, Holiday, and Specific Time. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for the same key, or the (-) icon to remove an existing rule.
Timeout	Configures the destination when the Timeout Repeat Loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (-) icon to remove an existing rule.

Invalid	Configures the destination when the Invalid Repeat Loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (-) icon to remove an existing rule.
End Key	Configures whether the caller can press a designated End Key to complete custom key entry and immediately trigger the destination. Options: Press the "#" key to end Press the "*" key to end Note: Ensure the End Key selected does not conflict with custom key sequences.

Voicemail

Configure Voicemail

If voicemail is enabled for UCM extensions, global voicemail configurations can be managed under **Basic Call Features -> Voicemail -> Voicemail**.



The table below describes the global voicemail configuration parameters:

Option	Description
Max Greeting Time (s)	Configure the maximum duration (in seconds) for voicemail greetings (range: 60-600, default: 60).
Dial "0" for Operator	If enabled, callers pressing 0 during voicemail exit the application to connect to the designated operator destination.
Operator Type	Select the operator destination type (Extension or Ring Group).
Operator Extension	Select the operator extension or ring group called when callers dial 0.
Max Messages Per Folder	Configures the maximum allowed messages per voicemail folder (range: 10-1000, default: 50).

Max Message Length (m)	Select the maximum recording duration for a voicemail message (1, 2, 5, 15, 30 minutes, or Unlimited; default: 15 minutes). Note: Silence and noise duration are excluded from message time.
Min Message Length (s)	Configures the minimum recording length required to save a message (No Minimum, 1, 2, 3, 4, 5 seconds). Messages shorter than this value are discarded. Note: Silence and noise duration are excluded from message length.
Announce Message Caller-ID	If enabled, announces the caller ID of the sender at the start of message playback (Default: No).
Announce Message Duration	If enabled, announces the message duration before playback (Default: No).
Play Envelope	If enabled, plays timestamp and sender information before message playback.
Play Most Recent First	If enabled, plays the newest voicemail messages first.
Allow User Review	If enabled, callers can review and re-record their message before submitting.
Voicemail Remote Access	If enabled, external callers arriving via DID are prompted with two choices: Press 1: Leave a message for the called extension. Press 2: Access the remote voicemail management system (requires extension number and PIN). Note: Applies strictly to inbound DID calls (Default: Disabled).
Forward Voicemail to Peered UCMs	Enables forwarding voicemail messages to remote extensions on peered UCM trunks (Default: Disabled).
Voicemail Password	Sets the default voicemail PIN used when extensions are reset. Numeric digits only (minimum 4 digits). Sequential or repetitive numbers (e.g., 1234, 1111) are rejected.
Audio Encoding Format	Selects the audio encoding codec used for voicemail file storage: GSM: Encodes audio using the GSM codec, producing compressed .WAV (uppercase) files to save disk space. PCM: Encodes audio using uncompressed PCM codec, producing high-quality .wav (lowercase) files (uses significantly more storage space).
Username Prompt	Configure or upload a custom username prompt file.

Resetting an extension resets the Voicemail Password, Send Voicemail to Email, and Keep Voicemail after Emailing values to defaults. Previous custom voicemail prompts and recorded messages will be deleted.

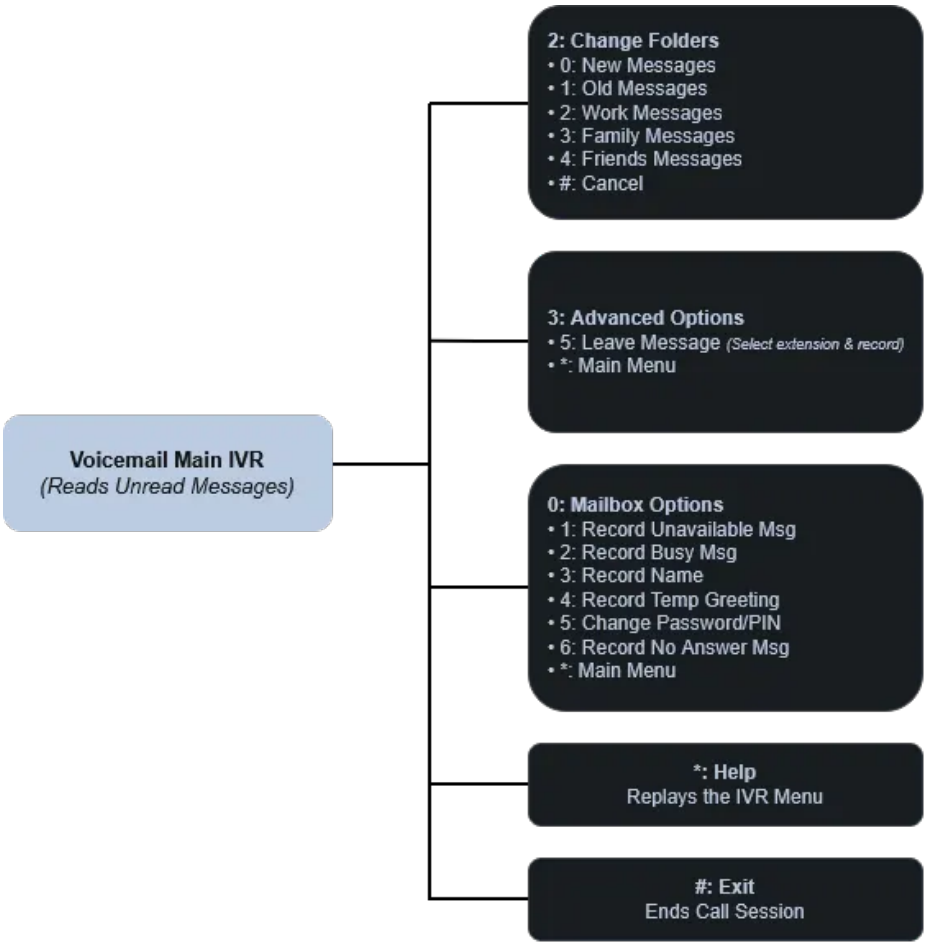
Access Voicemail

When voicemail is enabled for an extension, users can access voicemail using two distinct feature codes:

- **My Voicemail:** Dialing the dedicated feature code for the user's own extension (by default ***97**) directly accesses the user's mailbox without requiring the extension number to be entered. The user only needs to enter their voicemail password/PIN.
- **Voicemail Access:** Dialing the general voicemail feature code (by default ***98**) allows accessing any extension's mailbox. Users can dial ***98** alone and enter the target extension number when prompted, or dial ***98** directly followed by the target extension number (e.g., *981005), followed by the mailbox password/PIN.

After authenticating, both feature codes connect to the same interactive Voicemail IVR menu, which first announces unread voice messages.

The diagram below describes the structure of the Voicemail IVR Menu:



Leaving Voicemail

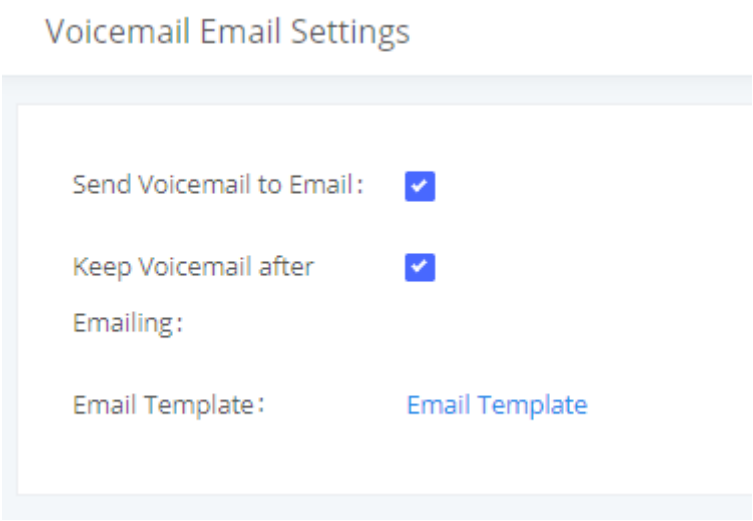
If an extension has voicemail enabled under basic settings "**Extension/Trunk → Extensions → Basic Settings**" and after a ring timeout or user not available, the caller will be automatically redirected to the voicemail in order to leave a message on which case they can press # in order to submit the message.

In case if the caller is calling from an internal extension, they will be directly forwarded to the extension's voicemail box. But if the caller is calling from outside the system and the incoming call is routed by DID to the destination extension, then the caller will be prompted with the choice to either press1 to access voicemail management or press 2 to leave a message for the called extension. This feature could be useful for remote voicemail administration.

Voicemail Email Settings

The UCM630X can be configured to send the voicemail as attachment to Email. Click on "Voicemail Email Settings" button to configure the Email attributes and content.

Send Voicemail to Email	If enabled, voicemail will be sent to the user's email address. Note: SMTP server must be configured to use this option.
Keep Voicemail after Emailing	Enable this option if you want to keep recording files after the Email is sent. The default setting is Enable.
Email Template	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending to the user. The template variables are: t: TAB ${VM_NAME}: Recipient's first name and last name ${VM_DUR}: The duration of the voicemail message ${VM_MAILBOX}: The recipient's extension ${VM_CALLERID}: The caller ID of the person who has left the message ${VM_MSGNUM}: The number of messages in the mailbox ${VM_DATE}: The date and time when the message is left

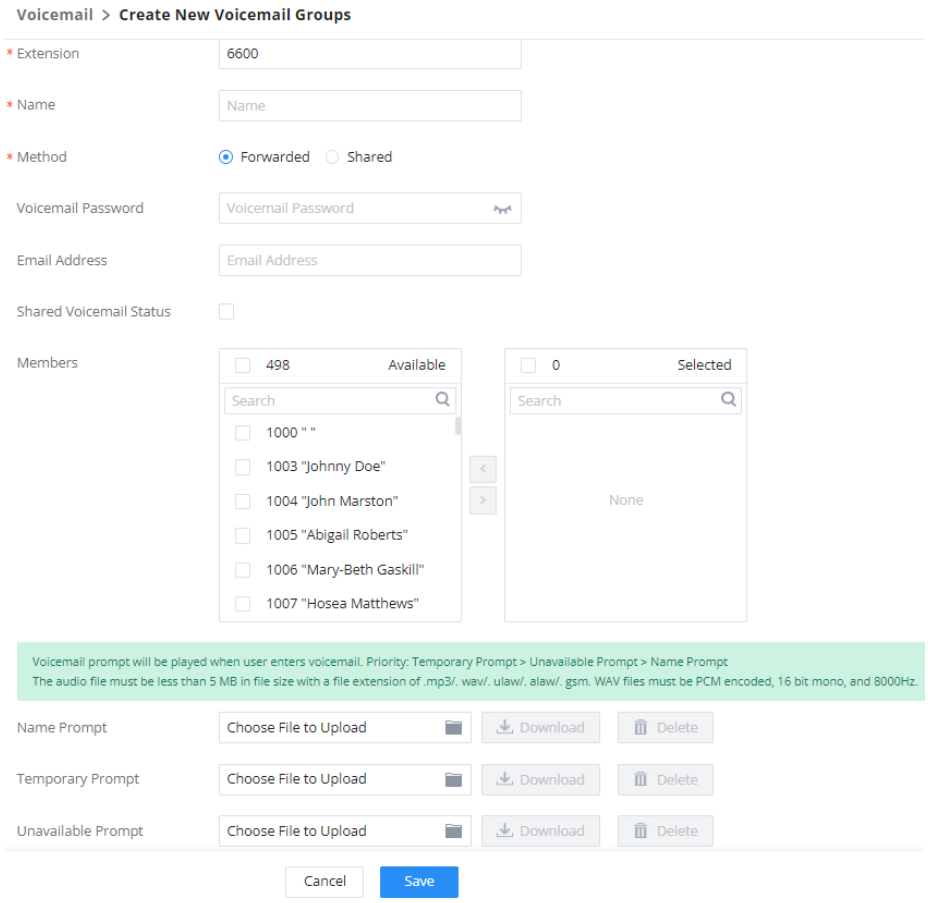


Voicemail Email Settings

Click on "Email Template" button to view the default template as an example.

Configure Voicemail Group

The UCM630X supports voicemail group and all the extensions added in the group will receive the voicemail to the group extension. The voicemail group can be configured under **Basic Call Features** > **Voicemail** > **Voicemail Group**. Click on "Add" to configure the group.



Voicemail Group

Extension	Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members.

Name	Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed.
Method	Select the preference for receiving and managing group voicemail. Forwarded: Voicemail will be stored in the group voicemail box, and each voicemail group member will be forwarded a copy of it. Shared: Voicemail will be stored in the group voicemail box, and voicemail status will be shared among all voicemail group members. If a member deletes a voicemail, it will also be deleted for all members. Likewise, if one member reads a voicemail, it will be considered read for the entire group.
Voicemail Password	Configure the voicemail password for the users to check voicemail messages.
Email Address	Configure the Email address for the voicemail group extension.
Shared Voicemail Status	If enabled, voicemail group status can be monitored via BLF. Green indicates no unread voicemail, and red indicates existing unread voicemail.
Members	Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list.
Greet Prompt	This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Temporary Prompt	This voicemail prompt will be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Unavailable Prompt	This voicemail prompt will be played when user enters voicemail. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.

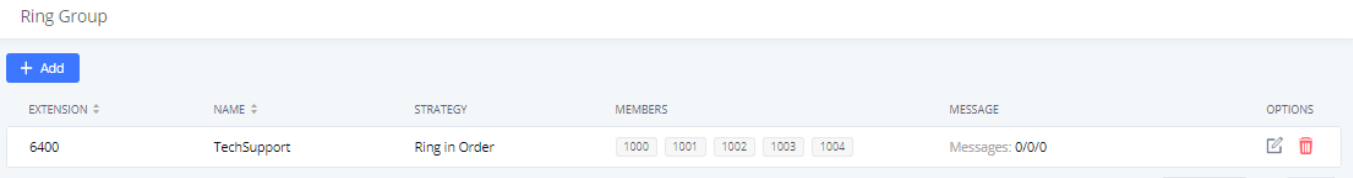
The administrator can add up to 150 extensions to a single voicemail group.

Ring Groups

The UCM630X supports ring group feature with different ring strategies applied to the ring group members. This section describes the ring group configuration on the UCM630X.

Configure Ring Group

Ring group settings can be accessed via **Basic Call Features > Ring Group**.



Ring Group

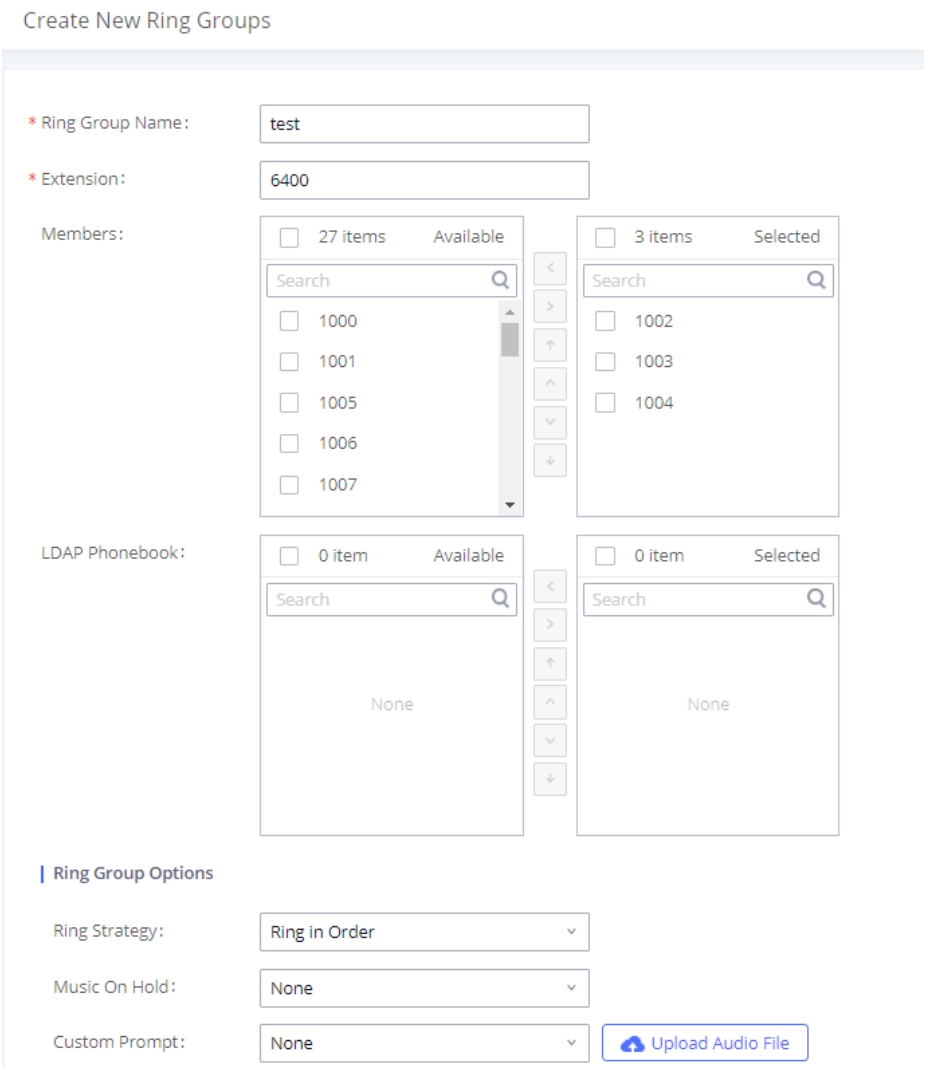
- Click on to add ring group.

- Click on to edit the ring group. The following table shows the ring group configuration parameters.

- Click on to delete the ring group.

Ring Group Name	Configure ring group name to identify the ring group. Letters, digits, _ and - are allowed.
Extension	Configure the ring group extension.
Members	Select available users from the left side to the ring group member list on the right side. Click on ? ? to arrange the order.
LDAP Phonebook	Select available remote users from the left side to the ring group member list on the right side. Click on ? ? to arrange the order. Note: LDAP Sync must be enabled first.
Ring Strategy	Select the ring strategy. The default setting is "Ring in order". Ring Simultaneously: Ring all the members at the same time when there is incoming call to the ring group extension. If any of the member answers the call, it will stop ringing. Ring in Order: Ring the members with the order configured in ring group list. If the first member does not answer the call, it will stop ringing the first member and start ringing the second member.
Music On Hold	Select the "Music On Hold" Class of this Ring Group, "Music On Hold" can be managed from the "Music On Hold" panel on the left.
Custom Prompt	This option is to set a custom prompt for a ring group to announce to caller. Click on 'Prompt', it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings? Voice Prompt? Custom Prompt, where they could record new prompt or upload prompt files.
Ring Timeout on Each Member	Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 60 seconds.Note: The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.
Auto Record	If enabled, calls on this ring group will be automatically recorded. The default setting is No. The recording files can be accessed from WebGUI? CDR? Recording Files.
Endpoint Call Forwarding Support	This allows the UCM to work with endpoint-configured call forwarding settings to redirect calls to ring group. For example, if a member wants to receive calls to the ring group on his mobile phone, he will have to set his endpoint's call forwarding settings to his mobile number. By default, it is disabled.However, this feature has the following limitations: This feature will work only when call forwarding is configured on endpoints, not on the UCM. If the forwarded call goes through an analog trunk, and polarity reversal is disabled, the other ring group members will no longer receive the call after it is forwarded. If the forwarded call goes through a VoIP trunk, and the outbound route for it is PIN-protected and requires authentication, the other ring group members will no longer receive the call after it is forwarded. If the forwarded call hits voicemail, the other ring group members will no longer receive the call.
Replace Display Name	If enabled, the UCM will replace the caller display name with the Ring Group name the caller know whether the call is incoming from a direct extension or a Ring Group.
Skip Busy Agent	If enabled, skip busy agents regardless of call waiting settings.
Enable Destination	If enabled, users could select extension, voicemail, ring group, IVR, call queue, voicemail group as the destination if the call to the ring group has no answer. Secret and Email address are required if voicemail is selected as the destination.
Default Destination	The call would be routed to this destination if no one in this ring group answers the call.Note: Users can now set the voicemail of ring groups as routing destinations and IVR key press event destinations and to do so ring group must have their Default Destination set to Voicemail with Ring Group Extensions.
Voicemail	Whether to enable the voicemail for the ring group or not.
Voicemail Password	Configure the voicemail password (only numbers).

Email Address	Fill in the user's Email address (s), the voice message will be sent to this address (s).
Busy Prompt	This voicemail prompt will be played when the callee is in another call or is in DND mode. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet PromptSound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Greet Prompt	This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Temporary Prompt	This voicemail prompt well be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Unavailable Prompt	This voicemail prompt will only be played when the callee's extension is unregistered. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.

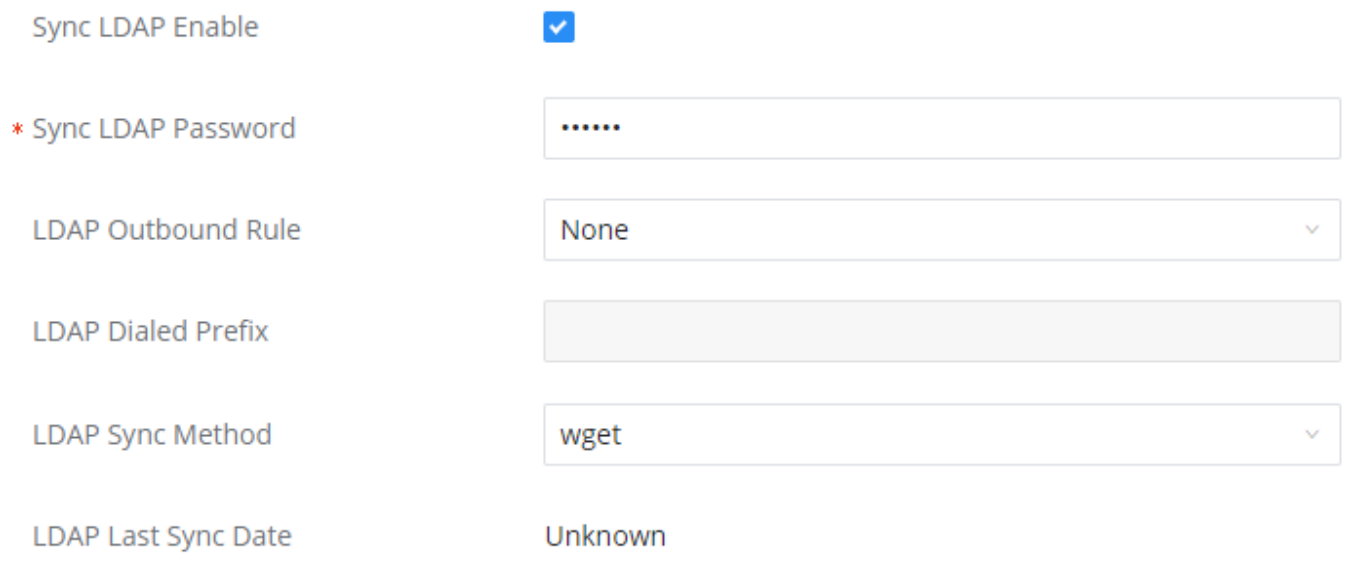


Ring Group Configuration

Remote Extension in Ring Group

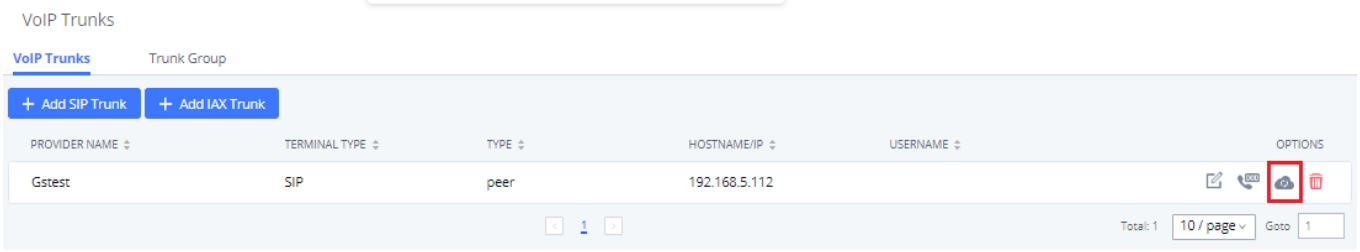
Remote extensions from the peer trunk of a remote UCM630X can be included in the ring group with local extension. An example of Ring Group with peer extensions is presented in the following:

1. Creating SIP Peer Trunk between both UCM630X _A and UCM630X _B. **SIP Trunk** can be found under Web GUI→**Extension/Trunk→VoIP Trunks.** Also, please configure their Inbound/Outbound routes accordingly.
2. Click edit button in the menu , and check if **Sync** LDAP **Enable** is selected, this option will allow UCM630X_A update remote LDAP server automatically from peer UCM630X _B. In addition, **Sync LDAP Password** must match for UCM630X _A and UCM630X _B to sync LDAP contact automatically. Port number can be anything between 0~65535, and use the outbound rule created in step 1 for the **LDAP Outbound Rule** option**.**



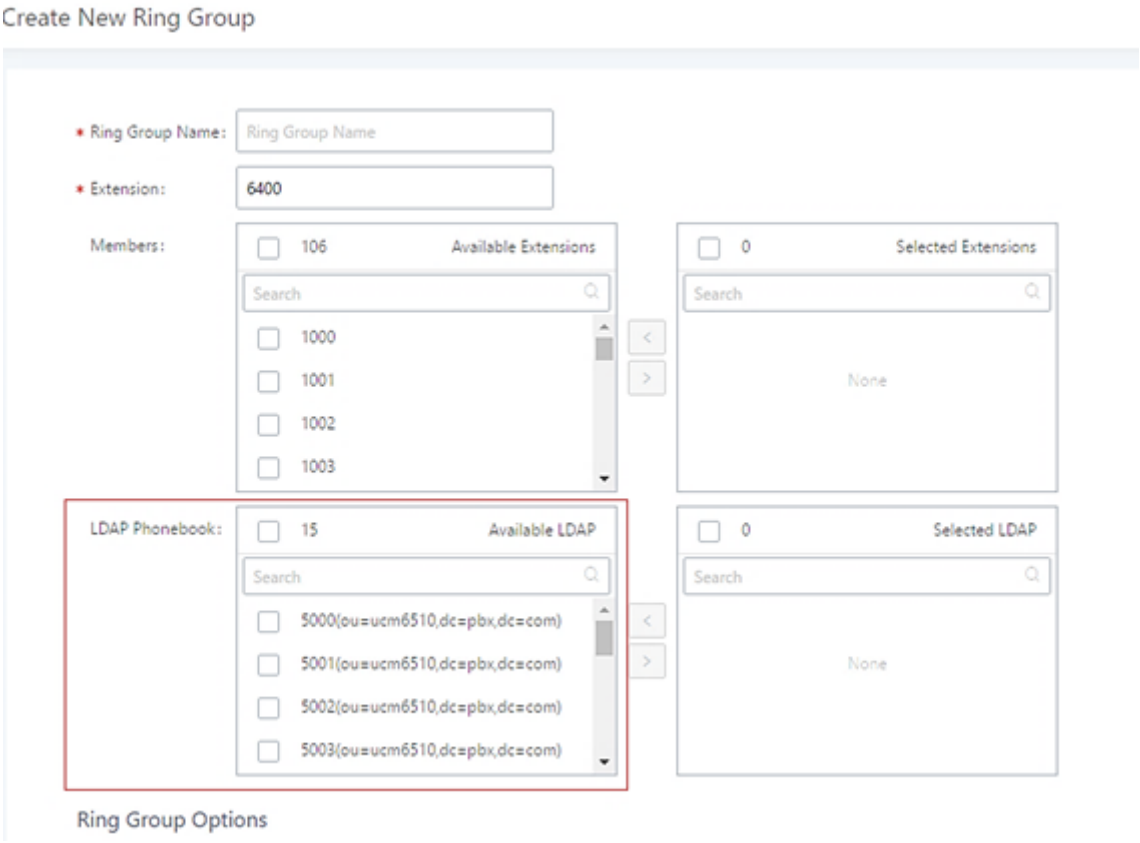
Sync LDAP Server Options

3. In case if LDAP server does not sync automatically, user can manually sync LDAP server. Under **VoIP Trunks** page, click sync button shown in the following figure to manually sync LDAP contacts from peer UCM630X.



Manually Sync LDAP Server

4. Under **Ring Groups** setting page, click "Add". **Ring Groups** can be found under Web GUI **Basic Call Features > Ring Groups**.
5. If LDAP server is synced correctly, **Available LDAP Numbers** box will display available remote extensions that can be included in the current ring group. Please also make sure the extensions in the peer UCM630X can be included into that UCM630X's LDAP contact.



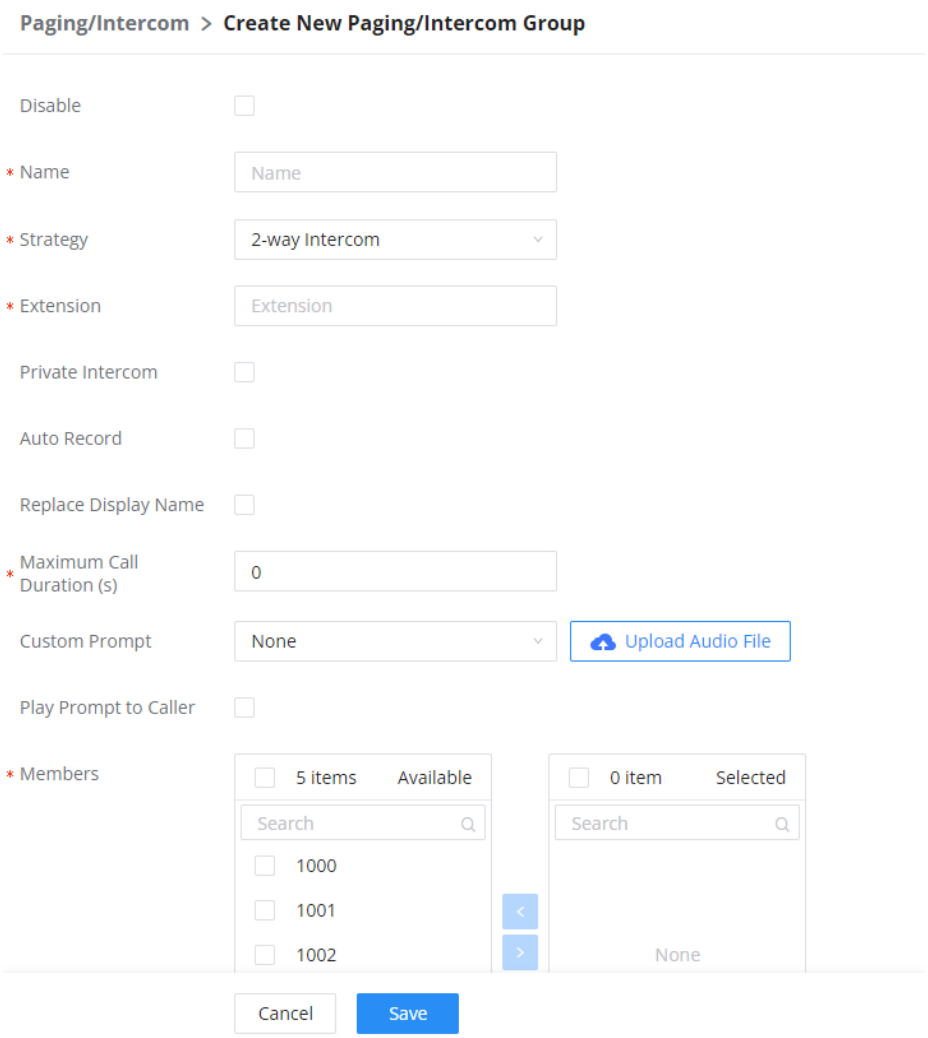
Ring Group Remote Extension

Paging/Intercom

Paging and Intercom Group can be used to make an announcement over the speaker on a group of phones. Targeted phones will answer immediately using speaker. The UCM630X paging and intercom can be used via feature code to a single extension or a paging/intercom group. This section describes the configuration of paging/intercom group under Web GUI **Basic Call Features > Paging/Intercom**.

Paging/Intercom Groups

2-way Intercom



2-way Intercom

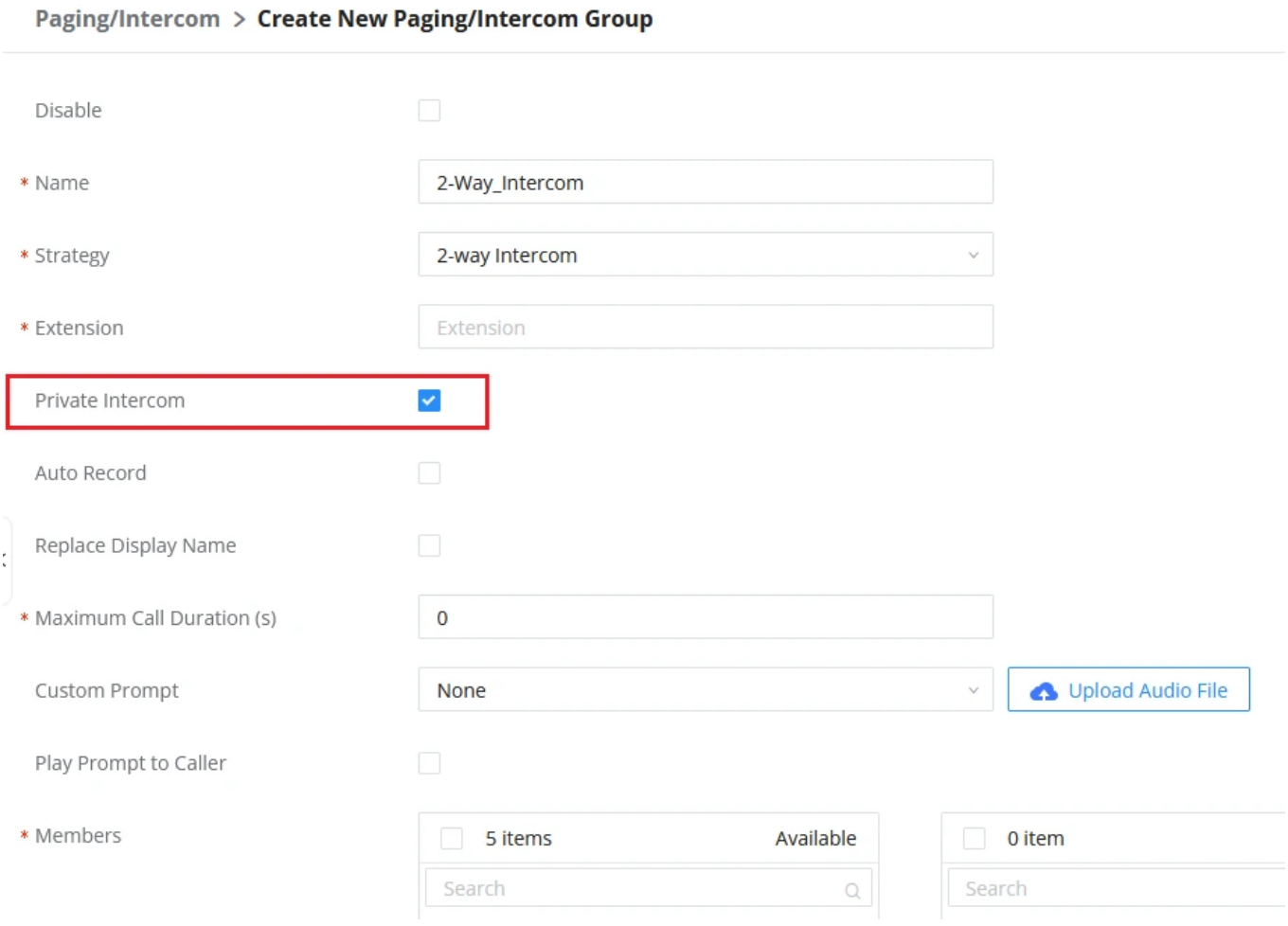
Parameter	Description
Name	Configure intercom group name.
Strategy	Select "2-way Intercom".
Extension	Configure the intercom group extension.
Private Intercom	If enabled, members can only hear the voice of the initiator and cannot hear the voice of other members. The initiator can hear the voice of all members.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the PBX will replace the caller display name with Intercom name.
First Answer Termination	Enabling this option will result in halting other phones from ringing once the intercom is answered.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Local Members	?Selected members will receive paging/intercom calls to this paging/intercom group.
LDAP Members	Select a number from the LDAP phonebook. If LDAP contacts were synchronized through the SIP trunk, the IPPBX will use that same trunk to send the call. Other trunks will not be used.

Paging/Intercom Allowlist	Select the extensions which are allowed to initiate the paging/intercom.Selected: Only selected extension will be allowed to initiate paging/intercom.All: Allow all extensions and configured services to initiate paging/intercom.
Custom Prompt	This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on 'Upload Audio File', it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings > Voice Prompt > Custom Prompt, where they could record new prompt or upload prompt files.
Play Prompt to Caller	Play the prompt to the caller.

The number of members of the intercom group is limited at 50 members.

Private Intercom

Private intercom allows the user to initiate an intercom to many endpoints. Whichever endpoint microphone has detected sound input first, only the intercom initiator and the responder will be able to hear each other. Once the first responder has finished talking, the second responder can start talking. To configure private intercom, the user can follow the steps mentioned above in 2-way intercom and while creating the intercom, the user may tick the option "Private Intercom" as indicated in the screenshot below.



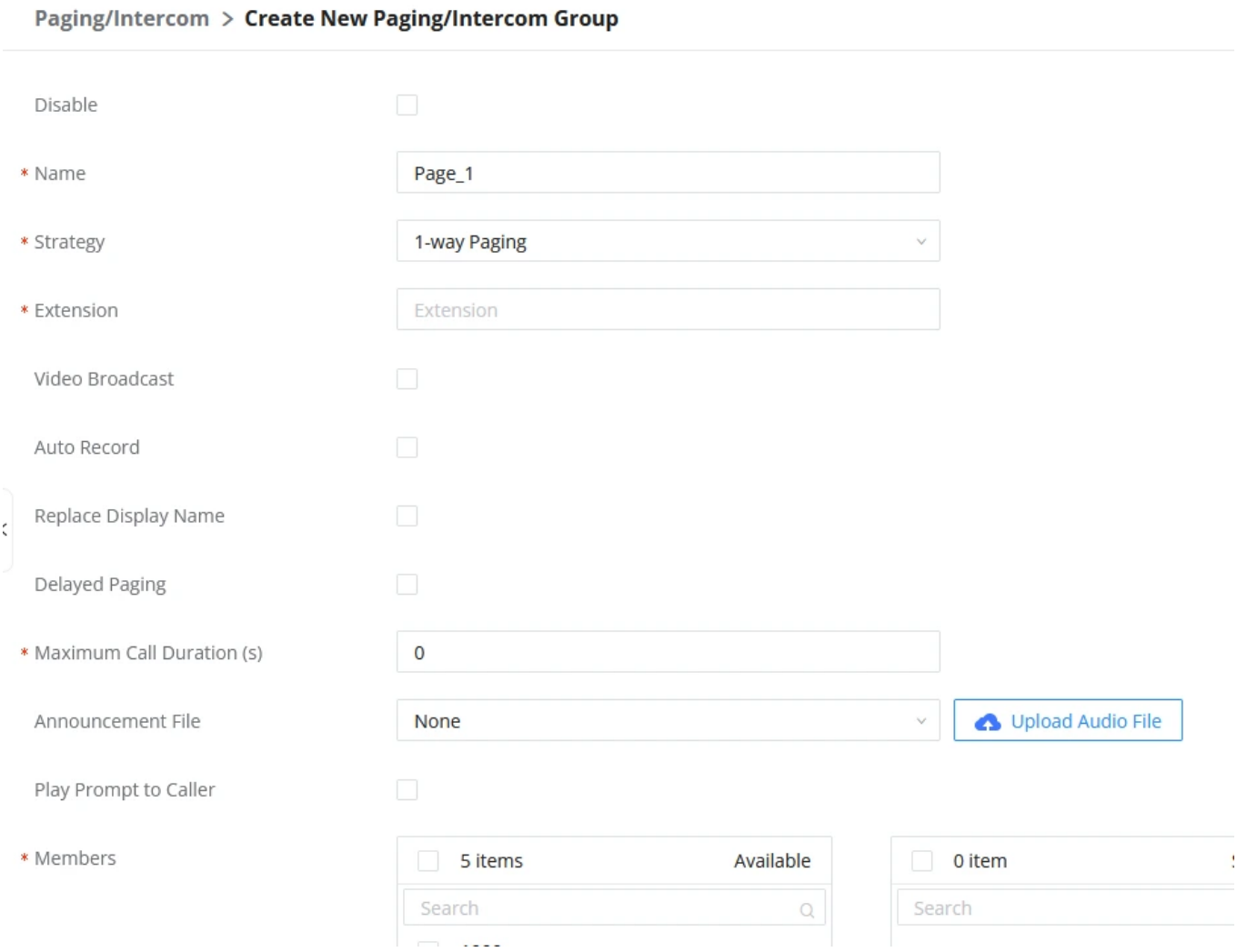
Private Intercom

Parameter	Configuration
Name	Enter a name for the intercom
Strategy	Choose "Private Intercom".
Extension	Configure the intercom group extension.

Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
Maximum Call Duration (s)	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Custom Prompt	This option sets a custom prompt to be used as an announcement to the person receiving a paging/intercom call. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add additional record.
Members	Selected members will receive paging/intercom calls to this paging/intercom group.
Paging/Intercom Whitelist	Only selected extensions will be able to use this paging /intercom group. If none is selected, all extensions will be able to use this paging/intercom group.

1-way Paging

1-way paging feature allows to send paging to multiple endpoints. The administrator can configure to have the paging message played upon answering on the IP phone's end, or to have the message played through the speaker as soon as the page is sent.



1-way Paging

Parameter	Description

Name	Configure paging/intercom group name.
Strategy	Select "1-way Paging".
Extension	Configure the paging/intercom group extension.
Video Broadcast	If checked, video paging will be supported. If the caller sends a video page, the paging group members will be able to receive and view the video.
Auto Record	Enable this option to record in WAV format (audio) and MKV format (video).
Replace Display Name	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
First Answer Termination	Enabling this option will result in halting other phones from ringing once the paging is answered.
Delayed Paging	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the prerecorded message will be played, and the call will end after it is finished playing.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Local Members	Selected members will receive paging/intercom calls to this paging/intercom group.
LDAP Members	Select a number from the LDAP phonebook. The LDAP number can use only the main trunk and specified trunks to make outbound calls. Other trunks cannot be used.
Announcement File	Configures an audio/video file to play to the paging members. This can be used to play preconfigured audio/video at the beginning of paging calls or to simply notify members that it is a paging/intercom call.
Play Prompt to Caller	Play the prompt to the caller.
Paging/Intercom Whitelist	Select which extensions are allowed to use the paging/intercom feature for this paging group.

The number of members of the paging group is limited at 50 members.

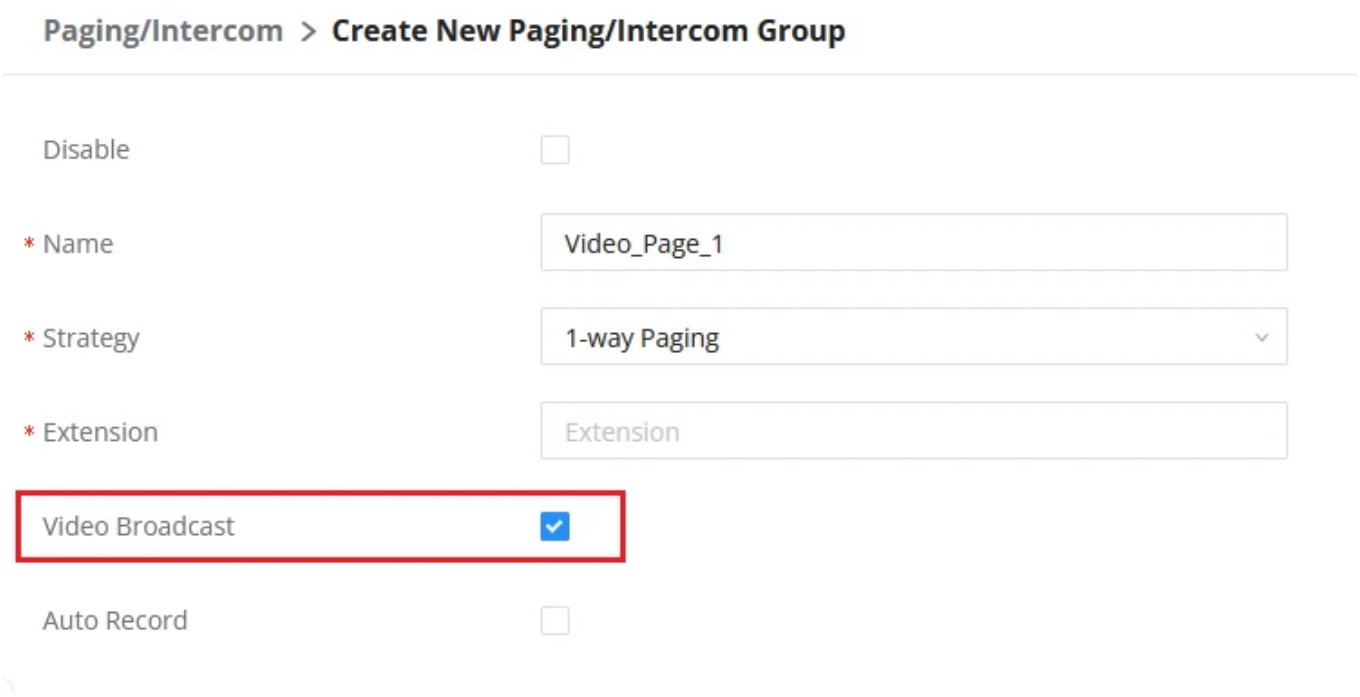
In case the user wants to broadcast a video, the following requirements should be respected.

- H.264 video encoding
- .mkv or .tar/.tgz/tar.gz format
- MKV files must be 30 MB file or less
- Compressed files (.tar/.tgz/tar.gz) must be 50 MB or less.
- File name can only contain alphanumeric characters, hyphens (-) and period (.)

If Auto Record is enabled, recorded video pages will be saved in MKV file format.Saved recordings can be found in the CDR→Recordings→Video Recordings page.

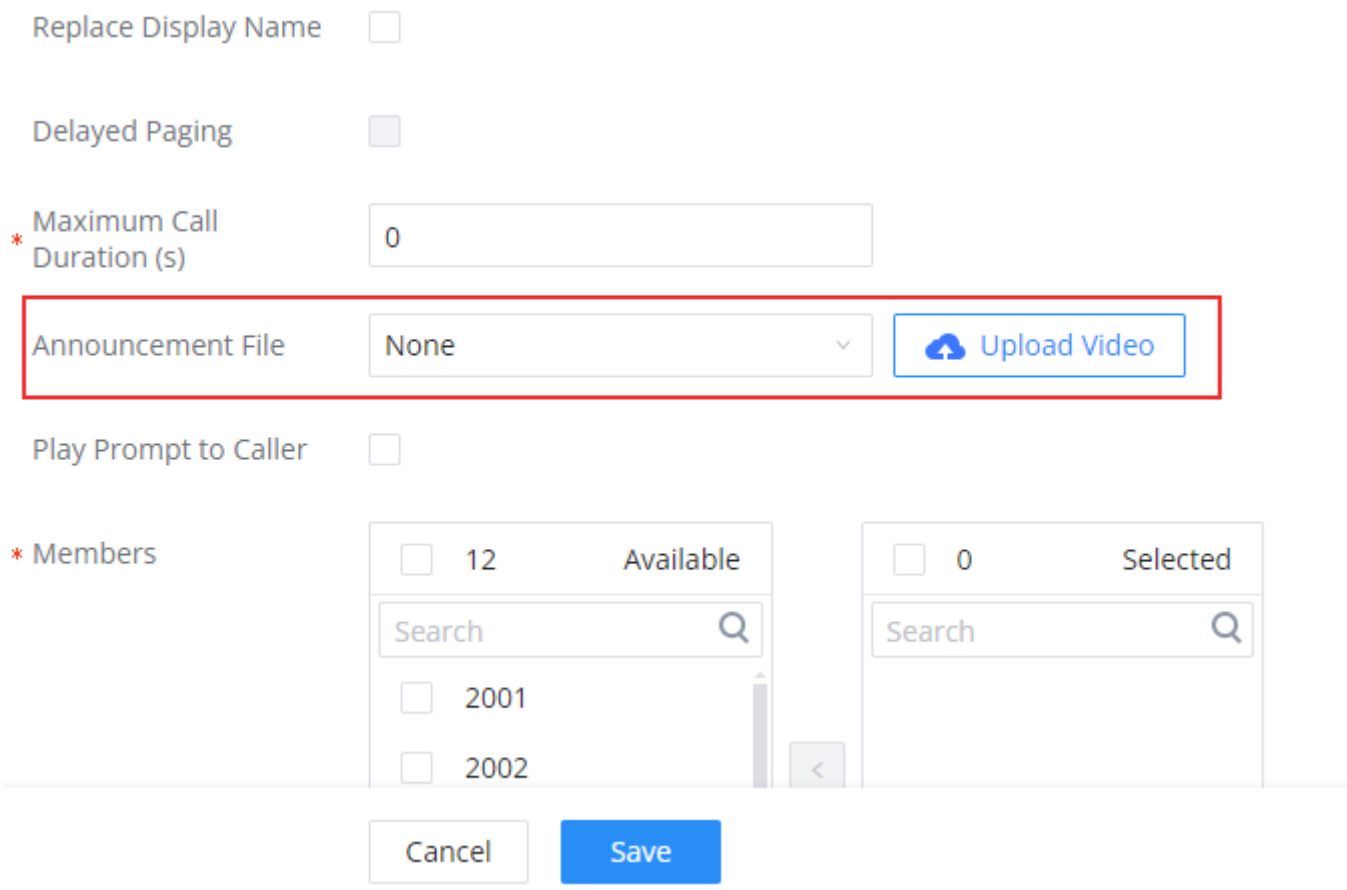
Video Broadcast

Using this feature, the user can send a video to the SIP endpoints which support streaming video to notify the users of the beginning of a paging. To configure Video Broadcast before a paging, the user can create a 1-way paging following the steps mentioned in the previous section. Then the user can enable "Video Broadcast" in the settings.

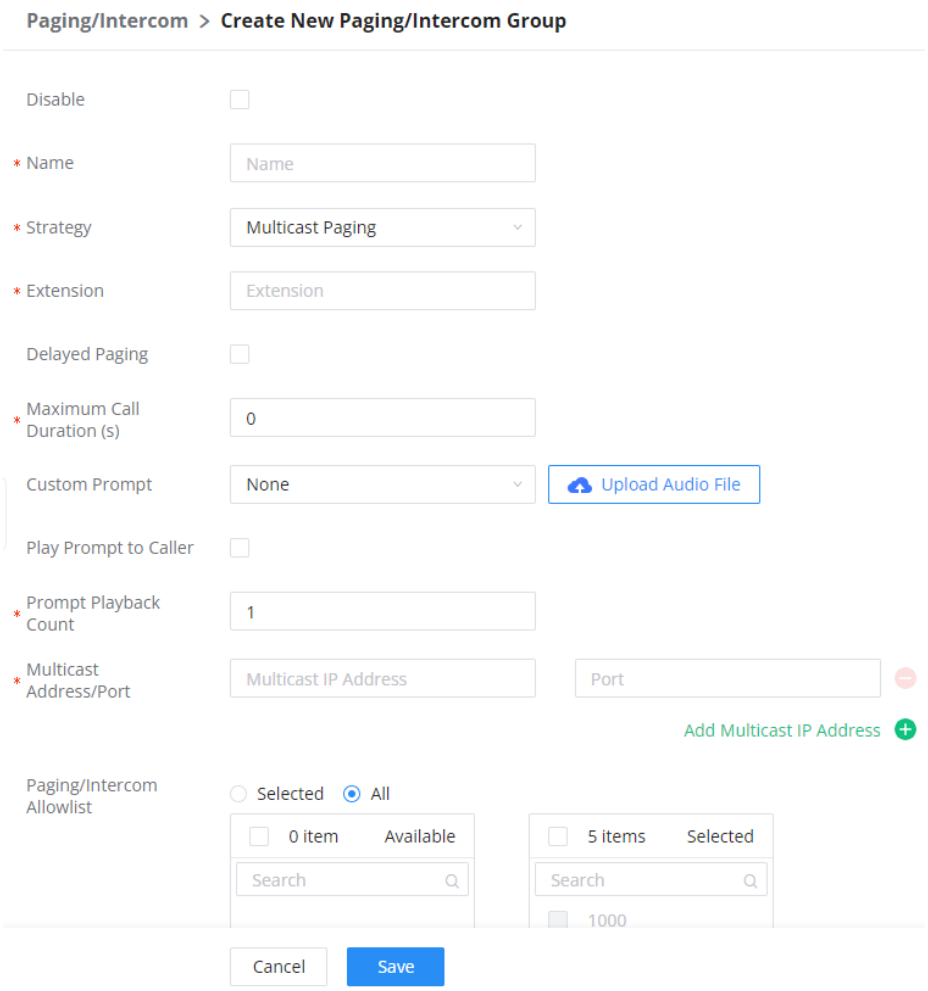


Video Broadcast

The user can upload the video in the "Announcement File" section as shown in the screenshot below.



Multicast Paging



Multicast Paging

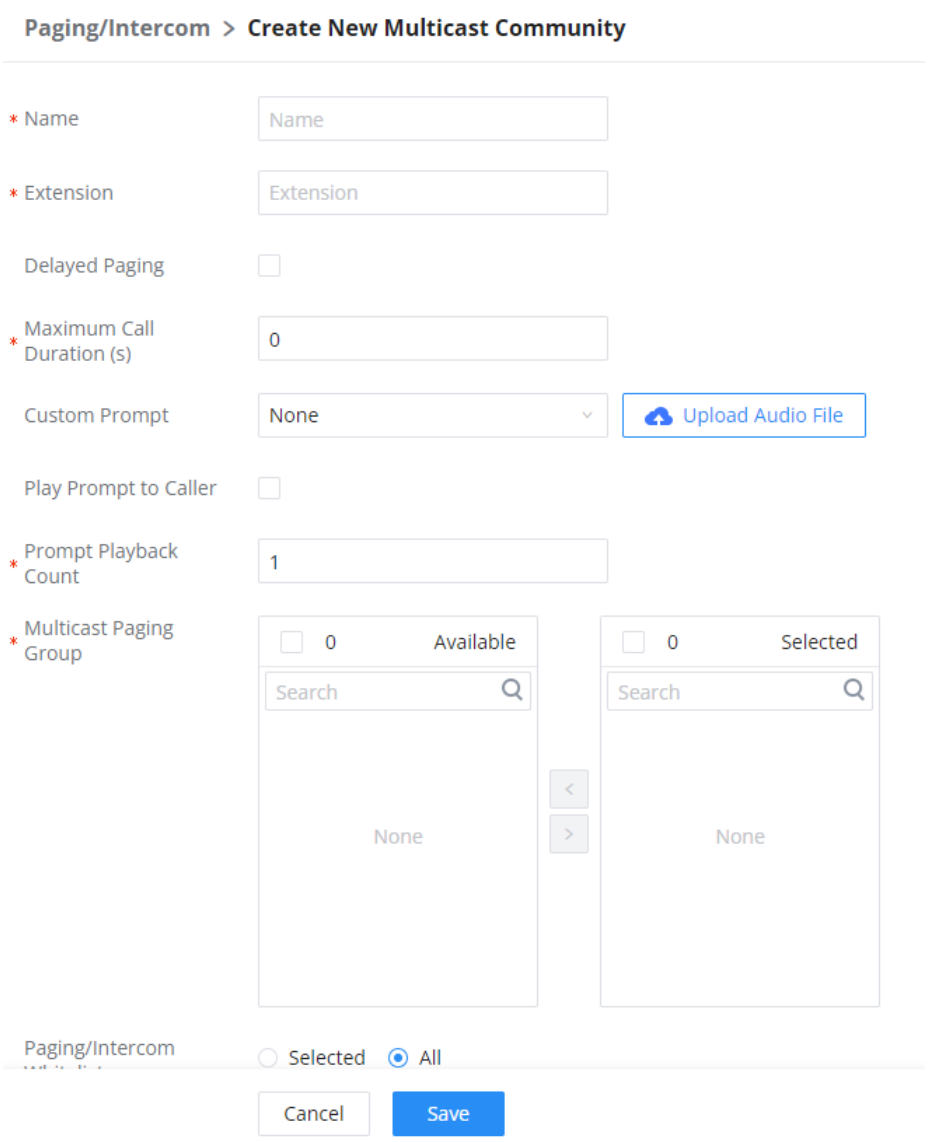
Parameter	Description
Name	Configure paging/intercom group name.
Strategy	Select "Multicast Paging".
Extension	Configure the paging/intercom group extension.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Multicast IP Address/Port	The allowed multicast IP address range is 224.0.1.0 - 238.255.255.255.Note: You can add up to 30 multicast addresses.
Paging/Intercom Allowlist	Select the extension which can initiate this paging. If none is selected, all extensions will be able to use this paging/intercom group.
Opening Prompt	Select the opening prompt for the paging.
Custom Prompt	This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on 'Prompt', it will direct the users to upload the customized voice prompts.Note: Users can also refer to the page PBX Settings?Voice Prompt?Custom Prompt, where they could record new prompt or upload prompt files.
Play Prompt to Caller	Play the prompt to the caller.
Prompt Playback Count	Sets the number of times the prompt is played during the page/intercom. To ensure the prompt is played the specified number of times, please set an appropriate max call duration.

Background Sound	Enable background sound.
Background Sound Source	If an extension is selected as the audio source, the audio from that extension will be automatically used as the background sound when the paging/intercom is initiated.Custom Background SoundExtension Shared Audio
Custom Background Sound	Choose or upload a custom background sound.
Announcement Command	While background sound is playing, callers can start and end an announcement by pressing *1.
Start/End Announcement Cue	If enabled, after pressing the Announcement command (*1) to start and end the announcement, the system will play this prompt. Otherwise, only a beep will play.
Mute Background Sound	If enabled, the ongoing background sound will be muted during the announcement.
Multicast Audio Format	Choose the format/codec of the multicast audio.
Delayed Paging	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the recorded message will be played, and the call will end after it is finished playing.
Delay (s)	Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds.

Multicast Paging Configuration Parameters

Multicast Community

Multicast community allows creating an extension, which when dialed, can send a preconfigured prompt as a multicast paging to a group of extensions. The user should create first a **Paging/Intercom Group** with **Multicast Paging** as the **Strategy** selected. Please see previous section for more information.



Multicast Community Parameters

Name	Enter the name of the multicast community.
Extension	Configure the extension number for the paging/intercom group. When this number is dialed, the paging/intercom will be initiated.
Delayed Paging	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the precorded message will be played, and the call will end after it is finished playing. Delay (s): Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds.
Maximum Call Duration (s)	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).Note: Please note that the call duration that can be configured can be within the range 0 - 86400.
Custom Prompt	Choose the custom prompt to play for the callees at the beginning of the paging. The user can also directly upload a prompt file directly on this page. Note: When uploading the custom prompt file, please make sure it respects the following requirements: The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters -_

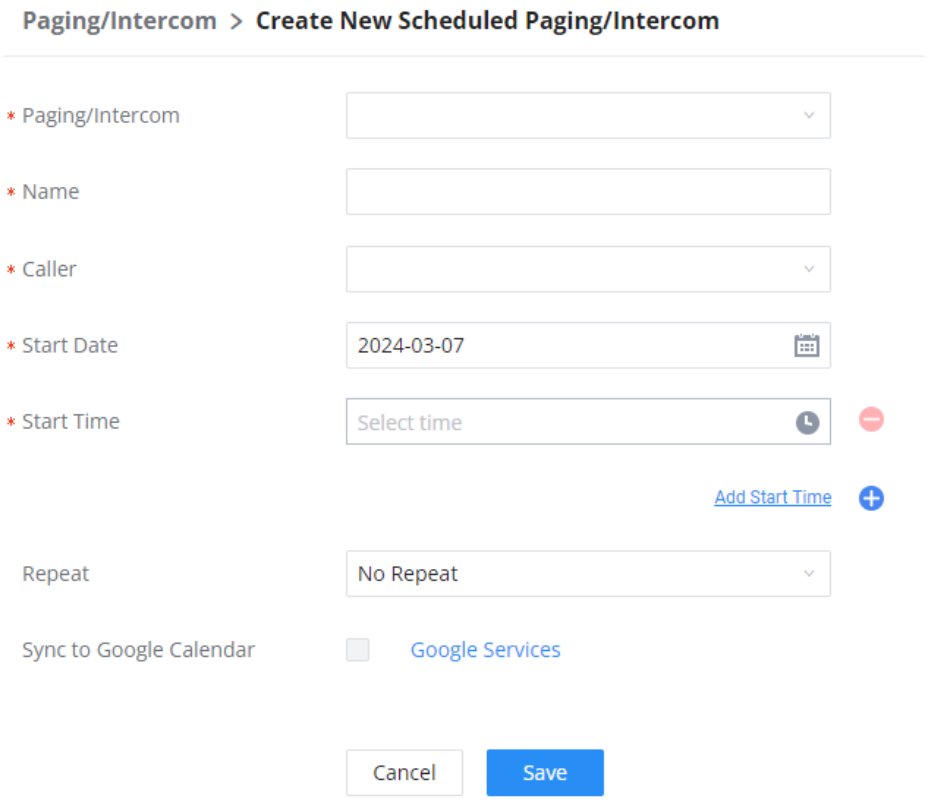
Play Prompt to Caller	When this option is enabled, the prompt will be played back on the caller's phone.
Prompt Playback Count	Sets the number of times the prompt is played during the page/intercom. To ensure the prompt is played the specified number of times, please set an appropriate max call duration.Note: The minimum number of playcounts which can be configured is 1 and the maximum is 10.
Multicast Paging Group	Configures multicast paging groups within a community. When dialing the extension number of the community, users may simultaneously initiate paging to linked multicast paging groups.
Paging/Intercom Whitelist	Selected: Only selected extension will be allowed to initiate paging/intercom. All: Allow all extensions and configured services to initiate paging/intercom.

Scheduled Paging/Intercom

Scheduled paging/intercom feature allows the users to program a paging or an intercom call to be triggers at a certain time and date. The paging/intercom can be scheduled to be triggered periodically, or it can be scheduled to be triggered once.

Pending Paging/Intercom

In this page, the user can create scheduled paging/intercom to be played automatically when the time scheduled arrives.

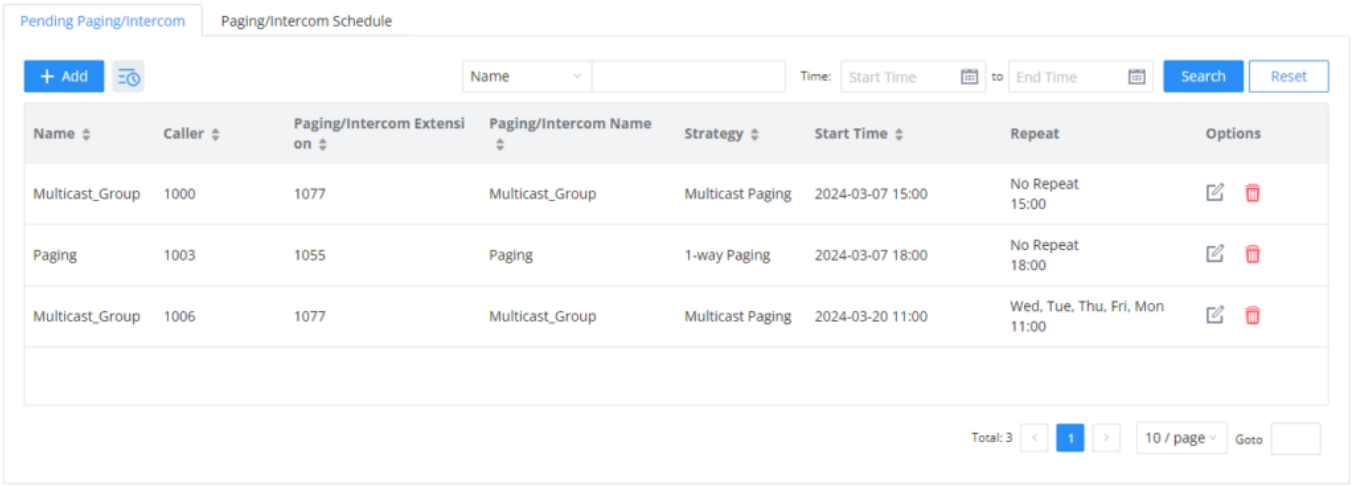


Create New Scheduled Paging/Intercom

Paging/Intercom	Select existing paging/intercom groups and multicast communities.
Name	Enter the name of the scheduled Intercom/Paging.
Caller	Once a caller is selected, and the specified start time is reached, the system will contact the caller. If this call is rejected, the page/intercom will be cancelled. If caller is set to None, the system will call all group members and play the configured prompt.
Start Date	Select the date of the start of the paging/intercom.

Start Time	Select the start time of the paging/intercom.
Repeat	Select the repeat interval of the paging/intercom. No Repeat: The intercom/paging will play once on the scheduled date and time. Everyday: The intercom/paging will play daily starting from the scheduled day and on the time scheduled every day. Weekly: The intercom/paging will play weekly on the selected day(s) of the week. Monthly: The intercom/paging will play monthly on the selected date of the month.
Include Holidays	When Every day, Weekly, or Monthly is selected. This option will appear. If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.
Sync to Google Calendar	This feature cannot be used if Google Services have not been authorized. Please resolve this in the Integrations > Google Services page.

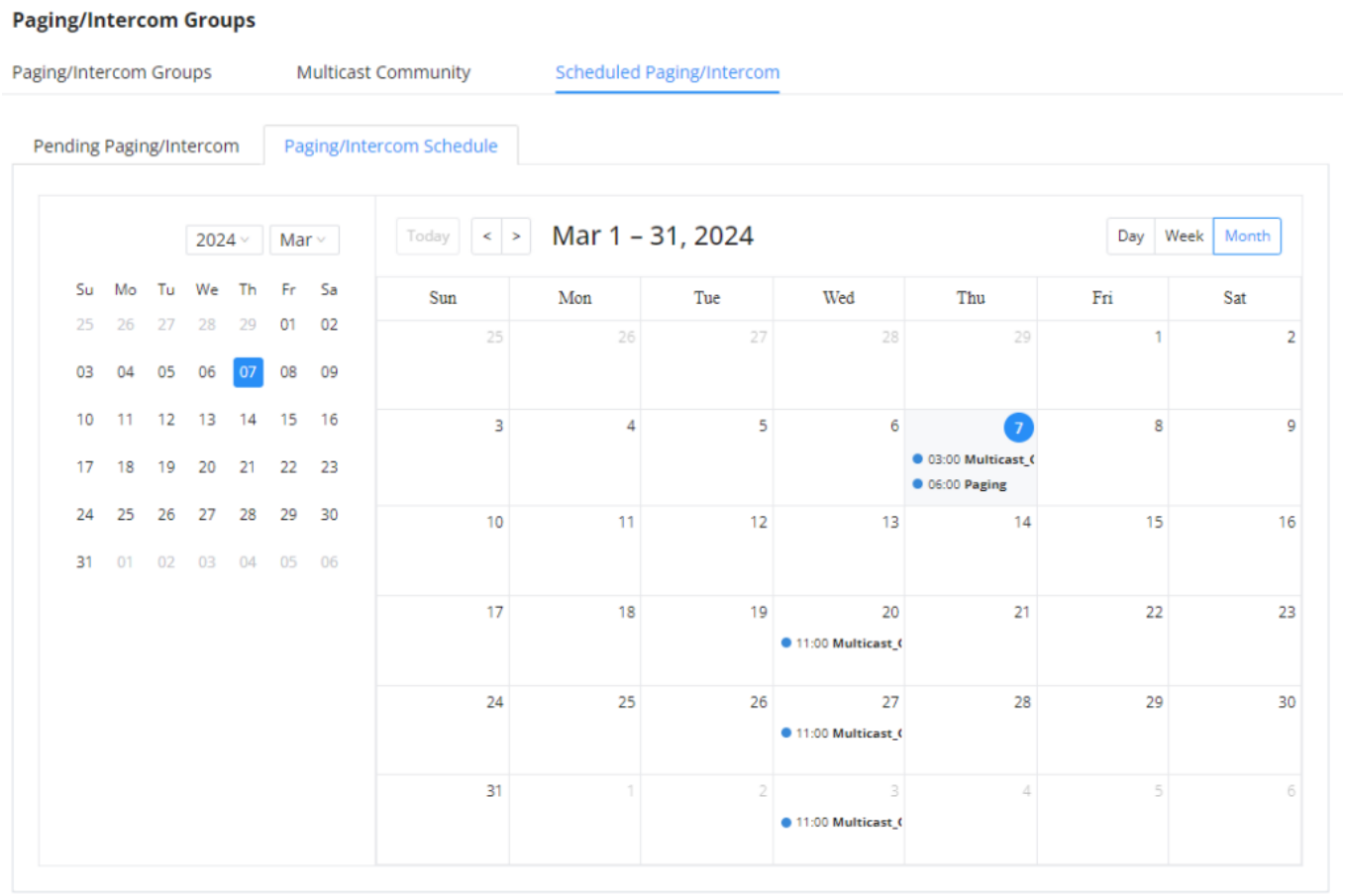
Once the paging and intercom has been created, it can be viewed on the same page.



Pending Paging/Intercom

Paging/Intercom Schedule

This section displays the schedule of the paging/intercom which have been scheduled. The user can choose to display per day, week, or per month.



Scheduled Paging/Intercom

Call Queue

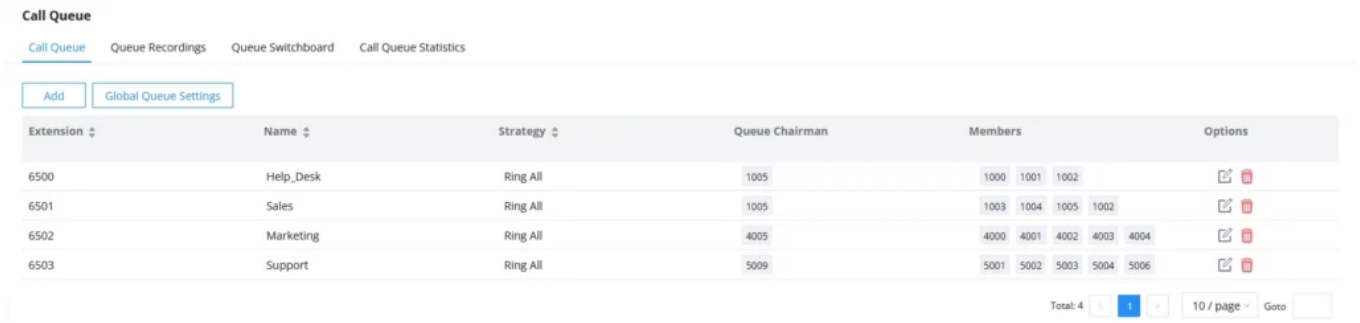
The UCM6300 series Call Queue system allows organizations to handle inbound call volumes exceeding available agent capacity. Incoming calls are held in queue and distributed according to configured strategies. Call Queue management features are located under Web GUI **Basic Call Features -> Call Queue**.

The Call Queue module consists of five main tabs:

- **Call Queue:** Add, edit, and manage call queue instances and global queue settings.
- **Queue Board:** Wallboard interface displaying real-time queue metrics, performance graphs, and agent availability.
- **Queue Operation Panel:** Interactive monitoring panel for real-time call control, waiting list positions, and dynamic agent status management.
- **Call Queue Statistics:** Comprehensive reporting tool for analyzing agent performance, SLA compliance, and call distribution logs.
- **Queue Recordings:** Storage and playback interface for queue call recordings and AI transcriptions.

Call Queue Configuration

Basic queue management can be accessed under **Basic Call Features -> Call Queue -> Call Queue**.



Call Queue Main Tab

- Click **Add** to create a new call queue.
- Click the pencil **Edit** icon under Options to edit queue settings.
- Click the trash **Delete** icon under Options to delete a call queue.

The call queue configuration parameters are listed in the table below.

Parameter	Description
Basic Settings	
General	
Extension	Configure the call queue extension number.
Name	Configure the call queue name to identify the call queue.
Proficiency Routing	If enabled, incoming calls will be routed to the agents with the highest available proficiency level (lower number = higher proficiency). If multiple agents have the same level, the Ring Strategy for Same Proficiency Level will be used to route calls among those agents. Please make sure to assign proficiency levels to the agents under the Agents tab. Note: This option applies to both static and dynamic agents.
Strategy	Select the strategy for the call queue: Ring All: Ring all available Agents simultaneously until one answers. Linear: Ring agents in the specified order. Least Recent: Ring the agent who has been called the least recently. Fewest Calls: Ring the agent with the fewest completed calls. Random: Ring a random agent. Round Robin: Ring the agents in Round Robin scheduling with memory. The default setting is "Ring All".
Ring Strategy for Same Proficiency Level	Select the strategy for the call queue: Ring All: Ring all available Agents simultaneously until one answers. Linear: Ring agents in the specified order. Least Recent: Ring the agent who has been called the least recently. Fewest Calls: Ring the agent with the fewest completed calls. Random: Ring a random agent. Round Robin: Ring the agents in Round Robin scheduling with memory. The default setting is "Ring All".
Music On Hold	Select the Music On Hold class for the call queue. Note: Music On Hold classes can be managed from Web GUI > PBX Settings > Music On Hold.
Max Queue Length	Configure the maximum number of calls to be queued at once. This number does not include calls connected with agents, only calls still in queue. When exceeded, callers hear a busy tone and are forwarded to the configured failover destination. Default is 0 (unlimited).
Agent Rest Time (s)	Configure the amount of time in seconds after ending a call where the agent will not receive additional calls. Default is 10 seconds.
Retry Time (s)	Configure the number of seconds to wait before ringing the next agent. Minimum is 1, default is 5 seconds.
Agent Ring Time	Configure the number of seconds to ring an agent. Minimum is 5, default is 30 seconds.
Auto Record	If enabled, calls on the queue will be automatically recorded. Choose to record internal calls, external calls, or all calls. Default is disabled.

Prompt Language	Choose the language of the prompt played to callers. Selecting "default" uses the language defined under PBX Settings > Voice Prompt > Language Settings.
Welcome Prompt	
Enable	Enable the welcome prompt.
Custom Prompt	Choose the initial tone that plays when the user dials the queue number. Note: Custom prompts can be uploaded directly in .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, or .ulaw formats.
Play Full Welcome Prompt	If enabled, queue agents will not be rung until after the welcome prompt finishes playing. Otherwise, agents are rung while the prompt plays.
Satisfaction Survey Prompt	
Custom Prompt	After an agent hangs up, a prompt plays asking the caller to rate satisfaction on a scale of 1 to 5. Survey results can be reviewed under Call Queue Statistics > Overview > Agent Satisfaction Statistics / Queue Satisfaction Statistics.
Max Wait Time	
Max Wait Time	Configures the amount of time (in seconds) a caller is kept in queue before automatic routing to the Max Wait Time Destination. Default is 60 seconds.
Destination	The destination where calls are routed if no agent answers before max wait time expires.
Transfer Call Based on Time Conditions	
Enable	Toggles time-based routing rules for holidays and non-working hours.
Destination During Holidays	Set the destination type and target destination during official holidays.
Destination During Non-working Hours	Set the destination type and target destination outside defined office time.
Priority Destination	Select whether holiday routing or non-working hours routing takes priority when overlapping.
Play Holiday Prompt During Holiday	Toggles playing the designated holiday voice prompt before transfer. The holiday prompt can be configured in Time Settings -> Holiday.
Reset Agent Call Counter	
Enable	Specifies the frequency at which the agent call counter is reset. Affects ring strategy counters and switchboard data.
Repeat	Set repeat frequency to One-time, Daily, Weekly, or Monthly.
Date/Time	Set the reset date and time.
Destination Prompt Cycle	
Enable	If enabled, callers hear a custom prompt at set intervals while waiting. Pressing "1" routes them immediately to a predefined failover destination.
Destination Prompt Cycle	Configure the voice prompt cycle interval (in seconds).
Custom Prompt	Select or upload the voice prompt file played during the cycle.
Destination	Select the failover destination when callers press "1".
Advanced Settings	
Virtual Queue	
Enable Virtual Queue	If enabled, activates a virtual queue allowing users to request an automated callback while retaining their position in line.

Virtual Queue Mode	Select the triggering mode for virtual queue: DTMF mode (Press 2): Callers can manually request a virtual queue callback at any time while waiting in line by pressing key 2 on their telephone keypad. The system will then play a prompt asking the caller to manually enter their preferred callback number. Timeout mode: The system automatically offers the virtual queue callback once the caller's wait time reaches the threshold configured in Virtual Queue Period (s). Callers will hear a prompt allowing them to choose a callback number, or if Auto-fill Callback Number is enabled, the field automatically populates using their detected Caller ID.The default mode is Timeout mode.
Virtual Queue Period (s)	The amount of time in seconds that must pass before virtual queue is offered in Timeout or Auto mode.
Auto-fill Callback Number	When enabled, automatically populates the callback field with the caller's Caller ID. Note: This option can only be enabled when Virtual Queue Mode is set strictly to Timeout mode.
Virtual Queue Outbound Prefix	System adds this prefix to dialed numbers when performing virtual queue callbacks.
Enable Virtual Queue Position Announcement	Informs waiting callers of their exact position in line.
Enable Virtual Queue Wait Time Announcement	Periodically announces estimated wait times to callers.
Enable Virtual Queue Custom Announcement	Enables to periodically play the custom prompt announcement to callers that enter the virtual queue.
Enable Virtual Queue Callback Timeout	Sets a maximum time limit for agents to answer a virtual queue callback.
Write Timeout	The amount of time in seconds agents have to answer a callback.
Virtual Queue Welcome Prompt	Upload the welcome prompt file for the virtual queue.
Queue Announcement	
Enable Position Announcement	Inform callers waiting in queue of their line position.
Enable Wait Time Announcement	Periodically announce estimated wait times (announced if greater than one minute).
Announcement Interval	Configure announcement frequency (20 to 600 seconds, default 20).
Agent ID Announcement	Plays the agent ID prompt to the caller upon connection.
Premium Code	Callers can enter a premium code and # to increase queue priority.
Premium Code Prompt	Shares the announcement cycle with position announcements.
Custom Announcement	
Custom Prompt	Periodically play custom audio announcements to queued callers.
Announcement Interval (s)	Interval between custom announcements (20 to 600 seconds, default 60).
Empty Queue	
Leave When Empty	Configure whether callers disconnect if no agents remain in queue (Yes, No, or Strict). Default is Strict.
Dial in Empty Queue	Configure whether callers can dial into an empty queue (Yes, No, or Strict). Default is No.
Failover Destination	Choose failover destination (Play Sound, Extension, Voicemail, Queue, Ring Group, Voicemail Group, IVR, External Number) when queue is empty or unstaffed.
CTI	
Allow Static Agent Login/Logout	Enabling static agent login restricts dynamic agent access.
Queue Chairman	Assign extensions permitted to operate and monitor the queue via Web UI.
Priority Queue	

Enable Priority Queue	Activates weighted call routing for agents who belong to multiple queues simultaneously. When enabled, the UCM prioritizes calls from queues with a higher overall weight.
Weight	Configures the base priority level for the call queue (Range: 1 to 99). Higher weight values take precedence when routing calls to multi-queue agents.
Enable Accelerated Weighting	Prevents excessive waiting times for callers in lower-weight queues. When enabled, the queue weight automatically increments by 1 after callers wait for a specified duration.
Accelerated Weighting Duration (seconds)	Configures the waiting time interval in seconds (Range: 10 to 1800) required for the queue's overall weight to increase by 1.
Service Level Agreement (SLA)	
Enable SLA	Toggles SLA measurement to track call response times against threshold goals.
SLA Time (s)	Maximum target time in seconds for agents to answer calls (1 to 180s, default 20).
SLA Alert Email Notification	Enable SLA breach email notifications.
Alert Threshold (%)	Minimum acceptable SLA answer percentage before triggering alerts (default 80%).
SLA Alert Interval (m)	Minimum time between breach email alerts (1 to 120 minutes, default 120).
SLA Alert Email Template	Select email template used for SLA breach notifications.
Alert Email Recipients	Designate email recipients for SLA breach alerts.
Other Settings	
Report Hold Time	If enabled, reports caller hold duration to the agent upon call connection.
Replace Display Name	Replaces caller display name with the Call Queue name on agent devices.
Enable Feature Codes	Enable feature code operations (e.g., *83 for Agent Pause) for this queue.
Autofill	Distributes waiting calls automatically to agents as soon as they become free.
Dynamic Login Password	Requires dynamic agents to enter a PIN when logging in.
Alert-info	Specifies custom Alert-Info SIP header for alternative ringtones.
Call Memory	Prioritizes connecting returning callers to the agent they last spoke with.
Memory Retention Time (Days)	Retention window for Call Memory matching (1 to 30 days, default 7).
Enable RPID Header	Toggles sending Remote-Party-ID SIP header to caller.
Skip Busy Agent	Configures whether the queue will ring agents who are currently on an active call. When enabled, busy agents are skipped during call distribution.
Agents	
Dynamic Agents	Assign users authorized to dynamically sign into or out of the queue via feature codes. When Proficiency Routing is enabled, individual skill levels can be configured here.
Static Agents	Assign static agents manually and configure their ringing order within the call queue. When Proficiency Routing is enabled, individual skill levels can be configured here.
Queue Permissions	
Queue Chairman Permissions	

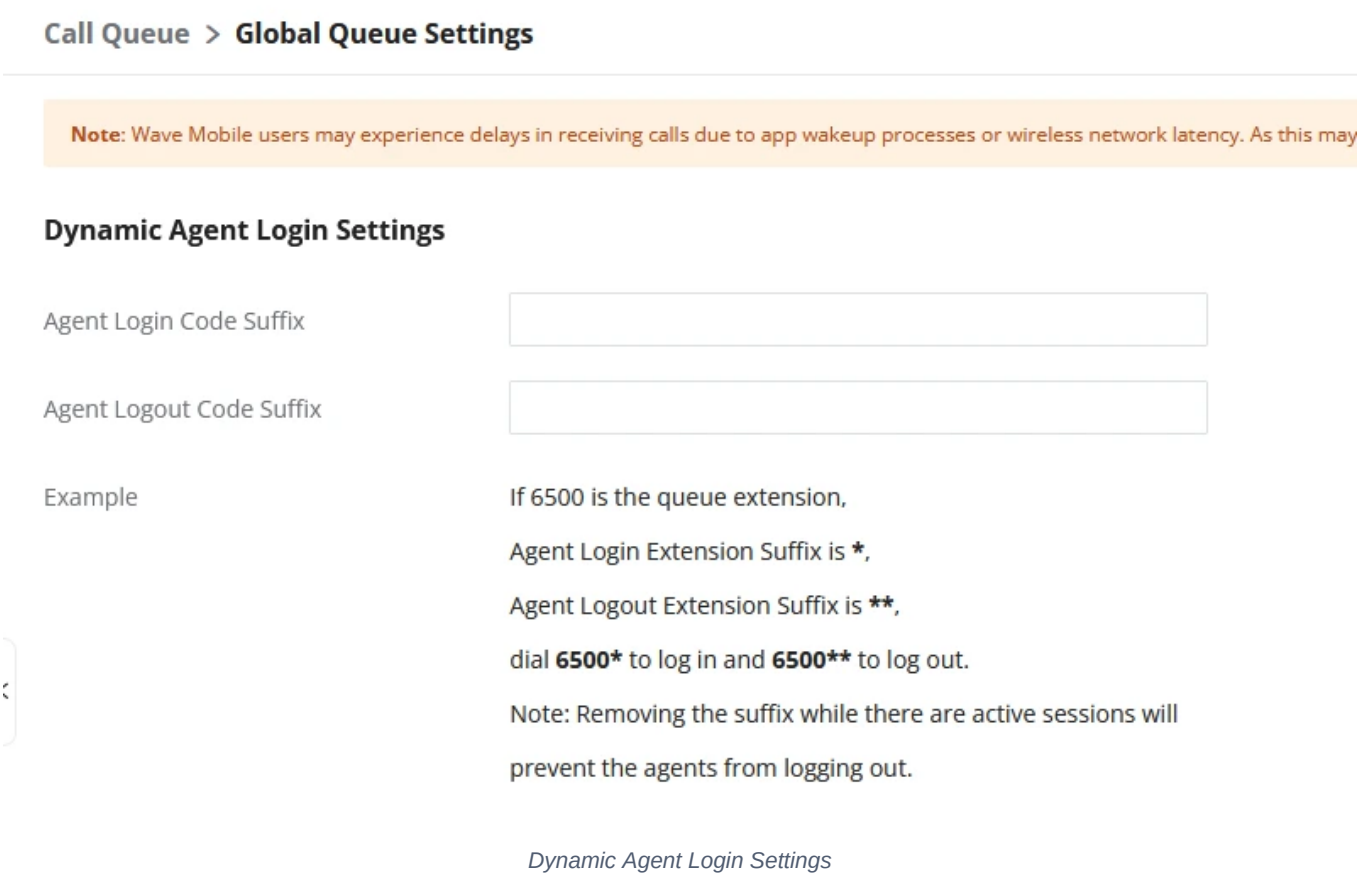
Queue Board	Grants access to view the Queue Board (Wallboard) metrics, real-time status charts, and agent statistics for this queue.
Queue Operation Panel	Enables access to the interactive Queue Operation Panel interface for this queue.
Change the status of the agent position	Allows the chairman to modify agent login states (Log In, Logout, Pause/Resume) directly from the Queue Operation Panel.
Call Assignment Management	Allows the chairman to assign waiting calls to agents, including manual drag-and-drop call dispatching from the queued list.
Allows for answering or hanging up calls on the agent's line	Grants remote control capabilities to answer or disconnect active calls on assigned agent lines.
Call monitoring operation	Enables live call supervision capabilities (Listen, Whisper, and Barge-In) for calls handled within this queue.
Call hold operation	Allows the chairman to remotely place active queue calls on hold or resume held calls.
View the CDR of this queue	Grants permission to view and review Call Detail Records (CDR) specifically filtered for this call queue.
Queue Agent Permissions	
Queue Board	Grants access to view the Queue Board wallboard for monitoring queue metrics and performance.
Queue Operation Panel	Enables access to the Queue Operation Panel for the agent.
Call Assignment Management	Allows the agent to manage call assignments and answer or retrieve queued calls from the waiting list.
Allows for answering or hanging up calls on the agent's line	Allows the agent to answer or hang up calls directly through the panel interface.
Call hold operation	Allows the agent to place calls on hold or resume held calls via the panel interface.
View the CDR of this queue	Grants permission to view and review Call Detail Records (CDR) specific to this call queue.

Static and Dynamic Agents

Call queues support two types of agents:

- **Static Agents:** Assigned manually by administrators under **Call Queue -> Edit Queue -> Agents**.
- **Dynamic Agents:** Can log in or log out of queues on-demand using feature code prefixes.

Dynamic Agent codes are managed under **Basic Call Features -> Call Queue -> Global Queue Settings -> Dynamic Agent Login Setting**:



Dynamic Agent Login Settings

When configuring the call queue settings, checking the option "Allow Static Agent Login/Logout" will cause the dynamic agents to be unavailable.

To maintain voice quality, UCM models enforce maximum agent limits. The maximum agent capacities per model are listed below:

UCM Model	Maximum Number of Agents in Call Queue
UCM6301	25
UCM6302	50
UCM6304	80
UCM6308	160

- Assigning an agent to multiple queues counts separately toward the model's total agent capacity limit. For example, adding an agent to 2 additional queues counts as 2 additional agents.
- If the user attempts to configure the number of static agents to be more than the maximum allowed number, a warning message will appear.

Call Queue Feature Codes

Call queue feature codes are managed under **Basic Call Features -> Feature Codes -> Direct Dial Feature Code**:

- **Agent Pause (*83):** Pauses an agent's queue availability across all queues. Agents can enter a pause reason code (0-9), or dial the code with the reason directly (e.g., *831 for Lunchtime).
- **Agent Unpause (*84):** Resumes active queue availability for the agent across all queues.

- **Dynamic Agent Logout (*85):** Logs dynamic agents out of all assigned call queues.

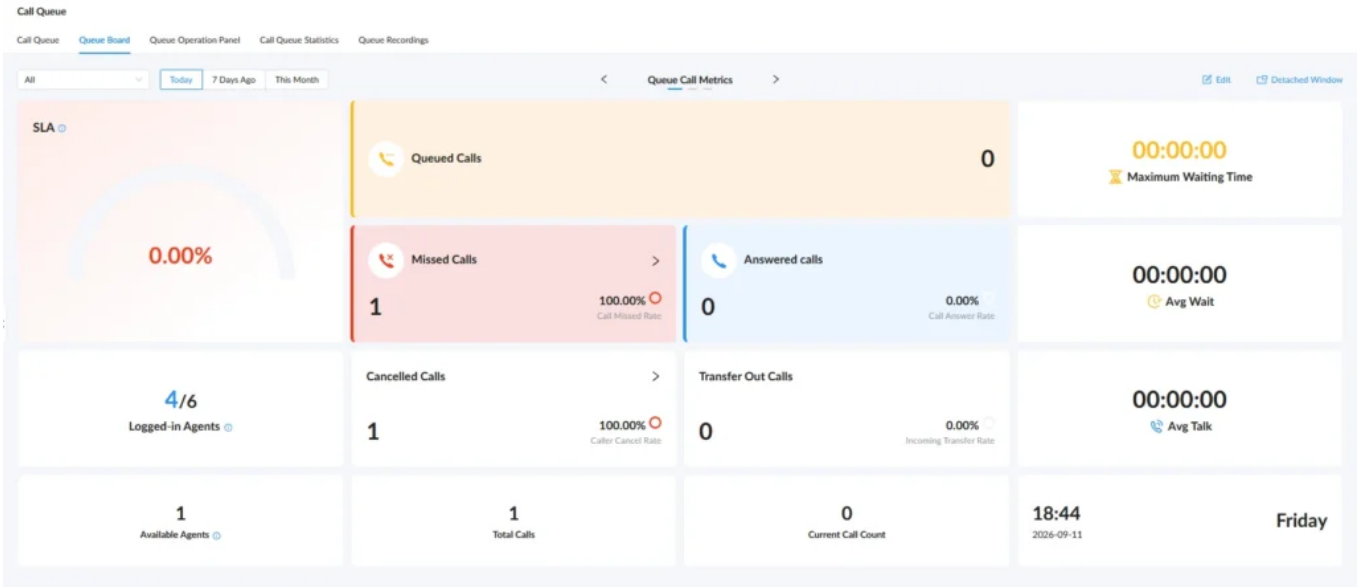
Up to 10 pause reasons can be configured under "Custom" settings. Default reasons include: (1) Lunch, (2) Hourly Break, (3) Backoffice, (4) Email, and (5) Wrap.

Queue Board

The **Queue Board** tab provides a real-time wallboard view for monitoring call center metrics, SLA compliance rates, and agent states across queues.

Click **Edit** to customize the board. The following operations are supported:

- Add or remove widgets.
- Add a description to a widget.
- Move and resize widgets, and lock a widget to prevent changes.
- Reset the board to its default layout.



The Wallboard features three analytical views:

- **Queue Call Metrics:** Displays real-time counts for Queued Calls, Missed Calls, Answered Calls, Cancelled Calls, Transferred Calls, Maximum Wait Time, Average Wait, and Average Talk Duration.
- **Queue Performance Metrics:** Provides analytical top-5 ranking charts for Average Wait, Caller Cancel Rate, and Answered Calls across queues.
- **Queue Agent Status:** Displays real-time agent login states, pause/resume timestamps, current call counts, total talk times, and answered call tallies.

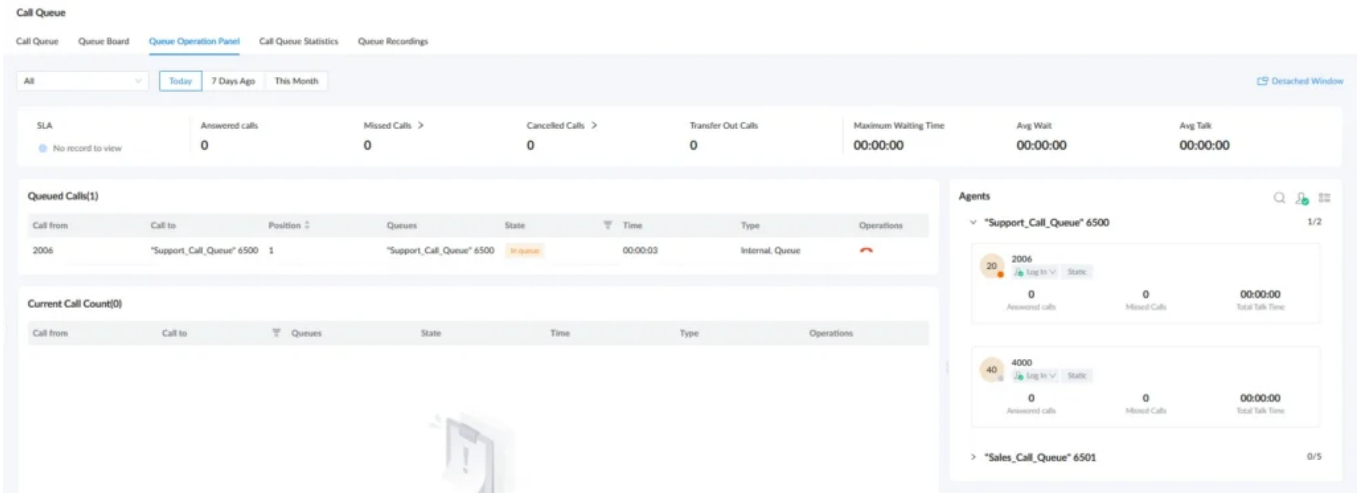
The following controls are available at the top of the Queue Board:

Option	Description
Time Range	Select the period of the displayed data: Today (default), Last 7 Days, or This Month.
Queue	If the user can view several queues, select All to display the combined data of all queues, or select a specific queue.
Board	Switch between the Queue Call Metrics, Queue Performance Metrics, and Queue Agent Status boards.
Edit	Customize the widgets displayed on the board. See Editing the Queue Board below. Note: Changes only apply to the board of the user who makes them and do not affect other users.

Open in New Window	Display the Queue Board in a standalone window. In this window, users can enable Auto Play to rotate between the boards automatically. Note: The rotation interval can be configured from 5 to 60 seconds. Default is 5 seconds.

Queue Operation Panel

The **Queue Operation Panel** replaces the legacy Queue Switchboard, providing supervisors and administrators with a real-time interactive workspace for active call management, drag-and-drop call dispatching, live call supervision, and agent status control.

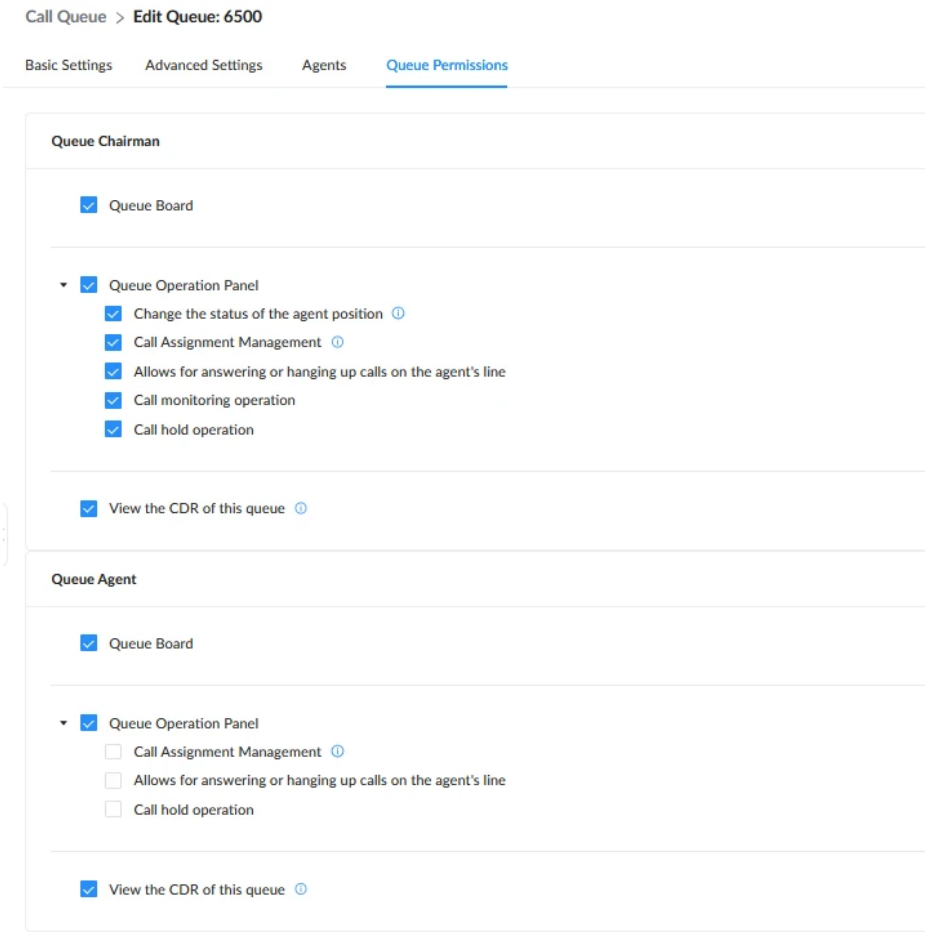


The main workspace is divided into three functional areas:

- **Queued Calls:** Displays all waiting callers in real time alongside their specific queue position, destination queue, state, wait time, and call type. Supervisors can manually manage waiting calls using available action controls or by clicking a waiting call from the list and dragging and dropping it directly onto an available agent card in the Agents panel to immediately assign and distribute the call.
- **Current Call Count:** Monitors calls currently in progress across queues, displaying the caller, target agent, queue association, call duration, and real-time call control options (such as call transfer, barge-in, listen, or whisper).
- **Agents Panel:** Displays agent cards grouped by queue, showing agent extension numbers, agent names, type (Static or Dynamic), current login status dropdown, and individual call count. Supervisors can toggle agent availability directly from this panel or receive drag-and-drop call assignments.

Queue Permissions

When adding a new call queue or editing an existing queue under **Basic Call Features -> Call Queue -> Add/Edit Queue -> Queue Permissions**, administrators can define specific operational privileges for the Chairman and Agent roles for that queue.



The table below describes the configurable permission options available for each role:

Role	Permission Option	Description
Queue Chairman	Queue Board	Grants access to view the Queue Board (Wallboard) metrics, real-time status charts, and agent statistics for this queue.
	Queue Operation Panel	Enables access to the interactive Queue Operation Panel interface for this queue.
	Change the status of the agent position	Allows the chairman to modify agent login states (Log In, Logout, Pause/Resume) directly from the Queue Operation Panel.
	Call Assignment Management	Allows the chairman to assign waiting calls to agents, including manual drag-and-drop call dispatching from the queued list.
	Allows for answering or hanging up calls on the agent's line	Grants remote control capabilities to answer or disconnect active calls on assigned agent lines.
	Call monitoring operation	Enables live call supervision capabilities (Listen, Whisper, and Barge-In) for calls handled within this queue.
	Call hold operation	Allows the chairman to remotely place active queue calls on hold or resume held calls.
	View the CDR of this queue	Grants access to the Queue CDR page in the User Portal for this queue. Users with this permission can view call details, call back callers, change the processing result of missed queue calls, and view or add call notes and labels.
Queue Agent	Queue Board	Grants access to view the Queue Board wallboard for monitoring queue metrics and performance.

Queue Agent	Queue Operation Panel	Enables access to the Queue Operation Panel for the agent.
	Call Assignment Management	Allows the agent to manage call assignments and answer or retrieve queued calls from the waiting list.
	Allows for answering or hanging up calls on the agent's line	Allows the agent to answer or hang up calls directly through the panel interface.
	Call hold operation	Allows the agent to place calls on hold or resume held calls via the panel interface.
	View the CDR of this queue	Grants permission to view and review Call Detail Records (CDR) specific to this call queue.

Overview

The overview page shows shows the following information:

- **Agent statistics:** shows the number of calls and call-related information of agents.
- **Queue Statistics**: counts the number of calls in the queue and information such as calls, waiting, and callback.
- **Agent satisfaction statistics**: used for user's rating of agents;
- **Queue satisfaction statistics:** counts the score survey statistics.

By selecting a time interval, administrators can get detailed statistics for agents such as total calls, answered calls etc, as well as queue statistics like abandoned calls, transferred calls and SLA.

Abandoned Call Calculation

When a call queue is configured with a failover destination pointing to another queue, the abandonment statistics are calculated independently for each queue.

- If a call enters CQ1 and is redirected to CQ2 (failover destination) and the call is answered, CQ1 records the call as abandoned, and CQ2 marks the call as answered.
- If the call is not answered in either queue, both call queues consider the call as abandoned.

A more detailed version of the queue statistics (as shown in image below) can be found under **Call Queue -> Call Queue Statistics -> Overview -> Queue Statistics -> Options -> Details**.

Details

Queue	6500	Total Calls	29	Answered Calls	10
Abandoned Calls	19	Answered Rate	34.48 %	Abandoned Rate	65.52 %
Transfer Out Calls	2	Transfer Out Rate	6.90 %	Average Wait Time	00:00:16
Average Talk Time	00:00:46	Callback Calls	1	SLA	0.00 %
Callback SLA	0.00 %				

Total Calls | Answered Calls | Abandoned Calls

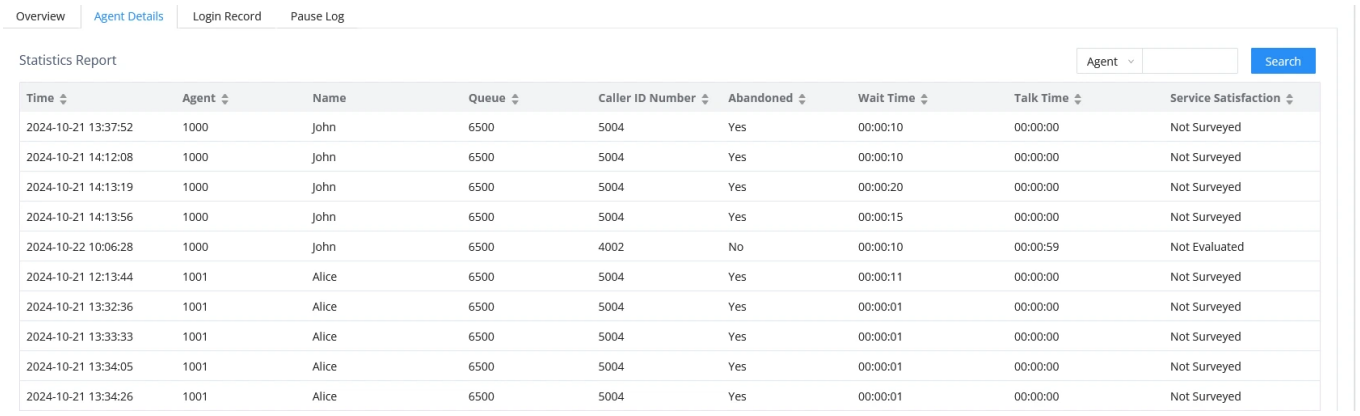
Date	Caller ID	Abandoned	Wait Time	Talk Time
2024-10-21 11:36:36	1001	No	00:00:10	00:01:22
2024-10-21 11:44:59	5004	Yes	00:00:30	00:00:00
2024-10-21 11:48:47	5004	Yes	00:00:35	00:00:00
2024-10-21 12:04:51	1001	No	00:01:14	00:00:27
2024-10-21 12:06:42	5004	No	00:00:29	00:00:25
2024-10-21 12:13:44	5004	Yes	00:00:11	00:00:00
2024-10-21 12:14:35	5004	Yes	00:00:04	00:00:00
2024-10-21 12:14:46	5004	Yes	00:00:04	00:00:00

Queue Statistics Details

Agent Details

Agent Detail**s** is a call log that shows every call to each individual agent from all queues. The following information is available:

- **Time:** the date and time the call was received.
- **Agent:** the agent extension that was rung for the call.
- **Name:** the name of to agent that received the call.
- **Queue:** the queue that the call went to.
- **Caller ID Number:** the CID of the caller
- **Abandoned:** indicates whether the call was picked up or not by that specific agent. If the call rang several agents simultaneously, and this specific agent did not pick up the call, the call will be considered abandoned even if a different agent in the same queue picked it up.
- **Wait Time:** the amount of time that the call was waiting in queue after dialing in.
- **Talk Time:** the duration of the call after it was picked up by agent.
- **Service Satisfaction:** Indicates whether the call was not surveyed, not evaluated, or provides the satisfaction score result.

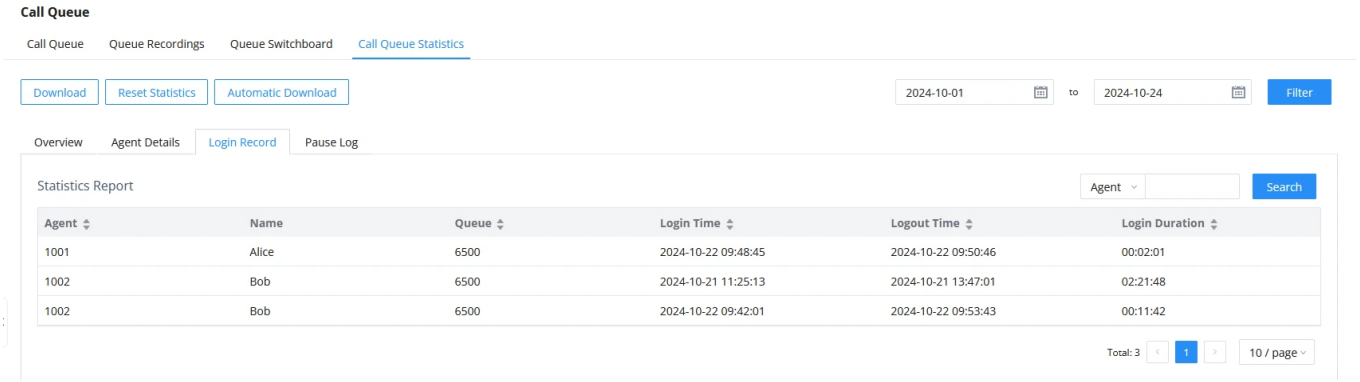


Agent details

Login Record

Login Record is a report that shows the timestamps of dynamic agent logins and logouts and calculates the login duration. The following information is available:

- **Agent:** the extension that logged in and out.
- **Queue:** the queue that the extension logged in and out of.
- **Login Time:** the time that the extension logged into the queue.
- **Logout Time:** the time that the extension logged out of the queue.
- **Login Duration:** the total length of time that the extension was logged in.

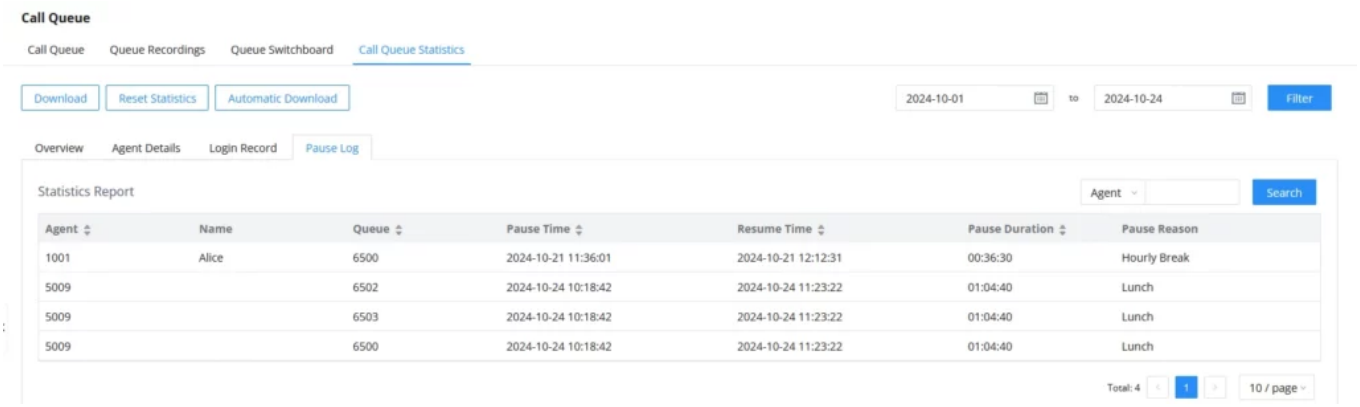


Login Record

Pause Log

Pause Log is a report that shows information related to agent pauses. An entry will only be created after an agent unpauses. The following information is available:

- **Agent**: The extension that paused/unpaused.
- **Name**: The name of the agents that paused/unpaused.
- **Queue**: The queue that the agent is in.
- **Pause Time**: The time when the agent paused.
- **Resume Time**: The time when the agent unpaused.
- **Pause Duration**: The total length of time the agent was paused for.
- **Pause Reason**: The reason of the pause (e.g., lunch, coffee break, etc...)



Pause Log

Dynamic Agent Login Settings	
Agent Login Code Suffix	Configure the code to dial after the queue extension to log into the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log in.
Agent Logout Code Suffix	Configure the code to dial after the queue extension to log out of the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log out.
Agent Pause Reason	
Agent Pause Reason Settings	Select the agent pause reason settings. Default: Use the default settings for the agent pause reason. Custom: User the custom settings. These settings should be configured using they corresponding key for each status. The user can upload a custom prompt which will be played for the agent once they set the pause reason.
Key Settings	Enter which key to press to set the different pause reasons.
Virtual Queue Callback Key Settings	
Enable	Select whether to enable or disable virtual queue callback feature. By default it's disabled.
Call Back Current Number	Press the feature key configured to set your current number as callback number.
Custom Callback Number	Press these feature key configured to set a custom callback number.
Continue Waiting	Press the feature key configured to continue waiting.

Queue Recordings

Queue call recordings are stored under **Basic Call Features -> Call Queue -> Queue Recordings**.



Administrators can play back recording files directly from the Web UI, view interactive AI transcriptions, or download audio files in .wav format. Files stored in GDMS Cloud Storage can be retrieved directly.

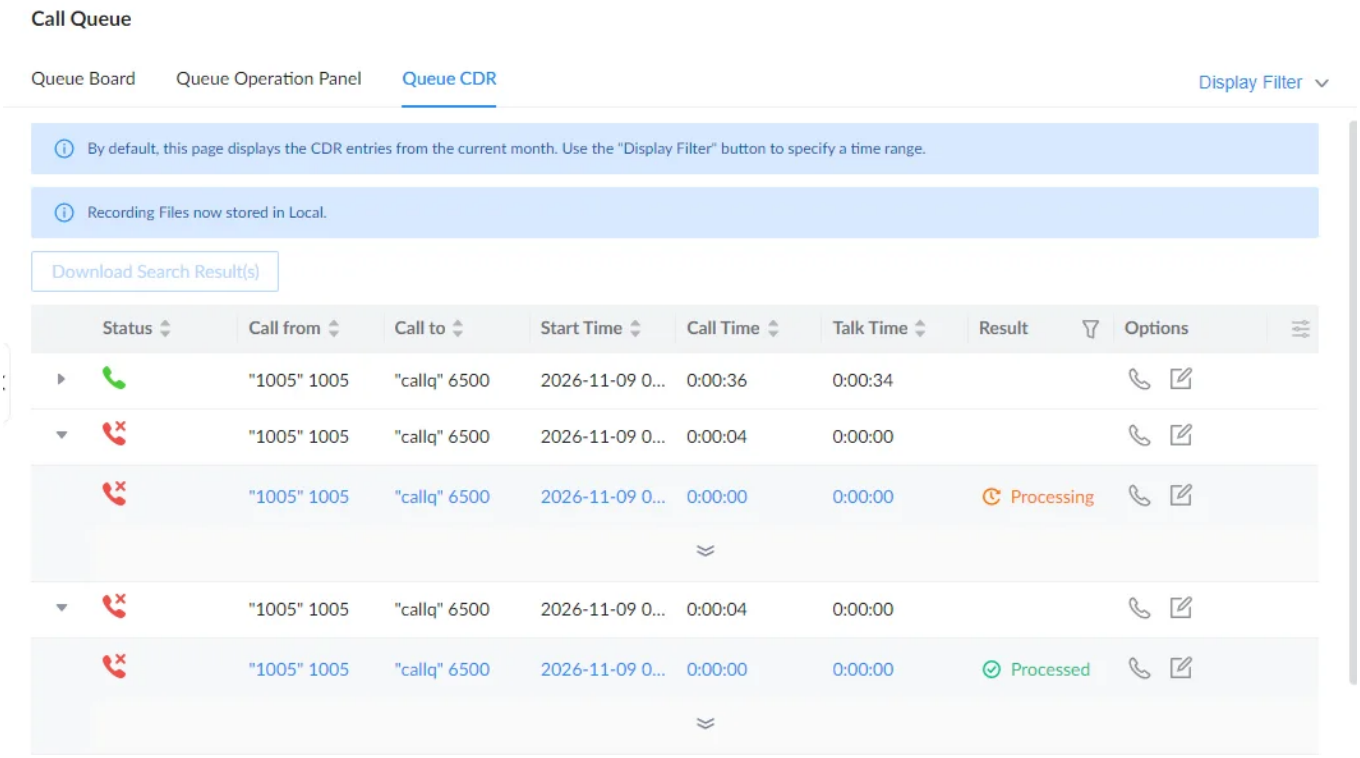
If file encryption is enabled for queue recordings, the UCM CDR/Recording Decryption Tool is required to decrypt downloaded audio files.

Queue CDR

The Queue CDR page allows authorized queue members to review the call records of their queues and follow up on missed queue calls. Unlike the standard CDR page, Queue CDR displays all calls of the queues the user is authorized for, not only the calls related to the logged-in user.

Queue CDR is available in the User Portal under **Other Features -> Call Queue -> Queue CDR**.

To access Queue CDR, the administrator must grant the View the CDR of this queue permission to the queue chairman or agent under **Basic Call Features -> Call Queue -> Edit Queue -> Queue Permissions**.

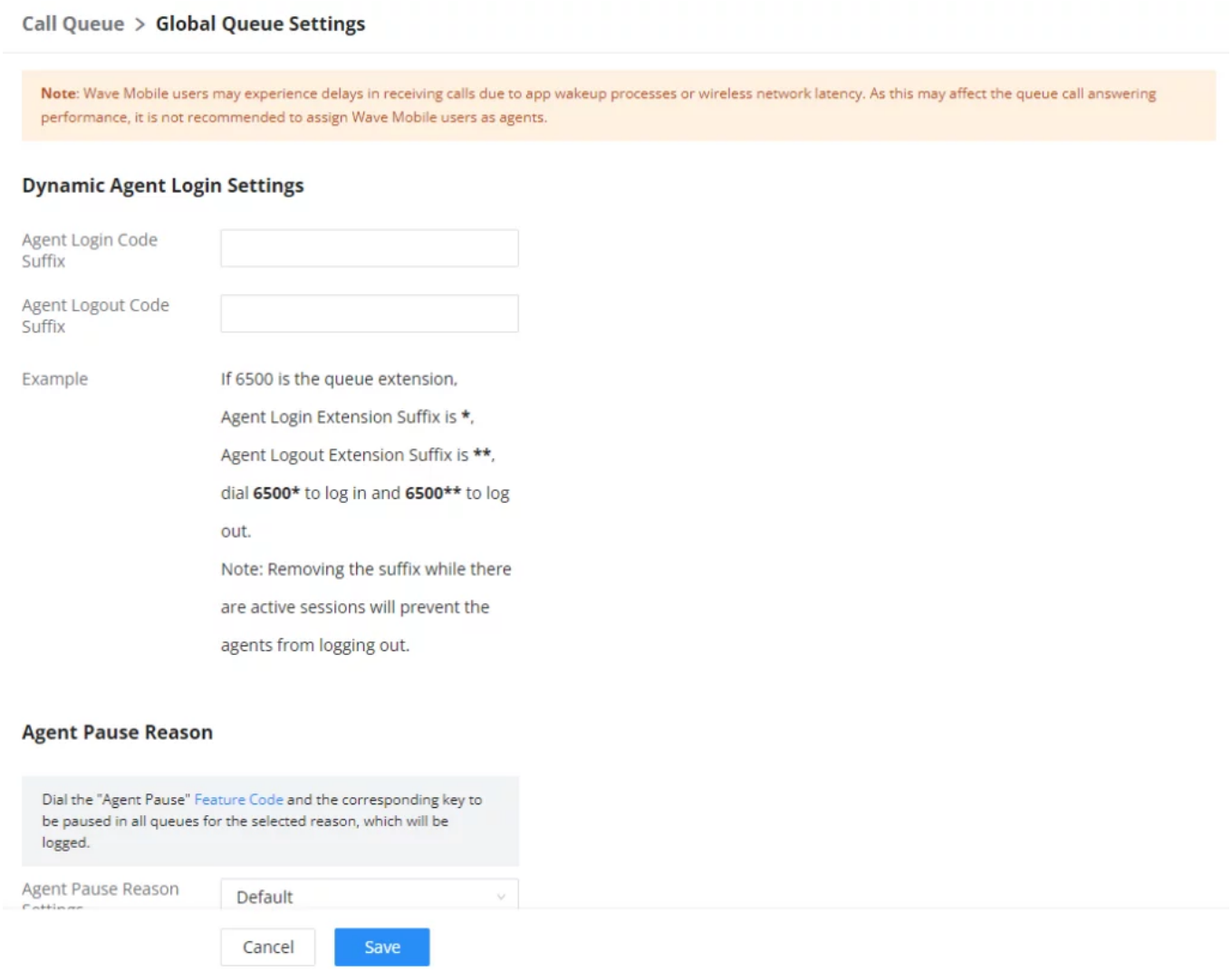


The table below describes the operations available on the Queue CDR page:

Operation	Description
Expand	View the details of CDR entries with multiple records.
Callback	Call back the caller of a queue. This option is only available if the User Portal was opened from Wave.
Result	Update the processing status of a missed queue call (Not Processed, Processing, or Processed). Note: Changes to the processing result are visible to all users who can view the queue CDR.
Call Note	View, add, and edit call notes and labels for a specific CDR entry.
Filter	Filter the queue CDR records.
Download Search Results	Download the records that match the current filter.

Global Queue Settings

As explained before, under this section users can configure the feature codes for Dynamic agent login and logout, and also can now customize the keys for virtual queue options like shown below.



Global Queue Settings

Speed Dial

Add Speed Dial

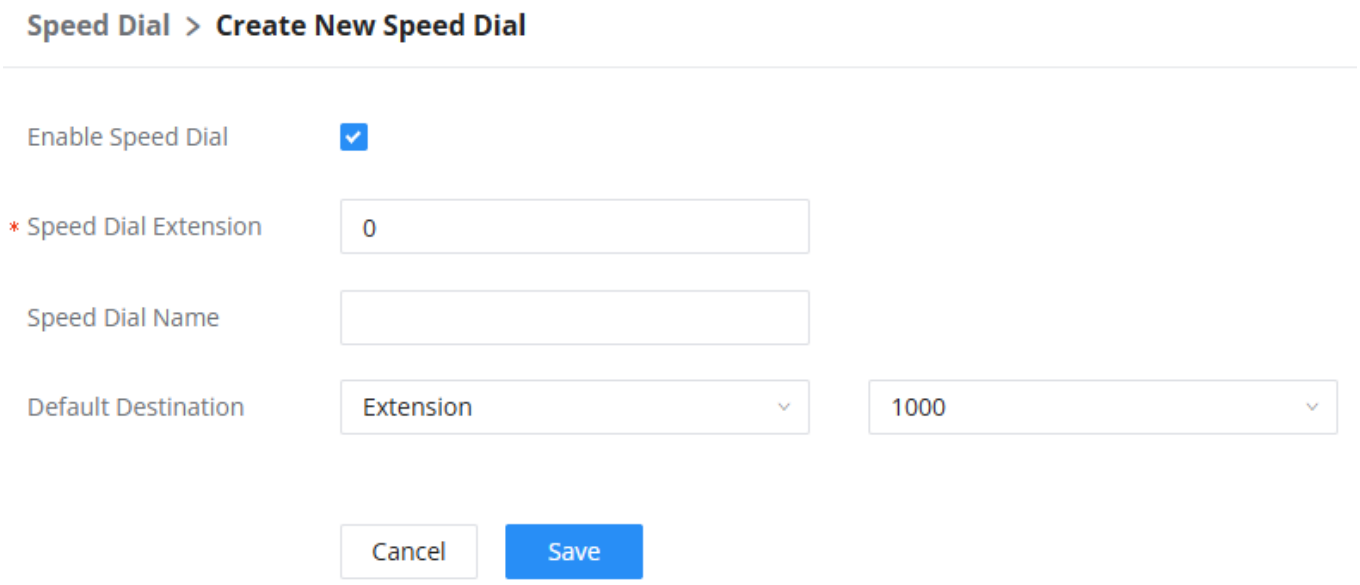
The UCM630X supports Speed Dial feature that allows users to call a certain destination by pressing one or four digits on the keypad. This creates a system-wide speed dial access for all the extensions on the UCM630X.

To enable Speed Dial, on the UCM630X Web GUI, go to page Web GUI **Basic Call Features→Speed Dial**.

User should first click on

. Then decide from one digit up to four digits combination used for Speed Dial and select a dial destination from "Default Destination". The supported destinations include extension, voicemail, conference room, voicemail group, IVR, ring group, call queue, page group, DISA, Dial by Name and external number.

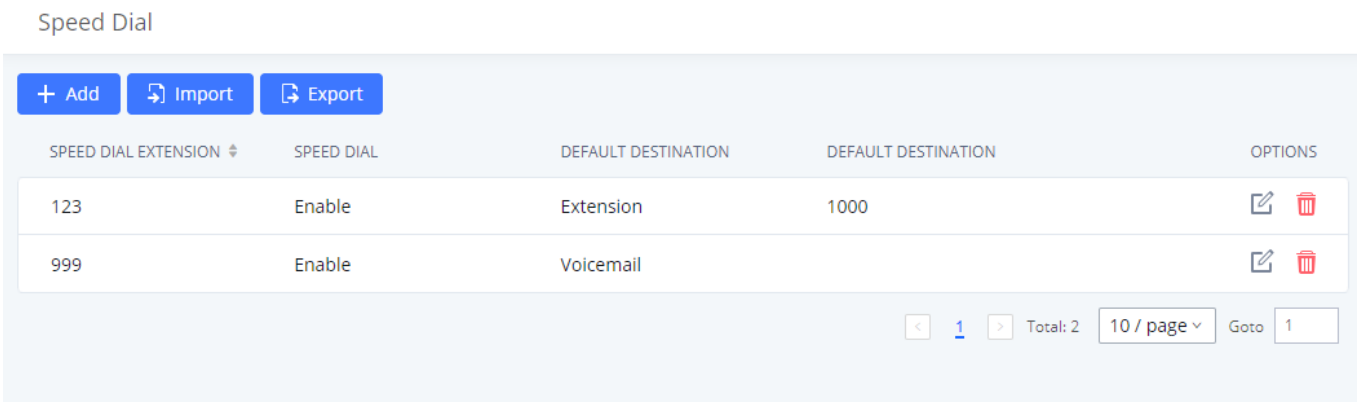
The maximum number of speed dial entries which can be configured is 1000 speed dial entries.



Speed Dial Destinations

The following can be configured as the default destination of a speed dial:

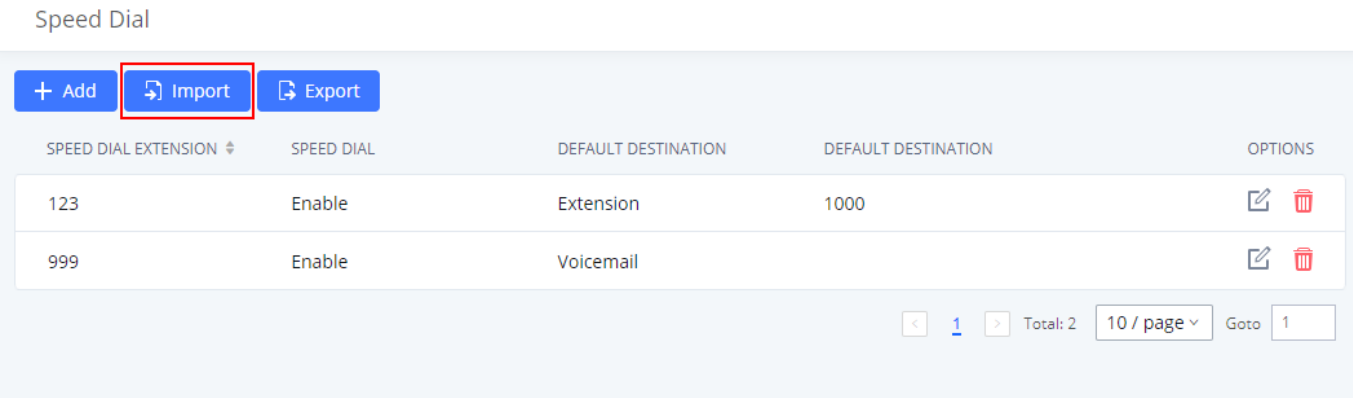
- **Extension**: Choose the extension to call when dialing the speed dial number.
- **Multimedia Meeting**: Choose the meeting room extension to call when dialing the speed dial number.
- **Voicemail**: Choose the extension which voicemail will be accessed to when dialing the speed dial number.
- **Voicemail Group**: Choose the voicemail group which will be accessed when dialing the speed dial number.
- **IVR**: Choose the IVR which will be accessed when dialing the speed dial number.
- **Ring Group**: Choose the ring group which will be called when dialing the speed dial number
- **Queues**: Choose the queue which will be called when dialing the speed dial number.
- **Paging/Intercom**: Choose the paging/intercom group which will be initiated when the speed dial number is dialed.
- **Fax**: Select the fax extension which will be used as a destination when the speed dial number is dialed.
- **DISA**: Choose DISA as the destination when the speed dial number is dialed.
- **Dial By Name**: Choose Dial By Name as the dialing destination.
- **Announcement**: Choose an announcement as the destination when the speed dial number is dialed.
- **External Number**: Enter an external number to call when the speed dial number is dialed.
- **Custom Number**: Choose a custom number to call when the speed dial number is dialed. This can also be a feature code.



List of Speed Dial

Import Speed Dial

The user can import speed dial entries, this reduces the amount of configuring the same speed dial entries on different UCMs. To do this, please click on "**Import**" as the figure below shows.



Import Dial Speed

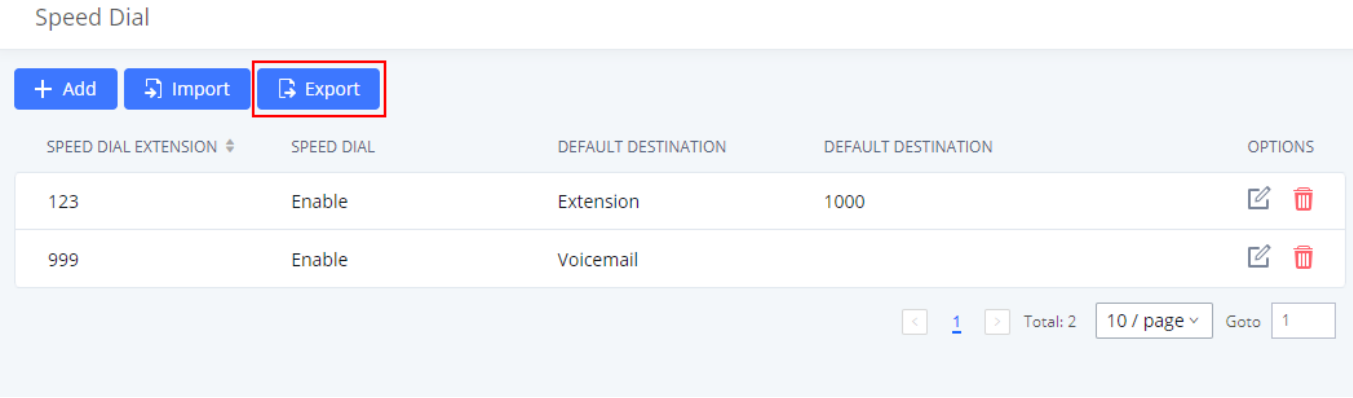
Then select the file of the speed dial entries and click

Please use UTF-8 encoding when importing a csv or xlsx.

Importing speed dial entries will overwrite the existing speed dials, if you wish to import new speed dial entries to the already existing ones, you will have to export them then combine them together in one file before you import it.

Export Speed Dial

To export speed dial entries, please click on export as the screenshot below shows, then choose the location where to save the file.



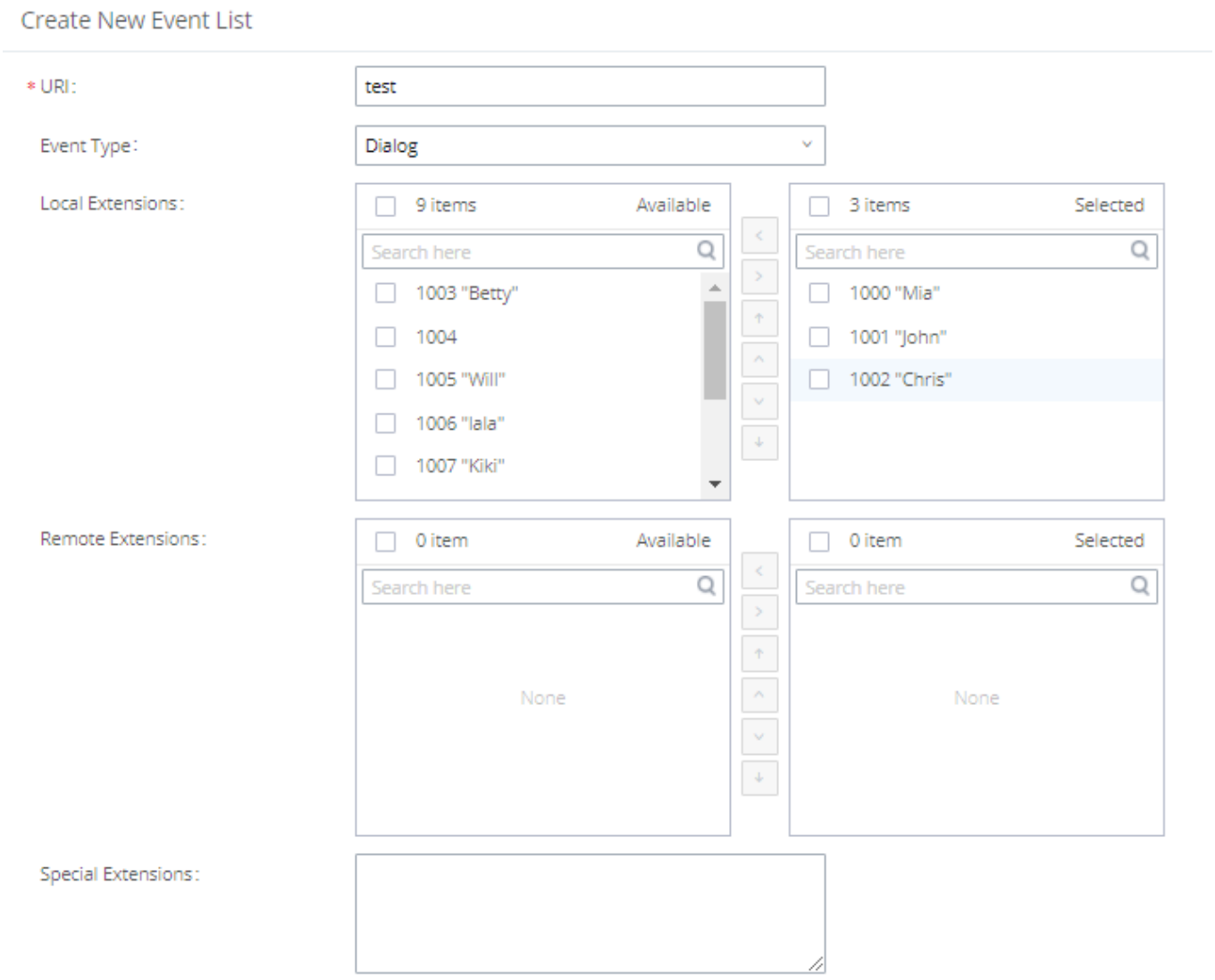
Export Dial Speed

Event List

Besides BLF, users can also configure the phones to monitor event list. In this way, both local extensions on the same UCM630X and remote extensions on the VOIP trunk can be monitored. The event list setting is under Web GUI **Basic Call Features > Event List**.

- Click on "Add" to add a new event list.
- Sort selected extensions manually in the Eventlist
- Click on to edit the event list configuration.
- Click on to delete the event list.

URI	Configure the name of this event list (for example, office_event_list). Please note the URI name cannot be the same as the extension name on the IPPBX. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions/Extension Groups listed on the local IPPBX to be monitored in the event list.
Remote Extensions	If LDAP sync is enabled between the IPPBX and the peer IPPBX, the remote extensions will be listed under "Available Extensions". If not, manually enter the remote extensions under "Special Extensions" field.
Special Extensions	Manually enter the remote extensions in the peer/register trunk to be monitored in the event list. Valid format: 5000,5001,9000



Create New Event List

Remote extension monitoring works on the UCM630X via event list BLF, among Peer SIP trunks or Register SIP trunks (register to each other). Therefore, please properly configure SIP trunks on the UCM630X first before using remote BLF feature. Please note the SIP end points need support event list BLF in order to monitor remote extensions.

When an event list is created on the UCM630X and remote extensions are added to the list, the UCM630X will send out SIP SUBSCRIBE to the remote UCM630X to obtain the remote extension status. When the SIP end points register and subscribe to the local UCM630X event list, it can obtain the remote extension status from this event list. Once successfully configured, the event list page will show the status of total extension and subscribers for each event list. Users can also select the event URI to check the monitored extension's status and the subscribers' details.

- To configure LDAP sync, please go to UCM630X Web GUI→Extension/Trunk→VoIP Trunk. You will see "Sync LDAP Enable" option. Once enabled, please configure password information for the remote peer UCM630X to connect to the local UCM630X. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM630X and remote UCM630X need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM630Xs.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM630X PBX. However, it might not work the other way around depending on whether the non-UCM630X PBX supports event list BLF or remote monitoring feature.

Feature Codes

Feature codes allow users to perform certain actions such as call park or enabling do not disturb mode, by dialing a configured code. (e.g. dialing #72 to park a call).

The UCM630x is by default configured with feature codes for different use cases, but users can change these codes manually by accessing **Basic Call Features -> Feature codes**.

- When manually configuring feature codes, please make sure there is no conflict between the values.
- In order to avoid incompatibility, some feature codes do not support being nested by other numbers. (e.g. if a feature code is *44, another feature code cannot be *441). This is important because there are a few codes that can be used in conjunction with a series of digits.
- For example, users can dial *72 (Call Forward Always Enable) followed by 1000 (*721000) to set the forwarding destination as extension 1000. However, if there is another feature code configured as *7210, it is impossible for the UCM to determine whether the user wants to use this code or to enable call forward always with extension 10 as the destination.

In-call Feature Code	
Global Settings	
Key Press Timeout (ms)	Configure the maximum interval (ms) between digits for feature code activation. The valid range is 800 to 10000 and the default setting is 1000.
Transfer	
Blind Transfer	- Default code: #1- Enter the code during active call. After hearing "Transfer", you will hear dial tone. Enter the number to transfer to. Then the user will be disconnected, and transfer is completed. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Attended Transfer	- Default code: *2 - Enter the code during active call. After hearing "Transfer", you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. In case of the called party does not answer, users could press *0 to cancel the call and retrieve the first call leg. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Transfer Dialing Timeout Period (s)	Configures the dial timeout period of blind and attended transfers.
Record Audio	

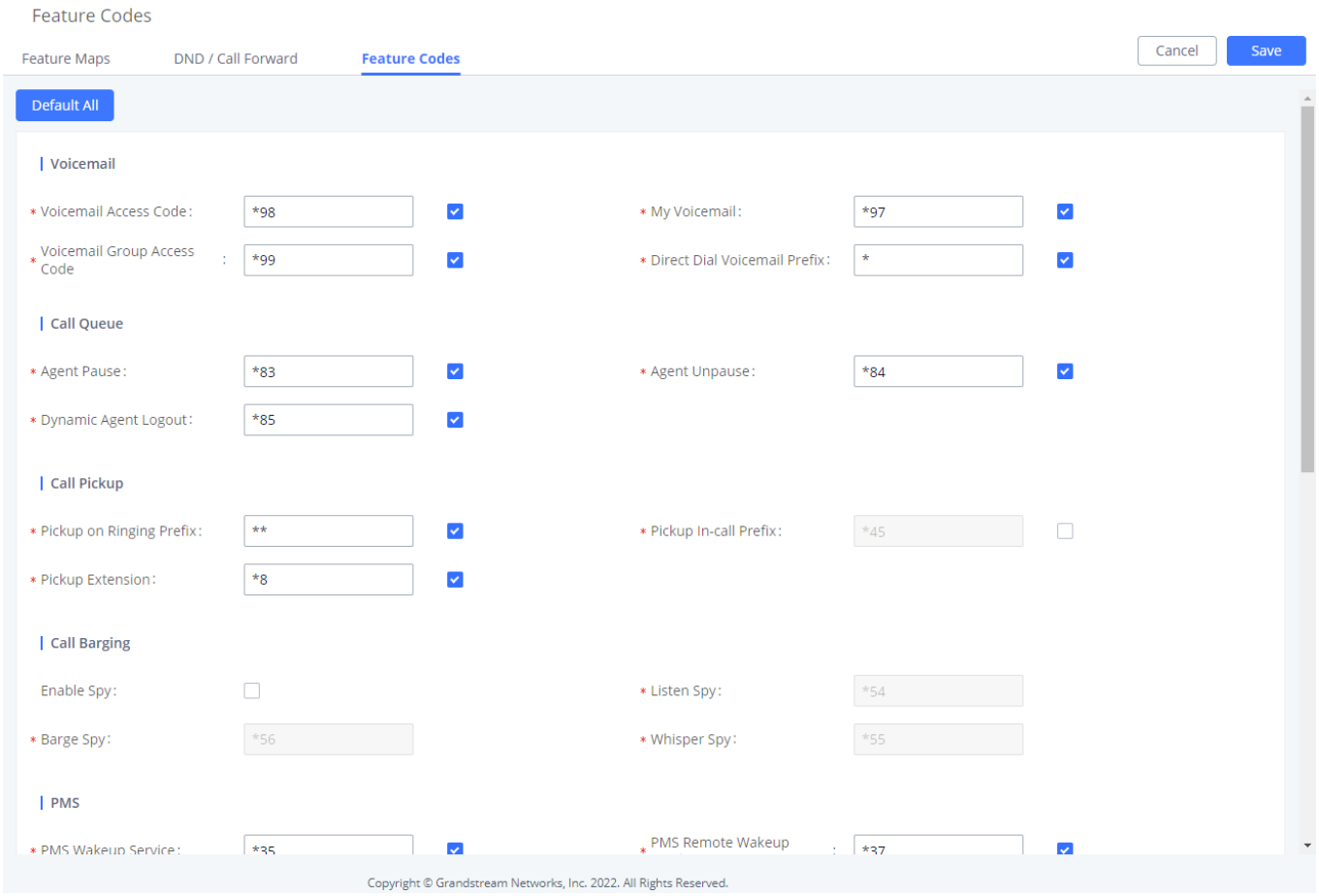
Start/Stop Call Recording	-Default code: *3 - Enter the code followed by # or SEND to start recording the audio call and the PBX will mix the streams natively on the fly as the call is in progress. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Enable Recording Allowlist	Enable the Recording Whitelist feature
Recording Allowlist	Select extension in the whitelist that can use the *3 recording function.
Other	
Disconnect	- Default code: *0 - Enter the code during active call. It will disconnect the call. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Call Park	- Default code: #72- Enter the code during active call to park the call. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
 Seamless Transfer	Default code: *44 (Disabled by default). Seamless Transfer allows user to perform blind transfer using PBX feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple. During an active call use the feature code (*44 by default) followed by the number you want to transfer to in order to perform the seamless transfer. (This feature code cannot be nested by other feature codes)
 Start/Stop AI Call Transcription	Allows authorized extension users to manually start or stop AI call transcription dynamically during an active call session. The default feature code for this option is *6 (This feature code cannot be nested by other feature codes)
DND/Call Forward	
Call Forward Setting Type	Basic Advanced If Advanced is selected, call forwarding can be set for all calls, internal calls and external calls. To do this, users can dial one of the feature codes below and then dial 0, 1 or 2. The feature code modifiers are as follow: → 0 corresponds to "All calls".→ 1 refers to "Internal calls". (calls that came within the PBX)→ 2 is used for "External calls". (calls from outside the PBX)
Do Not Disturb (DND) Activate	Default code: *77Activate DND feature to ignore any incoming calls.
Do Not Disturb (DND) Deactivate	Default code: *78Deactivate DND Feature.
 Call Forward Busy Enable	Default Code: *90 Enables Call Forward Busy (CFB) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced.(This feature code cannot be nested by other feature codes)
Call Forward Busy Disable	Default Code: *91Disables Call Forward Busy (CFB) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
 Call Forward No Answer Enable	Default Code: *92 Enables Call Forward No Answer (CFNA) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced.(This feature code cannot be nested by other feature codes)
Call Forward No Answer Disable	Default Code: *93Disables Call Forward No Answer (CFNA) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.

Call Forward Always Enable	Default Code: *72Enables Call Forward Always (CFA) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced. (This feature code cannot be nested by other feature codes)
Call Forward Always Disable	Default Code: *73Disables Call Forward Always (CFA) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
Remote Call Forward Enable	Enable this option and configure the Remote Call Forward Whitelist below to allow specific extensions to dial the remote call forwarding feature codes to set call forwarding for any extension.
Remote DND / Call Forward Settings	
Enable	Enable this option and configure the Whitelist below to allow specific extensions to dial feature codes to set DND or call forwarding for any extension.
Remote Call Forward Busy Enable	Default code: *65 Configures and enables CFB for any extension.
Remote Call Forward No Answer Enable	Default code: *66Configures and enables CFNA for any extension.
Remote Call Forward Always Enable	Default code: *67Configures and enables CFU for any extension.
Remote DND Enable	Default code: *68Enables Do Not Disturb for any extension.
Remote Call Forward Busy Disable	Default code: *651Disables CFB for any extension.
Remote Call Forward No Answer Disable	Default code: *661Disables CFNA for any extension.
Remote Call Forward Always Disable	Default code: *671Disables CFU for any extension.
Remote DND Disable	Default code: *681Disables Do Not Disturb for any extension.
Allowlist	Extensions in this whitelist can configure DND or call forwarding for any extension via feature codes.
Direct Dial Feature Code	
Voicemail	
Voicemail Access Code	- Default code: *98 - Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box.(This feature code cannot be nested by other feature codes)
My Voicemail	- Default code: *97 - Press *97 to access the voicemail box.
Voicemail Group Access Code	Default code: *99Dial this code to access group voicemail. If password is required, enter password followed by the pound (#) key.If Allow Members to Modify Voice Prompts is enabled under Voicemail Group settings, group members dialing *99 can also record, update, or customize voice prompts and greetings for the Voicemail Group via DTMF audio menus.
Direct Dial Voicemail Prefix	Prefix used to dial directly to voicemail.
Call Queue	
Agent Pause	Default code: *83Pause the agent in all call queues.(This feature code cannot be nested by other feature codes)
Agent Unpause	Default code: *84Unpause the agent in all call queues.
Dynamic Agent Logout	Default code: *85 Log the dynamic agent out of all queues.

Call Pickup	
 Pickup on Ringing Prefix	Picks up a ringing call for another extension. Example: If the prefix is **, and there is a call ringing ext 1008, dial **1008 from a different extension to pick up the call to 1008. (This feature code cannot be nested by other feature codes)
Pickup In-call Prefix	Picks up an ongoing call for another extension. Example: If the feature code is *45, and ext 1008 is in a call, dialing *45 and then 1008 following the prompt will take that call. Note: The feature code user must be in the extension's Allowed to seamless transfer list to pick up calls for it.
Pickup Extension	This is the feature code to pick up incoming calls for other extensions in the same pickup group. The default setting is *8.
Call Barging	
Enable Spy	Check this box to enable spy feature codes.
 Listen Spy	This is the feature code to listen in on a call to monitor performance. Your line will be muted, and neither party will hear you. The default setting is *54.(This feature code cannot be nested by other feature codes)
 Barge Spy	This is the feature code to join in on the call to assist both parties. The default setting is *56.(This feature code cannot be nested by other feature codes)
 Whisper Spy	This is the feature code to speak to only one party in the call. For example, you could whisper to employees to help them handle a call. Only an employee on your account will be able to hear you. The default setting is *55.(This feature code cannot be nested by other feature codes)
PMS	
PMS Wakeup Service	Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service.
PMS Remote Wakeup Service	Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions.
 Update PMS Room Status	2 methods are available:1. Dial the room status feature code + housekeeper code, listen to the prompt and then the dial the appropriate key for the desired room status. Example: The housekeeper with housekeeper code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available.2. Dial room status feature code*housekeeper code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: Housekeeper with Housekeeper code 0001 dials *23*0001*1 to change room status Available.(This feature code cannot be nested by other feature codes)
Paging/Intercom	
 Paging Prefix	Configure the paging prefix for paging. For example, if the Paging Prefix is set to *81, dial *816000 to initiate a paging call to extension 6000.(This feature code cannot be nested by other feature codes)

Delayed Paging	If enabled, a caller can enter this feature code before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the precorded message will be played, and the call will end after it is finished playing.
 Intercom Prefix	Configure the intercom prefix for intercom calls. For example, if the Intercom Prefix is set to *80, dial *806000 to initiate an intercom call to extension 6000.(This feature code cannot be nested by other feature codes)
Misc	
Blocklist Add	Follow the voice prompt to add a caller ID to blacklist.
Blocklist Last Caller	Add the last inbound caller ID number to blacklist.
Blocklist Remove	Follow the voice prompt to remove a caller ID from blacklist.
 Direct Dial Mobile Phone Prefix	If calling mobile phone numbers is permitted, use this prefix plus the extension number to dial the mobile phone number of this extension directly.(This feature code cannot be nested by other feature codes)
Call Completion Request	If the caller wants to use CC to complete a call, he/she can dial this code. After the CC has been registered successfully, the system will start to monitor the status of the callee. The system will call back the caller when the callee's extension is available.
Call Completion Cancel	If the caller has requested CC successfully, and he/she doesn't need to call back anymore, he/she can dial this code to cancel the request.
Presence Status	Dial this feature code to set the presence status of the extension.
Call Flip	- Default code: *46- Dial this code to move the call of this extension from another device to the current device.
Remote Extension Privilege Update	Whitelisted extensions will be able to use the Remote Extension Privilege Update feature code to remotely change any extension's outgoing call privilege.Note: After this function has been enabled, the extension is the whitelist can set the privilege for outgoing calls of any extension by dialing the feature code.
Remote Extension Privilege Update Allowlist	Remote Extension Privilege Update WhitelistProcedure: Dial *26 on the whitelisted extension, hear the prompt "Change extension's outgoing permission level, please enter the phone number, then enter # key." After the process, voice will prompt "Press 1 to set to internal, press 2 to set to local, press 3 to set to national, press 4 to set to international." After selecting, it will prompt "Change extension XXXX outgoing permission to XXX", and hang up.
 Priority Call	Makes a high priority call to a specified extension by dialing the feature + extension number. If the specified extension is an ongoing call, it will be forcibly hung up to allow the caller to ring the extension. (This feature code cannot be nested by other feature codes)
Priority Call Allowlist	Extension in the whitelist will be allowed to use this feature code to make priority calls.

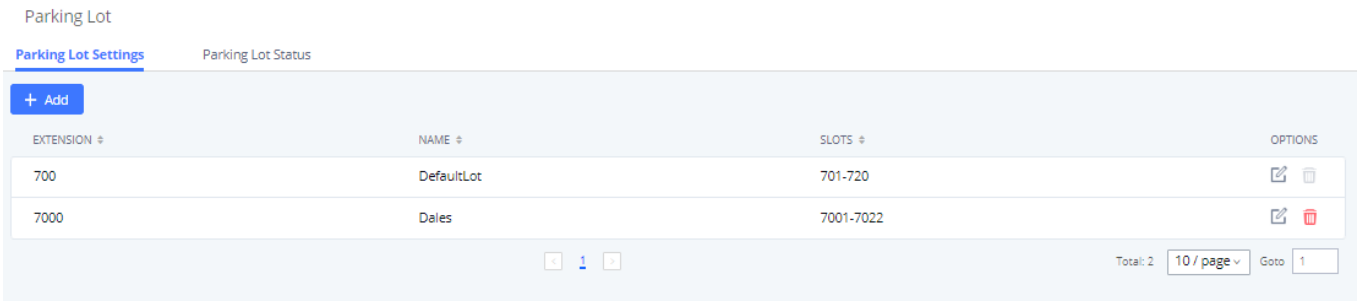
The UCM630X also allows user to one click enable / disable specific feature code as shown below:



Enable/Disable Feature codes

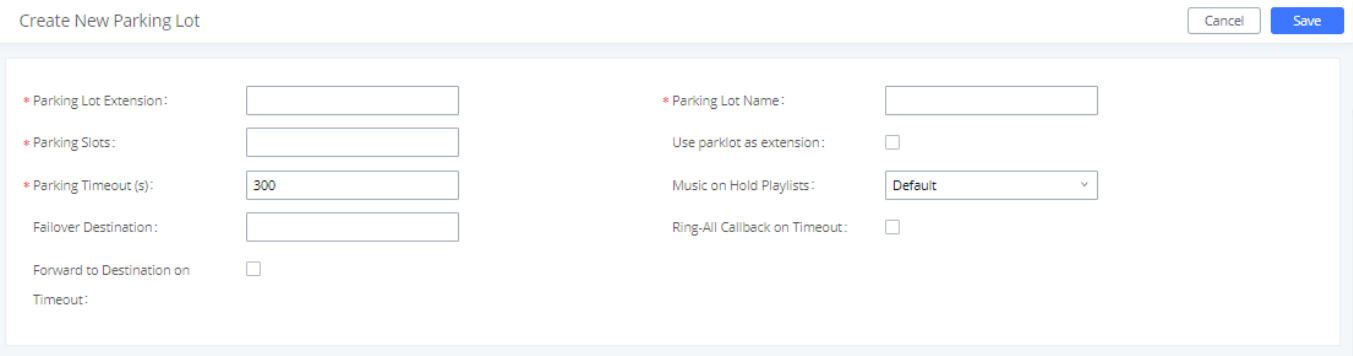
Parking Lot

User can create parking lots and their related slots under Web GUI **Basic Call Features > Parking Lot.** In the Parking Lot page, users can create lots of their own. This allows different groups within an organization to have their own parking lots instead of sharing one large parking lot with others. While creating a new parking lot, users can assign it a range that they think is appropriate for the group that will use the parking lot.



Parking Lot

User can create a new Parking lot by clicking on button "Add" :



New Parking Lot

Parking Lot Extension	Default Extension: 700 During an active call, initiate blind transfer and then enter this code to park the call. Note: The user change the default extension for the parking lot to a different extension.
Parking Lot Name	Set a name to the parking lot
Parked Slots	Default Extension: 701-720 These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.
Use Parking lot as Extension	If checked, the parking lot number can be used as extension. The user can transfer the call to the parking lot number to park the call. Please note this parking lot number range might conflict with extension range.
Parking Timeout (s)	Default setting is 300 seconds, and the maximum limit is 99.999 seconds. This is the timeout allowed for a call to be parked. After the timeout, if the call is not picked up, the extension who parks the call will be called back.
Music On Hold Classes	Select the Music on Hold Class.
Failover Destination	Configures a callback failover destination when the extension that is called back is busy. The call will be routed to the destination number and this reduces the chance of dropping parked calls.
Ring All Callback on Timeout	If enabled, all registered endpoints of the extension will ring when callback occurs. Otherwise, only the original endpoint will be called back.
Forward to Destination on Timeout	If enabled, the call will be routed to the configured destination upon timeout. Otherwise, the call will be routed back to the original caller.
Timeout Destination	This option appears once Forward to Destination on Timeout is enabled. Upon park timeout, the call will be routed to the configured destination.
Parking Lot Timeout Alert-Info	Adds an Alert-Info header to parking lot callbacks after the Parking Timeout has been reached.

Call Park

The UCM630X provides call park and call pickup features via feature code.

Park a Call

There are two feature codes that can be used to park the call.

- **Feature Maps→Call Park (Default code #72)**

During an active call, press #72 and the call will be parked. Parking lot number (default range 701 to 720) will be announced after parking the call.

- **Feature Misc→Call Park (Default code 700)**

During an active call, initiate blind transfer (default code #1) and then dial 700 to park the call. Parking lot number (default range 701 to 720) will be announced after parking the call.

Retrieve Parked Call

To retrieve the parked call, simply dial the parking lot number and the call will be established. If a parked call is not retrieved after the timeout, the original extension who parks the call will be called back.

Monitor Call Park CID Name Information (GXP21xx, GRP261x Phones Only)

Users can see the CID name information of parked calls. VPK/MPKs must be configured as "Monitored Call Park" with the desired parking lot extension. The display will alternate between displaying the parking lot extension and the call's CID name. There is no need to configure anything on the UCM.



Monitored Call Park CID name

ADVANCED CALL FEATURES

Call Flow Design

Call Flow Design allows administrators to visually build, customize, and automate complex call routing logic using an intuitive drag-and-drop workflow canvas. Instead of relying on static, single-destination routing rules, a Call Flow acts as an advanced, dynamic process that evaluates incoming caller interactions, variables, time conditions, and input sequences before directing calls to their final destinations.

Once a Call Flow is built and enabled, it can be assigned as a destination to an inbound route allowing complex and scenario based call routing.

For comprehensive step-by-step instructions on designing call flows, please refer to the dedicated Call Flow Design Configuration Guide.

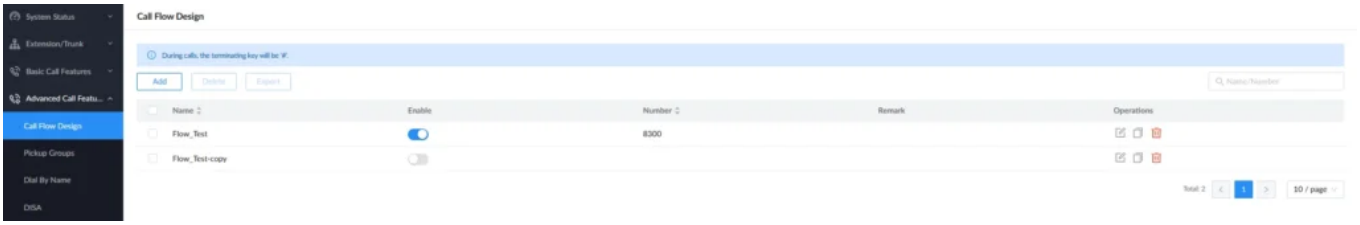
Call Flow System Specifications & Limits

The following table outlines the system capacity and operational limits for Call Flow Design on the UCM Series:

Parameter	Specification/Limit
Maximum Configurable Call Flows	Up to 200 total Call Flows
Maximum Nodes & Branches per Flow	Up to 200 total components (nodes and branches) per Call Flow
Maximum Sequential Steps per Flow	Up to 50 sequential execution steps per individual flow execution

Call Flow Management

To manage and configure Call Flows, navigate to **Call Features->Call Flow Design**.



The main Call Flow list page displays the following summary information:

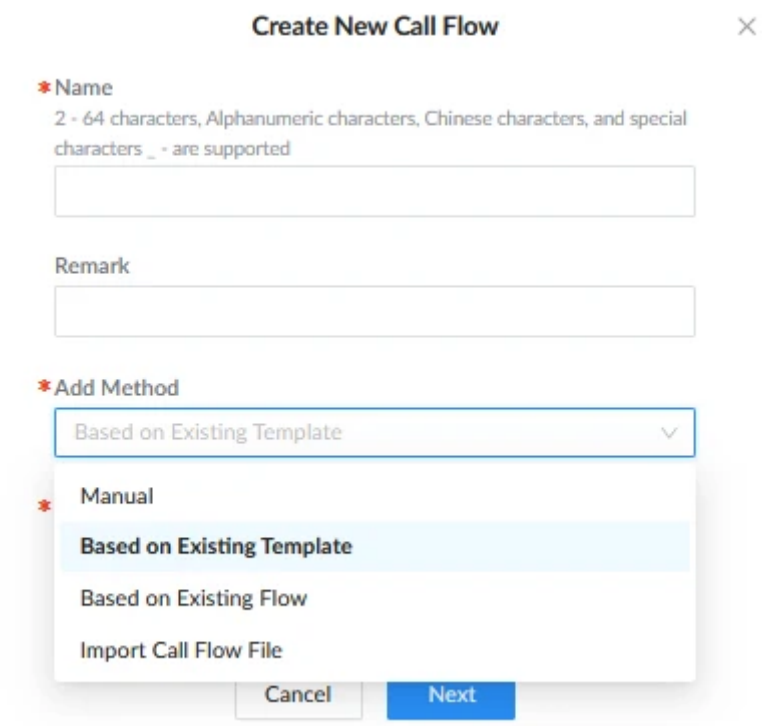
Parameter	Description
Name	The name identifier for the call flow.
Enable	Displays whether the call flow is active (Enabled).
Number	The internal extension assigned to trigger or route calls into the flow. The default range reserved for call flow is 8300-8499. Note: users can configure the extension ranges under PBX Settings->Extension Preferences.
Remark	Optional descriptive notes regarding the call flow's function.
Operations	Quick action icons to Edit (opens the visual editor), Copy (creates a duplicate call flow), or Delete the call flow.

Administrators can also select single or multiple Call Flows and click **Export** to save configuration files in .json (single) or .zip (multiple) formats.

Creating a Call Flow

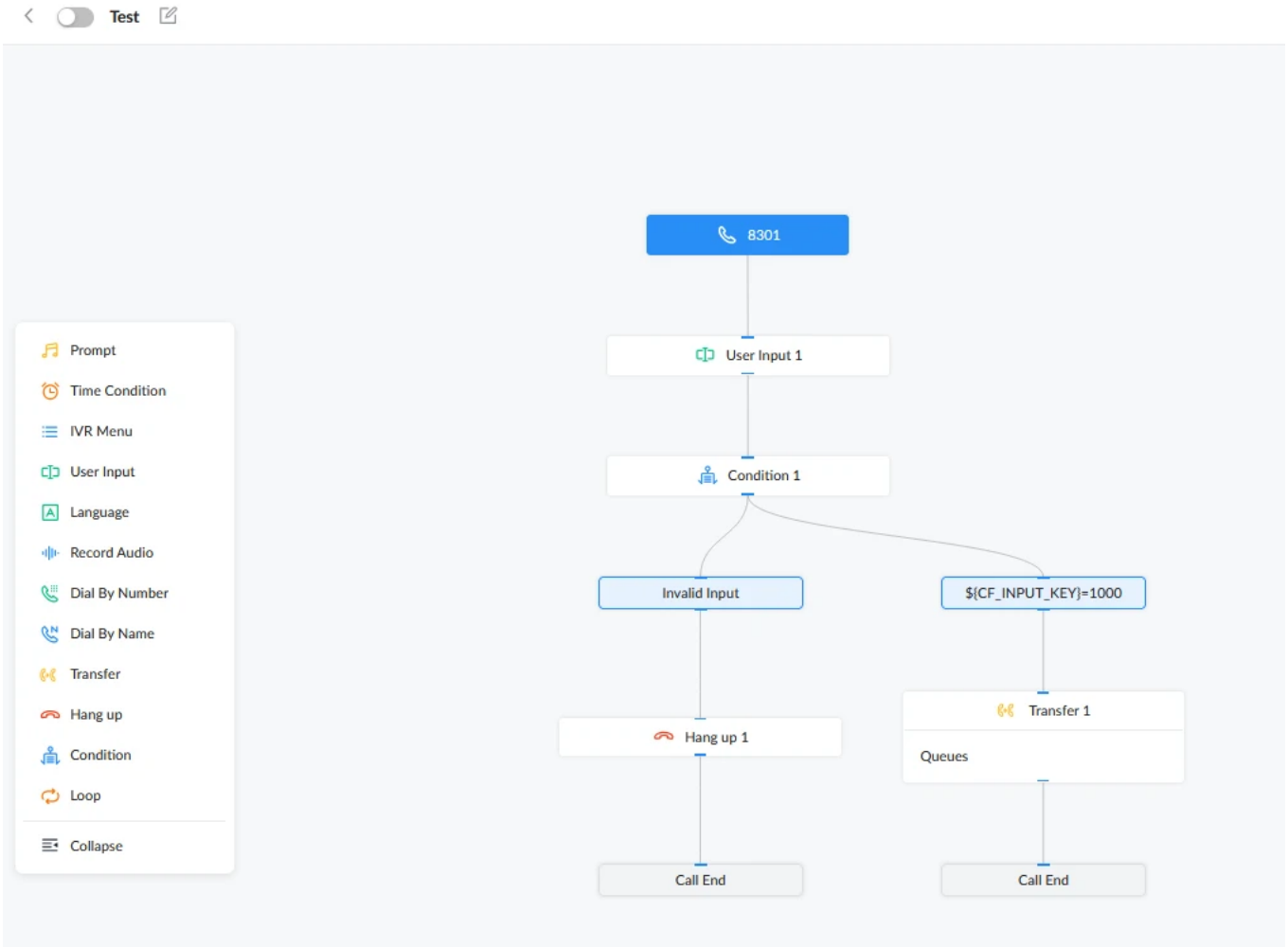
Click on **Add** to create a new Call Flow. The initial setup can be done using four creation methods:

- **Manual:** Starts with a blank canvas containing only the mandatory **Initial Action** component (call flow extension).
- **Based on Existing Templates:** Choose from pre-built workflow templates:
    - **Call Flow Based on IVR Key Press:** Routes callers to different destinations based on single-key DTMF selections.
    - **Call Flow Based on IVR Key Press:** Routes callers to different destinations based on single-key DTMF selections.
    - **Input Matching Authentication Flow:** Prompts for DTMF digit entry and matches caller inputs against predefined conditions.
- **Based on Existing Flow:** Duplicates an existing Call Flow configured on the UCM.
- **Import Call Flow File:** Uploads a pre-configured Call Flow definition file in .json format.



Call Flow Configuration Options

When users add or edit a call flow, they're immediately redirected to a separate editor page which provides drag-and-drop components organized by functionality.



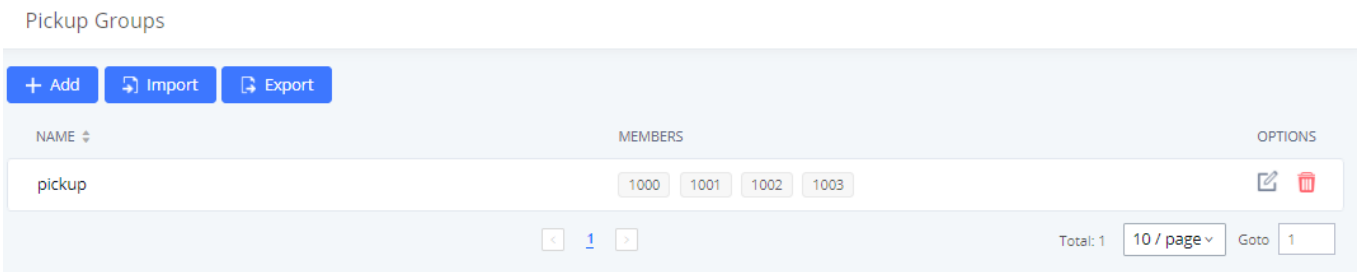
The table below describes each of the components supported in the editor.

Call Flow Node	Description
Initial Action (Start Component)	The mandatory entry point for every flow. Configures the assigned extension number, initial welcome audio prompt, and loop settings.
Prompt	Plays selected audio files or AI-generated Text-to-Speech (TTS) announcements to the caller. Users can also play the prompt on loop 3 times.
Time Condition	Evaluates system time conditions (Office Hours, Custom Time, or Custom Time Groups) and branches the routing path accordingly.
IVR Menu	Presents multiple DTMF menu options, stores keystroke entries into variables, and branches calls based on valid inputs, timeouts, or invalid entries.
User Input	The User Input component is used to play an instructional prompt and capture DTMF key sequences (such as PINs or account IDs) entered by the caller and passes the call to the next connected node (typically a Condition node) for expression evaluation.
Language	Overrides the system default voice prompt language for all subsequent components in the call flow path.
Record Audio	Dynamically enables or disables call recording at a specific stage in the flow, with options to play pre-recording notification prompts.
Dial by Number	Directs callers to manually enter numbers to reach allowed extension ranges, predefined internal destinations (IVR, Ring Group, Queue, Conference, Call Flow), or external numbers using a defined pattern or LDAP directory contacts.
Dial by Name	Allows callers to search for and connect to a target user by spelling the letters of the user's name with their phone keypad. The search directory can be configured using local extensions, LDAP phonebooks, or both.
Transfer	Directs the caller out of the Call Flow to a final internal or external destination (Extension, Voicemail, Ring Group, Queue, IVR, or another Call Flow).
Hang Up	Terminates the active call session.
Condition	Evaluates logical expressions configured under custom branches. Branches evaluate variables (such as ${CF_INPUT_KEY}, ${CALLERID(number)}, or ${CALLFLOW_LANGUAGE}), constants, or built-in functions to determine subsequent call routing. Note: Please refer to the Call Flow Design Configuration Guide for a list the supported expressions.
Loop	Repeats execution of its child components either for a fixed count (Range: 1-99) or until a custom logical condition expression.

Pickup Groups

The UCM630X supports pickup group feature which allows users to pick up incoming calls for other extensions if they are in the same pickup group, by dialing "Pickup Extension" feature code (by default *8).

Configure Pickup Groups

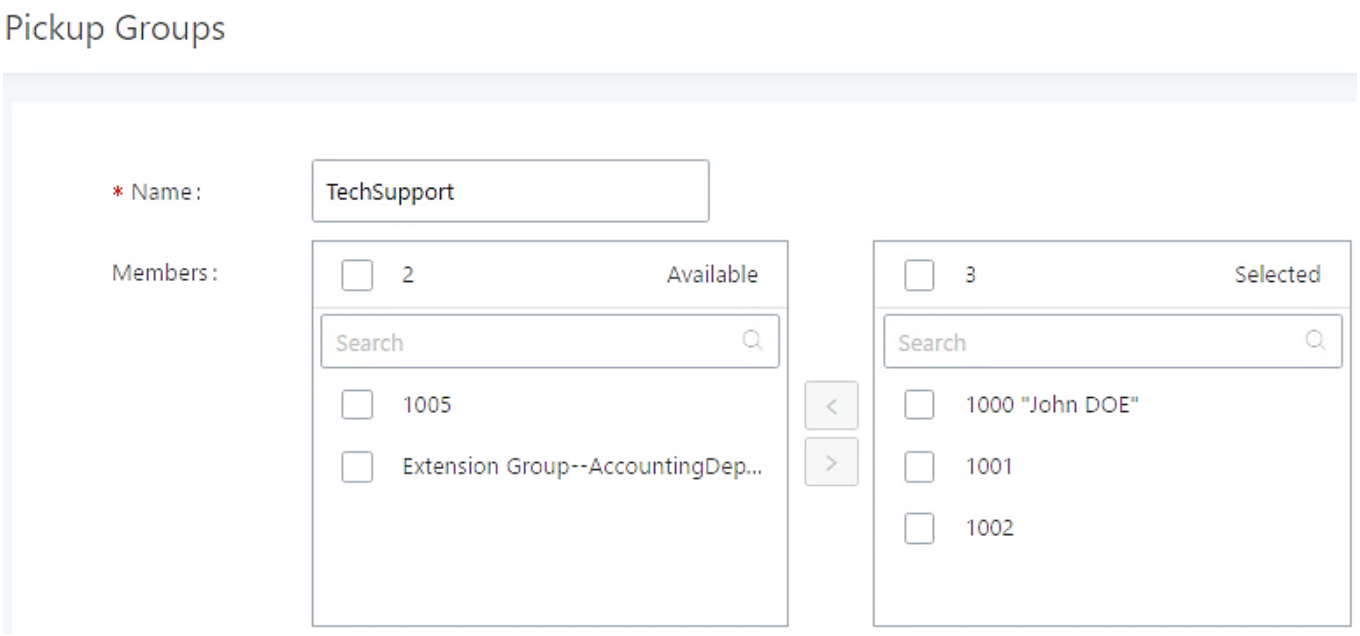


Pickup Groups interface

Pickup groups can be configured via Web GUI **Advanced Call Features→Pickup Groups**.

- Click on to create a new pickup group.
- Click the button to upload the pickup group information.
- Click the button to generate pickup group information.
- Click on to edit the pickup group.
- Click on to delete the pickup group.

Select extensions from the list on the left side to the right side.

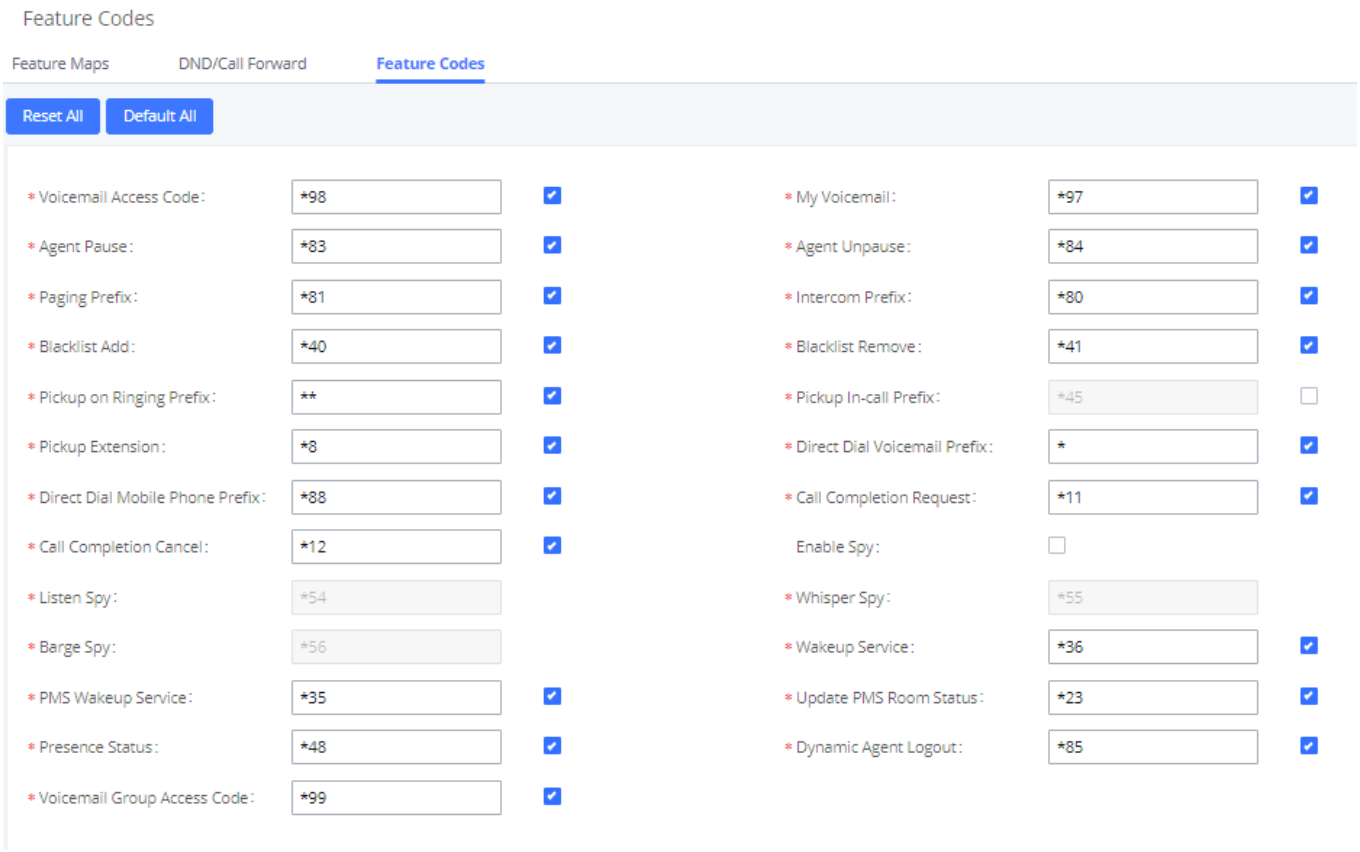


Edit Pickup Group

Configure Pickup Feature Code

When picking up the call for the pickup group member, the user only needs to dial the pickup feature code. It is not necessary to add the extension number after the pickup feature code. The pickup feature code is configurable under Web GUI **Basic Call Features→Feature Codes**.

The default feature code for call pickup extension is *8, otherwise if the person intending to pick up the call knows the ringing extension they can use ** followed by the extension number in order to perform the call pickup operation. The following figure shows where you can customize these features codes



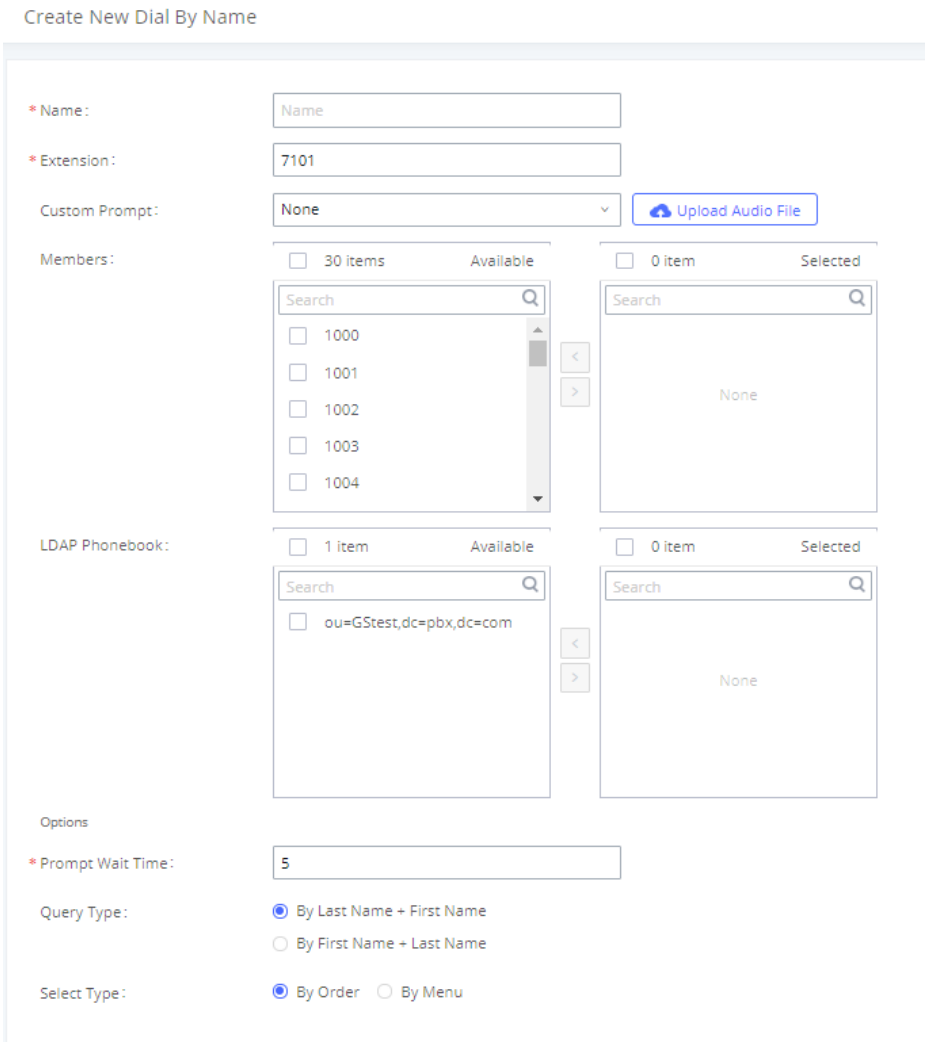
Edit Pickup Feature Code

Dial By Name

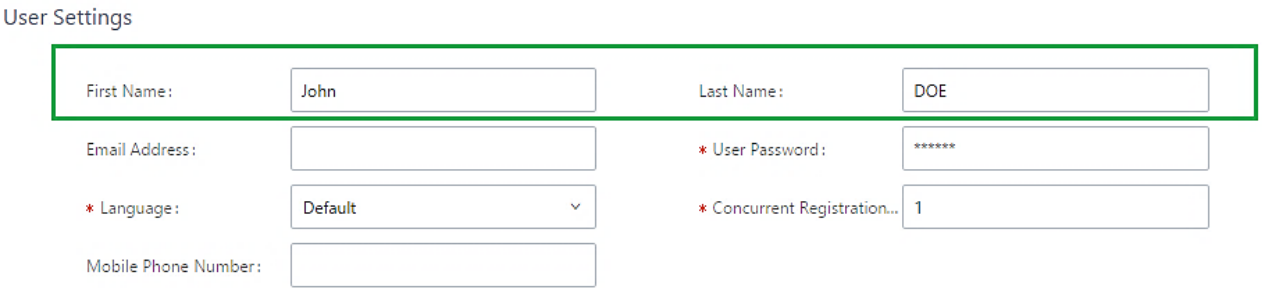
Dial by Name is a feature on the PBX that allows caller to search a person by first or last name via his/her phone's keypad. The administrator can define the Dial by Name directory including the desired extensions in the directory and the searching type by "first name" or "last name". After dialing in, the PBX IVR/Auto Attendant will guide the caller to spell the digits to find the person in the Dial by Name directory. This feature allows customers/clients to use the guided automatic system to contact the enterprise employees without having to know the extension number, which brings convenience and improves business image for the enterprise.

Dial by Name Configuration

The administrators can create the dial by name group under Web GUI **Advanced Call Features > Dial By Name**.



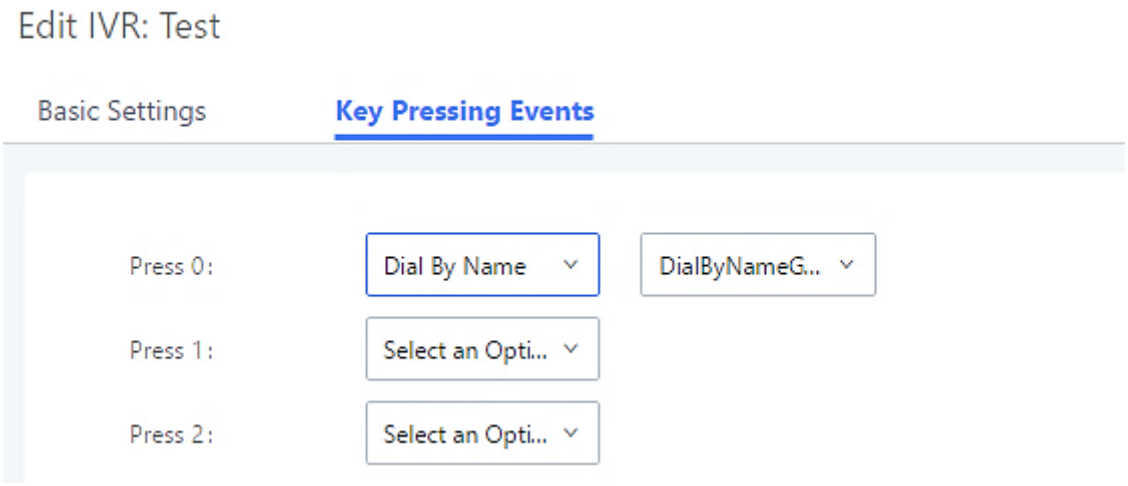
Create Dial by Name Group



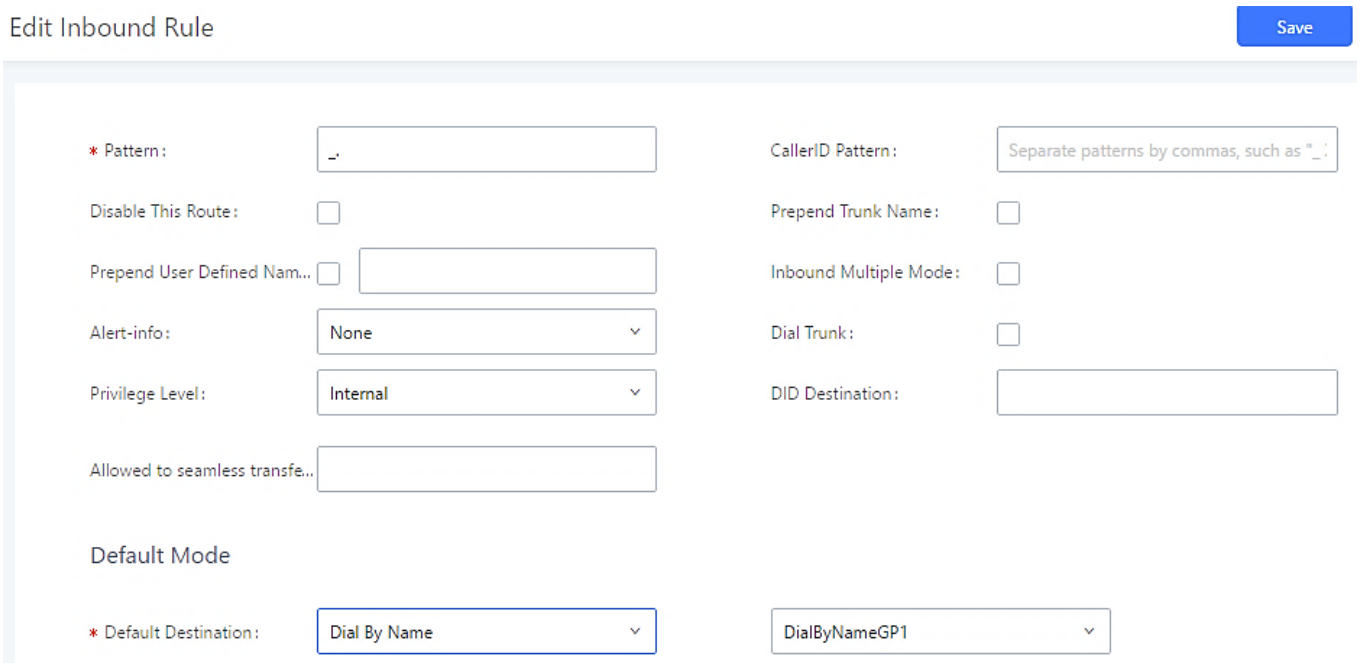
Configure Extension First Name and Last Name

1. **Name**: Enter a Name to identify the Dial by Name group.
2. **Extension**: Configure the direct dial extension for the Dial By Name group.
3. **Custom Prompt**: This option sets a custom prompt for directory to announce to a caller. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add additional record.
4. **Available Extensions/Selected Extensions**: Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have a valid first name and last name configured under Web GUI→**Extension/Trunk→Extensions** in order to be searchable in Dial By Name directory through IVR. By specifying the extensions here, the administrators can make sure unscreened calls will not reach the company employee if he/she does not want to receive them directly.

5. **Prompt Wait Time**: Configure "Prompt Wait Time" for Dial By Name feature. During Dial By Name call, the caller will need to input the first letters of First/Last name before this wait time is reached. Otherwise, timeout will occur, and the call might hang up. The timeout range is between 3 and 60 seconds.
6. **Query Type**: Specify the query type. This defines how the caller will need to enter to search the directory.
   By First Name: enter the first 3 digits of the first name to search the directory.
   By Last Name: enter the first 3 digits of the last name to search the directory.
7. **Select Type** Specify the select type on the searching result. The IVR will confirm the name/number for the party the caller would like to reach before dialing out.
   By Order: After the caller enters the digits, the IVR will announce the first matching party's name and number. The caller can confirm and dial out if it is the destination party, or press * to listen to the next matching result if it is not the desired party to call.
   By Menu: After the caller enters the digits, the IVR will announce 8 matching results. The caller can press number 1 to 8 to select and call or press 9 for results in next page.
   The Dial by Name group can be used as the destination for inbound route and key pressing event for IVR. The group name defined here will show up in the destination list when configuring IVR and inbound route. If Dial by Name is set as a key pressing event for IVR, user could use '*' to exit from Dial by Name, then re-enter IVR and start a new event. The following example shows how to use this option.



Dial By Name Group In IVR Key Pressing Events



Dial by Name Group In Inbound Rule

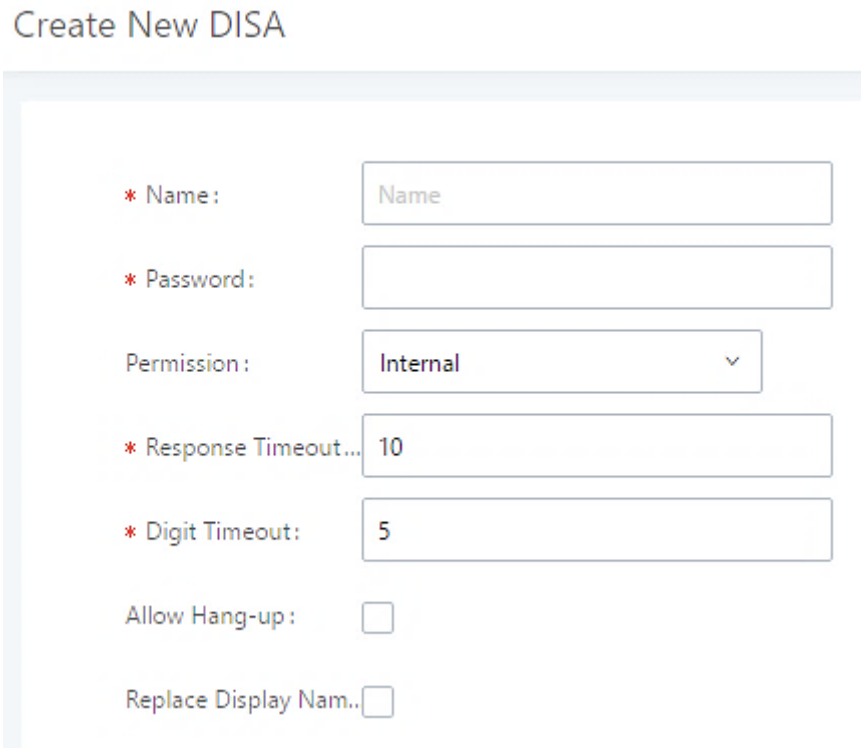
Please refer to [Username Prompt Customization] for Username Prompt Customization.

DISA

In many situations, the user will find the need to access his own IP PBX resources, but he is not physically near one of his extensions. However, he does have access to his own cell phone. In this case, we can use what is commonly known as DISA (Direct Inward System Access). Under this scenario, the user will be able to call from the outside, whether it is using his cell phone, pay phone, regular PSTN, etc. After calling into UCM630X, the user can then dial out via the SIP trunk or PSTN trunk connected to UCM630X as it is an internal extension.

The UCM630X supports DISA to be used in IVR or inbound route. Before using it, create new DISA under Web GUI **Advanced Call Features > DISA**.

- Click on to add a new DISA.
- Click on to edit the DISA configuration.
- Click on to delete the DISA.



Create New DISA

The following table details the parameters to set and configure DISA feature on UCM630X PBX.

Name	Configure DISA name to identify the DISA.
Password	Configure the password (digit only) required for the user to enter before using DISA to dial out.Note: The password must be at least 4 digits.
Permission	Configure the permission level for DISA. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the DISA, the IPPBX will compared the DISA's permission level with the outbound route's privilege level. If the DISA's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.

Response Timeout	Configure the maximum amount of time the IPPBX will wait before hanging up if the user dials an incomplete or invalid number. The default setting is 10 seconds.
Digit Timeout	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
Allow Hangup	If enabled, during an active call, users can enter the IPPBX Hangup feature code (by default it is *0) to disconnect the call or hang up directly. A new dial tone will be heard shortly for the user to make a new call. The default setting is "No".
Replace Display Name	If enabled, the IPPBX will replace the caller display name with the DISA name.

Once successfully created, users can configure the inbound route destination as "DISA" or IVR key event as "DISA". When dialing into DISA, users will be prompted with password first. After entering the correct password, a second dial tone will be heard for the users to dial out.

Callback

Callback is designed for users who often use their mobile phones to make long distance or international calls which may have high service charges. The callback feature provides an economic solution for reduce the cost from this.

The callback feature works as follows:

1. Configure a new callback on the UCM630X.
2. On the UCM630X, configure destination of the inbound route for analog trunk to callback.
3. Save and apply the settings.
4. The user calls the PSTN number of the UCM630X using the mobile phone, which goes to callback destination as specified in the inbound route.
5. Once the user hears the ringback tone from the mobile phone, hang up the call on the mobile phone.
6. The UCM630X will call back the user.
7. The user answers the call.
8. The call will be sent to DISA or IVR which directs the user to dial the destination number.
9. The user will be connected to the destination number.

In this way, the calls are placed and connected through trunks on the UCM630X instead of to the mobile phone directly. Therefore, the user will not be charged on mobile phone services for long distance or international calls.

To configure callback on the UCM630X, go to Web GUI **Advanced Call Features > Callback** page and click on . Configuration parameters are listed in the following table.

Name	Configure a name to identify the Callback. (Enter at least two characters)
CallerID Pattern	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the CallerID match this pattern so that the caller can get callback after hanging up the call.Note: If leaving as blank, all numbers are allowed to use this callback.
Outbound Prepend	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.
Delay Before Callback	Configure the number of seconds to be delayed before calling back the user.

Destination	Configure the destination which the callback will direct the caller to. Two destinations are available: IVR DISA The caller can then enter the desired number to dial out via UCM630X trunk.

Scheduled Call

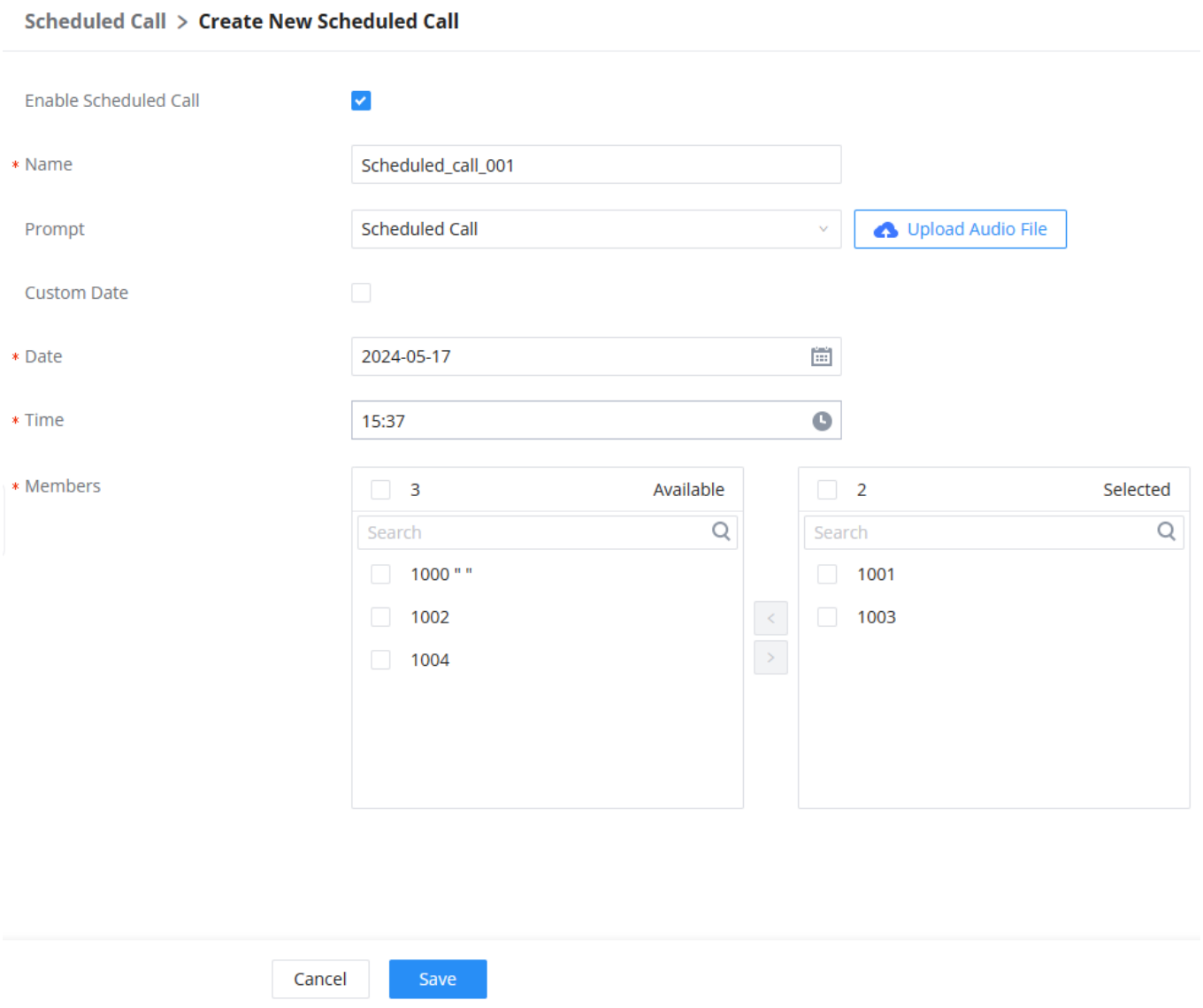
The Scheduled Call service can be used to schedule a call to any valid destination. This service is available on the UCM630X as a separated module.

There are three ways to set up a Scheduled Call service:

- Using admin login
- Using user portal
- Using feature code

Scheduled Call using Admin Login

1. Login to the UCM as admin.
2. Scheduled Call service can be found under Web GUI **Advanced Call Features > Scheduled Call**, click on "Add" to create a new scheduled call. The following window will pop up.



Create a New Scheduled Call

3. Fill out the required fields and select the members to add to the scheduled call group.

Enable Scheduled Call	Enable/disable Scheduled Call feature.
Name	Enter a name (up to 64 characters) to identify the wakeup service.
Prompt	Select/upload the prompt to play for that extension.
Custom Date	Check to select the weekday(s) to perform the scheduled call.
Date	Select the date to perfom the scheduled call.
Time	Select the time to perform the scheduled call.
Members	Select the destination extensions of the scheduled call.

4. Click and to apply the changes.

A scheduled call entry is created. The UCM will send a scheduled call to every extension in the member list at the scheduled date and time.

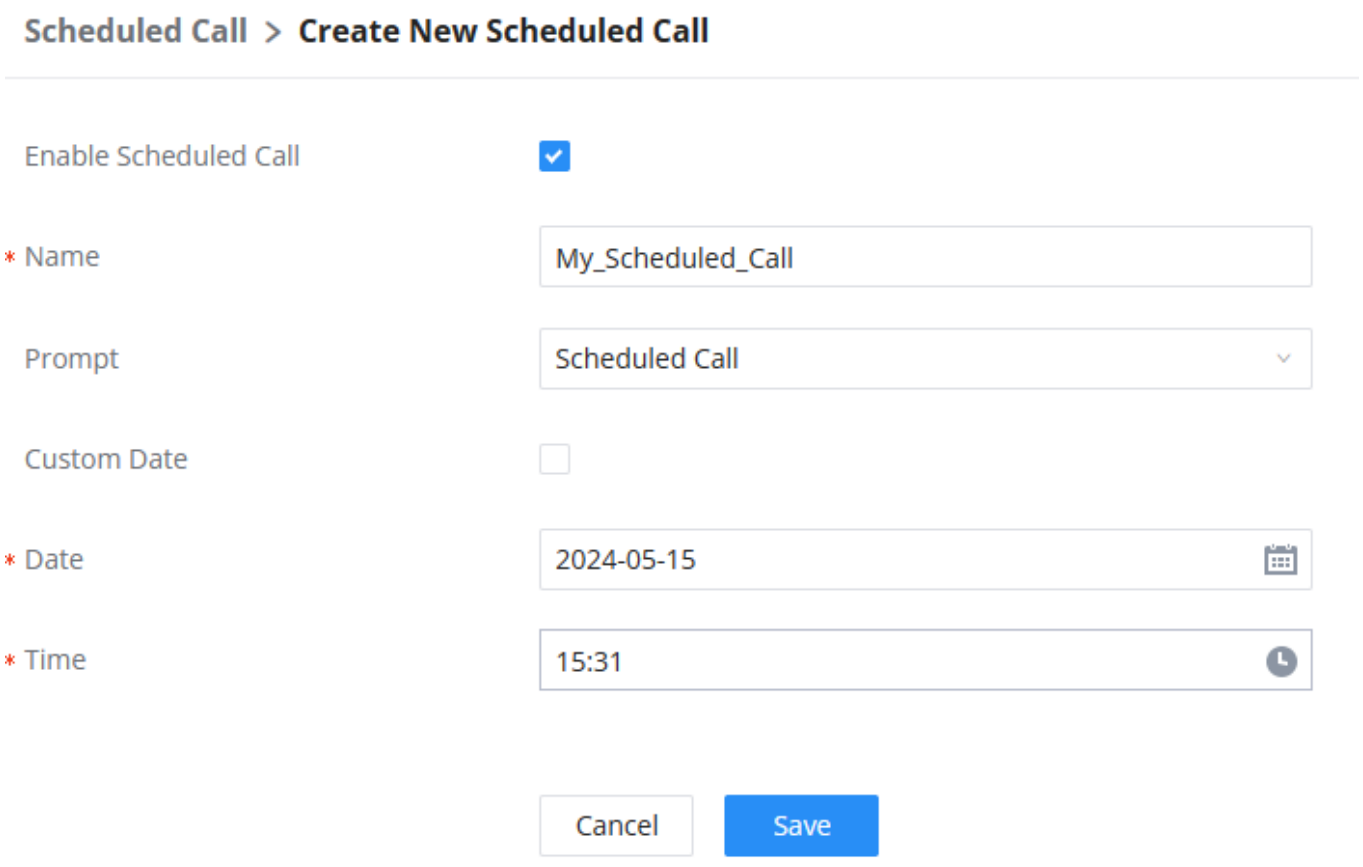
The scheduled call service has the following limitation on how many members can be added depending on UCM model.

UCM Model	Max members in a Scheduled Call
UCM6301	50
UCM6302	100
UCM6304	150
UCM6308	200

Scheduled Call from User Portal

1. Login to the user portal on the UCM630X.

2. Scheduled Call can be found under "**Advanced Call Features > Scheduled Call**", click on "Add" to create a new wakeup service.



User Portal - Create New Scheduled Call

3. Configures the Name, Prompt, Date and Time for the user to make the scheduled call to.

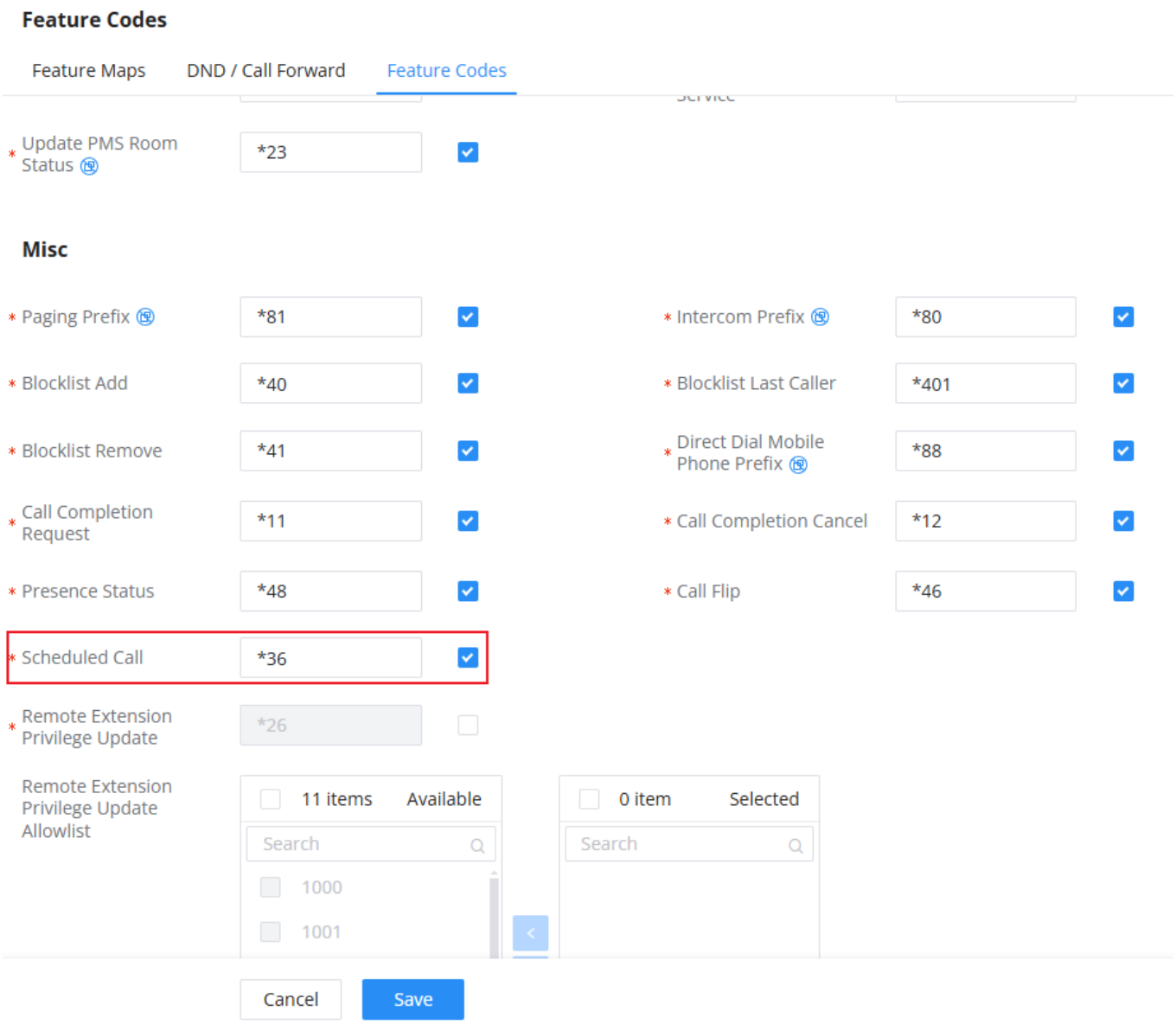
Enable Scheduled Call	Enable/disable Scheduled Call feature.
Name	Enter a name (up to 64 characters) to identify the wakeup service.
Prompt	Select the prompt to play for that extension.
Custom Date	Check to select the weekday(s) to perform the scheduled call.
Date	Select the date to perfom the scheduled call.
Time	Select the time to perform the scheduled call.

4. Click and to apply the changes.

Scheduled Call Feature Code

1. Login to the UCM as admin.

2. Enable "Scheduled Call" from the Web GUI under **Basic Call Features** > **Feature Codes** > **Feature Codes**.



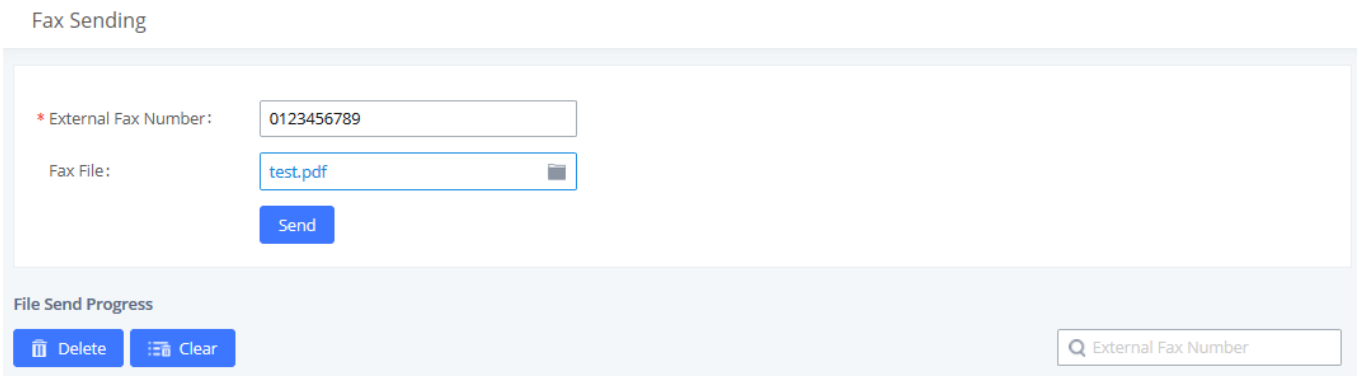
Scheduled Call Feature Code

3. Click and to apply the changes.
4. Dial "*36" which is the feature code by default to access to the UCM Scheduled Call to add, update, activate or deactivate UCM Scheduled Call.

Fax Sending

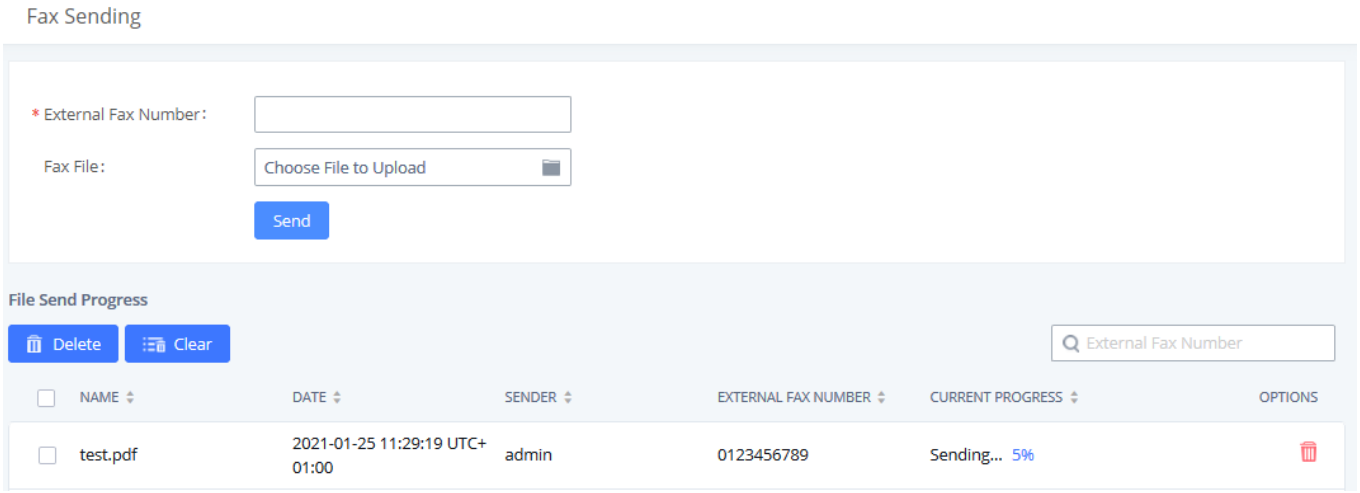
Besides the support of Fax machines, The UCM6300 supports also sending Fax via Web GUI access. This feature can be found on **Integrations** > **Fax Sending** page. To send fax, pre-setup for analog trunk and outbound route is required. Please refer to **[**ANALOG TRUNKS**], [**VOIP TRUNKS**]** and **[**Outbound Routes**]** sections for configuring analog trunk and outbound route.

After making sure analog trunk or VoIP Trunk is setup properly and UCM6300 can reach out to PSTN numbers via the trunk, on Fax Sending page, enter the fax number and upload the file to be faxed. Then click on "Send" to start. The progress of sending fax will be displayed in Web GUI. Users can also view the sending history is in the same web page.



Fax Sending in Web GUI

After that you can see the ongoing sending operation on the progress bar.



Fax Send Progress

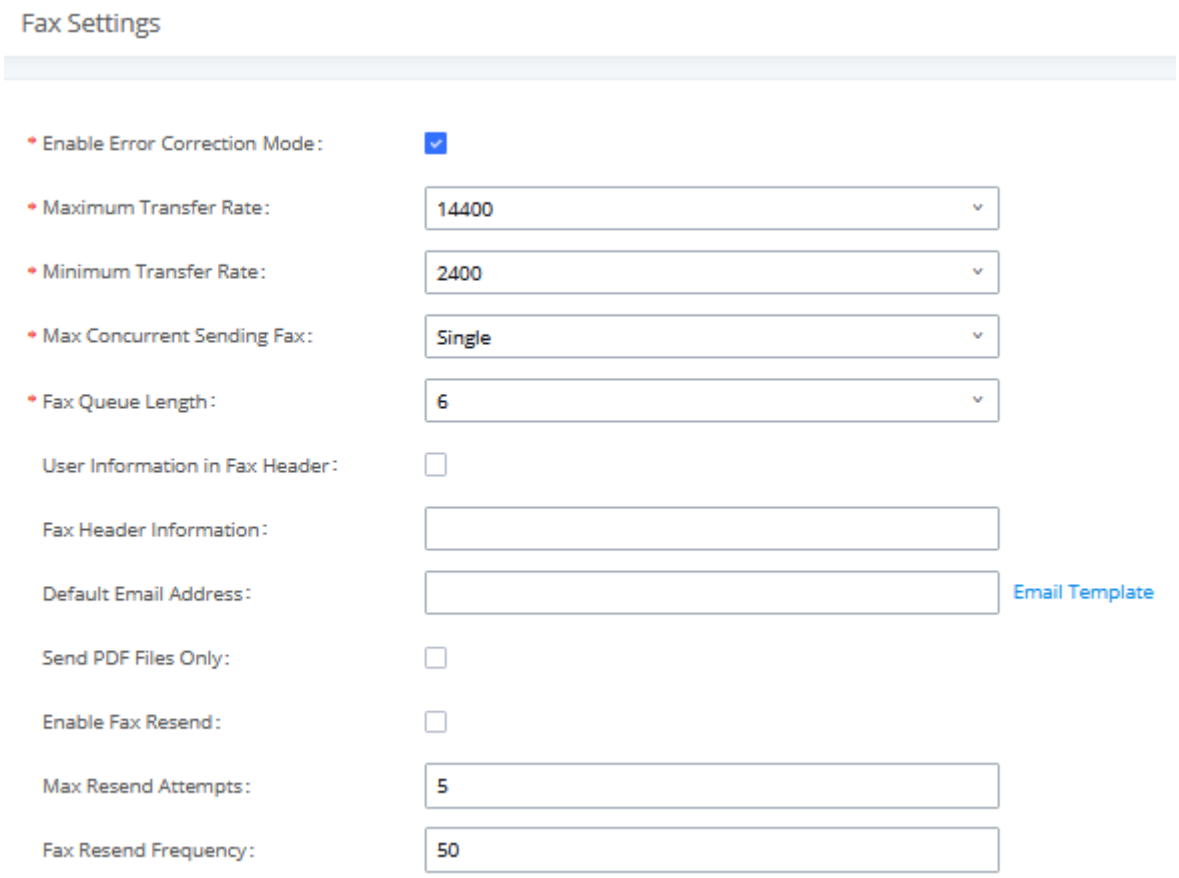
Only A3, A4, and B4 paper sizes are supported for the Fax Sending.

Fax/T.38

The UCM6300 series supports T.30/T.38Fax and Fax Pass-through. It can convert the received Fax to PDF format and send it to the configured Email address. Fax/T.38 settings can be accessed via Web GUI **Advanced Call Features** > **FAX/T.38**. The list of received Fax files will be displayed on the same web page for users to view, retrieve and delete.

Configure Fax/T.38

- Click on "Create New Fax Extension". In the popped-up window, fill the extension, name, and Email address to send the received Fax to.
- Click on **"Fax Settings"** to configure the Fax parameters.
- Click on to edit the Fax extension.
- Click on to delete the Fax extension.



Fax Settings

Parameter	Description
Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM).
Maximum Transfer Rate	Configure the maximum transfer rate during Fax rate negotiation.
Minimum Transfer Rate	Configure the minimum transfer rate during Fax rate negotiation.
Max Concurrent Sending Fax	Determines how many users can send fax at the same time.
Fax Queue Length	Maximum length of fax queue.
Fax Header Information	Adds header information to fax files.
Default Email Address	Send fax to this email address if the fax destination does not have an email address configured.
Send PDF Files Only	If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.
Enable Fax Resend	Enable Fax Resend.
Max Resend Attempts	Max Resend Attempts.
Fax Resend Frequency	Fax Resend Frequency.

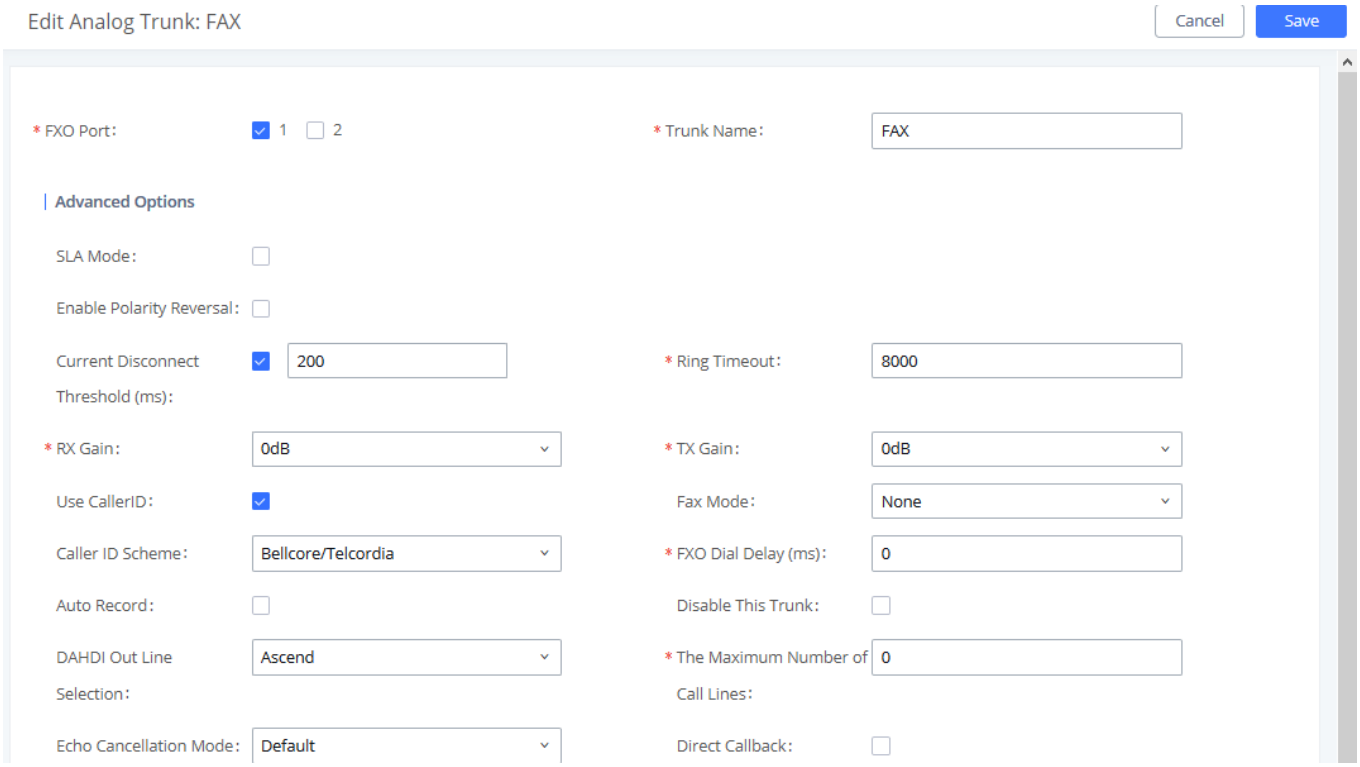
Receiving Fax

Example Configuration to Receive Fax from PSTN Line

The following instructions describe how to use the UCM6300 to receive fax from the PSTN line on the Fax machine connected to the UCM6300 FXS port.

1. Connect Fax machine to the UCM6300 FXS port.
2. Connect PSTN line to the UCM6300 FXO port.
3. Go to Web GUI→**Extension/Trunk** page.
4. Create or edit the analog trunk for Fax as below.

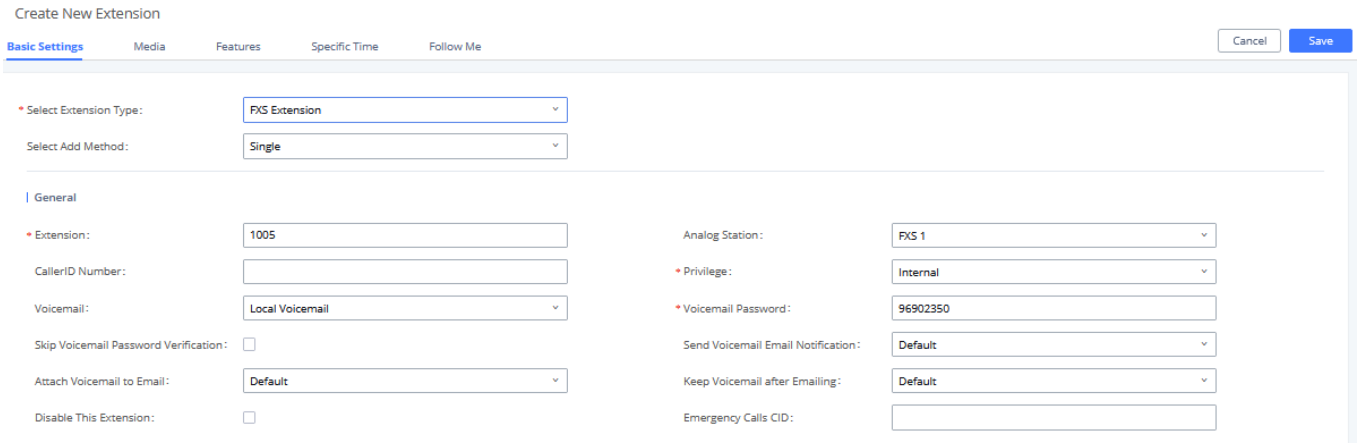
Fax Detection: Make sure the "Fax Detection" option is set to "NO".



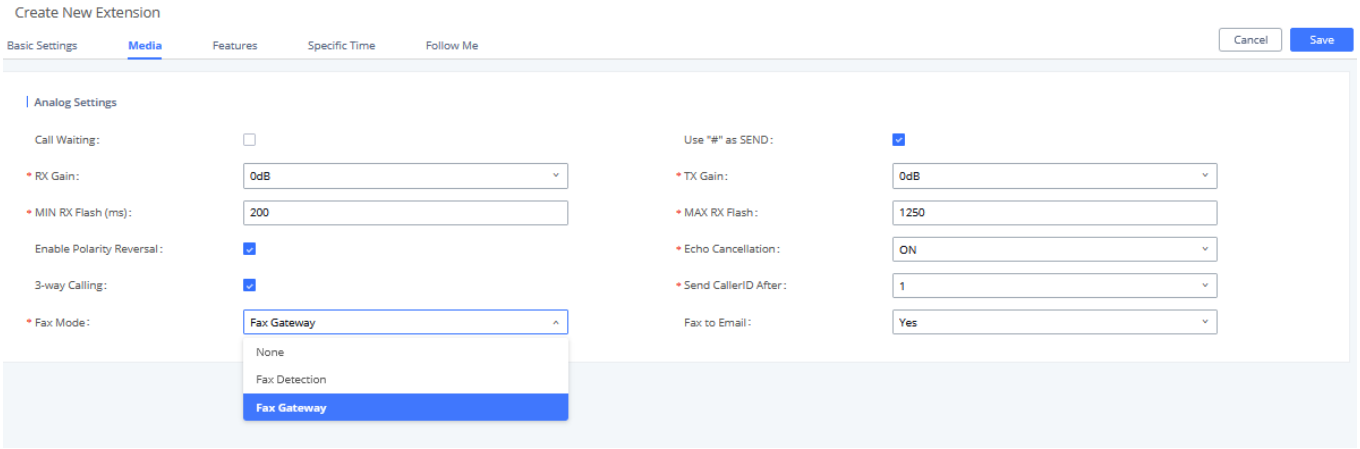
Configure Analog Trunk

5. Go to UCM6300 **Extension/Trunk** > **Extensions** page.
6. Create or edit the extension for FXS port.

- **Analog Station**: Select FXS port to be assigned to the extension. By default, it is set to "None".
- Once selected, analog related settings for this extension will show up in "**Analog Settings**" section.

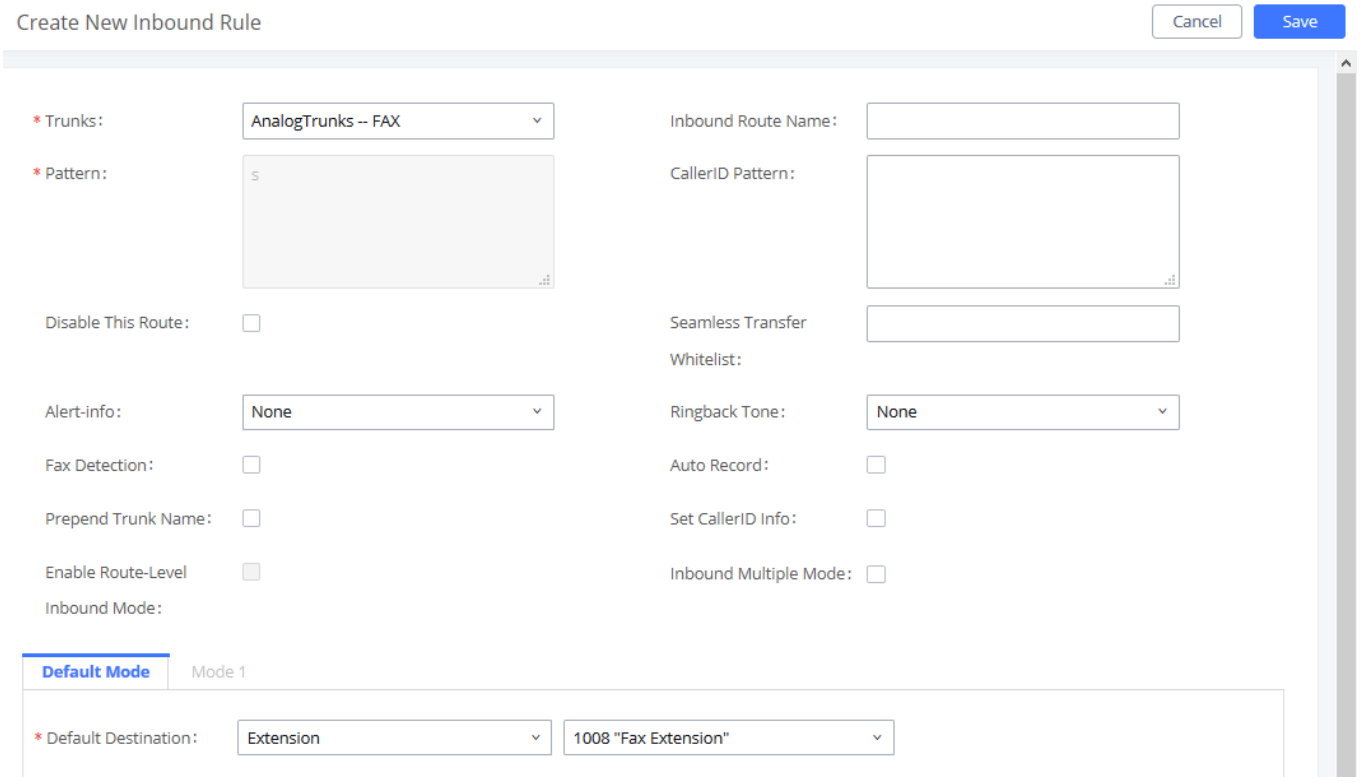


Configure Extension for Fax Machine: FXS Extension



Configure Extension for Fax Machine: Analog Settings

7. Go to **Extension/Trunk** > **Inbound Routes** page.
8. Create an inbound route to use the Fax analog trunk. Select the created extension for Fax machine in step 4 as the default destination.



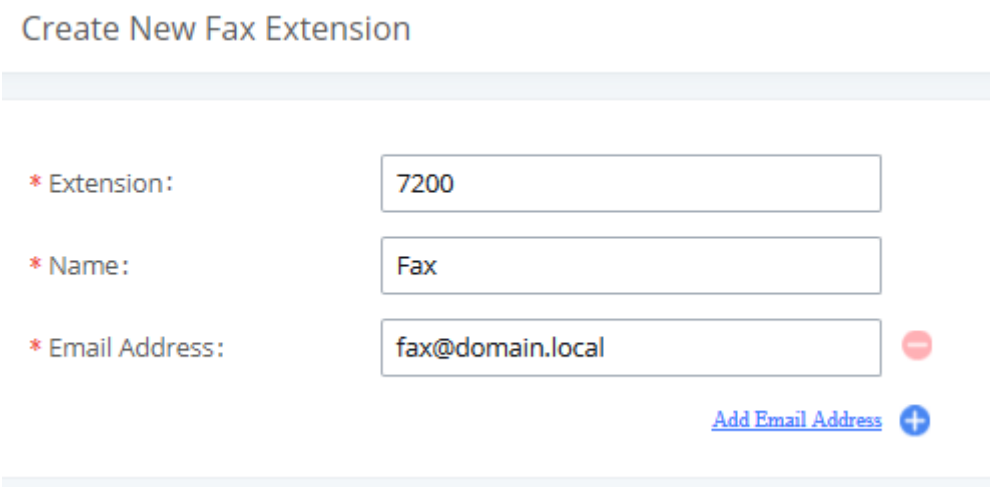
Configure Inbound Rule for Fax

Now the Fax configuration is done. When there is an incoming Fax calling to the PSTN number for the FXO port, it will send the Fax to the Fax machine.

Example Configuration for Fax-To-Email

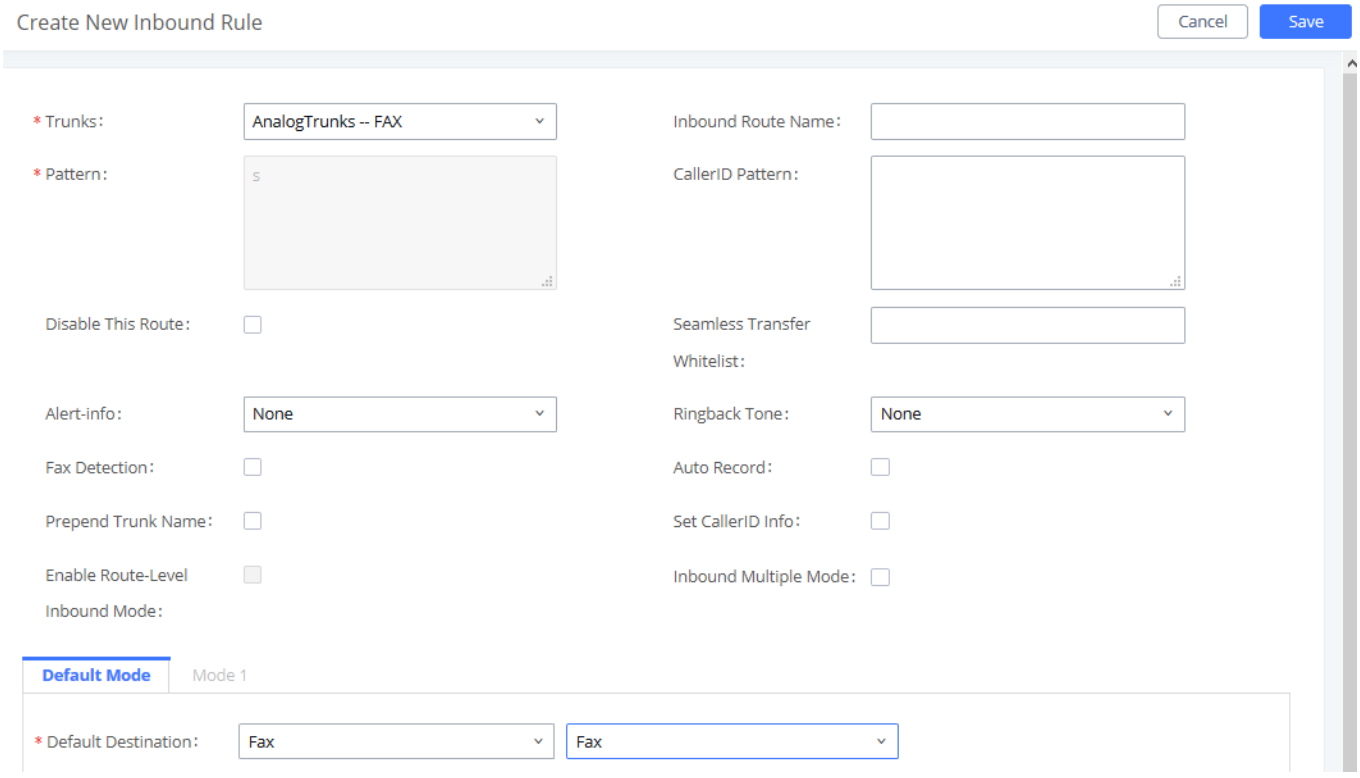
The following instructions describe a sample configuration on how to use Fax-to-Email feature on the UCM6300.

1. Connect PSTN line to the UCM6300 FXO port.
2. Go to UCM6300 Web GUI **Advanced Call Features > Fax/T.38** page. Create a new Fax extension.



Create Fax Extension

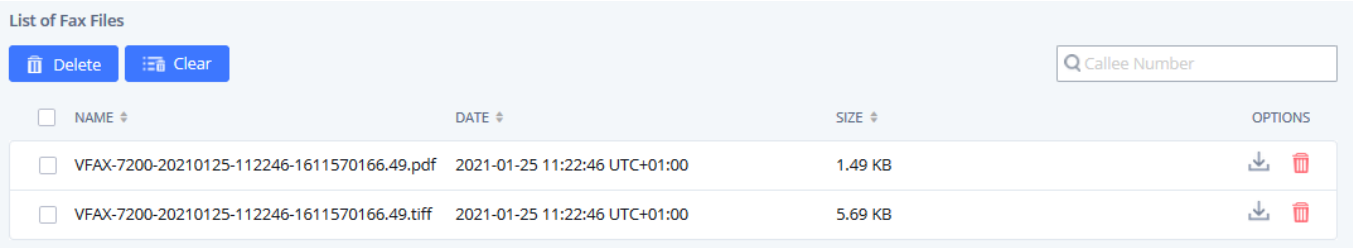
3. Go to UCM6300 **Extension/Trunk** > **Analog Trunks** page. Create a new analog trunk. Please make sure "Fax Detection" is set to "No".
4. Go to UCM6300 **Extension/Trunk** > **Inbound Routes** page. Create a new inbound route and set the default destination to the Fax extension.



Inbound Route to Fax Extension

5. Once successfully configured, the incoming Fax from external Fax machine to the PSTN line number will be converted to PDF+TIFF file and sent to the extension 7200 and email address **fax@domain.local** as attachment.

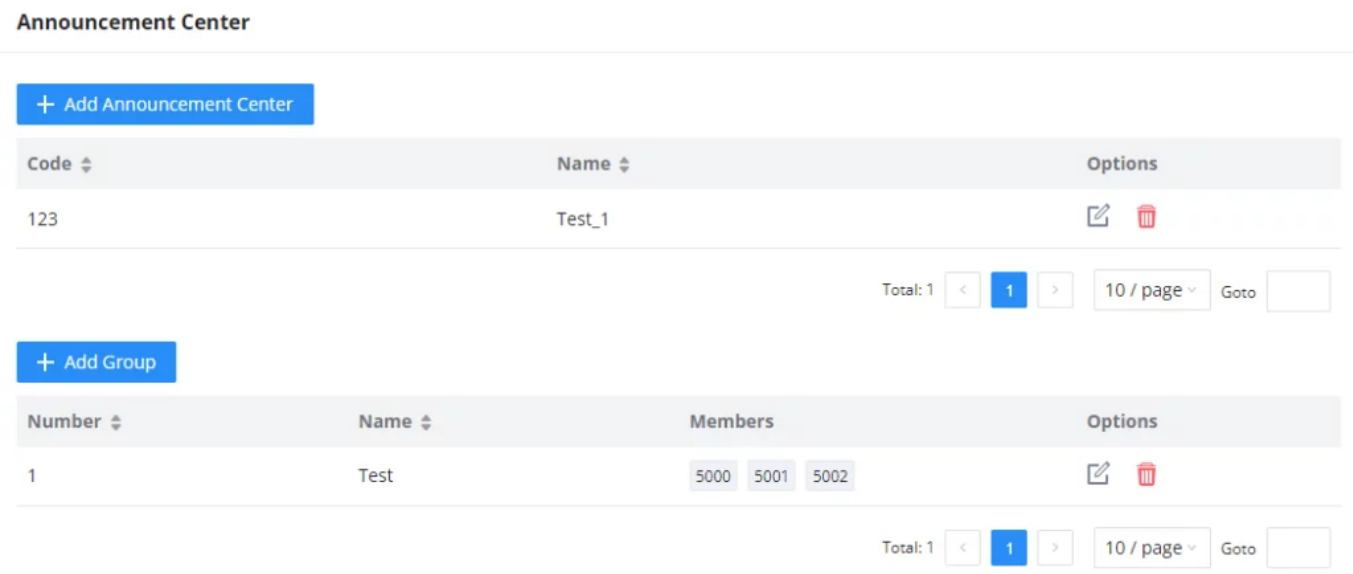
In order for the file to be sent to the email address configured on the external extension, please make sure that the email settings are well configured. Please refer to [**Email Settings**] section.



List of Fax Files

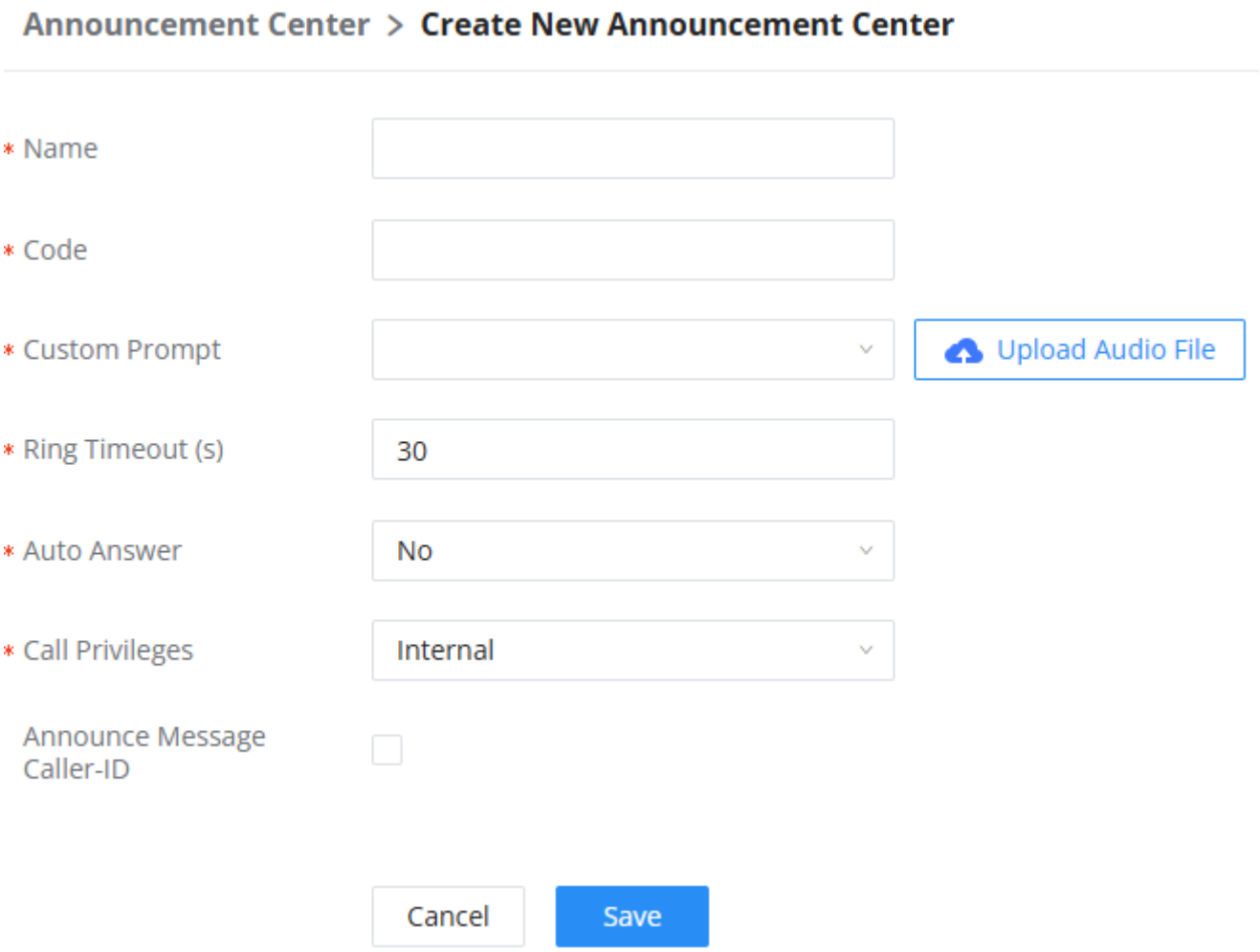
Announcement Center

The UCM630X supports Announcement Center feature which allows users to pre-record and store voice message into UCM630X with a specified code. The users can also create group with specified extensions. When the code and the group number are dialed together in the combination of **code + group number**, the specified voice message is sent to all group members and only extensions in the group will hear the voice message. To access the Announcement Center, please navigate to **Advanced Call Features > Announcement Center**.



Announcement Center

Announcement Center Settings



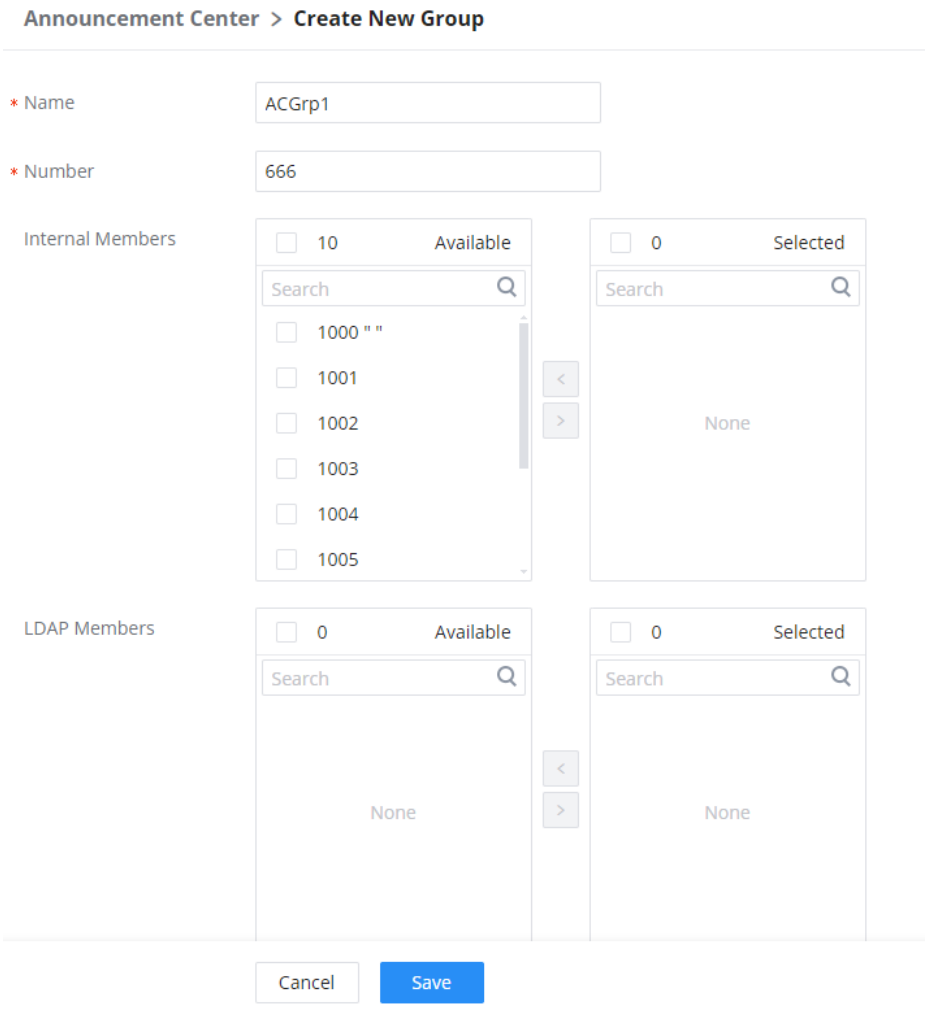
Name	Configure a name for the newly created Announcement Center to identify this announcement center.
Code	Enter a code number for the custom prompt. This code will be used in combination with the group number. For example, if the code is 55, and group number is 666. The user can dial 55666 to send prompt 55 to all members in group 666.Note: The combination number must not conflict with any number in the system such as extension number or conference number.
Custom Prompt	This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page 'Custom Prompt'. Click 'Prompt' to add additional record.Note: When uploading a custom, please ensure that the custom prompt file respect the following requirements. The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters -_
Ring Timeout	Configure the ring timeout for the group members. The default value is 30 seconds.
Auto Answer	If set to Yes, the Auto answer will be enabled by the members.
Call Privileges	Please select the permission level for outgoing calls.
Announce Message Caller-ID	If enabled, the caller's CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.

Group Settings

Name	Configure a name for the newly created group to identify the group.Note: Name cannot exceed 64 characters.
Number	Configure the group number. The group number is used in combination with the code. For example, if group number is 666, and code is 55. The user can dial 55666 to send prompt 55 to all members in group 666.Note: The combination number must not conflict with any number in the system such as extension number or conference number and cannot exceed 64 characters.
Internal Members	Choose the local extensions to add to the group.
LDAP Members	Choose the LDAP contacts to add to the group.
Custom Members	Enter the custom phone numbers to add to the group. Note: The maximum number of custom numbers which can be added are 50 custom number.

Announcement Center feature can be found under **Advanced Call Features > Announcement Center**. The following example demonstrates the usage of this feature.

1. Click to add new group.
2. Give a name to the newly created group.
3. Create a group number which is used with code to send voice message.
4. Select the extensions to be included in the group, who will receive the voice message.



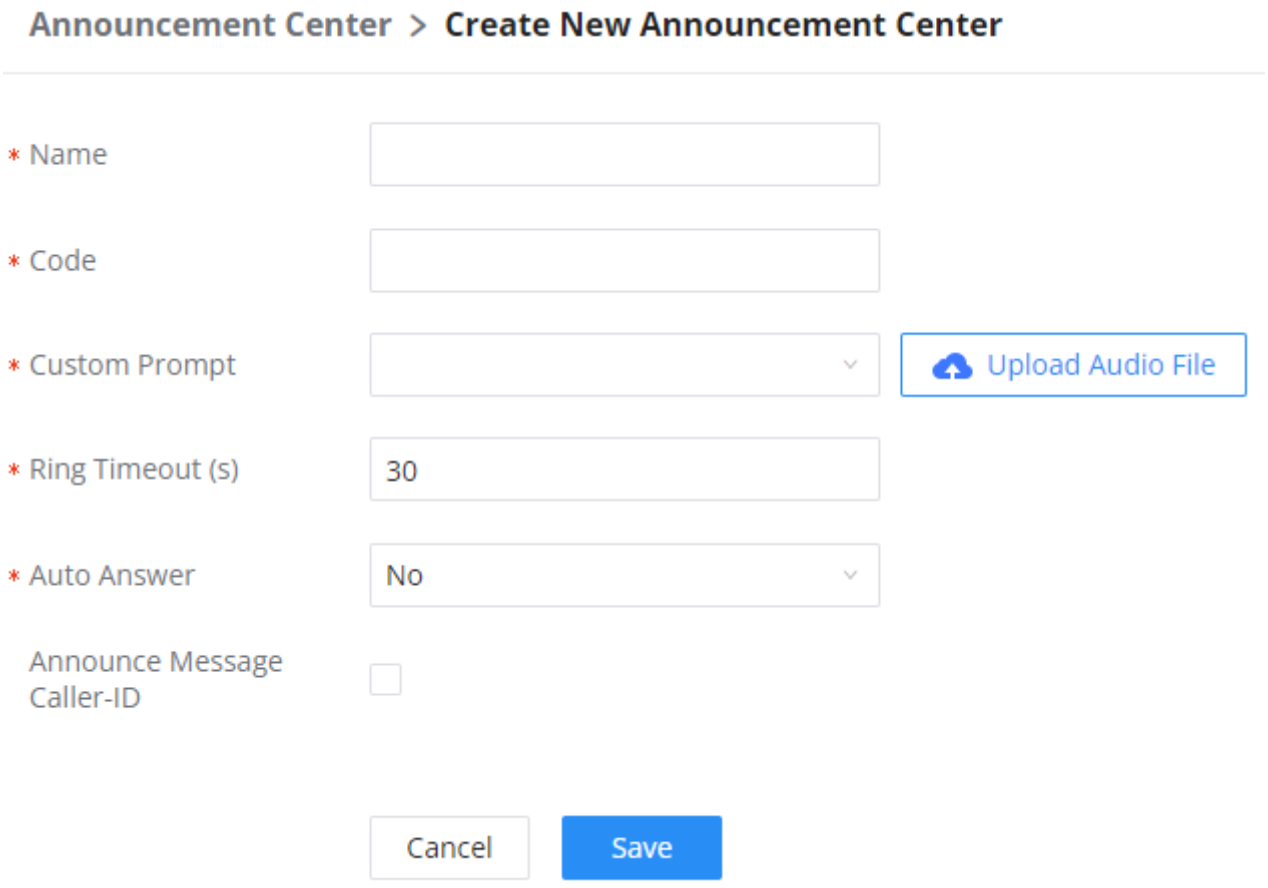
Announcement Center Group Configuration

Name	Configure a name for the newly created group to identify the group.Note: Name cannot exceed 64 characters.

Number	Configure the group number. The group number is used in combination with the code. For example, if group number is 666, and code is 55. The user can dial 55666 to send prompt 55 to all members in group 666.Note: The combination number must not conflict with any number in the system such as extension number or conference number and cannot exceed 64 characters.
Internal Members	Choose the local extensions to add to the group.
LDAP Members	Choose the LDAP contacts to add to the group.
Custom Members	Enter the custom phone numbers to add to the group. Note: The maximum number of custom numbers which can be added are 50 custom number.

In this example, group "Test" has number 666. Extension 1000, 1001 and 1002 are in this group.

5. Click to create a new Announcement Center.
6. Give a name to the newly created Announcement Center.
7. Specify the code which will be used with group number to send the voice message to.
8. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click "Prompt" link and follow the instructions in that page.

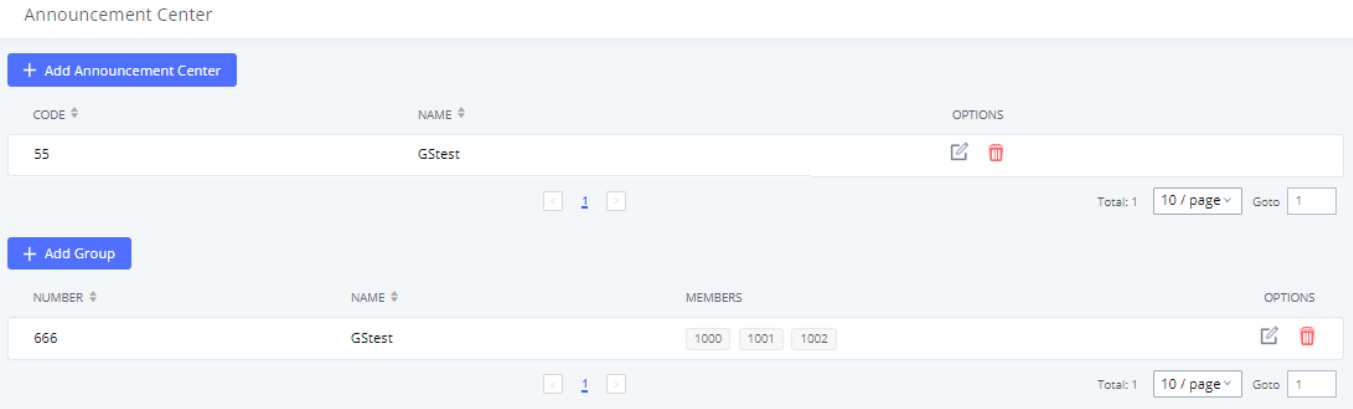


Announcement Center Code Configuration

Name	Configure a name for the newly created Announcement Center to identify this announcement center.
Code	Enter a code number for the custom prompt. This code will be used in combination with the group number. For example, if the code is 55, and group number is 666. The user can dial 55666 to send prompt 55 to all members in group 666.Note: The combination number must not conflict with any number in the system such as extension number or conference number.

Custom Prompt	This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page 'Custom Prompt'. Click 'Prompt' to add additional record.Note: When uploading a custom, please ensure that the custom prompt file respect the following requirements. The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters -_
Ring Timeout	Configure the ring timeout for the group members. The default value is 30 seconds.
Auto Answer	If set to Yes, the Auto answer will be enabled by the members.
Call Privileges	Please select the permission level for outgoing calls.
Announce Message Caller-ID	If enabled, the caller's CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the UCM630X. All the members in group 666 which are extension 1000, 1001 and 1002 will receive this voice message after they pick up the call.



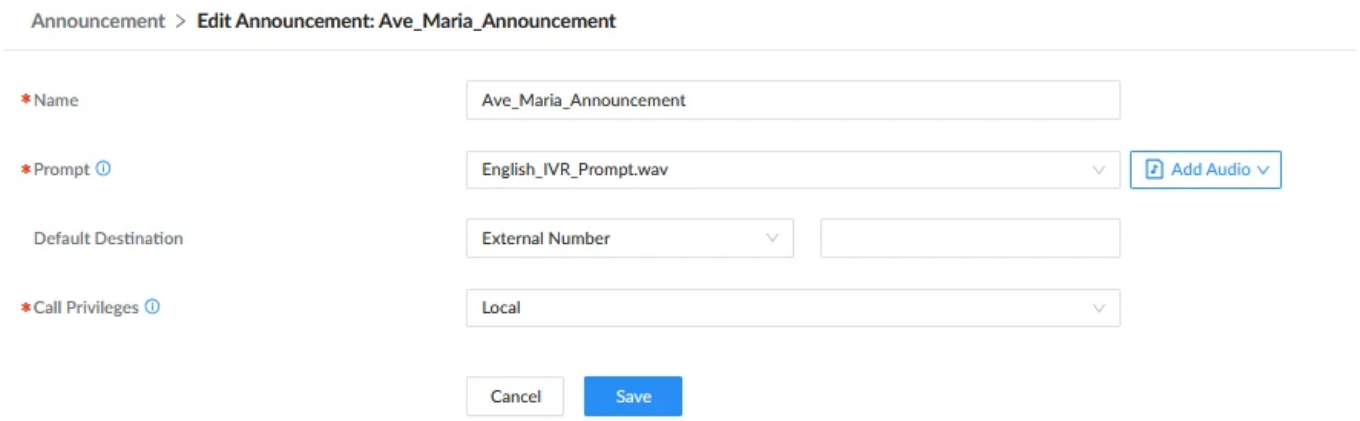
Announcement Center Example

Announcement

The Announcement feature (not to be confused with Announcement Paging and Announcement Center) allows users to set an unskippable audio prompt to play to callers before automatically routing them to a configured destination. Announcements can be assigned as a destination in the Inbound Routes page.

To configure an Announcement, follow the steps below:

1. Navigate on the Web GUI to **Advanced Call Features -> Announcement**.
2. Click on the **Add** button to create a new announcement entry.
3. Configure the required fields including **Name**, **Prompt**, **Default Destination**, and **Call Privileges** (when routing to external numbers).
4. Save and apply the configuration.



The table below describes the configuration parameters available when creating or editing an Announcement:

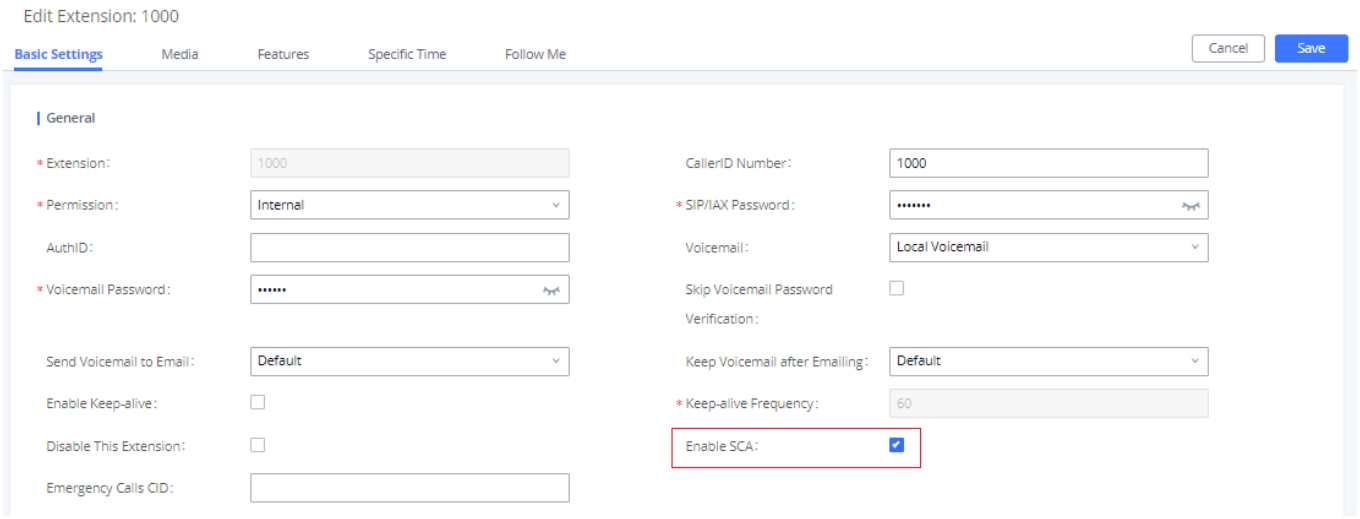
Parameter	Description
Name	Configure a unique name to identify the announcement entry.
Prompt	Select the audio file to play to the caller. Users can choose from the following options via the Add Audio dropdown: Existing Prompt: Select an existing audio file already saved on the PBX. Upload Prompt: Upload a pre-recorded audio file directly from the local computer. TTS Generation: Use the built-in Text-to-Speech (TTS) feature to generate a custom voice audio prompt from entered text.
Default Destination	Select the routing destination after the announcement audio finishes playing. Supported destinations include: Extension: Route to a specific system extension. Multimedia Meeting: Direct the caller into a meeting room. Voicemail / Voicemail Group: Route directly to a voicemail box or group. IVR: Send the call to an Interactive Voice Response system. Ring Group: Direct the call to ring a defined group of extensions. Queues: Place the call into a call queue. Fax: Route to a fax extension. DISA: Direct to Direct Inward System Access. Dial By Name: Route to the directory dial-by-name system. External Number: Route the call to an external phone number over an outbound trunk. Hang-up: Terminate the call immediately after the prompt finishes.
Call Privileges	Configures the permission level required when the Default Destination is set to an External Number. This ensures the outbound call complies with configured outbound route permission restrictions (e.g., Internal, Local, National, International).

SCA (Shared Call Appearance)

SCA (Shared Call Appearance) functionality has been added to the UCM. With SCA, users can assign multiple devices to one extension, configure endpoints to monitor that extension, make actions on behalf of that extension such as viewing call status and placing and receiving calls, and even barging into existing calls. To configure the SCA functionality, please follow the steps below:

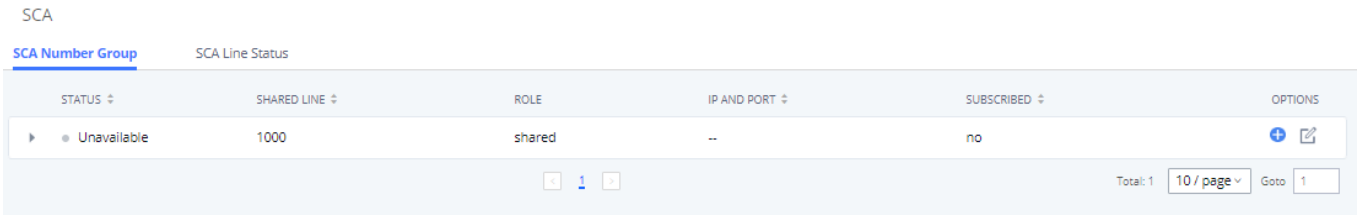
1. Users can enable SCA by navigating to the Extensions page, editing the desired extension, and enabling the option SCA.

With SCA enabled, the Concurrent Registrations field can only have a value of 1.



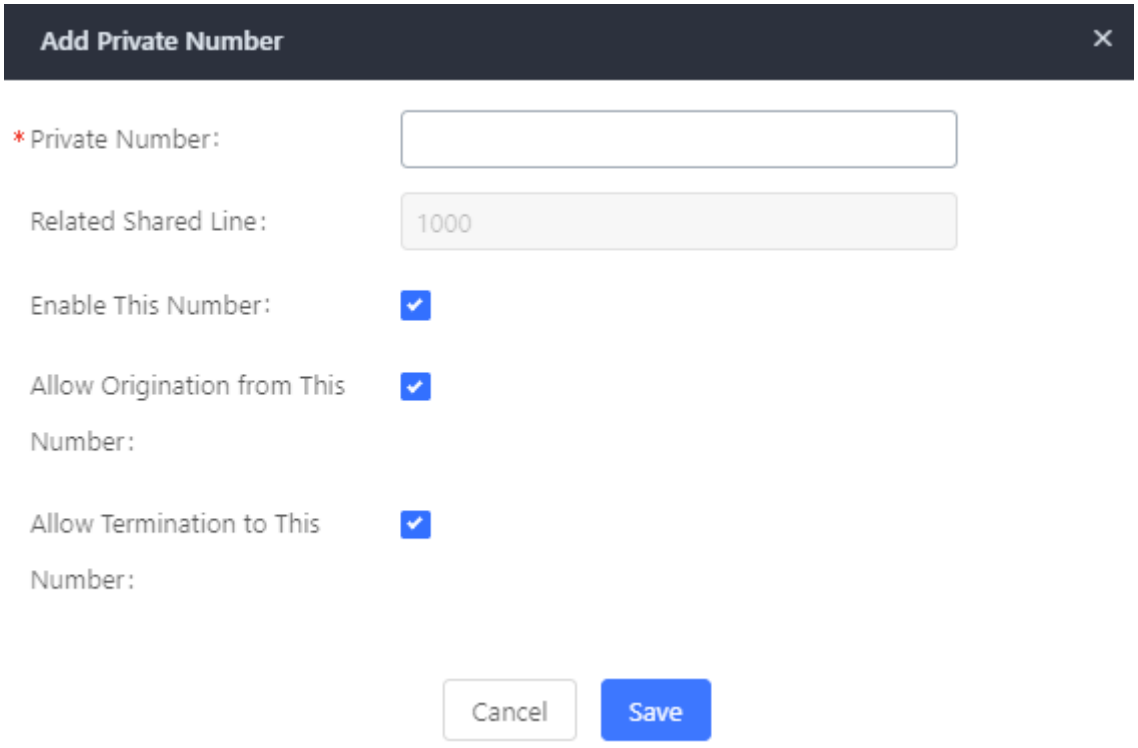
Enabling SCA option under Extension's Settings

2. After enabling the option, navigate to **Advanced Call Features -> SCA**. The newly enabled SCA extension will be listed. Click the "+" button under the Options column to add a number that will share the main extension's call appearance, which will be called private numbers.



SCA Number Configuration

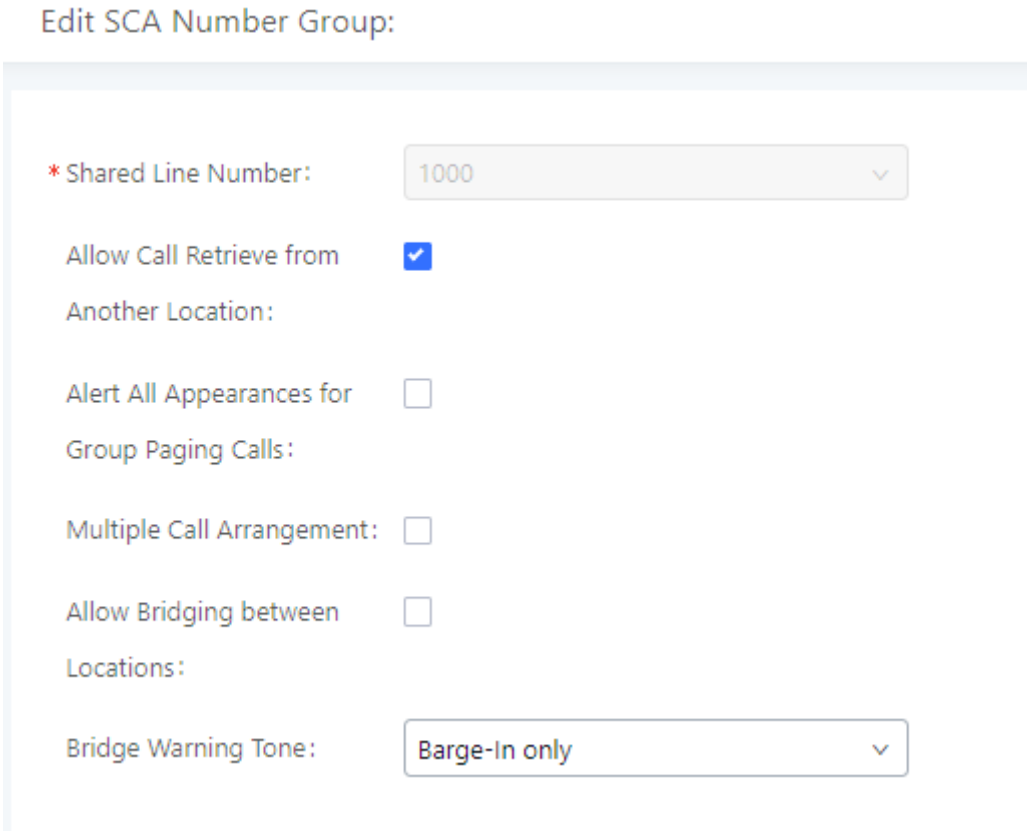
3. Configure the private number as desired.



SCA Private Number Configuration

4. Once the private number has been created, users must now register a device to it. To properly register a device to the private number, use the configured private number as the SIP User ID. Auth ID and

Password will be the same as the main extensions. Once registration is complete, SCA is now configured.



SCA Options

5. Next, configure the VPK or MPK to Shared for both the main extension and the private number. SCA is now configured for both endpoint devices.

The following table describe the SCA Number configuration setting:

Private Number	Configures the private number for the SCA.
Related Shared Line	Display the related shared line.
Enable this number	Whether enable this private number. If not enabled, this private number is only record in DB, it will not affect other system failure.
Allow Origination from This Number	Enable this option will allow calling from this private number.By default, it is enabled.
Allow Termination to This Number	Enable this option will allows calls to this private number. By default, it is enabled.

When editing the SCA number, additional options will be displayed. The following table explains all the additional options:

Shared Line Number	While SCA is enabled, this number will be the same as the extension number.
Allow Call Retrieve from Another Location	Allows remote call retrieval. Must be enabled in public hold. By default, it is enabled.
Alert All Appearances for Group Paging Calls	Allows all SCA group members to ring when the SCA shared number is paged. If disabled, only the SCA shared number will ring when paged. By default, it is disabled.
Multiple Call Arrangement	Allows simultaneous calls in an SCA group. By default, it is disabled.

Allow Bridging between Locations	Allows location bridging for SCA group. Must be enabled when using the Barge-In feature. By default, it is disabled.
Bridge Warning Tone	Configures the notification in the bridge when another party join. None: No notification sound. Barge-In only: Notification sound will play when another party join. Barge-In and Repeat: Notification sound will play when another party joins and repeat every 30 seconds.

Emergency Calls

UCM supports configuration and management of numbers to be called in emergency situation, thus bypassing the regular outbound call routing process and allowing users in critical situation to dial out for emergency help with the possibility to have redundant trunks as point of exit in case one of the lines is down.

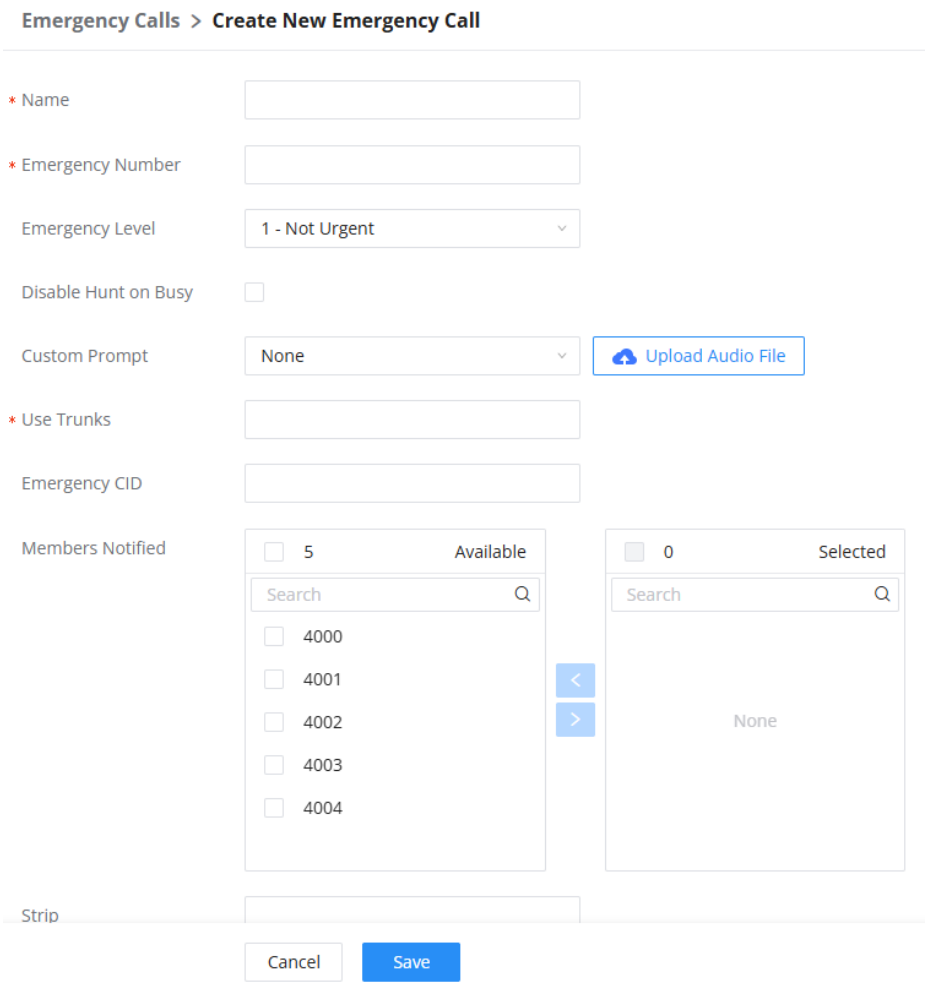
UCM63xx series are fully compliant with Kari's Law and Ray Baum's Act, for more information, please refer to the following links:

https://www.fcc.gov/general/9-1-1-and-e9-1-1-services

Emergency Calls

To configure emergency numbers, users need to follow below steps:

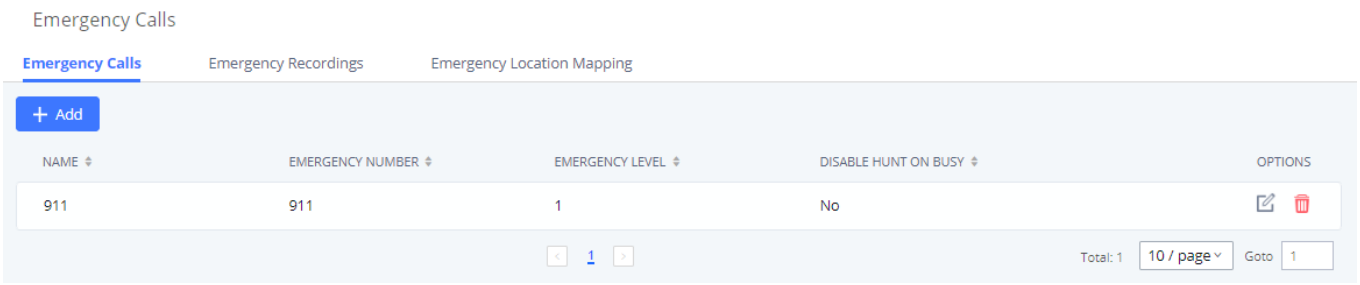
1. Navigate on the web GUI under **Advanced Call Features** > **Emergency Calls**"
2. Click on A close up of a sign
   Description generated with high confidence to add a new emergency number.
3. Configure the required fields "Name, Emergency Number and Trunk(s) to be used to reach the number".
4. Save and apply the configuration.



Emergency Number Configuration

The table below gives more description of the configuration parameters when creating emergency numbers.

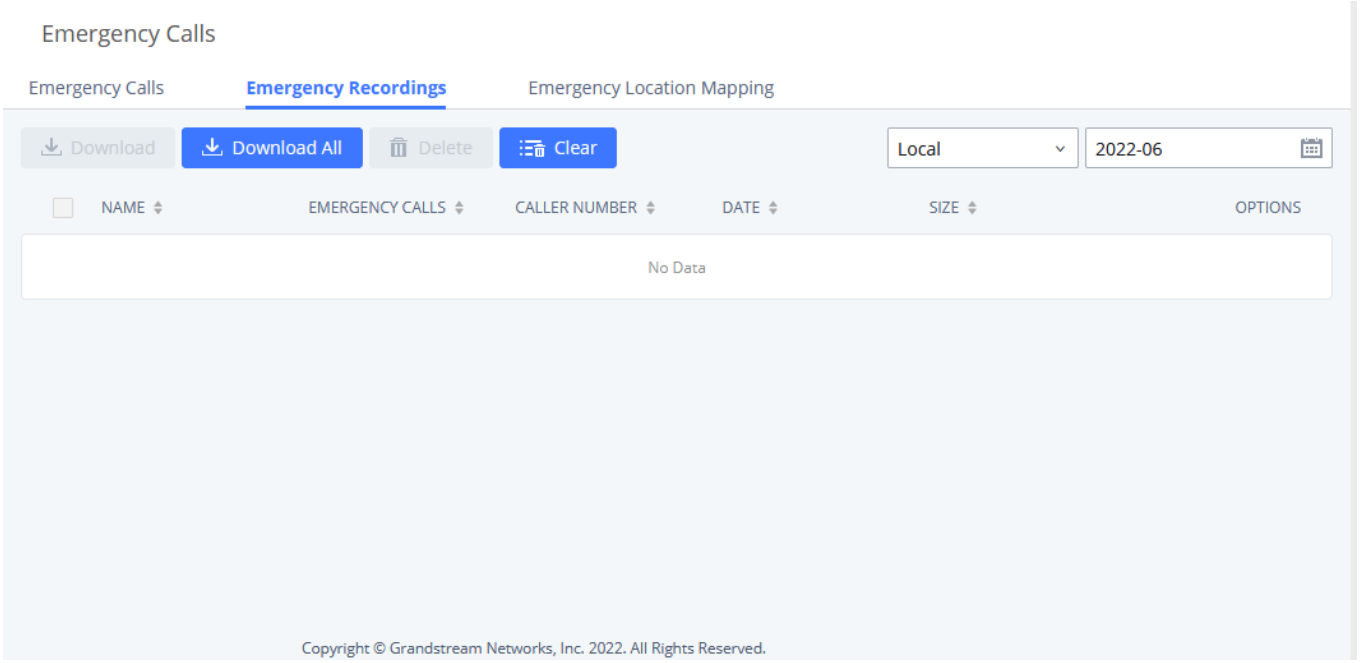
Name	Configure the name of the emergency call.For example, "emergency911","emergency211" and etc.
Emergency Number	Config the emergency service number. For example,"911","211" and etc.
Emergency Level	Select the emergency level of the number. Level "3" means the most urgent.
Disable Hunt on Busy	If this option is not enabled, when the lines of trunks which the coming emergency call routes by are completely occupied, the line-grabbing function will automatically cut off a line from all busy lines so that the coming emergency call can seize it for dialing out. This option is not enabled by default.
Custom Prompt	This option sets a custom prompt to be used as an announcement to the person receiving an emergency call. The file can be uploaded from the page "Custom Prompt". Click "Prompt" to add additional record.
Use Trunks	Select the trunks for the emergency call. Select one trunk at least and select five trunks at most.
Emergency CID	Used for emergency calls. The peer device will display the call number. Extension emergency CID takes priority over this settings. If that is not configured for the dialing extension, this value will be used by default.
Members Notified	Select the members who will be notified when an emergency call occurs.Note: You can select up to 30 members to notify.
Strip	Specify the number of digits that will be Stripped from the beginning of the dialed number before the call is placed via the selected trunk.
Prepend	Specify the digits to be Prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Auto Record	When enabled, emergency call will be automatically recorded.
Send Recording File	When enabled recording files will be sent to the configured email address.
Email Address	The email address to where the recording files will be sent.



911 Emergency Sample

Emergency Recordings

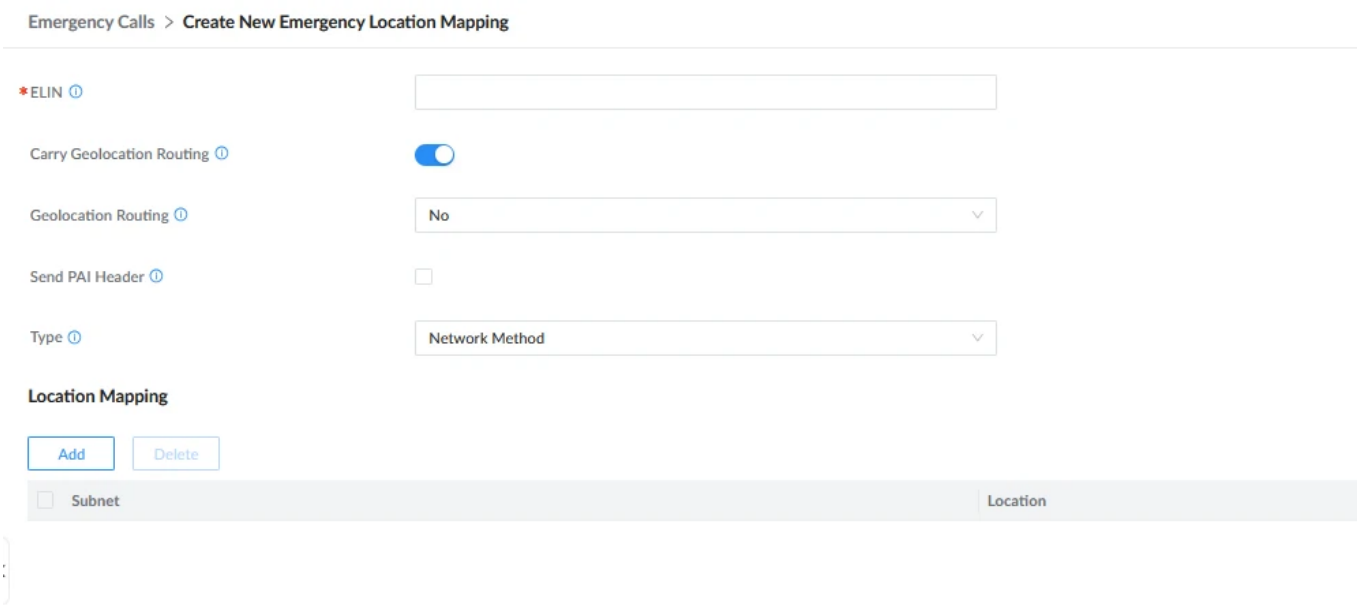
UCM6300 Series allows recording emergency calls and they can be found under **Advanced Call Feature -> Emergency Calls -> Emergency Recordings**



Emergency Recordings

Emergency Location Mapping

In compliance with Kari's Law and the Ray Baum's Act, UCM's Emergency Calls feature supports emergency location mapping. This allows users to associate subnets or extensions with emergency location identification numbers (ELINs), which are used by E911 service providers to determine the precise location of callers. These options can be found under **Advanced Call Features -> Emergency Calls -> Emergency Location Mapping**.



When creating or configuring an Emergency Location Mapping entry, users can set the parameters described in the table below:

Parameter	Description
ELIN	The emergency location identification number registered with the E911 provider. This number will be sent out as the emergency call's caller ID (CID) number.

Carry Geolocation Routing	If enabled, the UCM sends Geolocation-Routing and Geolocation headers in SIP messages, allowing downstream service providers and vendors to make location-based routing policy decisions for emergency calls.
Geolocation Routing	Toggles whether to include the Geolocation header in the emergency call SIP INVITE message. The Location field value will be used as the Geolocation header value.
Send PAI Header	PAI stands for P-Asserted-Identity. Once enabled, the ELIN number will be sent via the PAI header field to ensure accurate location tracking for emergency services. This PAI header field takes precedence over the PAI header field configured on the trunks.
Type	Selects the mapping method used to identify the caller's location: Network Method: Click Add to map specific IP subnets to location descriptions. Extension Method: Click Add to map specific extension numbers to location descriptions.

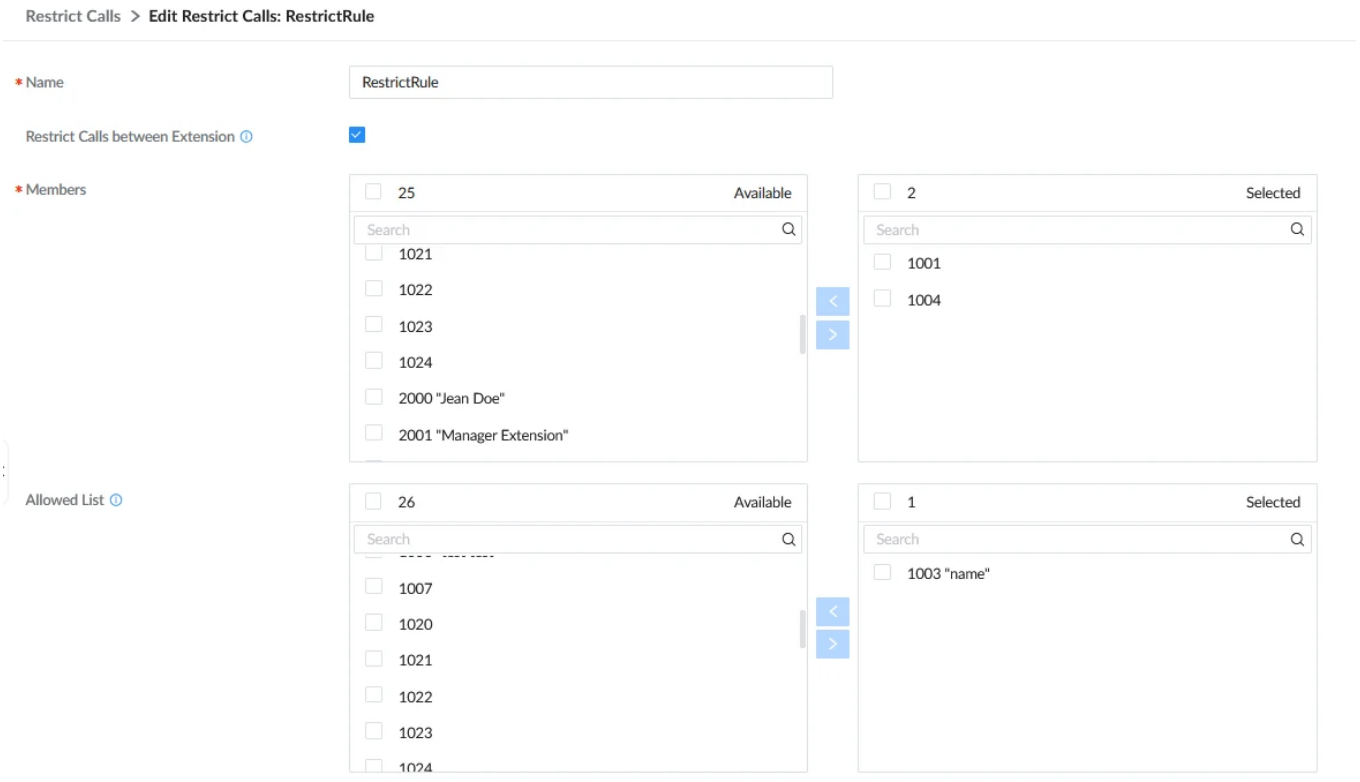
Please note that ELIN Mapping is supported only on peer trunks. It would not apply on register trunks.

Restrict Calls

The **Restrict Calls** feature allows administrators to control outgoing call permissions for specific internal extensions. When a rule is enabled, users designated as **Members** are restricted to placing outbound calls only to the extensions listed in the **Allowed List**.

This section describes the configuration of this feature in the **Advanced Call Features -> Restrict Calls** page.

This feature only restricts outbound calls placed by assigned Members. Non-allowed extensions can still place incoming calls to these Members. For strict two-way restriction between two groups, you must create two separate Restrict Calls rules.



Restrict Calls

Configure Restrict Calls

- Click **Add** to create a new Restrict Calls rule.
- Click the **Edit** icon to modify an existing rule.
- Click the **Delete** icon to remove a rule.

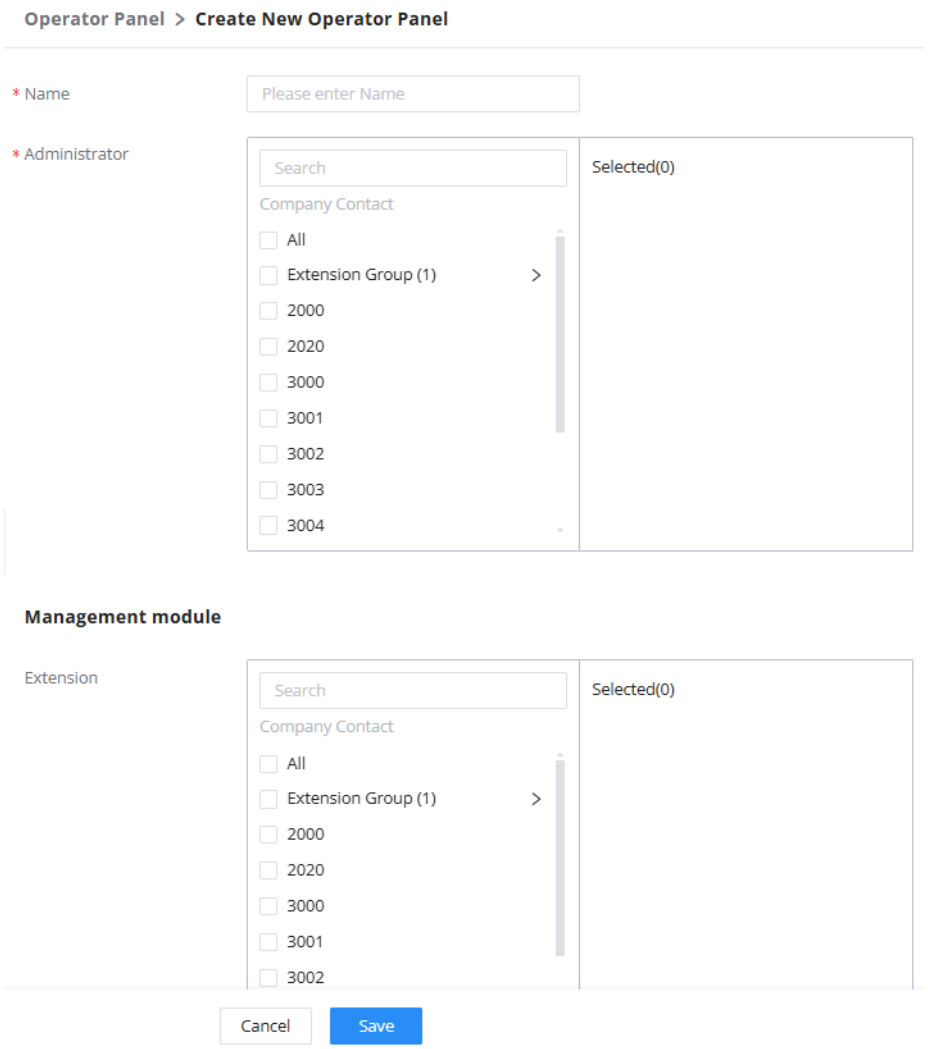
When creating or editing a rule, users can configure the following:

Name	Enter a descriptive name for the Restrict Calls rule.
Restrict Calls Between Extension	Toggles the restriction rule on or off.Enabled: Applies the rule. Members can only place outbound calls to numbers in the Allowed List.Disabled: Bypasses the rule entirely. Members will have no outbound call restrictions. (Enabled by default)
Members	Select the internal extensions whose outbound calling ability will be restricted when the rule is enabled.
Allowed List	Select the specific internal extensions that the Members are permitted to call.

Operator Panel

Operator Panel settings can be accessed via Web GUI **> Advanced Call Features > Operator Panel**.

The UCM630X supports the operator panel so that UCM extension can be used as admin to manage calls and activities such as extension status, call queue status, transfer, barge-in, hangup, etc. On Grandstream Wave client, it can display the extensions, ring group, voicemail, call queue, call park status under the management of the extension. This section describes how to configure the operator panel.



Operator Panel Configuration Page

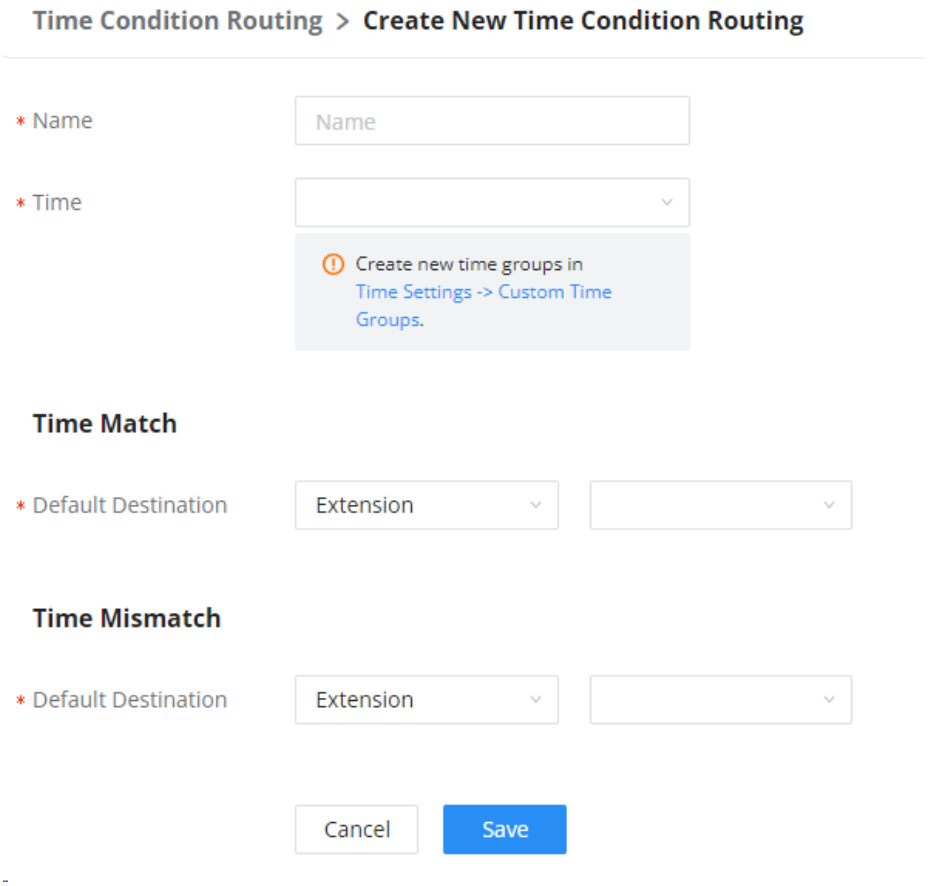
- Click on "Add" to create the operator panel.
- Click on to edit the operator panel.
- Click on to delete the operator panel.

Name	Configure the name for the operator panel created for identification purposes.
Administrator	Assign the administrator for the operator panel. It can be an extension, a extension group or a department. For the selected extension groups and departments, subsequent extensions will automatically become administrators.
Management Module	
Extension	The selected extensions will be supervised by the administrator, and you can choose extensions, extension groups, and departments. For the selected extension groups and departments, subsequent extensions will be automatically supervised by the administrator.
Ring Groups	The selected Ring Groups will be supervised by the administrator. If selecting "All", all Ring Groups and subsequent updates will be automatically supervised by the administrator.
Voicemail Groups	The selected Voicemail Groups will be supervised by the administrator. If selecting "All", all Voicemail Groups and subsequent updates will be automatically supervised by the administrator.
Call Queue	The selected Call Queue will be supervised by the administrator. If selecting "All", all Call Queue and subsequent updates will be automatically supervised by the administrator.

Parking Lot	The selected Parking Lot will be supervised by the administrator. If selecting "All", all Parking Lot and subsequent updates will be automatically supervised by the administrator.

Time Condition Routing

Time Condition Routing allows the user to create default destinations for call queues and ring groups which are based on time conditions under **Advanced Call Features > Time Condition Routing.**



Time Condition Routing

Parameter	Description
Name	Enter a unique and easily identifiable name for this routing.
Time	Configures the time period to use for this time-based routing.
Time Match	
Default Destination	Calls received during the selected time period will be routed to this destination.
Time Mismatch	
Default Destination	Calls received outside the selected time period will be routed to this destination.

MESSAGING

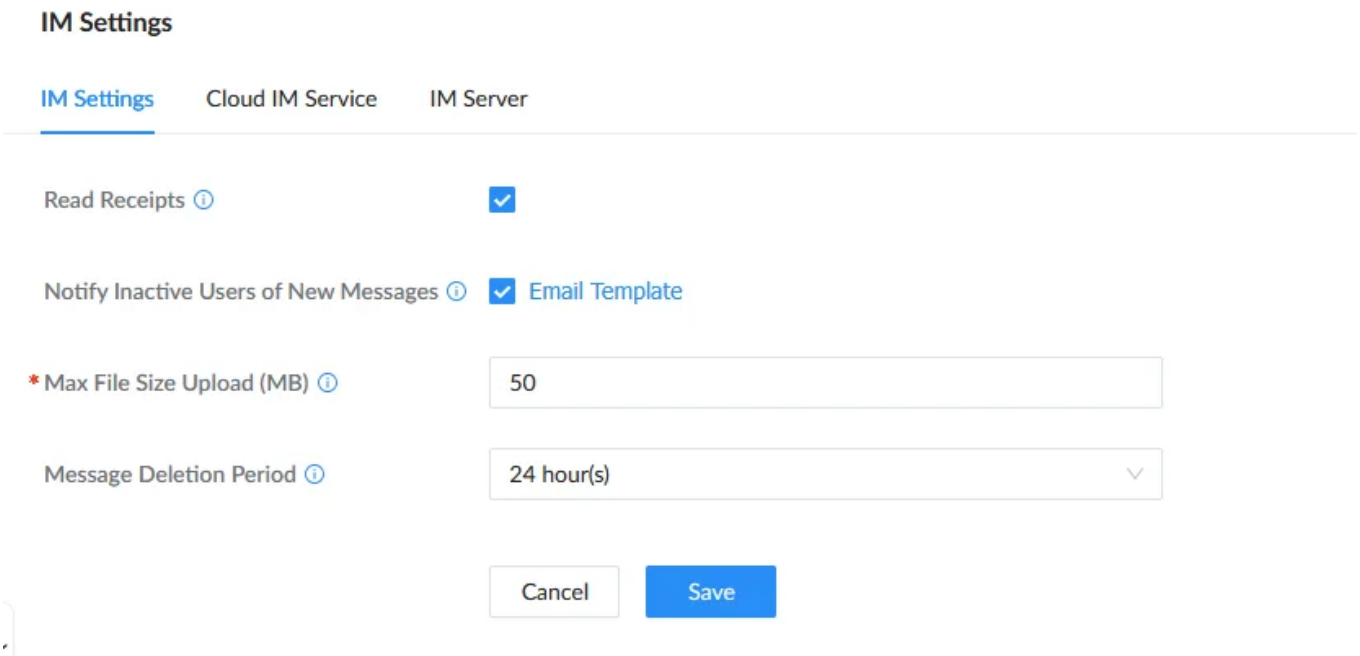
This section includes the messaging features offered by the UCM6300 Series. It includes instant messaging, live chat, message broadcast, and SMS features.

IM Settings

In this section the user can change the settings related to Wave instant messaging such as enabling or disabling read receipt, defining the maximum file size which the user can send on Wave. The user can also configure cloud instant messaging for the PBX, or configure the PBX as an instant messaging server.

IM Settings

The IM Settings page allows administrators to globally configure instant messaging parameters and chat behavior for Wave client users across the system.

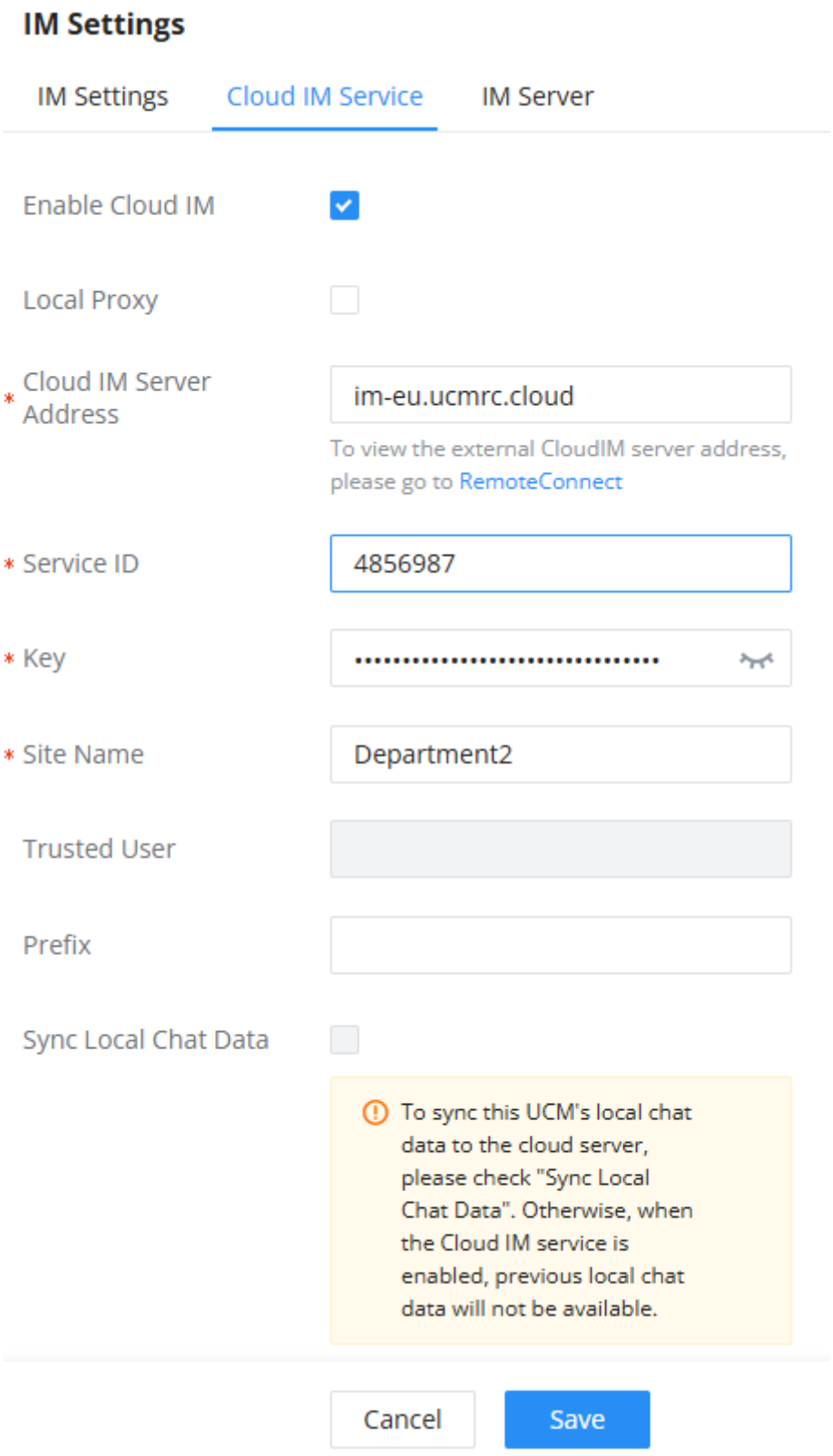


The table below describes the configuration parameters available under the IM Settings page:

Option	Description
Read Receipts	Toggles whether to allow instant messaging read receipts on Wave clients. When enabled, users can see if their sent messages have been read by the recipient.
Notify Inactive Users of New Messages	If enabled, the system automatically sends email notifications to inactive or offline users when they receive new instant messages. Note: Click the Email Template link next to the checkbox to configure or customize the notification email template.
Max File Size Upload (MB)	Configures the maximum size (in MB) of individual files users can upload to Wave chat. The valid range is 10 to 500 MB (Default: 50 MB). Note 1: This parameter applies strictly when using local IM. Note 2: If using Cloud IM or a custom IM server, the maximum file size upload must be configured on GDMS or the target IM server instead. On GDMS, navigate to Plans & Services -> My Plans -> Options column -> Edit Cloud IM page.
Message Deletion Period	Configures the time window within which users are permitted to delete or recall sent instant messages across Wave chat sessions, regardless of whether local IM or Cloud IM is utilized: Not Allowed to Delete: Prevents users from deleting or recalling sent chat messages. Unlimited: Allows users to delete or recall sent chat messages at any time without time restrictions. 1 hour: Allows message recall within 1 hour of sending. 24 hour(s): Allows message recall within 24 hours of sending (Default). Custom: Allows setting a custom message deletion time limit (1 to 168 hours).
Custom Duration (hour)	Configures the customized duration for message deletion period in hours.

Cloud IM Service

After enabling **Cloud IM**, it means that all IM data in Wave is stored in the external server Cloud IM, and is no longer stored locally in UCM.GDMS can configure the External Cloud IM service for UCM devices. At this time, the UCM device synchronizes the configuration item information.



Cloud IM Service

Cloud IM Service

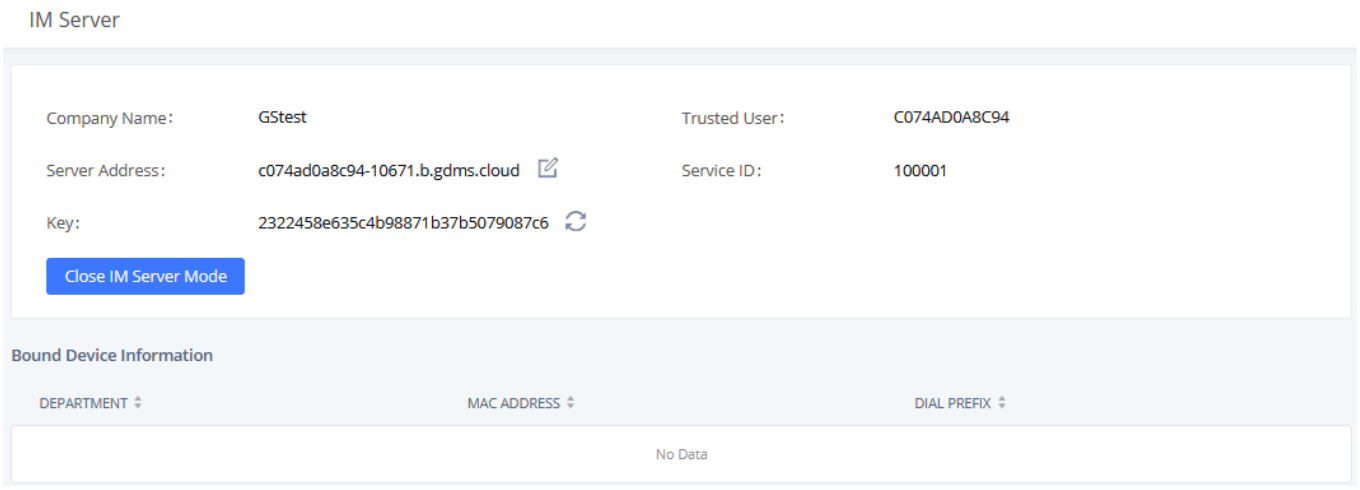
Enable Cloud IM	If you have purchased the Cloud IM package or purchased the Grandstream IM server, you can configure it. If you have not purchased it, the configuration will not take effect, but PBX local IM service is allowed. Please note that after enabling this feature, local chat data will not be visible.
Local Proxy	If enabled, the local proxy will be used to forward files and text messages if the IM server cannot be connected to upon Wave login due to certificate issues.
Cloud IM Server Address	The address of the server that provides IM service, you can fill in the address of the Cloud IM server provided by the RemoteConnect package or the IM server address of the GDMS.
Service ID	The service ID of the Cloud IM server.
Key	The Key to the Cloud IM server.
Site Name	Enter the name of the site.
Trusted User	The trusted user of the cloud IM. Only letters, numbers, and special characters are allowed.
Prefix	As the extension prefix, it is added before the extension number.
Sync Local Chat Data	Syncing existing local chat data to Cloud IM server. The Wave chat feature will not be available during the syncing process. It is recommended to avoid syncing during active working hours.- Time Range All Last 12 Months Last 6 Months Last 3 Months Last Month - Data Type IM Data Images Files

Please note that synchronization of the local chat can only occur in the initial connection to a Cloud IM Server . If the UCM is already connected to a Cloud IM server, or the Cloud IM server has already been synced to other UCMs, local chat data will not be able to be synced.

Only account details and department information will be synced on local IM and cloud IM. Other configurations such as profile picture, work status, and favorite contacts will not be synced and these are stored in local IM or cloud IM respectively. Therefore, please be aware that when switching between local IM and cloud IM, part of the data cannot be synced and the previously stored data on local IM or cloud IM (depending on which one is switched to) will be retrieved.

IM Server

If Enable IM Server Mode is toggled on, UCM will function only as an IM server. The UCM management portal will remove PBX-related services and supports the binding of multiple cross-region UCM devices. The UCM device that wants to bind the IM server address is also bound by turning on the Cloud IM mode, and the IM data in his Wave is stored in this IM server.

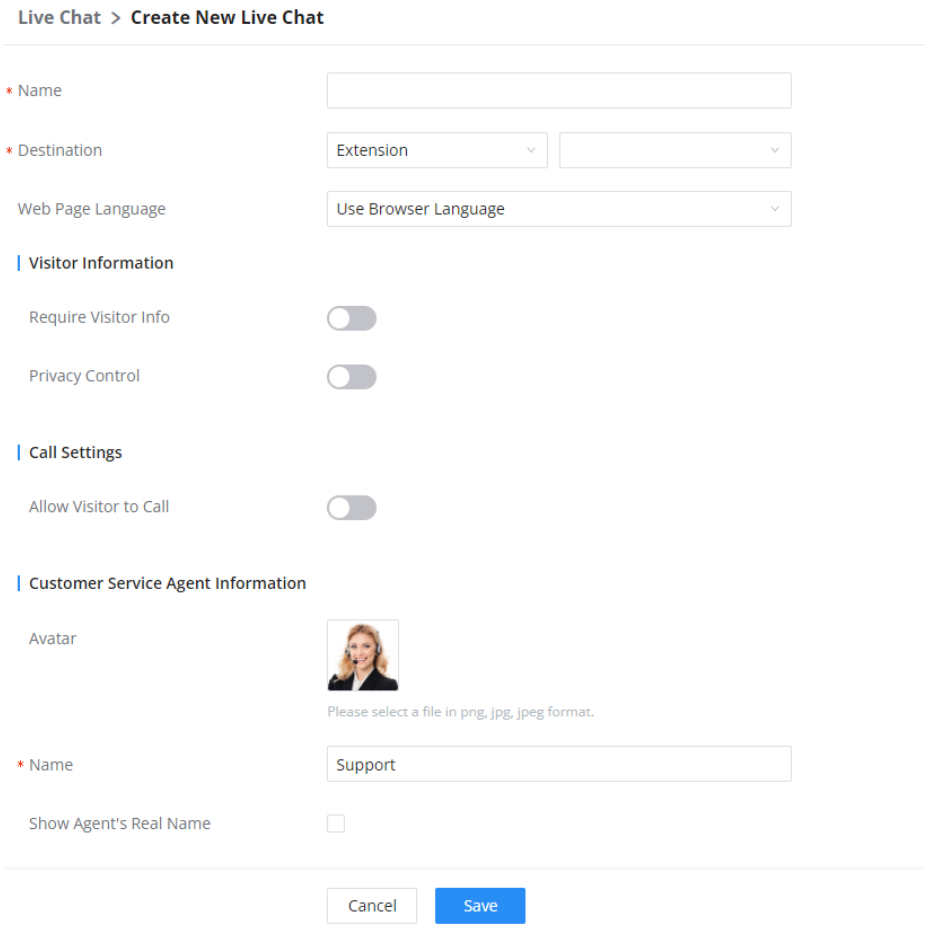


IM server configuration interface

Company name	The entered company name
Server Address	The domain name or IP address of the Cloud IM server.
Service ID	The service ID of the Cloud IM server.
Key	The Key of the Cloud IM server.
Trusted User	The trusted user of the cloud IM. Only letters, numbers, and special characters are allowed.
Bound Device Information	
Department	The department represented by the bound UCM.
MAC Address	MAC address of the bound UCM device.
Dial Prefix	Extension prefix

Live Chat

Live Chat feature allows to create chat channels that can be embedded on your website to enable your client to reach your customer service more easily. The client can contact your agents by text then



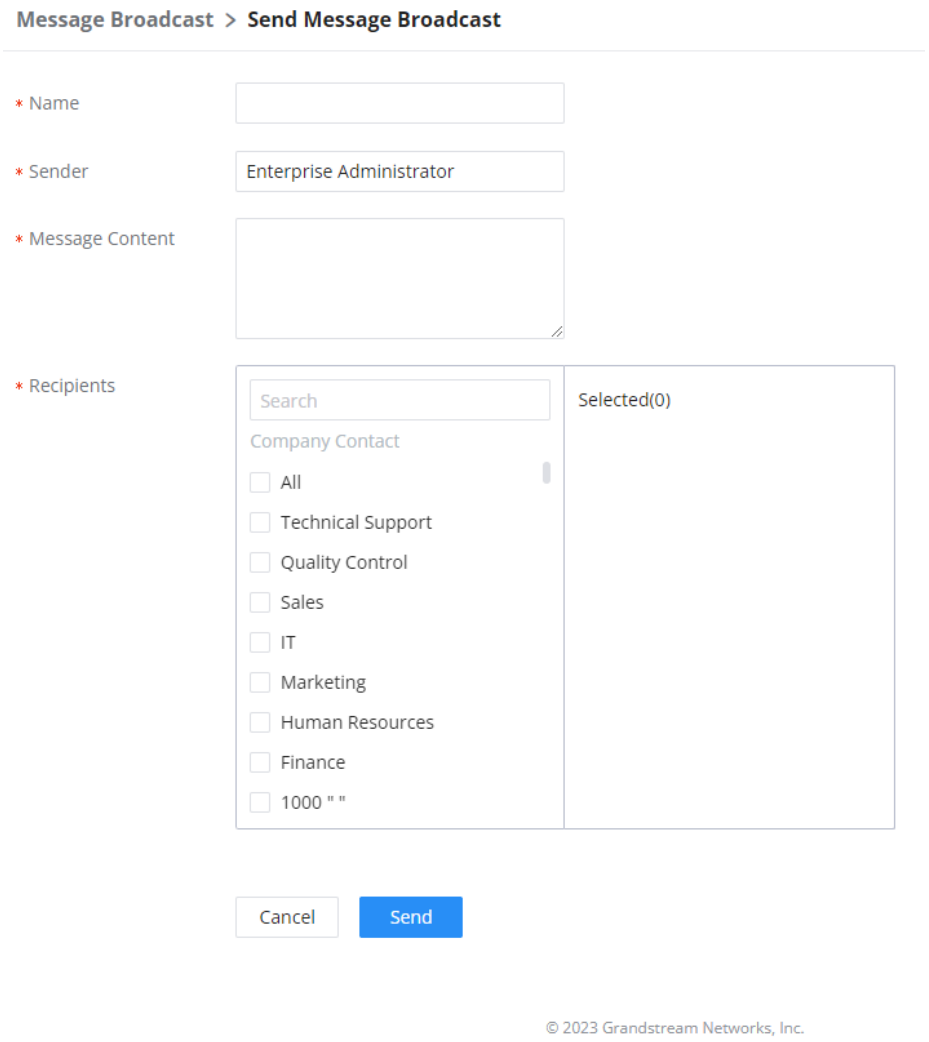
Name	Fill in the name of the Live Chat. It will be displayed on the chat session page of the agent (customer service), and the agent will know which Live Chat the visitor is accessing through.
Destination	Select the destination number, which is the extension or queue number of this Live Chat (receiving message).
Web Page Language	Select the display language on the visitor's Live Chat interface.
Disable	If disabled, this live chat will no longer be available for use.

Call Settings	
Allow Visitor to Call	Select whether to allow visitors to make calls.
Allow Calling Before Chat	Select whether to allow visitors to make phone calls before an agent (customer service) receive the session.
WebRTC Trunks	Select the WebRTC trunk of the phone customer service which is applicable. You can create it in Extension/Trunk -> WebRTC Trunk in advance. It is recommended that the destination number of the WebRTC Trunk be the same as the destination number of the live chat, so that after transferring the chat to a call the receiver will be the same agent.UCM6300 Series WebRTC Trunk - Guide
Customer Service Display Information	
Avatar	Select the profile picture that visitors will see. You can upload a picture or use the default picture.
Name	Fill in the name of the agent that visitors will see.
Show Customer Service Real Name	Select whether to display the extension name of the agent
Chat Settings	
Visitor Side Chat Log Retention Time (Days)	When the session ends, the visitor can view the chat history during this configured period. After this time, the chat history cannot be viewed.Note: If the session never ends, the visitor will always see the chat history.
Live Chat Link Address	This link can be embedded onto web pages. Clicking it will connect visitors to the configured Live Chat destination. This link can also be entered directly into the browser address bar for testing purposes.

For the complete configuration steps, please refer to the following link:
https://documentation.grandstream.com/knowledge-base/live-chat-user-guide/

Message Broadcast

Message broadcast feature allows the administrator to broadcast a text message to all the endpoints selected by the administrator. The administrator can select departments or individual extensions to boardcast a text message.



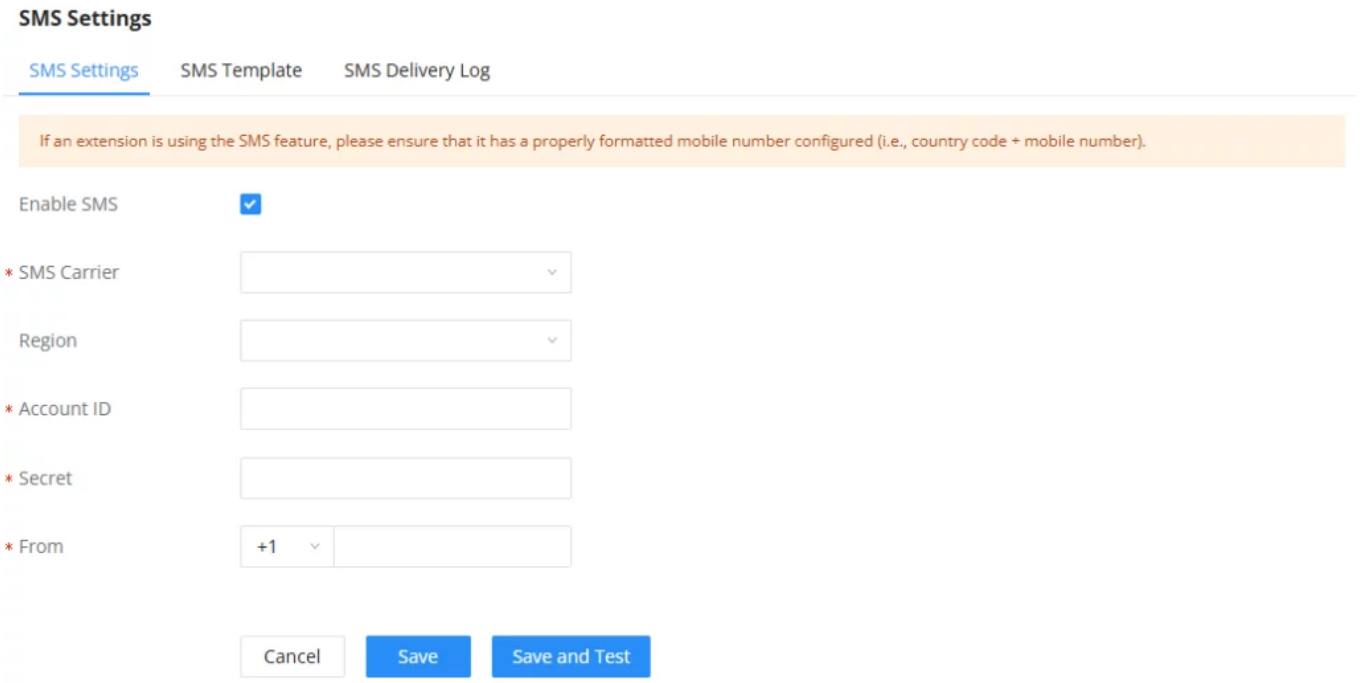
Name	Configure the name of this broadcast.
Sender	Configure the sender of this broadcast.
Message Content	Enter the message to broadcast to recipients. Please keep in mind the display size of recipient endpoints as long messages may be cut off.
Recepients	Select the recipients of the broadcasted message.

SMS Settings

SMS Configuration

Configuring the SMS feature on the UCM series allows administrators to enable two-factor authentication, send system alerts, transmit meeting notifications, and trigger automated SMS messages with links via IVR key presses (Smart Call SMS Link Service).

The UCM supports SMS integration through multiple third-party service providers, including **Twilio**, **Amazon SNS**, **VoiceMeUp**, and **Voxtelesys**.



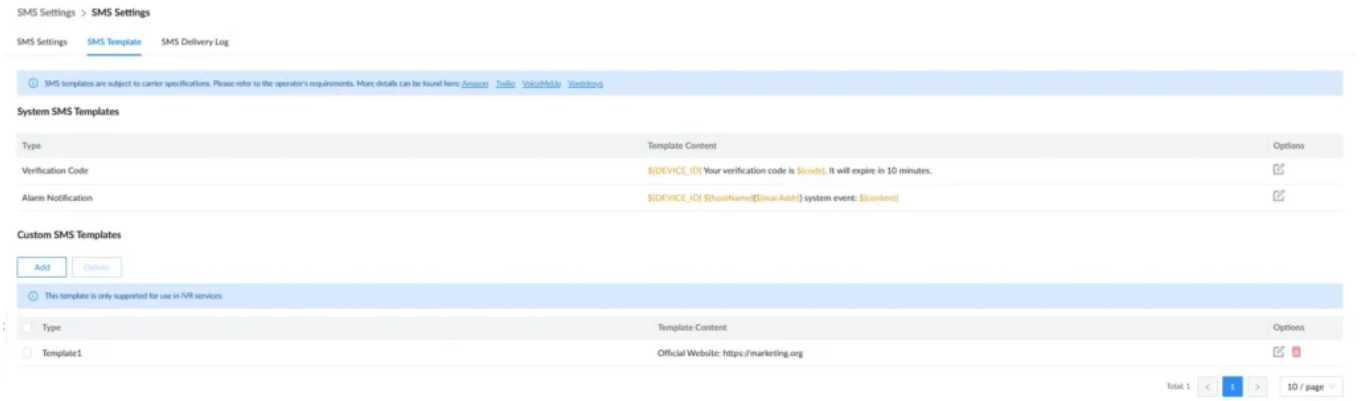
SMS Settings

When SMS is enabled, users can configure the following parameters based on the selected carrier:

SMS Carrier	Parameter	Description
Twilio	Account ID	The Account SID provided in your Twilio Console dashboard used to authenticate API requests.
	Auth Token	The secret authentication token associated with your Twilio Account SID.
	Messages Server ID	The Messaging Service SID created within Twilio for handling outgoing message pools.
	From	The authorized Twilio phone number (including country code) assigned to send outbound SMS messages.
Amazon	Region	The AWS region where your instance is hosted (e.g., us-east-1).
	Account ID	The AWS Access Key ID generated from the AWS IAM console for API access.
	Secret	The AWS Secret Access Key corresponding to the Access Key ID used for request signing.
VoiceMeUp	Account ID	The primary account or username credential assigned by VoiceMeUp for portal and API access.
	Auth Token	The API authentication token generated within the VoiceMeUp portal under API settings.
	From	The SMS-enabled VoiceMeUp DID or phone number configured as the originating sender ID.
Voxtelesys	API Key	The bearer/API authorization key generated in the Voxtelesys Portal under API Credentials.
	From	The SMS-enabled Voxtelesys phone number assigned to your account used as the sender ID.

SMS Template

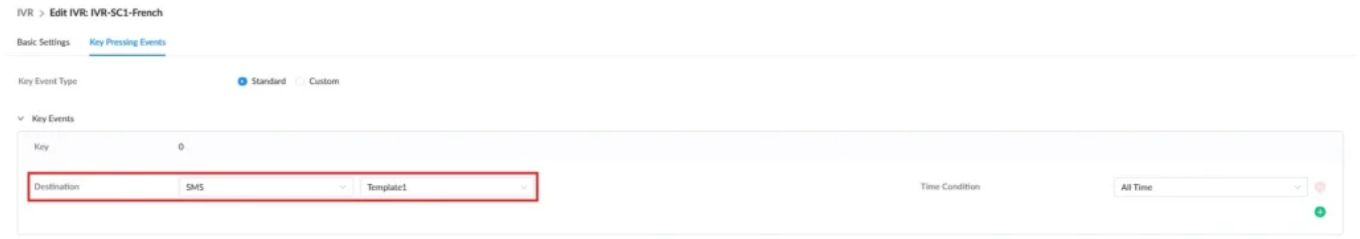
SMS templates can be managed under the **SMS Template** tab. SMS templates are subject to carrier specifications. Please refer to operator requirements before sending outbound messages. Additional details can be found in the documentation for Amazon, Twilio, VoiceMeUp, and Voxtelesys.



SMS Templates are categorized into two sections:

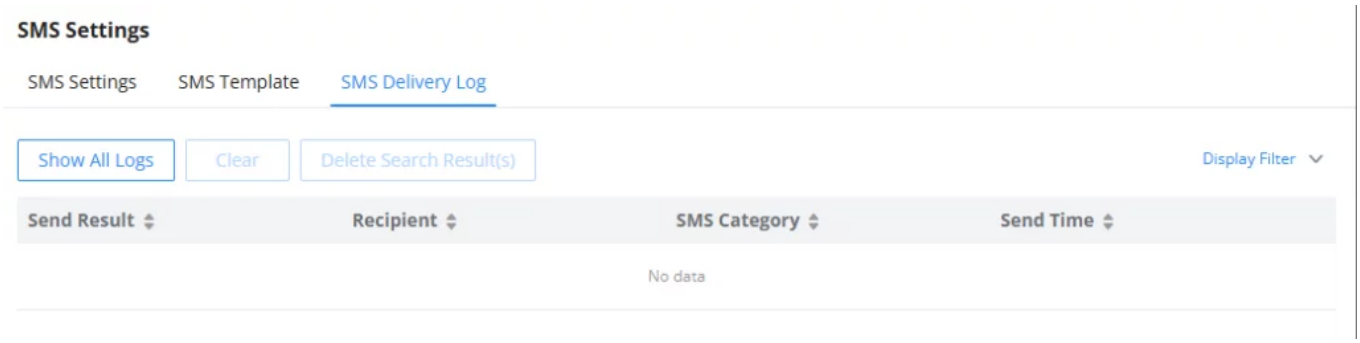
- **System SMS Templates:** Includes default templates for system-level notifications, such as Verification Code and Alarm Notification.
- **Custom SMS Templates:** Allows administrators to create custom SMS templates containing URLs or informational text. These templates can be assigned as destinations under IVR Key Events. When a caller presses a designated key during an IVR call, the system automatically sends the custom SMS message containing the configured link or text directly to the caller's mobile device.

To configure IVR SMS destination, please navigate to B**asic Call Features->IVR->Add/Edit IVR->Key Pressing Events**.



SMS Delivery Log

All outbound SMS messages sent by the system (including verification codes and alerts) will be logged under the **SMS Delivery Log** tab.



SMS Delivery Log

Advanced Messaging

The **Advanced Messaging** page provides a centralized interface for configuring chatbots, WhatsApp connectivity, and third-party messaging integrations directly from the UCM management portal. This allows administrators to easily create, manage, and integrate messaging services without relying on external tools.

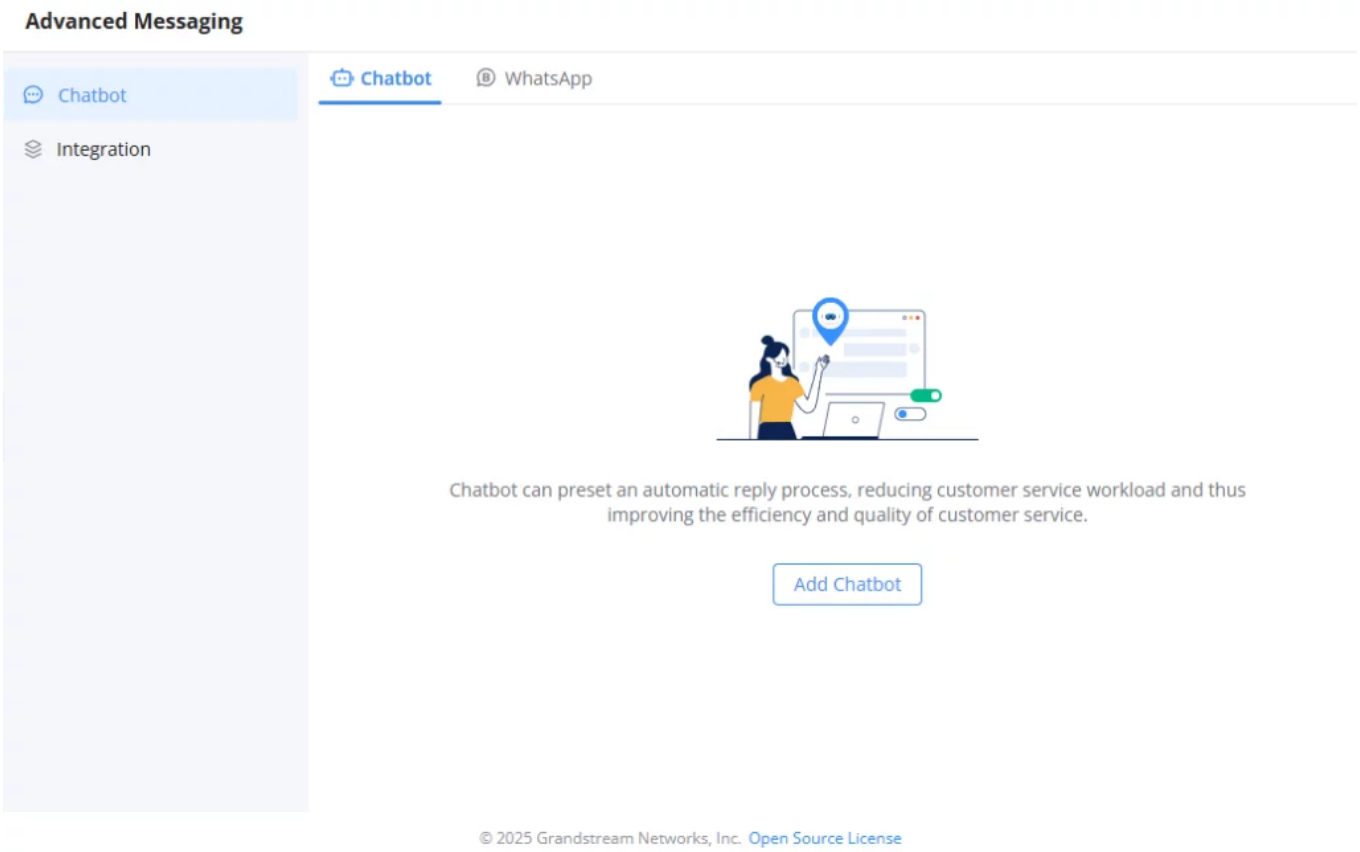
The advanced messaging feature supports configuring:

- **General Chatbot:** A customizable chatbot that can handle automated conversations and responses across supported messaging platforms.
- **Whatsapp Chatbot:** A chatbot integrated with WhatsApp to automate customer interactions, messaging, and service workflows within the WhatsApp ecosystem.

Chatbot

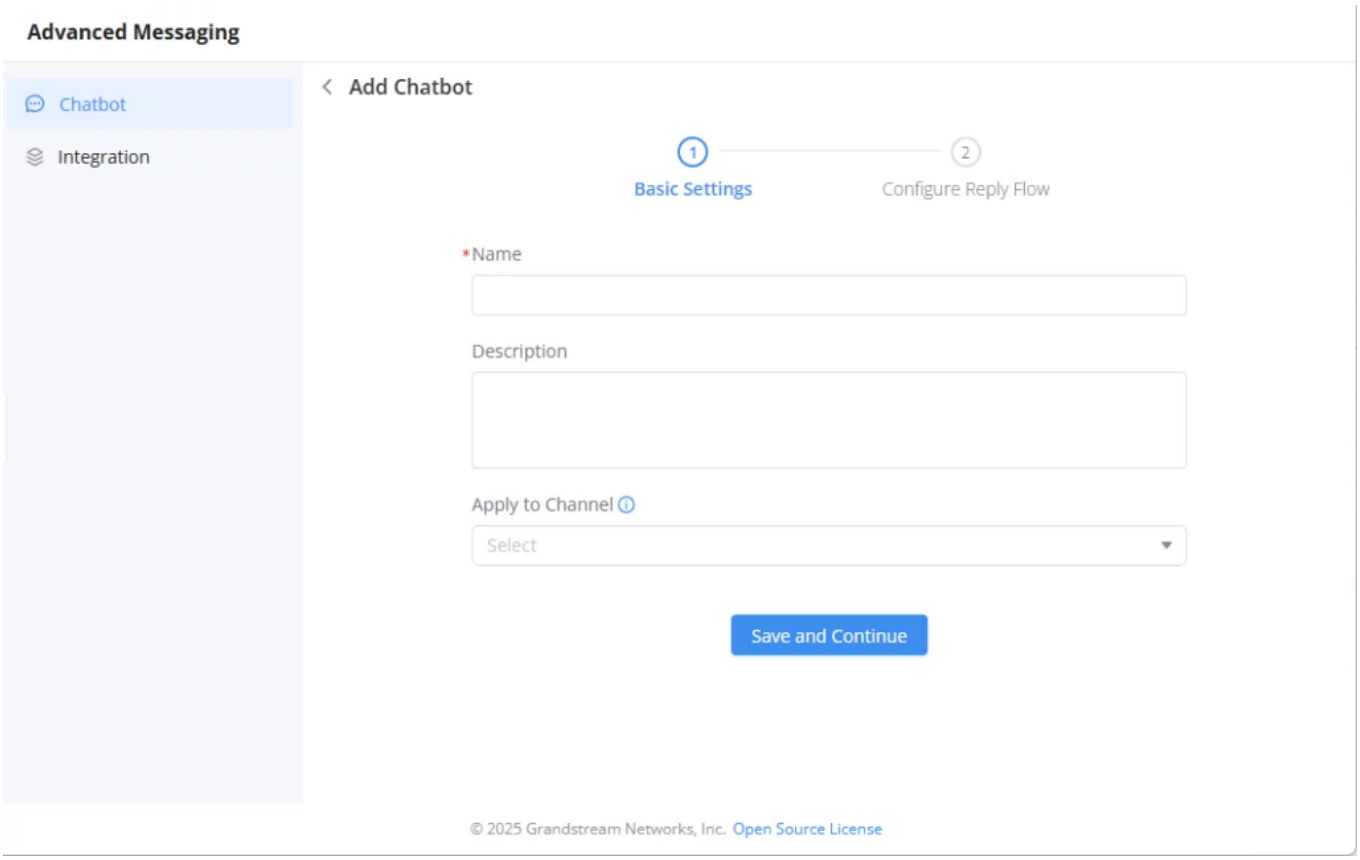
General Chatbot

- Navigate to **UCM Web UI -> Messaging -> Advanced Messaging -> Chatbot**. Click **Add** to create a new chatbot. This will open the chatbot configuration page where you can define the chatbot type and basic settings.



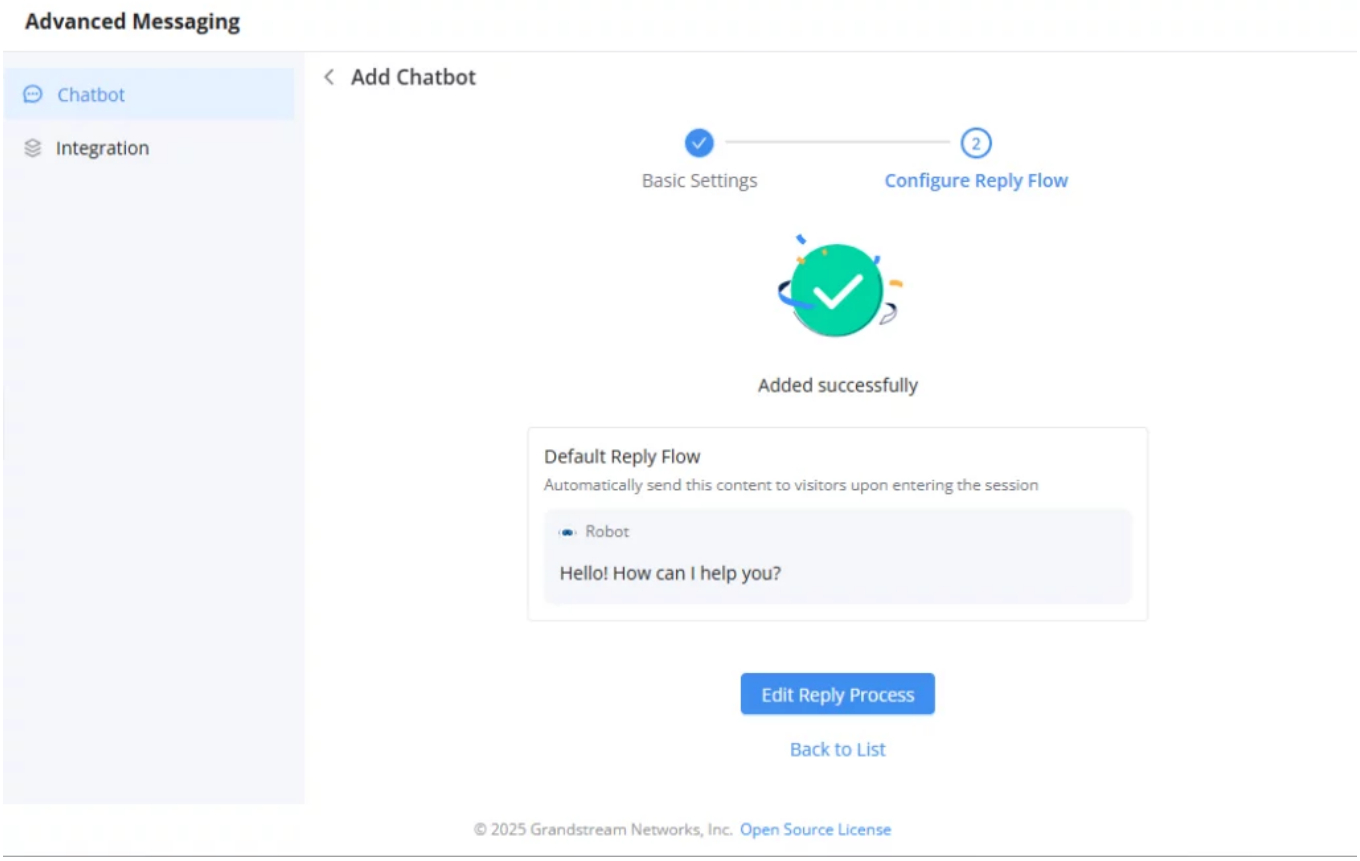
- In the **Add Chatbot - Basic Settings** page:

  - **Name** - Enter a unique name for the chatbot (e.g., SupportBot).
  - **Description** - (Optional) Add notes or details about the chatbot's purpose.
  - **Apply to Channel** - Select the messaging channel where the chatbot will be used (e.g., WhatsApp or General).



- After saving the basic settings, the chatbot will be created successfully. A **Default Reply Flow** is automatically applied, starting with a standard greeting (e.g., Hello! How can I help you?).

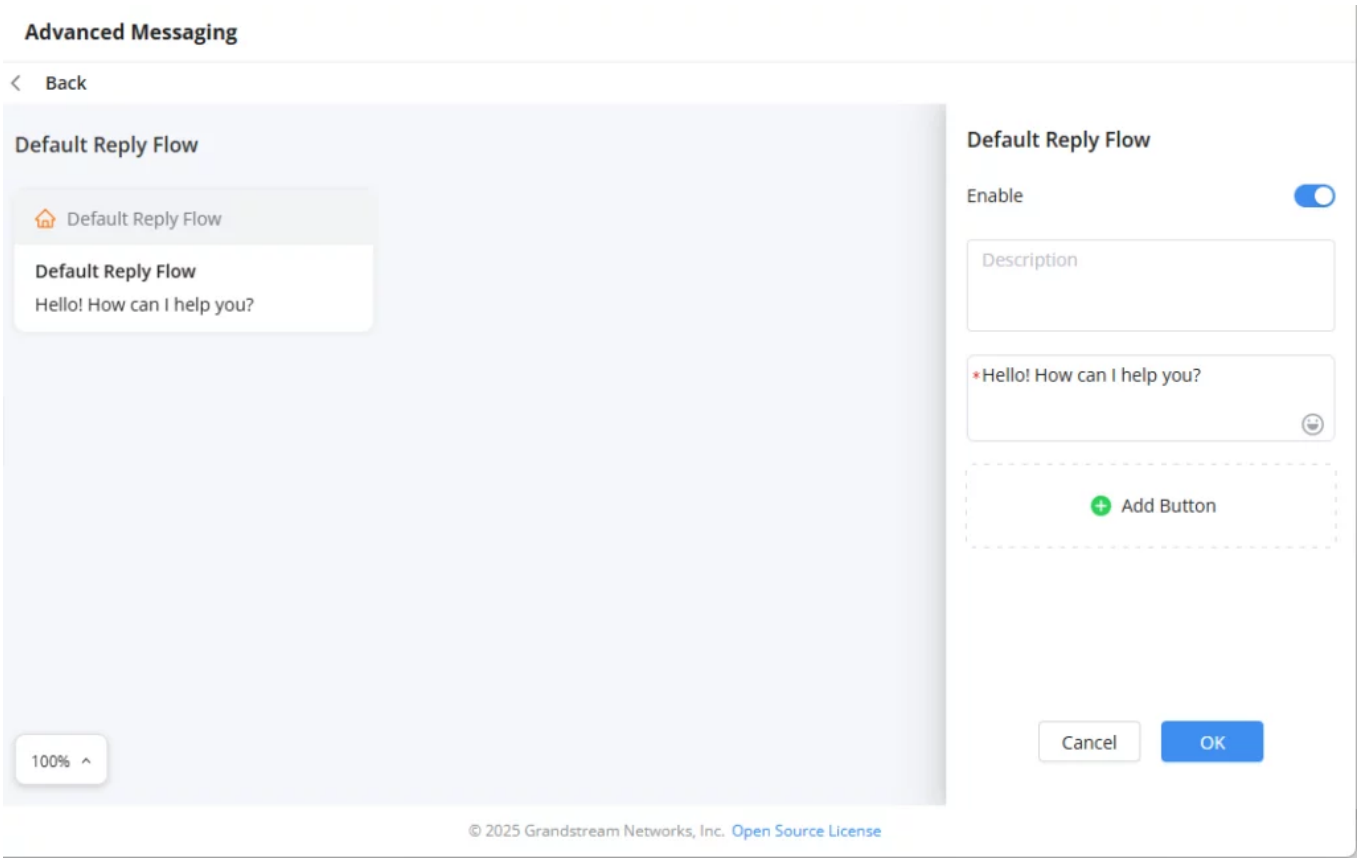
  - To customize this behavior, click **Edit Reply Process** and define the conversation flow according to your needs.
  - If no changes are required, click **Back to List** to return to the chatbot overview page.



In the **Default Reply Flow** editor:

- **Enable** - Toggle on/off to activate or disable the reply flow.
- **Description** - (Optional) Add details about the reply flow's purpose.
- **Message** - Enter the default greeting or automated response (e.g., Hello! How can I help you?).
- **Add Button** - Insert interactive buttons to guide users toward predefined options or actions.

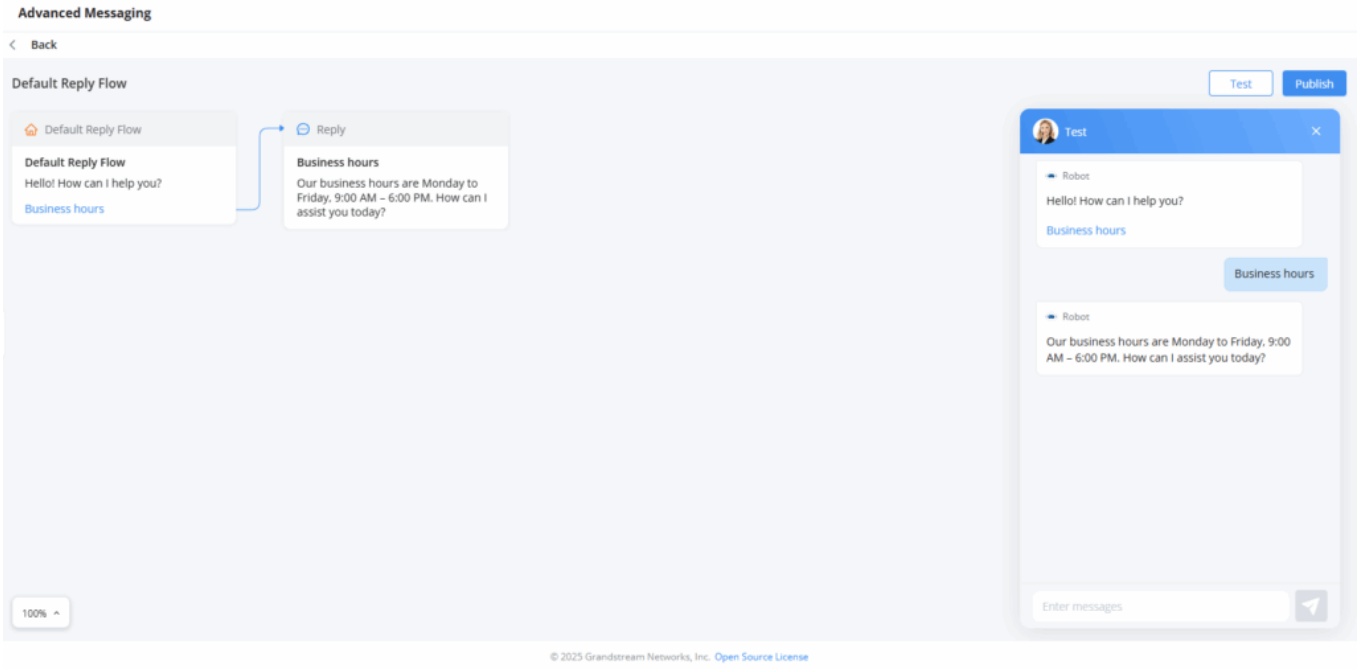
Click **OK** to save the changes.



In the **Default Reply Flow** editor, you can add interactive options and responses:

- Under the default greeting, click **Add Button** and label it (e.g., Business Hours).
- Link the button to a **Reply** block that contains the desired response (e.g., Our business hours are Monday to Friday, 9:00 AM - 6:00 PM. How can I assist you today?).
- Use the **Test** panel on the right to preview the chatbot's behavior.

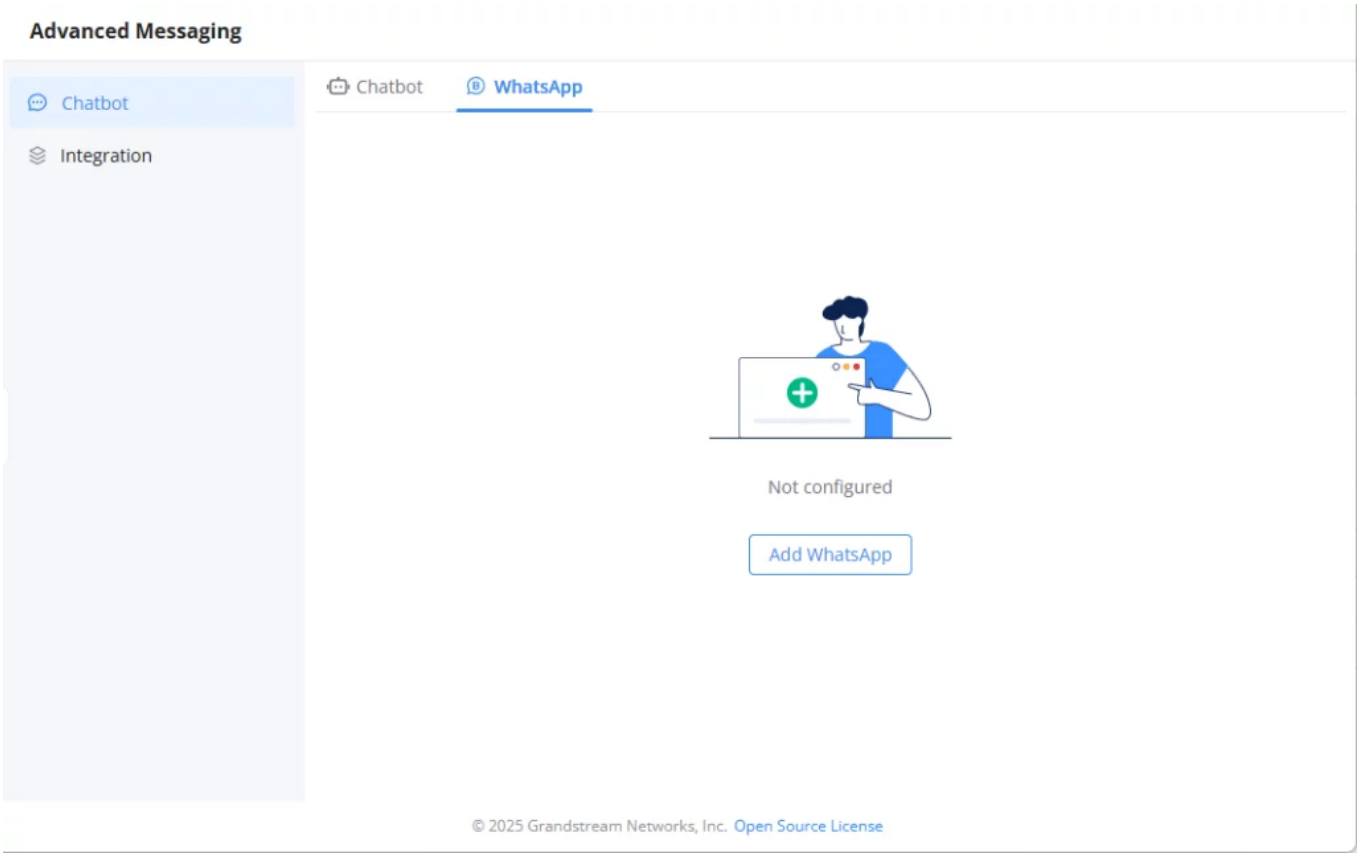
Once satisfied, click **Publish** to activate the chatbot flow.



Whatsapp Chatbot

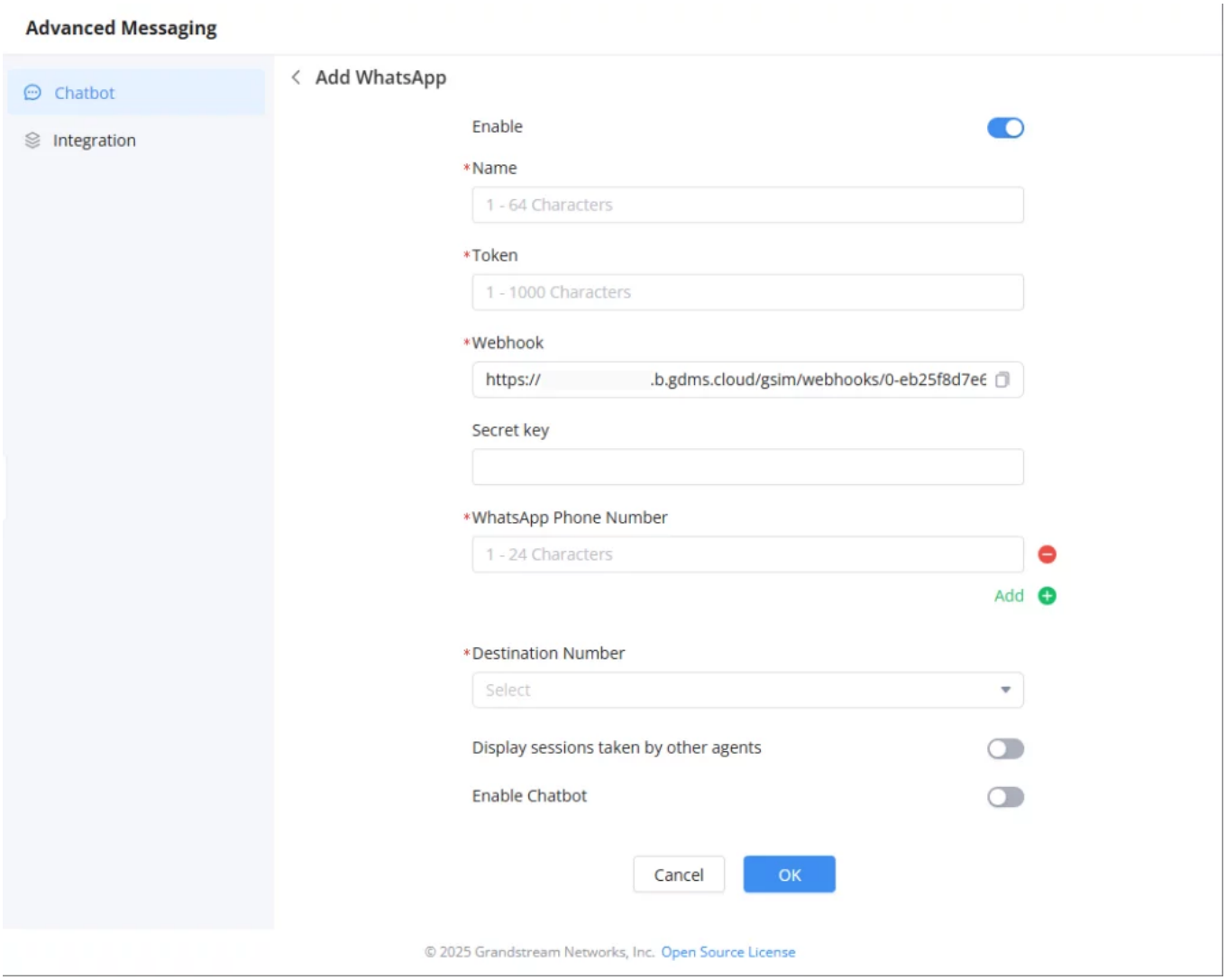
From the **Advanced Messaging -> WhatsApp** tab, click **Add WhatsApp**. This opens the configuration page

to register your WhatsApp account with the UCM.



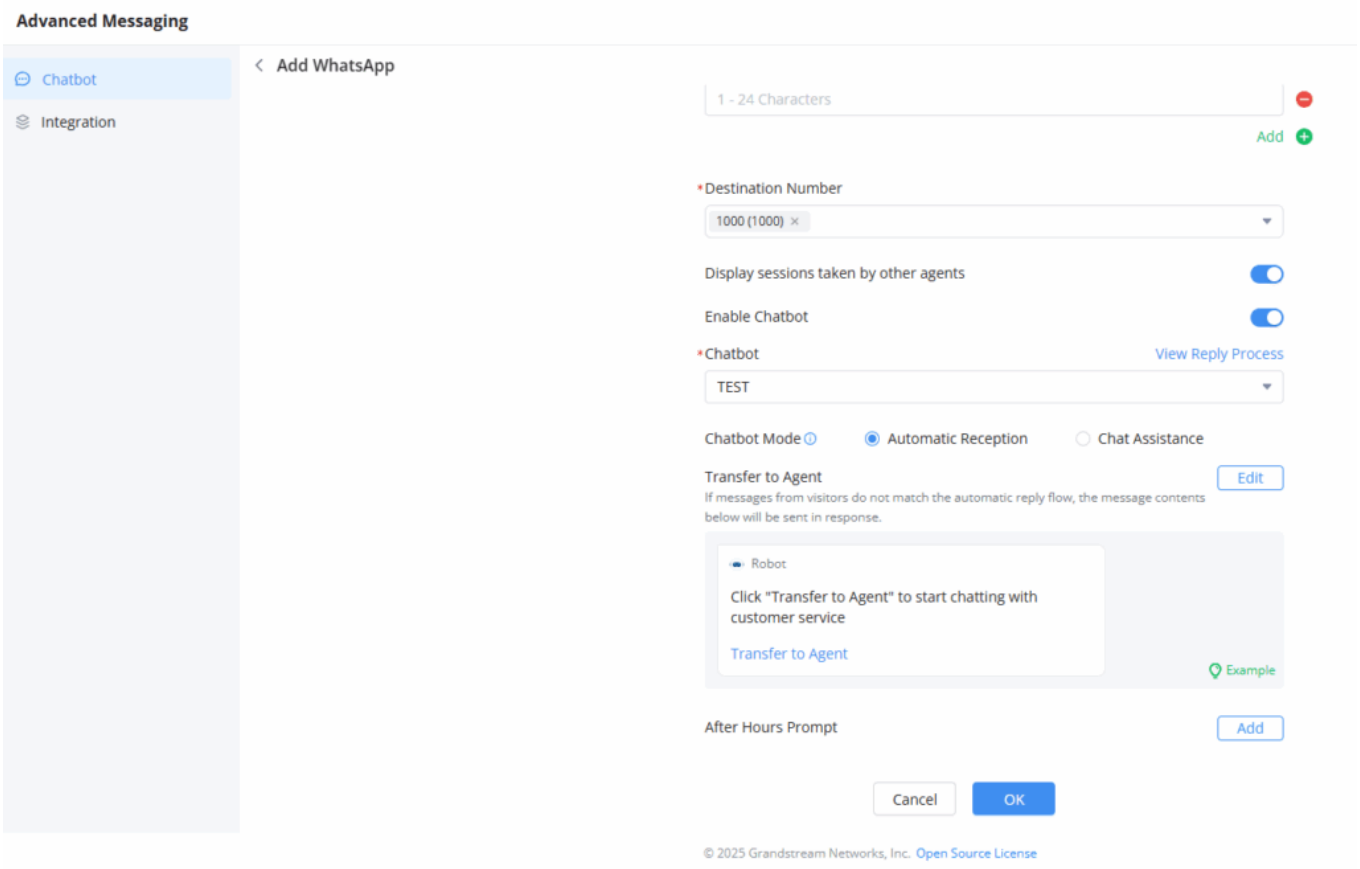
Fill in the required fields:

- **Name** - Enter a unique identifier for the WhatsApp integration.
- **Token** - Provide the authentication token generated by your WhatsApp service.
- **Webhook** - Enter the webhook URL for event callbacks.
- **Secret Key** - (Optional) Add a key for securing webhook communications.
- **WhatsApp Phone Number** - Enter the registered WhatsApp phone number.
- **Destination Number** - Select the UCM extension that will receive WhatsApp messages.
- **Display sessions taken by other agents:** Shows active chat sessions that are already handled by another agent.
- **Enable Chatbot** - Toggle on and choose the chatbot to handle automated replies.



Define Chatbot Behavior

- **Chatbot Mode** - Select how the chatbot should operate: Automatic Reception or Chat Assistance.
- **Transfer to Agent** - Configure the fallback message when the chatbot cannot handle the request (e.g., Click "Transfer to Agent" to start chatting with customer service).
- **After Hours Prompt** - Add a custom message to be sent outside business hours.

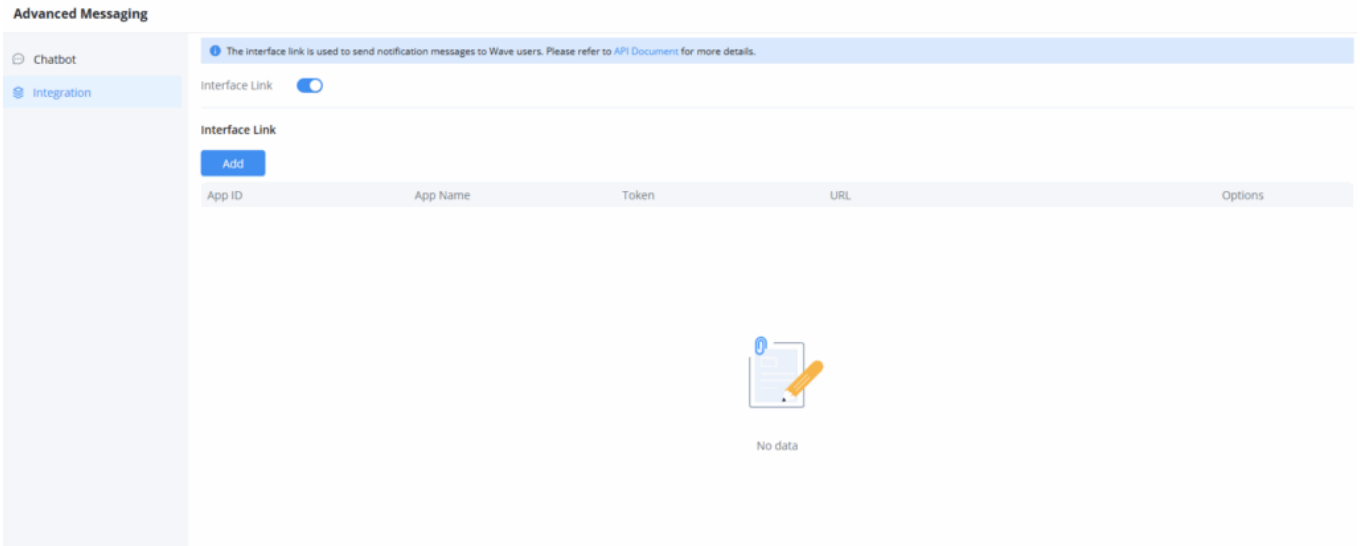


Integration

In the **Integration** tab, enable **Interface Link** to allow the UCM to send notification messages to Wave users.

- Click **Add** to create a new integration entry.
- Provide the **App Name**, **Token**, and **URL** as required.

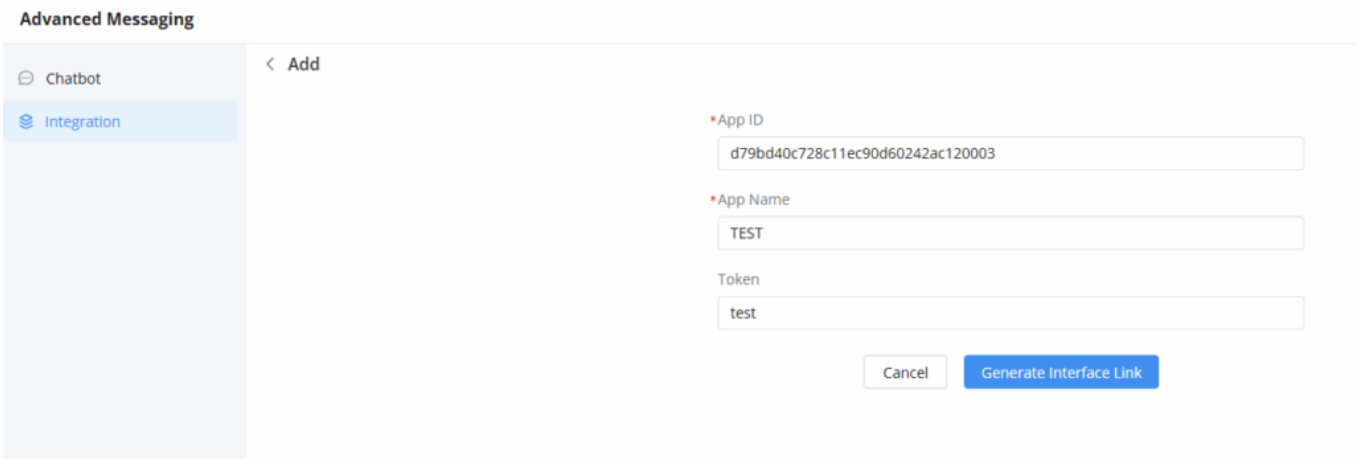
For detailed API usage, refer to the API documentation linked in the interface.



When creating a new integration, enter the following details:

- **App ID** - Automatically generated unique identifier for the application.
- **App Name** - Enter a descriptive name for the integration (e.g., TEST).
- **Token** - Provide the authentication token used for secure communication.

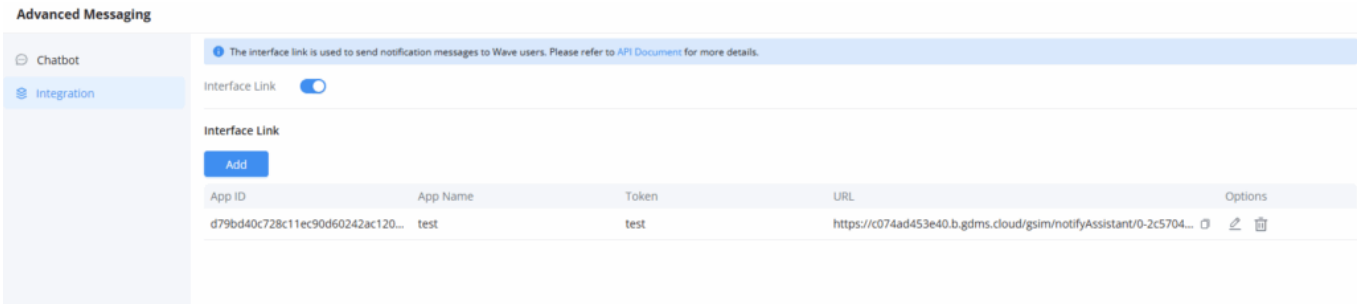
Click **Generate Interface Link** to complete the setup.



Once the interface link is generated, the application will appear in the list with its details:

- **App ID** - Unique identifier of the integration.
- **App Name** - Custom name assigned to the integration.
- **Token** - Authentication token used for communication.
- **URL** - Generated interface link for sending notifications.

Use the options on the right to **edit**, **copy**, or **delete** the configuration as needed.



PBX SETTINGS

This section describes internal options that have not been mentioned in previous sections yet. The settings in this section can be applied globally to the UCM630X, including general configurations, jitter buffer, RTP settings, ports config and STUN monitor. The options can be accessed via **PBX Settings** > **General Settings**.

General Settings

Option	Description
General Preference	
Global Outbound CID Number	Global-level CID Number used for all outgoing calls if no other CID numbers have been configured for the calling party.
Global Outbound CID Name	Global-level CID Name used for all outgoing calls if no other CID names have been configured for the calling party.
Ring Timeout (s)	Number of seconds to ring the extension before forwarding the call to voicemail. Default setting is 60 seconds. If Extensions > Features > Ring Timeout is not configured, this global setting is used.
Call Duration Limit	Block calls for the configured duration. If Extensions > Features > Call Duration Limit and Outbound Routes > Call Duration Limit are not configured, this value is used. Disabled by default.

International Call Prefix	Digits users dial before a country code to place an international call (e.g., 00 or 011). The PBX uses this prefix to detect and classify a dialed number as international for routing, permissions, and PMS billing/records. Input: digits only.
Domestic Long Distance Call Prefix	Digits users dial to reach a national (out-of-area) number within the same country (commonly 0 or 1 in NANP countries). Leave blank if not used.
Local Area Code	The area/city code of the PBX's location, used to normalize local dialing. Input the area/city code without the domestic long-distance prefix.
Station ID	Configures a unique device station identifier for the UCM. Note: This Station ID can be prepended as a prefix to randomly created meeting room numbers (configured under Basic Call Features > Multimedia Meeting > Meeting Settings), enabling cross-PBX routing so remote extension nodes can dial into random conference rooms via outbound routes.
Enterprise Contact Number	Configures contact phone numbers for the enterprise, which can be selected for inclusion in automated meeting invitations and notifications. Click Add to configure additional numbers.
Recording Settings	
Record Prompt	If enabled, the system will play the voice prompt "This call will be recorded" before recording starts. Disabled by default.
Allow External Numbers to Cancel Recording	If enabled, external calling parties will be given the option to decline call recording.
Merge Same Call Recordings	If enabled, the system merges all recordings created during a call regardless of how many times recording is started and stopped.
Stereo Recording	If enabled, caller and callee audio streams are split into separate audio channels during call recording. Applicable for two-party calls.
Calling Channel	Configures the audio channel assignment for caller and callee when Stereo Recording is enabled (e.g., Right Channel).
Start/Stop Recording Feature Codes	Provides a quick navigation link (Go to Page) to configure in-call recording feature codes under Feature Codes settings.
Extension Preference	
Enable Strong Password	If enabled, enforces a strong password policy for extension registration/user passwords.
Enable Random Password	If enabled, newly created extensions are automatically assigned a randomly generated password.
Send Extension Update Emails	If enabled, an email notification is automatically sent to an extension's configured email address upon creation or modification.
Enable Extension Range	Toggles whether extension ranges are strictly enforced across the IPPBX. Enabled by default. Note: Extension ranges allocate number pools for specific call features and do not dictate the maximum capacity of those features.
User Extensions	Defines the allocated range for user extensions (Default: 1000-6299).
Meeting Extensions	Defines the allocated range for multimedia meeting rooms (Default: 6300-6399).
Ring Group Extensions	Defines the allocated range for ring groups (Default: 6400-6499).
Queue Extensions	Defines the allocated range for call queues (Default: 6500-6599).
Voicemail Group Extension	Defines the allocated range for voicemail groups (Default: 6600-6699).
IVR Extensions	Defines the allocated range for IVR menus (Default: 7000-7100).
Dial By Name Extensions	Defines the allocated range for Dial By Name directory services (Default: 7101-7199).
Fax Extension	Defines the allocated range for T.38 Fax extensions (Default: 7200-8200).

Call Flow Number	Defines the allocated range for Call Flow Control numbers (Default: 8300-8499).
Zero Config Extension	
Pick Extensions	Defines the range of extensions (Default: 4000-4999) that can be manually selected from end devices during provisioning via Zero Config.
Auto Provision Extensions	Defines the range of extensions (Default: 5000-6299) automatically assigned to provisioned end devices during Zero Config discovery.
Default Extension Segment	Resets all allocated extension ranges back to factory default values.

SIP Settings

The UCM630X SIP global settings can be accessed via **PBX Settings** -> **SIP Settings**.

General

Realm for Digest Authentication	Configure this as the host name or domain name of the PBX. Realms MUST be globally unique according to RFC3261.
Bind UDP Port	Configure the UDP port used for SIP. The default setting is 5060.
Bind IPv4 Address	Configure the IPv4 address to bind to. "0.0.0.0" means to bind to all IP addresses.
Bind IPv6 Address	Configure the IPv6 address to bind to. "[::]" means to bind to all IP addresses.
MWI From Header	If disabled, the server will not transfer the Diversion Header
Enable Diversion Header	If set to "No", all transfers initiated by the endpoint in the IPPBX will be disabled (unless enabled in peers or users). The default setting is "Yes".
Send Deflection Diversion	If 'Enable Diversion Header' and this option enabled, the INVITE request will contain Diversion with reason 'deflection' while the inbound call been routed to an external number.
Block Collect Calls	If enabled, collect calls will be blocked.Note: Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call".
Unavailable Extension Cause	Sets the cause code to respond with when calling an unavailable extension. The options are:19 (No Answer)20 (Subscriber Absent)

Session Timer

Force Timer	Forces the UCM to always initiate and require SIP Session Timers for every call, regardless of whether the remote phone or SIP provider support. If the remote device refuses session timers, the call may be rejected.
Timer	Enables optional session timer support. When checked, the UCM will use session timers if requested by the remote endpoint or SIP provider, but will not force it if the remote side does not support it. (Enabled by default).
Session Expiration (s)	Sets the total lifespan (in seconds) of an active call before a session refresh is required. The UCM or endpoint must send a keep-alive message through this duration to keep the call active. If no keep-alive is received, the UCM automatically drops the call. Default setting is 1800 seconds (30 minutes).
Min SE (s)	Configures the Minimum Session Expiration threshold (in seconds) accepted by the UCM. If a remote endpoint or SIP provider requests a session timer shorter than this value, the UCM rejects the request. Default setting is 90 seconds.

TCP/TLS

The following table details the configuration parameters available under **PBX Settings -> SIP Settings -> TCP/TLS**. These options allow administrators to secure SIP communications by defining socket binding addresses, enforcing TLS certificate verification, managing CA/client certificates, and controlling allowed encryption cipher suites.

Enable TCP	Configure to allow incoming TCP connections with the PBX. The default setting is "No".
TCP Bind IPv4 Address	Configure the IP address for the TCP server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 5060. For example, 192.168.1.1:5062.
TCP Bind IPv6 Address	Configure the IPv6 address for the TCP server to bind to. "[::]" means bind to all interfaces. The port number is optional with the default being 5060. For example, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5060.
Enable TLS	Configure to allow incoming TLS connections with the PBX. The default setting is "Yes".
TLS Bind IPv4 Address	Configure the IPv4 address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 5061. For example, 192.168.1.1:5063. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.
TLS Bind IPv6 Address	Configure the IPv6 address for TLS server to bind to. "[::]" means bind to all interfaces. The port number is optional with default being 5061. For example, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5061. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.
Server Certificate Verification	If disabled, the TLS server's certificate will not be verified when acting as a client. The default setting is "No".
TLS CA Cert	This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server's public key. This file will be renamed as "TLS.ca" automatically.Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The size of the uploaded certificate file must be under 2MB.Users can click on the "Reset" button to reset this certificate
Private Certificate and Key	
TLS Cert	Upload the certificate file used for TLS connections. It must contain the client's private key and the server's signed certificate. Uploaded files will automatically be saved as "TLS.crt".Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The size of the uploaded certificate file must be under 2MB.
TLS Private Key	This file must be named with the CA subject name hash value. It contains CA's (Certificate Authority) public key, which is used to verify the accessed servers. This file will be renamed as "TLS.key" automatically.Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The size of the uploaded certificate file must be under 2MB.
Certificate & Private Key	Clicking on the Reset button will reset the certificates.
Cipher Suite	
Cipher Blocklist	By default, all SIP TLS encryption suites are in effect on the system, and when turned on, you can configure the encryption suites allowed to be used.
Cipher Suite	Select the encryption suites that are allowed to be used for SIP TLS connections, in the order of priority as configured.

NAT

External Host	
External Host	Configure a static IP address and port (optional) used in outbound SIP messages if the UCM630X is behind NAT. If it is a host name, it will only be looked up once.
Use IP address in SDP	If enabled, the SDP connection will use the IP address resolved from the external host.
Get External IP via STUN	If enabled, the external IP address will be retrieved via STUN. Please confirm the configured STUN server is working properly.
External UDP Port	Configure externally mapped UDP port when the PBX is behind a static NAT or PAT.
External TCP Port	Configure the externally mapped TCP port when the UCM630X is behind a static NAT or PAT.
External TLS Port	Configures the externally mapped TLS port when UCM630X is behind a static NAT or PAT.
Local Network Address	
Local Network Address	Specify a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly.A sample configuration could be as follows:192.168.0.0/16

ToS

The primary purpose of the Type of Service (ToS) page is allowing network administrators to configure QoS, SIP session lifecycles, and signaling behavior on the PBX.

The following table outlines the configuration options available under this page.

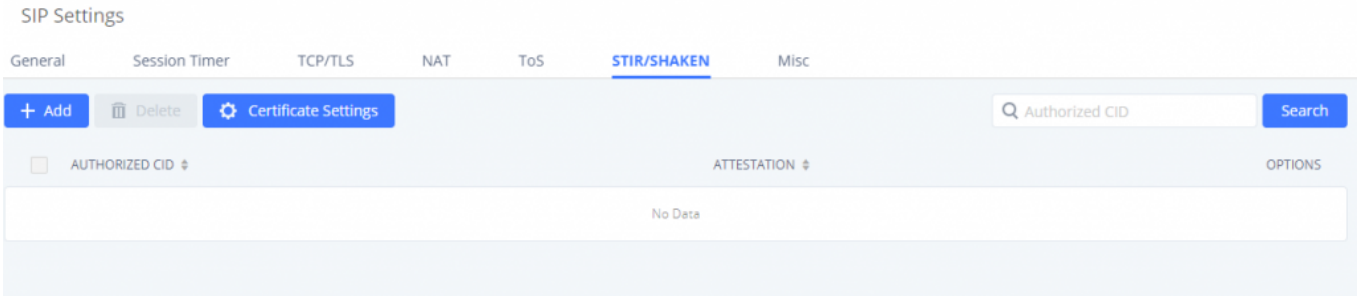
ToS for SIP	Configure the Type of Service for SIP packets. The default setting is None.
ToS for RTP Audio	Configure the Type of Service for RTP audio packets. The default setting is None.
ToS for RTP Video	Configure the Type of Service for RTP video packets. The default setting is None.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration.The default setting is 120.
Max Registration/Subscription Time	Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the UCM630X.The default setting is 3600.
Min Registration/Subscription Time	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM630X.The default setting is 60.
DTMF Mode	Select DTMF mode to send DTMF. The default setting is RFC4733. If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, "RFC4733" will be used if offered, otherwise "Inband" will be used.The default setting is "RFC4733".
RTP Timeout	During an active call, if there is no RTP activity within the timeout (in seconds), the call will be terminated. The default setting is no timeout.Note: This setting does not apply to calls on hold.
RTP Hold Timeout	When the call is on hold, if there is no RTP activity within the timeout (in seconds), the call will be terminated. This value of RTP Hold Timeout should be larger than RTP Timeout.The default setting is no timeout.
RTP Keep-alive (s)	This feature can be used to avoid abnormal call drop when the remote provider requires RTP traffic during proceeding.For example, when the call goes into voicemail and there is no RTP traffic sent out from UCM, configuring this option can avoid voicemail drop.When configured, RTP keep-alive packet will be sent to remote party at the configured interval. If set to 0, RTP keep-alive is disabled.

100rel	Configure the 100rel setting on UCM630X. The default setting is "Yes".
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted.The default setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not.The default setting is "No".
Generate In-band Ringing	Configure whether the UCM630X should generate Inband ringing or not. The default setting is "Never".Yes: The UCM630X will send 180 Ringing followed by 183 Session Progress and in-band audio.No: The UCM630X will send 180 Ringing if 183 Session Progress has not been sent yet. If audio path is established already with 183 then send in-band ringing.Never: Whenever ringing occurs, the UCM630X will send 180 Ringing as long as 200OK has not been set yet. Inband ringing will not be generated even the end point device is not working properly.
Server User Agent	Configure the user agent string for the UCM630X.
Send Compact SIP Headers	If enabled, compact SIP headers will be sent. The default setting is "No".
Passthrough PAI Header	Configures whether to preserve PAI headers from calling parties.
Replace '#' with %23 in SIP URI	If enabled, the '#' character in the SIP URI will be replaced with %23.

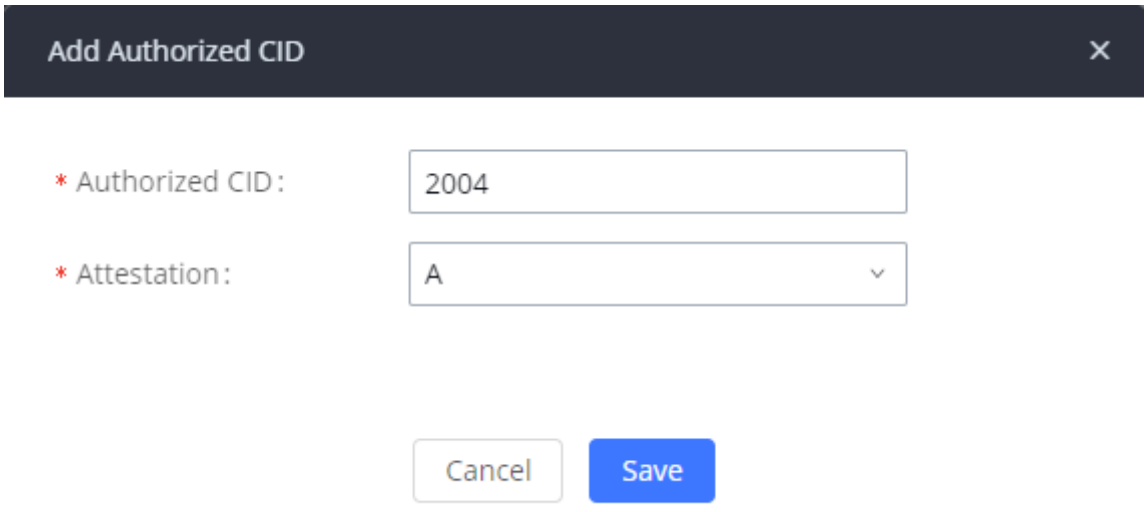
STIR/SHAKEN

To prevent robocalls, UCM now supports STIR/SHAKE protocols. Related options have been added as a new tab in the **SIP Settings** page.

Clicking on the **Add** button will show the following window:



STIR/SHAKEN

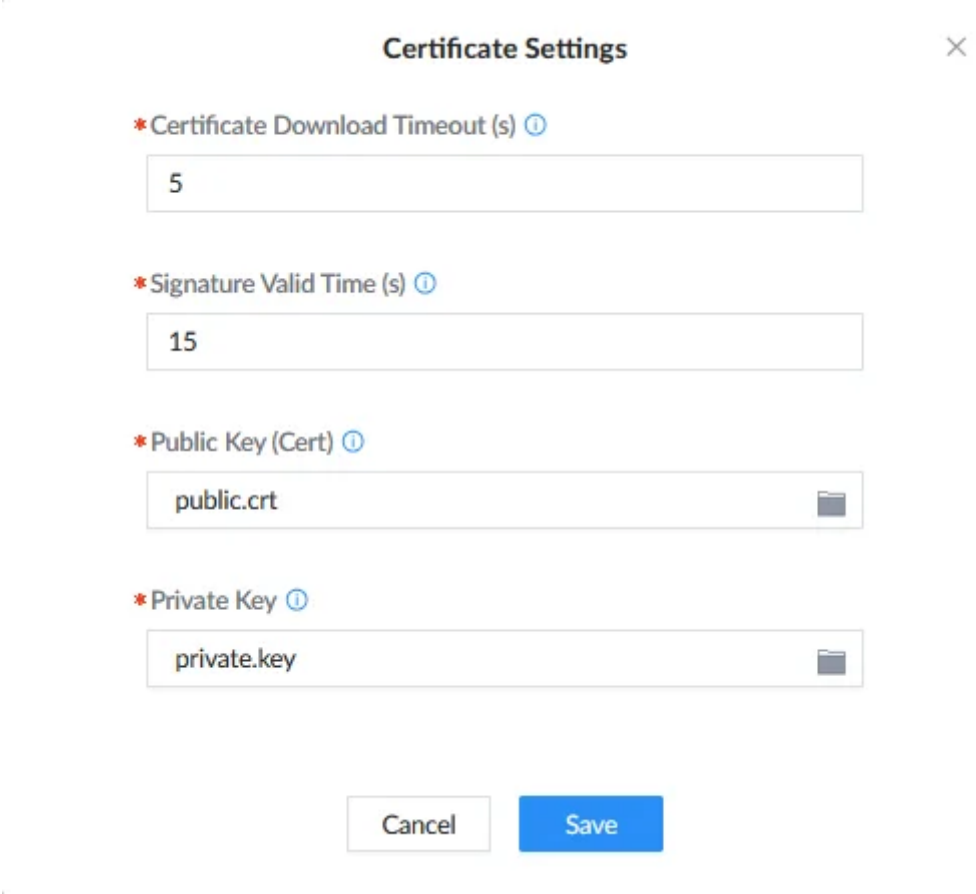


STIR/SHAKEN - Add Authorized CID and Attestation level

Authorized CID	Configure the authorized CID.

Attestation	Configure the attestation level, which is the level of confidence of the carrier that the CID has not been spoofed. The following options are available: A (Full attestation): The carrier is associated with the caller and the number. There is high confidence that the CID has not been spoofed. B (Partial attestation): The carrier is associated with the caller but not the number. There is uncertainty about whether the CID has been spoofed or not. C (Gateway attestation): The carrier is not associated with the caller and has no confidence at all about the number. Generally used for traceback.

Clicking on the **Certificate Settings** button will bring up the following window:



STIR/SHAKEN - Certificate Settings

Certificate Download Timeout (s)	Configure the public key download timeout period, the default value is 2 seconds.
Signature Valid Time (s)	Configure the validity period of the digital signature, the default value is 15 seconds.
Public Key (Cert)	Configure the Public Key.Note: The uploaded file must be less than 2MB in file size, only supports the .crt format and must be ECC type. This file will automatically be renamed to "public.crt".
Private Key	Configure the Private key. Note: The uploaded file must be less than 2MB in file size, only supports the .key format and must be ECC type. This file will automatically be renamed to "private.key".

MISC

This section allows administrators to configure general SIP protocol behavior, system security rules, call handling policies, and media options across the UCM6300 series.

Parameter	Description
Outbound SIP Registrations	
Register Timeout	Configure the register retry timeout (in seconds). The default setting is 20.
Register Attempts	Configure the number of registration attempts before the UCM630X gives up. The default setting is 0, which means the UCM630X will keep trying until the server side accepts the registration request.
Initial REGISTER Delay Interval (s)	Configures the time window within which to send initial trunk registration requests. Instead of sending out all initial trunk registration requests at once, requests will be randomly sent out within this period. The default setting is 10.
Video	
Support SIP Video	Select to enable video support in SIP calls. The default setting is "Yes".
Security	
Reject Non-Matching INVITE	If enabled, when rejecting an incoming INVITE or REGISTER request, the UCM630X will always reject with "401 Unauthorized" instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. Default setting is "No".
SDP Attribute Passthrough	
Enable Attribute Passthrough	If enabled, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passed through.
Early Media	
Enable Use of Final SDP	If enabled, call negotiation will use final response SDP.
Ignore 180 Response	If enabled, ringing indication after 183 response will be ignored.
Transfer	
Allow Transfer	If checked, all transfers initiated by endpoints will be enabled.
Allow callback to transferer when blind transfer fails	If enabled, the UCM will call back to the transferrer when blind transfer fails (reason of failure includes busy and no answer). Note: This feature takes effect only on internal calls.
Blind transfer timeout	Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s.
Allow Early Blind Transfer	Enabling this allows callers to perform transfers while the original callee's phone is still ringing during attended transfer. Note: Requires compatible endpoints such as Grandstream GRP261x on firmware 1.0.15.8 or higher.
Hold	
Forward HOLD Requests	Configure the UCM to forward HOLD requests instead of processing holds internally. This serves to meet the standards set by some providers that require HOLD requests to be passed along from endpoint to endpoint. This option is disabled by default. Note: Enabling this option may cause hold retrieval issues and MOH to not be heard.

Transparent Call-Info header

UCM supports transparent call info header in order to integrate GDS door system with GXP21XX/GRP261X phones, the UCM will forward the call-info header to the phone in order to request the live view from GDS door system and give the option to open the door via softkey.

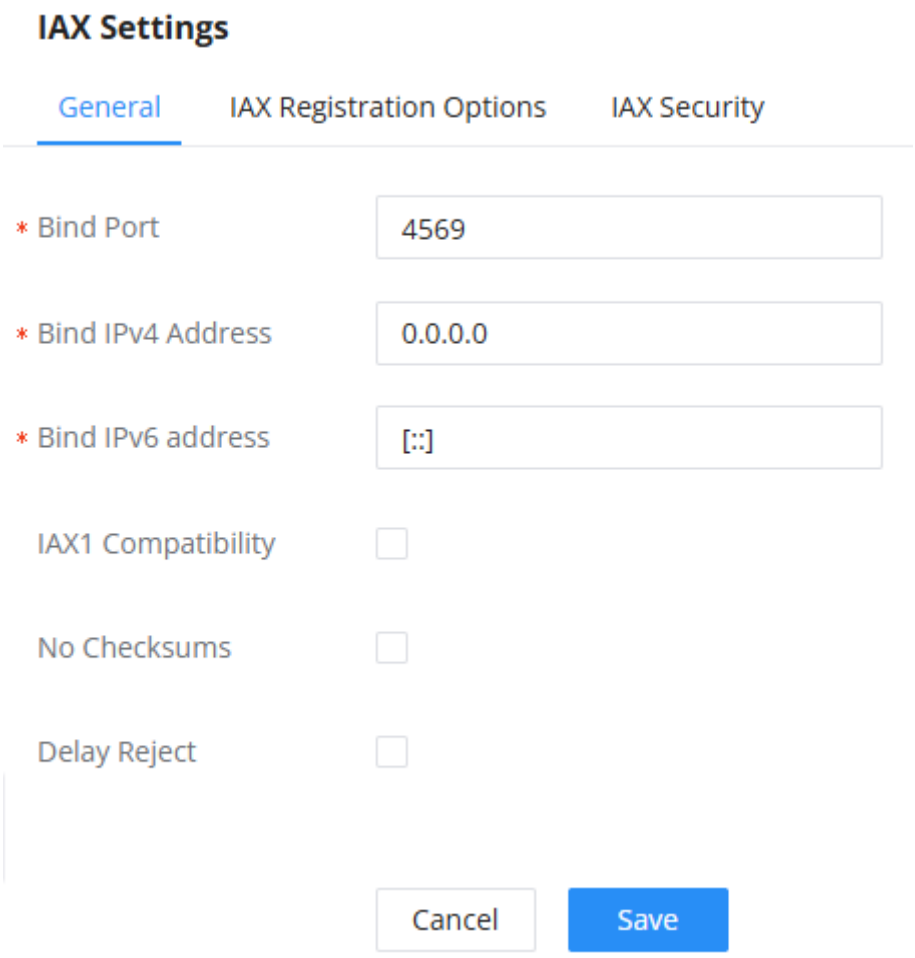
```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:3001@192.168.6.36:5064 SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 192.168.6.187:5060;rport;branch=z9hG4bKPj3217e67b-e74f-4f9f-b06f-afd3dcbbe29b
    From: "3002" <sip:3002@192.168.6.187>;tag=202dca4f-2b9d-4880-924c-d48cea7d0596
    To: <sip:3001@192.168.6.36>
    Contact: <sip:68aae6ea-f1d4-4e62-9987-446e718a2448@192.168.6.187:5060>
    Call-ID: 7f66bb20-0b9f-4828-a355-698853b8d9fb
    CSeq: 17559 INVITE
    Allow: OPTIONS, INFO, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REGISTER, REFER
    Supported: 100rel, timer, replaces, norefersub
    Session-Expires: 1800
    Min-SE: 90
    Call-Info: <https://192.168.6.186:443/capture/8001> ;purpose=GDS-view
    Max-Forwards: 70
    User-Agent: Grandstream UCM6202V1.5A 1.0.13.15
    Content-Type: application/sdp
    Content-Length:   547
  Message Body
```

Transparent Call-Info

IAX Settings

The UCM630X IAX global settings can be accessed via **PBX Settings** > **IAX Settings**.

General

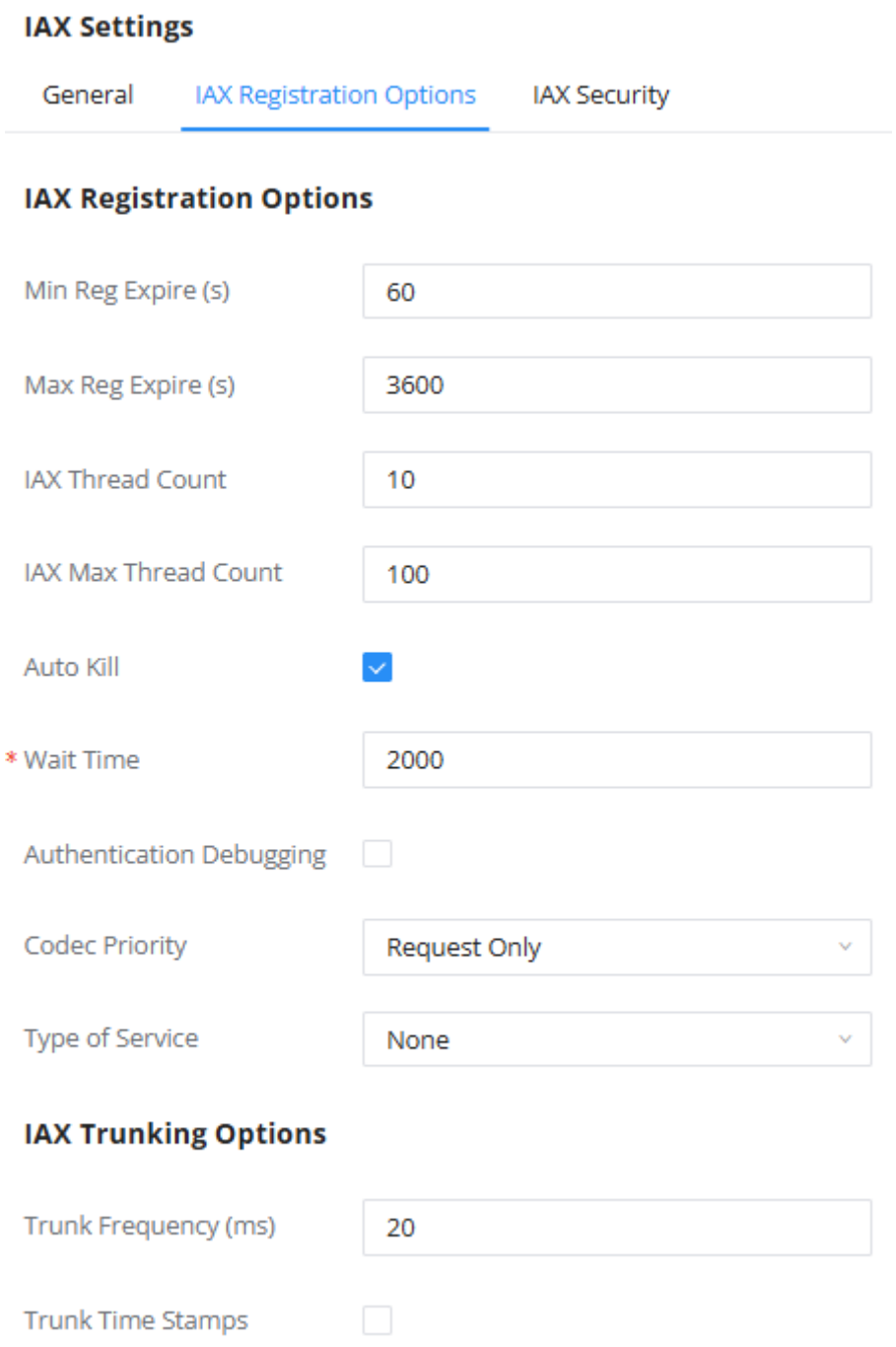


IAX General Settings

Bind Port	Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569.
Bind IPv4 Address	Force IAX2 to bind to a specific address instead of all addresses.

Bind IPv6 address	Configure the IPv6 address to bind to. "[::]" means to bind to all IP addresses.
IAX1 Compatibility	Select to configure IAX1 compatibility. The default setting is "No".
No Checksums	If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this feature. The default setting is "No".
Delay Reject	If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is "No".

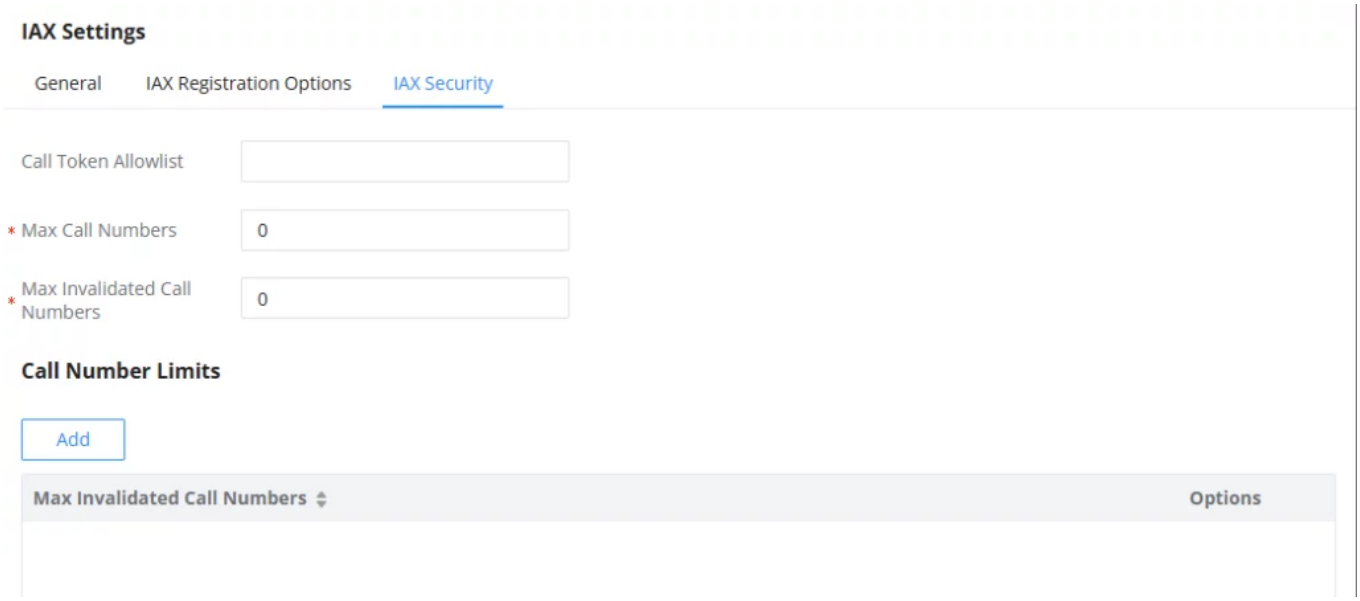
IAX Registration Options



IAX Registration Options	
Min Reg Expire (s)	Configure the minimum period (in seconds) of registration. The default setting is 60.

Max Reg Expire (s)	Configure the maximum period (in seconds) of registration. The default setting is 3600.
IAX Thread Count	Configure the number of IAX helper threads.The default setting is 10.
IAX Max Thread Count	Configure the maximum number of IAX threads allowed.The default is 100.
Auto Kill	If enabled and no ACK is received for new messages after the specified wait time, the connection will be terminated.
Wait Time	If no ACK is received within the configured waiting time, the connection will automatically be terminated. The default setting is 2000 ms.
Authentication Debugging	If enabled, authentication traffic in debugging will not show.The default is "No".
Codec Priority	Configure codec negotiation priority. The default setting is "Reqonly". Caller: Consider the callers preferred order ahead of the host's. Host: Consider the host's preferred order ahead of the caller's. Disabled: Disable the consideration of codec preference all together. Reqonly: This is the same as "Disabled", except when the requested format is not available. The call will only be accepted if the requested format is available.
Type of Service	Configure ToS bit for preferred IP routing.
IAX Trunking Options	
Trunk Frequency (ms)	Configure the frequency of trunk frames (in milliseconds).The default is 20.
Trunk Time Stamps	If enabled, time stamps will be attached to trunk frames.The default is "No".

IAX Security



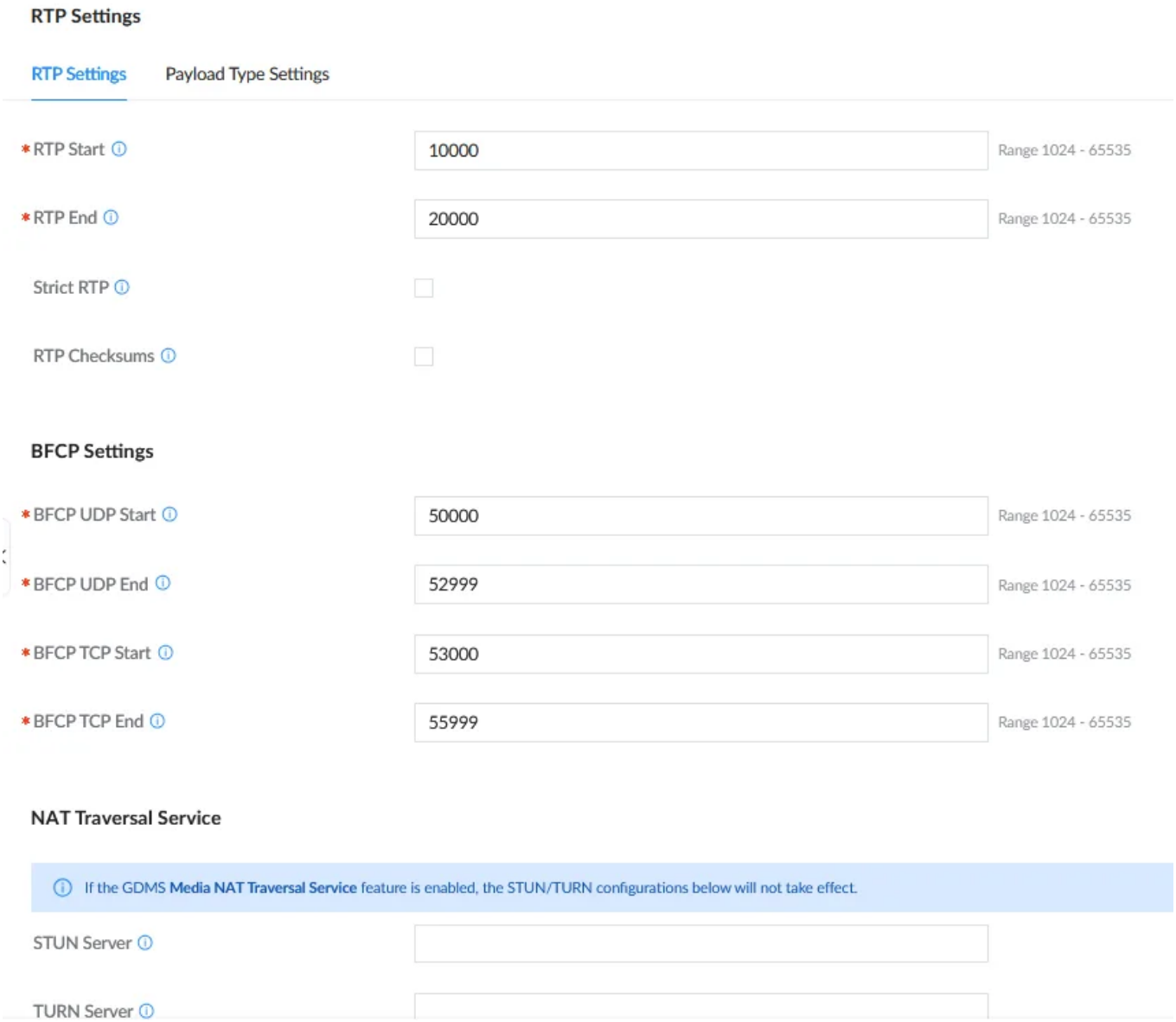
Call Token Allowlist	Enter a single IP address (e.g., 1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) for which call token validation is not required.
Max Call Numbers	Configure the maximum number of calls allowed for a single IP address. If set to 0, there will be no limit. The default setting is "0".
Max Invalidated Call Numbers	Configure the maximum number of invalidated calls for all IP addresses combined. If set to 0, there will be no limit. The default setting is "0".
Call Number Limits	
IP or IP Range	Enter the IP address (1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) to be considered for call number limits.

Max Call Numbers	Configure to limit the number of calls for a give IP address of IP range.

RTP Settings

RTP Settings

The configuration parameters under **PBX Settings -> SIP Settings -> RTP Settings** allow to manage real-time media port ranges, protocol security checks, and NAT traversal server addresses.



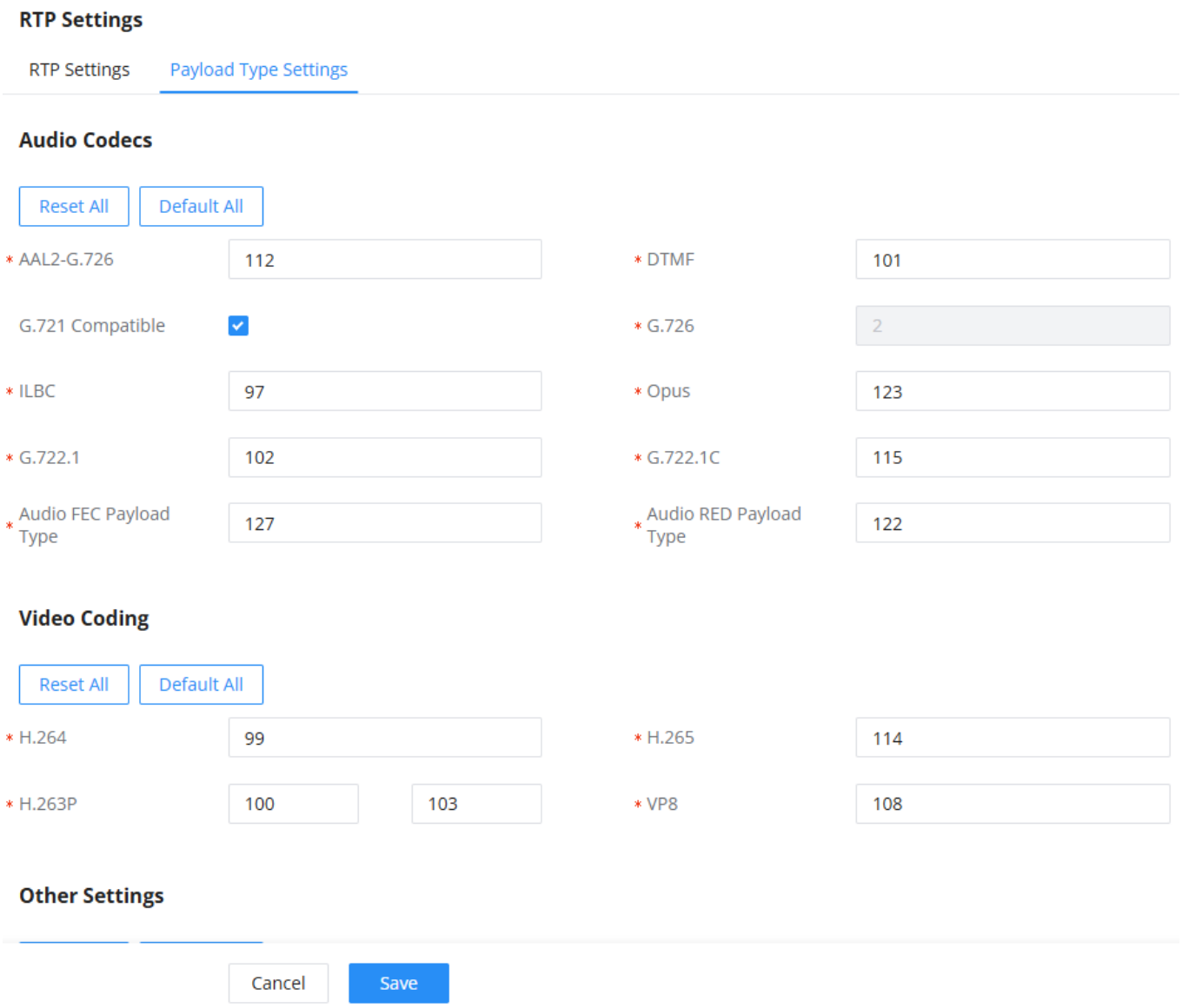
RTP Settings

RTP Start	Configure the RTP port starting number. The default setting is 10000.
RTP End	Configure the RTP port ending address. The default setting is 20000.
Strict RTP	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is "Disable".
RTP Checksums	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".
BFCP Settings	
BFCP UDP Start	Configure BFCP UDP port starting number. The default setting is 50000.

BFCP UDP End	Configure BFCP UDP port ending number. The default setting is 52999.
BFCP TCP Start	Configure BFCP TCP port starting number. The default setting is 53000.
BFCP TCP End	Configure BFCP TCP port ending number. The default setting is 55999.
NAT Traversal Service	
STUN Server	Configure STUN server address. STUN protocol is a Client/Server and also a Request/Response protocol. It is used to check the connectivity between the two terminals, such as maintaining a NAT binding entries keep-alive agreement. The default STUN Server is stun.ipvideotalk.com.Valid format:[(hostname | IP-address) [':' port]The default port number is 3478 if not specified.
TURN Server	Configure TURN server address. TURN is an enhanced version of the STUN protocol and is dedicated to the processing of symmetric NAT problems.
TURN Server Name	Configure turn server account name
TURN Server Password	Configure turn server account password.
Connection Protocol	Protocol used to connect to the TURN server.
Number of ICE Candidates	This configures the number of pre-collected ICE candidates to gather and send to remote peers. The higher the number, the greater the network traffic consumption.

Payload Type Settings

The UCM630X payload type for audio codecs and video codes can be configured here.



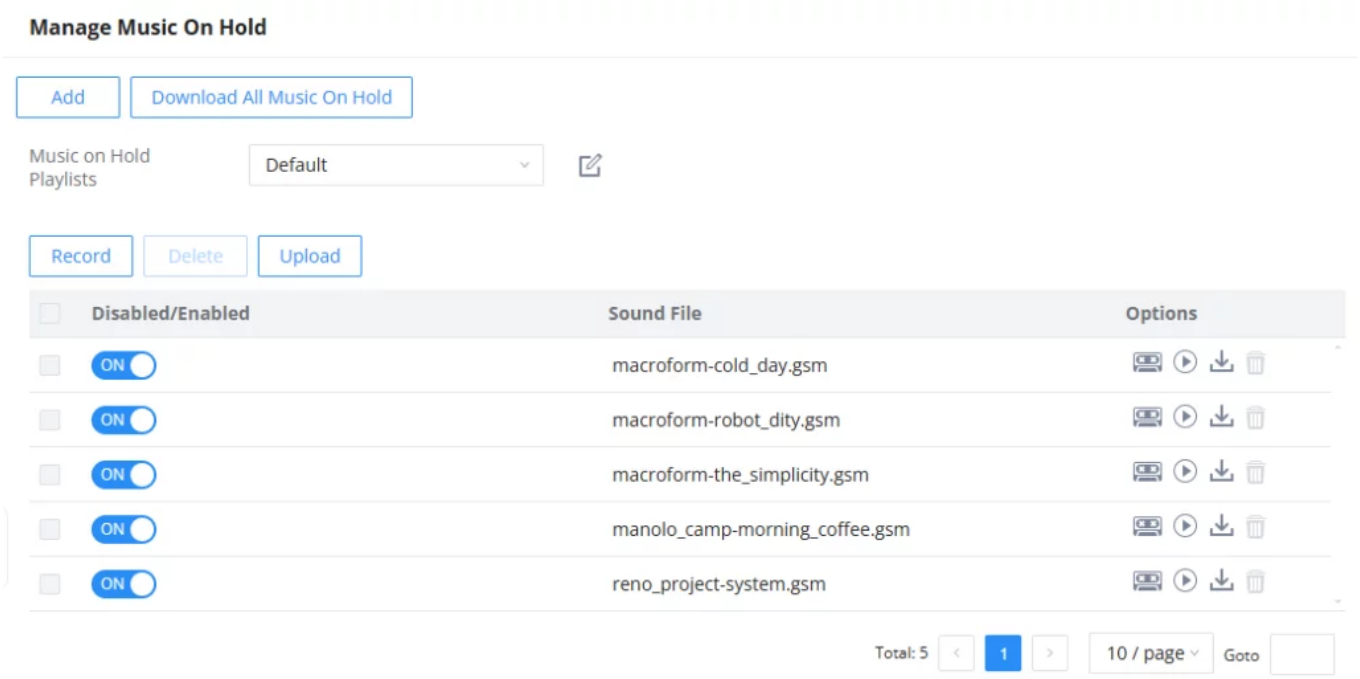
Payload Type Settings

Audio Codecs	
DTMF	Configured payload type for DTMF. The default setting is 101.
G.721 Compatible	Configure to enable/disable G.721 compatible. The default setting is Yes.
G.726	Configure the payload type for G.726 if "G.721 Compatible" is disabled. The default setting is 111.
iLBC	Configure the payload type for iLBC. The default setting is 97.
OPUS	Configure the payload type for OPUS. The default setting is 123.
G.722.1	G.722.1:Low-complexity coder, 24kbps.
G.722.1C	G.722.1C:Low-complexity coder, 48kbps.
Audio FEC Payload Type	Configure the Audio FEC Payload Type. The default setting is 127
Audio RED Payload Type	Configure the Audio RED Payload Type. Default setting is 122
Video Coding	
H.264	Configure the payload type for H.264. The default setting is 99.
H.265	Configure the payload type for H.265. The default setting is 114.
H.263P	Configure the payload type for H.263+. The default setting is 100 103.

VP8	Configure the payload type for VP8. The default setting is 108.
Other Settings	
Video FEC	Configure the Main Video FEC
RTP FECC	Configure the RTP FECC
RTX	Configure the RTX

Music On Hold

Music On Hold settings can be accessed via **PBX Settings** > **Music On Hold**. In this page, users could configure music on hold class and upload music files. The "default" Music On Hold class already has 5 audio files defined for users to use.



Music On Hold Default Class

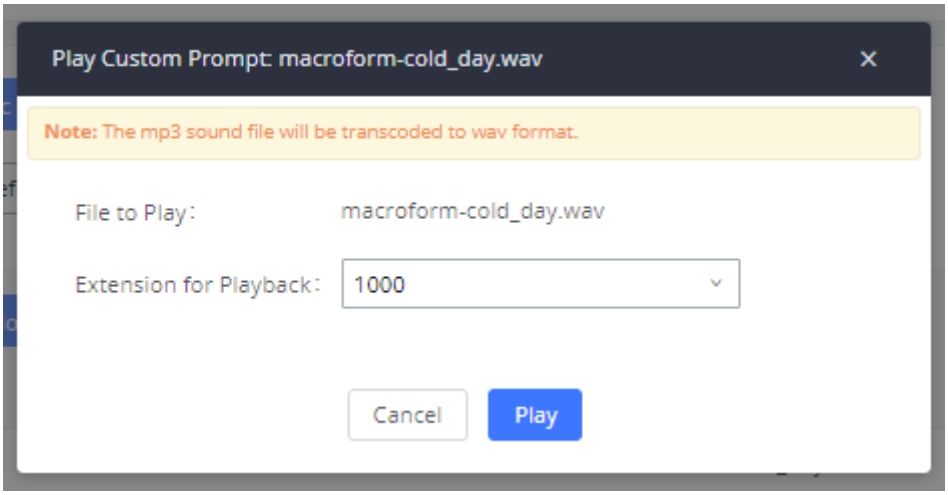
- Click on "Create New MOH Class" to add a new Music On Hold class.
- Click on to configure the MOH class sort method to be "Alpha" or "Random" for the sound files.
- Click on next to the selected Music On Hold class to delete this Music On Hold class.
- Click on to start uploading. Users can upload:
- Single files with 8KHz Mono Music file, or
- Music on hold files in a compressed package with .tar, .tar.gz and .tgz as the suffix. The file name can only be letters, digits, or special characters -_
- the size for the uploaded file should be less than 30M, the compressed file will be applied to the entire MoH.

- Users could also download all the music on hold files from UCM. In the Music On Hold page, click and the file will be downloaded to your local PC.
- Click on to disable it from the selected Music On Hold Class.
- Click on to enable it from the selected Music On Hold Class.
- Select the sound files and click on to delete all selected Music On Hold files.

The UCM630X allows Users to select the Music On Hold file from WebGUI to play it. The UCM630X will initiate a call to the selected extension and play this Music On Hold file once the call is answered.

Steps to play the Music On Hold file:

1. Click on the button for the Music On Hold file.
2. In the prompted window, select the extension to playback and click .

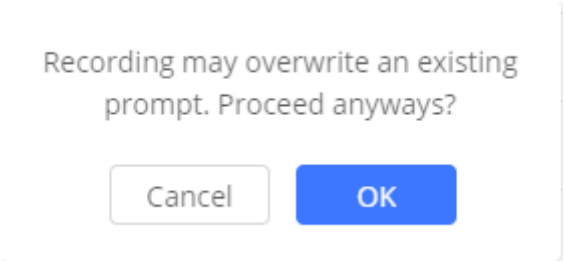


Play Custom Prompt

3. The selected extension will ring.
4. Answer the call to listen to the music playback.

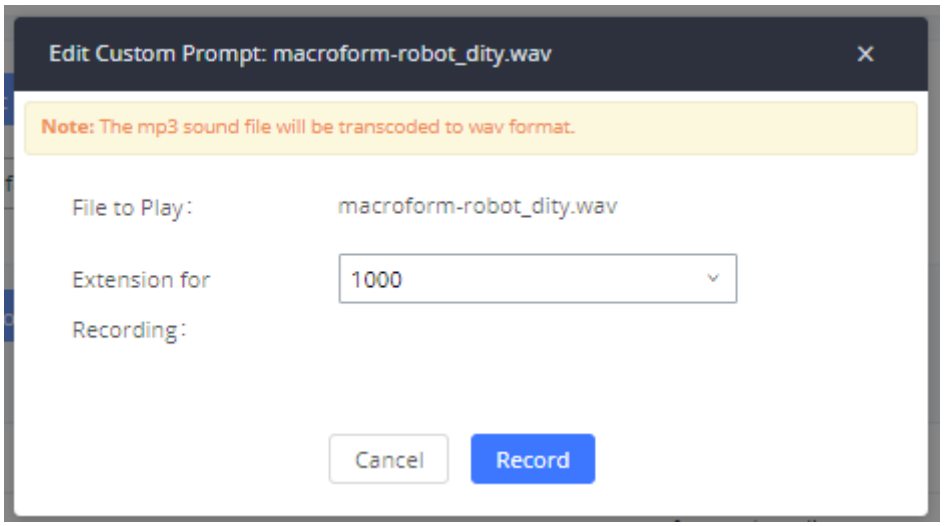
Users could also record their own Music On Hold to override an existing custom prompt, this can be done by following those steps:

1. Click on .
2. A message of confirmation will pop up, as shown below.



Information Prompt

3. Click .
4. In the prompted window, select the extension to playback and click .



Record Custom Prompt

5. Answer the call and start to record your new music on hold.
6. Hangup the call and refresh Music On Hold page then you can listen to the new recorded file.

Once the MOH file is deleted, there are two ways to recover the music files.

- Users could download the MOH file from this link: http://downloads.asterisk.org/pub/telephony/sounds/releases/asterisk-moh-opsound-wav-2.03.tar.gz

After downloading and unzip the pack, users could then upload the music files to UCM.

- Factory reset could also recover the MOH file on the UCM.

Voice Prompt

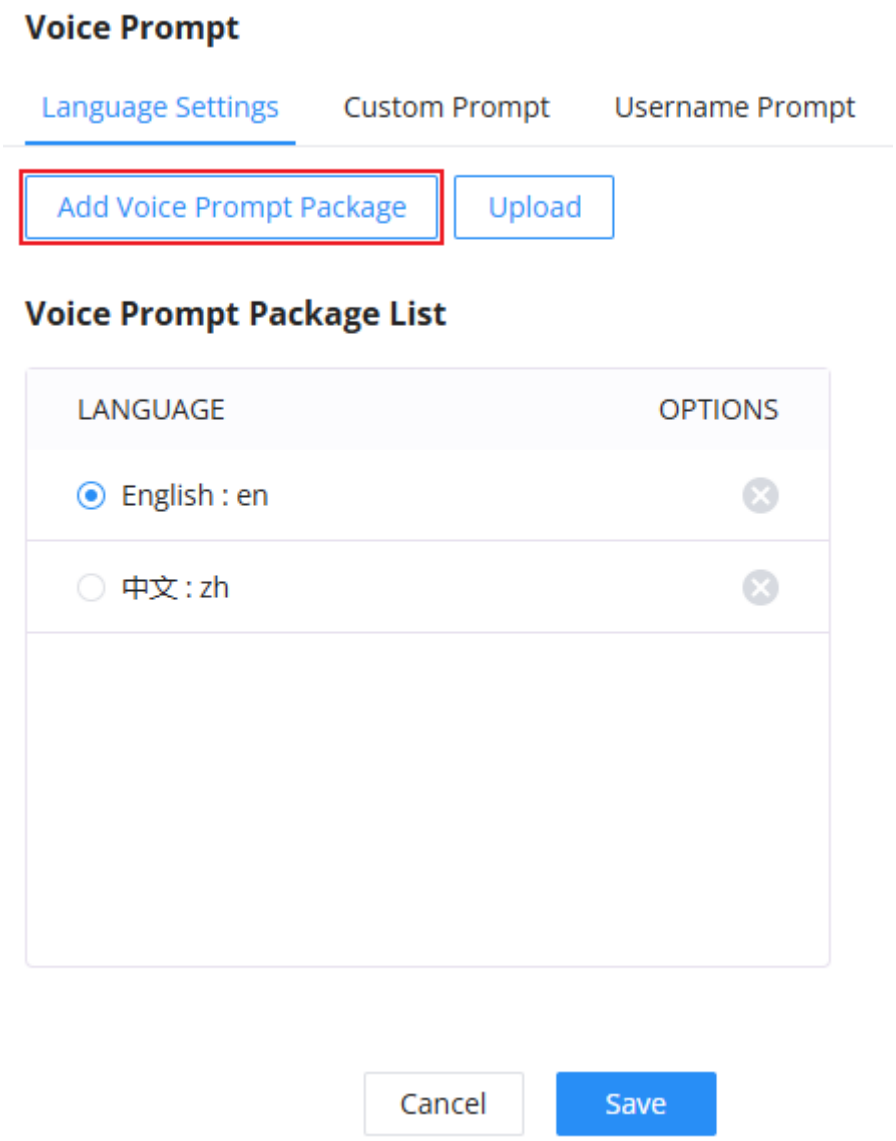
The UCM630X supports multiple languages in Web GUI as well as system voice prompt. Currently, there are 16 languages supported in system voice prompt: British English, Deutsch, English, Spanish, Spanish (Catalonia), Spanish (Spain), Greek, French, Italian, Dutch, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Swedish, Turkish, Czech, Ukrainian, Hebrew, Arabic, and Chinese.

English (United States) and Chinese voice prompts are built in with the UCM630X already. The other languages provided by Grandstream can be downloaded and installed from the UCM630X Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the UCM630X.

Language settings for voice prompt can be accessed under **PBX Settings** > **Voice Prompt** > **Language Settings**.

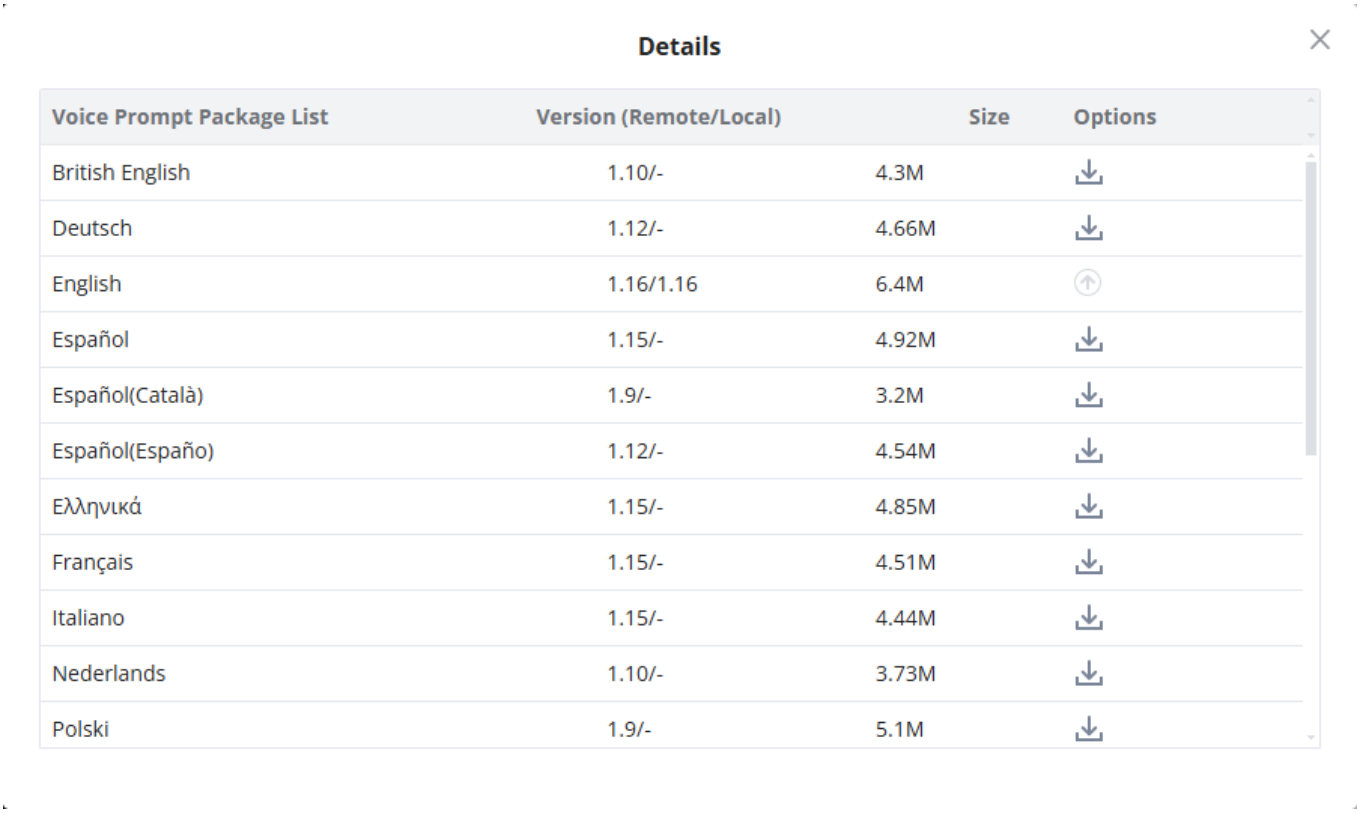
Download and Install Voice Prompt Package

To download and install voice prompt package in different languages from UCM630X Web GUI, click on "Add Voice Prompt Package" button.



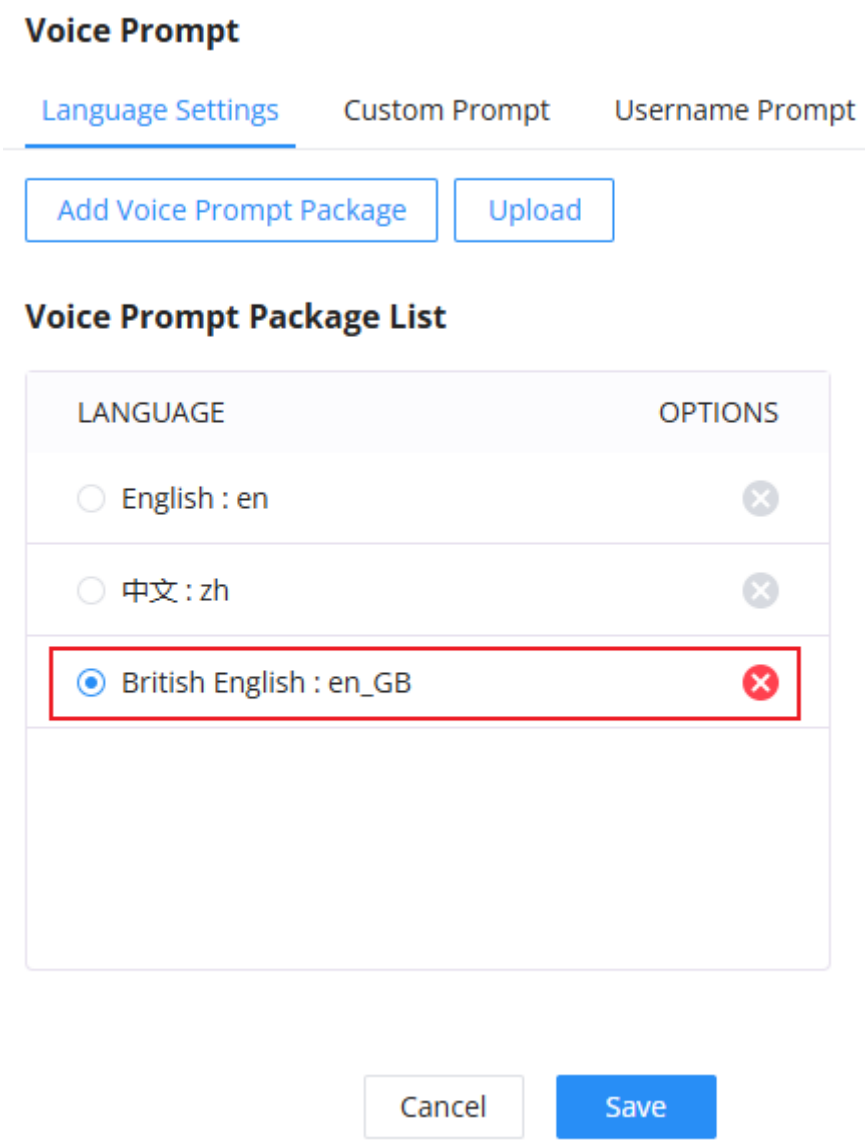
Language Settings for Voice Prompt

A new dialog window of voice prompt package list will be displayed. Users can see the version number (latest version available V.S. current installed version), package size and options to upgrade or download the language.



Voice Prompt Package List

Click on to download the language to the UCM630X. The installation will be automatically started once the downloading is finished.



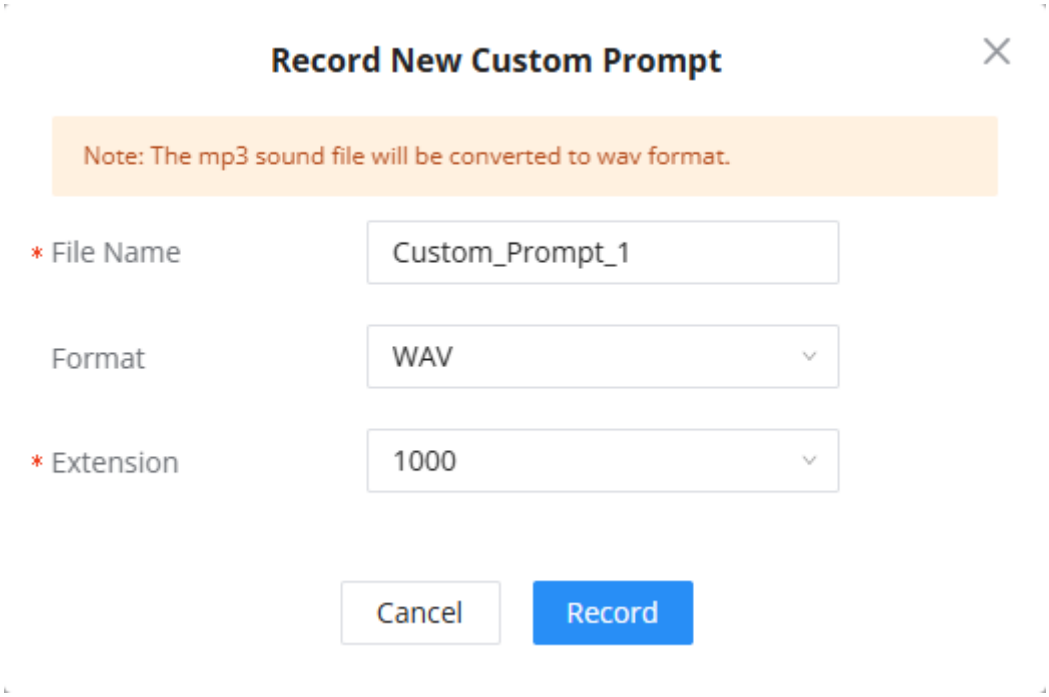
New Voice Prompt Language Added

A new language option will be displayed after successfully installed. Users then could select it to apply in the UCM630X system voice prompt or delete it from the UCM630X.

Custom Prompt

Record New Custom Prompt

In the UCM630X **PBX Settings > Voice Prompt > Custom Prompt** page, click on "Record" and follow the steps below to record new IVR prompt.



Record New Custom Prompt

1. Specify the file name.
2. Select the format (GSM or WAV) for the prompt file to be recorded.
3. Select the extension to receive the call from the CloudUCM to record the custom prompt.
4. Click the "Record" button. A request will be sent to CloudUCM to call the extension for recording the custom prompt from the phone.
5. Pick up the call from the extension and start the recording following the voice prompt.
6. Once saved, the new custom prompt will be listed on this page. From here, you can manage it by selecting an action:

- **Online Playback:** listen to the prompt directly from the Web GUI.
- **Playback Using Extension:** select an extension to hear the prompt played over a call.
- **Record Again:** replace the current recording with a new one.
- **Download:** download the custom prompt recorded.
- **Delete:** remove the prompt from the system.



Custom Prompt Page

Upload Custom Prompt

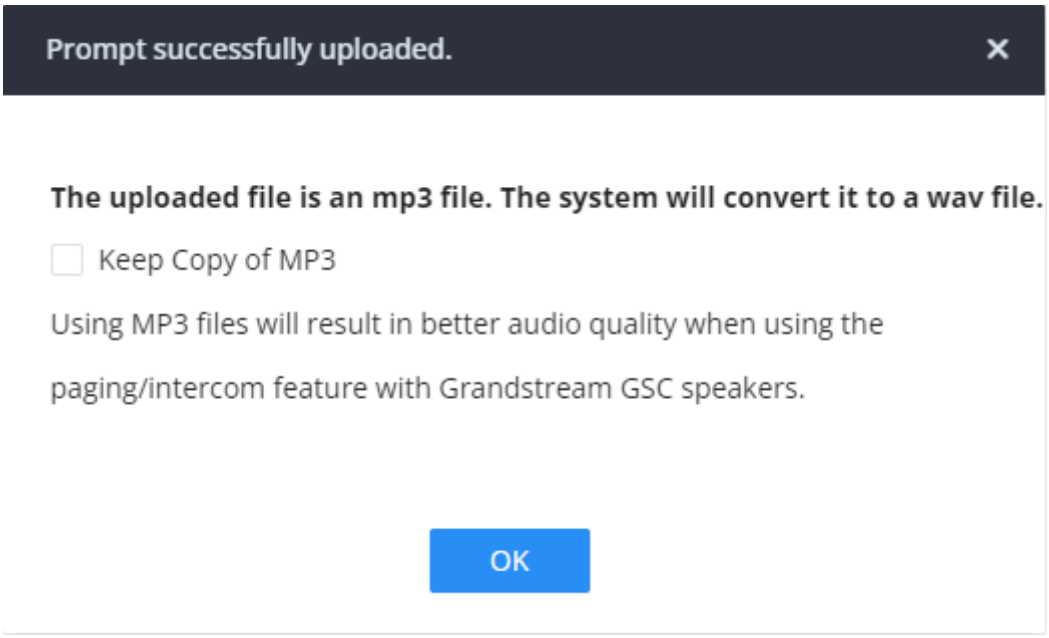
If the user has a pre-recorded IVR prompt file, click on "Upload" in Web GUI→PBX Settings→**Voice Prompt**

→**Custom Prompt** page to upload the file to the UCM630X. The following are required for the IVR prompt file to be successfully uploaded and used by the UCM630X:

- PCM encoded.
- 16 bits.
- 8000Hz mono.
- In .mp3 or .wav format; or raw/ulaw/alaw/gsm file with .ulaw or .alaw suffix.
- File size under 5MB.

Click on button, select the file you want to upload, then click on "choose file to upload" to start uploading. Once uploaded, the file will appear in the Custom Prompt web page.

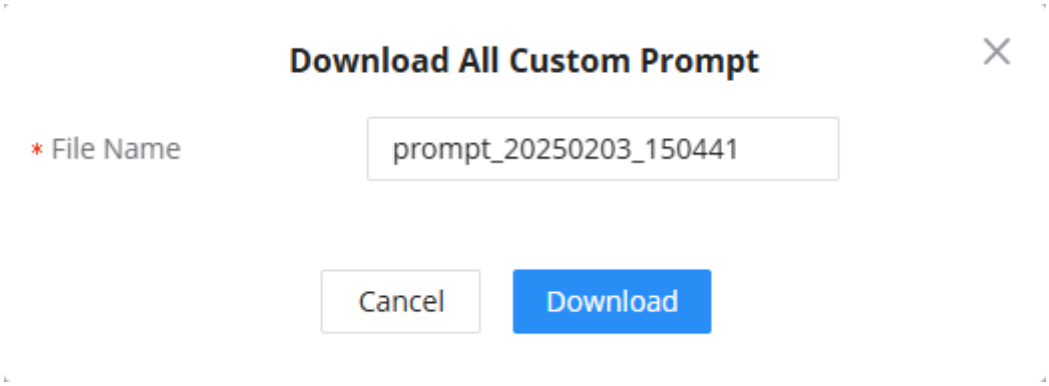
If the file uploaded is mp3, the following prompt will appear.



Tick "Keep Copy of MP3" to keep an mp3 copy of the file which can be diffused with certain GSC speakers. Diffusing the MP3 files result in a highr quality sound played by GCS speakers.

Download All Custom Prompt

On the UCM630X, the users can download all custom prompts from UCM Web GUI to local PC. To download all custom prompt, log in UCM Web GUI and navigate to **PBX Settings→Voice Prompt→Custom Prompt** and click on "Download All". The following window will pop up in order to set a name for the downloaded file.



Download All Custom Prompt

The downloaded file will have a .tar extension.

Username Prompt

There are two ways to customize/set new username prompt:

Upload Username Prompt File from Web GUI

1. First, Users should have a pre-recorded file respecting the following format:

   - PCM encoded / 16 bits / 8000Hz mono.
   - In .tar/.tar.gz/.tgz format
   - File size under 30M.
   - Filename must be set as the extension number with 18 characters max. For example, the recorded file name 1000.wav will be used for extension 1000.
2. Go under web GUI **PBX Settings → Voice Prompt → Username Prompt** and click on "**Upload**" button.
3. Select the recorded file to upload it and press Save and Apply Settings.

   - Click on to record again the username prompt.
   - Click on to play recorded username prompt.
   - Select username prompts and press to delete specific file or select multiple files for deletion using the button "**Delete**" .

Record Username via Voicemail Menu

The second option to record username is using voicemail menu, please follow below steps:

- Dial *98 to access the voicemail
- After entering the desired extension and voicemail password, dial "0" to enter the recordings menu and then "3" to record a name.

Another option is that each user can record their own name by following below steps:

- The user dials *97 to access his/her voicemail
- After entering the voicemail password, the user can press "0" to enter the recordings menu and then "3" to record his name.

Call Prompt Tones

SIP Trunk Prompt Tone

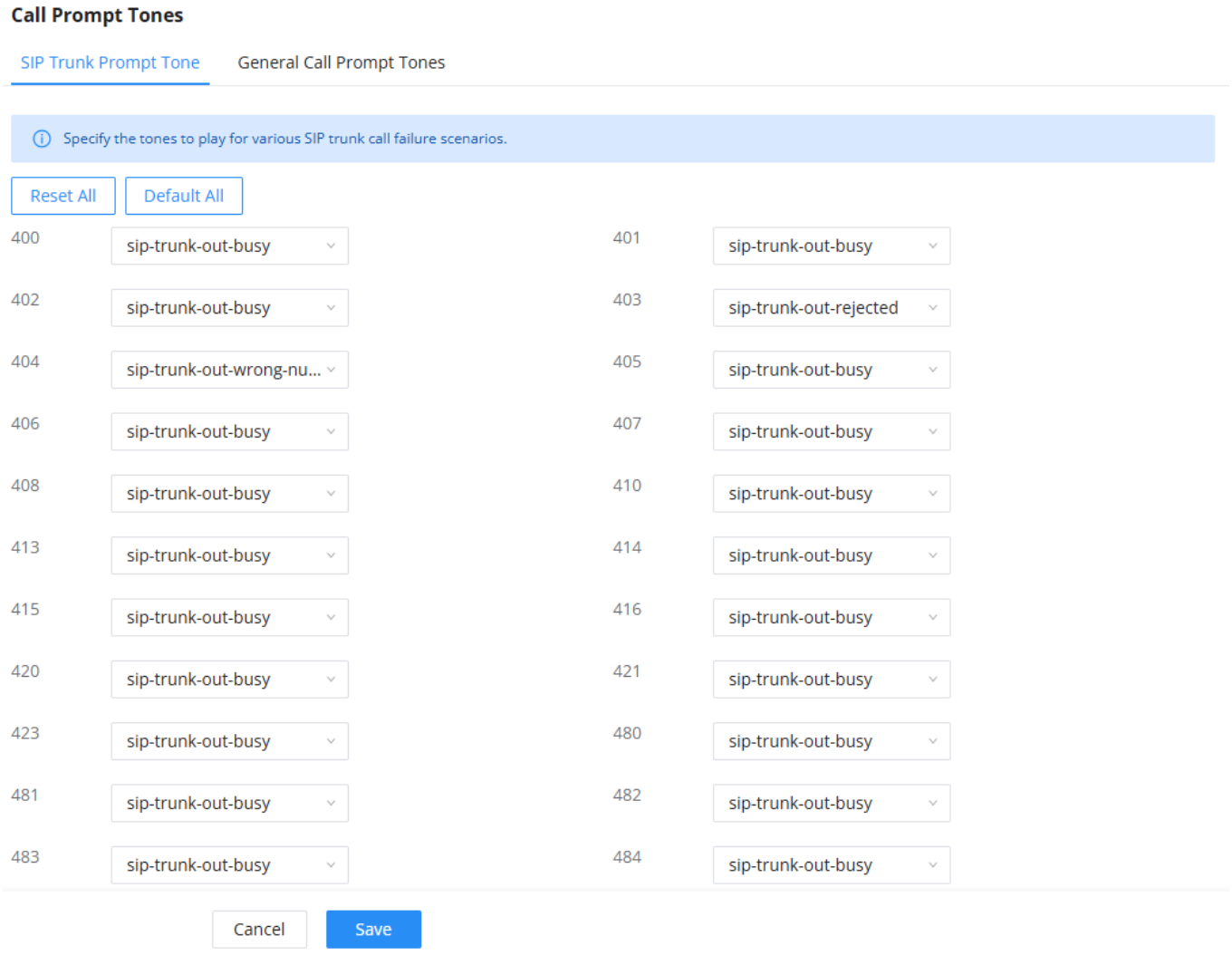
Prompt Tone Settings tab on the UCM helps users choose which prompt will be played by the UCM during call failure, the voice message responses can be set to be played for 4XX, 5XX, and 6XX call failures.

The following **default prompt names** and their associated messages are supported:

Prompt Name	Message Played
sip-trunk-out-busy	"All circuits are busy now. Please try again later."
sip-trunk-out-rejected	"The call was rejected by the server. Please try again later."
sip-trunk-out-server-error	"Server error. Please check your device."
sip-trunk-out-wrong-number	"Your call can't be completed as dialed. Please check the number and dial again."
general-failed	"Your call cannot be completed as dialed."

no-answer	"The number you dialed is not answering. Please try again later."
no-permission	"You are not allowed to dial this number."
user-busy	"The number you have dialed is busy. Please try again later."
wrong-number	"The number you dialed is incorrect. Please check the number and dial again."

Additionally, custom voice messages recorded and uploaded in **PBX Settings->Voice Prompt->Custom Prompt** can be used for the failure responses instead of the default messages.



SIP Trunk Prompt Tone

Use the following reference table to look up SIP status codes and their associated failure reasons when configuring SIP Trunk Prompt Tones.

SIP Response Code	Description
4xx Client / Request Failure Responses	
400	Bad Request: The request could not be understood due to malformed syntax.
401	Unauthorized: The request requires user authentication.
402	Payment Required: Reserved for future use (used by some providers for credit exhaustion).
403	Forbidden: The server understood the request but refuses to fulfill or authorize it.

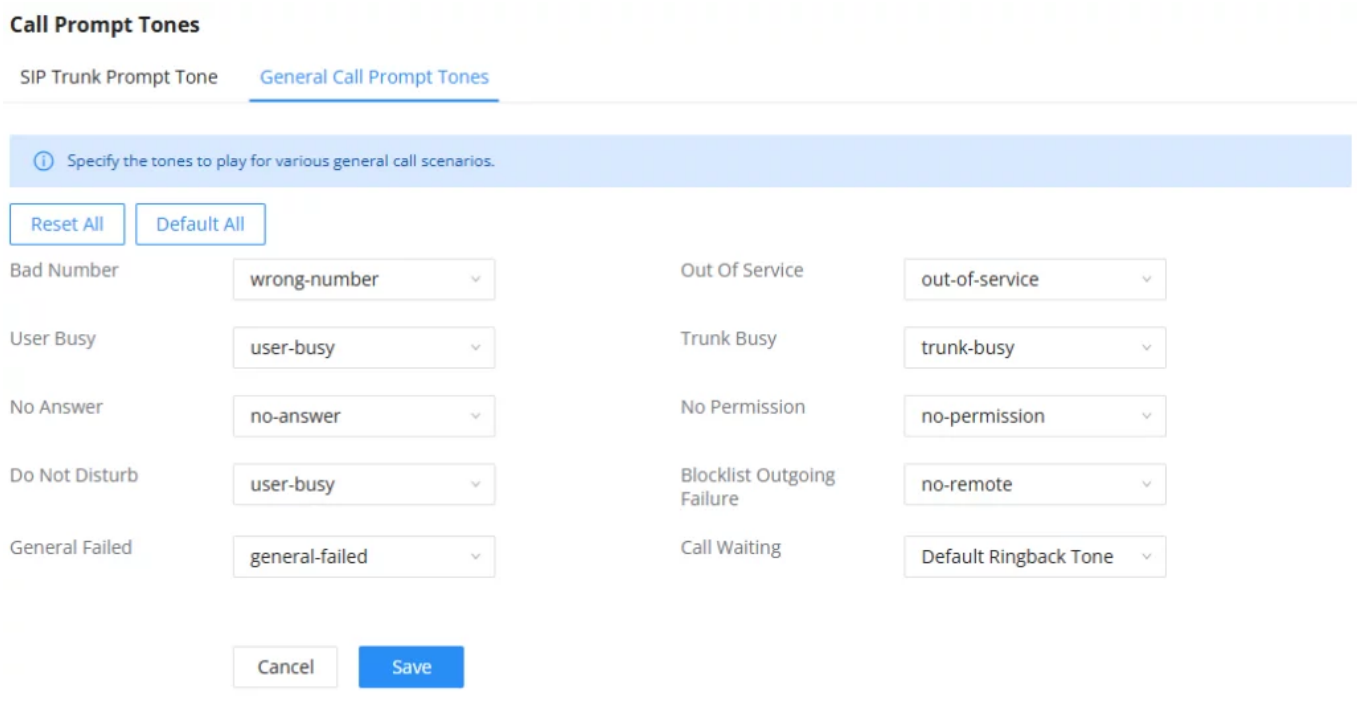
404	Not Found: The target user or URI does not exist in the system domain.
405	Method Not Allowed: The request method is not supported by the addressed resource.
406	Not Acceptable: The resource is only capable of generating responses not acceptable according to Accept headers.
407	Proxy Authentication Required: The request requires authentication with a proxy server first.
408	Request Timeout: The server could not produce a response within the timeout period.
410	Gone: The requested resource is no longer available and no forwarding address is known.
413	Request Entity Too Large: The request body payload is larger than the server is willing or able to process.
414	Request-URI Too Long: The server refuses to service the request because the Request-URI is too long.
415	Unsupported Media Type: The request body format is not supported by the destination.
416	Unsupported URI Scheme: The server cannot process the Request-URI scheme.
420	Bad Extension: Bad SIP protocol extension used; protocol extension not understood by server.
421	Extension Required: The server needs a specific extension not listed in the Supported header.
423	Interval Too Brief: The requested registration expiration time is too short.
480	Temporarily Unavailable: The callee is unavailable at this moment (e.g., offline or unassigned).
481	Call/Transaction Does Not Exist: The server received a request that does not match any existing dialog or transaction.
482	Loop Detected: The server detected a request routing loop.
483	Too Many Hops: The Max-Forwards header value has reached zero.
484	Address Incomplete: The Request-URI address is incomplete (e.g., partial extension dialed).
485	Ambiguous: The Request-URI is ambiguous and could match multiple destinations.
486	Busy Here: The callee's endpoint is currently busy on another call.
487	Request Terminated: The request was cancelled by a CANCEL message or timed out.
488	Not Acceptable Here: Media parameter negotiations (e.g., codecs) are not acceptable.
491	Request Pending: The server has a pending request for the same dialog.
493	Undecipherable: The body of the request is encrypted and the receiver cannot decrypt it.
5xx Server Failure Responses	
500	Server Internal Error: The server encountered an internal error and could not fulfill the call request.
501	Not Implemented: The server does not support the functionality required to fulfill the request.
502	Bad Gateway: The server received an invalid response from a downstream server while attempting to route the call.

503	Service Unavailable: The server is temporarily overloaded or undergoing maintenance and cannot process the request.
504	Server Time-out: The gateway server did not receive a timely response from an external server.
505	Version Not Supported: The SIP protocol version used in the request is not supported by the server.
513	Message Too Large: The SIP message size exceeds UDP transport limits and must be transmitted over TCP.
6xx Global Failure Responses	
600	Busy Everywhere: The destination user is busy across all registered devices and cannot accept the call.
603	Decline: The destination explicitly declined the incoming call attempt.
604	Does Not Exist Anywhere: The requested destination address does not exist on any reachable server network.
606	Not Acceptable: The requested session parameters are unacceptable across all available endpoints.

General Call Prompt Tones

Administrators can customize the voice prompt audio played to users when internal or external calls fail due to specific conditions.

To configure custom failure prompts, upload audio files under **PBX Settings -> Voice Prompt -> Custom Prompts**, then select the desired audio file for each scenario under **PBX Settings -> Call Prompt Tones -> General Call Prompt Tones**.



General Call Prompt Tones

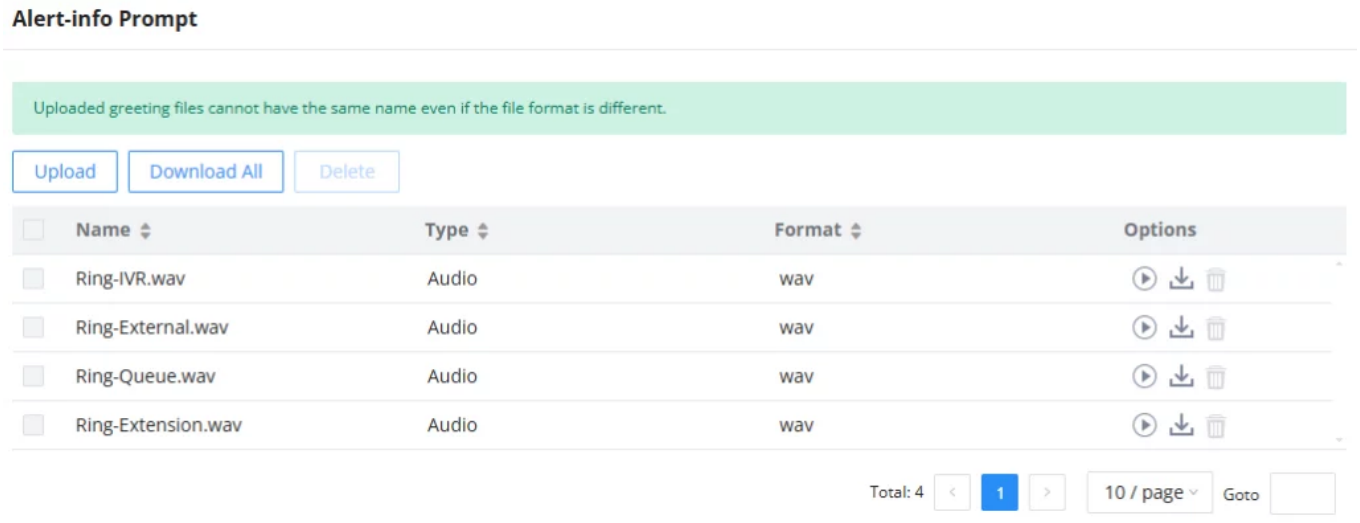
The table below describes the call failure scenarios and their default prompt tone selections:

Option	Description
Bad Number	Selects the prompt tone played when a caller dials an invalid extension or destination number.

Out Of Service	Selects the prompt tone played when the requested extension or service is unavailable or out of service.
User Busy	Selects the prompt tone played when the called user or extension is currently busy.
Trunk Busy	Selects the prompt tone played when all available outbound trunk lines are occupied.
No Answer	Selects the prompt tone played when the target destination fails to answer before the call timeout expires.
No Permission	Selects the prompt tone played when a caller lacks the required privilege level or routing permissions to dial the requested destination.
Do Not Disturb	Selects the prompt tone played when dialing an extension that has Do Not Disturb (DND) enabled.
Blocklist Outgoing Failure	Selects the prompt played when an outgoing call attempt is rejected because the destination number matches an active blocklist rule.
General Failed	Selects the prompt tone played for unspecified or unexpected call failures.
Call Waiting	Selects the audio tone played to a calling party when the recipient is on an active call with call waiting enabled.

Alert-info Prompt

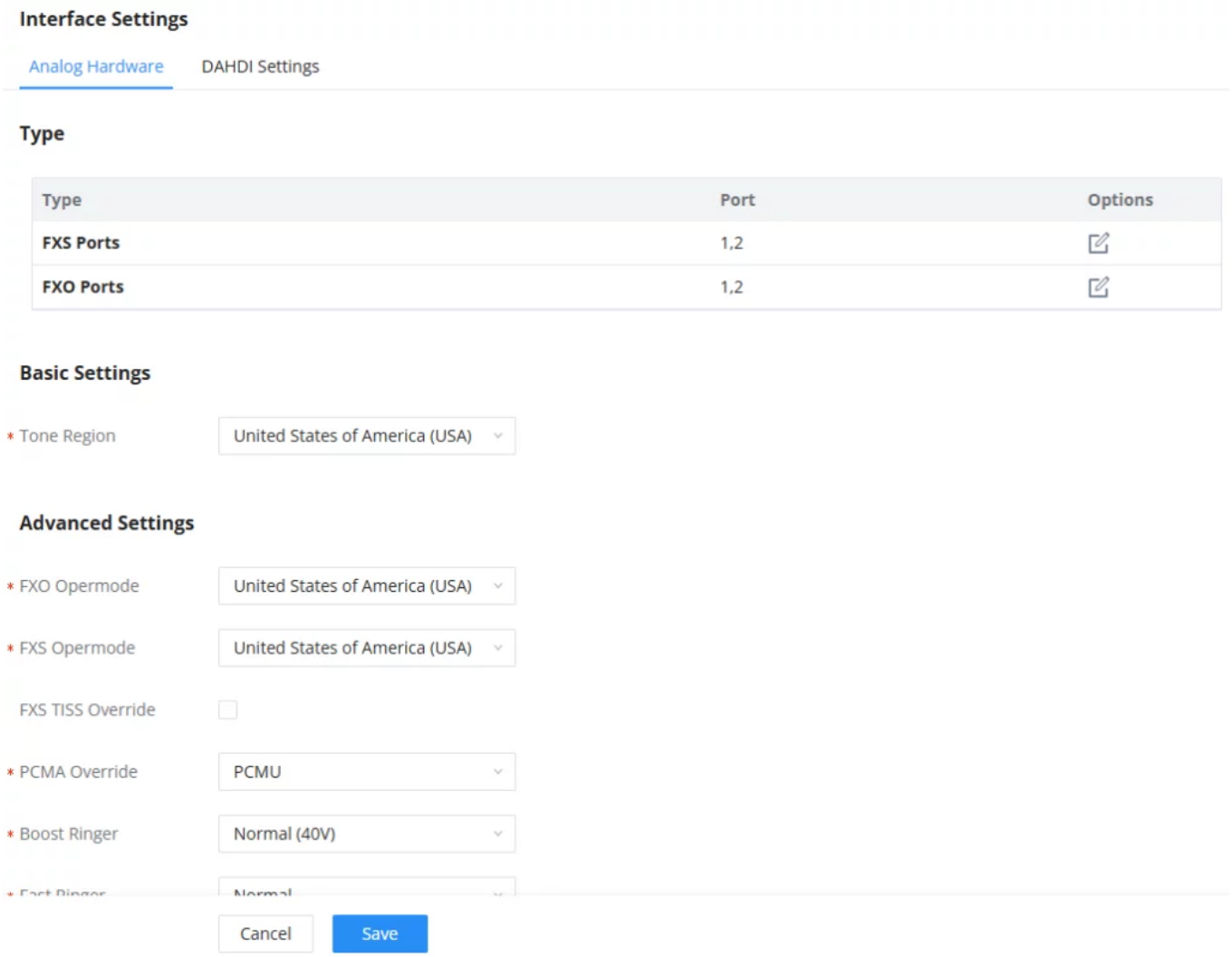
The user can change upload the ringtone files which can be used with Alert-info to play various ringtones depending on the configured behaviour. In this setting, the user can view all the ringtones uploaded, play them, download them, or delete them. If the user wishes to upload new ringtones, he/she can click on "Upload" and choose the ringtone files to upload.



Alert-info Prompt Ringtones

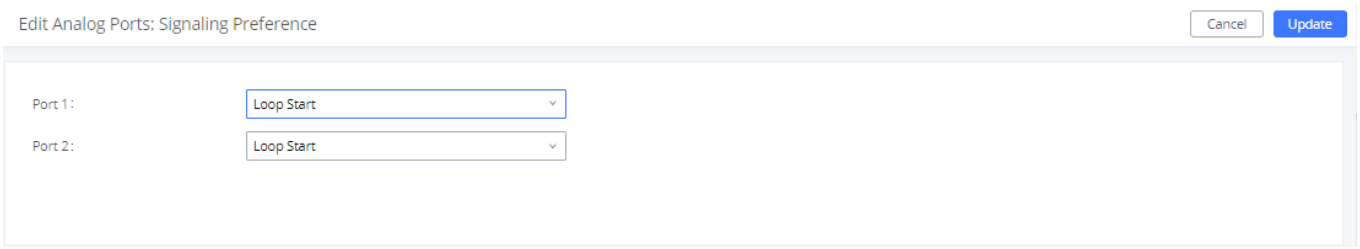
Interface Settings

Analog Hardware



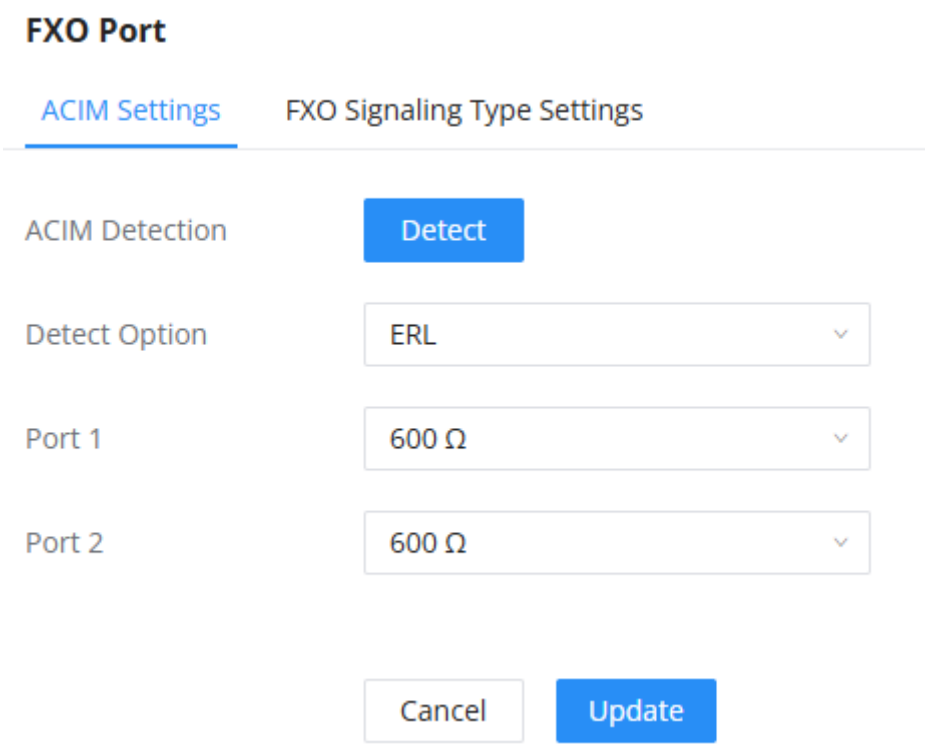
The analog hardware (FXS port and FXO port) on the UCM630X will be listed in this page. Click on to edit signaling preference for FXS port or configure ACIM settings for FXO port.

Select "Loop Start" or "Kewl Start" for each FXS port. And then click on "Update" to save the change.



FXS Ports Signaling Preference

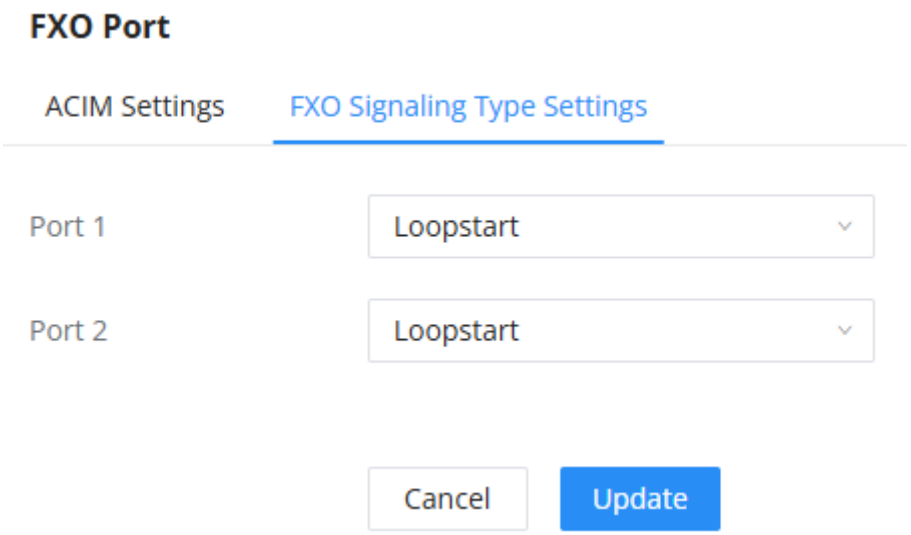
For FXO port, users could manually enter the ACIM settings by selecting the value from dropdown list for each port. Or users could click on "Detect" and choose the detection algorithm, two algorithms exist (ERL, Pr) for the UCM630X to automatically detect the ACIM value. The detecting value will be automatically filled into the settings.



FXO Ports ACIM Settings

Tone Region	Select country to set the default tones for dial tone, busy tone, ring tone and etc. to be sent from the FXS port. The default setting is "United States of America (USA)".
Advanced Settings	
FXO Opermode	Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)".
FXS Opermode	Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)".
FXS TISS Override	Configure to enable or disable override Two-Wire Impedance Synthesis (TISS). The default setting is No.If enabled, users can select the impedance value for Two-Wire Impedance Synthesis (TISS) override. The default setting is 600?.
PCMA Override	Select the codec to be used for analog lines. North American users should choose PCMU. All other countries, unless already known, should be assumed to be PCMA. The default setting is PCMU.Note: This option requires system reboot to take effect.
Boost Ringer	Configure whether normal ringing voltage (40V) or maximum ringing voltage (89V) for analog phones attached to the FXS port is required. The default setting is "Normal".
Fast Ringer	Configure to increase the ringing speed to 25HZ. This option can be used with "Low Power" option. The default setting is "Normal".
Low Power	Configure the peak voltage up to 50V during "Fast Ringer" operation. This option is used with "Fast Ringer". The default setting is "Normal".
Ring Detect	If set to "Full Wave", false ring detection will be prevented for lines where Caller ID is sent before the first ring and proceeded by a polarity reversal, as in UK. The default setting is "Standard".

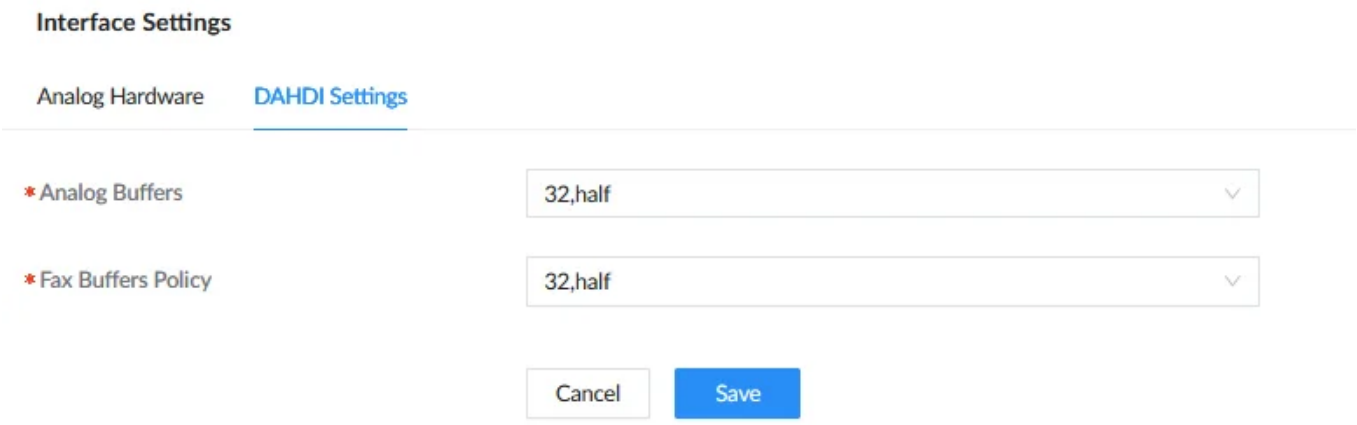
FXS MWI Mode	Configure the type of Message Waiting Indicator on FXS lines. The default setting is "FSK". FSK: Frequency Shift Key Indicator NEON: Light Neon Bulb Indicator.
FXO Frequency Tolerance	Allows users to adjust the tolerance of the FXO ringing frequency. 63Hz is considered the standard value and is selected by default.



FXO Signaling Type Settings

DAHDI Settings

DAHDI (Digium Asterisk Hardware Device Interface) settings manage TDM audio buffer allocations for physical FXO/FXS analog interfaces. Administrators can adjust these buffer policies when troubleshooting analog trunk issues such as audio latency, echoes, jitter, or fax transmission errors.



DAHDI Settings

DAHDI settings should generally be kept at their default values (32,half) and only adjusted when troubleshooting specific analog line or fax transmission issues.

Buffer options are formatted as [Buffer Count],[Read/Write Strategy] (e.g., 32,half):

- **Buffer Count** (e.g., 32)**:** Specifies the number of read/write buffers allocated for TDM audio processing.
- **Buffer Strategy:**

  - **Immediate:** Reads/writes audio packets as soon as any data enters the buffer (lowest latency, higher

risk of jitter/underrun).

- **Half:** Reads/writes audio packets when the buffer reaches half capacity (balanced latency and stability).
- **Full:** Reads/writes audio packets only when the buffer is completely filled (highest stability, higher latency).

The following table describes the configurable options on the DAHDI Settings page.

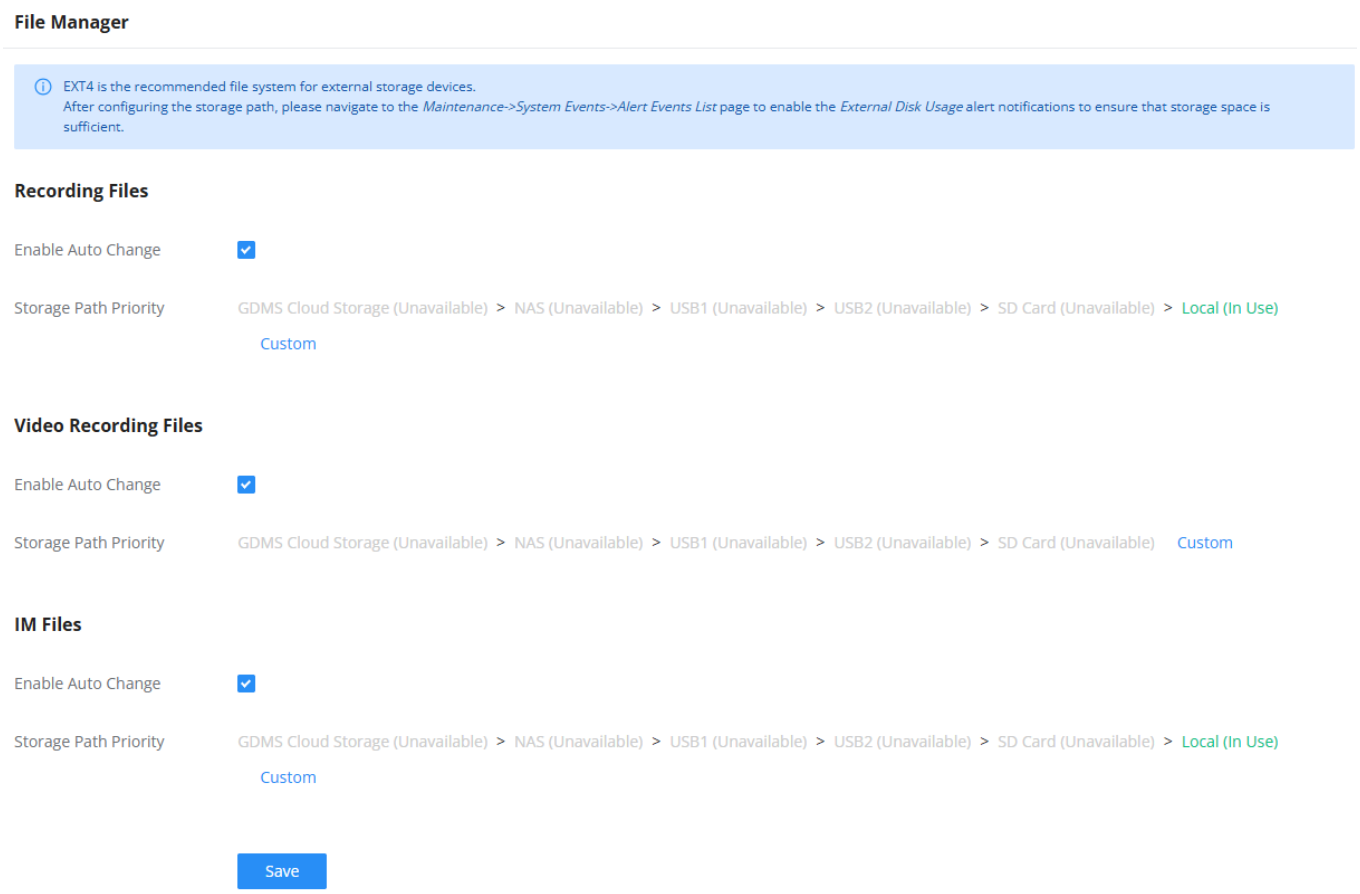
Option	Description
Analog Buffers	Configures the buffer size and read/write policy for general voice calls on analog FXO trunks and FXS ports. Default setting is 32,half.
Fax Buffers Policy	Configures the buffer size and read/write policy specifically for analog T.30 fax transmissions. Default setting is 32,half.

File Manager

The File Manager section defines the storage location and automatic storage switching behavior for files generated by the UCM630x system. Storage is configured separately for each file category. This section determines where new files are written and how the system behaves when multiple storage targets are available.

The following file types are supported:

- **Recording Files**
- **Video Recording Files**
- **IM Files**

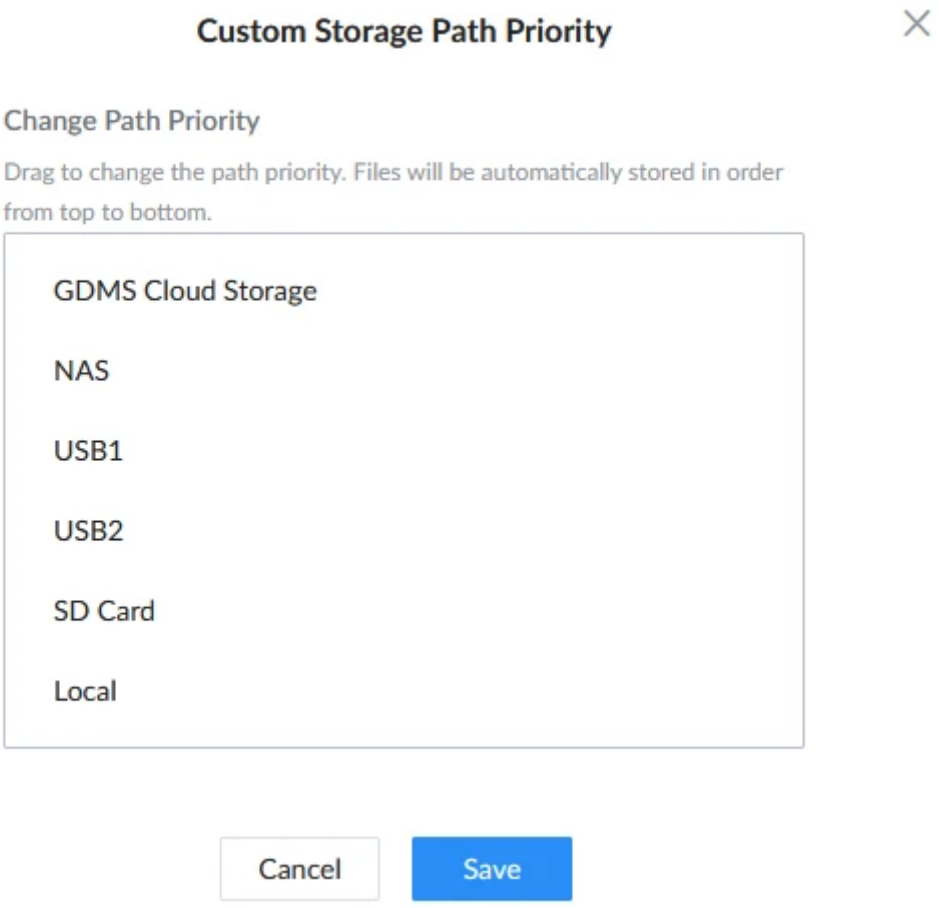


File Manager

Each file category allows the administrator to define the storage path used for newly generated files. Available options depend on system configuration and detected storage devices (e.g., Local storage, GDMS Cloud Storage, USB, NAS).

When Enable Auto Change is enabled, the system stores files according to the defined **Storage Path Priority**. If the active storage device becomes unavailable or reaches capacity, the system automatically switches to the next available device in the priority list.

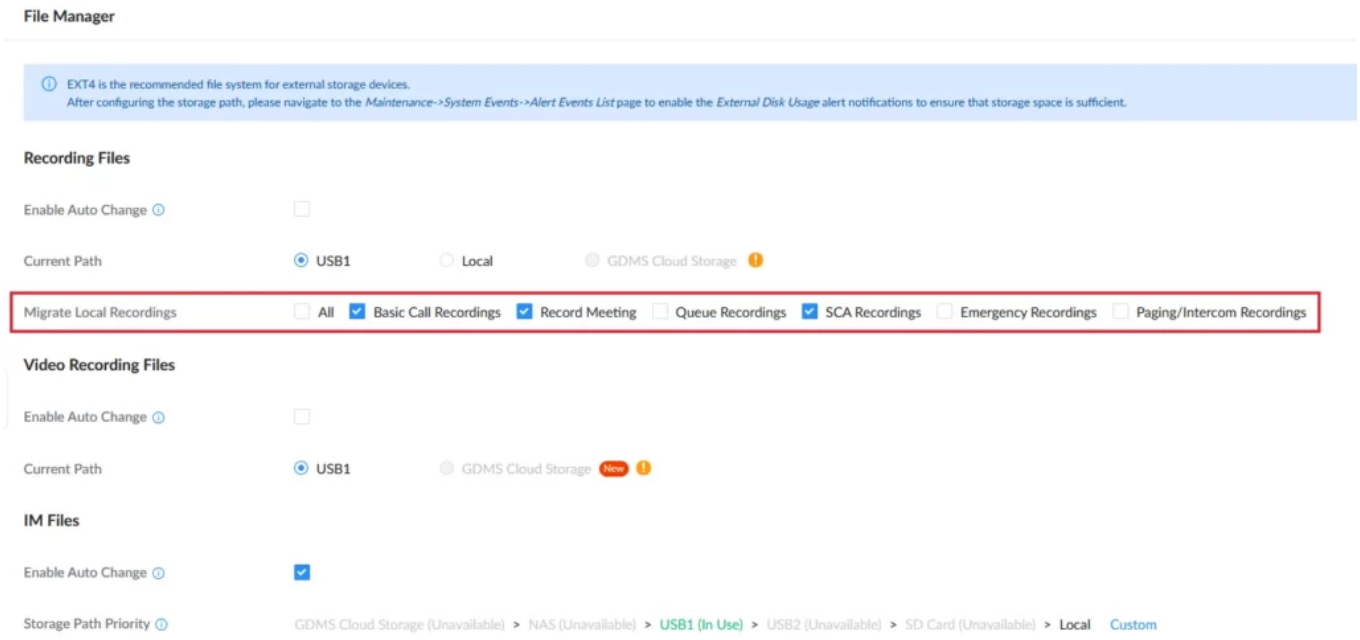
- After configuring storage paths, administrators should configure external disk usage alerts under **Maintenance->System Events->Alert Events List** to ensure sufficient storage capacity.
- Video Recording Files support external storage only and do not provide a Local storage option.



Custom Storage Path Priority

When the storage path for Recording Files is changed from **Local** to an external storage device (such as USB or NAS, if available), the Migrate Local Recordings option becomes available. This option allows existing recordings stored in internal memory to be copied to the newly selected external storage device. The administrator can select specific recording categories to migrate as shown below.

- This option does not appear when switching from Local to GDMS Cloud Storage.
- The function copies existing recordings to the selected storage device and does not delete the original files from local storage.

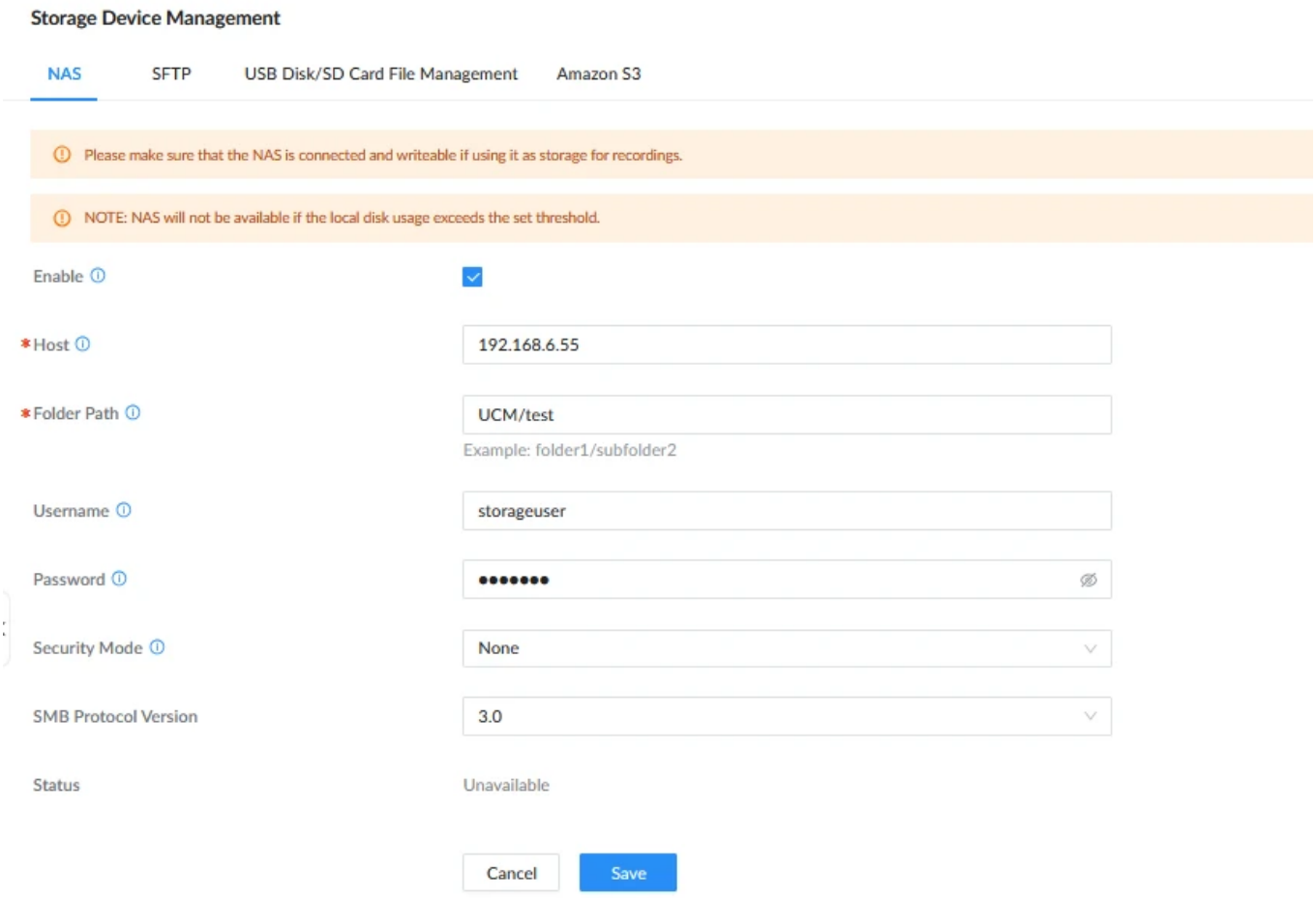


Migrate Local Recordings Option

Storage Device Management

NAS

The UCM supports adding and backing up recordings to a network-attached storage (NAS) server.



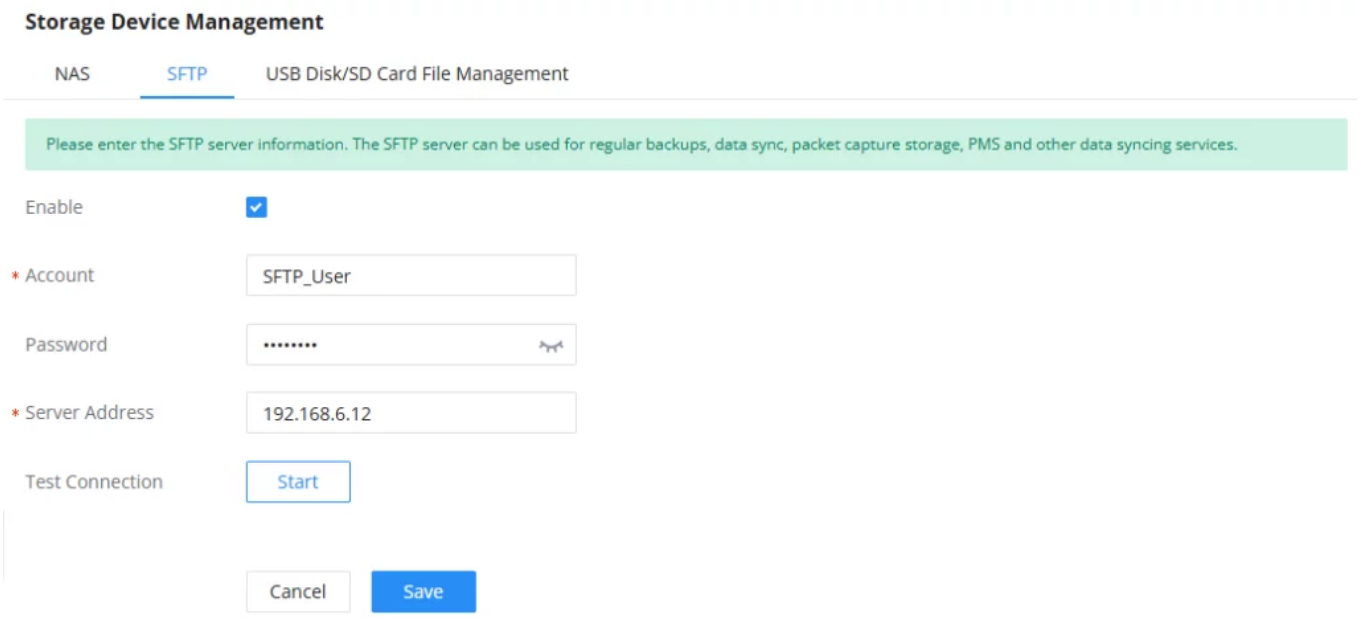
The following table describes the configurable NAS settings:

Option	Description
Enable	Check the box to enable Network Attached Storage (NAS) support on the UCM.
Host	Enter the IP address or hostname of the NAS server (e.g., 192.168.6.55).
Folder Path	Configure the directory path on the NAS storage where files will be saved (e.g., folder1/subfolder2).
Username	Enter the username required for authenticating with the NAS storage server.
Password	Enter the password required for authenticating with the NAS storage server.
Security Mode	Select the security authentication mode required by the NAS server (e.g., None, NTLM, NTLMv2).
SMB Protocol Version	Select the Server Message Block (SMB) protocol version used to communicate with the network storage server. Supported Options: 1.0: SMB version 2.0 protocol. 2.0: SMB version 3.0 protocol. 3.0: SMB version 3.0.2 protocol.
Status	Displays the real-time connection status between the UCM and the NAS server (e.g., Available, Unavailable).

If Network Storage Device has 1 GB of storage space left, it will be considered unavailable and the UCM will trigger the external disk usage alert.

SFTP

SFTP integration offers synchronizing files between from the UCM to the SFTP server. SFTP is used to synchronize the following data: CDR Records, Recording Files, Voicemail, and Fax.

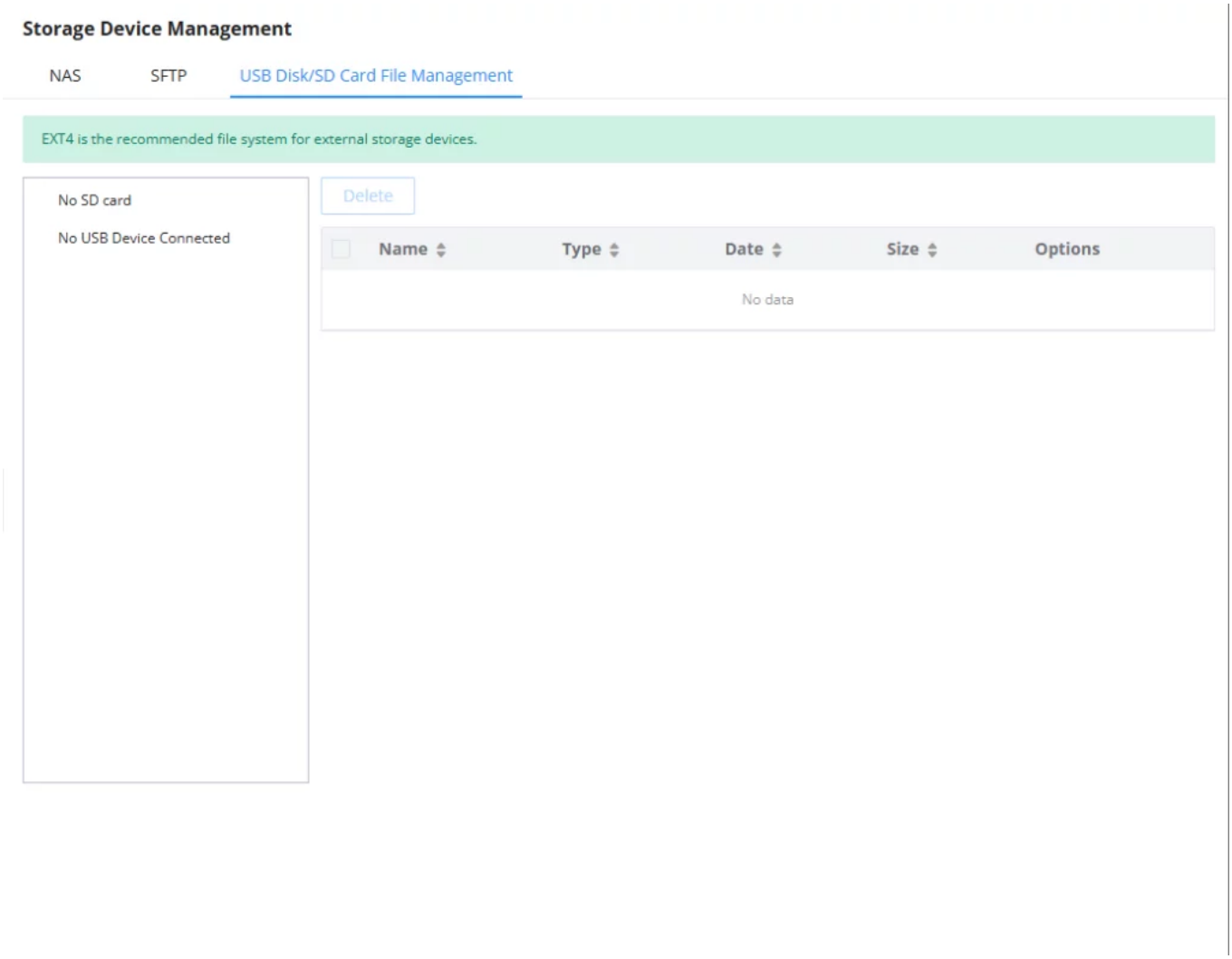


SFTP Integration

Enable	Tick this box to enable SFTP integration.
Account	Enter the account of the SFTP server.
Password	Enter the password of the account of the SFTP server.
Server Address	Enter the address of the SFTP server.

USB Disk/SD Card File Management

USB Disk/SD Card File Management is a feature which allows to manages the files stored on the USB flash drive attached to the UCM device, or an SD card attached to the system.



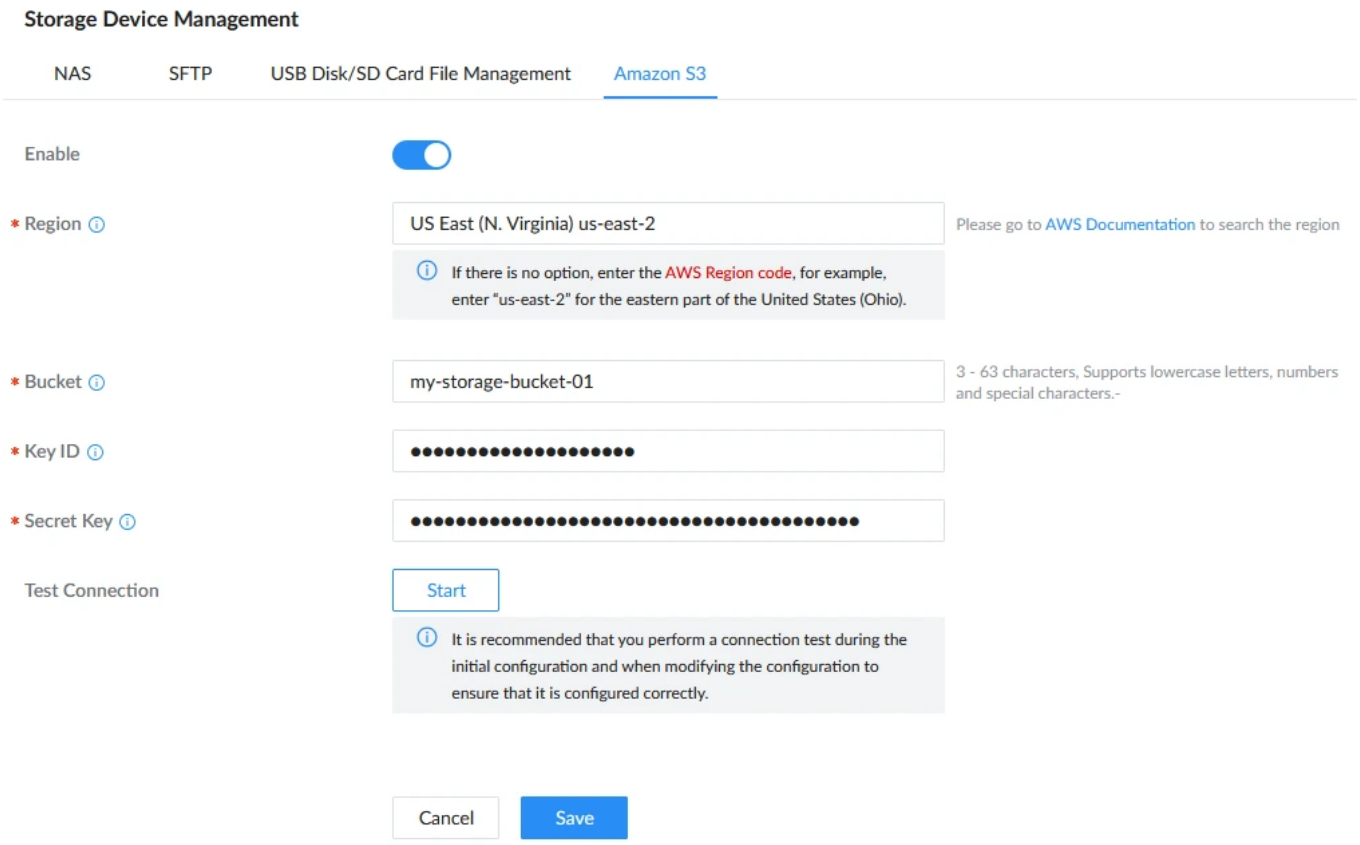
USB Disk/SD Card File Management

Amazon S3

The Storage Device Management module allows you to integrate your UCM63xx with external cloud storage services. This page provides the option to configure a connection to a third-party Amazon S3 bucket to archive a copy of your critical data, specifically backup files.

This feature is designed for organizations that require an additional, independent copy of their configuration and data for long-term retention, compliance, or disaster recovery purposes, separate from the primary Grandstream cloud storage.

This integration is used for storing backup files to your own S3 bucket. All other system data, such as call recordings and voicemails, will continue to be stored in your primary storage space.



Amazon S3 Storage Settings

The table below describes the parameters that can be found on the Amazon S3 configuration tab:

Enable	Enables or disables Amazon S3 integration. When enabled, the configuration fields below become editable.
Region	Manually enter, or select from the drop-down list the AWS region where the bucket is located.
Bucket	Enter the name of the S3 bucket. Must be 3-63 characters, lowercase letters, numbers, and hyphens only.
Key ID	Enter the AWS Access Key ID generated after creating an account on the AWS platform.This value is encrypted and cannot be viewed after saving.
Secret Key	Enter the AWS Secret Access Key generated after creating an account. This value is encrypted and cannot be viewed after saving.
Test Connection	Click on this button to Test the connection to AWS S3 with the current settings. Note: It is recommended to perform a connection test during the initial configuration to ensure your UCM can successfully communicate with the Amazon S3 bucket.

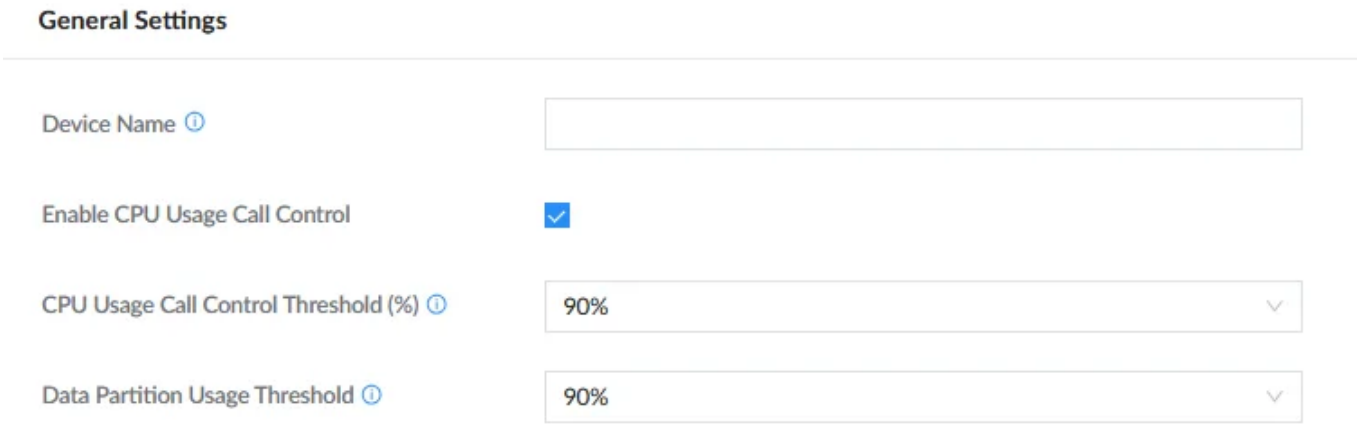
SYSTEM SETTINGS

This section will explain the available system-wide parameters and configuration options on the UCM630X series. This includes settings for the following items: General Settings, Cloud IM, HTTP server, network Settings, OpenVPN, DDNS Settings, Security Settings, LDAP server, Time settings, Email settings, and TR-069.

General Settings

System administrators can prevent the UCM from making calls and/or writing to the data partition (e.g., CDR,

recordings, etc.) once the system reaches a specified threshold of storage usage and CPU usage respectively. These options are located in the System Settings → General Settings page.



General Settings Interface

Device Name	Configure the name of the UCM.
Enable CPU Usage Call Control	Enables the CPU flow control.
CPU Usage Call Control Threshold (%)	Used to set the threshold generated by the CPU Flow Control. When the system CPU reaches the threshold, it will prohibit the new calls. The default value is 90%.
Data Partition Usage Threshold	Used to set a threshold to stop writing data partition. When the disk data partition reaches the threshold configured, the data partition writing will be stopped. The default value is 90%.

HTTP Server

The UCM630X's embedded web server responds to HTTPS GET/POST requests and allows users to configure the UCM via web browsers such as Microsoft IE, Mozilla Firefox, and Google Chrome.

By default, users can access the UCM by just typing its IP address into a browser address bar. The browser will automatically be redirected to HTTPS using port 8089. For example, typing in "192.168.40.50" into the address bar will redirect the browser to "https://192.168.40.50:8089". This behavior can be changed in the **System Settings -> HTTP Server page**.

Redirect from Port 80	Toggles automatic redirection to UCM's web portal from port 80. If disabled, users will need to manually add the UCM's configured HTTPS port to the server address when accessing the UCM web portal via browser. Default is "Enabled".
External Host	Configure a URL and port (optional) used to access the UCM web portal if the UCM is behind NAT.
Port	Specifies the port number used to access the UCM HTTP server. Default is "8089".
IP Address Allowlist	IP Allowlist restricts all IP addresses except for those in the allowlist from accessing the device via HTTP(S) (i.e., web portal, ZeroConfig, CTI apps).
Permitted IP(s)	List of addresses that can access the UCM web portal.Ex: 192.168.6.233 / 255.255.255.255
Wave Settings	

Cross-Server Address Allowlist	The UCM will accept cross-server requests from addresses in the whitelist, which should be formatted as https://domain, https://ip:port or *. Entering * will allow cross-server requests from all addresses.Note: This option allow third parties to embed a Wave portal into their websites. This allows the users to log into wave using their extension numbers and use limited Wave features.For more details, please refer to the following link: https://doc.grandstream.dev/WAVE-SDK/EN/#api-Quick%20Start-Overview
External Host	Specifies the public domain name or IP address (and port, if required) used by Wave clients to access UCM services when the UCM is behind NAT or accessed from an external network. This address is synchronized to Wave and used for external service access, including high-availability and disaster recovery scenarios.Note: When a RemoteConnect plan is enabled, this field is automatically populated with the Wave external host address provided by GDMS. Please ensure that Automatically Update the External Host Address for Wave is disabled to prevent the external host from being reset by GDMS.
Port	The port to access Wave Web and Wave Mobile. If behind NAT, please make sure to map the external port to this port.
Certificate Settings	
Default Certificate Auto Renewal	If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected.
Options	Selects the method of acquiring SSL certificates for the UCM web server. Two methods are currently available:Upload Certificate: Upload the appropriate files from one's own PC.Request Certificate: Enter the domain for which to request a certificate for from "Let's Encrypt".
TLS Cert	Upload the certificate for the HTTP server used for TLS connections. It contains the client's private key and the server's signed certificate. Once uploaded, the file will automatically be saved as "certificate.pem".Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The file size must not exceed 2MB.
TLS Private Key	Upload the private key for the HTTP server. Once uploaded, the file will automatically be saved as "private.pem".Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The file size must not exceed 2MB.
Certificate & Private Key	Click the "Reset" button to reset the TLS Cert and Private Key

If the protocol or port has been changed, the user will be logged out and redirected to the new URL.

Network Settings

After successfully connecting the UCM630X to the network for the first time, users could log in to the Web GUI and go to **System Settings** -> **Network Settings** to configure the network parameters for the device.

- UCM630X supports Route/Switch/Dual mode functions.

In this section, all the available network setting options are listed for all models. Select each tab in Web GUI -> **System Settings** -> **Network Settings** page to configure LAN settings, WAN settings, 802.1X, and Port Forwarding.

Basic Settings

Please refer to the following tables for basic network configuration parameters on the UCM6300 Series.

Method	Select Route, Switch, or Dual mode for the UCM630X network interfaces. The default setting is Switch. Route: The WAN port serves as the uplink connection, while the LAN port operates as a router port. Switch: The WAN port serves as the uplink connection, while the LAN port operates as a bridged interface. Dual: Both WAN and LAN ports serve as independent uplink connections, labeled as LAN2 and LAN1 respectively. The port designated as the Default Interface requires a Gateway IP address if configured with a static IP.
MTU	Specifies the Maximum Transmission Unit (MTU) packet size. The default value is 1492.
Default Interface	Available when Network Method is set to Dual. Specifies which network interface serves as the primary default route.
IPv4 Address	
Preferred DNS Server	If configured, this address will be used as the system's Primary DNS server.
If "Method" is set to "Route"	
WAN	
IP Method	Select the network assignment method for the WAN interface: DHCP (Default), Static IP, or PPPoE.
IP Address	Enter the IPv4 address for static IP configuration. The default value is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP configuration. The default value is 255.255.0.0.
Gateway IP	Enter the default gateway IP address for static IP configuration. The default value is 0.0.0.0.
DNS Server 1	Enter the primary DNS server address for static IP configuration.
DNS Server 2	Enter the secondary DNS server address for static IP configuration.
Username	Enter the account username required to establish a PPPoE connection.
Password	Enter the password required to establish a PPPoE connection.
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the 802.1Q VLAN tag for Layer 2 QoS packets on the WAN port.
Layer 2 QoS 802.1p Priority Value	Assigns the 802.1p priority value for Layer 2 QoS packets on the WAN port.
Enable VoIP VLAN	Enables a dedicated VLAN for VoIP data traffic when operating in Route or Switch network mode.When enabled, additional VLAN parameters will display to configure dedicated VoIP traffic routing.Note: This option is not supported when operating in HA or Cluster mode.
IP Method	The IP address assignment mode for the VoIP VLAN interface.Static IP: Manually configures network address settings.
IP Address	Enter the IPv4 address for the VoIP VLAN interface (format: xxx.xxx.xxx.xxx).
Subnet Mask	Enter the subnet mask for the VoIP VLAN interface (e.g., 255.255.255.0).
Gateway IP	Enter the gateway IP address for the VoIP VLAN interface (format: xxx.xxx.xxx.xxx).
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the 802.1Q VLAN tag for Layer 2 QoS packets. Setting to 0 disables VLAN. If unsure, do not alter Layer 2 QoS VLAN tags and priority values, as incorrect settings may prevent the device from acquiring an IP address.
Layer 2 QoS 802.1p Priority Value	Assigns the 802.1p priority value for Layer 2 QoS packets.
LAN	
IP Address	Enter the IP address assigned to the LAN port. The default setting is 192.168.2.1.

Subnet Mask	Enter the subnet mask. The default setting is 255.255.255.0.
DHCP Server Enable	Enables or disables local DHCP server capabilities on the LAN port. The default setting is Yes.
DNS Server 1	Enter DNS server address 1. The default setting is 8.8.8.8.
DNS Server 2	Enter DNS server address 2. The default setting is 208.67.222.222.
Allow IP Address From	Specifies the starting IP address for the DHCP pool. The default setting is 192.168.2.100.
Allow IP Address To	Specifies the ending IP address for the DHCP pool. The default setting is 192.168.2.254.
Default IP Lease Time	Enter the IP address lease duration in seconds. The default setting is 43200.
If "Method" is set to "Switch"	
LAN	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP configuration. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP configuration. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP configuration. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP configuration.
DNS Server 2	Enter the DNS server 2 address for static IP configuration.
Username	Enter the username to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the Layer 2 QoS VLAN tag for the LAN port. The accepted range is 2 to 4094.
Layer 2 QoS 802.1p Priority Value	Assign the Layer 2 QoS priority value for the LAN port. The default value is 0.
Enable VoIP VLAN	Enables a dedicated VLAN for VoIP data traffic when using Router or Switch mode.If enabled, additional VLAN parameters will be displayed to isolate VoIP data.Note: This option is not supported in High Availability (HA) or Cluster mode.
IP Method	The IP address assignment mode for the VoIP VLAN interface.Static IP: Manually configures network address settings.
IP Address	The IPv4 address of the device (format: xxx.xxx.xxx.xxx).
Subnet Mask	Enter the subnet mask address (e.g., 255.255.255.0).
Gateway IP	Enter the gateway IP address (format: xxx.xxx.xxx.xxx).
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the 802.1Q VLAN tag for Layer 2 QoS packets. Setting to 0 disables VLAN. If unsure, do not alter Layer 2 QoS VLAN tags and priority values, as incorrect settings may cause the device to lose IP connectivity. Valid range: 2 to 4094.
Layer 2 QoS 802.1p Priority Value	Assigns the 802.1p priority value for Layer 2 QoS packets.
If "Method" is set to "Dual"	
LAN 1	
IP Method	Select the network assignment method for LAN 1: DHCP (Default), Static IP, or PPPoE.
IP Address	Enter the IP address for static IP configuration. The default setting is 192.168.0.160.

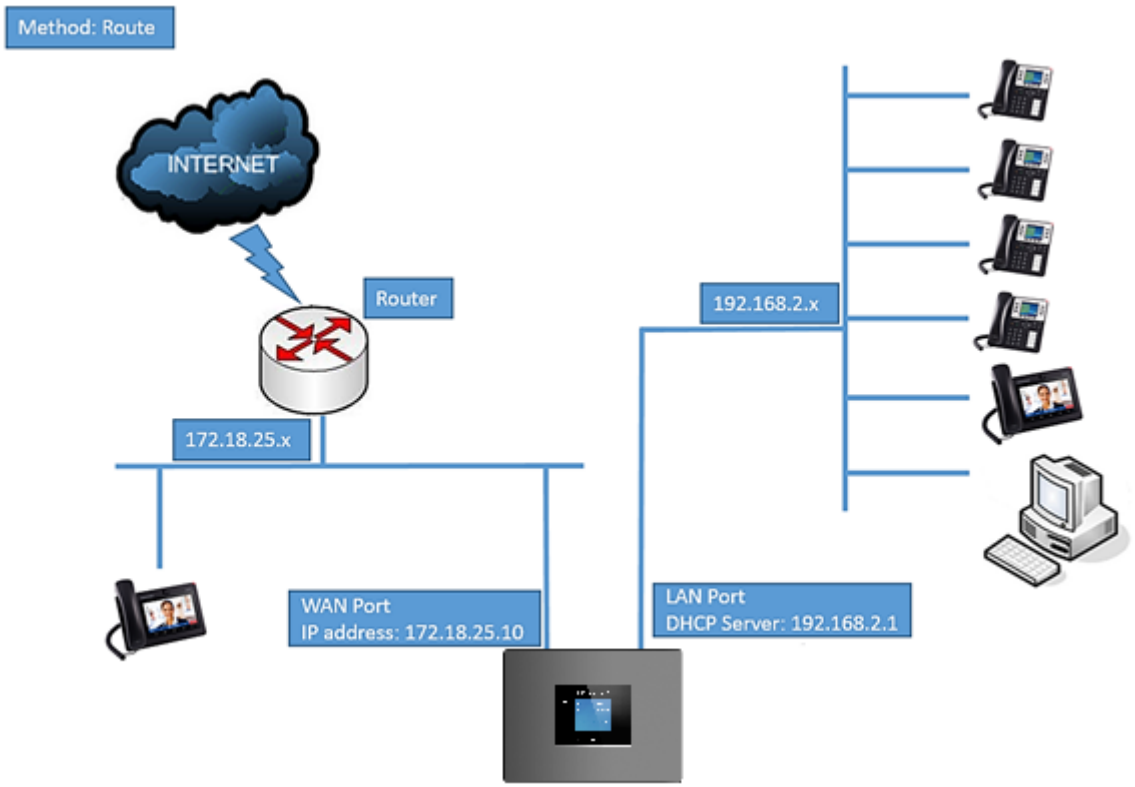
Subnet Mask	Enter the subnet mask address for static IP configuration. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static configuration when this port is selected as default interface. The default value is 0.0.0.0.
DNS Server 1	Enter the primary DNS server address for static configuration.
DNS Server 2	Enter the secondary DNS server address for static configuration.
Username	Enter the account username required for PPPoE connection.
Password	Enter the password required for PPPoE connection.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the Layer 2 QoS VLAN tag for the LAN port. Accepted range: 2 to 4094.
Layer 2 QoS 802.1p Priority Value	Assign the Layer 2 QoS priority value for the LAN port. Default value is 0.
LAN 2	
IP Method	Select the network assignment method for LAN 2: DHCP (Default), Static IP, or PPPoE.
IP Address	The static IPv4 address of the device (format: xxx.xxx.xxx.xxx).
Subnet Mask	Enter the subnet mask (e.g., 255.255.255.0).
Gateway IP	Enter the gateway IP address (format: xxx.xxx.xxx.xxx).
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the Layer 2 QoS VLAN tag. Setting to 0 disables VLAN. If unsure, do not alter Layer 2 QoS VLAN tags and priority values, as incorrect settings may cause the device to lose IP connectivity. Valid range: 2 to 4094.
Layer 2 QoS 802.1p Priority Value	Assigns the Layer 2 QoS priority value.
IPv6 Address	
If "Method" is set to "Route"	
WAN	
IP Method	Select Auto or Static. The default setting is Auto.
IP Address	Enter the IPv6 address for static IP configuration.
IP Prefixlen	Enter the IPv6 prefix length for static configuration. Default is 64.
DNS Server 1	Enter the primary IPv6 DNS server address for static configuration.
DNS Server 2	Enter the secondary IPv6 DNS server address for static configuration.
Enable VLAN	Enable VLAN tagging for this interface.
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the Layer 2 QoS VLAN tag. If unsure, do not change Layer 2 QoS VLAN tags and priority values, as incorrect configuration may cause the device to fail to obtain an IP address.Range: 2 - 4094
Layer 2 QoS 802.1p Priority Value	Assigns the priority value for Layer 2 QoS packets.Range: 0 - 7, where 7 indicates higher priority and 0 indicates lower priority.
Enable VoIP VLAN	This configuration is not supported in HA or Cluster mode.If enabled, additional VLAN settings will be displayed to isolate VoIP data.
IP Method	The IP address assignment mode for the device. Static IP: Manual configuration of address information.
IP Address	The IPv4 address of the device (format: xxx.xxx.xxx.xxx).
Subnet Mask	Enter the subnet mask address (e.g., 255.255.255.0).
Gateway IP	Enter the gateway IP address (format: xxx.xxx.xxx.xxx).
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the Layer 2 QoS VLAN tag. If unsure, do not alter Layer 2 QoS VLAN tags and priority values, as incorrect settings may cause the device to lose IP connectivity.Range: 0 - 4094

Layer 2 QoS 802.1p Priority Value	Assigns the priority value for Layer 2 QoS packets.Range: 0 - 7, where 7 indicates higher priority and 0 indicates lower priority.
LAN	
DHCP Server	Select Disable, Auto, or DHCPv6. Disable: The DHCPv6 server is disabled. Auto: Stateless address autoconfiguration using the NDP protocol. DHCPv6: Stateful address autoconfiguration using the DHCPv6 protocol. The default setting is Disabled.
DHCP Prefix	Enter the IPv6 DHCP prefix. Default is 2001:db8:2:2::
DHCP Prefixlen	Enter the prefix length for static settings. Default is 64.
DNS Server 1	Enter the primary DNS server address for static settings. Default is 2001:4860:4860::8888
DNS Server 2	Enter the secondary DNS server address for static settings. Default is 2001:4860:4860::8844
Allow IP Address From	Configures the starting IP address determined by the DHCP prefix and prefix length.
Allow IP Address To	Configures the ending IP address determined by the DHCP prefix and prefix length.
Default IP Lease Time (s)	Configures the lease duration (in seconds) for assigned IP addresses.
If "Method" is set to "Switch"	
LAN	
IP Method	Select Auto or Static. The default setting is Auto.
IP Address	Enter the IPv6 address for static IP settings.
IP Prefixlen	Enter the prefix length for static settings. Default is 64.
Gateway	Enter the default gateway IPv6 address.
DNS Server 1	Enter the primary DNS server address for static settings.
DNS Server 2	Enter the secondary DNS server address for static settings.
If "Method" is set to "Dual"	
LAN 1	
IP Method	Select Auto or Static. The default setting is Auto.
IP Address	Enter the IPv6 address for static IP settings.
IP Prefixlen	Enter the prefix length for static settings. Default is 64.
Gateway	Enter the default gateway IPv6 address.
DNS Server 1	Enter the primary DNS server address for static settings.
DNS Server 2	Enter the secondary DNS server address for static settings.
LAN 2	
IP Method	Select Auto or Static. The default setting is Auto.
IP Address	Enter the IPv6 address for static IP settings.
IP Prefixlen	Enter the prefix length for static settings. Default is 64.
DNS Server 1	Enter the primary DNS server address for static settings.
DNS Server 2	Enter the secondary DNS server address for static settings.
Network Port Traffic Control	
Enable Network Port Traffic Storm Alert	The UCM will send an alert notification or email when excessive packet volume on the LAN impacts overall network performance.Note: To enable this feature, email or HTTP notifications must be configured correctly under Maintenance -> System Events.

Ignore User Operation Traffic	When enabled, traffic storm alarms triggered by administrative actions after login (such as firmware upgrades, uploading backups, beeping, zero-config provisioning, recording files, and downloading network disk files) are suppressed.
If "Method" is set to "Switch"	
LAN	
Network Port Incoming Traffic Control	Monitors incoming (RX) traffic on the network port and triggers an alarm when the enabled alert threshold is exceeded.The threshold range is 1 to 1024000 kbps or 1 to 1000 mbps.
If "Method" is set to "Dual"	
LAN 1	
Network Port Incoming Traffic Control	Monitors incoming (RX) traffic on the network port and triggers an alarm when the enabled alert threshold is exceeded.The threshold range is 1 to 1024000 kbps or 1 to 1000 mbps.
LAN 2	
Network Port Incoming Traffic Control	Monitors incoming (RX) traffic on the network port and triggers an alarm when the enabled alert threshold is exceeded.The threshold range is 1 to 1024000 kbps or 1 to 1000 mbps.
If "Method" is set to "Route"	
WAN	
Network Port Incoming Traffic Control	Monitors incoming (RX) traffic on the network port and triggers an alarm when the enabled alert threshold is exceeded.The threshold range is 1 to 1024000 kbps or 1 to 1000 mbps.
LAN	
Network Port Incoming Traffic Control	Monitors incoming (RX) traffic on the network port and triggers an alarm when the enabled alert threshold is exceeded.The threshold range is 1 to 1024000 kbps or 1 to 1000 mbps.

- **Method: Route**

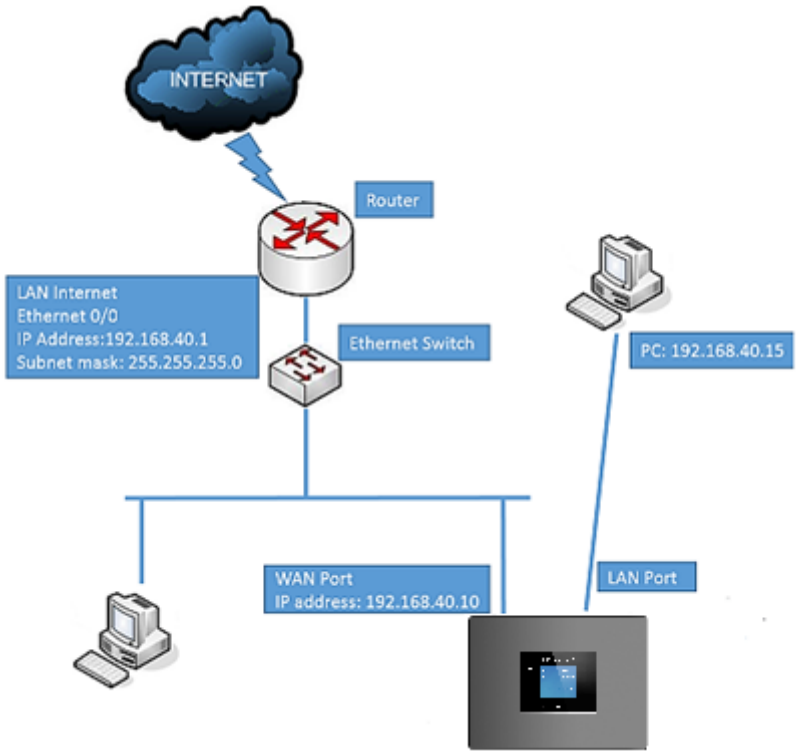
When the UCM630X has the method set to Route in network settings, WAN port interface is used for uplink connection and LAN port interface is used as a router. Please see a sample diagram below.



UCM6302 Network Interface Method: Route

- **Method: Switch**

WAN port interface is used for uplink connection; LAN port interface is used as a room for PC connection.

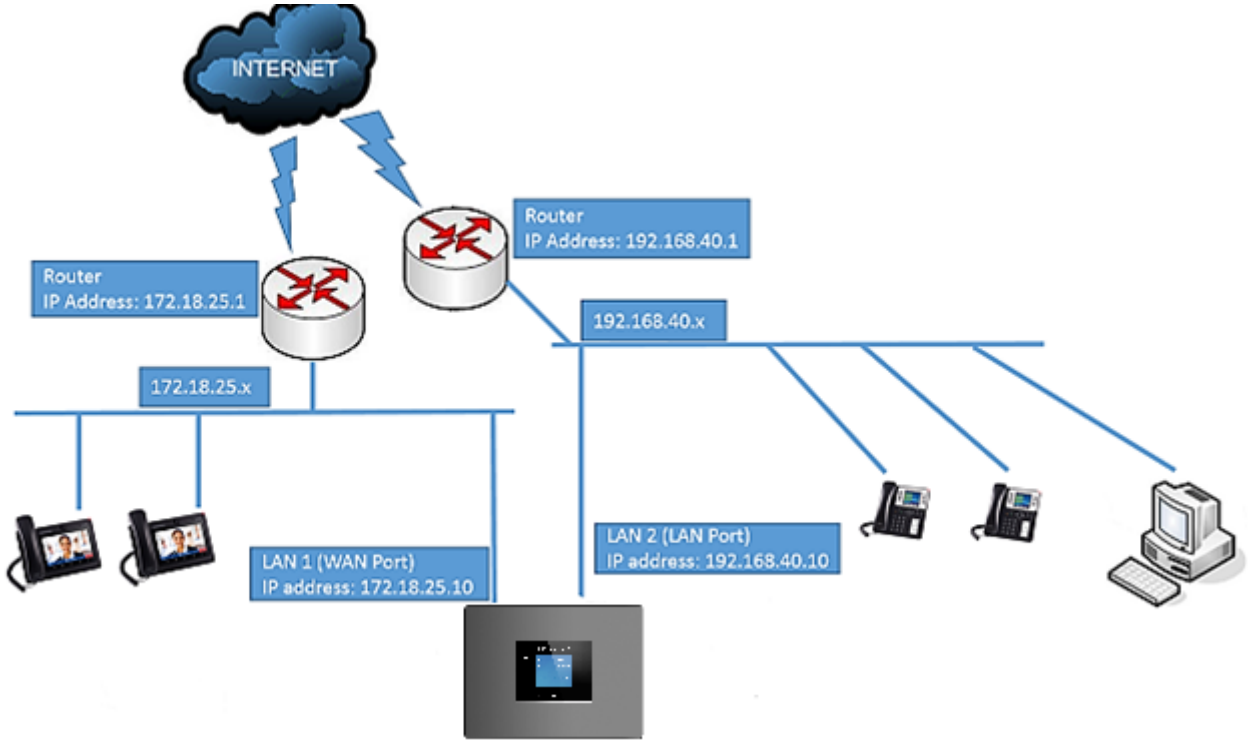


UCM6302 Network Interface Method: Switch

- **Method: Dual**

Both WAN port and LAN port are used for the uplink connection. Users will need to assign LAN 1 or LAN 2

as the default interface in option "Default Interface" and configure "Gateway IP" if static IP is used for this interface.

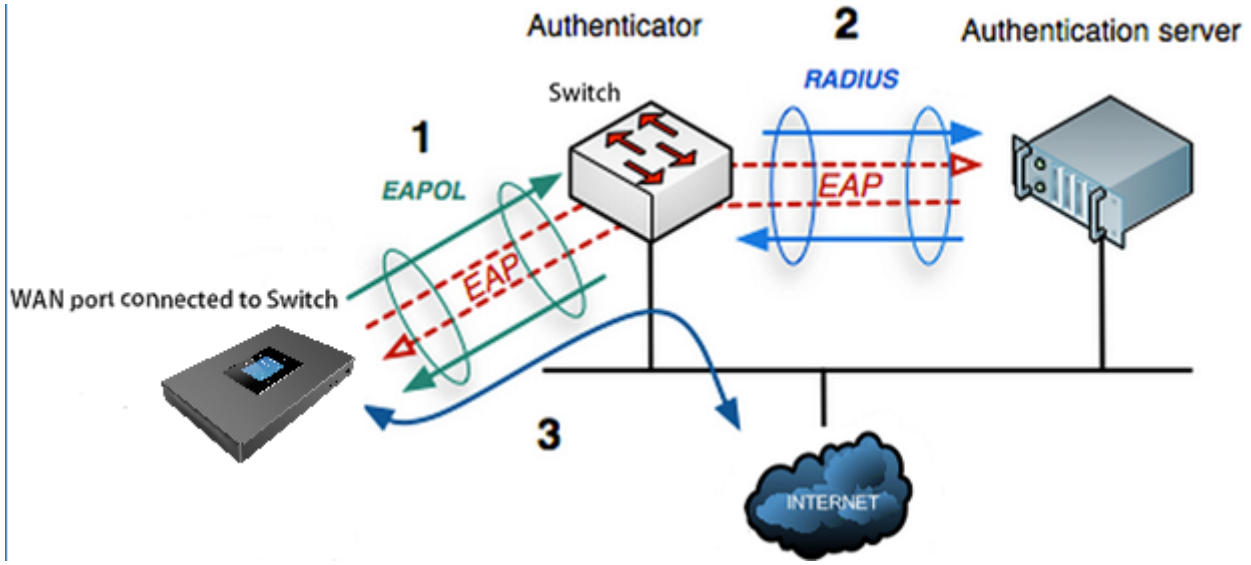


UCM6302 Network Interface Method: Dual

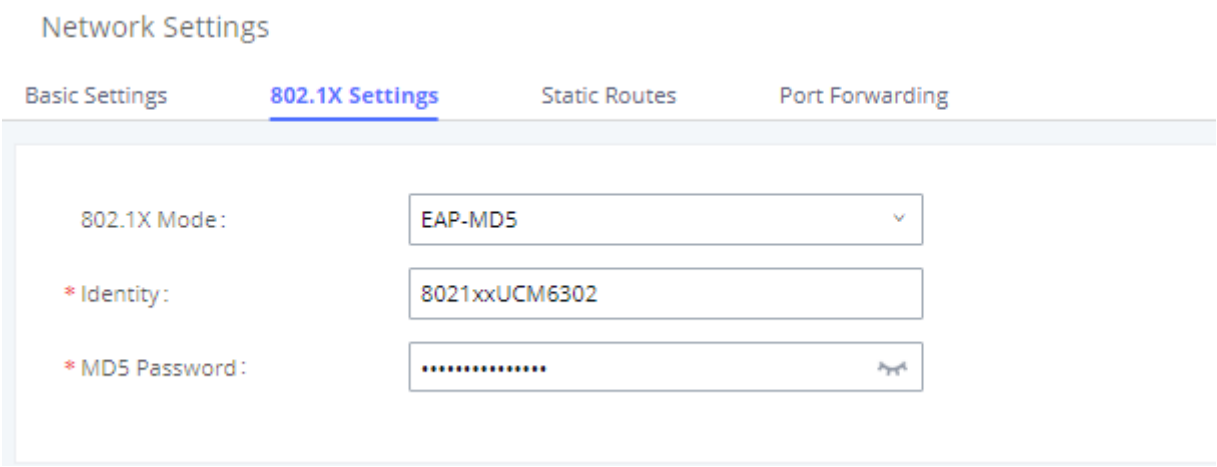
802.1X Settings

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to a device before the device can access the Internet or other LAN resources. The UCM630X supports 802.1X as a supplicant/client to be authenticated.

The following diagram and figure show UCM630X uses 802.1X mode "EAP-MD5" on the WAN port as a client in the network to access the Internet.



UCM630X Using 802.1X as Client



UCM630X Using 802.1X EAP-MD5

The following tables shows the configuration parameters for the different 802.1X modes.

- **MD5**

Parameter	Description
802.1X Mode	EAP-MD5
Identity	Enter the Identity for the 802.1X mode.
MD5 Password	Enter the MD5 Password for the 802.1X mode.

- **EAP TLS**

Parameter	Description
802.1X Mode	EAP-MD5
Identity	Enter the Identity for the 802.1X mode.
802.1X Client Private Key Password	The private key password corresponding to the 802.1X client certificate.
802.1X CA Certificate	Upload 802.1X CA certificate. This file will be renamed as "8021x_ca_cert" automatically.
802.1X Client Certificate	Upload 802.1X client certificate. This file will be renamed as 8021x_client_cert automatically.
802.1X Client Private Key	Upload the private key corresponding to the 802.1X client certificate. This file will be renamed as 8021x_client_key automatically.

- EAP PEAPv0/MSCHAPv2

Parameter	Description
802.1X Mode	EAP-MD5
Identity	Enter the Identity for the 802.1X mode.
MD5 Password	Enter the MD5 Password for the 802.1X mode.
802.1X CA Certificate	Upload 802.1X CA certificate. This file will be renamed as "8021x_ca_cert" automatically.
802.1X Client Certificate	Upload 802.1X client certificate. This file will be renamed as 8021x_client_cert automatically.

Static Routes

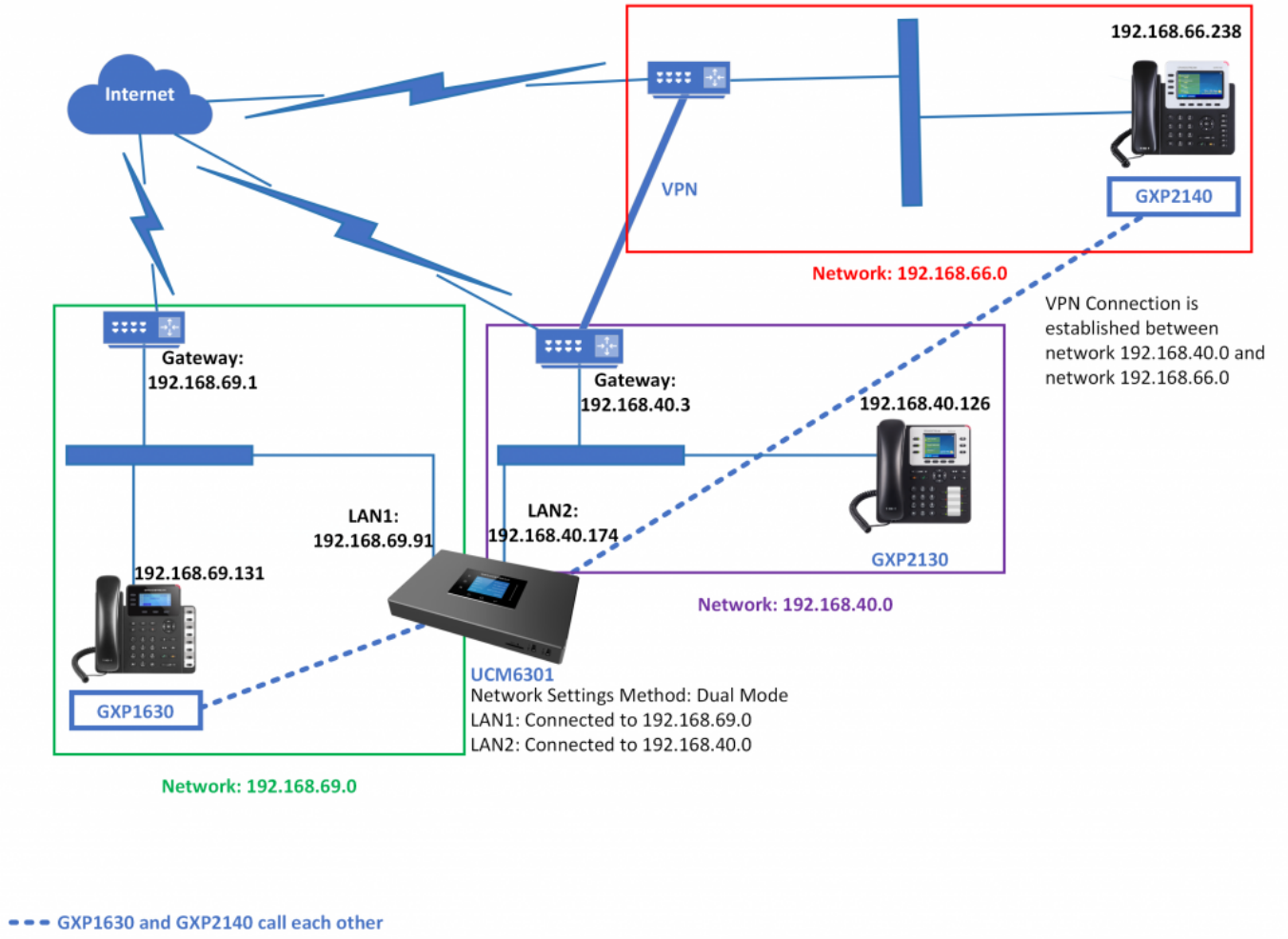
The UCM630X provides users static routing capability that allows the device to use manually configured routes, rather than information only from dynamic routing or gateway configured in the UCM630X Web GUI **-> System Settings -> Network Settings -> Basic Settings** to forward traffic. It can be used to define a route when no other routes are available or necessary or used in complementary with existing routing on the UCM630X as a failover backup, etc.

- Click on **"Add IPv4 Static Route"** to create a new IPv4 static route or click **"Add IPv6 Static Route"** to create a new IPv6 static route. The configuration parameters are listed in the table below.
- Once added, users can select to edit the static route.
- Select to delete the static route.

Parameter	Description
Destination	Configure the destination IPv4 address or the destination IPv6 subnet for the UCM630X to reach using the static route. Example: IPv4 address - 192.168.66.4 IPv6 - 2001:740:D::1/64
Subnet Mask	Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255. Example:255.255.255.0
Gateway	Configure the IPv4 or IPv6 gateway address so that the UCM630X can reach the destination via this gateway. The gateway address is optional.Example:192.168.40.5 or 2001:740:D::1
Interface	Specify the network interface on the UCM630X to reach the destination using the static route. LAN interface is eth0; WAN interface is eth1.

Static routes configuration can be reset from the **LCD menu > Network Menu**.

The following diagram shows a sample application of static route usage on UCM6304.

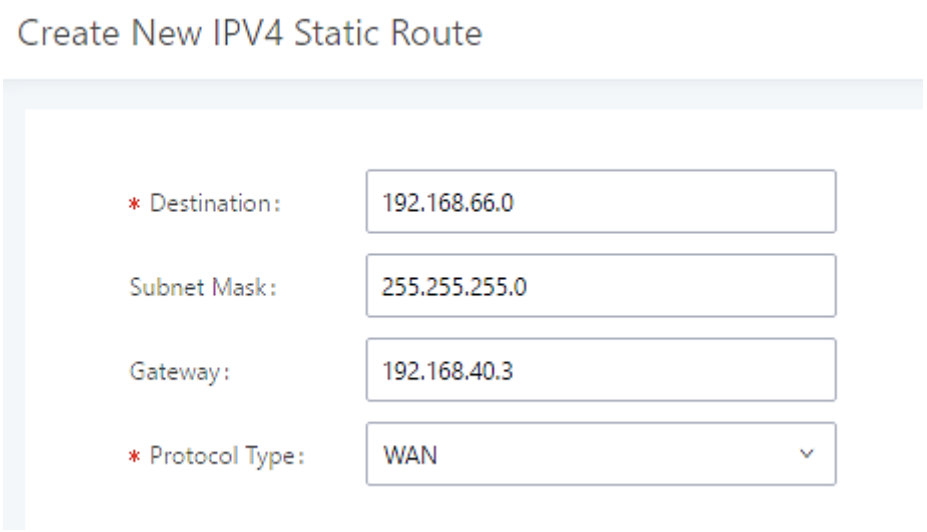


UCM630X Network Settings→Static Routes

The network topology of the above diagram is as below:

- Network 192.168.69.0 has IP phones registered to UCM6304 LAN 1 address
- Network 192.168.40.0 has IP phones registered to UCM6304 LAN 2 address
- Network 192.168.66.0 has IP phones registered to UCM6304 via VPN
- Network 192.168.40.0 has a VPN connection established with network 192.168.66.0

In this network, by default, the IP phones in network 192.168.69.0 are unable to call IP phones in network 192.168.66.0 when registered on different interfaces on the UCM6304. Therefore, we need to configure a static route on the UCM6304 so that the phones in isolated networks can make calls between each other.



UCM6304 Static Route Configuration

Port Forwarding

The UCM network interface supports the router function which provides users the ability to do port forwarding. If LAN mode is set to "Route" under Web GUI→**System Settings→Network Settings→Basic Settings** page, port forwarding is available for configuration.

The port forwarding configuration is under Web GUI→**System Settings→Network Settings→Port Forwarding** page. Please see related settings in the table below.

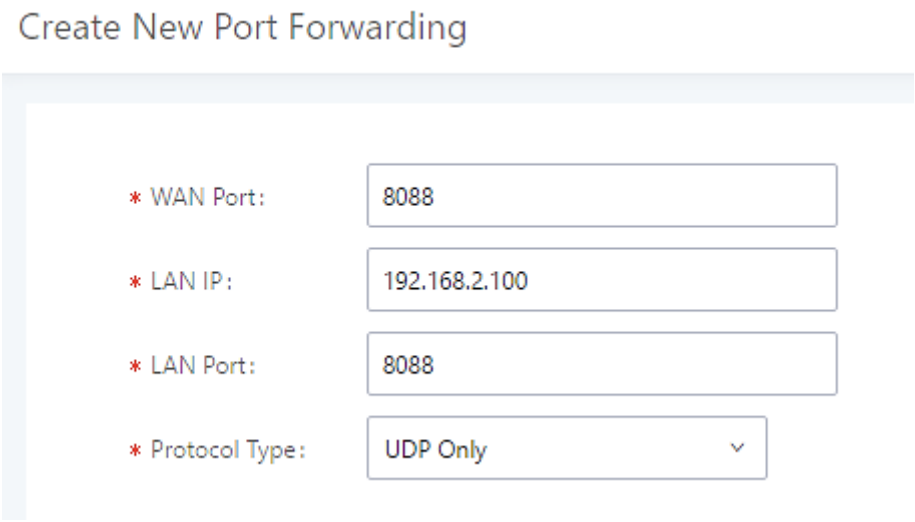
WAN Port	Specify the WAN port number or a range of WAN ports. An unlimited number of ports can be configured.Note:When it is set to a range, the WAN port, and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from the WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
LAN IP	Specify the LAN IP address.
LAN Port	Specify the LAN port number or a range of LAN ports. Note:When it is set to a range, the WAN port, and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from the WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
Protocol Type	Select protocol type "UDP Only", "TCP Only" or "TCP/UDP" for the forwarding in the selected port. The default setting is "UDP Only".

UCM630X Network Settings > Port Forwarding

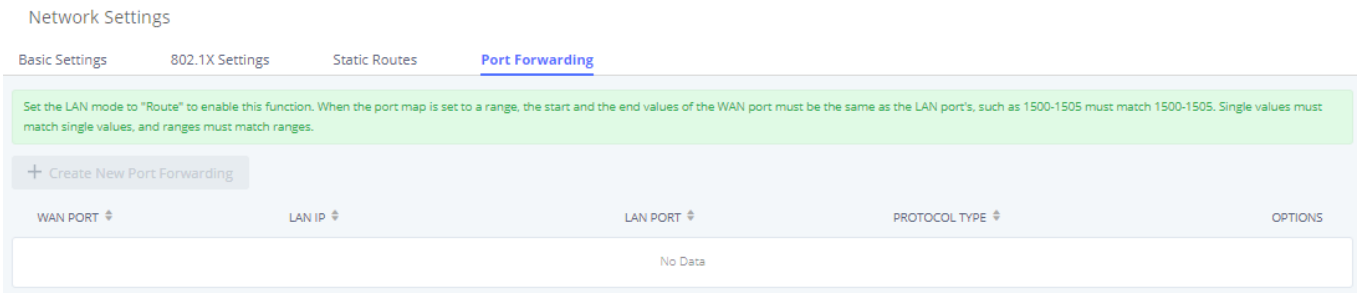
The following figures demonstrate a port forwarding example to provide a phone's Web GUI access to the public side.

- UCM630X network mode is set to "Route".
- UCM630X WAN port is connected to the uplink switch, with a public IP address configured, e.g. 1.1.1.1.
- UCM630X LAN port provides a DHCP pool that connects to multiple phone devices in the LAN network 192.168.2.x. The UCM60X is used as a router, with gateway address 192.168.2.1.
- There is a GXP2160 connected under the LAN interface network of the UCM630X. It obtains IP address 192.168.2.100 from the UCM630X DHCP pool.
- On the UCM630X Web GUI→**System Settings→Network Settings→Port Forwarding**, configure a port forwarding entry as the figure shows below.
- **WAN Port**: This is the port opened on the WAN side for access purposes.
- **LAN IP**: This is the GXP2160 IP address, under the LAN interface network of the UCM630X.

- **LAN Port**: This is the port opened on the GXP2160 side for access purposes.
- **Protocol Type**: We select TCP here for Web GUI access using HTTP.

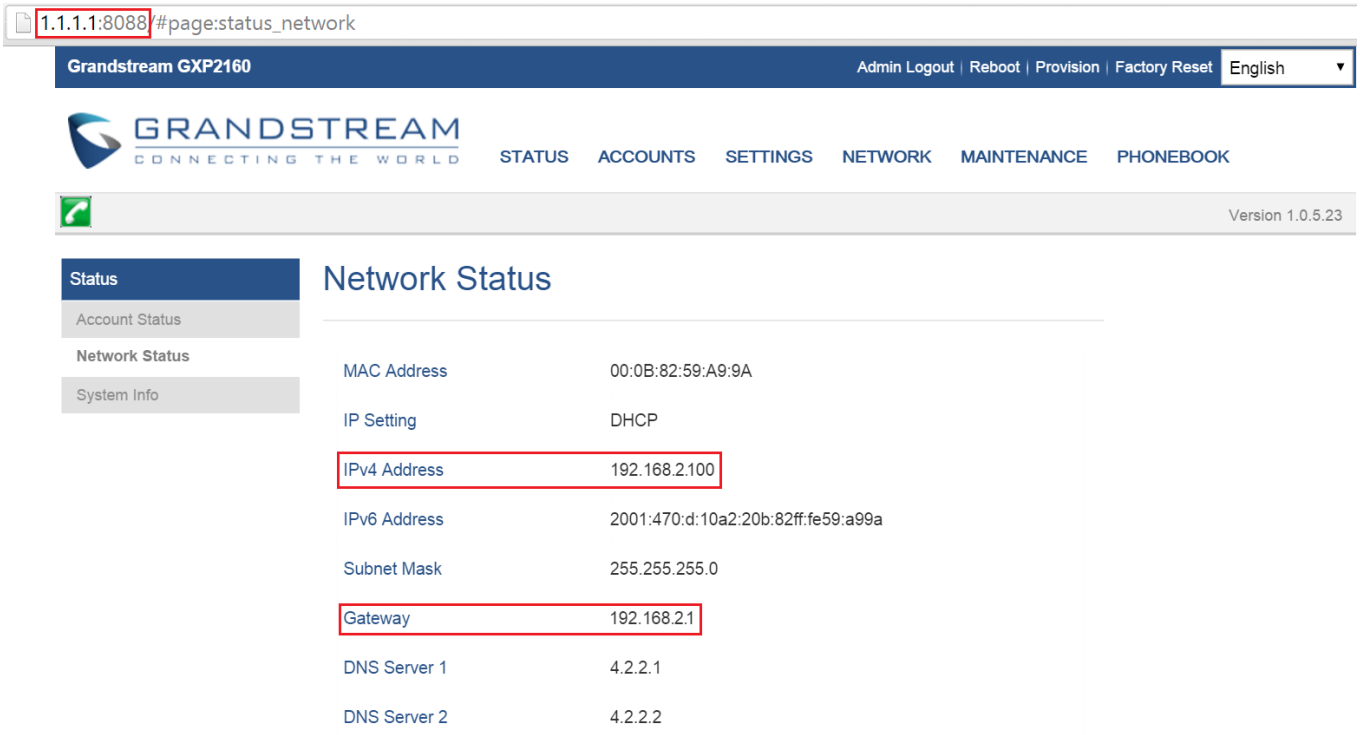


Create New Port Forwarding



UCM630X Port Forwarding Configuration

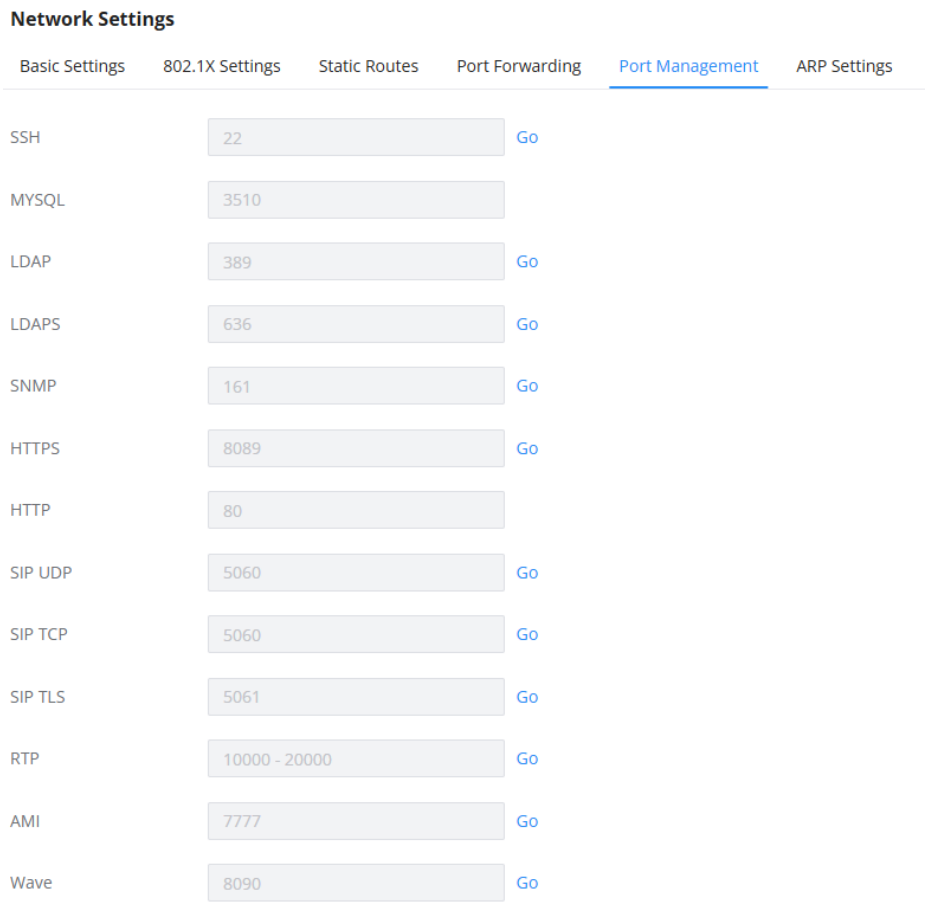
This will allow users to access the GXP2160 Web GUI from the public side, by typing in the public IP address (example: 1.1.1.1:8088).



GXP2160 Web Access using UCM6302 Port Forwarding

Port Management

In this page, the user can view and change the default ports for the different services of the UCM. The user can click on "Go" to navigate to the page to edit the corresponding service port.



ARP Settings

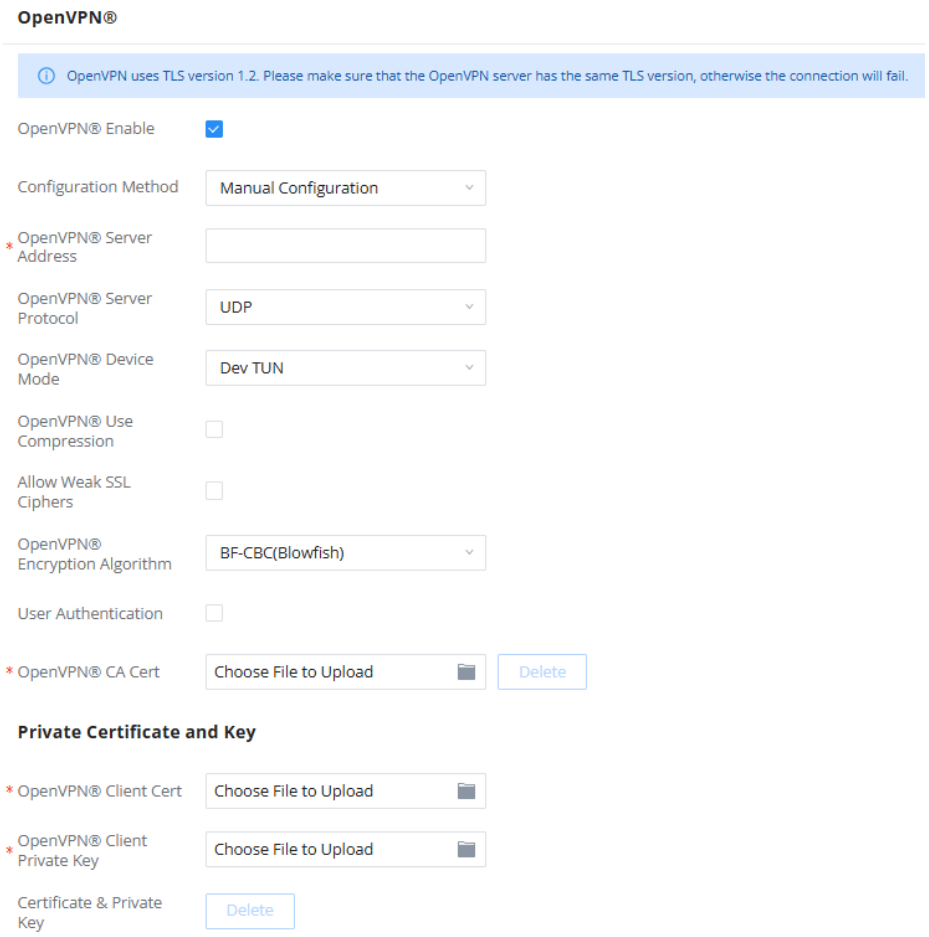
The ARP settings can be configured under Web GUI→**System Settings→Network Settings→ARP Settings**

ARP GC Threshold 1	A minimum number of entries to keep. The garbage collector will not purge entries if there are fewer than this number. The default value is 128.
ARP GC Threshold 2	Threshold when garbage collector becomes more aggressive about purging entries. Entries older than 5 seconds will be cleared when over this number. The default value is 512.
ARP GC Threshold 3	The maximum number of non-PERMANENT neighbor entries allowed. Increase this when using large numbers of interfaces and when communicating with large numbers of directly connected peers. The default value is 1024.

ARP Settings

OpenVPN(R)

OpenVPN(R) settings allow the users to configure UCM630X to use VPN features, the following table gives details about the various options to configure the UCM as OpenVPN Client.



Open VPN(R) Feature on the UCM630X

OpenVPN(R) Enable	Enable / Disable the OpenVPN(R) feature.
Configuration Method	Select the OpenVPN(R) configuration method.Manual Configuration: Allows to configure OpenVPN(R) settings manually.Upload Configuration File: Allows to upload .ovpn and .conf files to the UCM and to automatically configure OpenVPN(R) settings.

OpenVPN(R) Configuration File	Allows to upload the OpenVPN(R) Configuration File when the configuration method is set to "Upload Configuration File".
OpenVPN(R) Server Address	Configures the hostname/IP and port of the server. For example 192.168.1.2:22
OpenVPN(R) Server Protocol	Specify the protocol user, user should use the same settings as used on the server
OpenVPN(R) Device mode	Use the same setting as used on the server. Dev TUN: Create a routed IP tunnel. Dev TAP: Create an Ethernet tunnel.
OpenVPN(R) Use Compression	Compress tunnel packets using the LZO algorithm on the VPN link. Do not enable this unless it is also enabled in the server config file.
Enable Weak SSL Ciphers	Either to enable the Weak SSL ciphers or not.
OpenVPN(R) Encryption Algorithm	Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server.
User Authentication	Specifies whether username and password authentication is required by the remote OpenVPN server. When turned on, additional input fields display to enter the user credentials required alongside the SSL/TLS root certificate
Username	Username used to authenticate into the server.
Password	Password used to authenticate into the server.
OpenVPN(R) CA Cert	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
Private Certificate and Key	
OpenVPN(R) Client Cert	Upload a client certificate. This file will be renamed as 'client.crt' automatically.
OpenVPN(R) Client Private Key	Upload a client private key. This file will be renamed as 'client.key' automatically.
Certificate & Private Key	Allows to delete the certificate and private key.

DDNS Settings

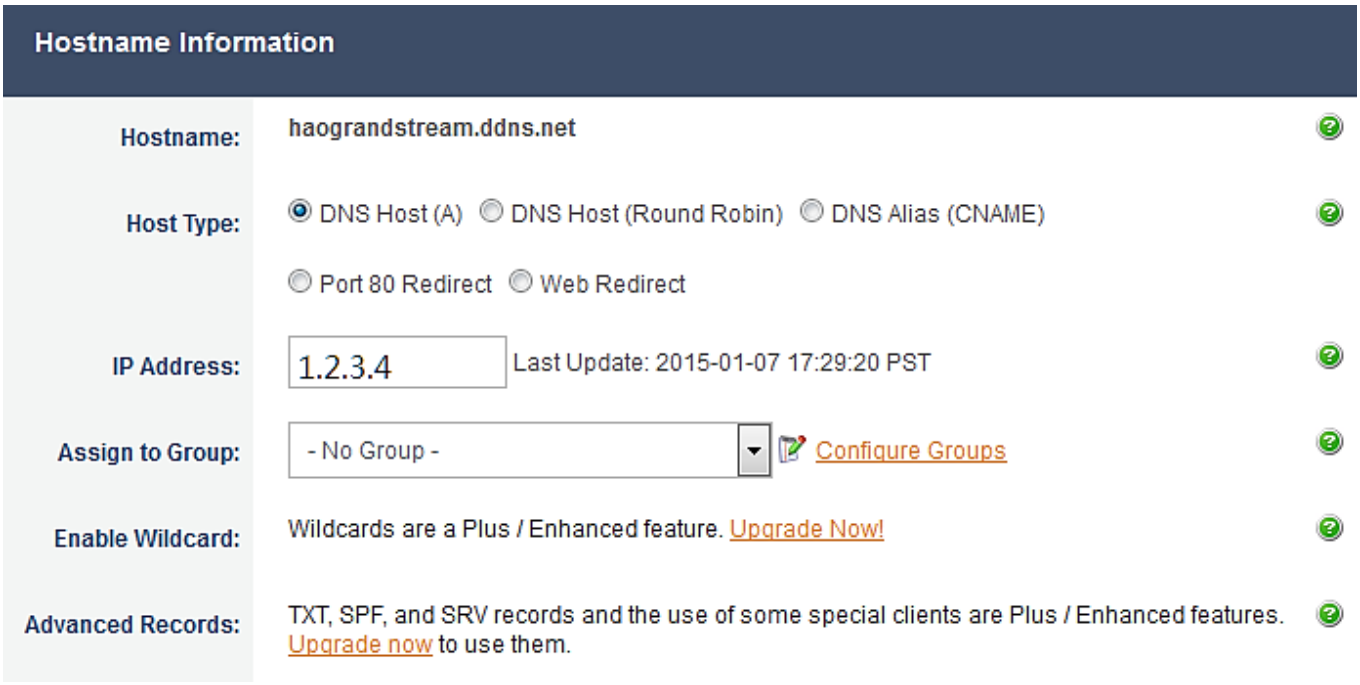
DDNS setting allows users to access UCM630X via domain name instead of IP address.

The UCM supports DDNS service from the following DDNS provider:

- dydns.org
- noip.com
- freedns.afraid.org
- zoneedit.com
- oray.net

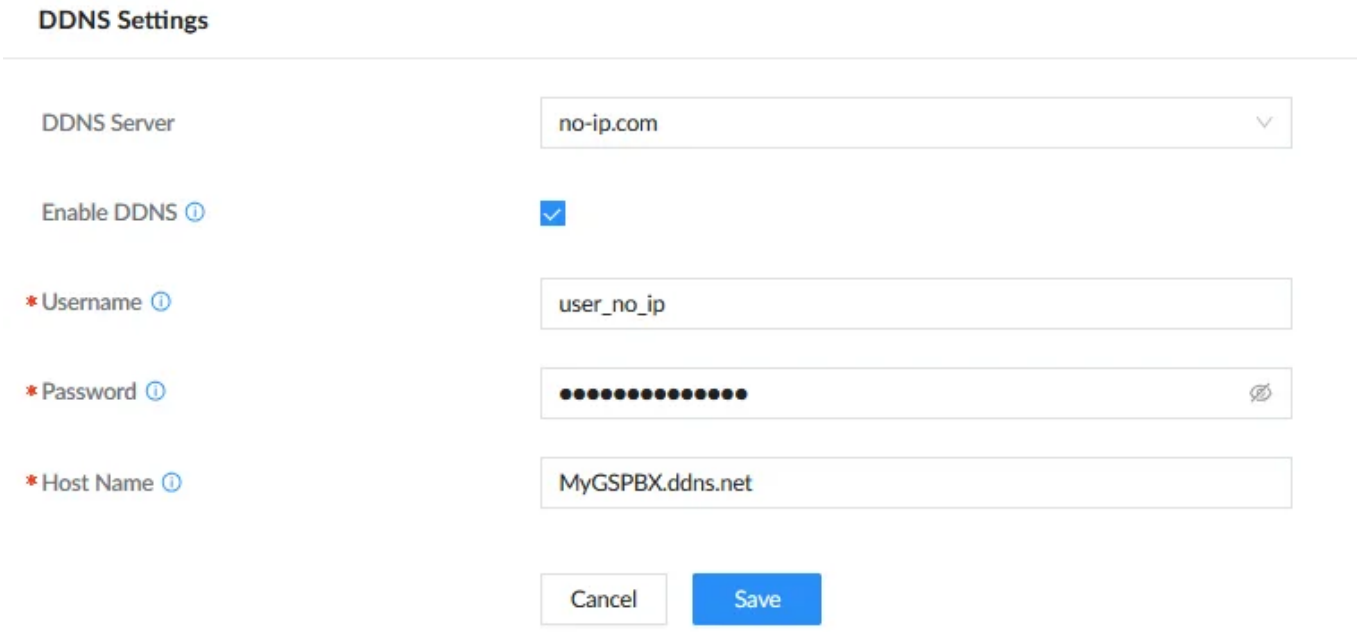
Here is an example of using noip.com for DDNS.

1. Register domain in DDNS service provider. Please note the UCM630X needs to have public IP access.



Register Domain Name on noip.com

2. To configure DDNS Settings, navigate to Web GUI -> **System Settings** -> **Network Settings** -> **DDNS Settings**. The configurable parameters on this page are described below:

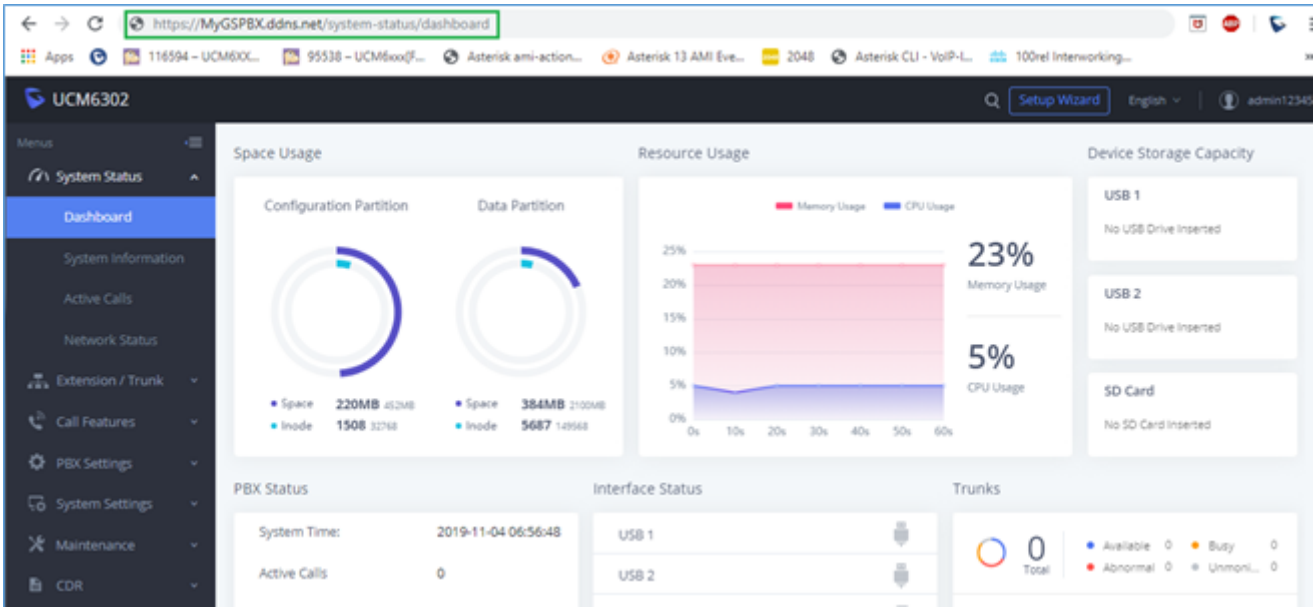


UCM630X DDNS Setting

Option	Description
DDNS Server	Select the Dynamic DNS service provider to handle IP updates (e.g., freedns.afraid.org, dyndns.org, noip.com, zoneedit.com, or oray.net).
Enable DDNS	Enables or disables automatic DDNS updates for the PBX.
Username	Enter the account username for authenticating with the selected DDNS provider.
Password	Enter the account password for authenticating with the selected DDNS provider.
Hash	Enter the authentication hash token provided by the DDNS service (required by providers such as freedns.afraid.org).

Host Name	Enter the registered domain or host name to be dynamically updated with the PBX's public IP address (e.g., myucm.freedns.org).

3. Now you can use a domain name instead of an IP address to connect to the UCM630X Web GUI.



Using Domain Name to Connect to UCM630X

Security Settings

The UCM630X provides users firewall security configurations to prevent certain malicious attacks to the UCM630X system. Users could configure to allow, restrict, or reject specific traffic through the device for security and bandwidth purpose. The UCM630X also provides the Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. To configure firewall settings in the UCM630X, go to Web GUI→**System Settings**→**Security Settings** page.

Static Defense

Under Web GUI→**System Settings**→**Security Settings**→**Static Defense** page, users will see the following information:

- Current service information with port, process, and type.
- Typical firewall settings.
- Custom firewall settings.

The following table shows a sample current service status running on the UCM630X.

Port	Process	Type	Protocol or Service
7777	Asterisk	TCP/IPv4	SIP
389	Slapd	TCP/IPv4	LDAP
6060	zero_config	UDP/IPv4	UCM630X zero_config service
5060	Asterisk	UDP/IPv4	SIP
4569	Asterisk	UDP/IPv4	IAX
38563	Asterisk	udp/ipv4	SIP
10000	gs_avs	udp/ipv4	gs_avs
10001	gs_avs	udp/ipv4	gs_avs

10002	gs_avs	udp/ipv4	gs_avs
10003	gs_avs	udp/ipv4	gs_avs
10004	gs_avs	udp/ipv4	gs_avs
10005	gs_avs	udp/ipv4	gs_avs
10006	gs_avs	udp/ipv4	gs_avs
10007	gs_avs	udp/ipv4	gs_avs
10010	gs_avs	udp/ipv4	gs_avs
10012	gs_avs	udp/ipv4	gs_avs
10013	gs_avs	udp/ipv4	gs_avs
10014	gs_avs	udp/ipv4	gs_avs
10015	gs_avs	udp/ipv4	gs_avs
10018	gs_avs	udp/ipv4	gs_avs
10019	gs_avs	udp/ipv4	gs_avs
10020	gs_avs	udp/ipv4	gs_avs
6066	Python	udp/ipv4	python
3306	Mysqld	tcp/ipv4	mysqld
45678	Python	udp/ipv4	python
8439	Lighttpd	tcp/ipv4	HTTP
8088	asterisk	tcp/ipv4	SIP
8888	Pbxmid	tcp/ipv4	pbxmid
25	Master	tcp/ipv4	master
636	Slapd	tcp/ipv4	SLDAP
4569	asterisk	udp/ipv6	SIP
42050	asterisk	udp/ipv6	SIP
7681	Pbxmid	tcp/ipv4	pbxmid

UCM630X Firewall→Static Defense→Current Service

For typical firewall settings, users could configure the following options on the UCM630X.

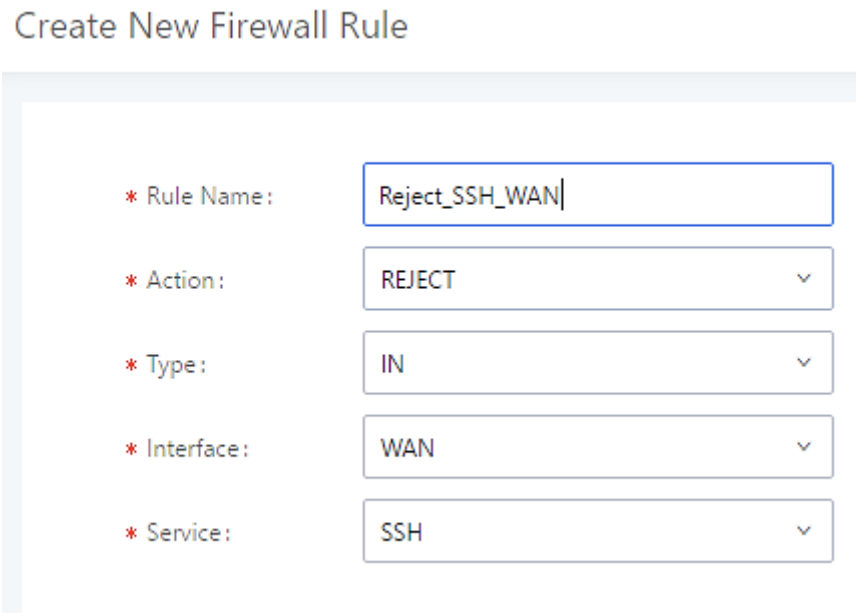
Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping requests. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (UCM630X) interface.
SYN-Flood Defense Enable	Allows the UCM630X to handle excessive amounts of SYN packets from one source and keep the web portal accessible. There are two options available and only one of these options may be enabled at one time. eth(0)LAN defends against attacks directed to the LAN IP address of the UCM630X. eth(1)WAN defends against attacks directed to the WAN IP address of the UCM630X. SYN Flood Defense will limit the amount of SYN packets accepted by the UCM from one source to 10 packets per second. Any excess packets from that source will be discarded.
Ping-of-Death Defense Enable	Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (UCM630X) interface.

Typical Firewall Settings

Under "Custom Firewall Settings", users could create new rules to accept, reject or drop certain traffic going through the UCM630X. To create a new rule, click on the "Create New Rule" button and a new window will pop up for users to specify rule options.

Right next to the "Create New Rule" button, there is a checkbox for the option "Reject Rules". If it is checked, all the rules will be rejected except the firewall rules listed below. In the firewall rules, only when there is a rule that meets all the following requirements, the option "Reject Rules" will be allowed to check:

- Action: "Accept"
- Type "In"
- The destination port is set to the system login port (e.g., by default 8089)
- The protocol is not UDP



Create New Firewall Rule

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. ACCEPT REJECT DROP
Type	Select the traffic type. IN If selected, users will need to specify the network interface "LAN" or "WAN" (for UCM630X) for the incoming traffic. OUT
Interface	Select the interface to use the Firewall rule.
Service	Select the service type. FTP SSH Telnet HTTP LDAP Custom If "Custom" is selected, users will need to specify Source (IP and port), Destination (IP and port), and Protocol (TCP, UDP, or Both) for the service. Please note if the source or the destination field is left blank, it will be used as "Anywhere".
Source IP Address and Port	Configure a source subnet and port. If set to "Anywhere" or left empty, traffic from all addresses and ports will be accepted. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
Destination IP Address and Port	Configure a destination subnet and port. If set to "Anywhere" or left empty, traffic can be sent to all addresses and ports. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
Protocol	Select the protocol for the rule to be used.

Save the change and click on the "Apply" button. Then submit the configuration by clicking on "Apply Changes" on the upper right of the web page. The new rule will be listed at the bottom of the page with sequence number, rule name, action, protocol, type, source, destination, and operation. More operations are below:

- Click on the pencil icon to edit the rule.
- Click on the trash icon to delete the rule.

Dynamic Defense

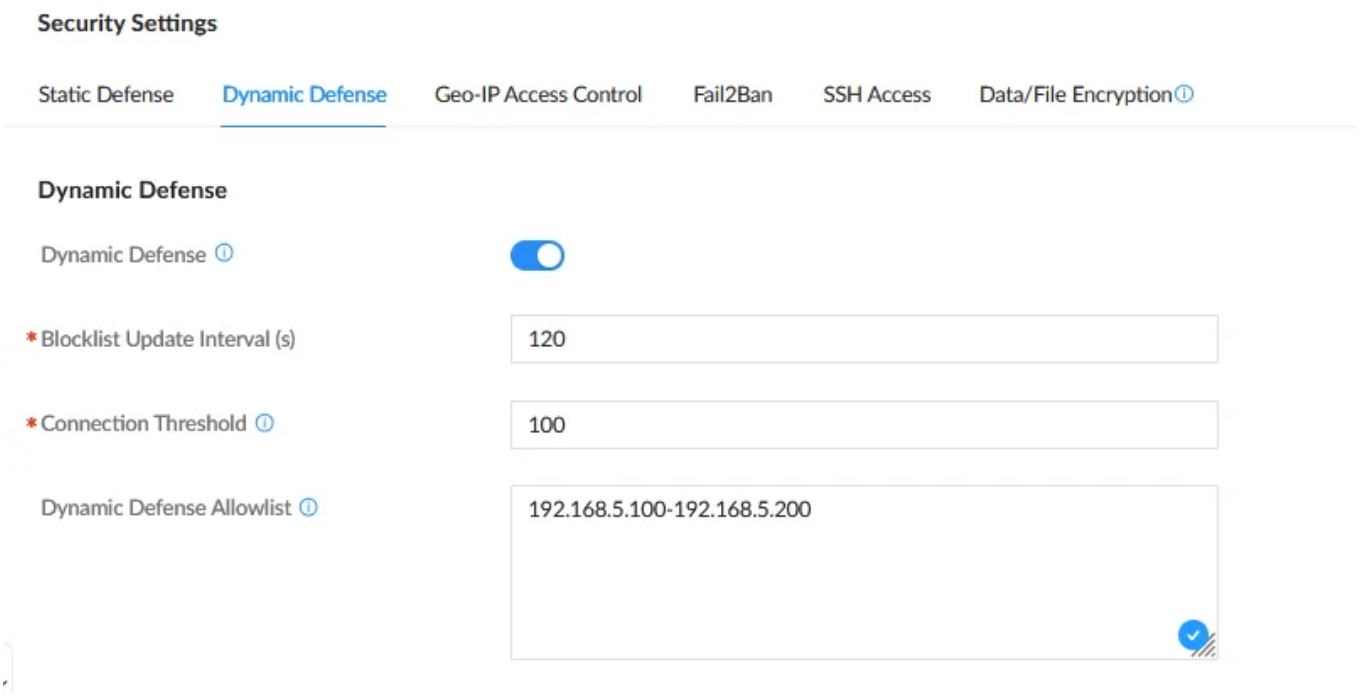
Dynamic defense is supported on the UCM630X series. It can blacklist hosts dynamically when the LAN mode is set to "Route" under Web GUI **System Settings** -> **Network Settings** -> **Basic Settings** page. If enabled, the traffic coming into the UCM630X can be monitored, which helps prevent massive connection attempts or brute force attacks to the device.

The blacklist can be created and updated by the UCM630X firewall, which will then be displayed on the web page. Please refer to the following table for dynamic defense options on the UCM630X.

Dynamic Defense	Enable dynamic defense. The default setting is disabled.
Blocklist Update Interval (s)	Configure the blacklist update time interval (in seconds). The default setting is 120.
Connection Threshold	Configure the connection threshold. Once the number of connections from the same host reaches the threshold, it will be added to the blacklist. The default setting is 100.
Dynamic Defense Allowlist	Allowed IPs and ports range, multiple IP addresses, and port range. For example: 192.168.2.100-192.168.2.105, 1000:9999
Blocklist	Displays IP addresses blocked by Dynamic Defense and allows administrators to manually unblock them.

The following figure shows a configuration example like this:

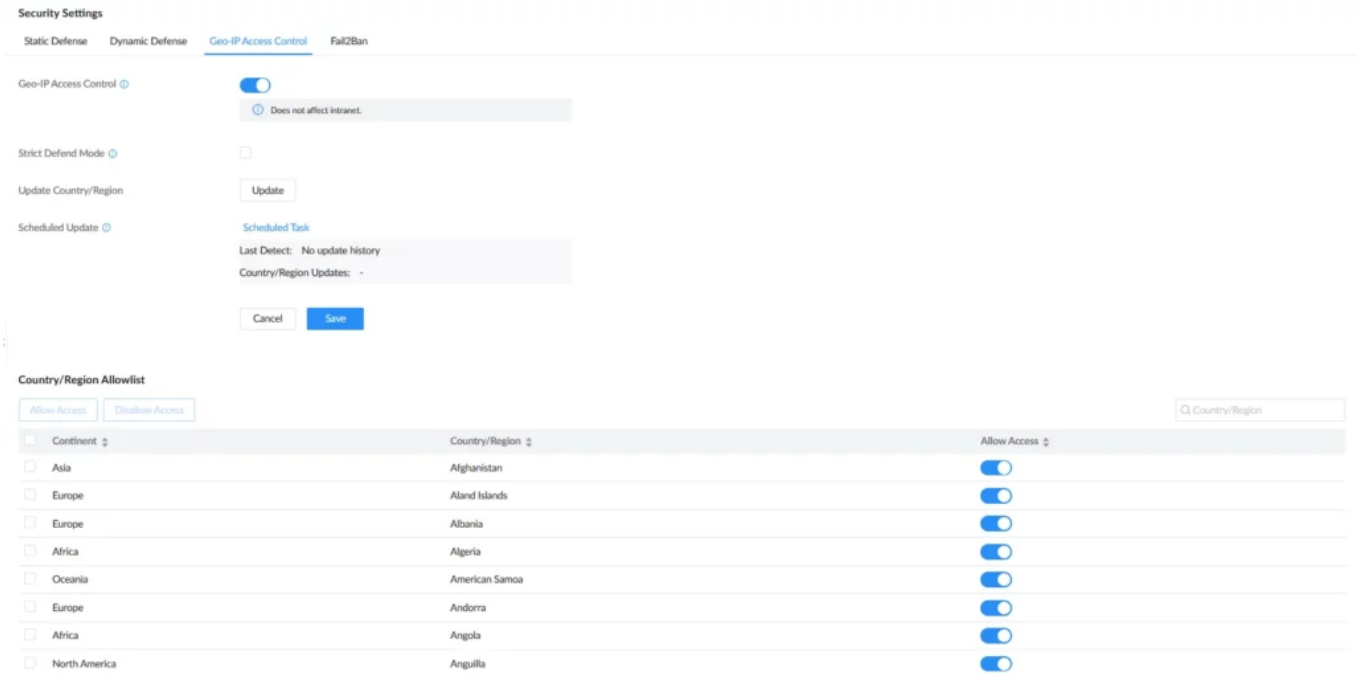
- If a host at IP address 192.168.5.7 initiates more than 20 TCP connections to the UCM630X it will be added to the UCM630X blacklist.
- This host 192.168.5.7 will be blocked by the UCM630X for 500 seconds.
- Since IP range 192.168.5.100-192.168.5.200 is in the whitelist if a host initiates more than 20 TCP connections to the UCM630X it will not be added to the UCM630X blacklist. It can still establish a TCP connection with the UCM630X.



Geo-IP Access Control

This feature allows administrators to control access to the UCM based on the source country or region of incoming IP addresses. When enabled, access from selected countries can be restricted for all external services, including Web GUI access, API access, SIP signaling, and extension registration.

The country/region IP database can be updated manually or automatically to ensure accurate IP-to-location mapping.



UCM Geo-IP Access Control Page

Country/Region IP Defense supports **two enforcement methods**, which determine how and when traffic from blocked countries is handled.

1. **Non-Strict Defend Mode:** In this mode, Country/Region IP Defense is enforced with business priority. Traffic from blocked countries is rejected at the application/service layer. The UCM returns explicit responses (for example, SIP error responses or HTTP error pages). Services remain reachable, but

access is denied.

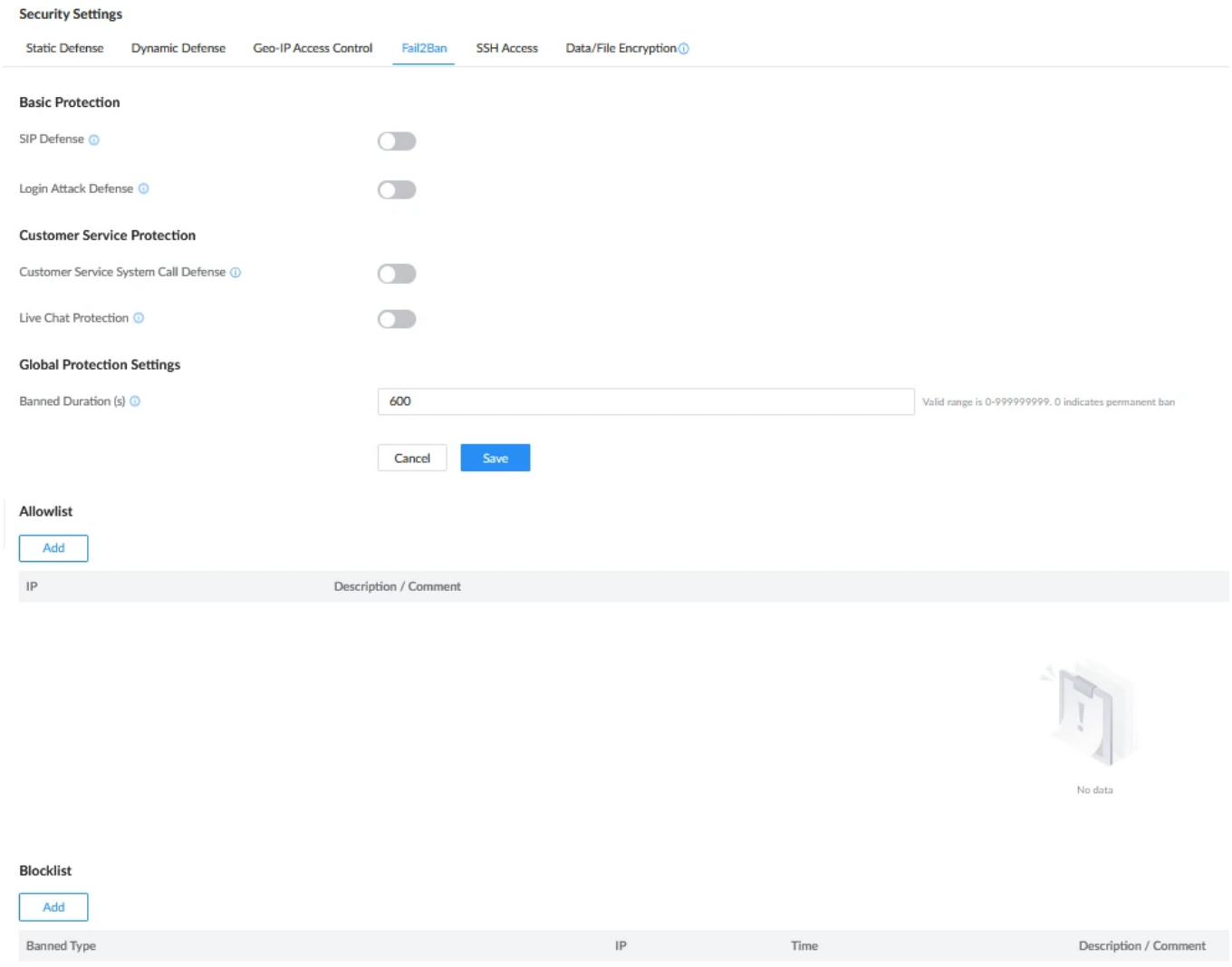
2. **Strict Defend Mode:** In this mode, Country/Region IP Defense is enforced with security priority. Traffic from blocked countries is dropped at the network level, and no SIP, HTTP, or HTTPS response is returned. Requests do not reach the Web server, SIP stack, API services, or Wave services.

- The defense priority is: Static Defense (firewall rules) -> Country/Region IP Defense (Strict) -> Dynamic Defense -> Fail2Ban -> Extension/Service ACLs -> Country/Region IP Defense (Non-Strict).
- Strict Defend Mode is disabled by default. Enabling or disabling this option may reload the Web service and interrupt active management sessions.

Fail2ban

Fail2Ban feature on the UCM630X provides intrusion prevention for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. Once the entry is detected within "Max Retry Duration", the UCM630X will act to forbid the host for a certain period as defined in "Banned Duration". This feature helps prevent SIP brute force attacks on the PBX system.

Fail2ban is enabled by default.



Fail2ban Settings

The table below descibes the main parameters of the Fail2Ban feature:

Basic Protection	
SIP Defense	If enabled, which is the default setting, The UCM will monitor failed SIP registration attempts and heartbeat timeouts based on the security logs. Once the number of failed attempts from an IP address has reached SIP Defense's configured Max Retries value, the IP address will banned for the amount of time configured in the Banned Duration field.
Listening port number	Configure the listening port number for the SIP defense service.
Max Retries	The maximum number of failed SIP attempts allowed before the IP address is banned.
Login Attack Defense	When enabled, which is the default setting, once the number of login attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will banned for the amount of time configured in the Banned Duration field.
Listening port number	Configure the listening port number for the login attack defense service.
Max Retries	The maximum number of failed login attempts allowed before the IP address is banned.
Max Retry Duration (s)	If an IP address exceeds the maximum number of retry login attempts within the configured time frame (in seconds), the IP address will be banned.
Customer Service Protection	
Customer Service System Call Defense	Once the number of call attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will banned for the amount of time configured in the Banned Duration field.
Listening port number	Configure the listening port number for the customer service system defense service.
Max Retries	The maximum number of call attempts allowed within the amount of time configured in the Max Retry Duration field.
Max Retry Duration (s)	Within this time window (in seconds), if the number of visitor chat attempts from an IP address exceeds the value configured in the Max Retries field for Live Chat Protection, the IP address will be banned.
Live Chat Protection	Once the number of chat attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will banned for the amount of time configured in the Banned Duration field.
Max Retries	The maximum number of visitor chat attempts allowed within the amount of time configured in the Max Retry Duration field.
Max Retry Duration (s)	Within this time window (in seconds), if the number of visitor chat attempts from an IP address exceeds the value configured in the Max Retries field for Live Chat Protection, the IP address will be banned.
Global Protection Settings	
Banned Duration (s)	Configure the duration (in seconds) that an IP address is banned. 0 indicates a permanent ban.
Allowlist	Configure IP address, CIDR mask or DNS host in the allowlist. Fail2ban will not ban the host with matching address in this list.
Blocklist	Users will be able to manually add or view the IPs that have been automatically blocked by the UCM.

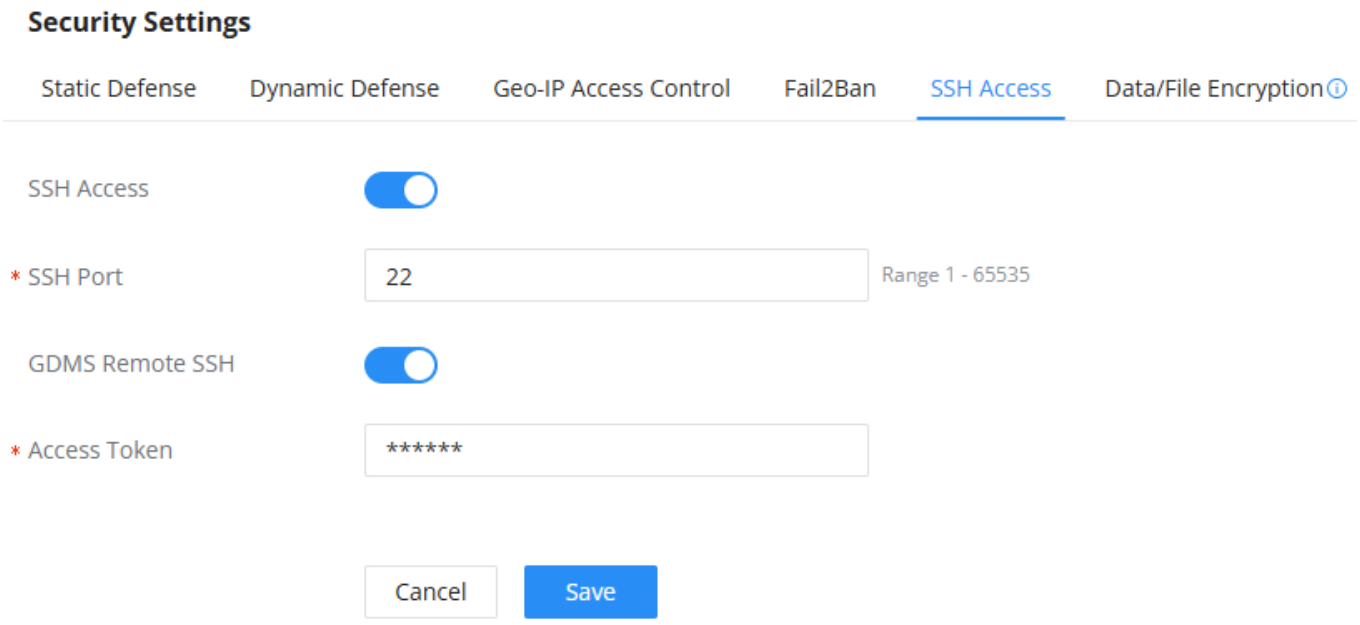
SSH Access

SSH switch now is available via Web GUI and LCD. Users can enable or disable SSH access directly from Web GUI or LCD screen. For web SSH access, please log in to UCM630X web interface and go to Web GUI

-> System Settings -> Security Settings -> SSH Access.

The "Enable SSH access" option is for system debugging. If you enable this option, the system will allow SSH access. The SSH connection require using the username "admin" and the super administrator's password. This option is turned off by default. It is recommended to turn off this option when debugging is not required.

Tick "Enable remote SSH" option, the system will allow remote SSH access via the GDMS platform. This option is turned off by default, and it is strongly recommended to turn off this option when remote troubleshooting is not required.

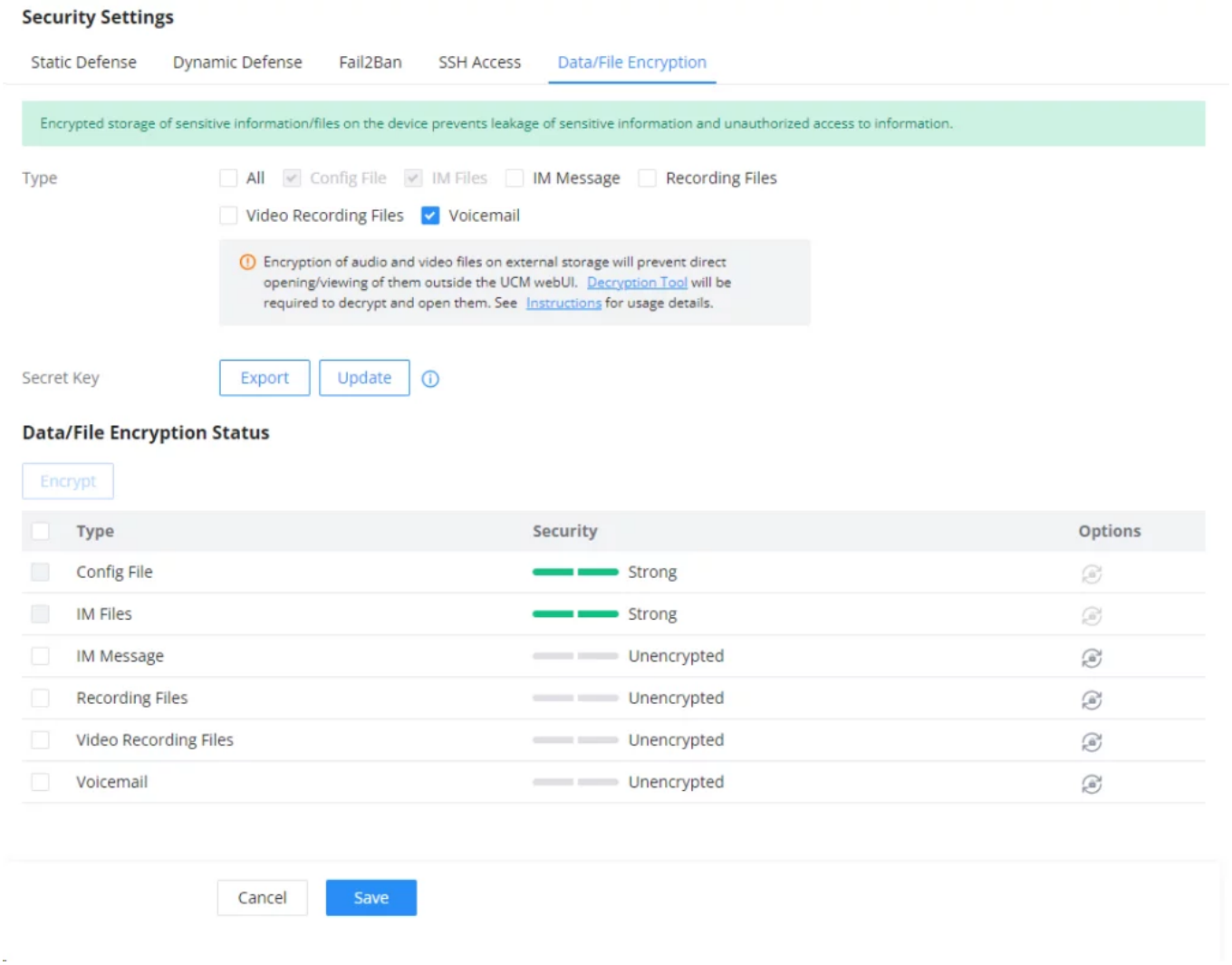


SSH Access

SSH Access	This option is used for system debugging. Once enabled, UCM will allow SSH access. The SSH connection requires super administrator's username and password. The default setting is "No". It is recommended to set it to "No" if there is no need for debugging.
SSH Port	Define the SSH service port.
GDMS Remote SSH	If enabled, remote SSH access will be made available via the platform for 2 days. Once expired, it will need to be re-enabled to refresh the timer.Note: It is highly recommended to keep this disabled unless remote troubleshooting is necessary.
Access Token	Enter the token to establish SSH access.

Data/File Encryption

The UCM6300 Series offers encryption for your data stored on the internal storage space of the UCM or on the attached storage units (e.g., SD Card, USB HDD/SSD, USB Flash Drive). This feature will harden the security and confidentiality of your data, which renders it impossible to read data in case they end up acquired by unauthorized parties. To access this feature, please navigate to **PBX Settings -> Security Settings -> Data/File Encryption**.

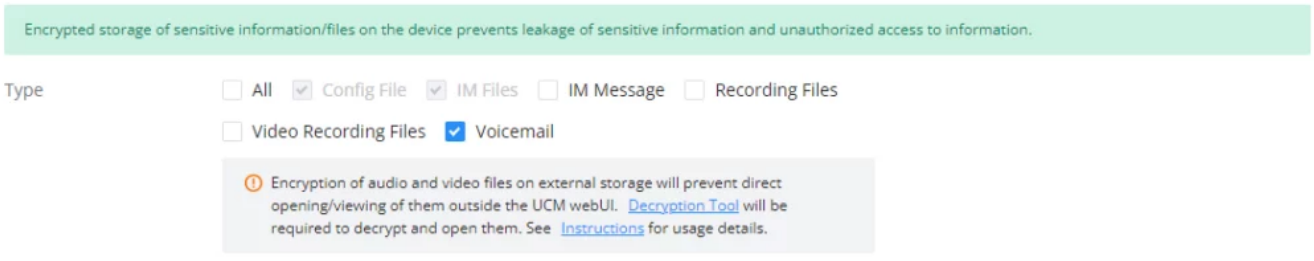


Data/File Encryption

Encrypting the data stored on attached storage units will prevent the user from browsing the data directly from the UCM USB/SD Card file explorer.

Enabling Data/File Encryption

To choose which files are going to encrypted, use the following settings to enable the encryption for specific types of data.



File/Data Type

Once the user chooses which data to encrypt, the user can save the setting. This means that any data created after this configuration will be encrypted, however, all the data which has been created prior to this configuration is not encrypted. To encrypt it please see the sections below.

Encrypting Files

When the user click on "Export" button, a file which contains the secret key will be downloaded. This key can be stored safely and used to decrypt the data later on.



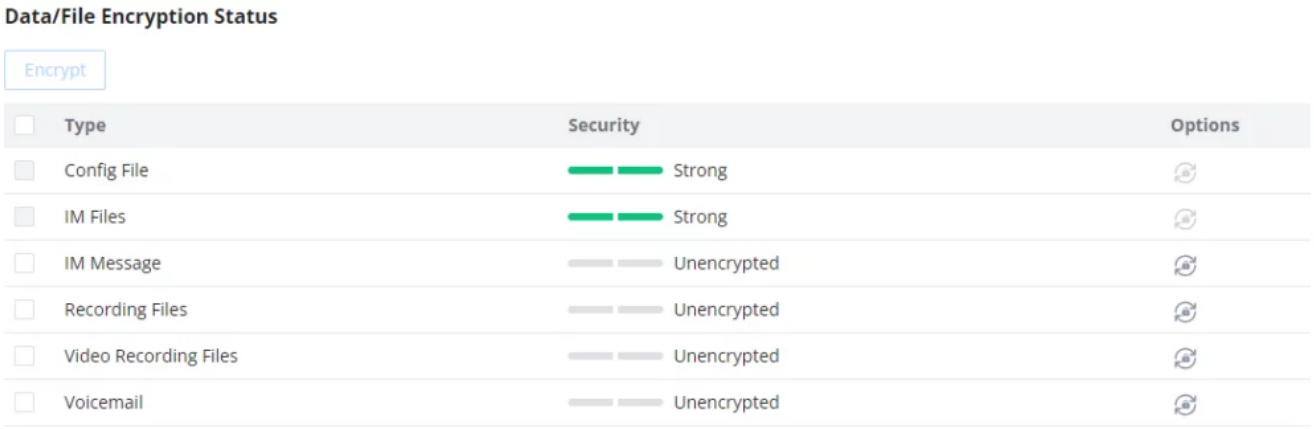
Secret Key Export/Update

You can update the secret key using the "Update" button, this would require entering the administrator's password to allow the user to change the secret key.

Please note that only the super administrator can change the secret key.

If the key has been updated after it has been exported, this will render the old key obsolete and the user will not be able to decrypt the data. We highly recommend that you do not change the encryption key after it has been backed up. In case you need to change the encryption key, please make sure to export the new one and store it safely.

In the following section, the user can view the status of the files, whether they are encrypted or not. The user can also select the different data types to encrypt. This will encrypt the existing data.



Data/File Encryption Status

The user can select the types of stored files to encrypt, then use the button to start the encryption. Or you can encrypt the files using the following encrypting button .

To open and play encrypted audio/video files outside of the UCM system, users need a decryption tool (found on the Grandstream Tools page), a key file and the password for it (set when exporting the key file).

For more information on how to use the decryption tool, please refer to the following guide :

UCM6300/A Series IP PBX - CDR Tool Guide

- In an HA environment, the Primary UCM's key will be used as the Master Key, and this will be synced with the Secondary UCM so both UCMs will use the same key to encrypt and decrypt files.
- Files on the standby machine are not automatically encrypted so users will need to manually re-encrypt all new files that were created before the failover.

- Downgrading from a firmware version with data encrypted to a firmware version which does not support data encryption will require the user to perform a factory reset.
- Backing up the data of the PBX before upgrading the firmware is highly recommended to avoid the possibility of data corruption/loss.

LDAP Server

The UCM630X has an embedded LDAP/LDAPS server for users to manage the corporate phonebook in a centralized manner.

- By default, the LDAP server has generated the first phonebook with **PBX DN** "ou=pbx,dc=pbx,dc=com" based on the UCM630X user extensions already.
- Users could add new phonebook with a different **Phonebook DN** for other external contacts. For example, "ou=people,dc=pbx,dc=com".
- All the phonebooks in the UCM630X LDAP server have the same **Base DN** "dc=pbx,dc=com".

Term Explanation:

cn= Common Name

ou= Organization Unit

dc= Domain Component

These are all parts of the LDAP Data Interchange Format, according to RFC 2849, which is how the LDAP tree is filtered.

If users have the Grandstream phone provisioned by the UCM630X, the LDAP directory will be set up on the phone and can be used right away for users to access all phonebooks.

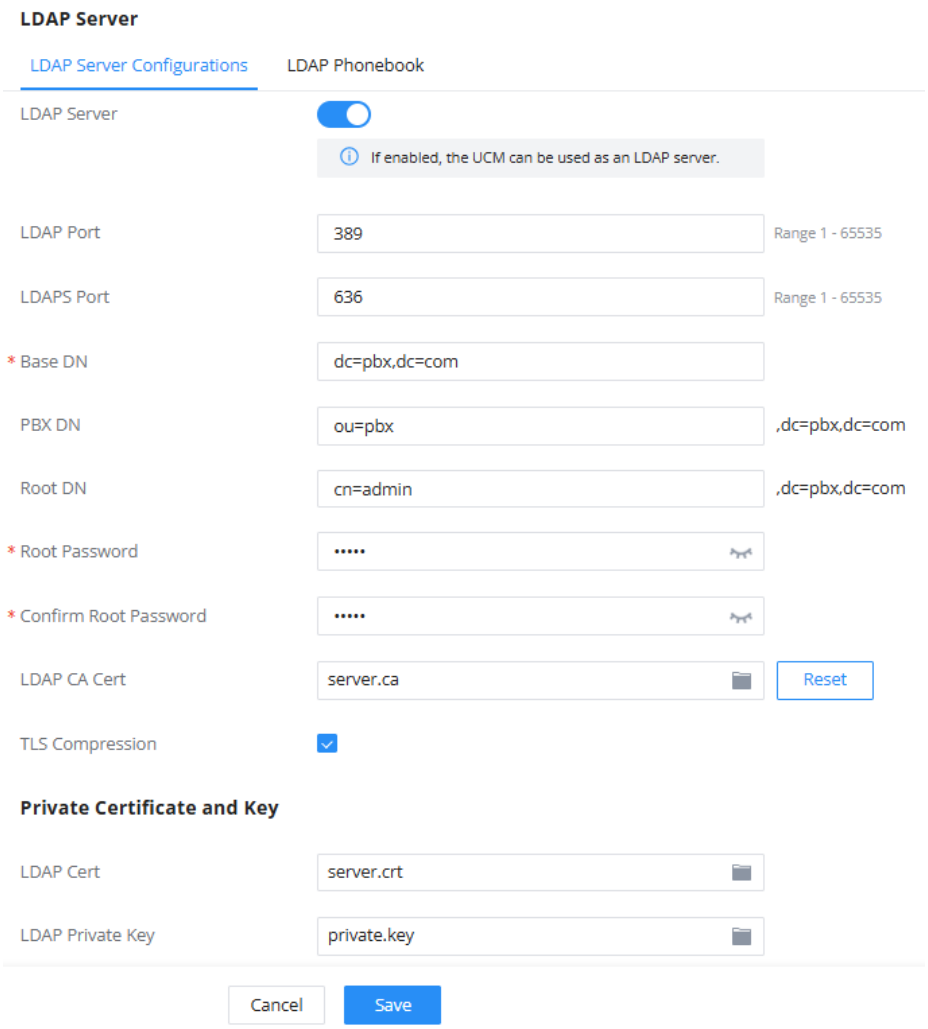
Additionally, users could manually configure the LDAP client settings to manipulate the built-in LDAP server on the UCM630X. If the UCM630X has multiple LDAP phonebooks created, in the LDAP client configuration, users could use "dc=pbx,dc=com" as Base DN to have access to all phonebooks on the UCM630X LDAP server, or use a specific phonebook DN, for example "ou=people,dc=pbx,dc=com", to access to phonebook with Phonebook DN "ou=people,dc=pbx,dc=com " only.

UCM can also act as an LDAP client to download phonebook entries from another LDAP server.

To access the LDAP server and client settings, go to Web GUI→**Settings→LDAP Server**.

LDAP Server Configurations

The following figure shows the default LDAP server configurations on the UCM630X.



LDAP Server Configuration

Enable LDAP Server	Enable LDAP Server
LDAP Port	Enter the port number for LDAP service. The default port number is 389. The allowed range is 1 - 65535
LDAPS Port	LDAPS server port is predefined and cannot be set by the user. The default port number is 636. The allowed range is 1 - 65535
Base DN	Specifies the location in the directory where the search is requested to begin. It is predefined and cannot be modified.
PBX DN	Specifies the location in the directory where the search for PBX entry is requested to begin. It narrows the search scope and decreases directory lookup time.
Root DN	Specifies the location in the directory where the search for the admin user entry is requested to begin. It narrows the search scope and decreases directory lookup time.
Root Password	Defines the root password for authentication.
Confirm Root Password	Confirms the root password for authentication.
LDAP CA Cert	Upload the LDAPS certification authority certificate.
TLS Compression	If this option is enabled, compression will be performed when transmitting the data. Enabling this option is not recommended since it may present a security risk.Note: This option is disabled by default.
LDAP Cert	Upload the LDAP server certificate

LDAP Private Key	Upload the LDAP private key.
Certificate & Private Key	Click this button to reset the certificate and key configuration.

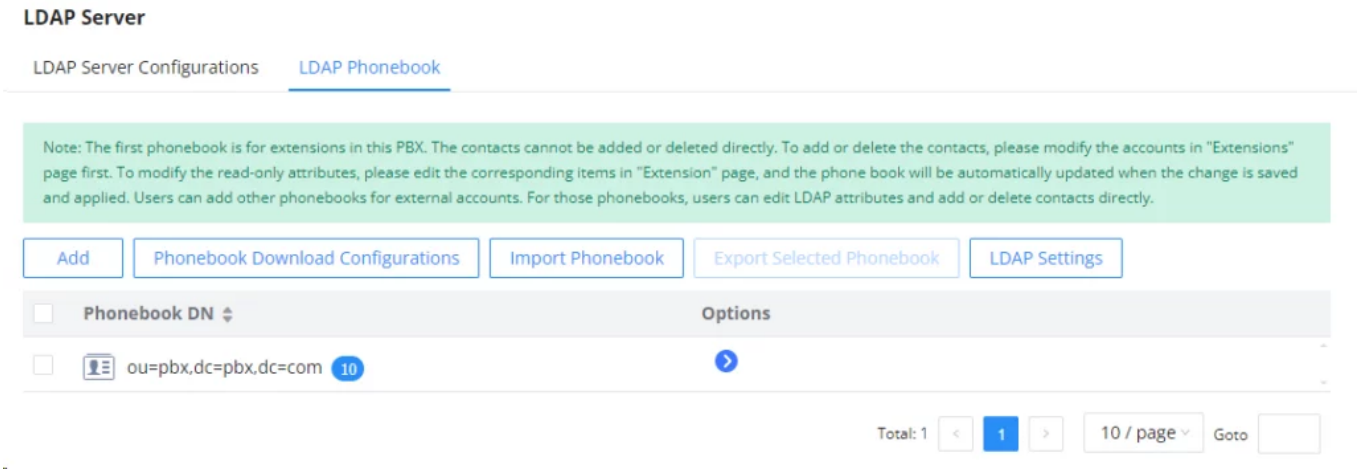
The UCM630X LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client does not have to configure a username and password to access the phonebook directory. The "Root DN" and "Root Password" here are for LDAP management and configuration where users will need to provide for authentication purposes before modifying the LDAP information.

The default phonebook list in this LDAP server can be viewed and edited by clicking on/for the first phonebook under LDAP Phonebook.

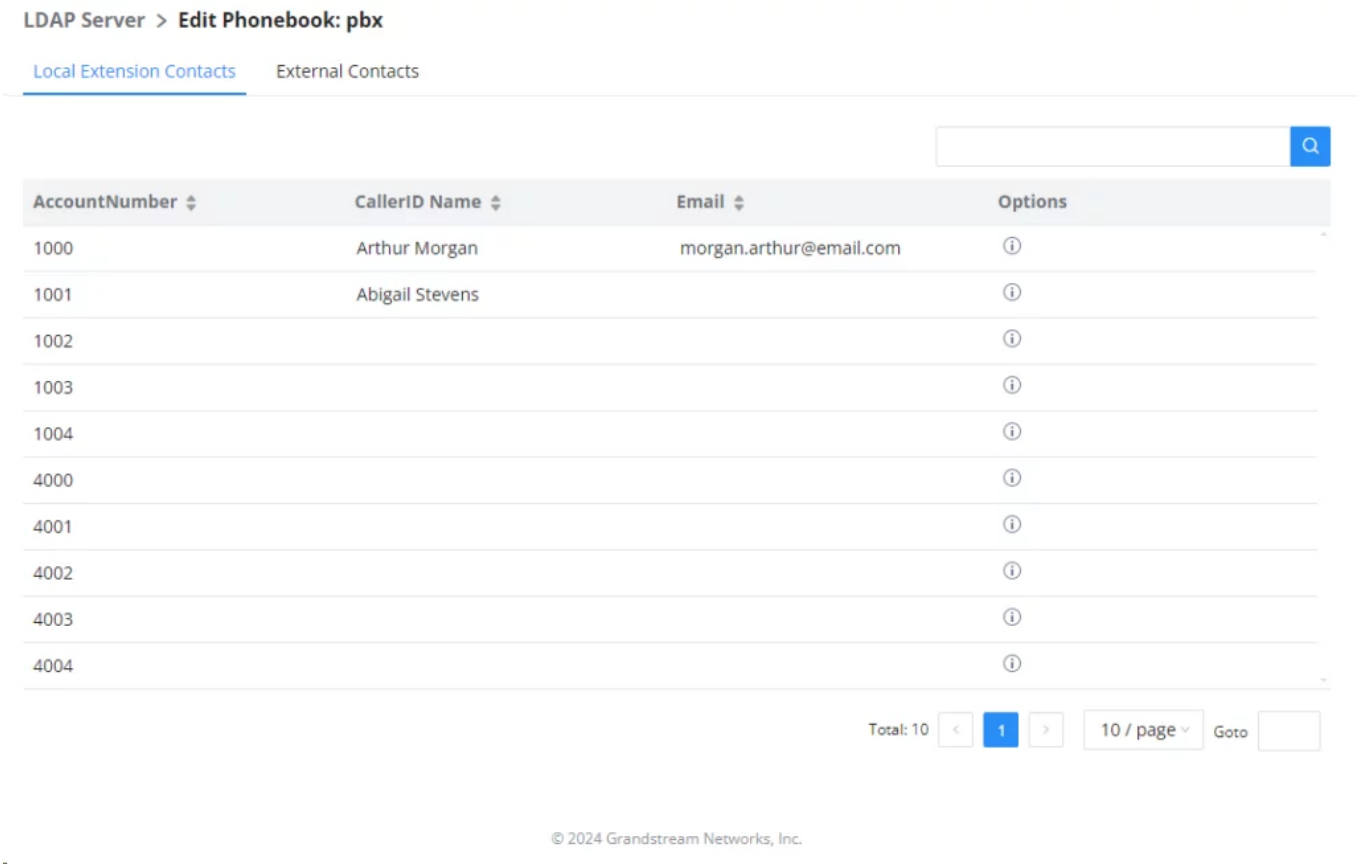
The UCM630X support secure LDAP (LDAPS) where the communication is encrypted and secure.

LDAP Phonebook

Users could use the default phonebook, edit the default phonebook, add new phonebook, import phonebook on the LDAP server as well as export phonebook from the LDAP server.



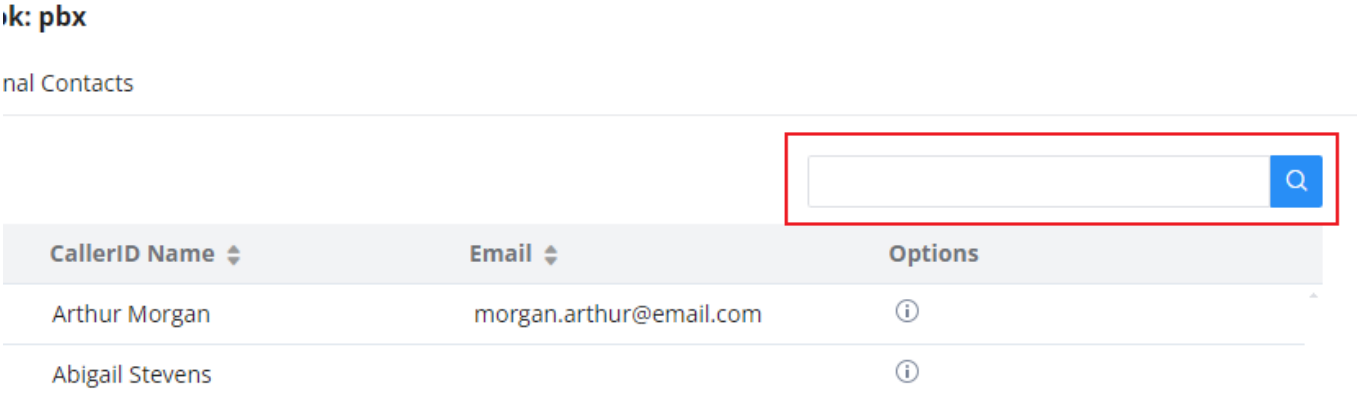
LDAP Server > LDAP Phonebook



Local Phonebook

The user can use the search bar on the top right corner of page, please see the screenshot below.

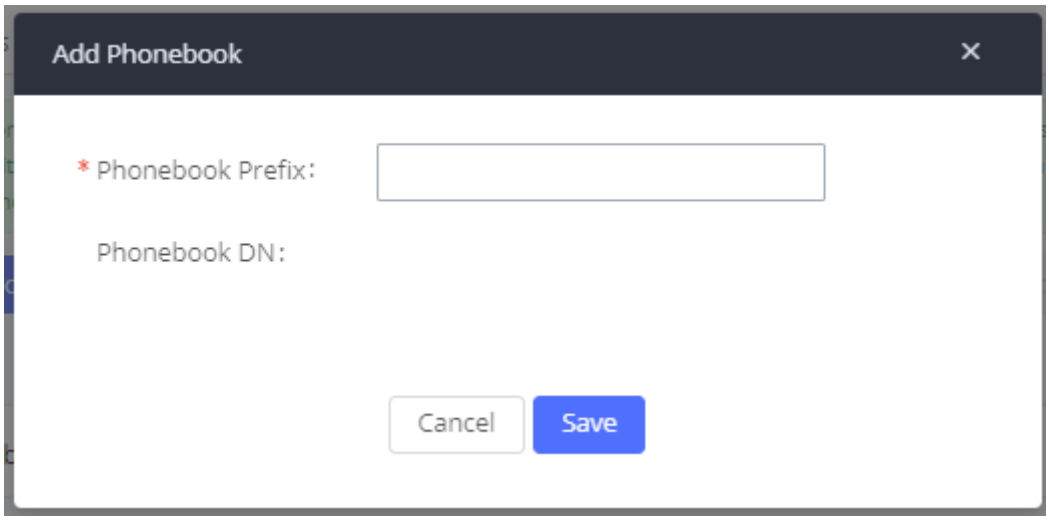
You can enter the extension number or the name of the contact; if you are unsure about the name or the extension, the search feature supports fuzzy matching.



LDAP Phonebook Search Bar

- **Add new phonebook**

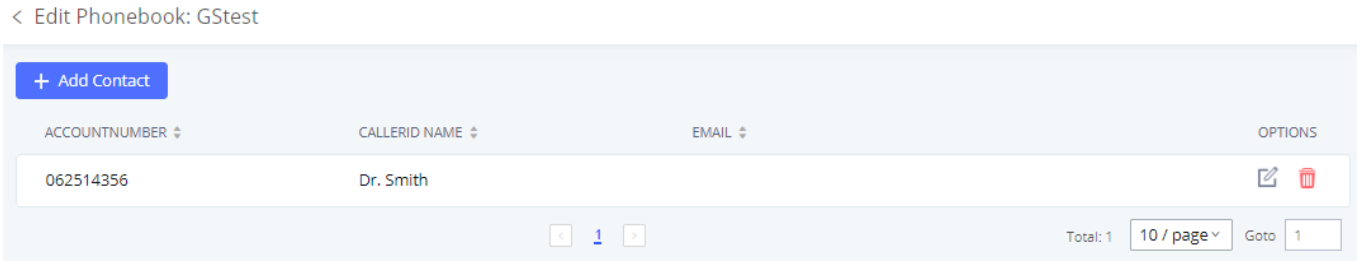
A new sibling phonebook of the default PBX phonebook can be added by clicking on "Add" under "LDAP Phonebook" section.



Add LDAP Phonebook

Configure the "Phonebook Prefix" first. The "Phonebook DN" will be automatically filled in. For example, if configuring "Phonebook Prefix" as "people", the "Phonebook DN" will be filled with "ou=people,dc=pbx,dc=com".

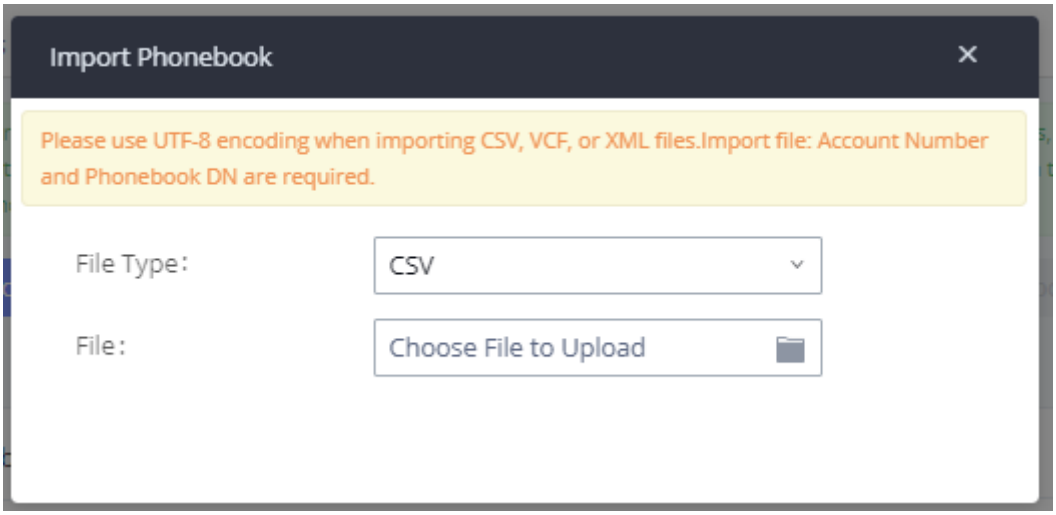
Once added, users can select to edit the phonebook attributes and contact list (see figure below) or select to delete the phonebook.



Edit LDAP Phonebook

- **Import phonebook from your computer to LDAP server**

Click on "Import Phonebook" and a dialog will prompt as shown in the figure below.



Import Phonebook

The file to be imported must be a CSV, VCF, XLSX, or XML file with UTF-8 encoding. Users can open the file with Notepad and save it with UTF-8 encoding.

Here is how a sample file looks like. Please note "Account Number" and "Phonebook DN" fields are required. Users could export a phonebook file from the UCM630X LDAP phonebook section first and use it as a sample to start with.

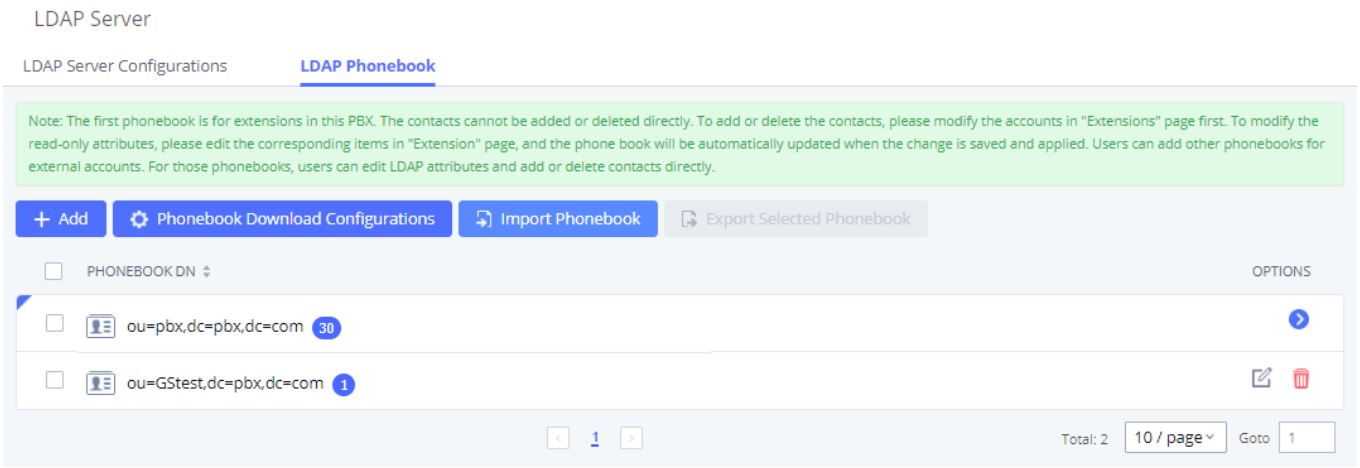
	A	B	C	D	E	F	G	H	I	J
1	First Nam	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	1004	1004		Accounting	1004000000			phonebook
6	Steve	Chang	1005	1005		Support	1005000000			others

Phonebook CSV File Format

The Phonebook DN field is the same "Phonebook Prefix" entry as when the user clicks on "Add" to create a new phonebook. Therefore, if the user enters "phonebook" in "Phonebook DN" field in the CSV file, the actual phonebook DN "ou=phonebook,dc=pbx,dc=com" will be automatically created by the UCM630X once the CSV file is imported.

In the CSV file, users can specify different phonebook DN fields for different contacts. If the phonebook DN already exists on the UCM630X LDAP Phonebook, the contacts in the CSV file will be added into the existing phonebook. If the phonebook DN does not exist on the UCM630X LDAP Phonebook, a new phonebook with this phonebook DN will be created.

The sample phonebook CSV file in above picture will result in the following LDAP phonebook in the UCM630X.

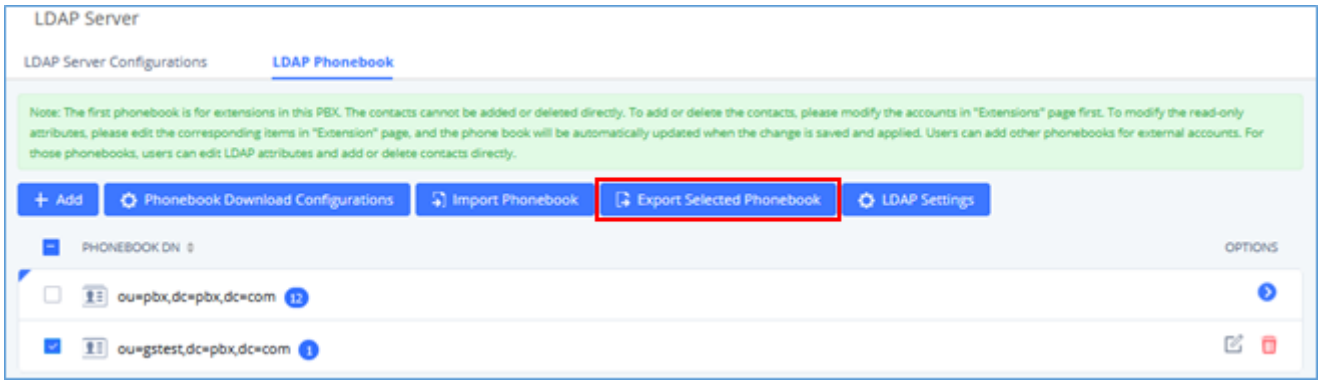


LDAP Phonebook After Import

As the default LDAP phonebook with DN "ou=pbx,dc=pbx,dc=com" cannot be edited or deleted in LDAP phonebook section, users cannot import contacts with Phonebook DN field "pbx" if existed in the file.

- **Export phonebook to your computer from UCM630X LDAP server**

Select the checkbox for the LDAP phonebook and then click on "Export Selected Phonebook" to export the selected phonebook. The exported phonebook can be used as a record or a sample CSV, VFC, XLSX, or XML file for the users to add more contacts in it and import to the UCM630X again.



Export Selected LDAP Phonebook

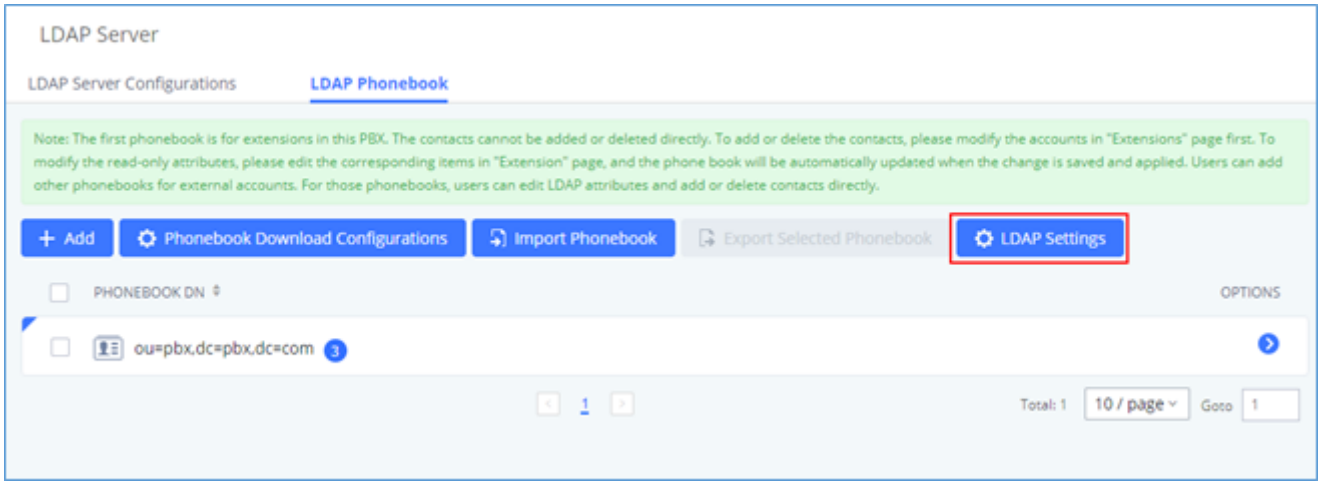
LDAP Settings

Prerequisites to support contacts sync-up to IP Phones, UCM needs to support the following:

1. If Cloud IM is enabled, UCM can send remote UCM's contacts to each end device.
2. Contacts from remote UCM can be synced by Cloud IM or LDAP sync via trunk. The contacts data must be complete and consistent.
3. If Cloud IM is enabled, the contacts sent from UCM to end device should integrate Cloud IM contacts.
4. If Cloud IM is disabled, the contacts sent from UCM to end device should only contain contacts on the UCM.

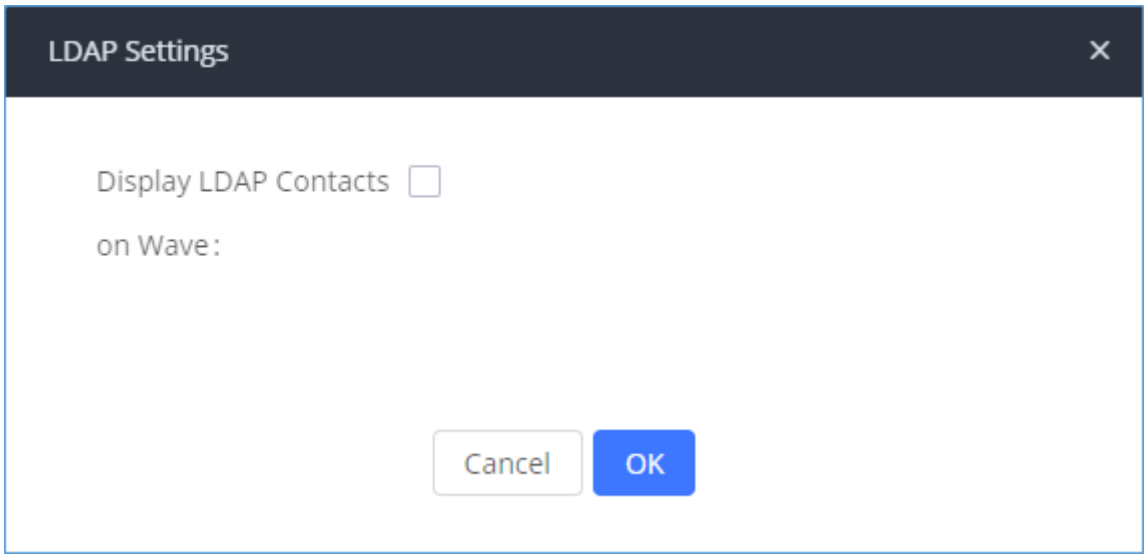
To support contacts sync-up to Wave, it allows Wave to obtain enterprise contacts from Cloud IM or LDAP. On UCM SIP peer trunk, if LDAP sync is enabled, end point can obtain remote UCM extensions' info via LDAP. Also, it will allow configuring whether to sync up LDAP contacts on Wave so that Wave doesn't receive duplicate contacts info.

Under UCM **webUI > System Settings > LDAP Server**, click on "LDAP Settings", option "Wave enable LDAP phonebook" is available for configuration. If enabled, all Wave users on this UCM will display LDAP contacts. Otherwise, it will not display.



LDAP Settings

Please note the LDAP contacts displayed on Wave will exclude the duplicate contacts from Cloud IM.



Display LDAP Contacts on Wave

LDAP Client Configurations

The configuration on LDAP client is useful when you use other LDAP servers. Here we provide an example on how to configure the LDAP client on the UCM.

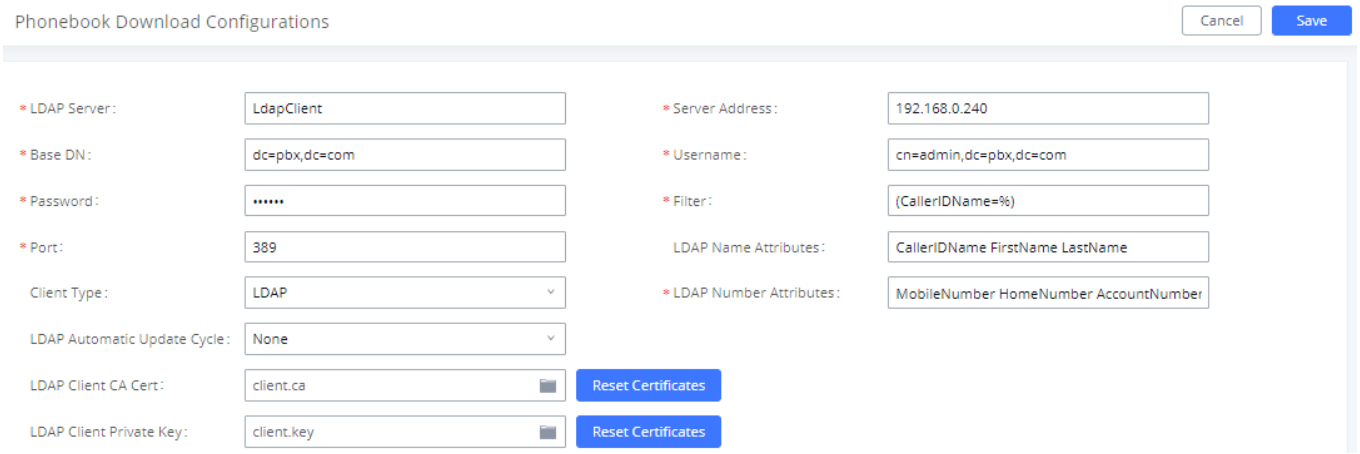
Assuming the remote server base dn is "**dc=pbx,dc=com**", configure the LDAP client as follows:

LDAP Client Type

Phonebook Name	Enter a name for the phonebook
Server Address	The IP address of the LDAP server
Base DN	Enter the base domain name.
Username	Enter the username used to authenticate into the LDAP server, if authentication is required.
Password	Enter the password used to authenticate into the LDAP server, if authentication is required.
Filter	Enter the filter. Ex: (|(CallerIDName=%)(AccountNumber=%))
Port	Enter the port number. Default port is 389
LDAP Number Attributes	Enter the number attributes for the remote server.
Automatic Update Cycle	If "None" is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
LDAP Name Attributes	Enter the name attributes for the remote server.
Client Type	Choose the client type. For encrypted data transfer please choose LDAPS.
LDAP Client CA Cert	LDAP Client Public Certification
LDAP Client Private Key	LDAP Client Private Certification

The UCM can automatically update the phonebook, by configuring the 'LDAP Automatic Update Cycle'. Available options are: 1 day/2days/7 days. It is set to 'None' by default.

The following figure gives a sample configuration for UCM acting as a LDAP client.

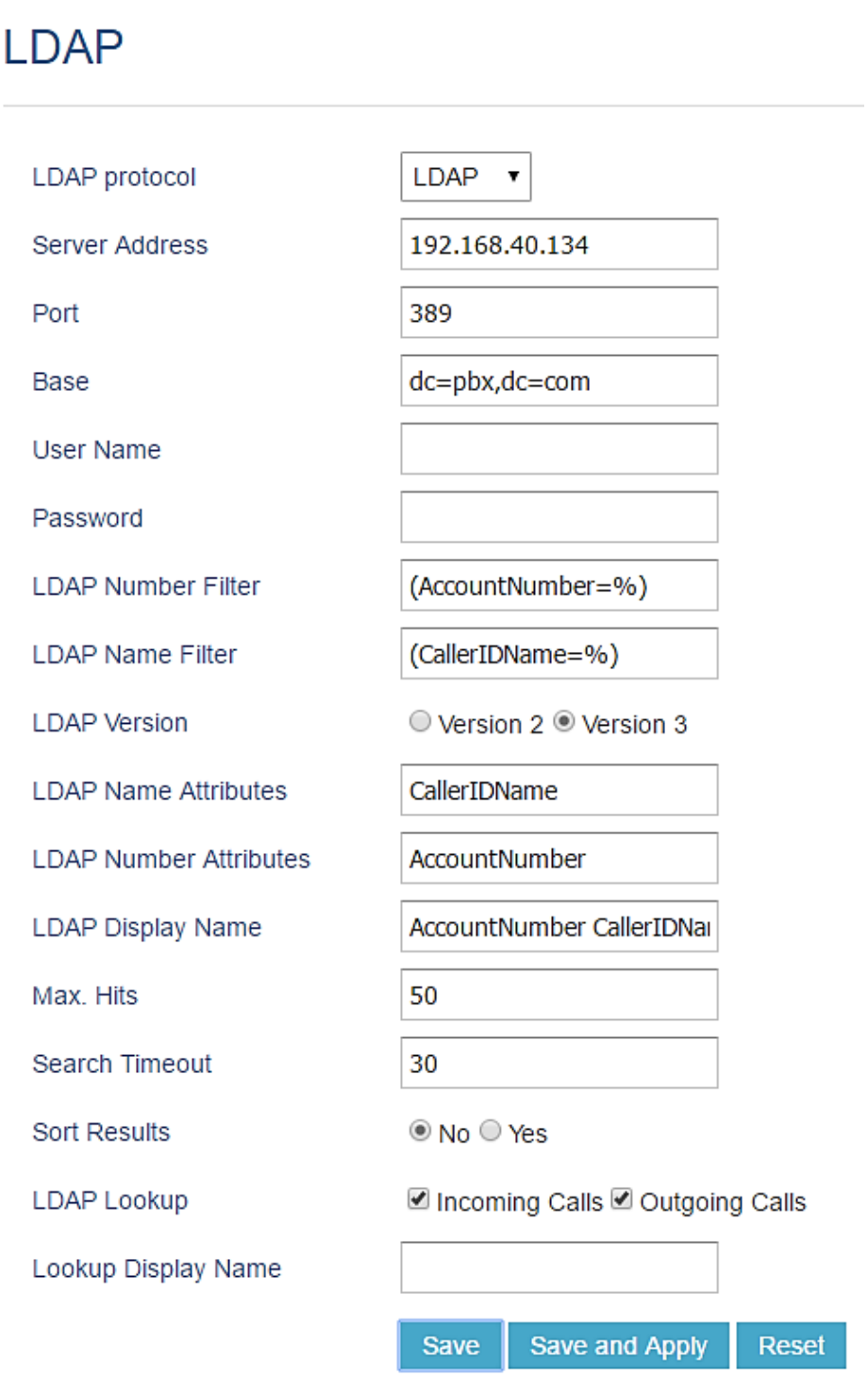


LDAP Client Configurations

To configure Grandstream IP phones as the LDAP clients for UCM, please refer to the following example:

- **Server Address:** The IP address or domain name of the UCM
- **Base DN:** dc=pbx,dc=com
- **Username:** cn=admin,dc=pbx,dc=com
- **Password:** admin (by default)
- **LDAP Name Attribute:** CallerIDName Email Department FirstName LastName
- **LDAP Number Attribute:** AccountNumber MobileNumber HomeNumber Fax
- **LDAP Number Filter:** (AccountNumber=%)
- **LDAP Name Filter:** (CallerIDName=%)
- **LDAP Display Name:** AccountNumber CallerIDName
- **LDAP Version:** If existed, please select LDAP Version 3
- **Port:** 389

The following figure shows the configuration information on a Grandstream GXP2170 to successfully use the LDAP server as configured in **[LDAP Server Configurations]**.



GXP2170 LDAP Phonebook Configuration

The UCM63xx LDAP server is no longer supporting the anonymous binding of the LDAP client.

AD Client Type

Phonebook Name	Enter a name for the phonebook
Server Address	The IP address of the AD server
Base DN	Enter the base domain name.
Username	Enter the username used to authenticate into the LDAP server, if authentication is required.
Password	Enter the password used to authenticate into the LDAP server, if authentication is required.

Filter	Enter the filter. Ex: (|(CallerIDName=%)(AccountNumber=%))
Port	Enter the port number. Default port is 389
AD Attributes	AccountNumber must be included if the default configuration is used.
Automatic Update Cycle	If "None" is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
Host Name	Enter the host name of the remote AD server.

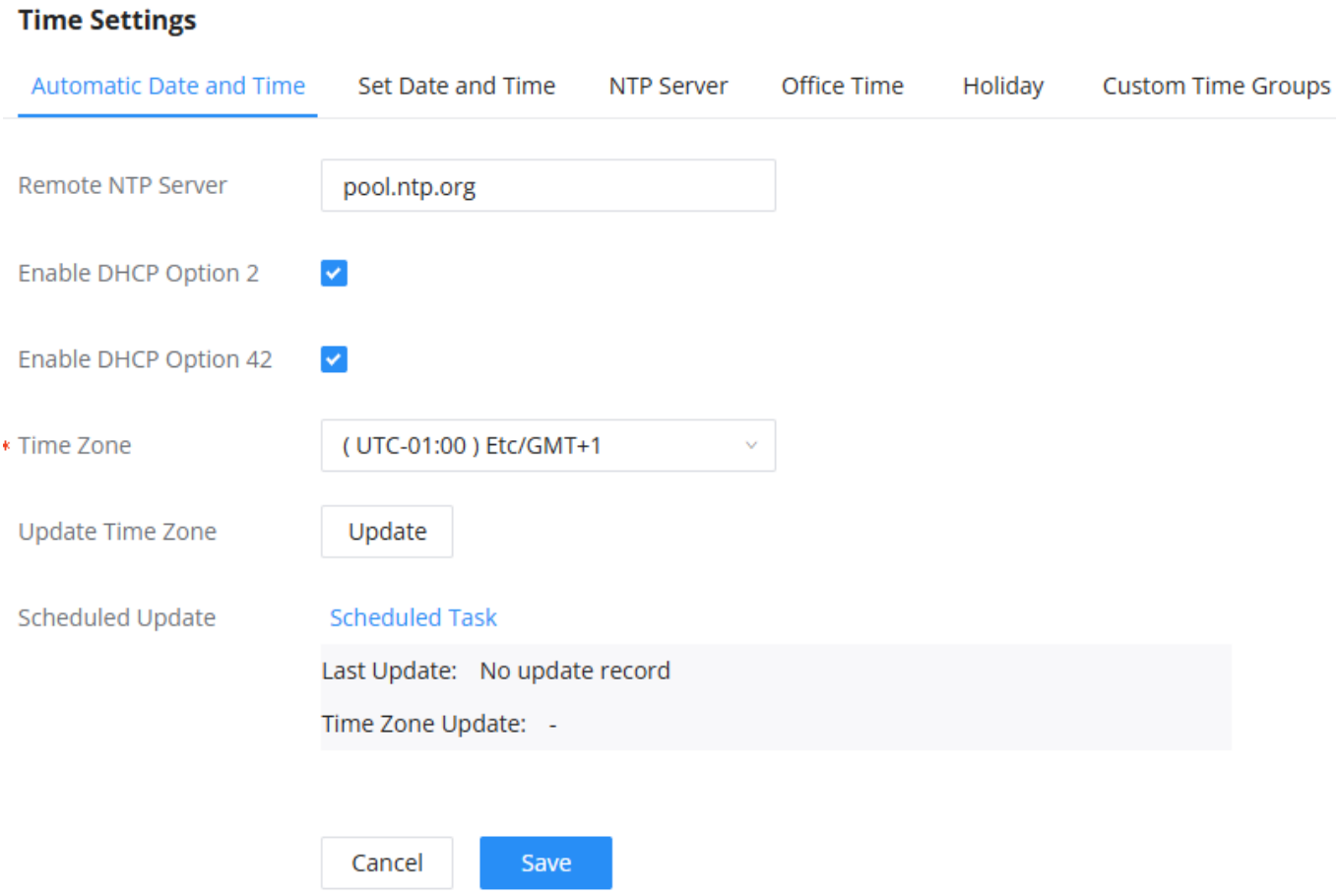
Time Settings

Automatic Date and Time

The current system time on the UCM630X can be found under Web GUI→**System Status→Dashboard→ PBX Status**.

To configure the UCM630X to update time automatically, go to Web GUI→**System Settings→Time Settings→Automatic date and Time**.

The configurations under Web GUI→**Settings→Time Settings→ Automatic date and Time** page require reboot to take effect. Please consider configuring auto time updating related changes when setting up the UCM630X for the first time to avoid service interrupt after installation and deployment in production.



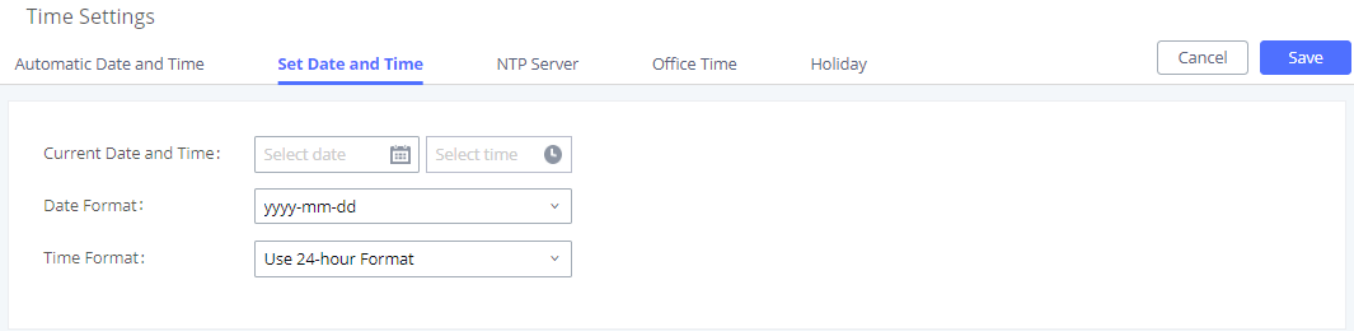
Automatic Date and Time Settings

Parameter	Description
Remote NTP Server	Configure the NTP server address to synchronize the time and date from.

Enable DHCP Option 2	If enabled, DHCP Option 2 will override the Time Zone setting on the PBX.
Enable DHCP Option 42	If enabled, DHCP Option 42 will override the NTP server configured on the PBX.
Time Zone	Choose the correct time zone according to your location.
Update Time Zone List	Clicking this button updates the list of timezones.
Scheduled Update	Configure schedule time zone update.

Set Date and Time

To manually set the time on the UCM630X, go to Web GUI→**System Settings→Time Settings→Set Date and Time**. The format is YYYY-MM-DD HH:MM:SS.



Time Auto Updating

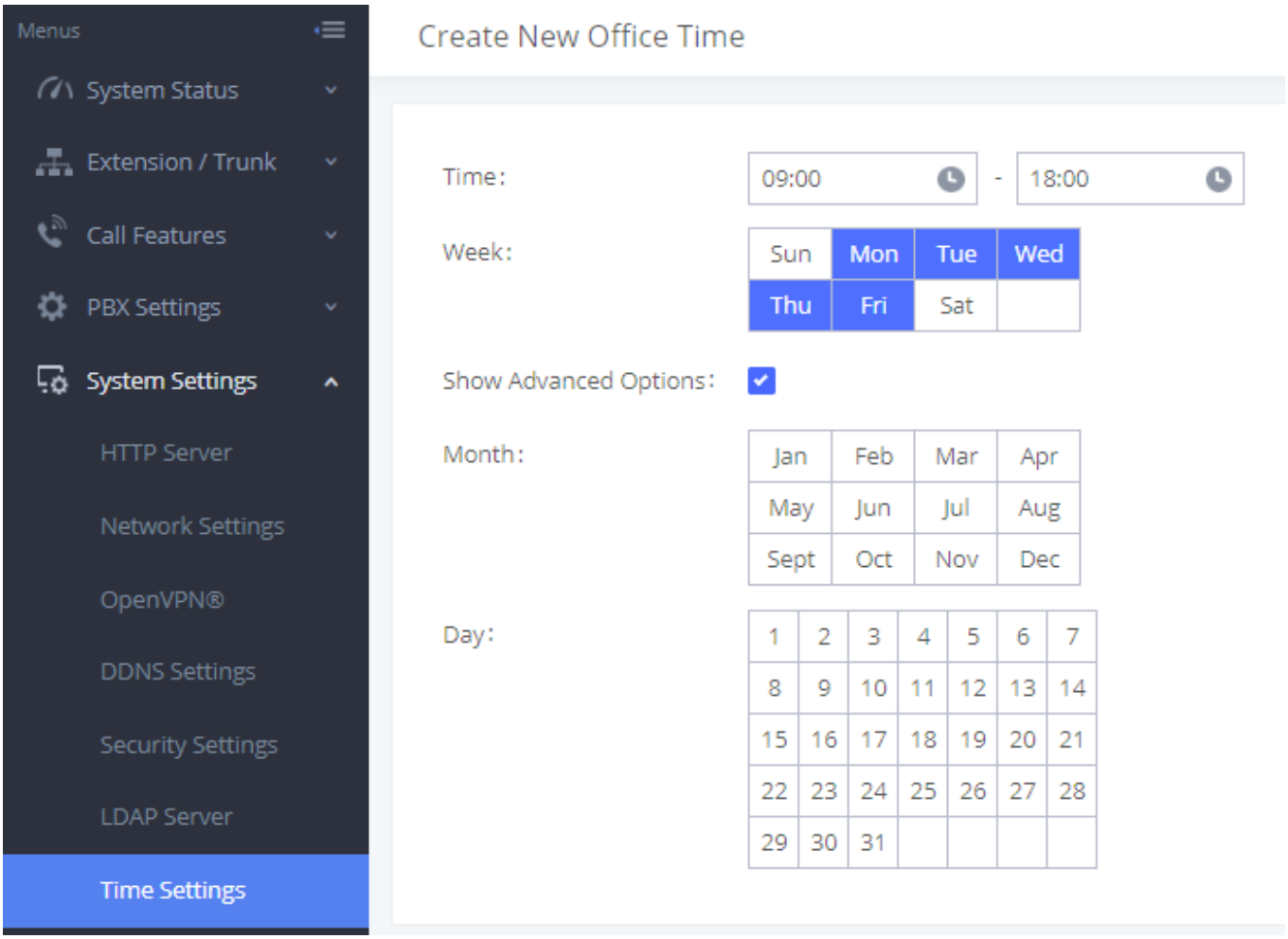
Note: Manually setup time will take effect immediately after saving and applying change in the Web GUI. If users would like to reboot the UCM630X and keep the manually setup time setting, please make sure "Remote NTP Server", "Enable DHCP Option 2" and "Enable DHCP Option 42" options under **Web GUI>Settings>Time Settings>Auto Time Updating** page are unchecked or set to empty. Otherwise, time auto updating settings in this page will take effect after reboot.

NTP Server

The UCM630X can be used as an NTP server for the NTP clients to synchronize their time with. To configure the UCM630X as the NTP server, set "Enable NTP server" to "Yes" under Web GUI **> System Settings > Time Settings > NTP Server**. On the client side, point the NTP server address to the UCM630X IP address or host name to use the UCM630X as the NTP server.

Office Time

On the UCM630x, the system administrator can define "office time" which can be used to configure time condition for extension call forwarding and inbound rules. To configure office time, log in to the Web GUI, enter the **System Settings > Time Settings > Office Time**, and click the "Add" button to see the following configuration page.

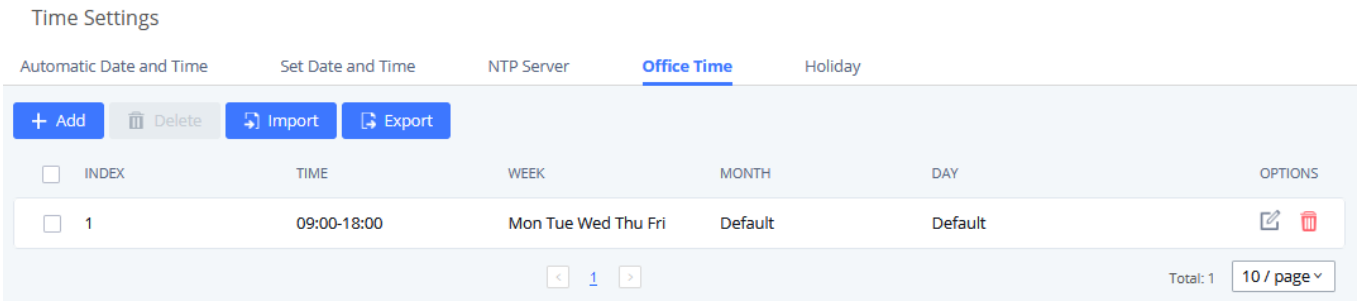


Create New Office Time

Start Time	Configure the start time for office hour.
End Time	Configure the end time for office hour
Week	Select the workdays in one week.
Show Advanced Options	Check this option to show advanced options. Once selected, please specify "Month" and "Day" below.
Month	Select the months for office time.
Day	Select the workdays in one month.

Create New Office Time

Select "Start Time", "End Time" and the day for the "Week" for the office time. The system administrator can also define month and day of the month as advanced options. Once done, click on "Save" and then "Apply Change" for the office time to take effect. The office time will be listed in the web page as the figure shows below.



Settings→Time Settings→Office Time

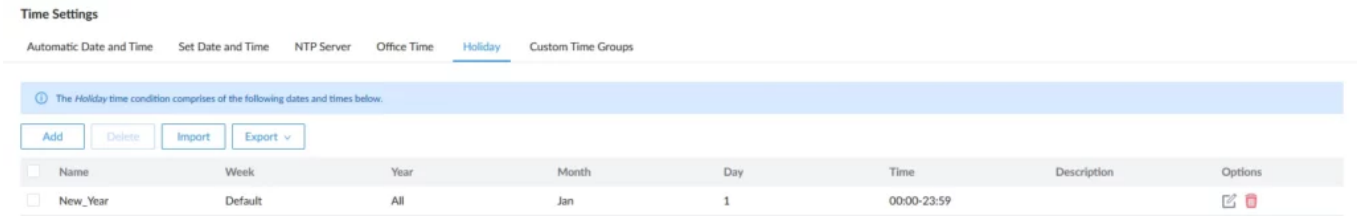
- Click on to edit the office time.
- Click on to delete the office time.
- Click on **"Delete"** to delete multiple selected office times at once.

Holiday

On the UCM, the system administrator can define Holidays, which can be used by Inbound Routes, Call Forwarding, and other time based features such as Paging/Intercom. To configure holidays, log in to the Web GUI and navigate to System **Settings->Time Settings->Holiday**.

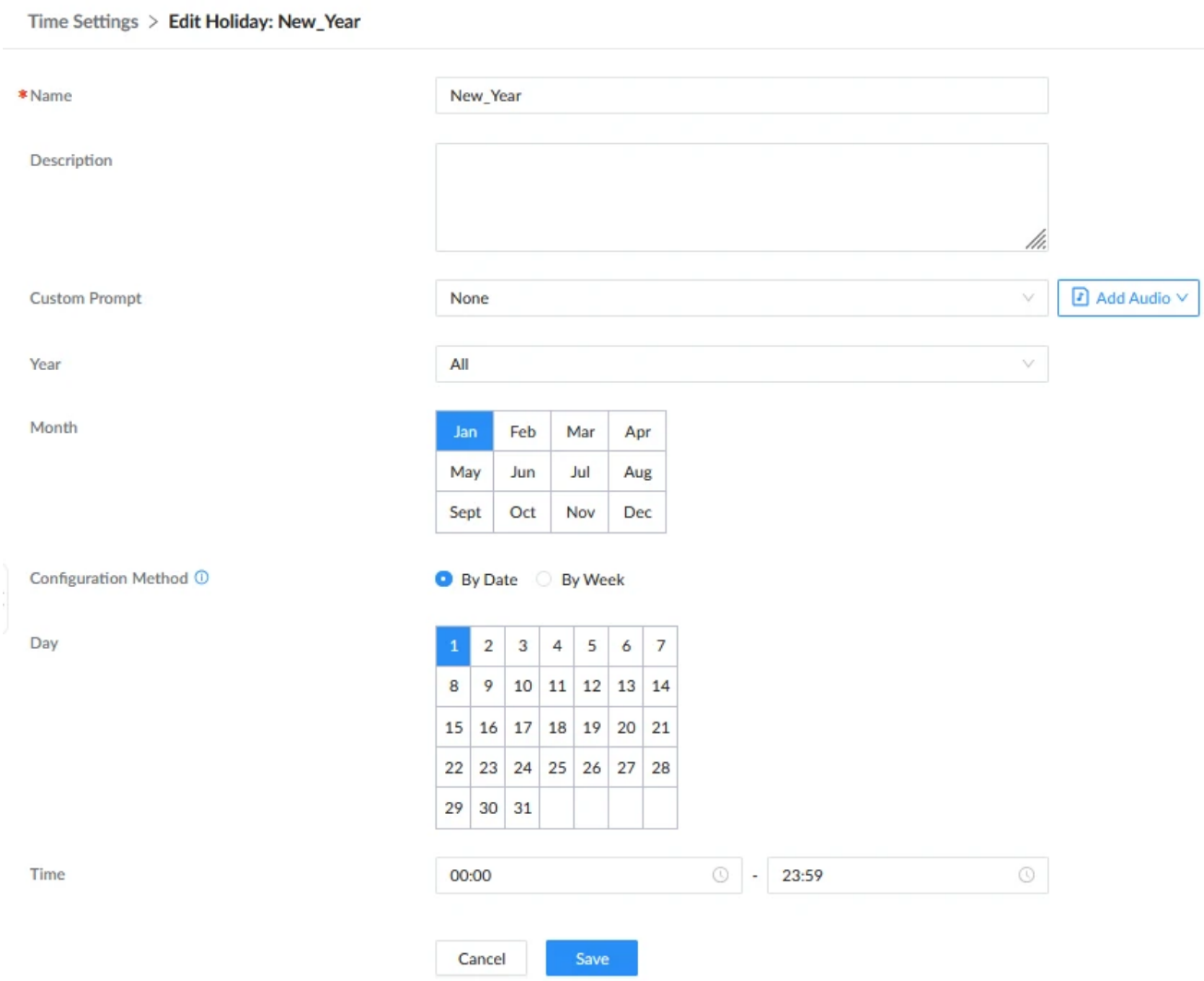
From this page, the administrator can:

- Configure **new** holidays using the "Add" button.
- **Edit** existing holidays by clicking the "Edit" icon for a specific holiday.
- **Delete a single** holiday by clicking the "Delete" icon.
- **Delete multiple** holidays at once by selecting them and clicking the "Delete" button.
- **Import** holiday configurations using the "Import" button.
- **Export** holiday configurations using the "Export" button.



Holiday Settings

When creating/editing a holiday, users can configure the parameters described in the table below:



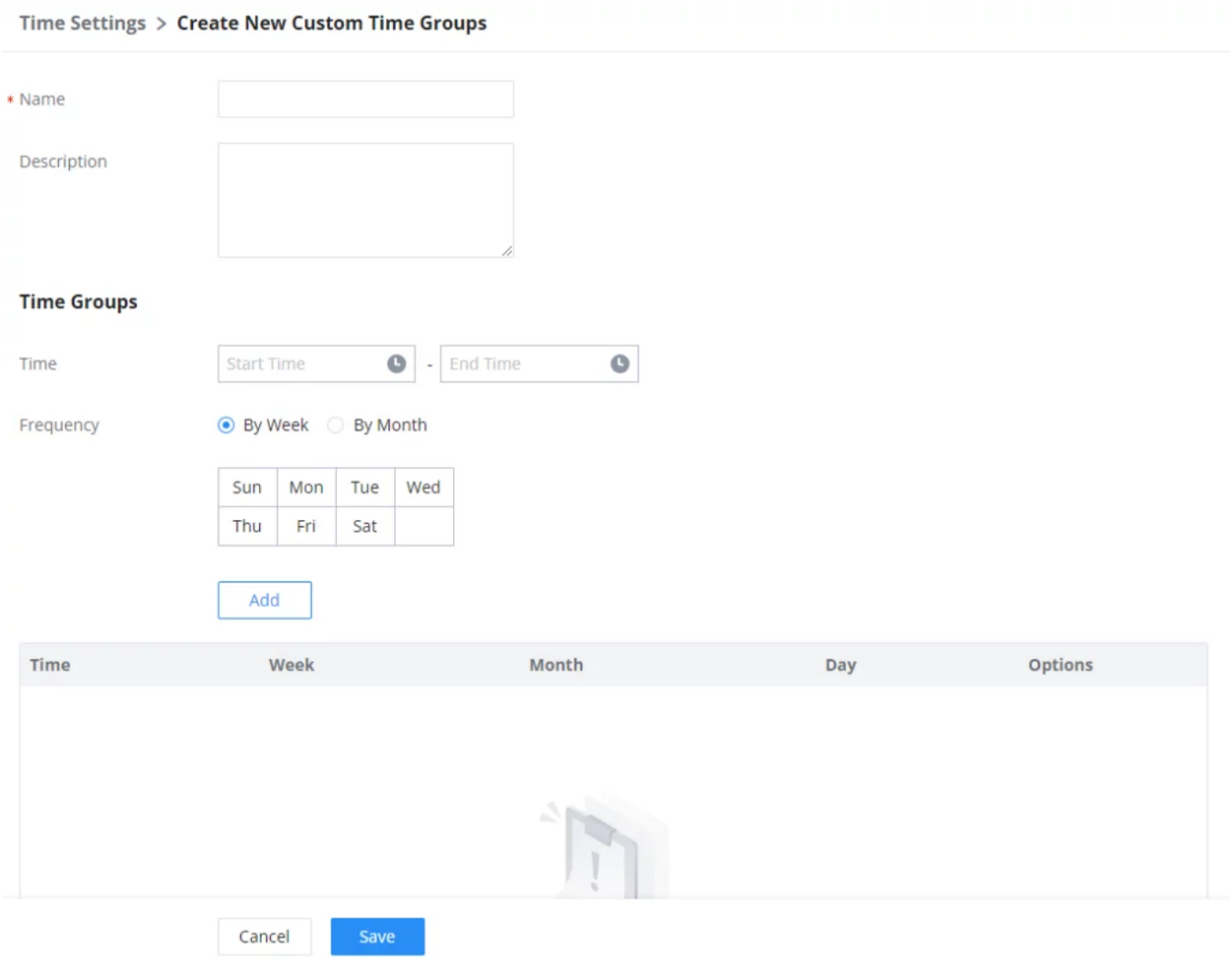
Parameter	Description
Name	Specifies the name of the holiday. Used to identify the holiday in related features.
Description	Optional description for the holiday.
Custom Prompt	Selects a custom voice prompt or generate a prompt using AI to play during the holiday period for inbound calls or time-based routing rules. Custom prompts can be managed under PBX Settings -> Voice Prompt -> Custom Prompt.
Year	Specifies the year in which the holiday applies. Select All to configure a recurring annual holiday.
Month	Select the month in which the holiday occurs.
Configuration Method	Defines how the holiday date is determined. The options are: By Date: Used for holidays with a fixed calendar date. By Week: Used for holidays defined by a weekday pattern within a month (for example, the fourth Thursday of a month).
Day	Displayed when Configuration Method is "By Date". Choose one or more calendar dates within the selected month to be treated as holidays.
Sequence	Displayed when Configuration Method is "By Week". Select the occurrence of the weekday within the month, such as First, Second, Third, Fourth, or Fifth.
Week	Displayed when Configuration Method is "By Week". Select the day of the week (Sunday through Saturday).

Time	Specifies the effective time range of the holiday. The holiday is active from the start time to the end time on the configured date(s).

Custom Time Groups

Users can create custom time frames which can be used as a routing condition in the inbound routes. Multiple time ranges can be added and the frequency can be customized to be every specific weekday or every specific day/week of the selected months.

To access Custom Time Groups, please navigate to **System Settings > Time Settings > Custom Time Groups**



Custom Time Groups

Parameter	Description
Name	Enter the name of the time group.
Description	Enter the description of the time group.
Time Groups	
Time	Select the time period for this group.
Frequency	Select the frequency of this group per week/month.

Email Settings

The Email application on the UCM630X can be used to send out alert event emails, voicemail notifications

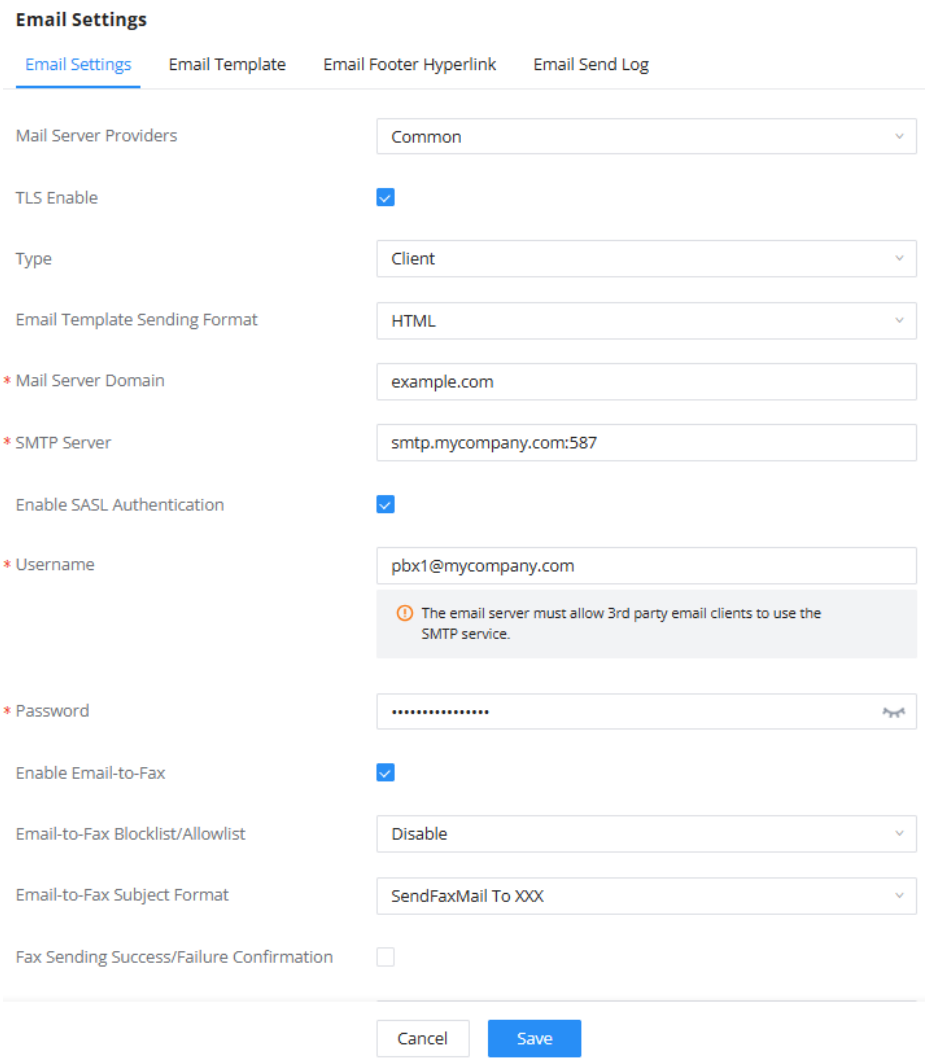
(Voicemail-to-Email), fax delivery reports, and system notifications. The configuration parameters can be accessed via Web GUI -> **System Settings -> Email Settings -> Email Settings**.

Parameter	Description
Mail Server Providers	Select the mail server provider type: Common: Select this option when integrating email services such as Gmail or on-premise email servers. Microsoft: Select this option when integrating email services provided by Microsoft Outlook. Note: The settings below appear when selecting "Common".
TLS Enable	If enabled, TLS will be used when forwarding emails to the SMTP server.
Type	Select the mail processing type: MTA: Mail Transfer Agent. The configured domain will be used in the sender address. Warning: Emails sent by MTA may be considered spam by the destination SMTP server. Client: Send emails to the configured SMTP server, which will then forward the emails to the destination address.
Email Template Sending Format	Select the email template format to be sent. The "HTML" format is compatible with most mail clients and is recommended. If the mail client does not support HTML, select "Plain Text".
Mail Server Domain	Enter the domain name of the mail server (e.g., grandstream.com).
SMTP Server	Enter the SMTP server address (e.g., smtp.gmail.com:587). Port number is optional.
Enable SASL Authentication	Toggles SASL authentication. If disabled, the IPPBX will not use username and password for email client authentication. Most email servers require login authentication. If using Microsoft Exchange Server or if credentials are not required, disable this option.
Username	Enter the username of the email account.
Password	Enter the password of the email account. It is highly recommended to use HTTPS when saving and applying password changes.
Enable Email-to-Fax	Monitors the inbox of the configured email address for the specified subject. If detected, the IPPBX retrieves the attachment and sends it to the target extension by fax. The attachment must be in PDF/TIF/TIFF format.
Email-to-Fax Blocklist/Allowlist	Enable or disable the Email-to-Fax Blacklist or Whitelist.
Email-to-Fax Subject Format	Select the email subject format to use for email-to-fax. XXX refers to the target extension that the fax will be sent to.
Notify Sender of Result	If enabled, the UCM will send an email notification back to the sender containing the fax transmission result.
Notify Admin of Fax Failure	Configures a unified administrator email address. When enabled, the UCM automatically sends an email notification to this specified address whenever an Email-to-Fax transmission fails.
Internal Block/Allowlist	Email address blacklist/whitelist for local extensions. Displayed when Email-to-Fax Blocklist/Allowlist is enabled.
External Block/Allowlist	Email address blacklist/whitelist for non-local contacts. Separate multiple addresses with semicolons (;). Displayed when Email-to-Fax Blocklist/Allowlist is enabled.
POP/POP3 Server Address	Enter the IP address or domain of the POP/POP3 server.
POP/POP3 Server Port	Enter the port number of the POP/POP3 server.
Display Name	Enter the name of the PBX that will be displayed in sent emails.
Sender	Enter the email address used to send out emails from the PBX.
Email Settings (Test)	Click Test to verify if the email integration is functioning correctly. Note: Save and apply changes before running the email test.

For a step-by-step configuration of Microsoft Outlook email services, please refer to the following guide:

https://documentation.grandstream.com/knowledge-base/grandstream-ippbx-microsoft-outlook-authentication-guide/

The following figure shows a sample Email setting on the UCM630X, assuming the Email is using 192.168.6.202 as the SMTP server.



UCM630X Email Settings

Once the configuration is finished, click on **Test**. In the prompt, fill in a valid email address to send a test email to verify the Email settings on the UCM630X.

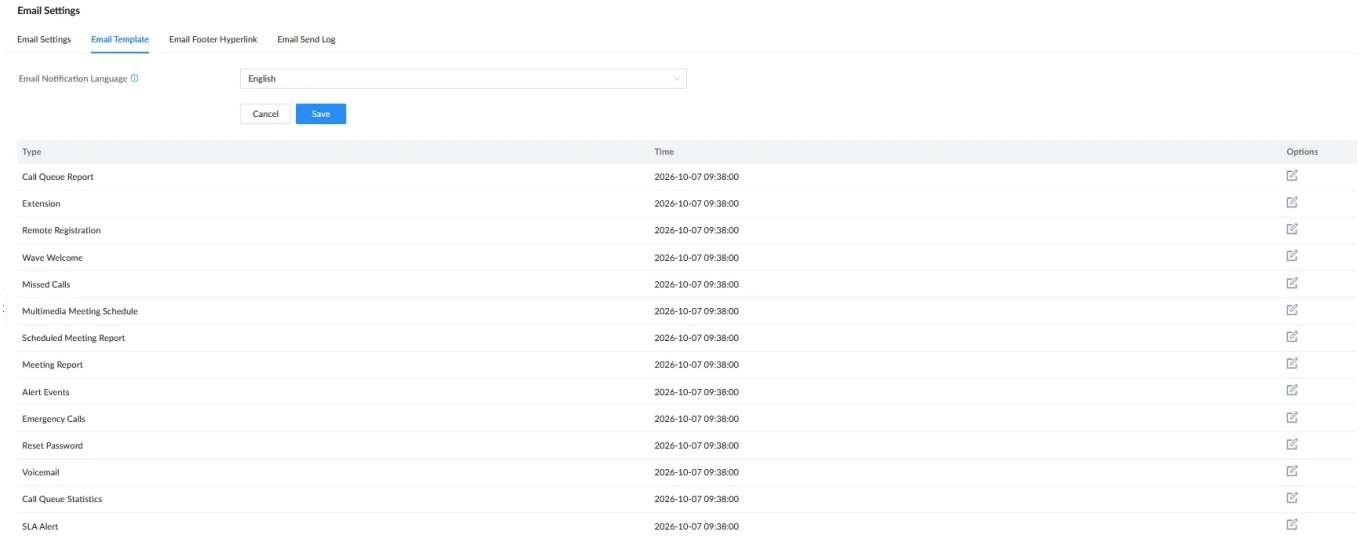
Email Template

The Email templates on the UCM630X can be used for email notification, the configuration parameters can be accessed via Web GUI->**System Settings**->**Email Settings**->**Email Templates**.

On this page, users can customize email templates for password reset, voicemail, meeting scheduling, extensions, fax, meeting report, PMS, CDR, emergency call, missed calls, alert events, call queue statistics and etc.

- Select the preferred email template language (this only applies to the default template).
- Click on the "Edit" icon to edit the template.

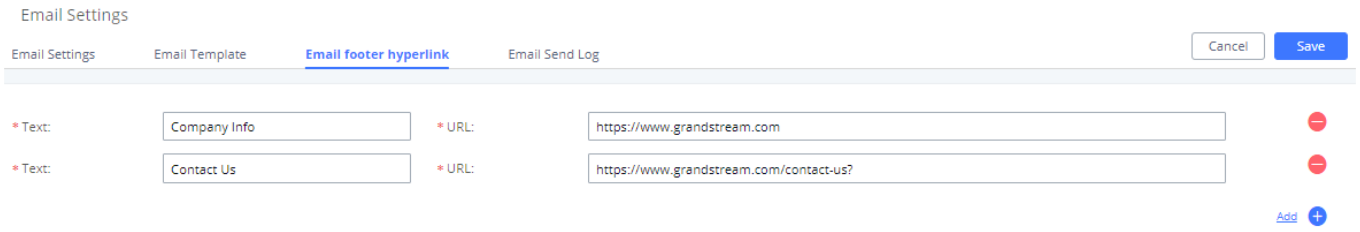
For more detailed information about each template variable and Email configuration, please refer to the Email Templates Guide.



Email Template

Email Footer Hyperlink

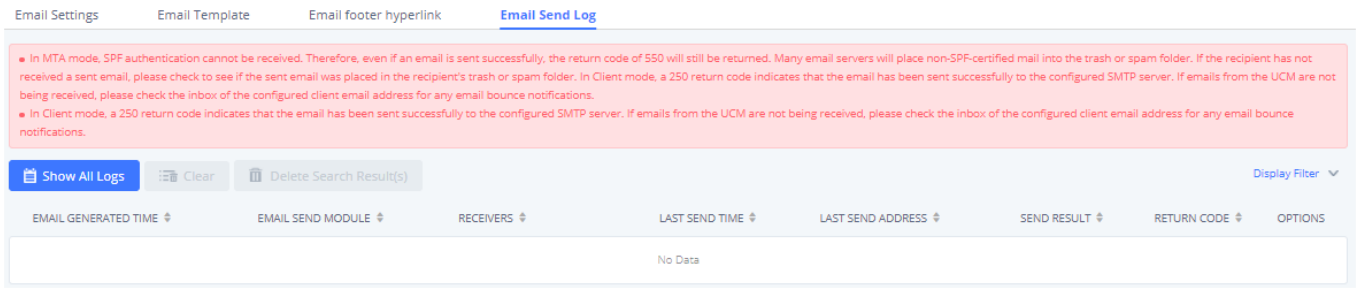
Under UCM Web GUI→**System Settings→Email Settings→Email Footer Hyperlink**, users could edit the text and URL to modify the email footer hyperlink.



Email Footer Hyperlink

Email Send Log

Under UCM Web GUI→**System Settings→Email Settings→Email Send Log**, users could search, filter, and check whether the Email is sent out successfully or not. This page will also display the corresponding error message if the Email is not sent out successfully.



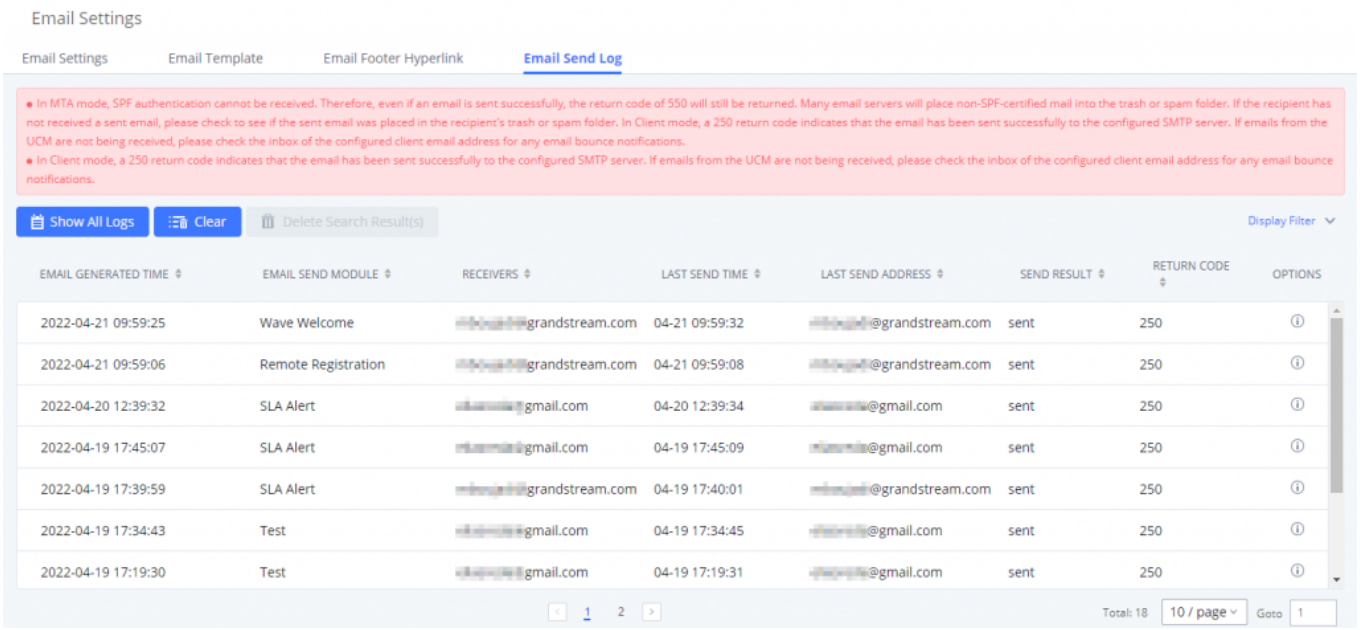
Email Send Log

Start Time	Enter the start time for the filter
End Time	Enter the end time for the filter
Receivers	Enter the email recipient, while searching for multiple recipients, please separate them with a comma and no spaces.
Send Result	Enter the status of the send result to filter with
Return Code	Enter the email code to filter with

Email Send Module	Select the email module to filter with from the drop-down list, which contains: All Modules Extension Voicemail Conference Schedule User Password Alert Events CDR Test

Email Log - Display Filter

Email logs will be shown at bottom of the "Email Send Log" page, as shown in the following figure.



Email Logs

Below are the codes returned when sending emails and their description:

Email Codes:

Code	Description
250	Mail sent successfully
501	Address format parsing error, 501 will be returned when there are unacceptable characters in the recipient's email address in MTA mode. Please check if the recipient's email address format is correct. The "sender" configured on the client is your mail account.
535	The username and password verification in the client mode is incorrect. Please check whether the username and password are configured correctly.
550	Possible reasons: The recipient's mailbox username does not exist or is in a banned state, please check whether the email recipient is the correct email address. The number of destination addresses sent by the sender exceeds the maximum limit per day and is temporarily blacklisted. Please reduce the sending frequency or try again the next day. The sender's IP does not pass the SPF permission test of the sending domain. Emails sent in MTA mode may return this error code even if they are sent.
552	The sent email is too large or the email attachment type is prohibited
553	The sender and the email account are inconsistent, please configure the sender as your email account correctly.
554	The email was identified as spam. Please reduce the sending frequency or try again the next day

none	This indicates that there is no return code.If the sending result is "deferred", the general reason is that the mail service area is configured incorrectly. Please check whether the server configuration is correct.If the sending result is "bounced", the general reason is that the receiving email address domain name is wrong, please check whether the email recipient is the correct email address. If it is in MTA mode, please check whether the "domain" is configured to be in the same domain name as the "recipient".

HA

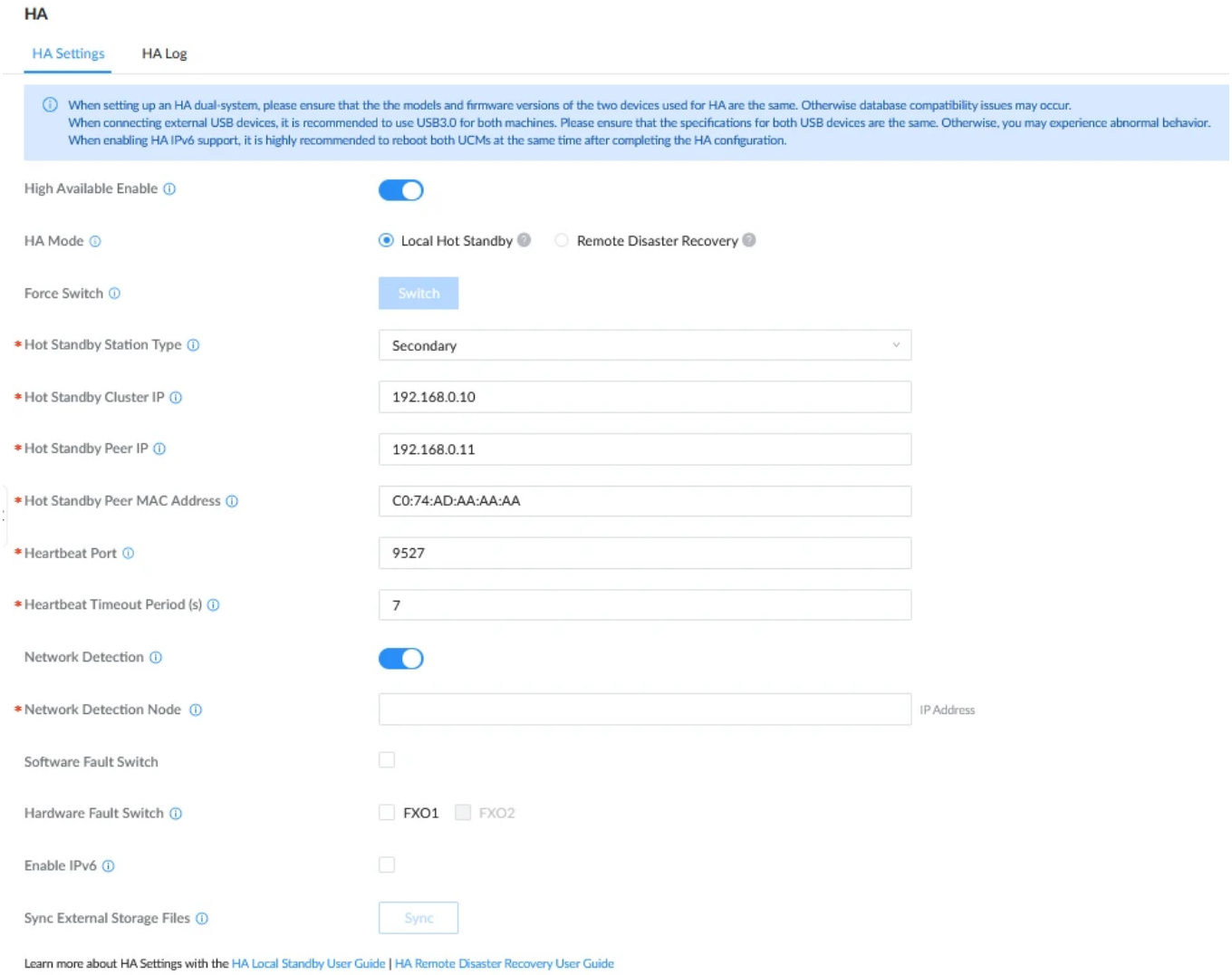
Dual-system hot standby provides a highly reliable and fault-tolerant solution for enterprises using the UCM6300 series/UCM6300A series. Based on two UCM devices of the same product model and software version, one of them is in the "Active" working state in real-time, and the other is in the "Standby" working state. The daily data on the host server will be synchronized to the standby machine in real-time, and the standby machine always monitors the running status of the host. When the host fails, including hardware failures and severe software failures, the standby machine will immediately take over the business and enter the "Active" working state, and Upgrade to a host to ensure that the business is not interrupted, and the call will automatically resume.

The HA function provides two modes of operating. The first mode of function is **Local Hot Standby,** which offers a deployment that switches dynamically when the primary UCM encounters an issue. The second mode is **Remote Disaster Recover,** it offers deploying a back up UCM remotely, this offers an architecture that would not be affected by any disaster that might occur on the geolocation of the primary UCM.

In order to set HA, both UCMs should have static IP addresses.

HA Settings

The users can configure the HA under **System Settings->HA settings** page.



Local Hot Standby Settings

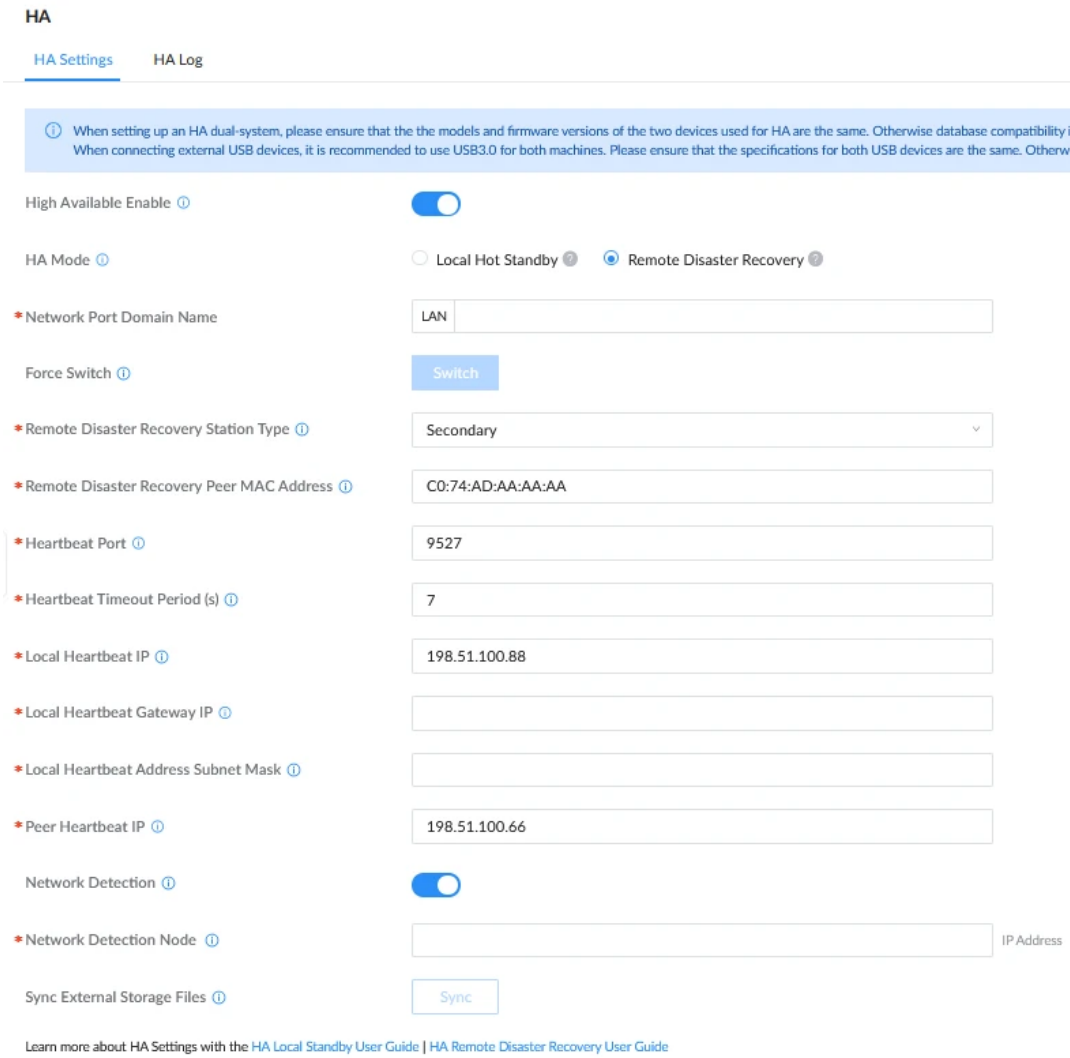
This table describes parameters used when configuring local HA between two UCM systems within the same site.

Parameter	Description
High Available Enable	Enables/disables the HA functionality. By default, it's disabled.
Force Switch	Clicking the button will immediately force a switchover to the standby UCM.
Hot Standby Station Type	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the intial active device. If set to Secondary, the peer UCM system will be assigned as the initial standby device. The roles of the UCM systems may change as HA switchovers occur.
Hot Standby Cluster IP	Used in single-NIC mode. This is the shared virtual IP address used by both active and standby UCMs. The IP must be static and must not match the local IP of either device.
Hot Standby Cluster IP 1	Displayed in Dual-NIC mode. Cluster virtual IP used for the LAN1 subnet. Mandatory. Must not match the local LAN1 IP and must be unique.
Hot Standby Cluster IP 2	Displayed in Dual-NIC mode. Cluster virtual IP used for the LAN2 subnet. Mandatory. Must not match the local LAN2 IP and must be unique.
Hot Standby Peer IP	Local IP address of Hot Standby peer device.
Hot Standby Peer MAC Address	The MAC address of Hot Standby peer device.

Heartbeat Port	The number of the heartbeat port should be consistent with the peer heartbeat port.
Heartbeat Timeout Period (s)	Upon timeout, the Standby UCM will take over services.
Network Detection	Enable/Disable Network Detection feature. When enabled, the active device continuously checks reachability to the configured detection node(s). If the active device loses connectivity to any configured detection node a switchover is triggered and the standby device assumes the active role. Note: HA settings on both the active and standby UCM must be consistent. In case of inconsistency, the settings on the active device will be prioritized.
Network Detection Node	Displayed in Switch and Route mode. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on active and standby devices.
Network Detection Node 1	Displayed in Dual mode. This detection node associated with Cluster IP1 / LAN1. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 2	Displayed in Dual mode. Detection node associated with Cluster IP2 / LAN2. If configured, loss of connectivity to this node on the active device will also trigger a switchover. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Software Fault Switch	Enable Software Fault Switch.
Hardware Fault Switch	If issues are detected with the selected connection interfaces, the backup UCM will take over services after the master/slave handover. If not checked, UCM will send only a fault alarm.
Enable IPv6	If enabled, HA on UCM can be used with IPv6 while compatible with IPv4.
Scan External Storage Files	Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page. It is recommended to configure external storage data synchronization when forming HA for the first time, If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.

Local Hot Standby

The table below describes parameters used for Remote Disaster Recovery HA, where two UCM systems are deployed at different sites.



Remote Disaster Recovery Settings

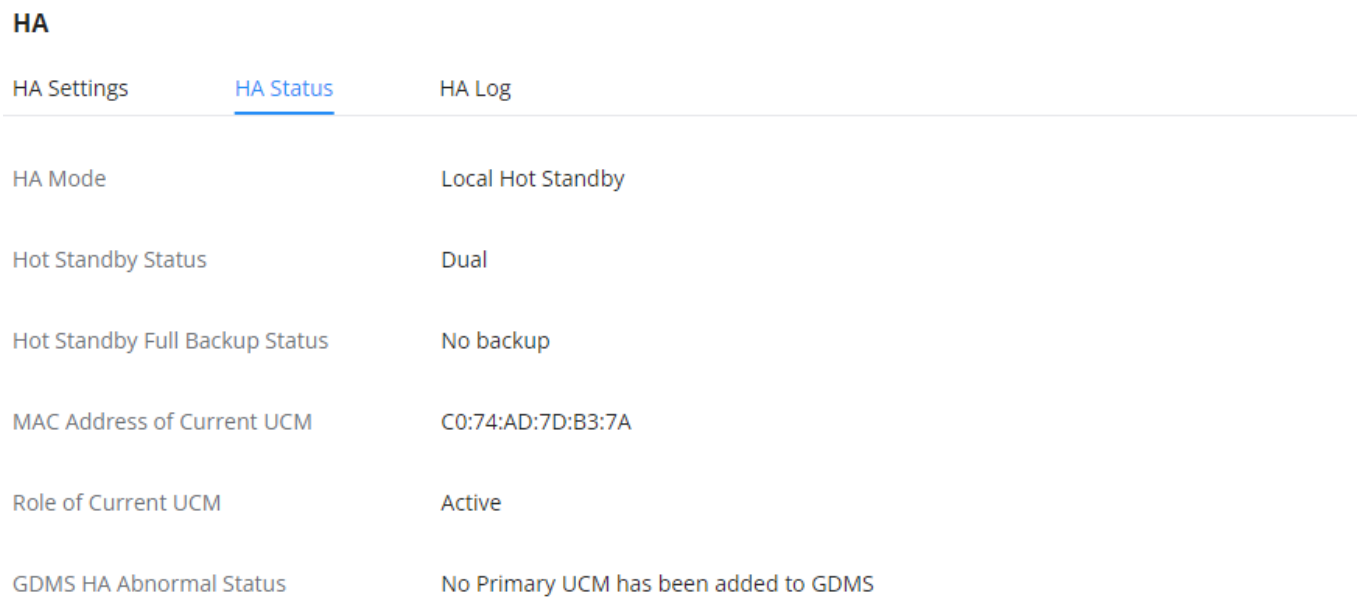
Parameter	Description
Network Port Domain Name	Selects the network domain used for remote disaster recovery. In single NIC mode, available options are WAN and LAN. In dual NIC mode, available options are LAN1 and LAN2, corresponding to the two physical LAN interfaces.
Force Switch	Clicking the button will immediately force a switchover to the standby UCM.
Remote Disaster Recovery Station Type	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the intial active device. If set to Secondary, the peer UCM system will be assigned as the initial standby device. The roles of the UCM systems may change as HA switchovers occur.
Remote Disaster Recovery Peer MAC Address	The MAC address of Remote Disaster Recovery peer device
Heartbeat Port	The heartbeat port should be the same as the peer device's heartbeat port.
Heartbeat Timeout Period (s)	Upon timeout, the Standby UCM will take over services.
Local Heartbeat IP	Fill in the IP address of the heartbeat port of the local site, in the format: xxx.xxx.xxx.xxx, which is used for the peer end to detect the local machine status, heartbeat negotiation, and communication address for data synchronization.
Local Heartbeat Gateway IP	Fill in the IP address of the local heartbeat gateway for remote disaster recovery, in the format: xxx.xxx.xxx.xxx

Local Heartbeat Address Subnet Mask	Fill in the subnet mask of the heartbeat address of the remote disaster recovery local end, in the format: xxx.xxx.xxx.xxx, such as: 255.255.255.0.
Peer Heartbeat IP	Fill in the IP address of the heartbeat port of the peer site, in the format: xxx.xxx.xxx.xxx, which is used to detect peer status, heartbeat negotiation, and communication address for data synchronization.
Network Detection	Enable/Disable Network Detection feature. When enabled, the active device continuously checks reachability to the configured detection node(s). If the active device loses connectivity to any configured detection node a switchover is triggered and the standby device assumes the active role.Note: HA settings on both the active and standby UCM must be consistent. In case of inconsistency, the settings on the active device will be prioritized.
Network Detection Node	Displayed in Switch and Route mode. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 1	Displayed in Dual mode. This detection node associated with Cluster IP1 / LAN1. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 2	Displayed in Dual mode. Detection node associated with Cluster IP2 / LAN2. If configured, loss of connectivity to this node on the active device will also trigger a switchover. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Scan External Storage Files	Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page.It is recommended to configure external storage data synchronization when forming HA for the first time, If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.

Remote Disaster Recovery

HA Status

Once the HA is configured, the user can view its status under **System Settings → HA → HA Status** as shown below



HA Status

HA Log

The user can view the HA log through the **system settings → HA → HA log** page. The HA log effectively records the execution results of past full backup actions, as well as the history records that triggered the active/standby switchover.

The UCM63xx series suppots SNMP to be able to use 3rd party monitoring tools to monitor both UCMs in HA setup.

Cluster

Clustering allows the user to deploy many units in the same environment to handle telephony features collectively. This allows the user to enact a system that is capable with a higher processing bandwidth that many calls require. By clustering multiple UCM devices, the system will be able to offer more concurrent calls and meeting participants.

- Cluster feature is supported only on the UCM6304 and UCM6308
- The user can deploy a maximum of 5 media servers.
- Each cluster deployment requires at least one business server and one media server.

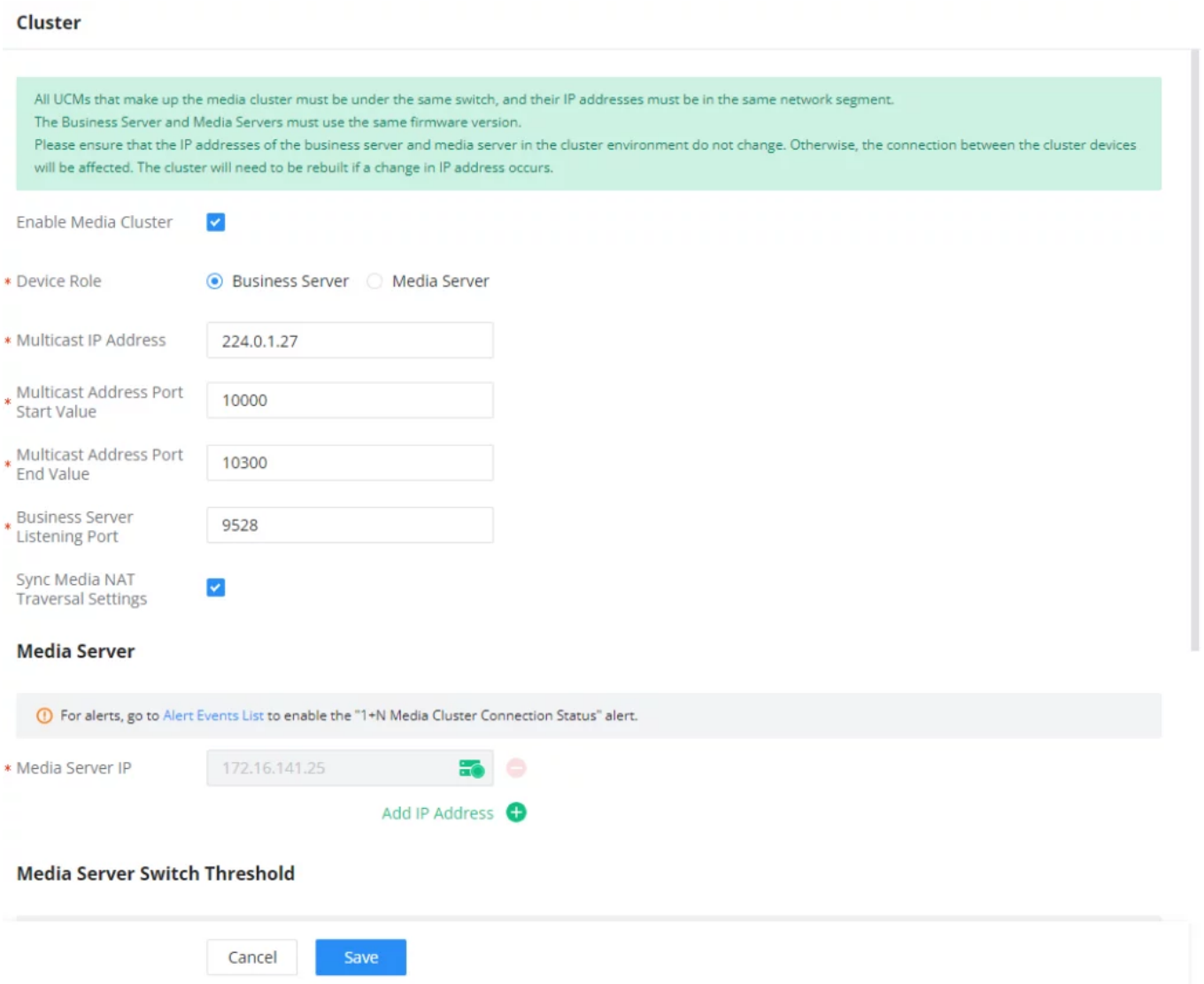
To configure the cluster, we will need two types of servers; a Business server, which is a one and only server that will be used for the administration of the operations. And a media server, which can either be one singular server, or for deployments that require more resource, the user can deploy up to 5 UCM units as media server. Media server will handle media related traffic.

- All the UCM units that form the media cluster must be under the same switch, and their IP addresses must be in the same network segment.
- The Business server and the Media servers must use the same firmware version.

- Please ensure that IP addresses reservation is created for the business server and the media server(s) in the DHCP server to ensure that the servers will use the same IP addresses to communicate. In the case the IP addresses have been changed, the cluster needs to be rebuilt.

Business Server

To configure Business server, please access the UCM web UI then navigate to **System Settings > Cluster**, then tick the option "Enable Media Cluster", and choose "Business Server" as the **Device Role.**

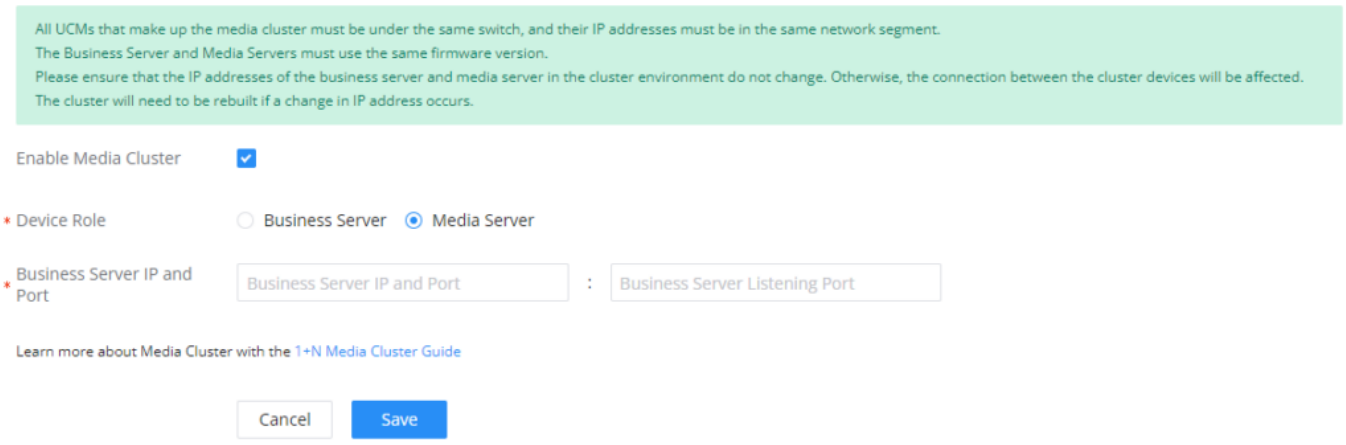


Parameter	Description
Enable Media Cluster	Enable Media Cluster feature.
Device Role	Configure the device role. Business Server: Choosing this role will make the UCM as the main server for operations. Media Server: Choosing this role will make the UCM as a media server only. All the PBX related features will be disabled.
Multicast Network Port	Choose the network port which will be used for the multicast.
Multicast IP Address	The allowed multicast IP address range is 224.0.1.0 - 238.255.255.255
Multicast Address Port Start Value	Enter the multicast address port start value. The port number value can be within the range 1024 - 65535. Note: The multicast address port start value must be lower or equal to the multicast address port end value.

Multicast Address Port End Value	Enter the multicast address port end value. The port number value can be within the range 1024 - 65535.Note: The multicast address port end value must be greater or equal to the multicast address port start value.
Business Server Listening Port	The port on which the business server listens and receives information reported by the media server. The value of the listening port value can be within 1024 - 65535.
Sync Media NAT Traversal Settings	If enabled, all media servers in the cluster will use the same Media NAT Traversal settings as the business server. If disabled, each server will need to be configured individually.
Media Server IP	Enter the IP address of the media server. The user can pair up to 5 media servers with one Business server. The statuses of the media servers are indicated using three colors:? Green: The server is available. Yellow: The server is in use. Gray: The server is offline.
Memory Usage Threshold (%)	When the memory usage of this media server is exceeded, media services will be assumed by another media server in the cluster with the lowest usage at the time.
CPU Usage Call Control Threshold (%)	When the CPU usage of this media server is exceeded, media services will be asssumed by another media server in the cluster with the lowest usage at the time.
Memory Usage Threshold (%)	When this server's memory usage exceeds the specified threshold, service from this server will be temporarily paused.
CPU Usage Call Control Threshold (%)	When this server's CPU usage exceeds the specified threshold, service from this server will be temporarily paused.
Disk Available Space (MB)	When the percentage of available space in the device's disk data partition falls below the set value, this server will not be used until the amount of available space is above the threshold again.

Media Server

To configure Media server, please access the web UI then navigate to **System Settings > Cluster,** then tick "Enable Media Cluster".



Enable Media Cluster	Enable Media Cluster feature.
Device Role	Configure the device role.
Business Server IP and Port	Enter the IP address of the business server with the listening port. If the business server is using HA Local Hot Standby, the Hot Standby Cluster IP address must be used. If the business server is using HA Remote Disaster Recovery, the primary UCM and secondary UCM must have their own respective cluster environments.

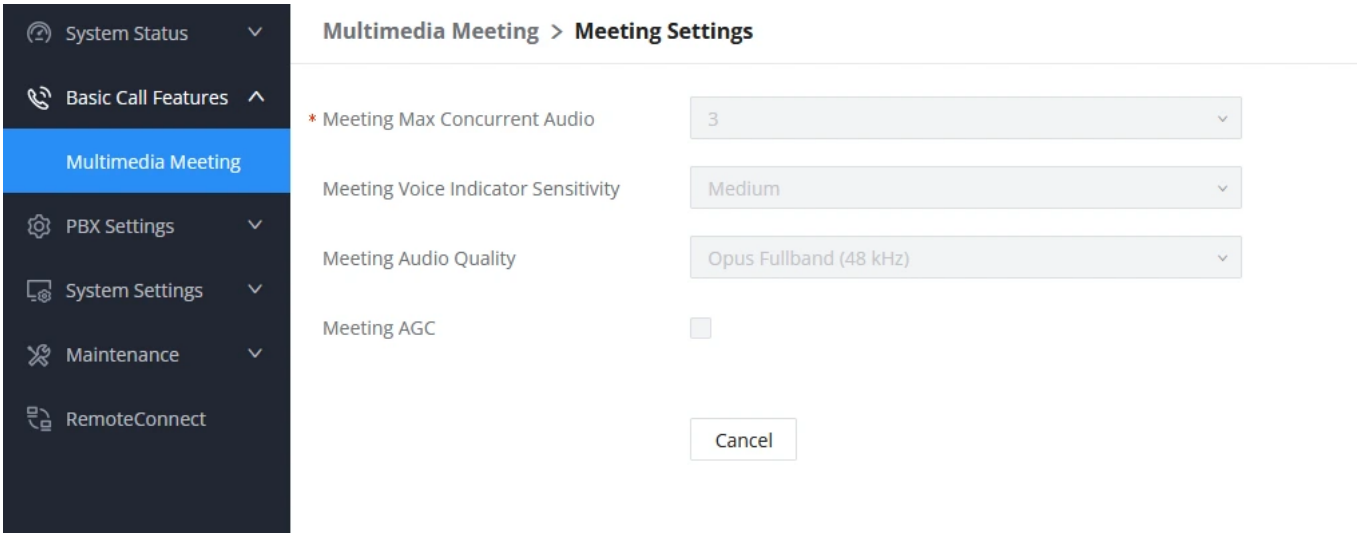
For step-by-step configuration of the 1+N clustering feature, please refer to the following guide: https://documentation.grandstream.com/knowledge-base/ucm630x-1n-media-cluster-guide/

1+N Media Cluster Synchronization

In order to avoid inconsistencies between the configurations of the media server and the business server in a cluster, the following configuration parameters can be synchronized:

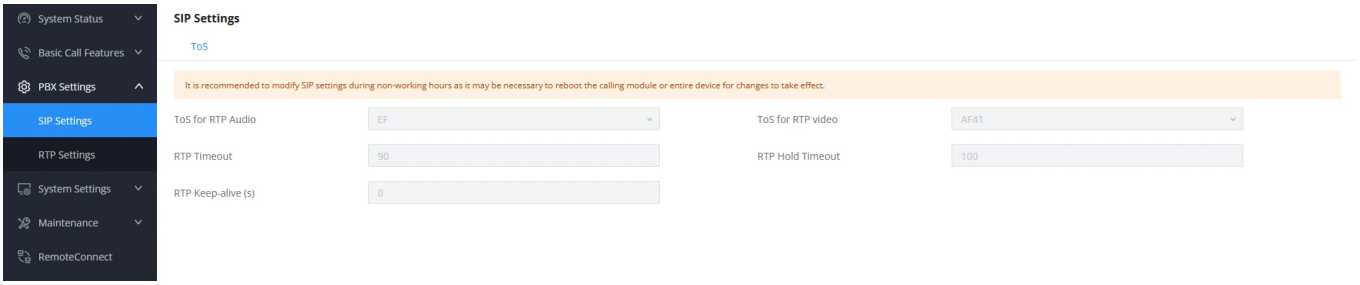
- **Basic Call Features -> Multimedia Meeting**

For media servers, all the configuration options on this page are greyed out to display the information configured on the business server.



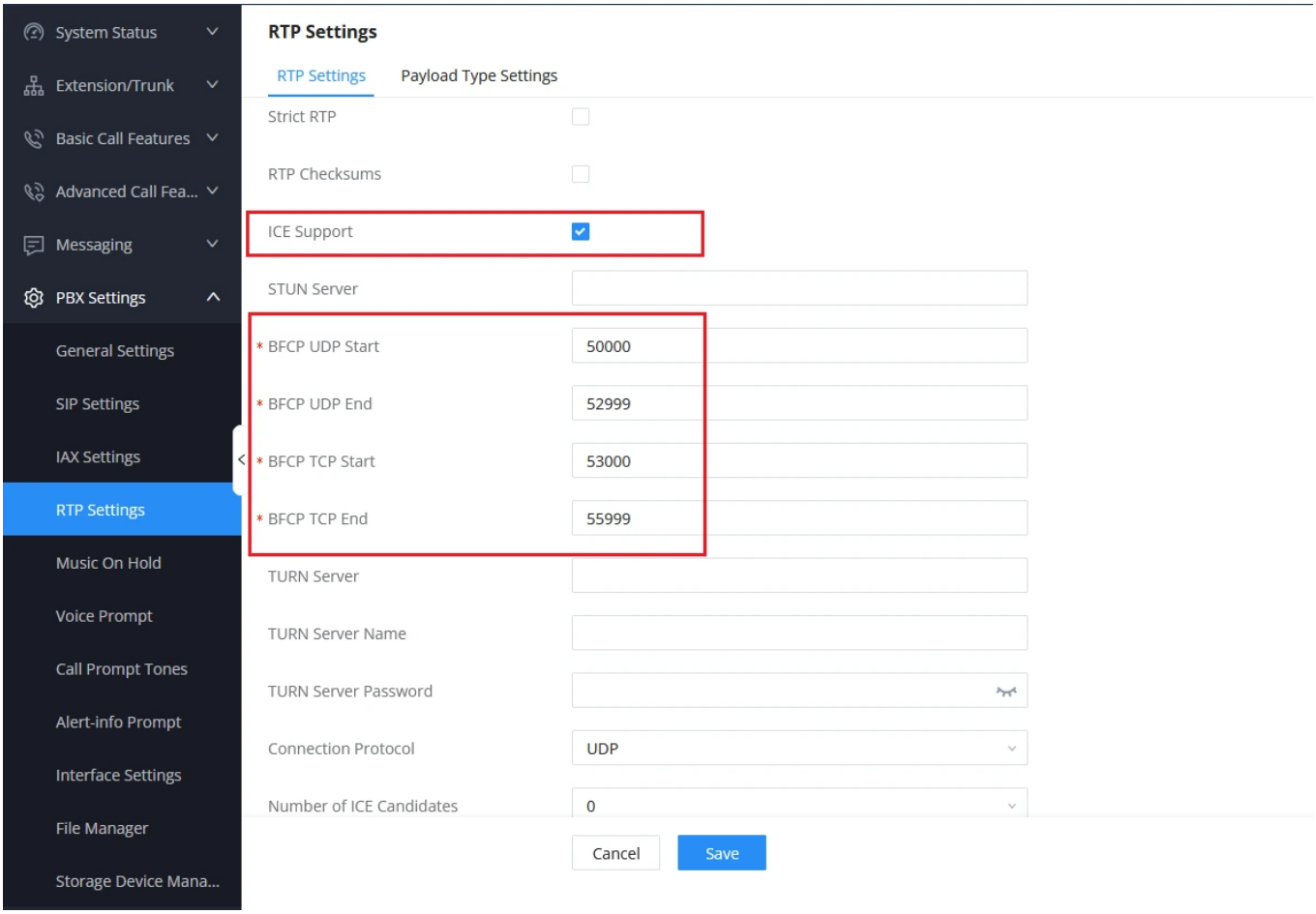
- **PBX Settings -> SIP Settings -> ToS**

This page for media servers shows the RTP related configurations of the business server.

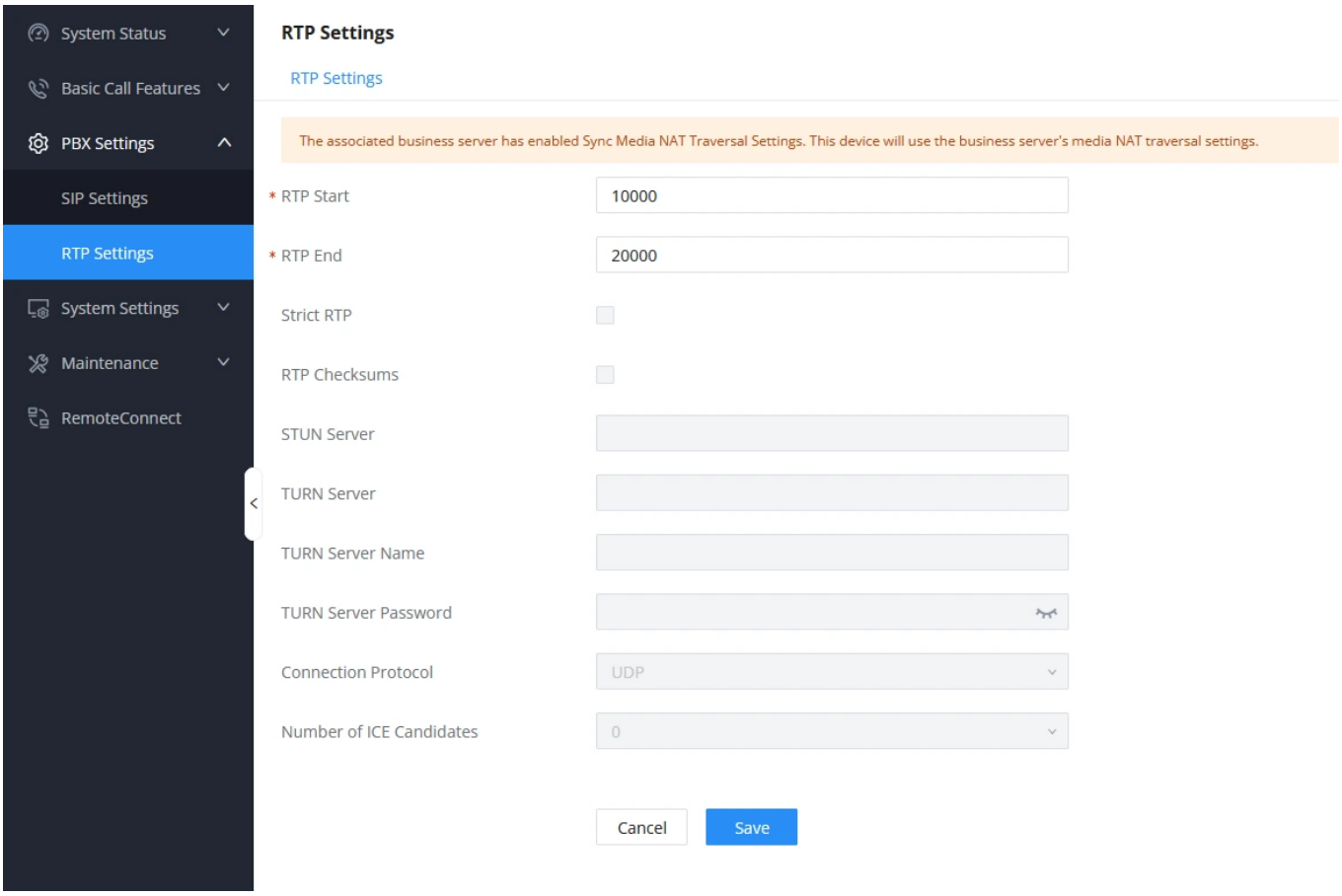


- **PBX Settings -> RTP Settings**

The following media NAT Traversal parameters will only be visible on the business server:



The remaining settings will be greyed out on the media server's side. Only the configuration on the business server will be taken into consideration.

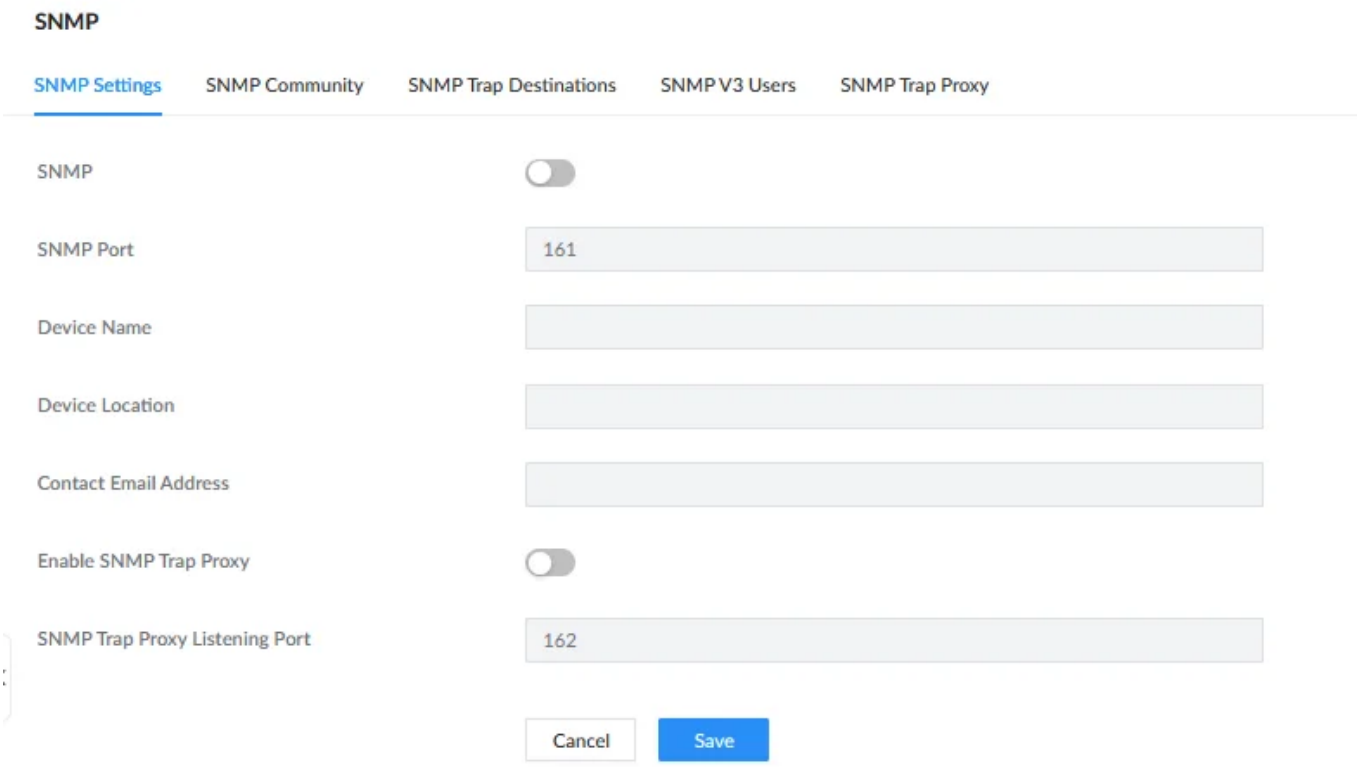


The SRTP Debugging option to allow decryption of packet captures will not be available on the media server under **Maintenance -> Network Troubleshooting -> Ethernet Capture**.

SNMP

SNMP integration in the UCM allows the administrator to monitor the components of the UCM remotely. SNMP is a useful integration to have a centralized monitoring dashboard that shows all the devices on your network, with that status of internal component. To configure the SNMP integration, please navigate to the web GUI of the UCM, then go to **System Settings -> SNMP -> SNMP Settings**

SNMP Settings

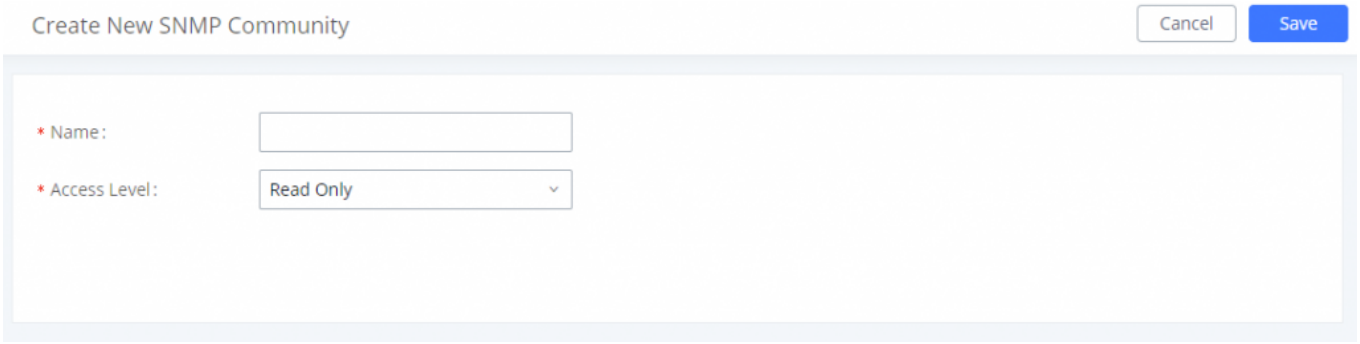


SNMP Settings

Enable	Tick this box to enable SNMP.
SNMP Port	Configure the port for the SNMP service.
Device Name	Enter the device name.
Device Location	Enter the location.
Contact Email Address	Enter the email address used to send the SNMP alerts to.
Enable SNMP Trap Proxy	Tick this box to enable a proxy for SNMP Trap.
SNMP Trap Proxy Listening Port	The port number on which the SNMP Trap Proxy is listening on.

SNMP Community

You can also create SNMP communities and affect a certain level of access. An SNMP community is a group created to aggregate many management stations. The community name is used to authenticate and identify these machines in the NMS (Network Management System).

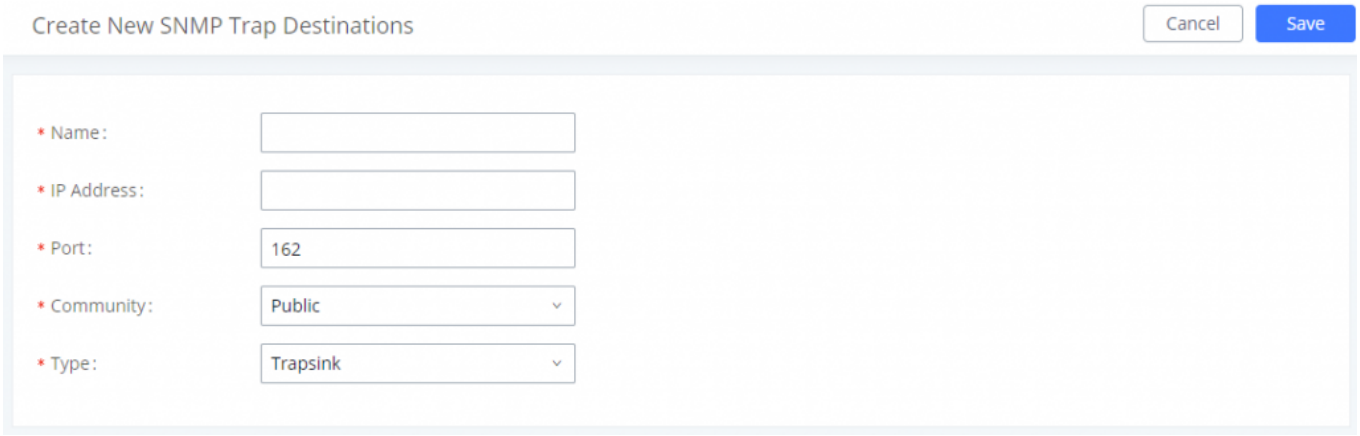


Create SNMP Community

Name	Enter a name for the community
Access Level	Select an access level: Read Only: The SNMP community will be able only to read SNMP messages.

SNMP Traps Destination

SNMP Traps is a very useful feature when there are many network components to manage. Instead of sending requests to all the machines in the network in order to view their SNMP logs risking slowing down or bringing the network to a complete halt, SNMP Traps can be configured so these machines can send unrequested messages to the manager to notify it about critical events and general failures.

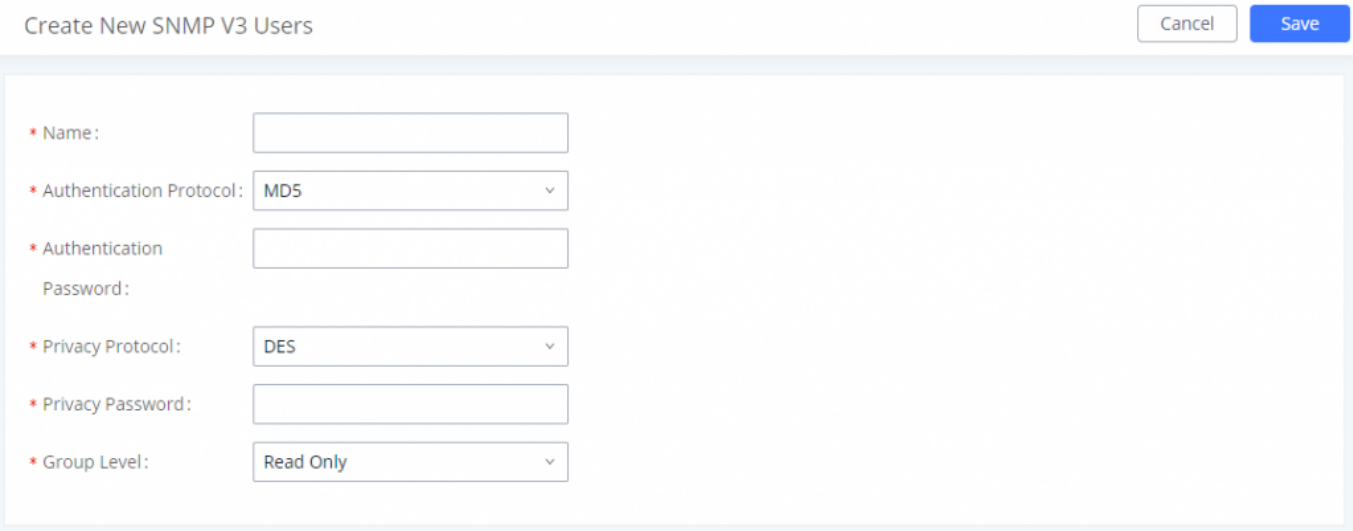


Create SNMP Trap Destination

Name	Enter a name of your SNMP Trap destination.
IP Address	Enter the SNMP Trap destination's IP address.
Port	Enter the port of the SNMP Trap destination.
Community	Select the community that you want
Type	Select the type of SNMP: Trapsink: Select this option if you want to send SNMP v1 traps. Trap2sink: Select this option if you want to send SNMP v2 traps. Informsink: Select this option if you want to send "Inform" notifications only.

SNMP Version 3

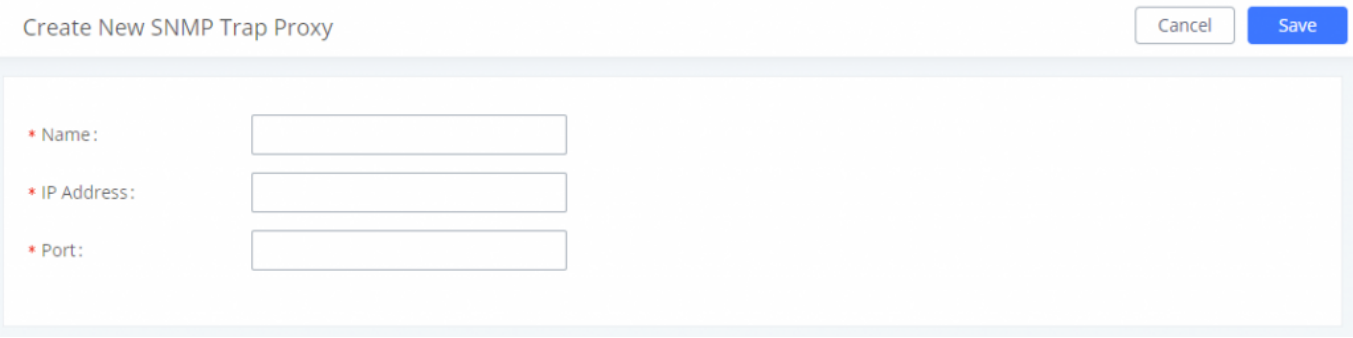
UCM63xx also supports SNMP v3 in case the system administrator decides to add more security to the monitoring process. SNMP v3 is a very good solution to monitor devices that interface directly with Internet. SNMP v3 offers more security than its predecessors by hashing the authentication information, encrypting the SNMP messages exchanged between the managed devices and the network management system which prevent eavesdropping. Also, it prevents any data tampering which protects the integrity of the data exchanged.



SNMP V3 Configuration

Name	Set the user's name
Authentication Protocol	Select the authentication protocol: MD5 SHA
Authentication Password	Set the authentication password.
Privacy Protocol	Select the protocol to use to encrypt the data DES AES-128 AES-192 AES-256
Privacy Password	Set the privacy password.
Group Level	Set the group level: Read Only. Read/Write.

SNMP Trap Proxy

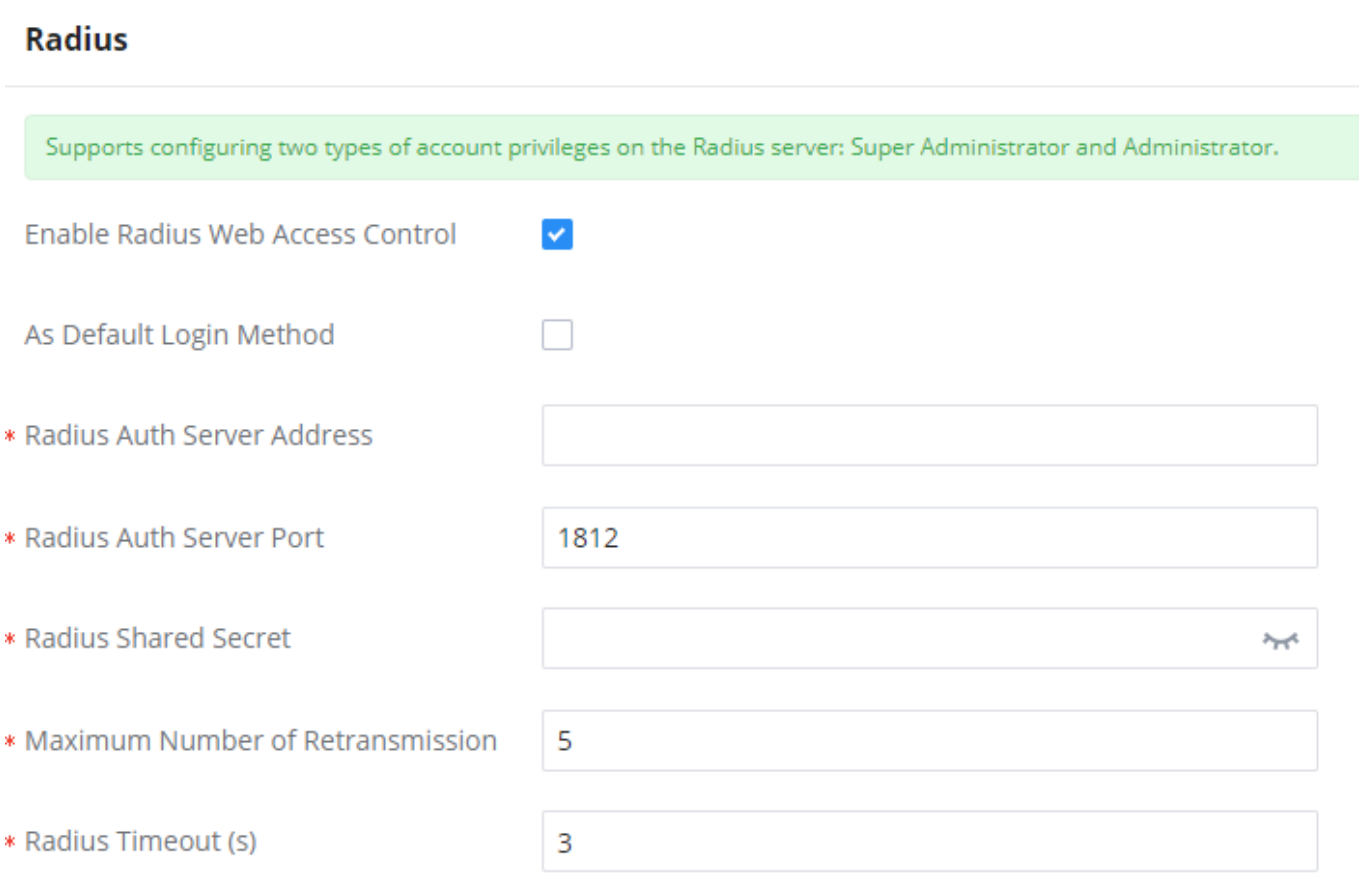


SNMP Trap Proxy

Name	Enter a name for the proxy server.
IP Address	Enter the proxy server's IP address.
Port	Enter the proxy server's port.

RADIUS

The UCM6300 offers Radius-based authentication for the super administrator and other administrators. This requires configuring a Radius server then enabling Radius client on the UCM6300 which can be found under **System Settings -> RADIUS**



Enable RADIUS Web Login Authentication	Enable or disable Radius.
Set as Default Login Method	Enable Radius as the default login method to the web UI of the UCM
RADIUS Auth Server Address	Enter the IP address/hostname of Radius server.
Radius Auth Server Port	Enter the port of radius serverDefault port number is: 1812
RADIUS Shared Secret	Enter Radius Shared Secret
Max Number of Retransmissions	Enter the number of retransmissions. The interval is 1 to 5.
RADIUS Timeout (s)	The maximum seconds before a session expires if there is no response from the server. The interval is between 1 to 30 seconds.

TR-069

To configure TR-069 on Grandstream devices, set the following parameters:

Parameter	Description
Enable TR-069	Toggle it on to enable TR-069. It is enabled by default
ACS URL	URL for TR-069 Auto Configuration Servers (ACS), e.g., http://myacs.grandstream.com
TR-069 Username	ACS username for TR-069 must be the same as in the ACS configuration.
TR-069 Password	ACS password for TR-069 must be the same as in the ACS configuration.
Verify ACS Server	Enables verification of the server certificate when interacting with GDMS. For security purposes, it is recommended to enable this option. However, verification is not needed for self-signed certifications.

Enable Periodic Inform	If enabled, Inform messages will be sent periodically based on the Inform Interval value.
Enable Periodic Inform	Enables periodic inform. If set to Yes, the device will send inform packets to the ACS.
Inform Interval (s)	A periodic time when PBX will send inform packets to TR-069 ACS serverThis option is specified in seconds.The default value is 86400.
ACS Connection Request Username	The username for the ACS to connect to PBX.
ACS Connection Request Password	The password for the ACS to connect to the PBX.
ACS Connection Request Port	Port for incoming connection requests.The default value is 7547.
CPE Cert File	The Cert file for PBX to connect to the ACS via SSL.
CPE Cert Key	The Cert key for PBX to connect to the ACS via SSL.

CONTACTS

Address book management is under UCM web UI->Maintenance, and it has two sections "Contact Management" and "Department management".

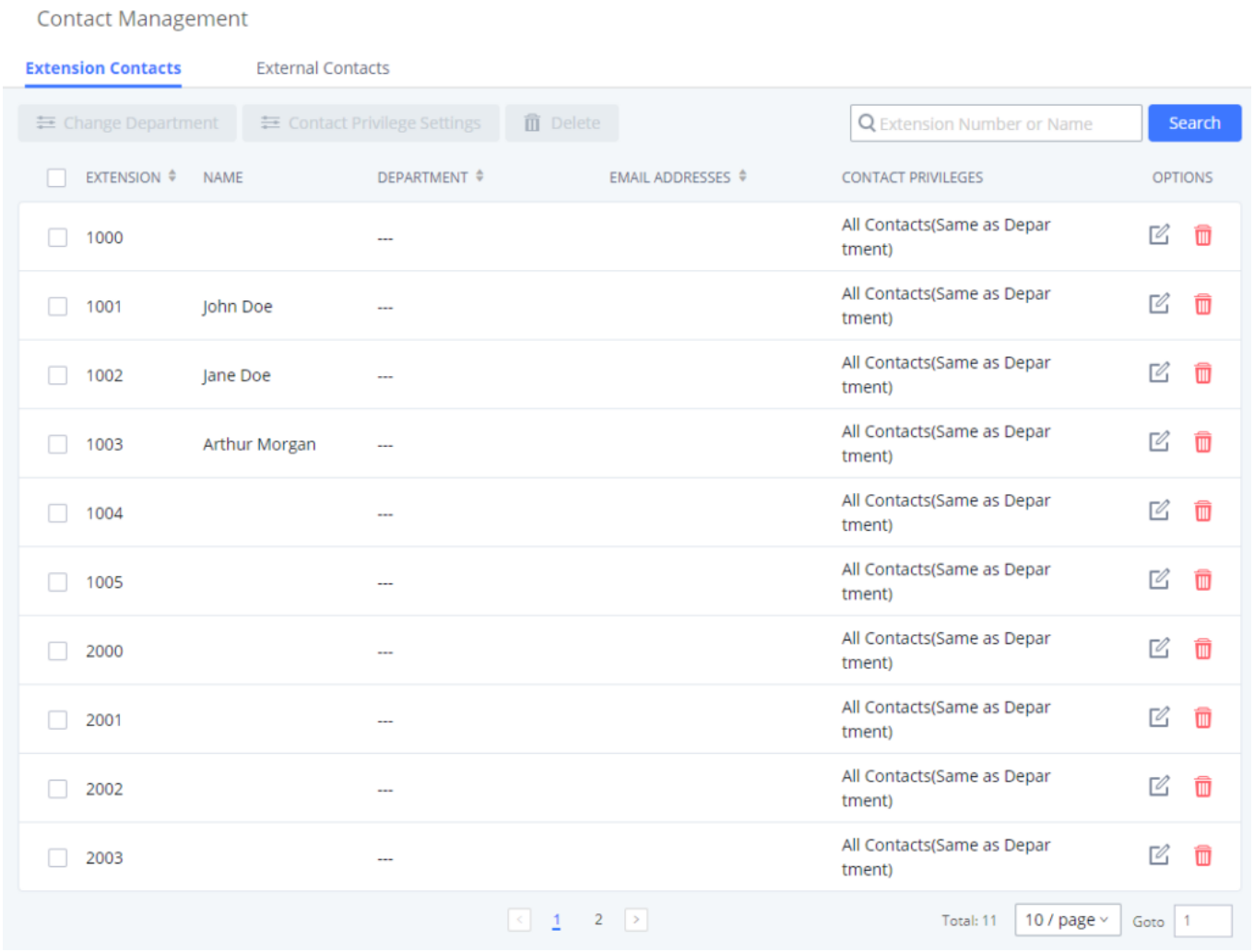
Contact Management

Contact management page displays extension contacts and external contacts information.

- Extension contacts

Extension contacts page shows all the extensions that has "Sync Contact" option enabled in extension settings page. The extension contacts here can be edited or deleted individually or in batch. No new extension contact can be added directly from this page. If an extension contact is deleted from this page, "Sync Contact" option is disabled from this extension. This will not delete the extension from UCM.

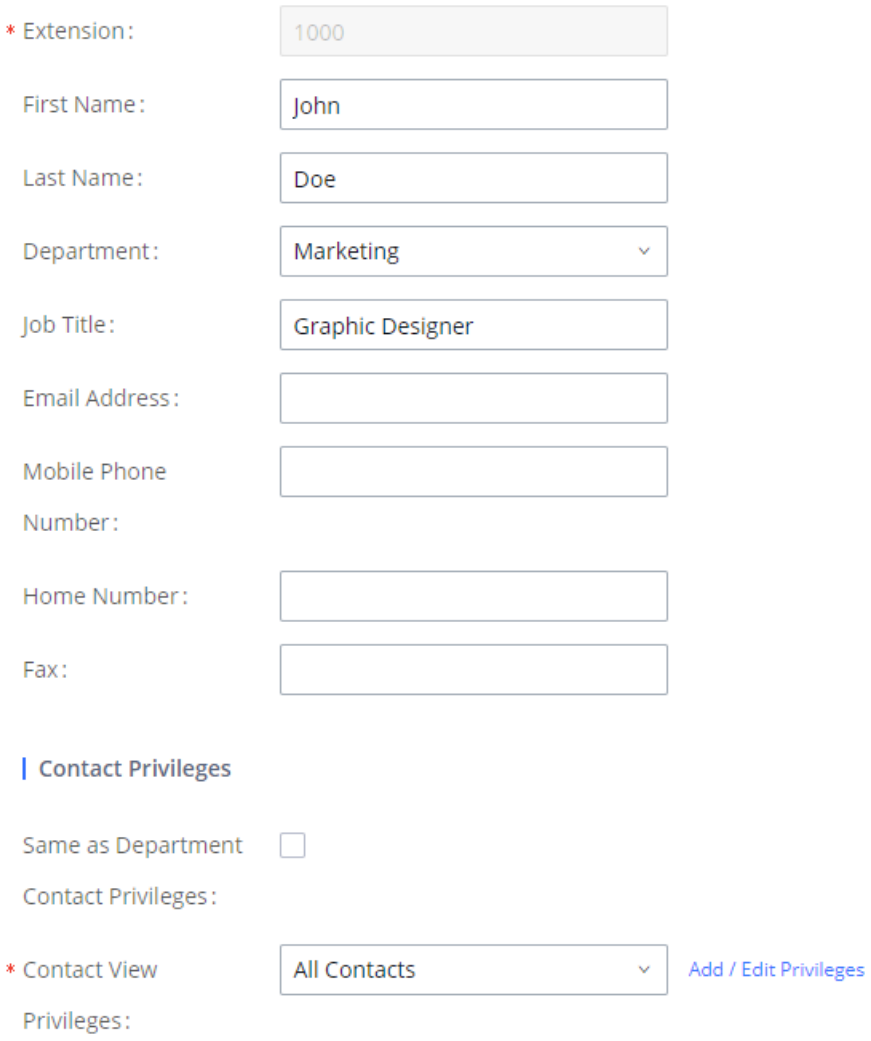
"Delete" extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.



Extension Contacts

"Delete" extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

Click Edit icon to configure name, department, email address and etc for each extension contact.



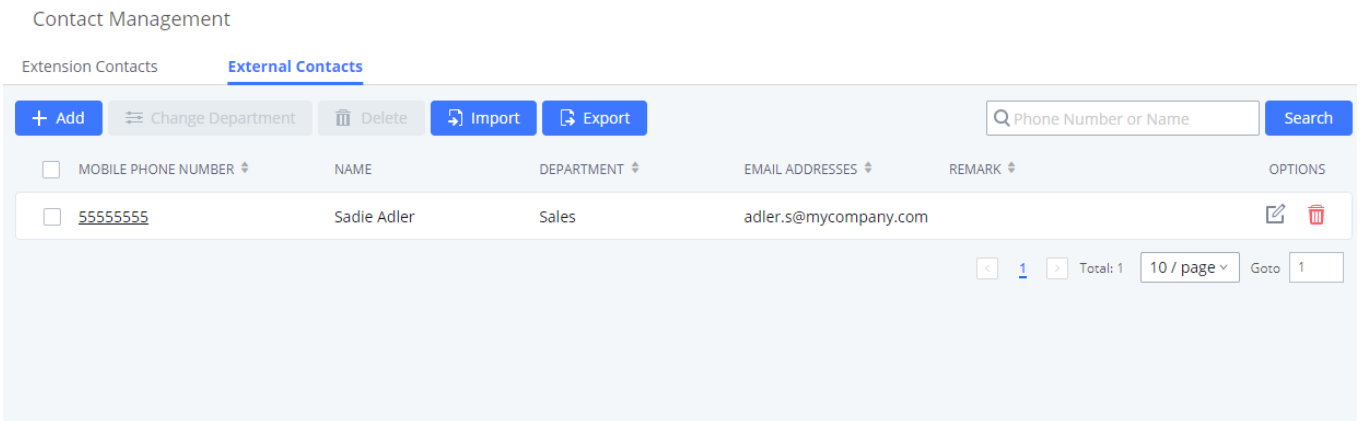
Edit Extension Contact

Extension	Displays extension number.
First Name	Configure first name for the extension contact.
Last Name	Configure last name for the extension contact.
Department	Select department for the extension contact. Department can be created in "Department Management" page.
Department Title	Configure the job title for the extension contact.
Email Address	Configure email address for the extension contact.
Mobile Phone Number	Configure mobile phone number for the extension contact.
Home Number	Configure home number for the extension contact
Fax	Configure Fax for the extension contact.
Same as Department Contact Privileges	When this option is enabled, the contact extension will inherit the same privilege as the department it belongs to.
Contact View Privileges	This option allows configuring privileges for the contact extension.Note: This option will be disabled if "Same as Department Contact Privileges" has been enabled.

-

External contacts

On external contacts page, the admin can create single external contact, import contacts in batch, edit contacts, delete contacts and export contacts.

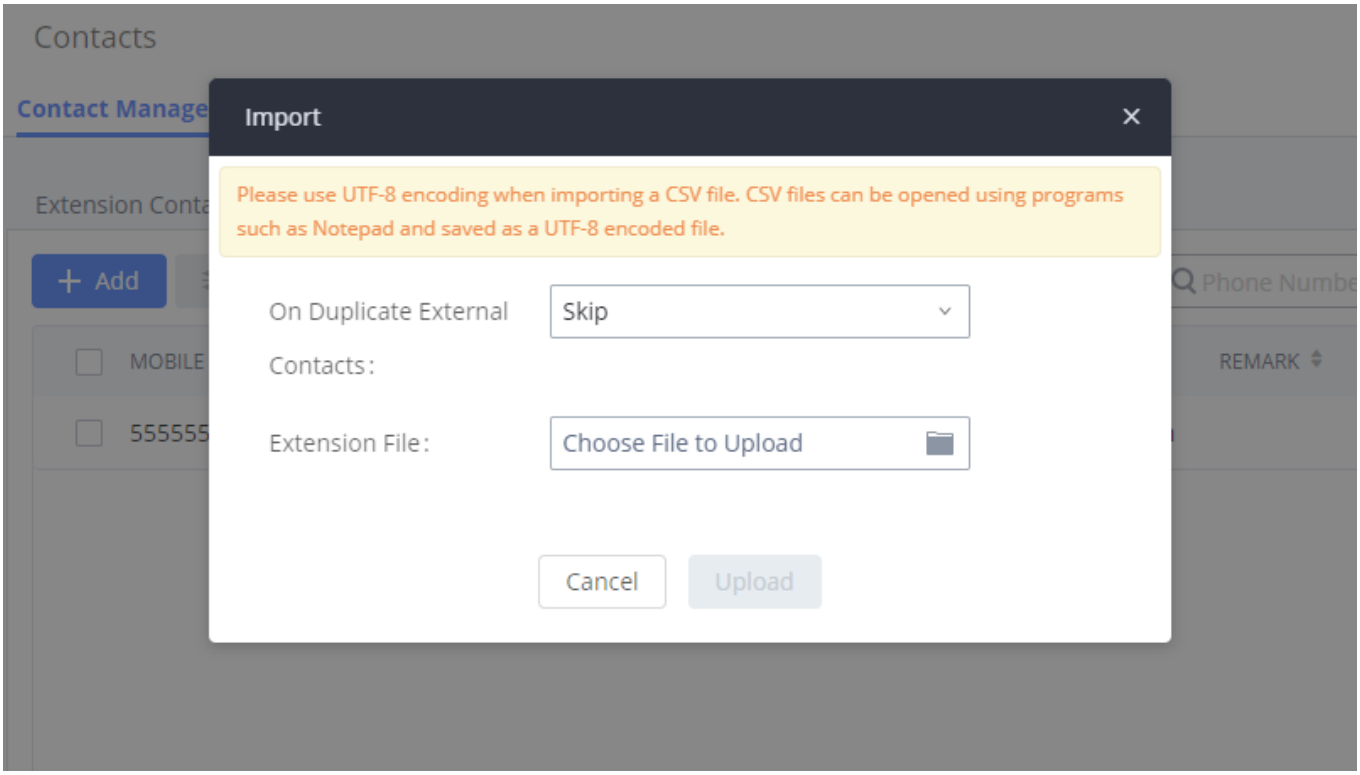


External Contacts

Click on "Export" icon, a file will be generated with the current external contacts.

Click on "import" icon, then follow the steps below to add external contacts in batch:

- **Step 1**: For option "On Duplicate External Contacts", select whether to skip duplicate contact on the imported CSV file or update the duplicate UCM contact with the information in the CSV.
- **Step 2**: Choose file from local PC to upload.
- **Step 3**: Click on "Upload".
- **Step 4**: Click on "Apply" to complete importing external contacts.



Import External Contacts

Department Management

Departments are organizational units that allows organizing extensions within groups that specify the specialty of a the extension owners within a company. This makes finding contacts easier within the UCM contact books.



Department Management

Click on "Add" to create a new department. Configure the department name and select the superior department. By default the superior department is the root directory. If the UCM has cloud IM configured, the root directory will be the department in cloud IM.

On the department list:

- Click on

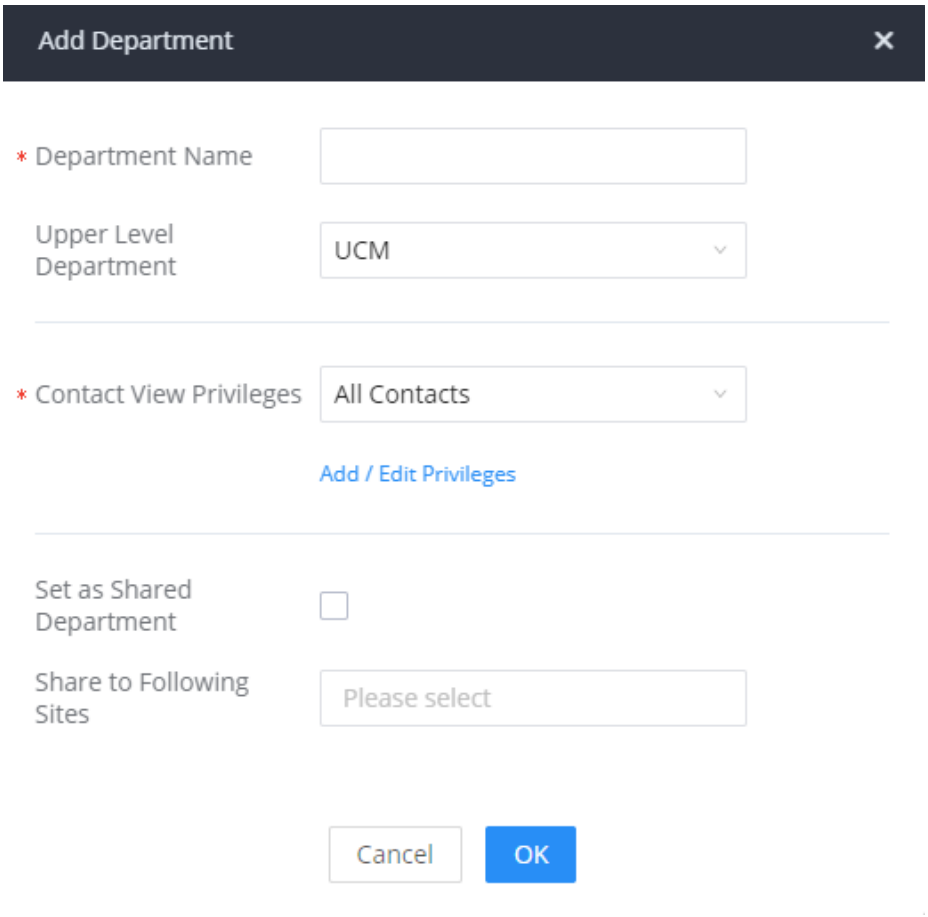
  to create sub department.

- Click on

  to add member to the department.

- Click on

  to edit the department.



Edit Department

If the UCM has Cloud IM enabled and configured, the following options will be available:

- **Set as Shared Department:** Toggles the shared status of the department. If there are existing cross-server members in this department, this option will be grayed out.
- **Share to Following Sites:** Select the sites (servers) to that will be allowed to move their extensions in and out of the shared deparmtent.
- **Apply Settings to Sub-Level Departments:** Only available when editing an exisiting deparmtent. Apply the same sharing settings to its sub-department. If a department has sharing enabled and is configured to be shared with specific sites, its sub-department will also have sharing enabled and be shared with the same sites.

Shared departments can be distinguished by an icon next to their name.



Shared Department Symbol

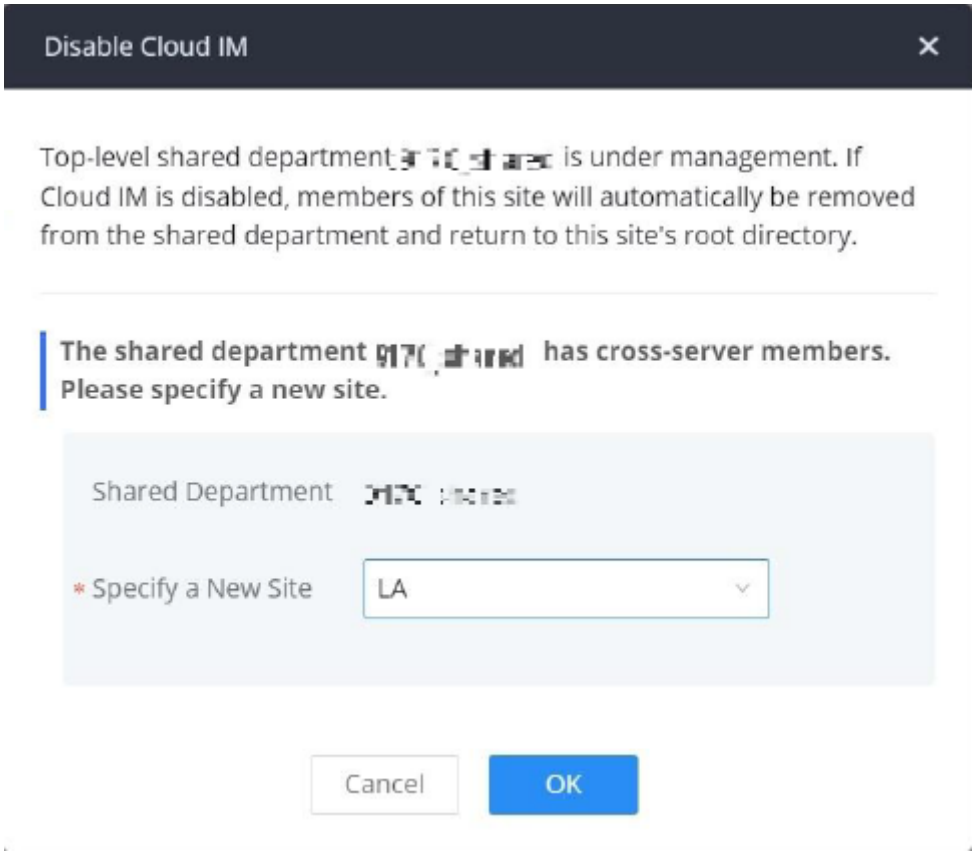
There are 3 potential marks in the center of that icon that represent the permission level that the current UCM has for that site

- : The + symbol indicates that the current UCM is the creator of the shared department. It has full management priviliges over it, which include the ability to edit it, delete it, add sub-departments under it, add its own extensions to it and remove **any** extensions from it, including extensions from other servers.
- : The checkmark symbol indicates that the department was shared to the current UCM has been authorized to move its own extensions in and out of department.
- : No symbol indicates that the department is from a UCM that is under the same Cloud IM account as the current UCM, but it has not been shared to the current UCM for management. The current UCM can only view this shared department and its members but cannot interact with it unless the shared depratment has the current UCM's extensions as members. In this case, the current UCM can still remove members from the shared department.

- Removing a member from a shared department will move it to the root directory of its original site.
- A shared department cannot be deleted unless all cross-server memebers are removed from it

If a UCM with a shared depratment no longer wants to use CloudIM, it must first do the following:

- If there are no cross-server memebers in its shared departments, it must set them as local departments and assign new parent departments to them.
- If there are existing cross-server members in its shared departments, it must assign the shared departments to another site for management.



Assign Shared Department

If the UCM re-enables Cloud IM, it will not reclaim ownership of its original shared departments.

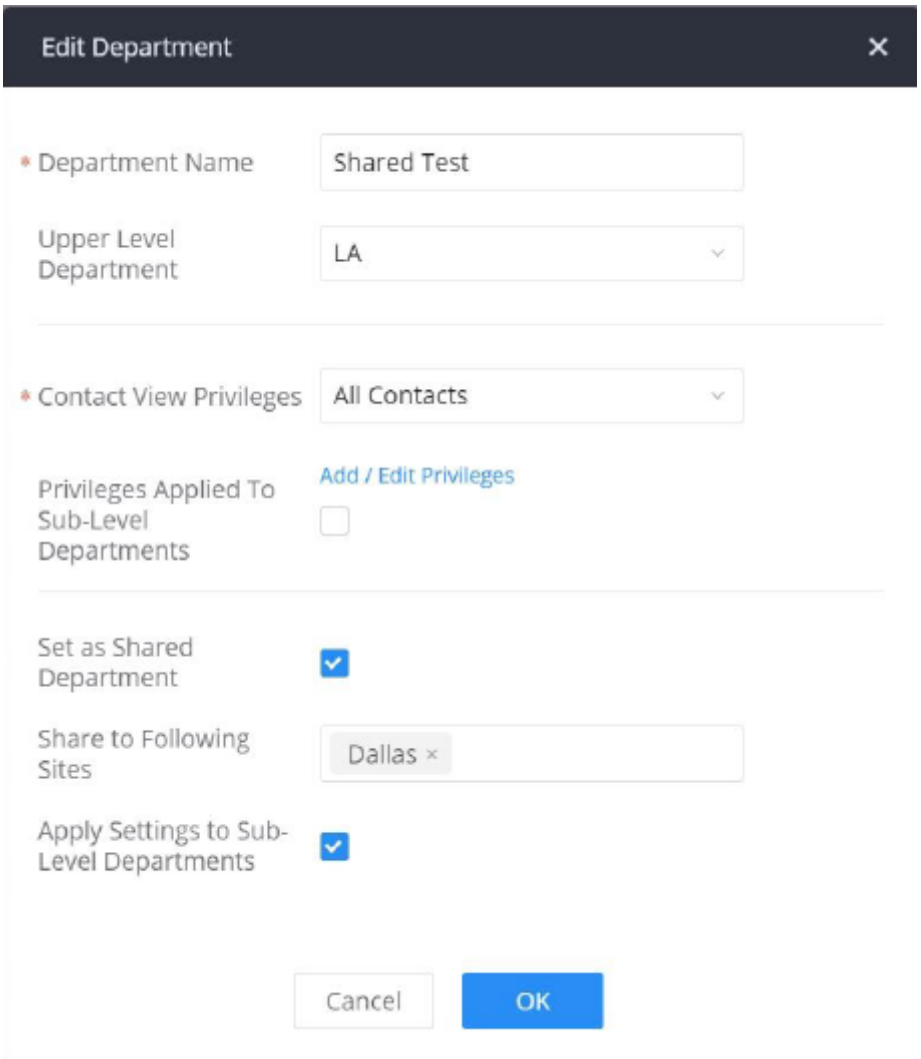
The user can create up to 100 departments with up to 4 levels of nested departments.

To be able to use shared department, the UCM devices will have to be subscribed to a RemoteConnect plan that offers Cloud IM service. For more information please refer to: https://ucmrc.gdms.cloud/plans

Shared Departments

Share departmens offer a centralized way for administrators to manage departments and members across multiple servers using the same Cloud IM account. To get started, make sure that the UCM has Cloud IM enabled and configured. Then, navigate to **Contacts -> Department Management**, then add/edit a specific department.

Tick the option **Set as Shared Department**, then select the sites to which the department will be shared. If the user wishes to apply the same sharing settings to the departments nested under the parent department, please tick the option **Apply Settings to Sub-Level Departments.**



Edit Department

Privilege Management

The user can configure custom privileges other than the default ones (All contacts, Departments and sub-departments contacts). These custom privileges allow more flexible ways of allowing contacts to view all or specific contacts from other departments.

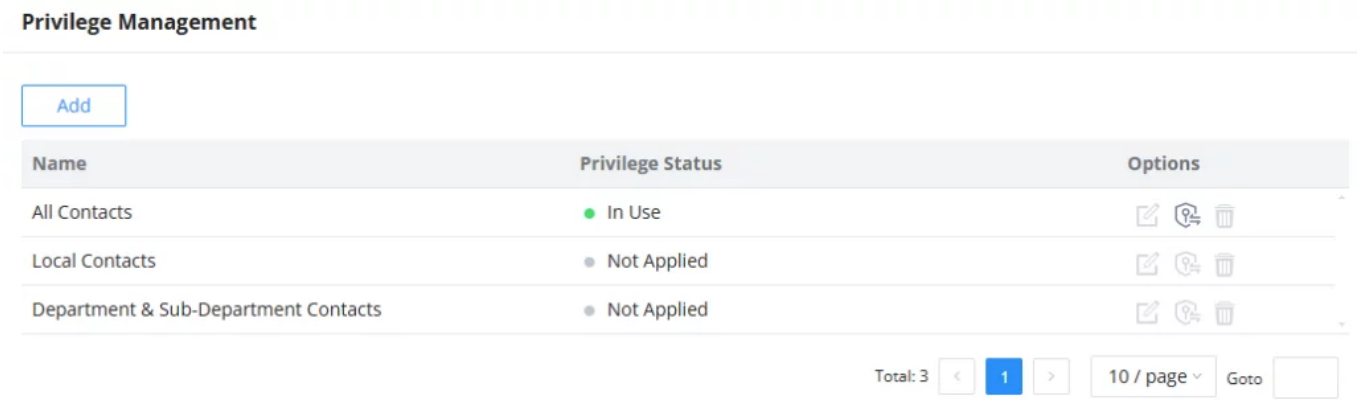
UCM admin can add or edit Privilege Management; under UCM web UI→**Contacts Privilege Management**,

there are 2 default privileges:

- Visible to all contacts.
- Only the contact person's department and sub-department contacts are visible.

When Cloud IM is enabled on the UCM, a third privilege becomes available to choose:

- Local Contacts: Restricts the contacts shown to the contacts of the local UCM.

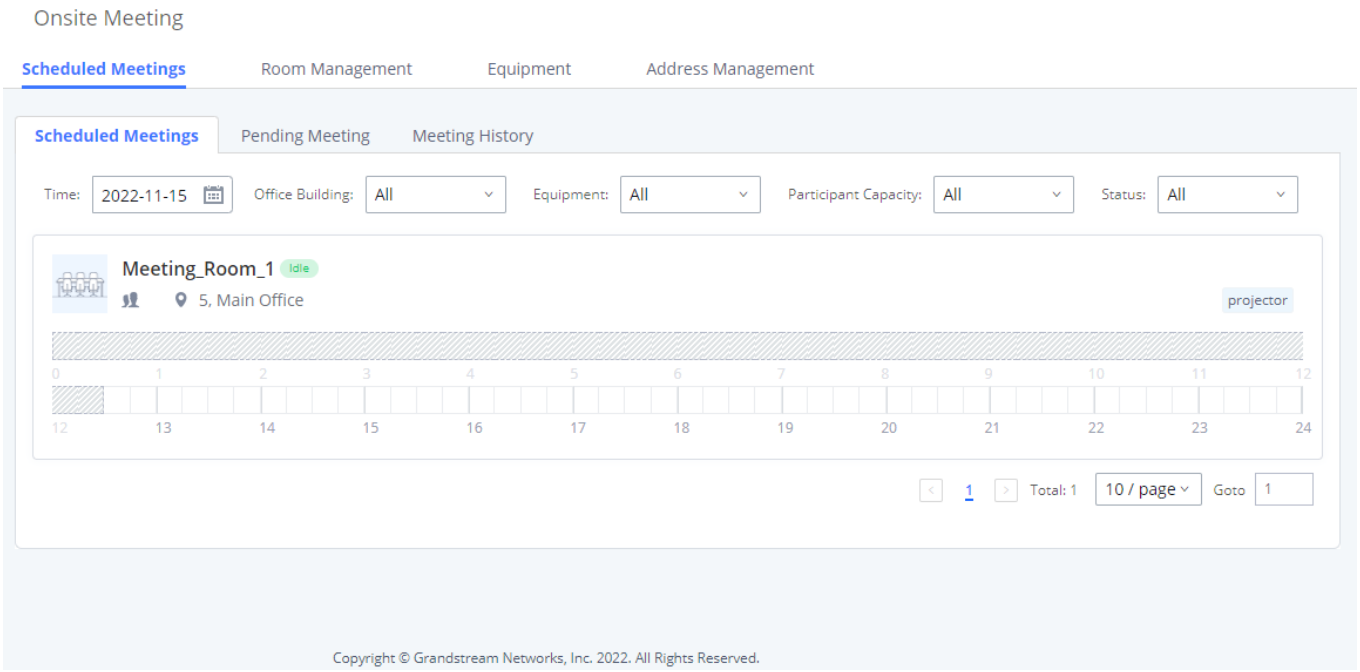


Privilege Management

DEVICE MANAGEMENT

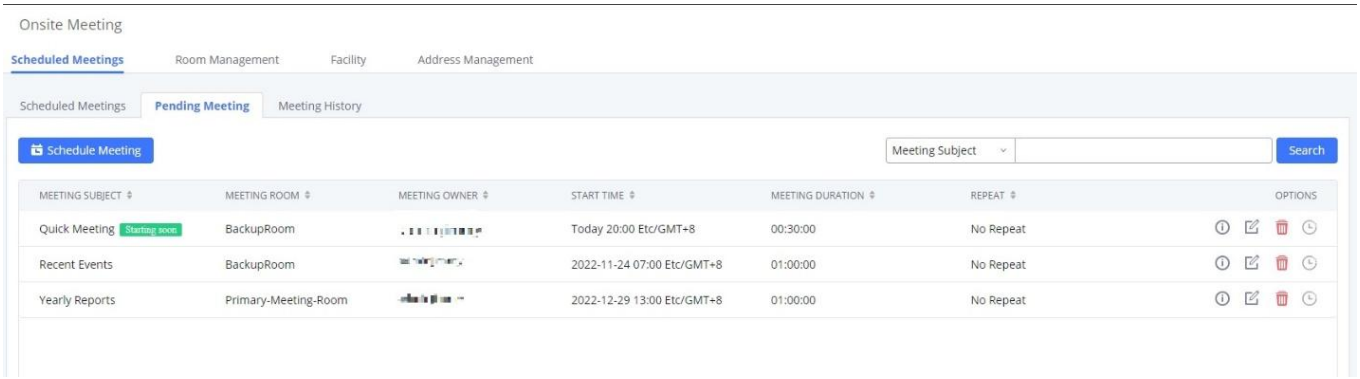
Onsite Meeting Room

For workplaces that require employees to return to physical offices for work, The UCM6300 Series offers the Onsite Meetings feature, a new way to stay organized and keep up-to-date with in-person meetings. This feature allows administrators to create and manage onsite meeting rooms, specify meeting room locations, schedule meetings, and add conferencing equipment. The new feature can be found under the **Device Management > Onsite Meeting** page. The first page that appears is the **Scheduled Meetings** page and tab page, which provide an overview of all created meeting rooms. It provides information about the rooms' meeting schedules for the day, their locations, their member capacity, and their equipment.



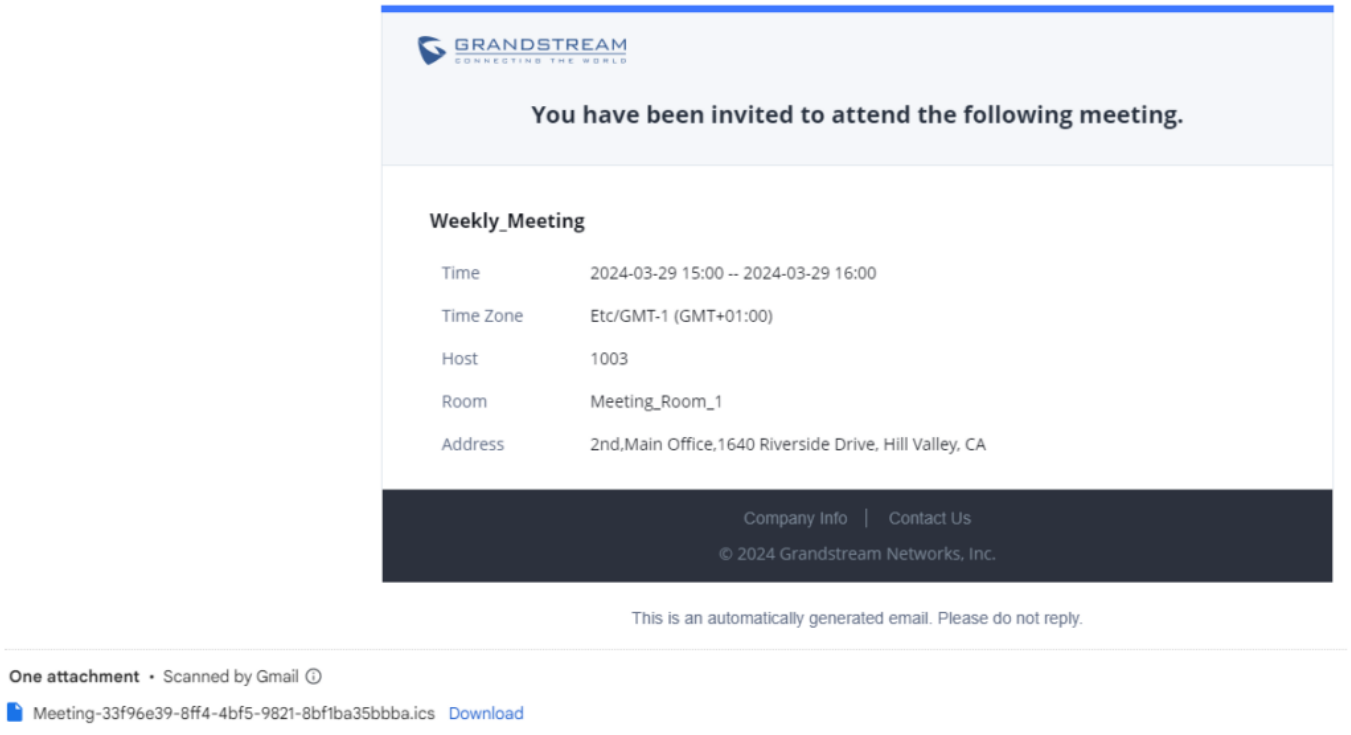
Schedule Onsite Meetings

The **Pending Meeting** tab and **Meeting History** tab show detailed information about upcoming meetings and previous meetings respectively. From the **Pending Meeting** tab, users can delete upcoming meetings and extend the duration of ongoing meetings. **The Meeting History** tab will display the last 6 months of onsite meetings.



Pending Onsite Meetings

When a meeting is scheduled the invitees will receive an invitation via email which contains all the information regarding the onsite meeting. The email will be attached with an .ics file which can be imported to a calendar to mark your calendar of the onsite meeting, please see the screenshot below.

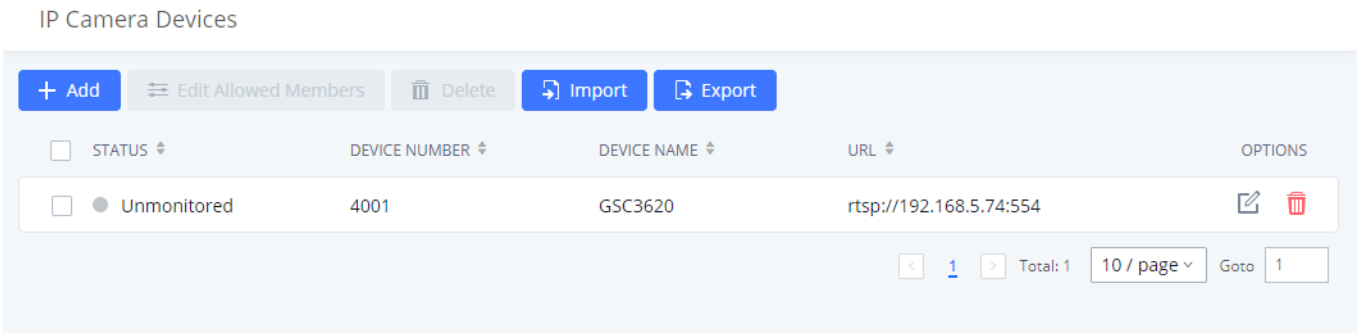


Onsite Meeting Email Invitation

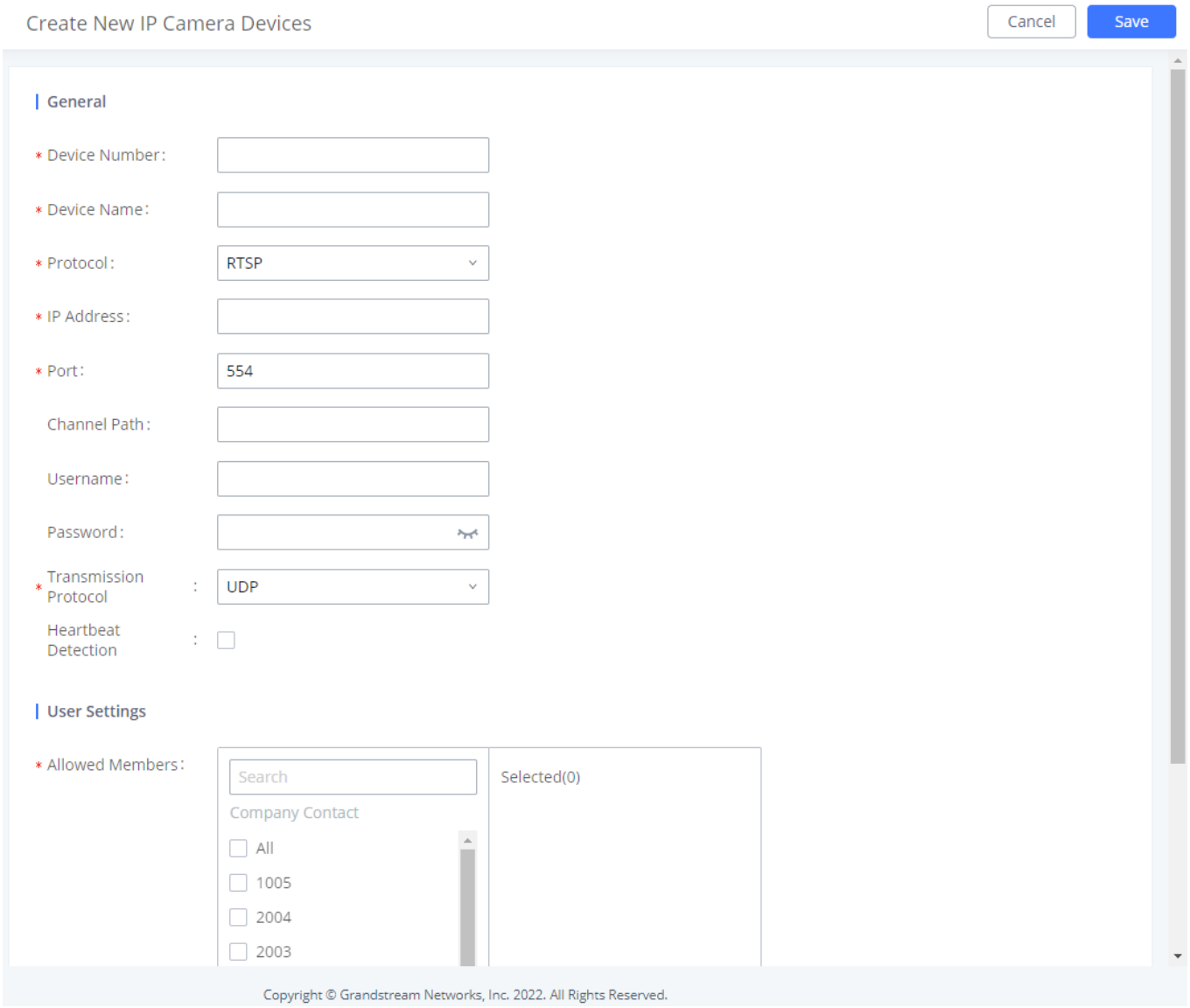
IP Camera Devices

The UCM admin can add IP camera devices and edit accessible extensions so these extensions can view the surveillance streams for the IP camera devices.

Click on "Add" to add IPC device.



IPC Devices



IPC Devices Settings

Device Number	The number that allowed members can dial to access the IP camera.
Device Name	Enter the name that you want to allocate for the device.
Protocol	The media control protocol used. RTSP
IP Address	Enter the IP address of the IP camera.
Port	Enter the port of the IP camera. The default is 554
Channel Path	If you want to view the stream of the specified channel, please configure the path of this stream.

Username	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Password	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Transmission Protocol	Transport protocol of the IP camera. Default is UDP.
Heartbeat Detection	If enabled, the PBX will regularly send RTSP OPTIONS to check of the device is still online.
Allowed Members	Extensions, Extension Groups, and Departments can be selected to access this IP camera by dialling the configured Device Number.

Zero Config

Overview

Grandstream SIP Devices can be configured via Web interface as well as via configuration file through TFTP/HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file and XML format configuration file.

The UCM630x provides a Plug and Play mechanism to auto-provision the SIP devices in a zero-configuration manner by generating an XML config file and having the device download it within the LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

Zero Config supports centralized provisioning for Grandstream SIP devices and selected third-party enterprise SIP phones. Supported third-party devices can be discovered, configured, and managed using the same Zero Config workflow, except where explicitly limited.

To provision a phone, three steps are involved, i.e., discovery, configuration, and provisioning. This section explains how Zero Config works on the UCM630x. The settings for this feature can be accessed via **Device Management->Zero Config**.

Zero Config Supported Devices

The following table lists all Grandstream and third-party SIP device series that support auto-provisioning via Zero Config, including IP phones, conference devices, door systems, and analog gateways.

Availability of specific models depends on whether the corresponding model template package is installed under **Device Management -> Zero Config -> Model Update**.

Vendor	Supported Device Series & Models
Grandstream	GXP Series
	GRP Series
	GXV Series
	GHP Series
	GVC Series
	GAC Series
	GSC Series
	GDS Series
	GXW Series
	HT Series
	DP Series
	WP Series

Avaya	J100 Series
Cisco	CP-3905
	CP-6921
	CP-78xx Series
	CP-88xx Series
	DP-98xx Series
Poly	Edge-E Series
	Edge-B Series
	VVX Series (non-OBi)
Yealink	AX Series
	T4 Series
	T5 Series
	T7 Series
	T8 Series

Third-party enterprise device provisioning (Avaya, Cisco, Poly, and Yealink) can be managed and enabled under **Device Management -> Zero Config -> Zero Config Settings -> Manage 3rd-Party Enterprise Phones**.

- Cisco IP Phones support line registration, remote Do Not Disturb (DND) synchronization, and conferencing features.
- Poly Edge B Series support multi-account template mapping across line keys.

Configuration Architecture for Endpoint Device

The end point device configuration in ZeroConfig is divided into the following three layers with priority from the lowest to the highest:

- **Global**

This is the lowest layer. Users can configure the most basic options that could apply to all SIP devices during provisioning via Zero config.

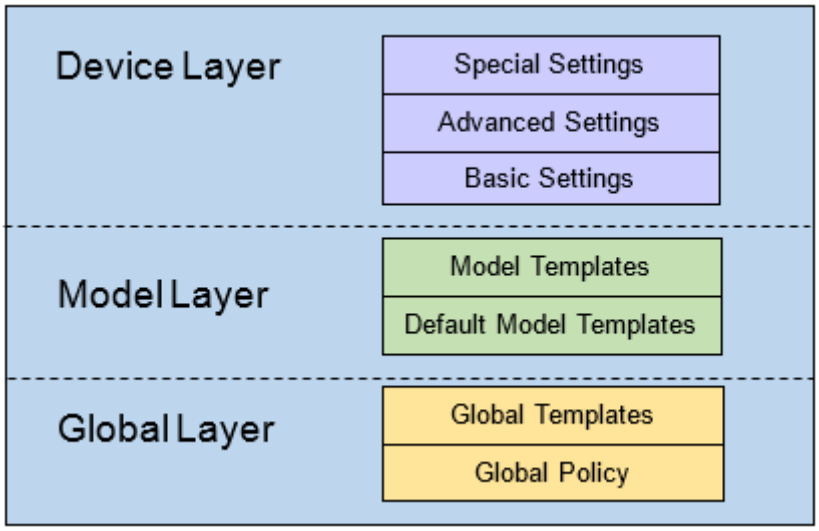
- **Model**

In this layer, users can define model-specific options for the configuration template.

- **Device**

This is the highest layer. Users can configure device-specific options for the configuration for the individual device here.

Each layer also has its own structure at different levels. Please see the figure below. The details for each layer are explained in sections **[Global Configuration]**, **[Model configuration]** and **[Device Configuration]**.



Zero Config Configuration Architecture for End Point Device

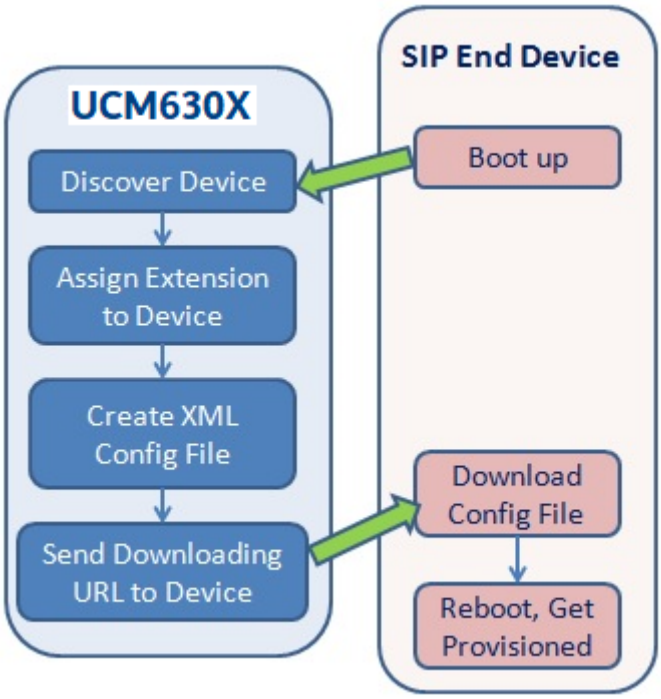
The configuration options available in the **Model** and **Device** layers fully include those defined in the **Global** layer. In other words, the Global layer options are a subset of the options available at both the Model and Device layers.

When the same option is configured in multiple layers with different values, the value from the higher-priority layer overrides those from lower-priority layers. Layer priority is as follows (from lowest to highest): **Global->Model->Device**.

Example: if English is selected as the language in the Global Policy, and Spanish is selected in the Default Model Template, the device being provisioned will use Spanish, because the Model layer has higher priority than the Global layer.

Auto-Provisioning Settings

By default, the Zero Config feature is enabled on the UCM630x for auto-provisioning. Three methods of auto-provisioning are used.



UCM630X Zero Config

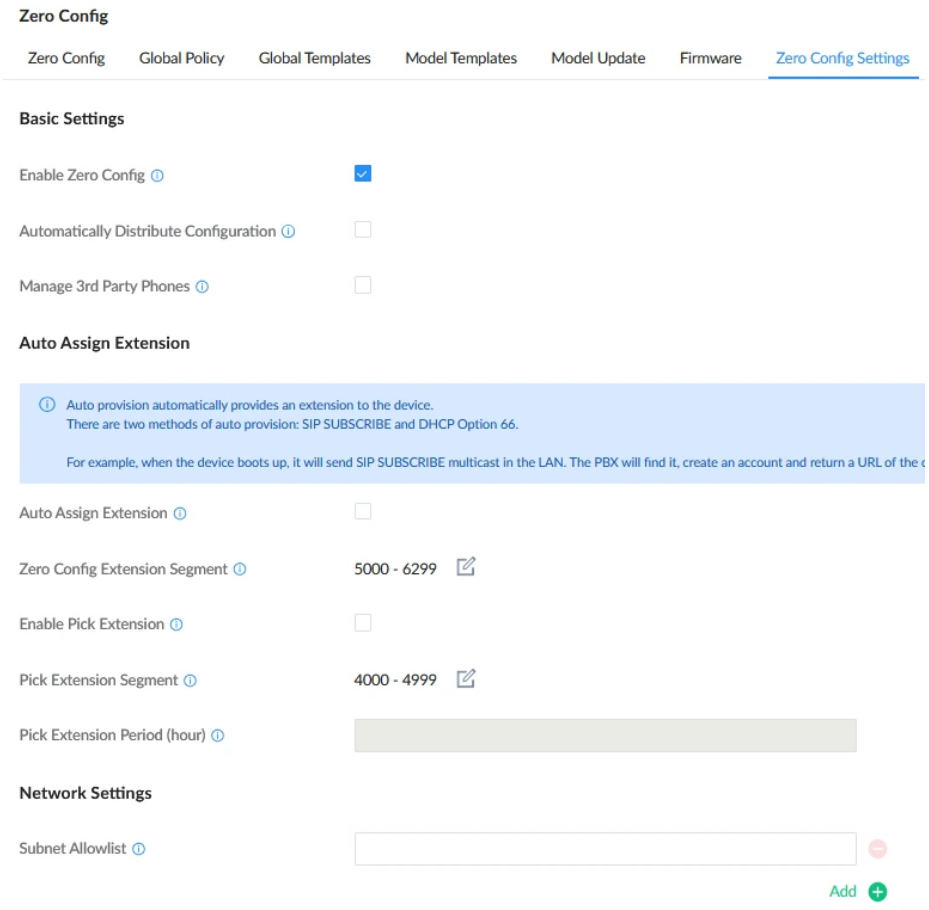
- **SIP SUBSCRIBE**

When the phone boots up, it sends out SUBSCRIBE to a multicast IP address in the LAN. The UCM630x discovers it and then sends a NOTIFY with the XML config file URL in the message body. The phone will then use the path to download the config file generated in the UCM630X and take the new configuration.

- **DHCP OPTION 66**

Route mode needs to be set to use this feature. When the phone restarts (by default DHCP Option 66 is turned on), it will send out a DHCP DISCOVER request. The UCM630X receives it and returns DHCP OFFER with the config server path URL in Option 66, for example, https://192.168.2.1:8089/zccgi/. The phone will then use the path to download the config file generated in the UCM630X.

To start the auto-provisioning process, under **Device Management**->**Zero Config**->**Zero Config Settings**, fill in the auto provision information.



Zero Config Settings Page

The table below explains all the configurable parameters that can be found on the Zero Config Settings page:

Basic Settings	
Enable Zero Config	Enable or disable the zero-config feature on the PBX. The default setting is enabled.
Auto Provision	By default, this is disabled. If disabled, when the SIP device boots up, the PBX will not send the SIP device the URL to download the config file, and therefore the SIP device will not be automatically provisioned by the PBX.

Manage 3rd-Party Enterprise Phones	This option controls whether third-party SIP phones can be provisioned using Zero Config. When enabled, port 69 (TFTP) and port 6970 (HTTP) are automatically opened on the UCM for non-encrypted provisioning communication. Only the phone models listed under the [Zero Config Supported Devices] section can be provisioned using this feature. To allow third-party SIP phones to be provisioned, configure the DHCP server in the phone's network with the following options:DHCP Option 66: UCM IP addressDHCP Option 160: http://<UCM-IP>:6970/zccgi Notes :All supported third-party enterprise phones share the same DHCP Option 66 and Option 160 configuration.DHCP Option 66 and Option 160 must be placed before any other identical DHCP options in the DHCP server configuration.HTTP provisioning traffic is not encrypted.Port 6970 is reserved for Zero Config provisioning and cannot be modified.
Auto Assign Extension	
Auto Assign Extension	If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in "Zero Config Extension Segment" to the device. The default setting is disabled.
Zero Config Extension Segment	Click on the link "Zero Config Extension Segment" to specify the extension range to be assigned if "Automatically Assign Extension" is enabled. The default range is 5000-6299. Zero Config Extension Segment range can be defined in Web GUI->PBX Settings->General Settings->General page->Extension Preference section: "Auto Provision Extensions".
Enable Pick Extension	If enabled, the extension list will be sent out to the device after receiving the device's request. This feature is for the GXP series phones that support selecting extensions to be provisioned via the phone's LCD. The default setting is disabled.
Pick Extension Segment	Click on the link "Pick Extension Segment" to specify the extension list to be sent to the device. The default range is 4000 to 4999. Pick Extension Segment range can be defined in Web GUI->PBX Settings->General Settings->General page->Extension Preference section: "Pick Extensions".
Pick Extension Period (hour)	Specify the number of minutes to allow the phones being provisioned to pick extensions.
Network Settings	
Subnet Allowlist	This feature allows the UCM to provision devices in different subnets other than the UCM network.Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is <IP>/<CIDR>.Examples: 10.0.0.1/8, 192.168.6.0/24NotesOnly private IP ranges (10.0.0.0 | 172.16.0.0 | 192.168.0.0) are supported.Up to 10 subnets can be configured in the allowlist

Please make sure an extension is manually assigned to the phone or "Automatically Assign Extension" is enabled during provisioning. After the configuration on the UCM630x Web GUI, click on "Save" and "Apply Changes". Once the phone boots up and picks up the config file from the UCM630X, it will take the configuration right away.

Discovery

SIP endpoints are automatically discovered after bootup. Users could also manually discover devices by specifying the IP address or scanning the entire LAN network. Three methods are supported to scan the devices.

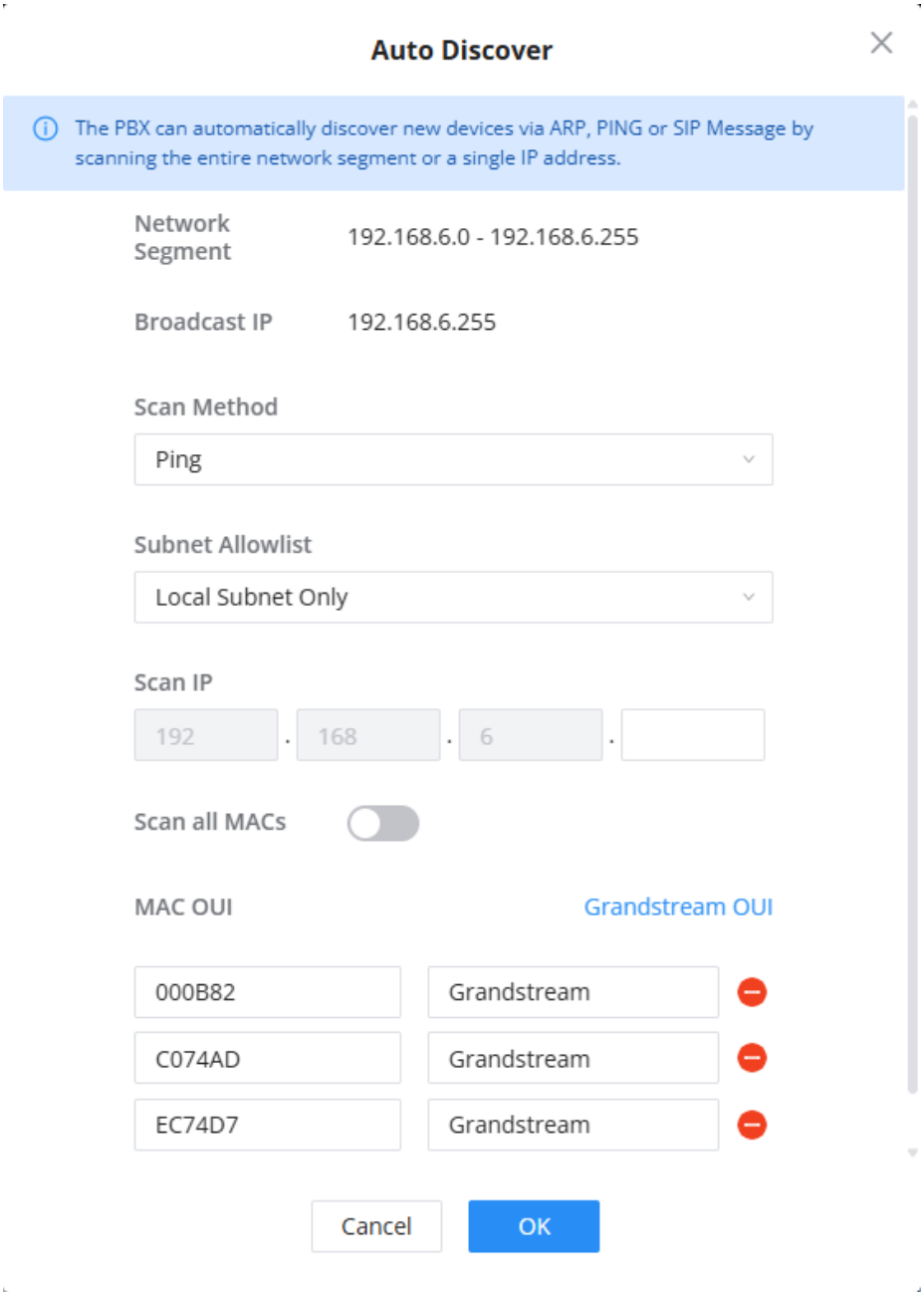
- PING
- ARP
- SIP Message (NOTIFY)

To start the discover process:

1. Click on "Auto Discover" under **Device Management**->**Zero Config**->**Zero Config**.
2. Choose the "Scan Method" and enter the "Scan IP". The IP address segment will be automatically filled in

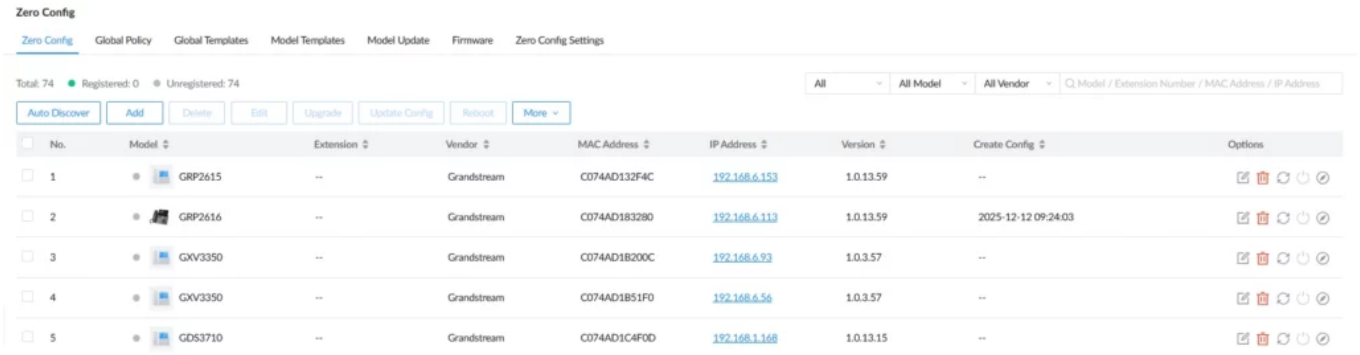
based on the network mask detected on the UCM630X. If users need to scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address.

3. Click on "Save" to start discovering the devices within the same network. To successfully discover the devices, "Zero Config" needs to be enabled on the **Device Management**->**Zero Config**->**Auto Provisioning Settings**.



Auto Discover

The following figure shows a list of discovered phones, displaying the MAC address, IP address, extension (if assigned), version, vendor, model, connection status, Create Config option, and available actions (Edit, Delete, Update, Reboot, and Access Device Web GUI).

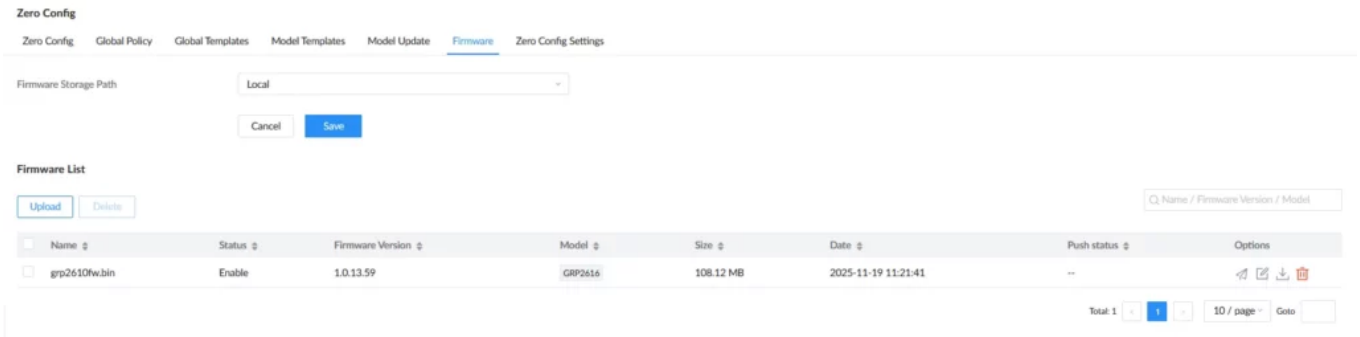


Zero Config Main Page

Firmware

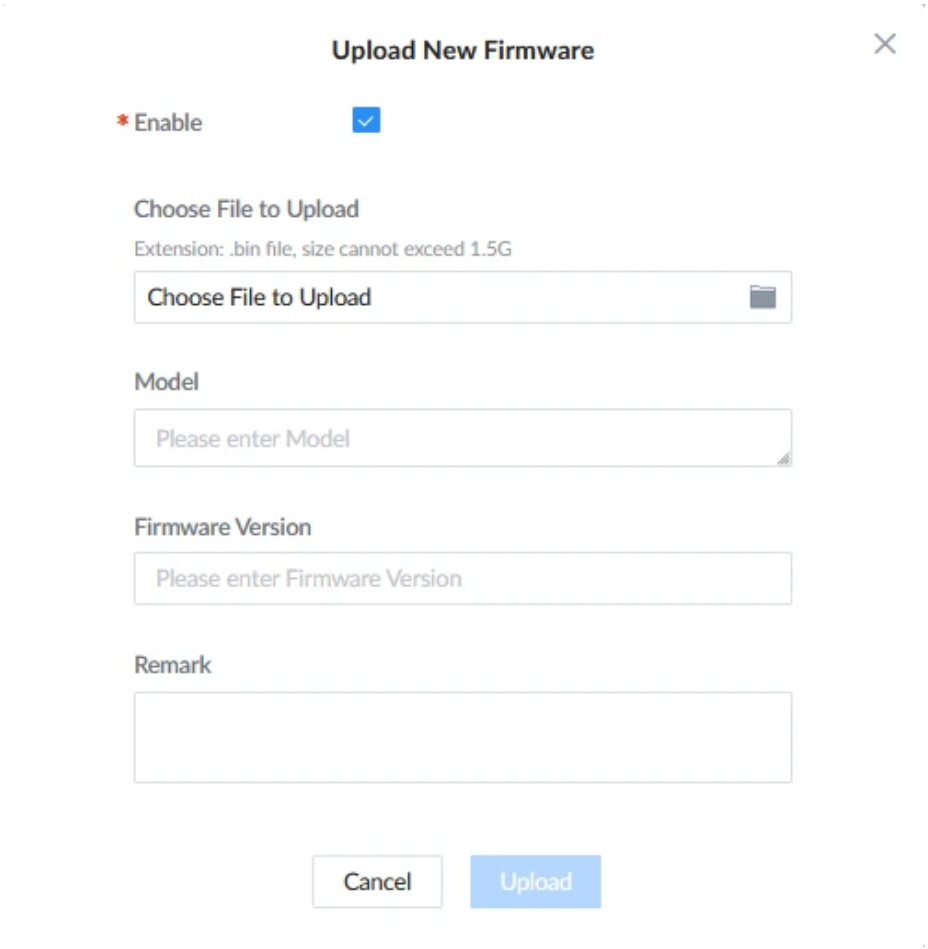
In the Firmware tab, users can upload and manage endpoint firmware. Upgrades can be performed per device or in batch across multiple managed IP phones and gateways.

The uploaded files must use the .bin extension and must not exceed 1.5 GB in size.



Firmware Zero Config Page

After clicking "Upload", a window appears displaying the configuration parameters below:



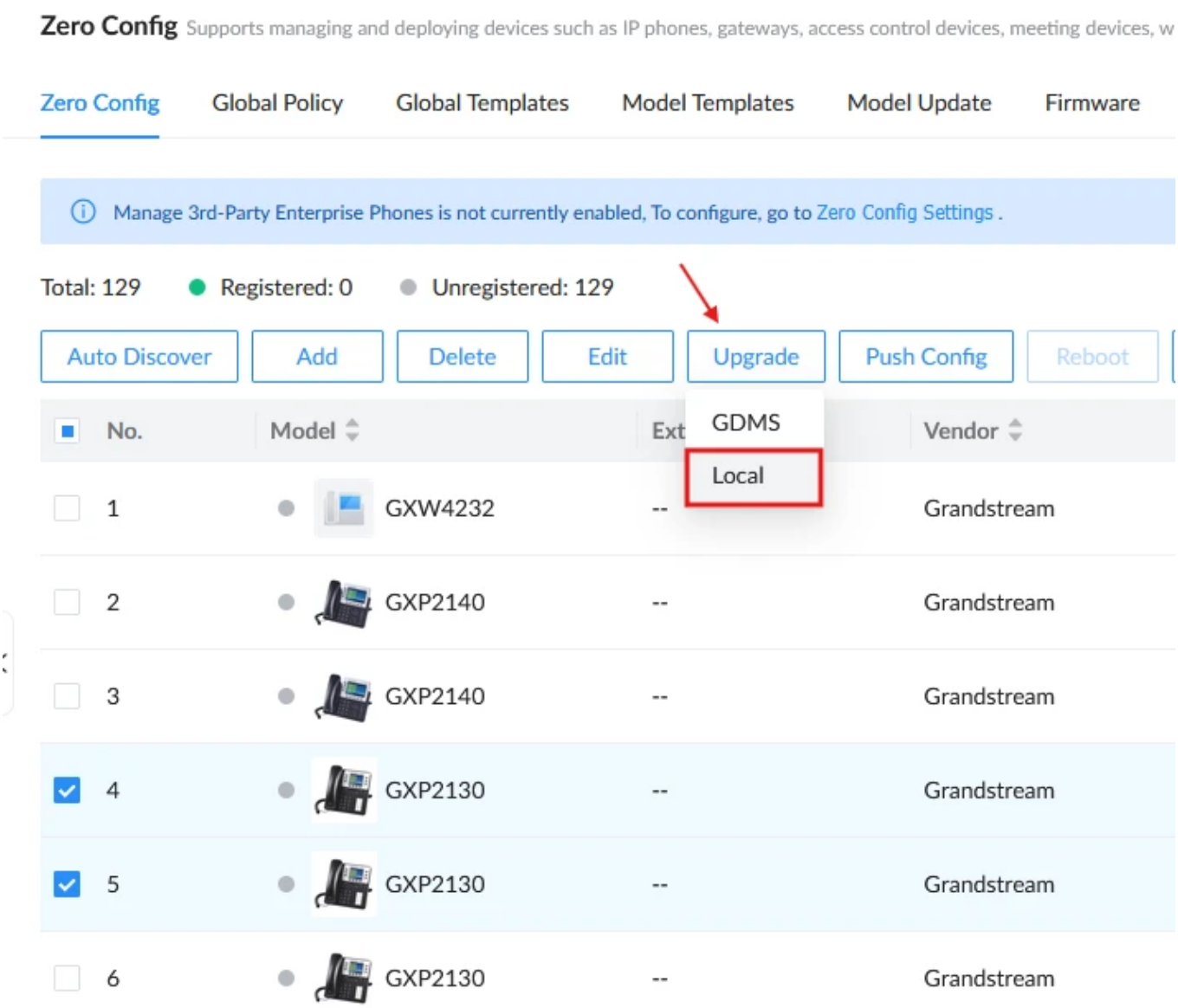
Upload New Firmware Window

Option	Description
Enable	Toggles whether the UCM will provision this firmware to endpoints using the UCM as their firmware server. If disabled, the UCM rejects firmware requests for this file.
Choose File to Upload	Select the firmware file to upload from the user's PC. The file name must match the firmware file name requested by the endpoint.
Model	The device model for which this firmware is intended. For self-reference only; has no effect on provisioning.
Firmware	The firmware version of the file being uploaded. For self-reference only; has no effect on provisioning.
Remark	Add a comment about the uploaded firmware. For self-reference only; has no effect on provisioning.

Administrators can perform local firmware updates across one or multiple managed IP phones and gateways simultaneously via Zero Config.

To execute a local firmware upgrade:

1. Navigate to **Extension/Trunk -> Zero Config -> Zero Config**.
2. Select the target devices from the device list using the checkboxes.
3. Click the **Upgrade** button dropdown and select **Local**.
4. Choose the desired locally uploaded firmware file from the prompt to trigger the upgrade across all selected targets.



Batch Local Firmware Upgrade Selection

Uploading Devices List

Besides the built-in discovery method on the UCM, users could prepare a list of devices on a xlsx or csv file and upload it by clicking on the button **"Import"**, after which a success message prompt should be displayed.

Users need to make sure that the CSV file respects the format as shown on the following figure and that the entered information is correct (valid IP address, valid MAC address, device model, and an existing account), otherwise the UCM will reject the file and the operation will fail:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	======== Device Start ========													
2	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
3		Grandstream	1	192.168.5.172		https://192.168.5.147:808		##########	000B82495	1.0.7.10	0	GXW4248	no	5060
4														
5	======== Device Start ========													
6	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
7		Grandstream	1	192.168.5.114		https://192.168.5.147:808		##########	000B826B	1.0.3.227	0	GXV3240	no	5060
8														
9	======== Device Start ========													
10	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
11		Grandstream	1	192.168.5.201		https://192.168.5.147:808		##########	000B826F9	1.0.1.106	0	--	no	5080

Device List - CSV file Sample

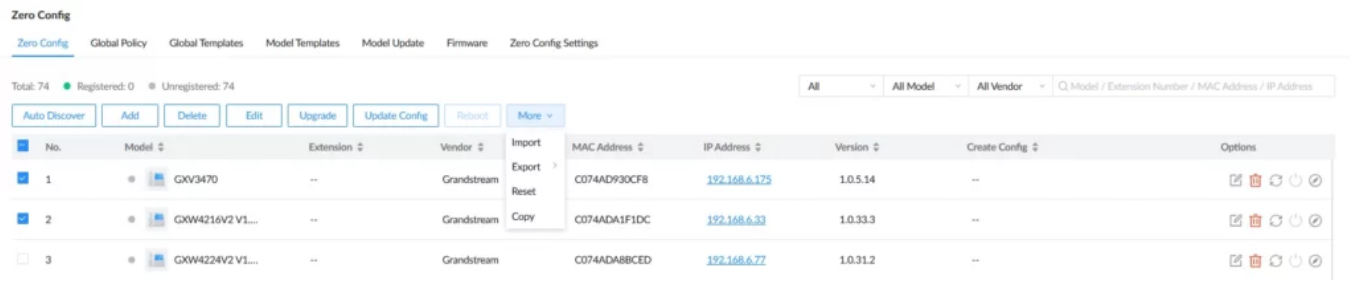
Please ensure that the file is encoded in UTF-8 to be able to import the devices correctly into the UCM.

Managing Discovered Devices

Users can manage the discovered devices in the Zero Config tab as follows:

- **Sorting:** Press or to sort per MAC Address, IP Address, Version, Vendor, Model or Create Config columns from lower to higher or higher to lower, respectively.
- **Filter:** Select a filter to display corresponding results. Users can filter by registration staus, models, or vendors. The "All" filter displays all discovered devices.
- **Search:** Search in the list of discovered devices by model, extension number, MAC address, or IP address.
- **Add:** Use the "Add" button to add a new device to the Zero Config database using its MAC address.
- **Delete:** Use the "Delete" button delete selected devices from the Zero Config database.
- **Edit:** Modify selected devices by clicking the "Edit" button.
- **Upgrade:** Upgrade the software of the discovered devices to the latest version. Select the devices which you want to upgrade. If no devices are selected, all the discovered devices will be upgraded.
- **Update Config:** Batch update a list of devices, the UCM on this case will send SIP NOTIFY message to all selected devices to update them at once.
- **Reboot:** Use the "Reboot" option for selected devices (the selected devices should have provisioned extensions since the phone will authenticate the server sending the reboot command).
- **More:** Perform additional action like:

  - **Import:** Import a list of devices. Devices with duplicate MAC addresses can either be skipped, replaced or updated. The imported file should be in CSV or XLSX format.
  - **Export**: Export the list of the discovered devices in CSV or XLS format. Select the devices before exporting. If no devices are selected, all the discovered devices will be exported.
  - **Reset:** Reset the discovered devices. Select the devices to reset before clicking this button. If no devices are selected, all the discovered devices will be reset to their initial configuration.
  - **Copy:** Copy the configuration across devices.



Managing Discovered Devices

Global Configuration

The global configuration will apply to all the connected SIP endpoint devices in the same LAN with the UCM630x regardless of the device model. It is divided into two levels:

- **Global Policy**

- **Global Templates**

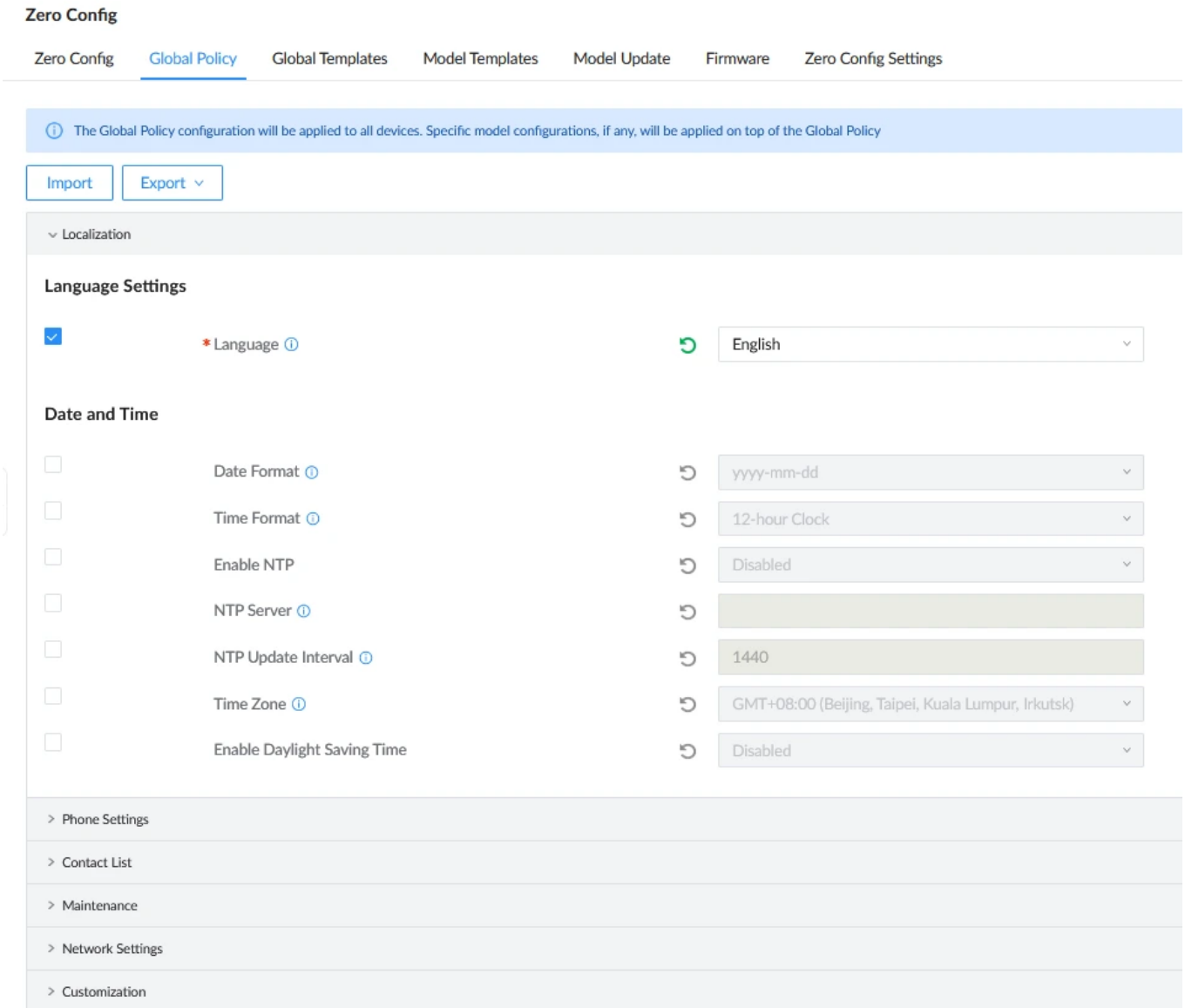
Global Templates configuration has higher priority to Global Policy configuration.

Global Policy

Global Policy can be accessed in **Device Management**->**Zero Config**->**Global Policy** page. On the top of the configuration table, users can select a category in the "Options" dropdown list to quickly navigate to the category or they can also complete the configuration by importing/exporting. The categories are:

- **Localization**: configure display language, data, and time.
- **Phone Settings**: configure the dial plan, call features, NAT,call progress tones, etc.
- **Contact List**: configure LDAP and XML phonebook download.
- **Maintenance**: configure upgrading, web access, Telnet/SSH access, and Syslog.
- **Network Settings**: configure the IP address, QoS, and STUN settings.
- **Customization**: customize LCD screen wallpaper for the supported models.
- **Communication Settings**: configure Email and FTP settings

Select the checkbox on the left of the parameter you would like to configure to activate the dropdown list for this parameter.



Global Policy Page

The following tables list the Global Policy configuration parameters for the SIP end device sorted by category.

Language Settings	
Language	Select the LCD language on the SIP device.
Date and Time	
Date Format	Configure the date display format on the SIP end device's LCD.
Time Format	Configure the time display in 12-hour format on the SIP end device's LCD.
Enable NTP	Enables NTP service.
NTP Server	Configure the URL or IP address of the NTP server. The SIP device may obtain the date and time from the server.
NTP Update Interval	Configure the NTP update interval.
Time Zone	Configure the time zone used on the SIP end device.
Enable Daylight Time	Select either to enable or disable the DST.

Global Policy Parameters - Localization

Default Call Settings	
Dial Plan	Configure the default dial plan rule. For syntax and examples, please refer to the user manual of the SIP devices to be provisioned for more details.
Enable Call Features	When enabled, "Do Not Disturb", "Call Forward" and other call features can be used via the local feature code on the phone. Otherwise, the ITSP feature code will be used.
Use # as Dial Key	If set to "Yes", pressing the number key "#" will immediately dial out the input digits.
Auto Answer by Call-info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info header sent from the server/proxy. The default setting is enabled.
NAT Traversal	Configure if NAT traversal mechanism is activated.
User Random Port	If set to "Yes", this parameter will force random generation of both the local SIP and RTP ports.
General Settings	
Call Progress Tones	Configure call progress tones including ring tone, dial tone, second dial tone, message waiting tone, ring back tone, call waiting tone, busy tone, and reorder tone using the following syntax: f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; Frequencies are in Hz and cadence on and off are in 10ms). "on" is the period (in ms) of ringing while "off" is the period of silence. Up to three cadences are supported. Please refer to the user manual of the SIP devices to be provisioned for more details
HEADSET Key Mode	Select "Default Mode" or "Toggle Headset/Speaker" for the Headset key. Please refer to the user manual of the SIP devices to be provisioned for more details.

Global Policy Parameters - Phone Settings

LDAP Phonebook	
Source	Select "Manual" or "PBX" as the LDAP configuration source. If "Manual" is selected, the LDAP configuration below will be applied to the SIP end device. If "PBX" is selected, the LDAP configuration built-in from UCM630X Web GUI→System Settings→LDAP Server will be applied.

Address	Configure the IP address or DNS name of the LDAP server.
Port	Configure the LDAP server port. The default value is 389.
Base DN	This is the location in the directory where the search is requested to begin. Example: dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com
Username	Configure the bind "Username" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Password	Configure the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Number Filter	Configure the filter used for number lookups. Please refer to the user manual for more details.
Name Filter	Configure the filter used for name lookups. Please refer to the user manual for more details.
Version	Select the protocol version for the phone to send the bind requests. The default value is 3.
Name Attribute	Specify the "name" attributes of each record that are returned in the LDAP search result. Example: gn cn sn description
Number Attribute	Specify the "number" attributes of each record that are returned in the LDAP search result. Example: telephoneNumber telephoneNumber Mobile
Display Name	Configure the entry information to be shown on the phone's LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber
Max Hits	Specify the maximum number of results to be returned by the LDAP server. The valid range is 1 to 3000. The default value is 50.
Search Timeout	Specify the interval (in seconds) for the server to process the request and the client waits for the server to return. The valid range is 0 to 180. The default value is 30.
Sort Results	Specify whether the searching result is sorted or not. The default setting is No.
Incoming Calls	Configure to enable LDAP number searching when receiving calls. The default setting is No.
Outgoing Calls	Configure to enable LDAP number searching when making calls. The default setting is No.
Lookup Display Name	Configures the display name when LDAP looks up the name for an incoming call or outgoing call. It must be a subset of the LDAP Name Attributes.
XML Phonebook	
Phonebook XML Server	Select the source of the phonebook XML server. Disable Disable phonebook XML downloading. Manual Once selected, users need to specify downloading protocol HTTP, HTTPS, or TFTP and the server path to download the phonebook XML file. The server path could be an IP address or URL, with up to 256 characters. Local UCM Server Once selected, click on the Server Path field to upload the phonebook XML file. Please note after uploading the phonebook XML file to the server, the original file name will be used as the directory name and the file will be renamed as phonebook.xml under that directory.
Phonebook Download Interval	Configure the phonebook download interval (in minutes). If set to 0, the automatic download will be disabled. The valid range is 5 to 720.
Remove manually edited entries on download	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed.

Global Policy Parameters - Contact List

Upgrade and Provision

Firmware Source	Firmware source via ZeroConfig provisioning could be a URL for external server address, local UCM directory, or USB media if plugged into the UCM630X. Select a source to get the firmware file: URL If selected to use URL to upgrade, complete the configuration for the following four parameters: "Upgrade Via", "Server Path", "File Prefix" and "File Postfix". Local UCM Server Firmware can be uploaded to the UCM630X internal storage for firmware upgrade. If selected, click on the "Manage Storage" icon next to the "Directory" option, upload the firmware file, and select a directory for the end device to retrieve the firmware file. Local USB Media If selected, the USB storage device needs to be plugged into the UCM630X and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory. Local SD Card Media If selected, an SD card needs to be plugged into the UCM630X and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory.
Upgrade via	When URL is selected as firmware source, configure upgrade via TFTP, HTTP, or HTTPS.
Server Path	When URL is selected as firmware source, configure the firmware upgrading server path.
File Prefix	Configure the Config Server Path.
Config Server Path	When URL is selected as firmware source, configure the firmware file postfix. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Allow DHCP Option 43/66	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
Automatic Upgrade	If enabled, the end point device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week, or by minute. By week Once selected, specify the day of the week to check the HTTP/TFTP server for firmware upgrades or configuration files changes. By day Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes. By minute Once selected, specify the interval X that the SIP end device will request for new firmware every X minutes.
Firmware Upgrade Rule	Specify how firmware upgrading and provisioning requests are to be sent.
Zero Config	Select either to enable or disable Zero Config.
Web Access	
Admin Password	Configure the administrator password for admin-level login.
End-User Password	Configure the end-user password for the end-user level login.
Web Access Mode	Select HTTP or HTTPS as the web access protocol.
Web Server Port	Configure the port for web access. The valid range is 1 to 65535.
RTSP Port	Configure the RTSP Port.
Enable UPnP Discovery	Select either to enable or disable Enable UPnP Discovery
Login Settings	Configure the login settings.
User Login Timeout	Configure User Login Timeout.
Maximum Consecutive Failed Login Attempts	Configure Maximum Consecutive Failed Login Attempts.
Login Error Lock Time	Configure Login Error Lock Time.
Security	
Disable Telnet/SSH	Enable Telnet/SSH access for the SIP end device. If the SIP end device supports Telnet access, this option controls the Telnet access of the device; if the SIP end device supports SSH access, this option controls the SSH access of the device.
Syslog	
Syslog Server	Configure the URL/IP address for the Syslog server.

Syslog Level	Select the level of logging for Syslog.
Send SIP Log	Configure whether the SIP log will be included in the Syslog message.

Global Policy Parameters - Maintenance

Basic Settings	
IP Address	Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected. DHCP Once selected, users can specify the Host Name (option 12) of the SIP end device as DHCP client, and Vendor Class ID (option 60) used by the client and server to exchange vendor class ID information. PPPoE Once selected, users need to specify the Account ID, Password, and Service Name for PPPoE.
Host Name	Specify the name of the client. This field is optional but may be required by Internet Service Providers.
Vendor Class ID	Used by clients and servers to exchange vendor class ID.
Account ID	Enter the PPPoE account ID.
Password	Enter the PPPoE Password.
Service Name	Enter the PPPoE Service Name.
Advanced Setting	
Layer 3 QoS	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv, or MPLS. The valid range is 0-63.
Layer 3 QoS For RTP	Assign the priority value of the Layer 3 QoS for RTP packets. The valid range is 0 -63.
Layer 3 QoS For SIP	Assign the priority value of the Layer 3 QoS for SIP packets. The valid range is 0 -63.
Layer 2 QoS Tag	Assign the VLAN Tag of the Layer 2 QoS packets. The valid range is 0 -4095.
Layer 2 QoS Priority Value	Assign the priority value of the Layer 2 QoS packets. The valid range is 0-7.
STUN Server	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Keep-Alive	Select either to enable or disable Keep Alive.
Keep Alive Interval	Specify how often the phone will send a blank UDP packet to the SIP server to keep the "ping hole" on the NAT router open. The valid range is 10-160.
Register Expiration	Specify the Register Expiration.
Local SIP Port	Configure Local SIP Port.
Local RTP Port	Configure Local RTP Port.
Auto On-Hook Timer(s)	Configure Auto On-Hook Timer(s).
Ring Timeout	Configure Ring Timeout.
SIP Transport	Select either UDP, TCP, or TLS/TCP as SIP transport protocol.
Direct IP Call	Select either to disable or enable Direct IP Call support.
SIP Proxy Compatibility Mode	Select either to disable or enable SIP Proxy Compatibility Mode.
Unregister On Reboot	Select either to disable or enable Unregister On Reboot.
Whitelist	
Whitelist	Select either to enable or disable Whitelist

SIP Phone Number Whitelist	Configure the SIP Phone Number Whitelist.

Global Policy Parameters - Network Settings

Email Settings	
SMTP Settings	Check this option to configure the email settings that will be sent to the provisioned phones: Server The IP address of the SMTP server Port SMTP server port From E-Mail address Email address Sender Username Username of the sender Password Recovery Email Email where the recovered password will be sent Alarm receive Email 1 Email address where alarms notifications will be sent Alarm receive Email 1 Email address where alarms notifications will be sent Enable SSL Enable SSL protocol for SMTP
FTP	
FTP	Check this option to configure the FTP settings that will be sent to the provisioned phones: Storage Server Type Either FTP or Central Storage Server FTP server address Port FTP port to be used Username FTP username Path FTP Directory path

Global Policy Parameters - Customization

Wallpaper	
Screen Resolution 1024 x 600	Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 800 x 400	Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 480 x 272	Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 320 x 240	Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.

Global Policy Parameters - Communication Settings

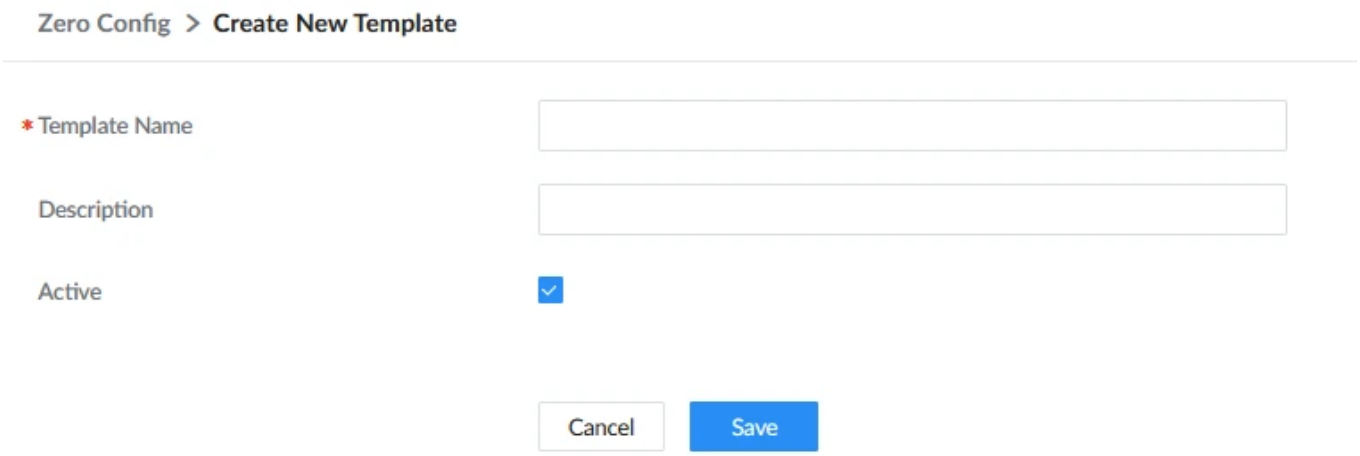
Global Templates

Global Templates can be accessed in **Device Management**->**Zero Config**->**Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates, or click on the "Import/Export" button to add multiple global templates.

When the user configures the device in the **Edit Device dialog->Advanced Settings**, they can select to use one of the global templates for the device. Please refer to section **[Manage Devices]** for more details on using the global templates.

When creating a Global Template, users can select the categories and specific parameters within each category to include in the template. Both the Global Policy and the selected Global Template are applied when generating the configuration file. However, for overlapping configuration options, the Global Template takes precedence over the Global Policy.

1. Click on "Add" to add a global template. Users will see the following configurations.

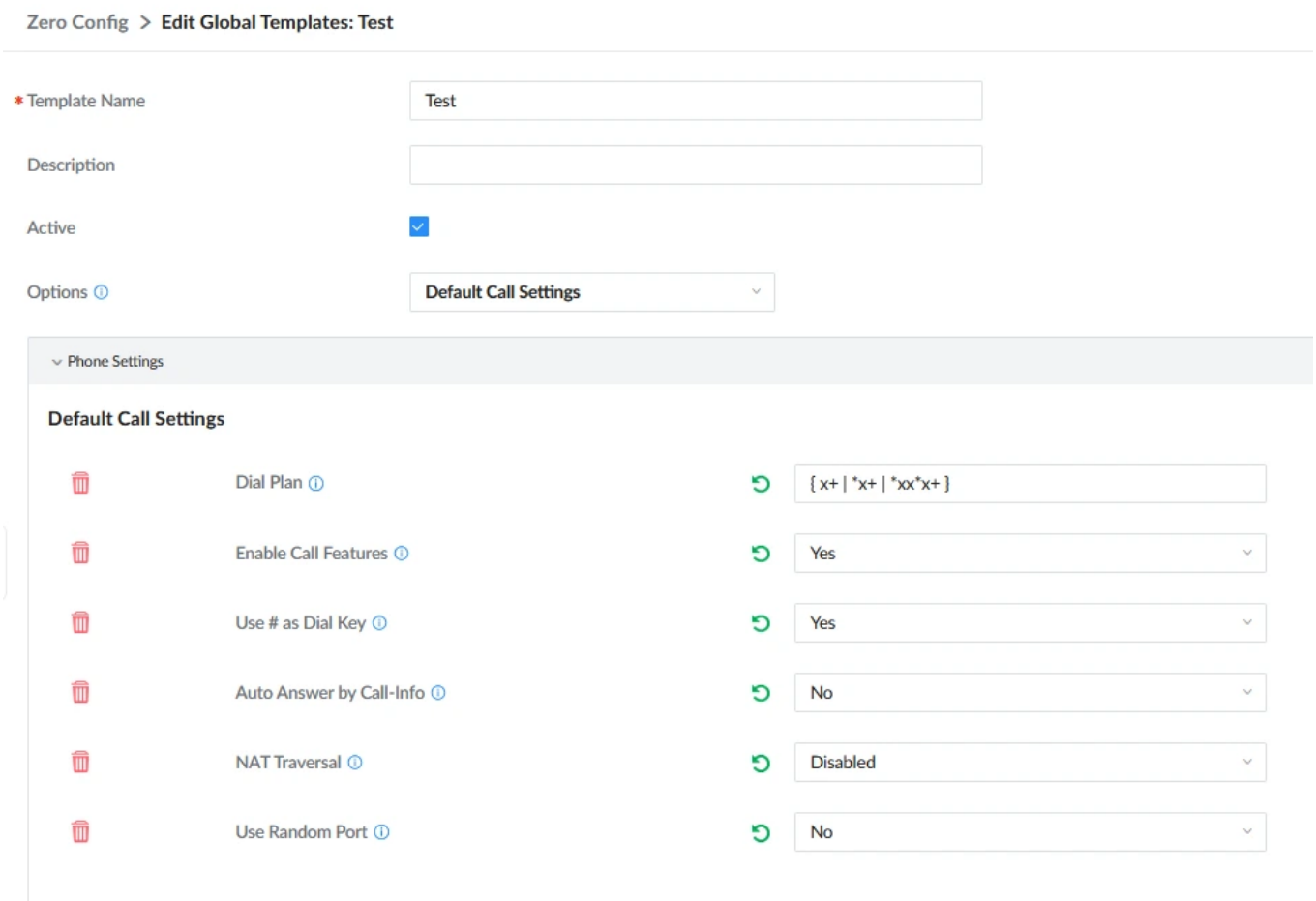


Create New Global Template

Template Name	Create a name to identify this global template.
Description	Describe the global template. This is optional.
Active	Check this option to enable the global template.

Create New Template

2. Click on the "Edit" icon to edit the global template.
3. In the "Options" field, after entering the option name keyword, the options containing the keyword will be listed. Users could then select the options to be modified under the global template.



Global Template Configuration Settings

1. Enter or select the value for each option to be used in the global template.

2. On the left side of each added option, click the "Trash" icon to delete this option from the template, or click on the "Reset" icon to reset the option value to the default value.
3. Click on "Save" to save this global template.

The created global templates will show in the **Device Management->Zero Config->Global Templates** page. Users can delete one or multiple templates or click on "Toggle Selected Template Status" to toggle between enabled/disable status for the selected templates.

Model Configuration

Model templates

The Model layer configuration allows users to apply model-specific settings to devices. Users can create, edit, or delete Model Templates through the Web GUI at **Device Management->Zero Config->Model Templates**.

If multiple Model Templates are created and enabled, users can select a specific template for a device in the **Edit Device** dialog under **Advanced Settings**. The selected Model Template is then applied to that device.

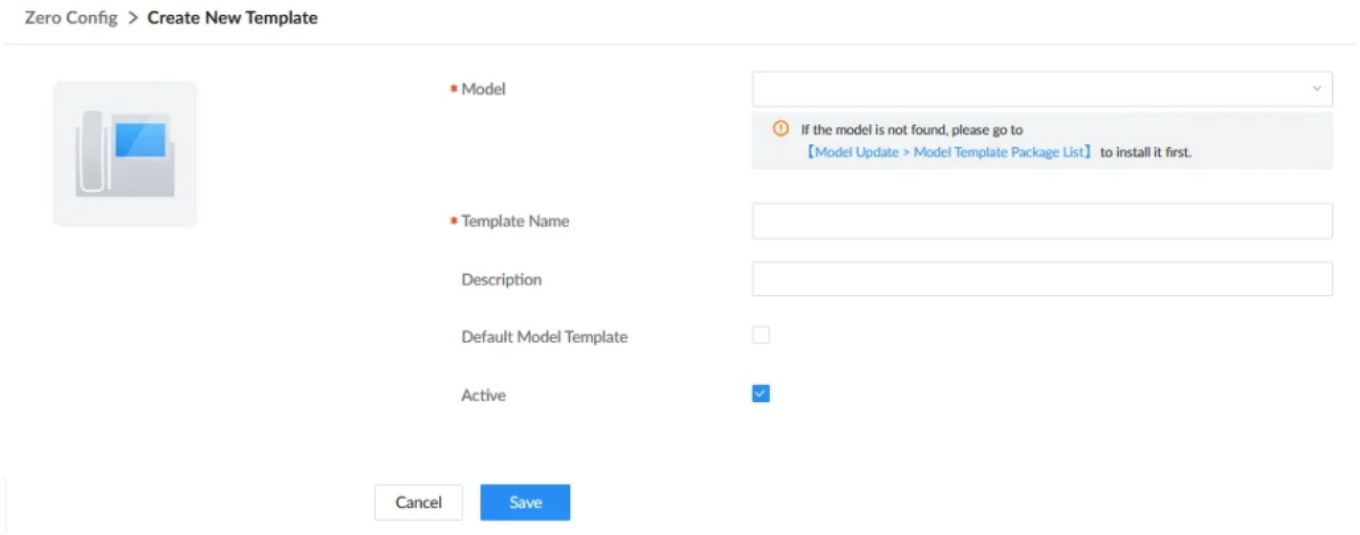
For each Model Template, users can designate it as the default template. When a Model Template is set as the default, its configuration values are applied to all devices of the corresponding model.

Only one default Model Template can be assigned at any given time on the UCM630x.

Both the default Model Template and the selected Model Template are applied during configuration generation. For overlapping options, the selected Model Template takes precedence and overrides the default Model Template.

To configure a model template:

1. Click on "Add" to add a model template, and configure the following parameters:

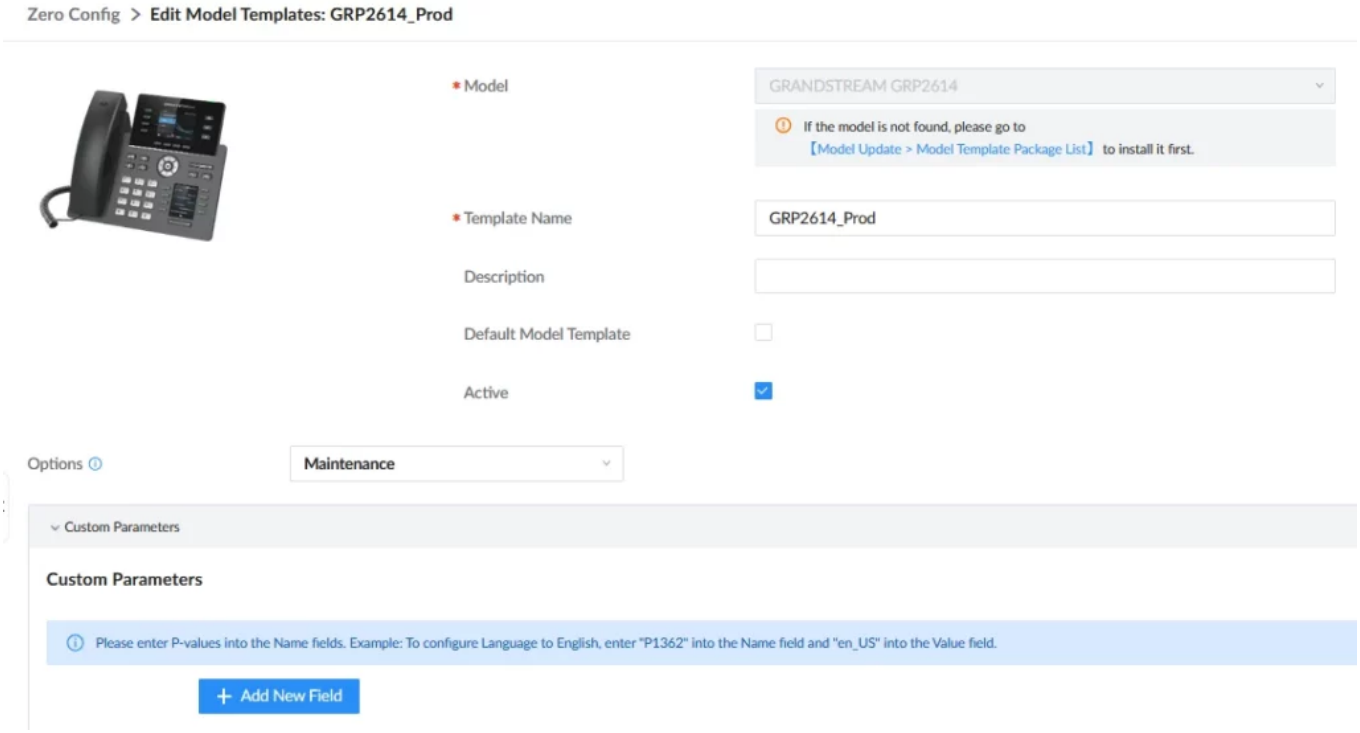


Create New Model Template

Model	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
Template Name	Create a name for the model template.
Description	Enter a description for the model template. This is optional.
Default Model Template	Select to assign this model template as the default model template. The value of the option in the default model template will be overridden if another selected model template has a different value for the same option.
Active	Check this option to enable the model template.

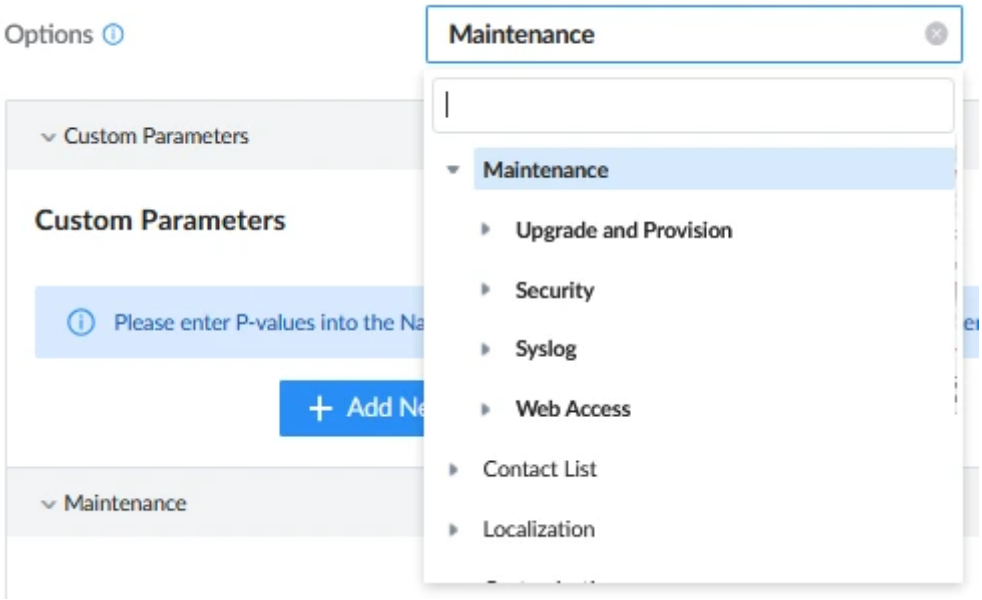
Create New Model Template

2. Click on the "Edit" icon to edit the model template. The editing window for a model template is shown in the following figure.



Edit Model Template

3. On the left side of each added option, click the "Trash" icon to delete this option from the template, or click on the "Reset" icon to reset the option value to the default value.
4. In the "Options" field, enter the option name key word, the option that contains the keyword will be listed. The user could then select the option to be modified under the model template.



Model Template Options

5. Use "Add New Field" to add a P-value number and the value to the configuration. The following figure shows setting P-value "P1362" to "en", which means the display language on the LCD is set to English.

For P-value information of different models, please refer to the configuration template here

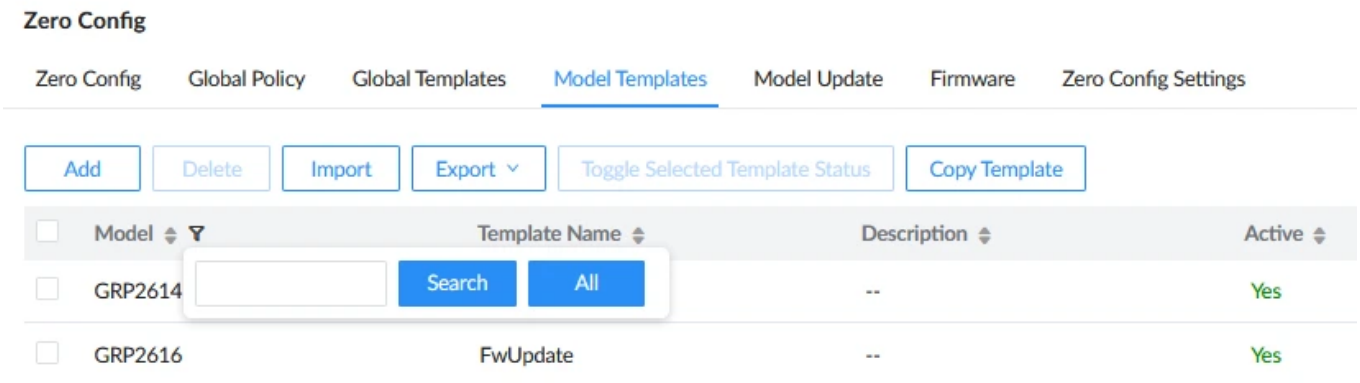
http://www.grandstream.com/support/tools



Custom Model Template Prameters

6. Click on Save when done. The model template will be displayed on **Device Management**->**Zero Config**->**Model Templates** page.
7. Click on the "Trash" icon to delete the model template or use the "Delete" button delete multiple selected templates at once.
8. Click on "Toggle Selected Template Status" to toggle between enabled/disable status for the selected templates.
9. Use the "Import/Export" buttons to upload/export the model template list in CSV or XLS format.

The filter option allows to search through the model templates. Please see the screenshot below:



Model Template Search Filter

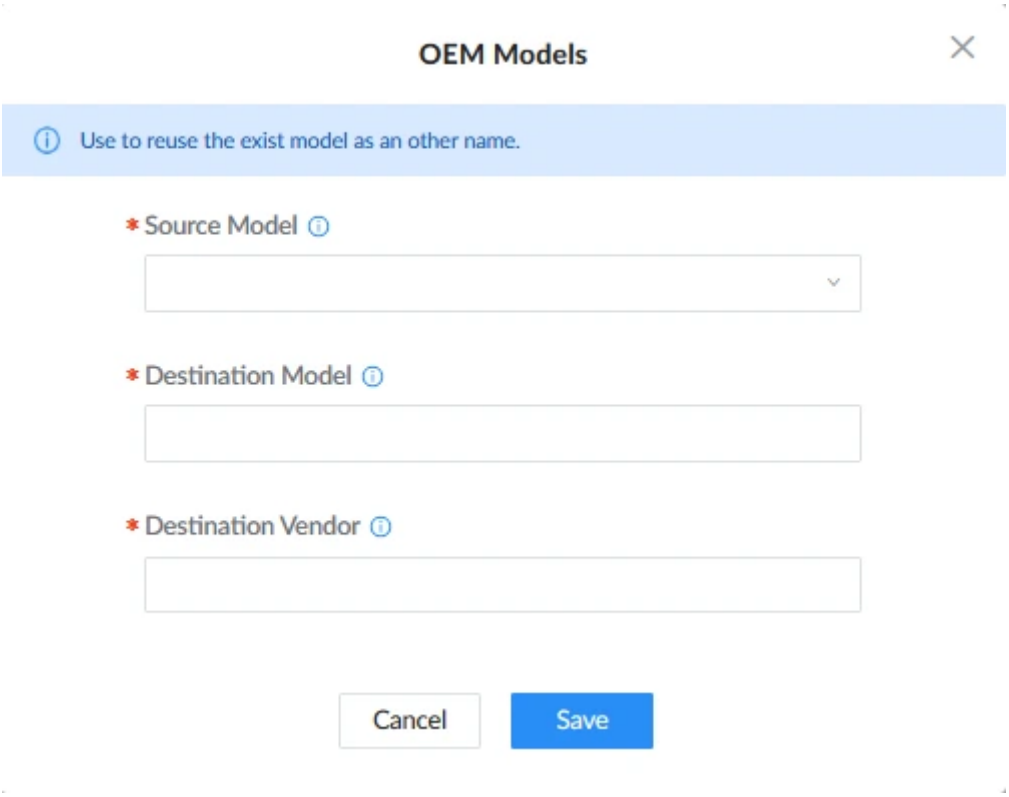
Model Update

UCM630x Zero Config feature supports provisioning all models of Grandstream SIP end devices including OEM device models, and supported third-party models.

OEM Models

Users can associate OEM device models with their original Grandstream-branded models, allowing these OEM devices to be provisioned appropriately.

1. Click on "Add OEM Models" button.
2. In the Source Model field, select the Grandstream device that the OEM model is based on from the dropdown list.
3. For the Destination Model and Destination Vendor field, enter the custom OEM model name and vendor name.
4. The newly added OEM model should now be selectable as an option in Model fields.



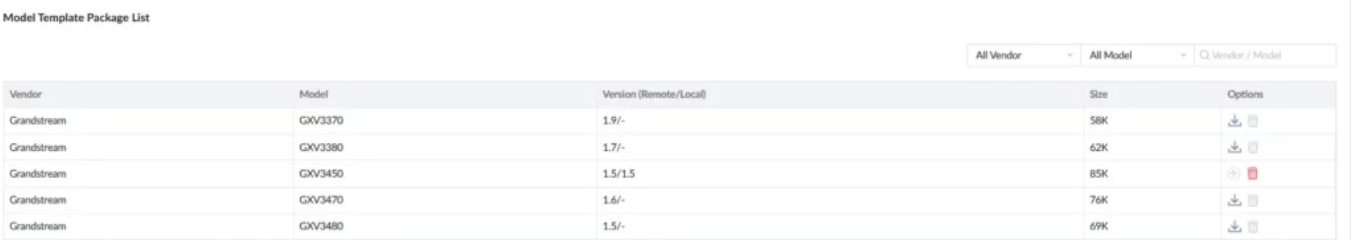
Add OEM Models

Model Template Package List

Templates for most of the Grandstream models are built-in with the UCM630X already. Templates for Wave, Grandstream surveillance products, and third-party devices require users to download and install under **Device Management**->**Zero Config**->**Model Update** first before they are available in the UCM630X for selection.

After downloading and installing the model template to the UCM630x, it will show in the dropdown list for "Model" selection when editing the model template.

1. Click on the "Download" icon to download the template.
2. Click on "Upgrade" to upgrade an existing model template.



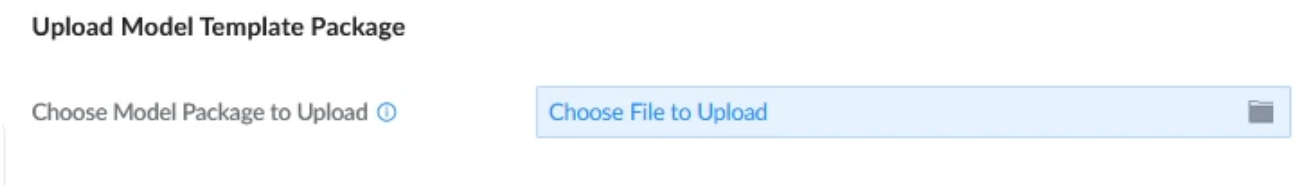
Model Template Package List

Upload Model Template Package

By default, third-party model templates are not available on the UCM630x and must be uploaded manually through the Web GUI.

In environments with restricted Internet connectivity, Grandstream model packages must also be uploaded manually.

Contact Grandstream customer support to obtain the required model template packages.



Upload Model Template Package

Device Configuration

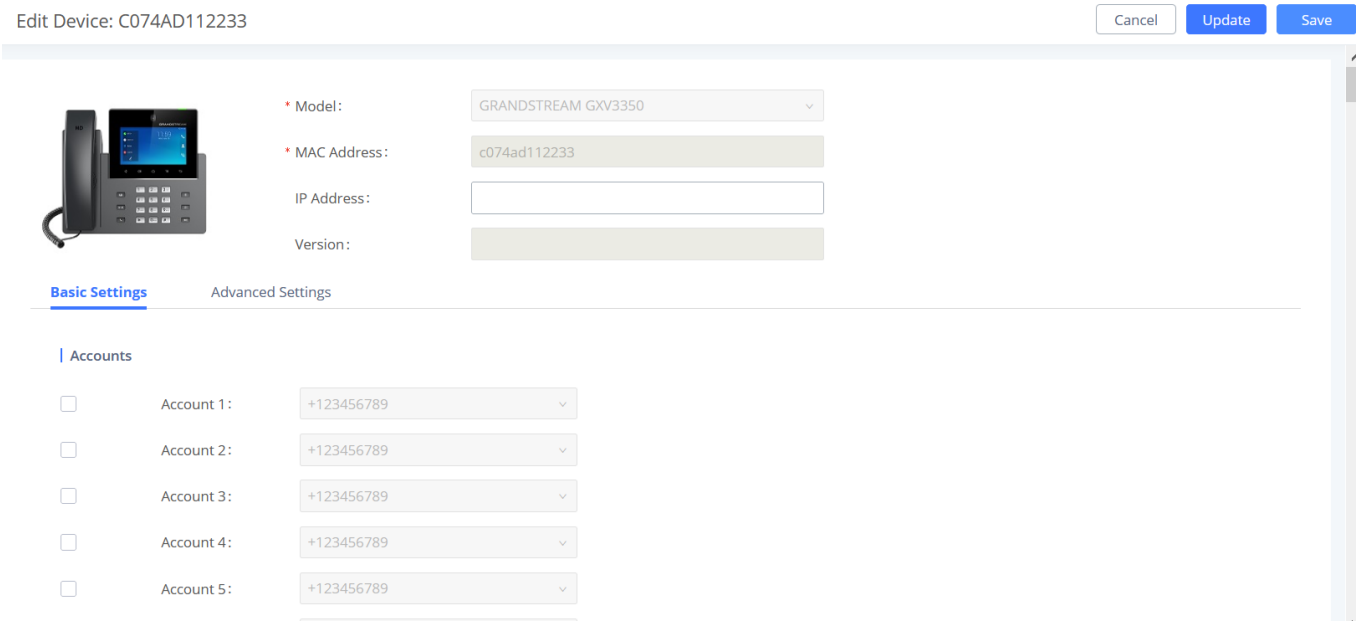
On Web GUI, page **Device Management**->**Zero Config->Zero Config**, users could create a new device, delete existing device(s), make special configuration for a single device, or send NOTIFY to an existing device(s).

Create New Device

Users can directly create a new device and configure basic settings before the device is discovered by the UCM630X. Once the device is plugged in, it can then be discovered and provisioned. This gives the system administrator adequate time to set up each device beforehand.

Click on "Add" and the following dialog will show. Follow the steps below to create the configurations for the new device.

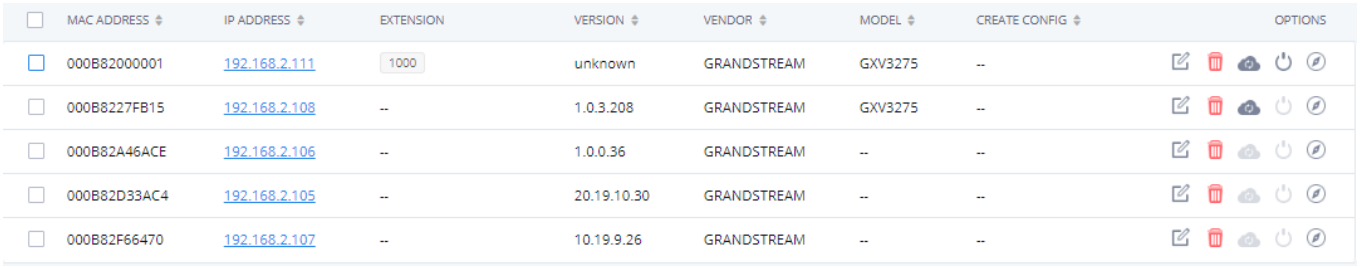
1. Firstly, select a model for the device to be created and enter its MAC address, IP address, and firmware version (optional) in the corresponding field.
2. Basic settings will show a list of settings based on the model selected in step 1. Users could assign extensions to accounts, assign functions to Line Keys and Multiple-Purposed Keys if supported on the selected model.
3. Click on "Save" to save the configuration for this device.



Create New Device

Manage Devices

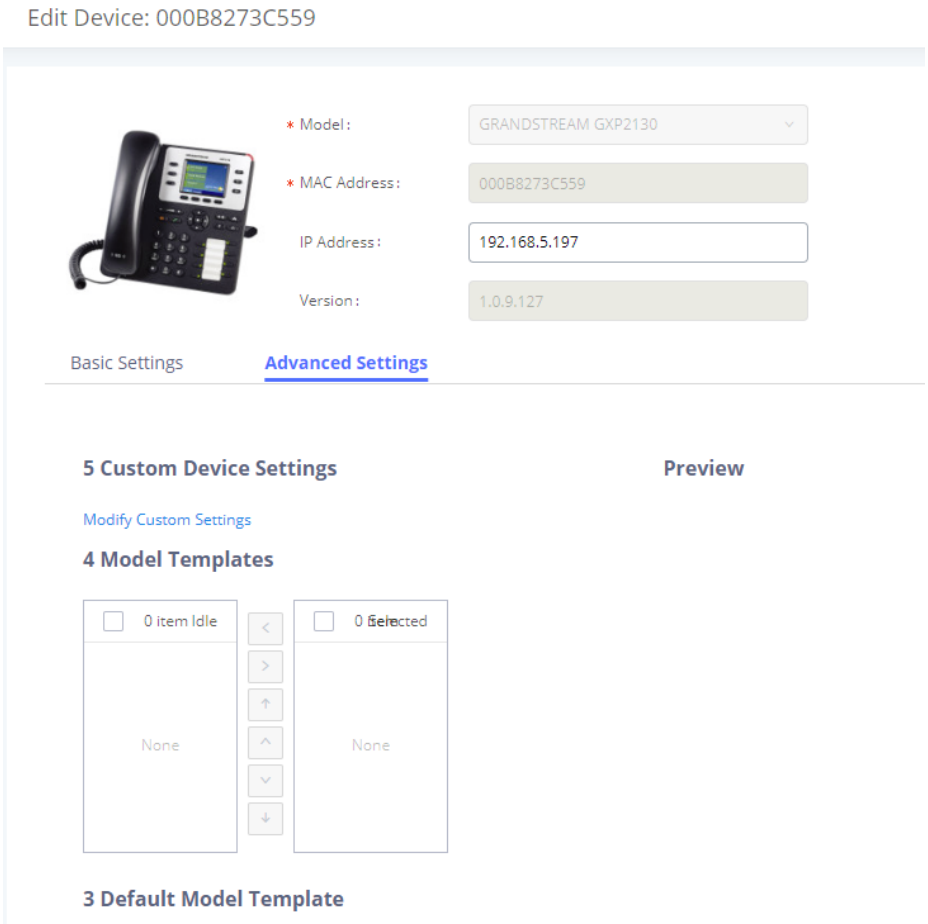
The device manually created or discovered from Auto Discover will be listed in the **Device Management**-> **Zero Config**->**Zero Config** page. Users can see the devices with their MAC address, IP address, vendor, model, etc.



Manage Devices

- Click on "Access Device Web UI" to access the Web GUI of the device.
- Click on the "Edit" icon to edit the device configuration.

A new dialog will be displayed for the users to configure "Basic" settings and "Advanced" settings. "Basic" settings have the same configurations as displayed when manually creating a new device, i.e., account, line key, and MPK settings; "Advanced" settings allow users to configure more details in a five-level structure.



Edit Device

A preview of the **Advanced Settings** is shown in the figure above. There are five configuration levels, as described in items (1) through (5) below, ordered from lowest to highest priority. All configuration levels are applied to the device.

If the same option is defined at multiple levels with different values, the value from the higher-priority level overrides the value from the lower-priority level.

1. Global Policy

This is the lowest level configuration. The global policy configured in **Device Management**->**Zero Config**->**Global Policy** will be applied here. Clicking on "Modify Global Policy" to redirect to page **Device Management**->**Zero Config**->**Global Policy**.

2. Global Templates

Select a Global Template and click the right arrow to add it to the device. Multiple Global Templates can be selected, and their priority can be adjusted using the up and down arrows. All selected templates take effect.

If the same option is defined in multiple selected Global Templates, the value from the higher-priority template overrides that of the lower-priority template. Click the left arrow to remove a Global Template from the selected list.

3. Default Model Template

Default Model Template will be applied to the devices of this model. Default model template can be configured in the model template under **Device Management**->**Zero Config**->**Model Templates** page. Please see the default model template option in **[Create New Model Template].**

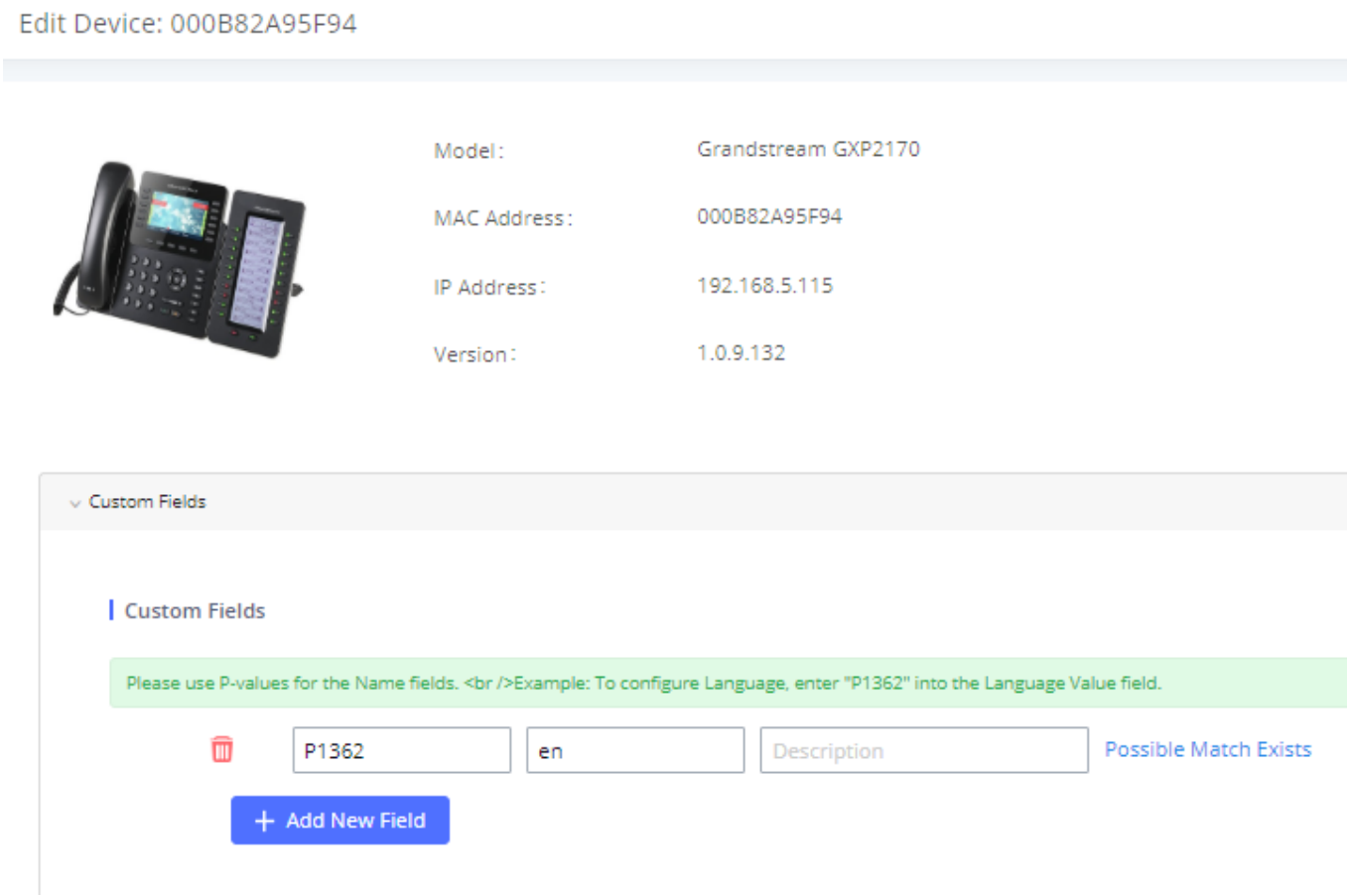
4. Model Templates

Select a Model Template to apply to the device and click the right arrow to add it. Multiple Model Templates can be selected, and their priority can be adjusted using the up and down arrows. All selected templates take effect.

If the same option is defined in multiple selected Model Templates, the value from the higher-priority template overrides that of the lower-priority template. Click the left arrow to remove a Model Template from the selected list.

5. Customize Device Settings

This is the highest-level configuration for the device. Click on "Modify Customize Device Settings" and the following dialog will show.



Edit Customize Device Settings

Scroll down in the dialog to view and edit device-specific options. To add options that are not included in the predefined list, click **Add New Field** and specify the P-value and its corresponding value.

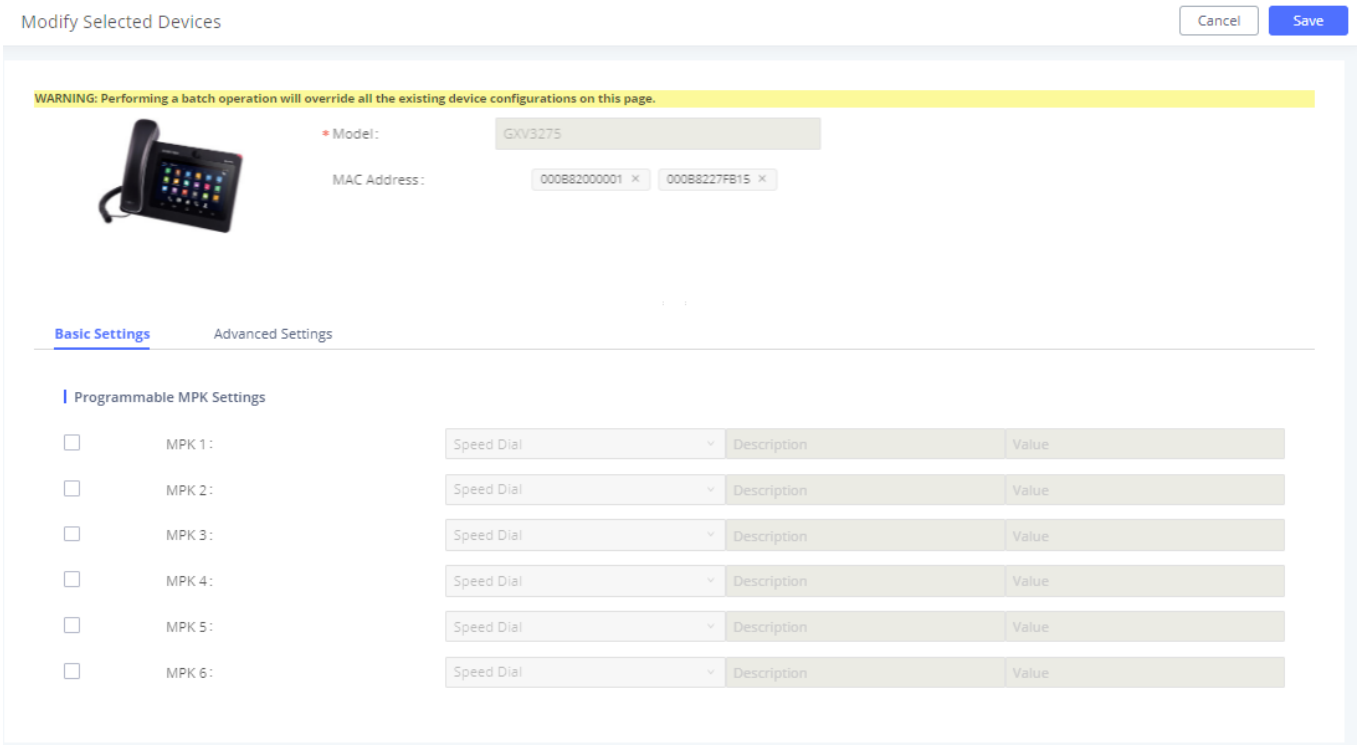
In the example shown above, P-value **P1362** is set to **en**, which configures the LCD display language to English. The warning message on the right indicates that a predefined option matching this P-value already

exists; clicking it navigates to the corresponding option.

For P-value information of different models, please refer to the configuration template here http://www.grandstream.com/support/tools

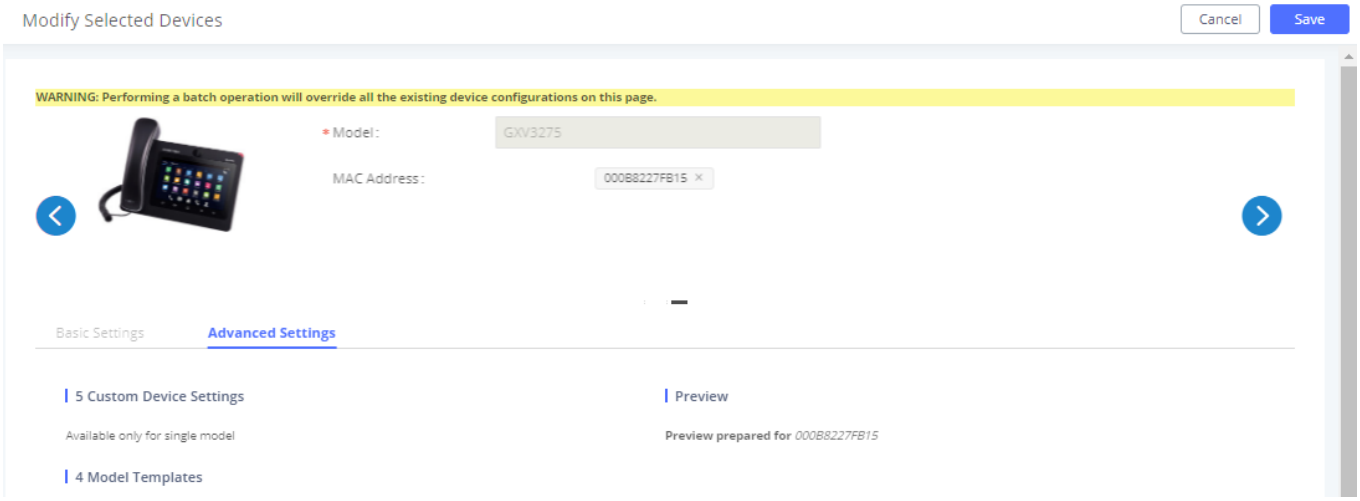
Select multiple devices that need to be modified and then click on "Update Config" to batch modify devices.

If selected devices are of the same model, the configuration dialog is like the following figure. Configurations in five levels are all available for users to modify.



Modify Selected Devices - Same Model

If selected devices are of different models, the configuration dialog is like the following figure. Click on the arrows to view more devices of other models. Users are only allowed to make modifications to the Global Templates and Global Policy level.



Modify Selected Devices - Different Models

Performing batch operation will override all the existing device configuration on the page.

After the above configurations, save the changes and go back to **Device Management**->**Zero Config**->**Zero**

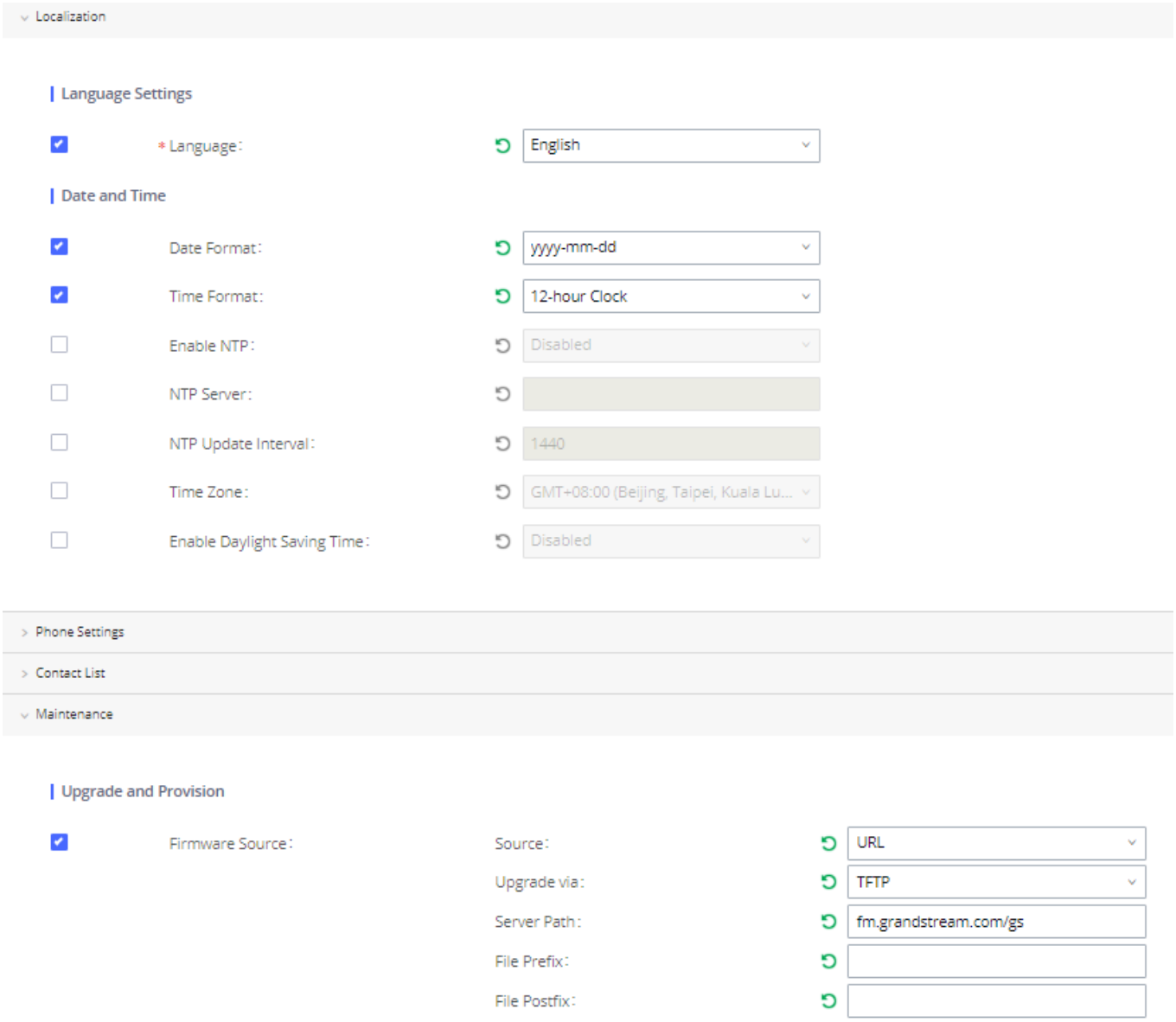
Config page. Users could then click on the "Update" icon to send NOTIFY to the SIP end point device and trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.

On this web page, users can also click on "Reset All Extensions" to reset the extensions of all the devices.

Sample Application

Assuming in a small business office where there are 8 GXP2140 phones used by customer support and 1 GXV3275 phone used by customer support supervisor. 3 of the 8 customer support members speak Spanish and the rest speak English. We could deploy the following configurations to provision the office phones for the customer support team.

1. Go to **Device Management**->**Zero Config**->**Zero Config Settings**, select "Enable Zero Config".
2. Go to **Device Management**->**Zero Config**->**Global Policy**, configure Date Format, Time Format, and Firmware Source as follows.

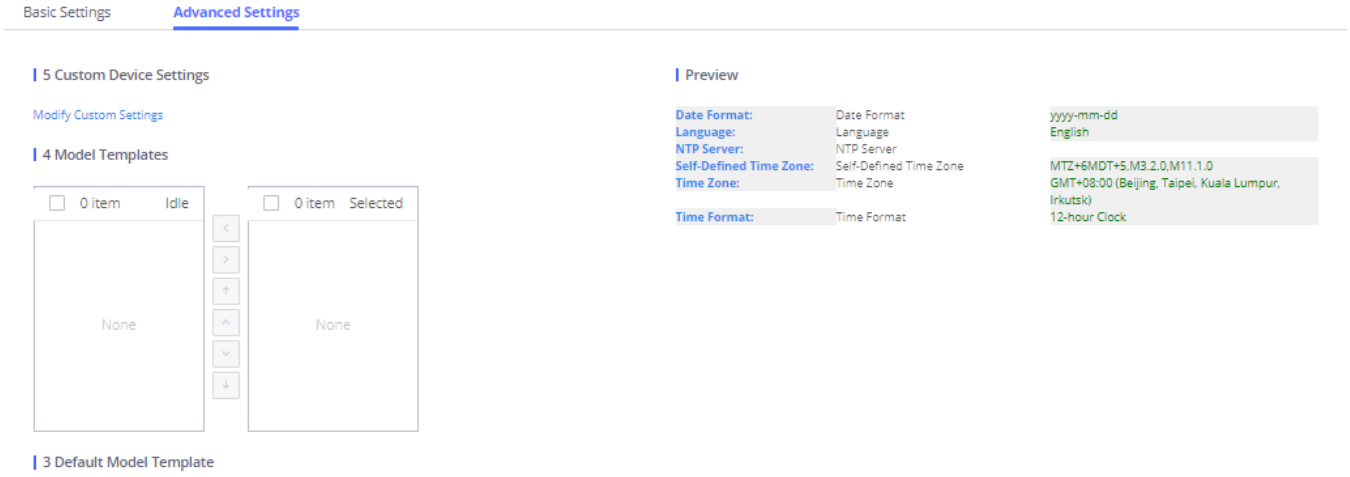


Zero Config Sample - Global Policy

3. Go to **Device Management**->**Zero Config->Model Templates**, create a new model template "English Support Template" for GXP2170. Add option "Language" and set it to "English". Then select the option

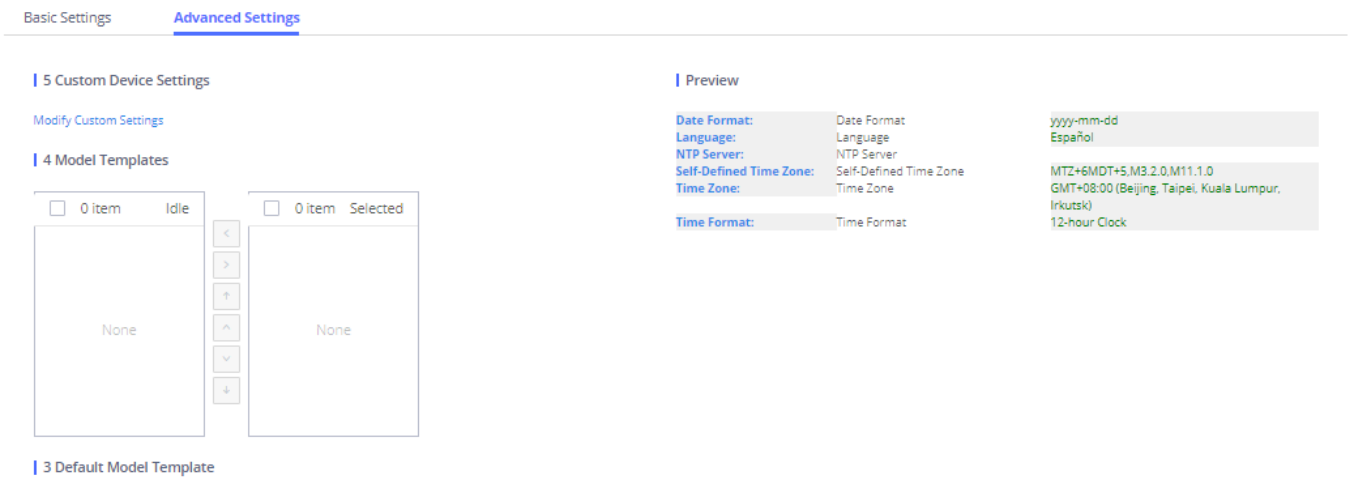
"Default Model Template" to make it the default model template.

4. Go to **Device Management**->**Zero Config ->Model Templates**, create another model template "Spanish Support Template" for GXP2170. Add option "Language" and set it to "Espanol".
5. After 9 devices are powered up and connected to the LAN network, use the "Auto Discover" function or "Create New Device" function to add the devices to the device list on **Device Management**->**Zero Config** ->**Zero Config**.
6. On Web GUI->**Device Management**->**Zero Config**->**Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on the "Edit" icon to edit the device settings.
7. For each of the 5 phones used by English-speaking customer support, in "Basic settings" select an available extension for account 1 and click on "Save". Then click on the "Advanced settings" tab to bring up the following dialog. Users will see the English support template is applied since this is the default model template. A preview of the device settings will be listed on the right side.



Zero Config Sample - Device Preview 1

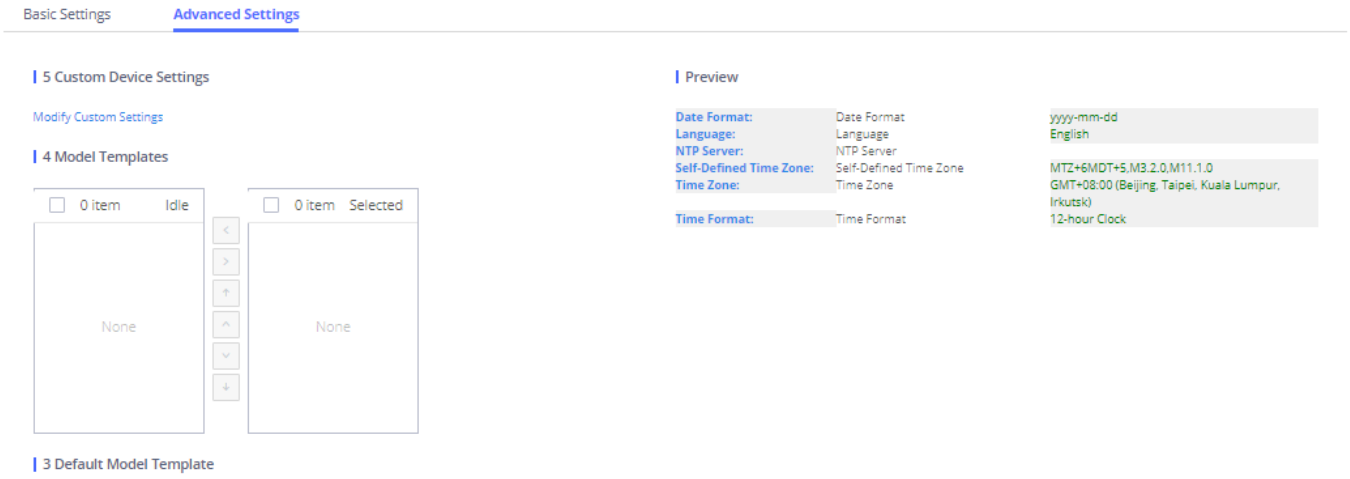
8. For the 3 phones used by Spanish support, in "Basic settings" select an available extension for account 1 and click on "Save". Then click on the "Advanced settings" tab to bring up the following dialog.



Zero Config Sample - Device Preview 2

9. Select "Spanish Support Template" in "Model Template". The preview of the device settings is displayed on the right side and we can see the language is set to "Espanol" since Model Template has the higher priority for the option "Language", which overrides the value configured in the default model template.
10. For the GXV3275 used by the customer support supervisor, select an available extension for account 1 on "Basic settings" and click on "Save". Users can see the preview of the device configuration in "Advanced

settings". There is no model template configured for GXV3275.



Zero Config Sample - Device Preview 3

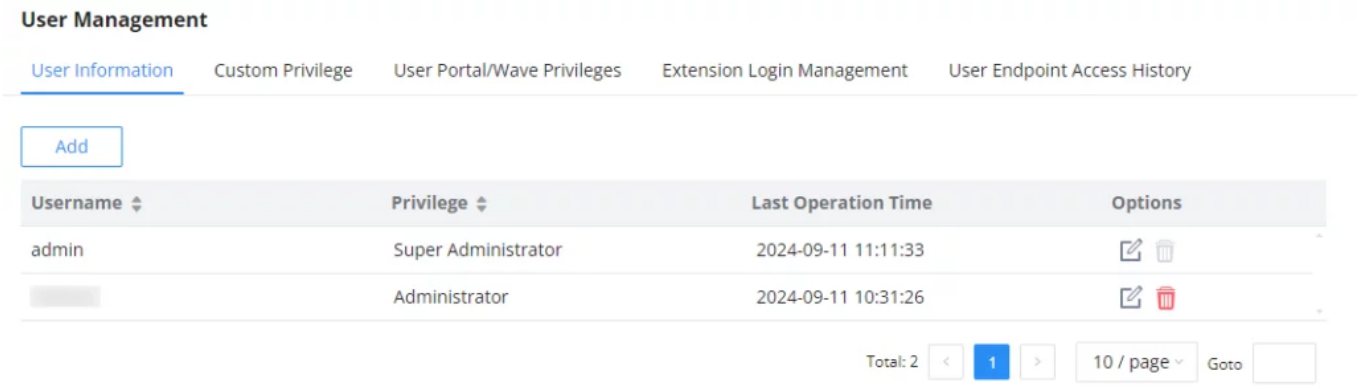
11. Click on "Apply Changes" to apply saved changes.
12. On the **Device Management**->**Zero Config**->**Zero Config** page, click on the "Update" icon to send NOTIFY to trigger the device to download the config file from UCM630x.

Now all the 9 phones in the network will be provisioned with a unique extension registered on the UCM630X. 3 of the phones will be provisioned to display Spanish on LCD and the other 5 will be provisioned to display English on LCD. The GXV3275 used by the supervisor will be provisioned to use the default language on the LCD display since it is not specified in the global policy.

MAINTENANCE

User Management

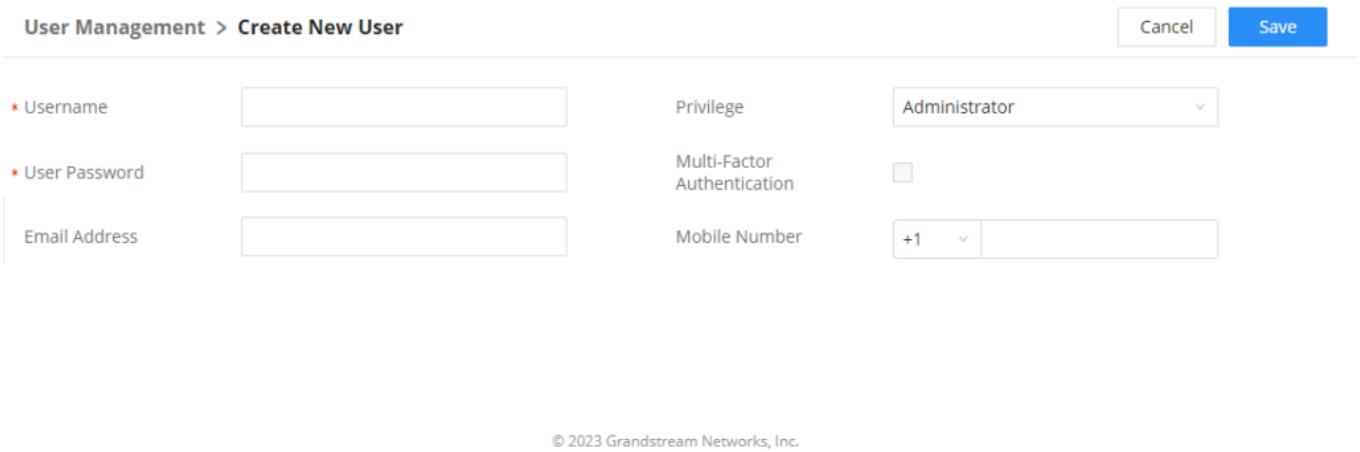
User management is on **Maintenance > User Management** page. User could create multiple accounts for different administrators to log in the UCM630X Web GUI. Additionally, the system will automatically create user accounts along with creating new extensions for extension users to login to the Web GUI using their extension number and password. All existing user accounts for Web GUI login will be displayed on User Management page as shown in the following figure.



User Management Page Display

User Information

When logged in as Super Admin, click on "Add" to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.



Create New User

Username	Configure a username to identify the user which will be required in Web GUI login. Letters, digits, and underscore are allowed in the username.
User Password	Configure a password for this user which will be required in Web GUI login. English input is allowed without space,' and ". Note: The password should contain at least 10 characters, with at least, one lower-case letter, one upper-case letter, one numeral, and one special character.
Email Address	Configure the email address for the user. This is optional.
Privilege	This is the role of the Web GUI user. When super admin creates new user, "Adminstrator" or customized privilege can be selected.
Multi-Factor Authentication	If enabled, the user account will be required to enter an MFA code in addition to login credentials when logging into the UCM management web portal.
Mobile Number	The user's mobile phone number. This can be used for scenarios such as SMS verification code login and resetting password. It is recommended to configure country code to avoid potential SMS sending issues.

When the super admin creates new user, the email address for the new user is optional. However, when the admin user created by super admin logs in to edit user information, email address is mandatory. This email address is the same and will be sync up with the email address configured in login settings.

Once created, the Super Admin can edit the users by clicking on or delete the user by clicking on .

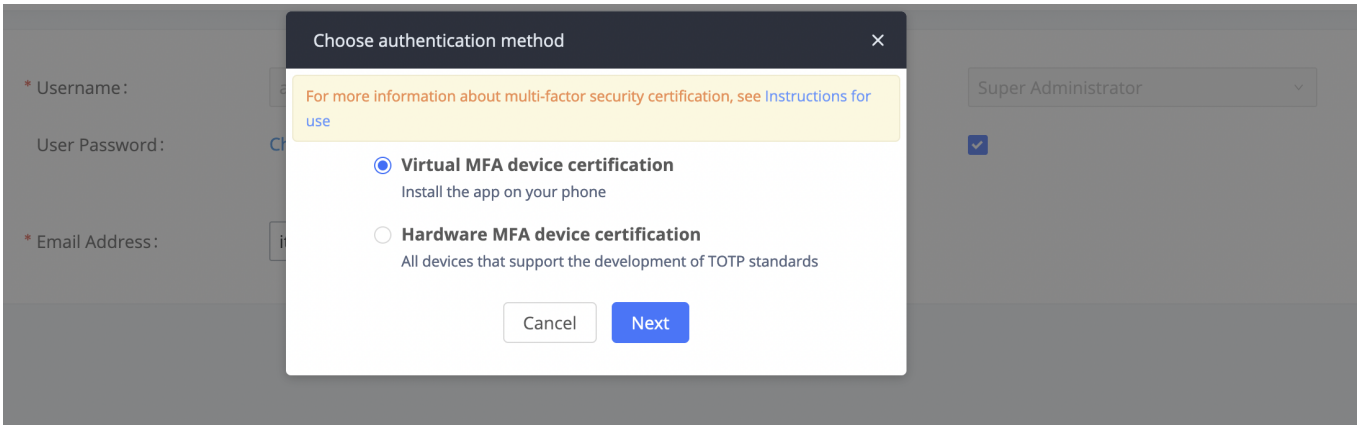
Multi-Factor Authentication

To enhance the security for UCM, super admin and admin can select to use multi-factor authentication method for login to protect the login information. Virtual MFA and hardware MFA are supported and can be selected. Once enabled, the user must use MFA code to verify before login.

- The user cannot enable or disable MFA for another different user.
- Super admin can edit user settings for admin but cannot edit Multi-Factor Authentication option. MFA option is only viewable for super admin when super admin edits other users.
- When the user sees MFA enabled, only this user can disable or enable it again.
- Email address and email settings are required before enabling Multi-Factor Authentication. Please ensure email setting has "Client" type configured. Otherwise, MFA cannot be enabled.
- If a "Client" type email server is configured on the UCM and the administrator or extension user has not enabled MFA, a reminder is added near the user's own MFA switch, stating that the device supports MFA

and that it can be enabled to improve account security.

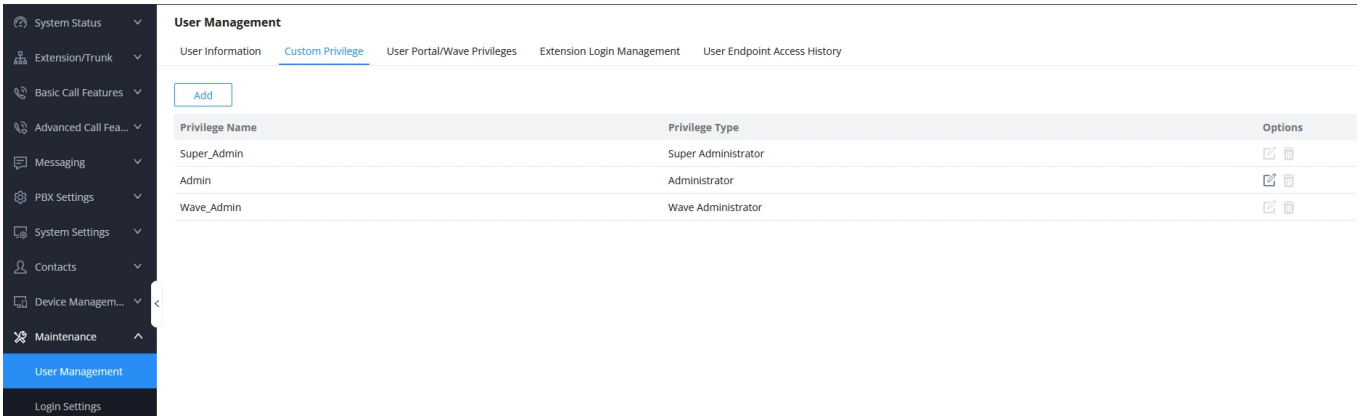
Please refer to MFA how to guide here for more information.



MFA Settings

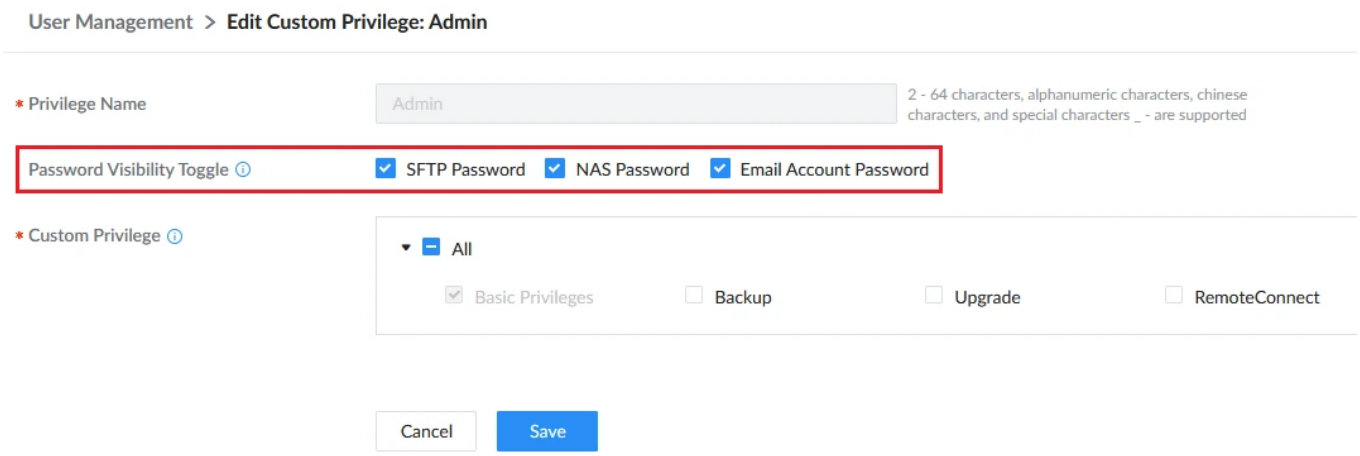
Custom Privilege

By default, three levels are supported: **Super Administrator**, **Administrator**, **Wave Administrator**:



Super Administrator

- This is the highest privilege. Super Admin can access all pages on UCM630X Web GUI, change configuration for all options and execute all the operations.
- Super Admin can create, edit, and delete one or more users with the "Admin" privilege
- Super Admin can edit and delete one or more users with the "Consumer" privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account "admin" is configured with the "Super Admin" privilege and it is the only user with the "Super Admin" privilege. The Username and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on **Maintenance**->**Login Settings** page.
- Super Admin could view operations done by all the users in **Maintenance**->**User Management->Operation Log**
- The Super Admin can allow administrators to view SFTP, NAS and Email Account passwords.



Password Visibility Toggle

Administrator

- Users with "Admin" privilege can only be created by "Super Admin" user.
- "Admin" privilege users cannot create new users for login.
- "Admin" privilege users are by default not allowed to access the following pages:

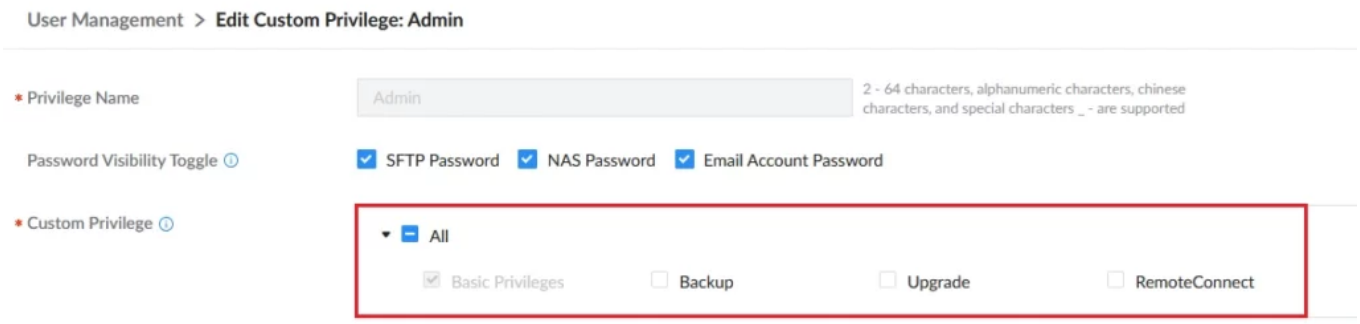
Maintenance → Backup

Maintenance → Upgrade

RemoteConnect

Settings→User Management→Operation Log

Note: By default, administrator accounts are not allowed to access backup menu, but this can be assigned to them by editing the option "**Maintenance**->**User Management**->**Custom Privilege**" then press the "Edit" icon to edit the "Admin" account and include backup operation permission for these types of users.

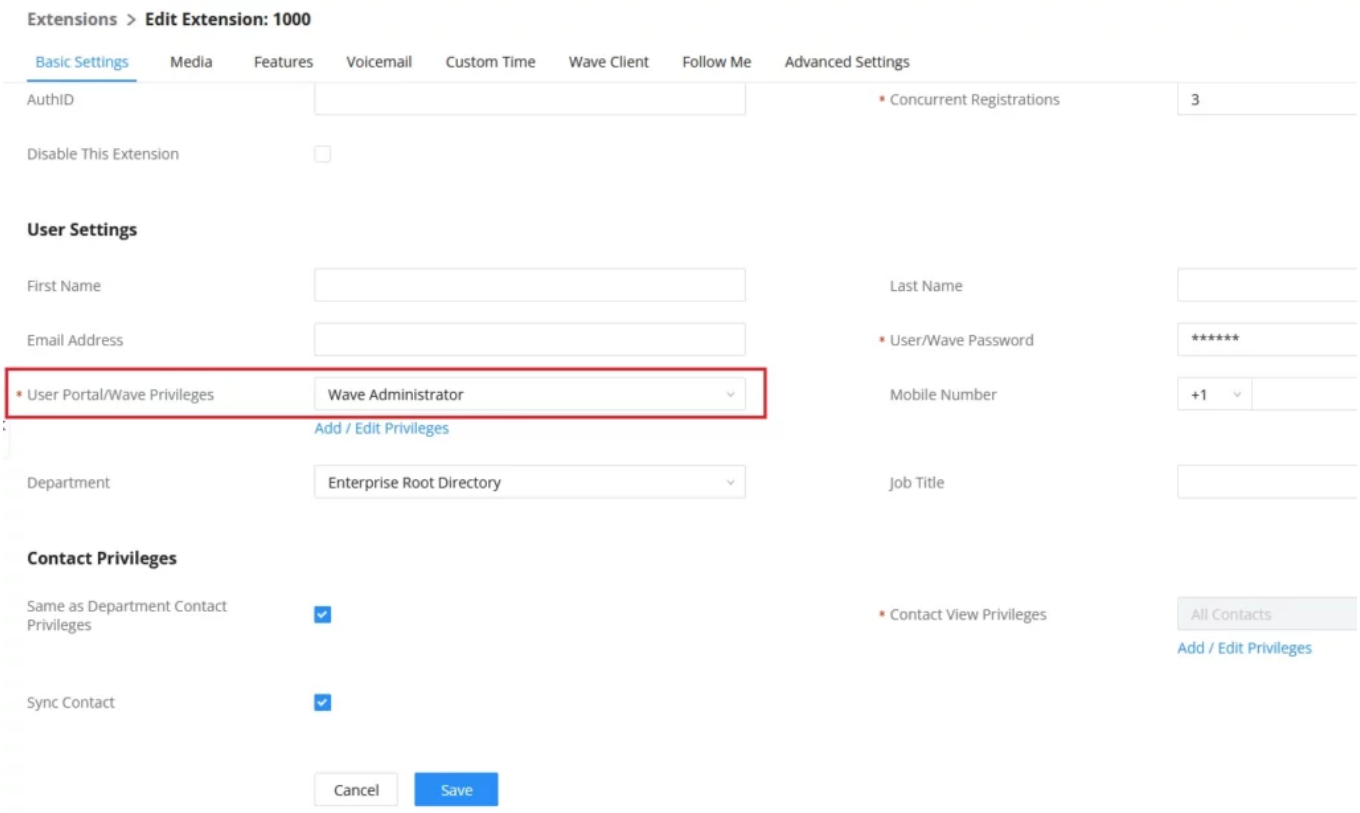


Assigning Permissions to "Admin" Users

Wave Administrator

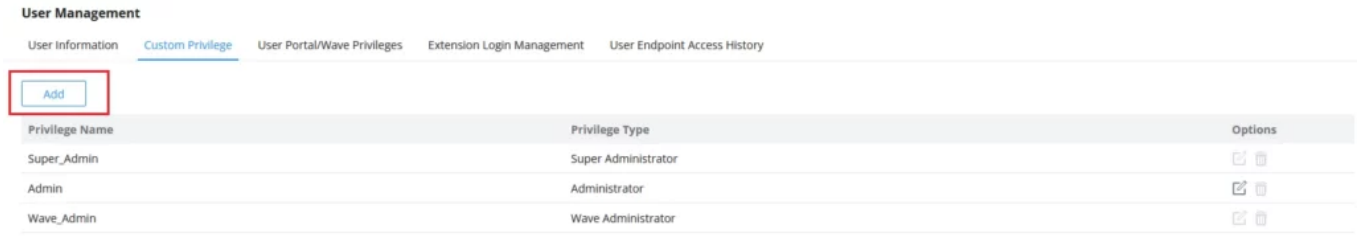
- This permission type does not support editing or deletion.
- This includes management of Wave-related function settings only and does not involve access to the UCM module.
- Users can set the Wave Admin privilege for specific extension under **Extension/Trunk->Extensions->Edit Extension**.

For more information, please refer to the Wave Administrator Guide guide.



Add Custom Privilege

The Super Admin can create customized user privileges to grant sub-administrators or specific users access to select Web GUI configuration modules and operational tools. Custom privileges are configured under **Maintenance -> User Management -> Custom Privilege**.

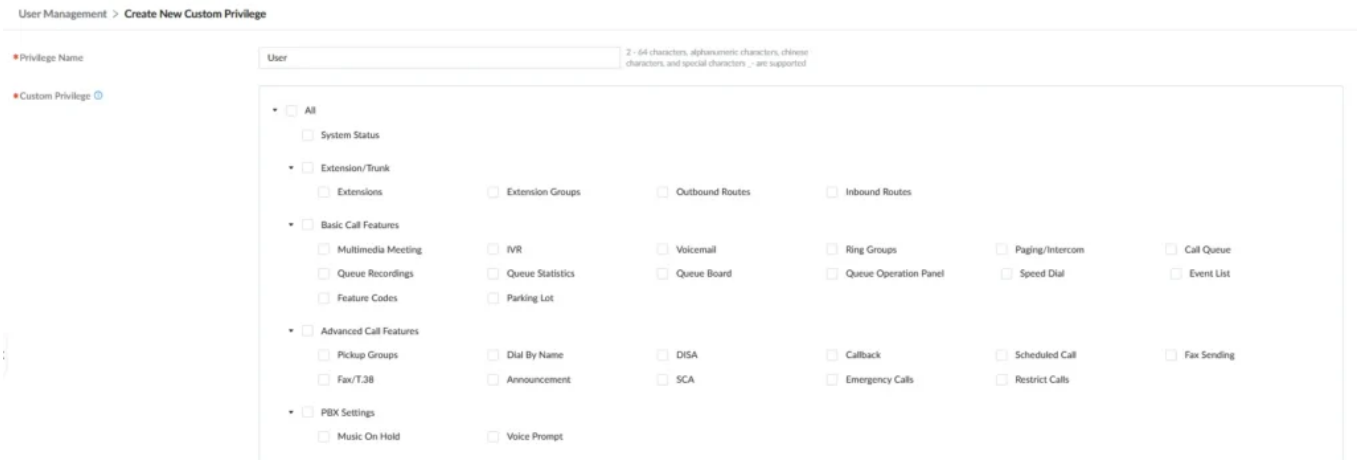


Custom Privilege Management

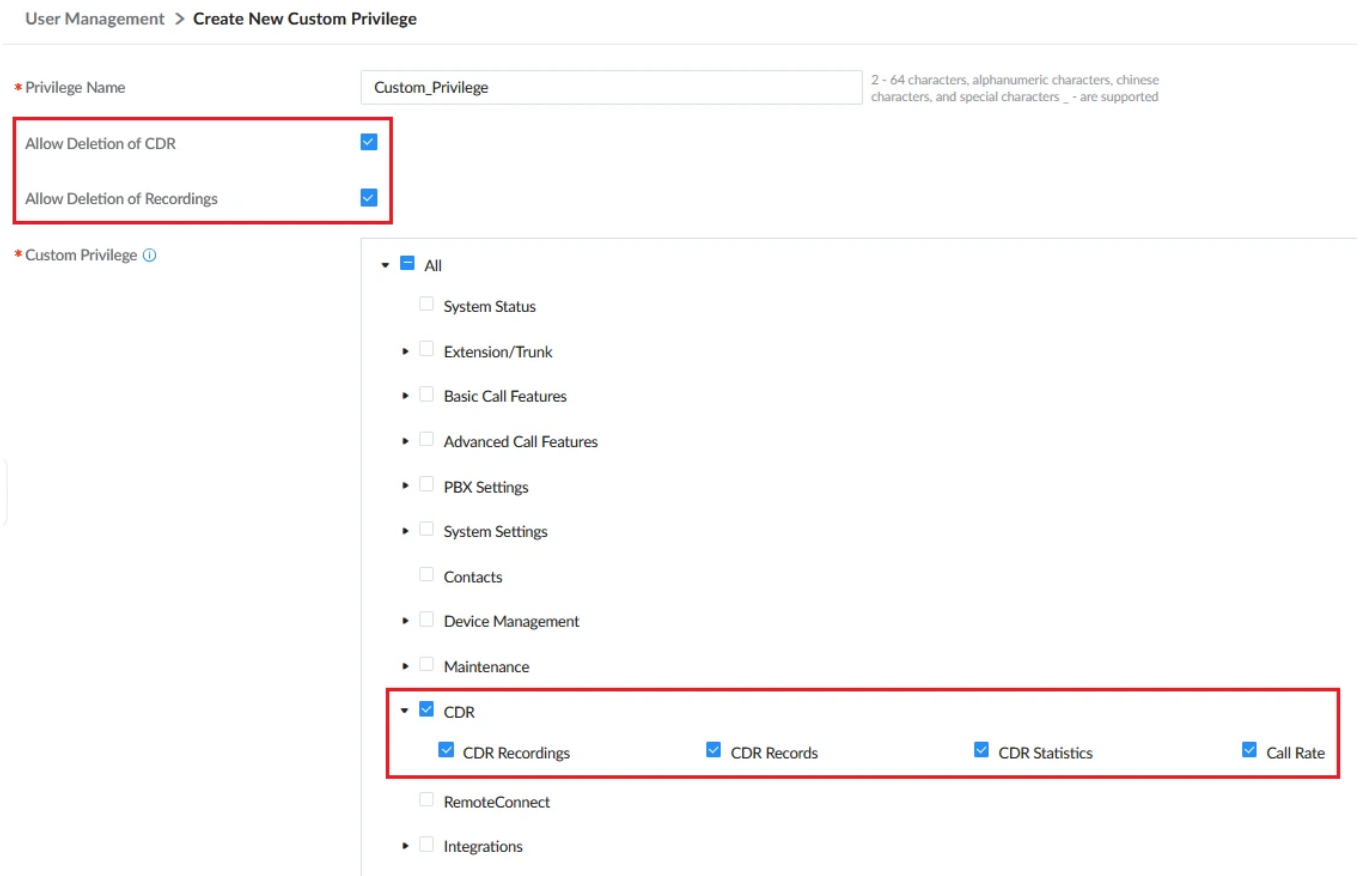
To create a custom privilege role, click **Add** and select the accessible modules from the table below:

Module	Custom Privileges
System Status	System Status
Extension/Trunk	Extensions, Extension Groups, Outbound Routes, Inbound Routes
Basic Call Features	Multimedia Meeting, IVR, Voicemail, Ring Groups, Paging/Intercom, Call Queue, Queue Recordings, Queue Statistics, Queue Board, Queue Operation Panel, Speed Dial, Event List, Feature Codes, Parking Lot
Advanced Call Features	Pickup Groups, Dial By Name, DISA, Callback, Scheduled Call, Fax Sending, Fax/T.38, Announcement, SCA, Emergency Calls, Restrict Calls
PBX Settings	Music on Hold, Voice Prompt
System Settings	Time Settings, LDAP Server
Contacts	Contacts

Device Management	Zero Config
Maintenance	System Events, Backup
CDR	CDR Recordings, CDR Records, Call Note, CDR Statistics, Call Rate
RemoteConnect	UCM RemoteConnect
Integrations	AI Settings, API Configuration, PMS - Basic Settings, PMS - Room Management, PMS - Check-in Management, PMS - Wakeup Service, PMS - Mini Bar, PMS - Housekeeper



When enabling specific privileges such as **CDR Records** or **CDR Recordings**, granular sub-options will appear (such as Allow Deletion of CDR and Allow Deletion of CDR Recordings), providing precise control over data retention permissions.



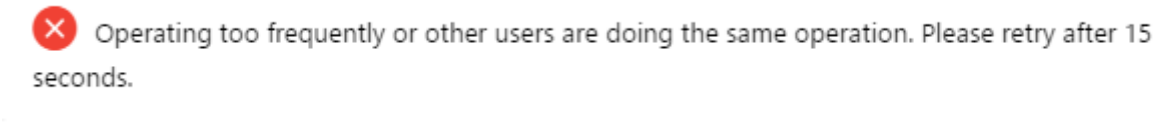
CDR Related Custom Privileges

To assign a custom privilege to a user or sub-administrator, navigate to **Maintenance -> User Management -> User Information**, create a new user or edit an existing user, and select the configured role from the

Privilege dropdown menu.

Concurrent Multi-User Login

When there are multiple Web GUI users created, concurrent multi-user login is supported on the UCM630X. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on "Apply Changes"), a prompt will pop up as shown in the following figure.



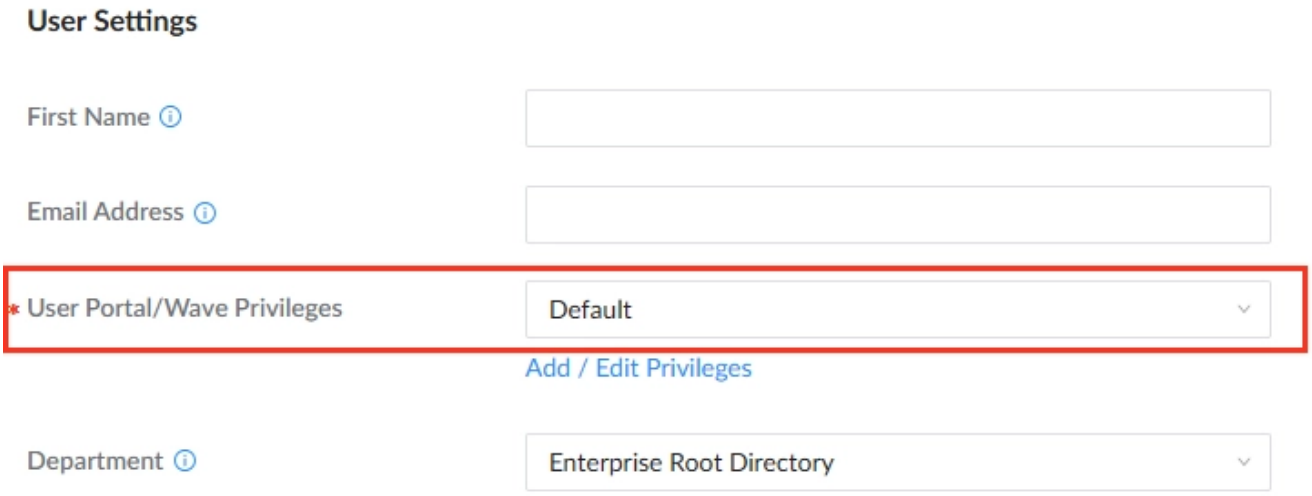
Multiple User Operation Error Prompt

Only one session can be opened per user. If a new session has been opened for an account that had already been opened. The older session will be terminated upon the login of the user.

User Portal/Wave Privileges

The administrator can create customized privileges related to an extension's User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.

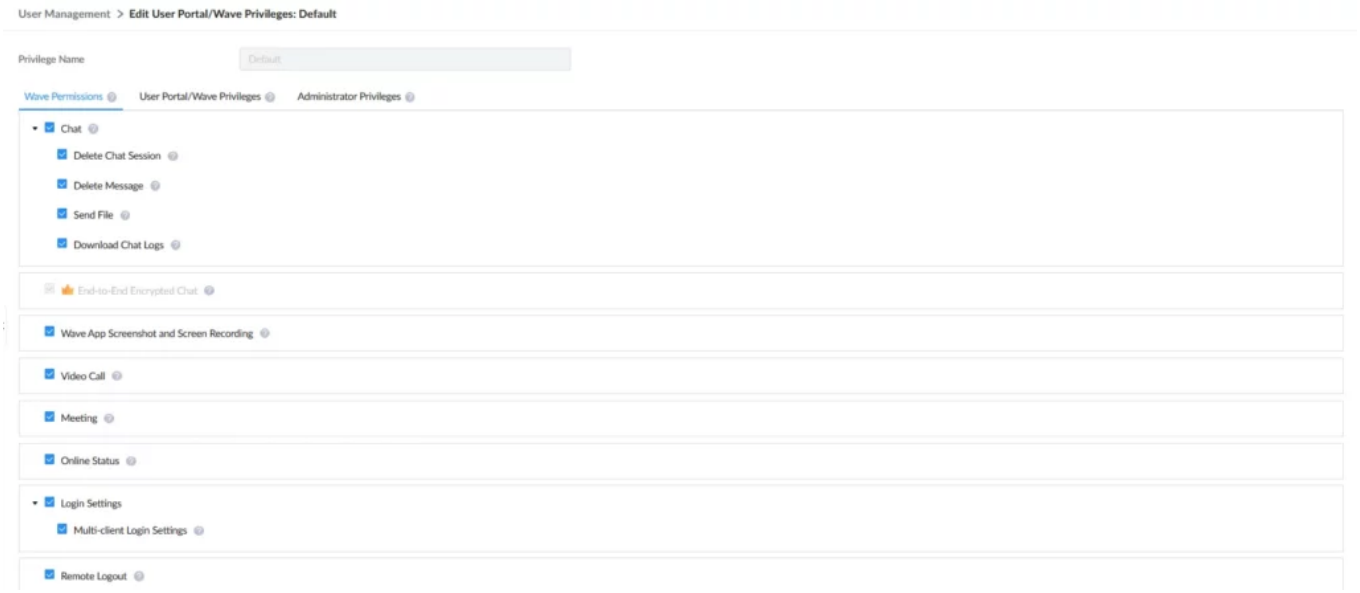
After the creation of the privilege, the administrator can assign the privilege to a specific extensions by navigating to **Extension/Trunk->Extensions->Basic Settings->User Portal/Wave Privileges.**



User Portal/Wave Configuration

Wave Permissions

Under Wave Permissions category, the user can configure the various permissions for the basic features of Wave such as using the chat, making audio/video calls, meeting, use application store, etc...



Wave Permissions Tab

- **Chat:** Toggles ability to use the Wave Chat feature.
    - **Delete Chat Session:** Toggles support for Wave to delete chats and chat history. This data will only be deleted on the Wave client side.
    - **Delete Message:** Controls whether Wave users will be allowed to delete messages that have been sent. Deleted messages will not be visible to anyone.
    - **Send File:** Toggles file/image sending support in Wave chat. If disabled, users will still be able to download, view and forward chat files.
    - **Download Chat Logs:** If enabled, chat logs will be downloadable from the Wave client, including chat logs from Wave/WhatsApp/Telegram/LiveChatsessions.
- **End-to-End Encrypted Chat*:** Toggles ability to use the Wave End-to-End Encrypted Chat feature.
- **Wave App Screenshot and Screen Recording:** Controls whether users are allowed to take screenshots and perform screen recordings in the Wave mobile app.
- **Video Call:** Toggles ability to use the Wave Video Call feature.
- **Meeting:** Toggles ability to use the Wave Meeting feature.
    - **Start Video During Meeting:** Toggles ability to use the Wave Start During Meeting feature.
- **Online Status:** Toggles ability to set Wave online status such as "Busy", "Appear Away", "Do Not Disturb", "Appear Offline", etc. If unchecked, the status will be displayed as only either "Online" or "Idle".
- **Login Settings**
    - **Multi-client Login Settings**: If enabled, users will be allowed to enable or disable the option "Allow Simultaneous Logins from the Same Client Type".
- **Remote Logout:** If enabled, Wave users will be able to log out of their accounts from other logged-in devices.
- **Recording Status:** Controls whether the recording status is displayed in all calls/conferences of the extensions. **Note**: If the call recording prompt is enabled, it will be played as this setting affects the indicator that shows that a call is being recorded on Wave.

- **Clear Recent Call History:** Toggles ability to delete recent call history entries and entire recent call history on Wave.
- **Application:** Toggles ability to access the "Applications" page under Wave Desktop and Wave Web.
- **Smart Devices:** Toggling off privileges will hide the corresponding pages and options in Wave.

    - **Door System**
    - **Monitor**
    - **Call Device (CTI)**
- **3rd Party Applications**

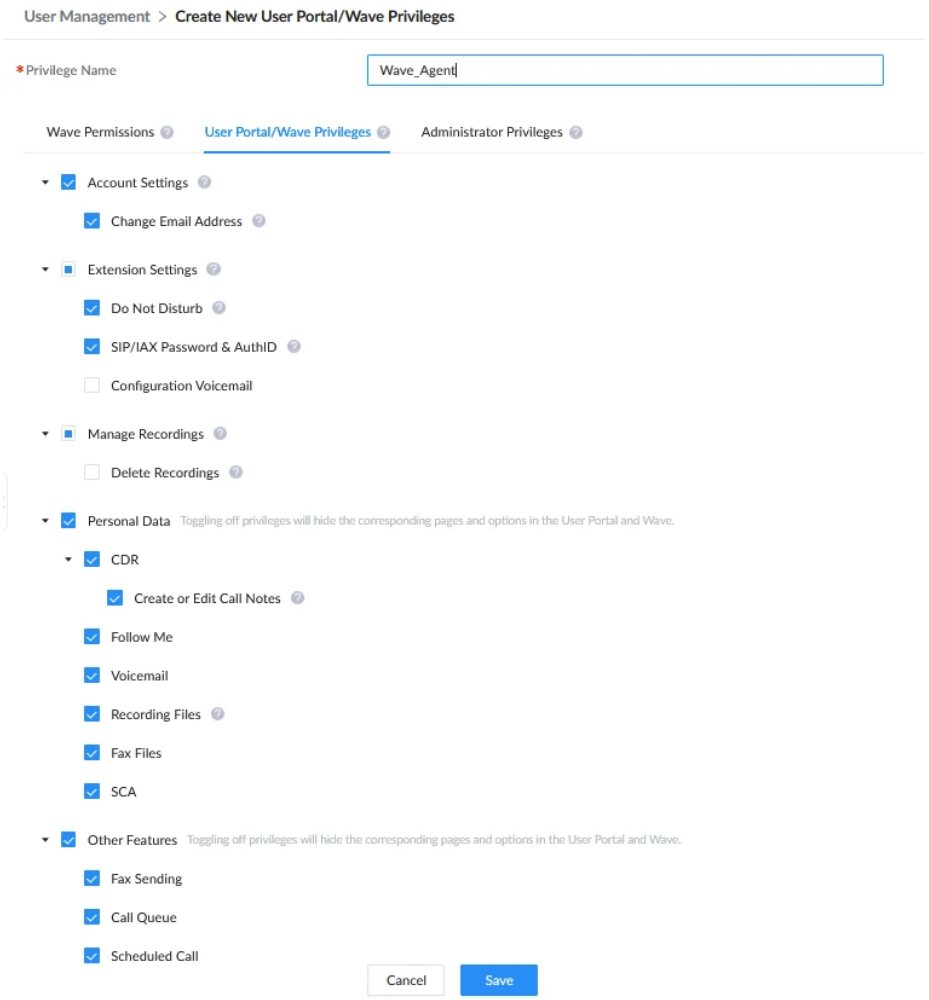
    - **App Store**: Toggles ability to install applications from Wave application store. If unchecked, the application store will be hidden, but installed apps can still be used.

User Portal/Wave Privileges

Under User Portal/Wave Privileges, the administrator can configure access privileges to specific settings and features, such as adjusting account settings, changing SIP/IAX passwords and AuthIDs, setting DND, or managing personal data (e.g., CDRs, Follow Me, Voicemail, recordings, etc.).

To improve account security, the UCM reminds extension users to change passwords they have not changed themselves.

- A password is considered unchanged if it is the default password, a randomly generated password, a password configured by the administrator, or a password regenerated after the administrator resets the extension.
- Reminders apply only to extensions created after upgrading to firmware 1.0.35.8. Existing extensions do not receive the reminders.
- If the related privilege is disabled, the user cannot change the password, so no reminder is displayed.



The table below describes the privilege options available under the User Portal/Wave Privileges tab:

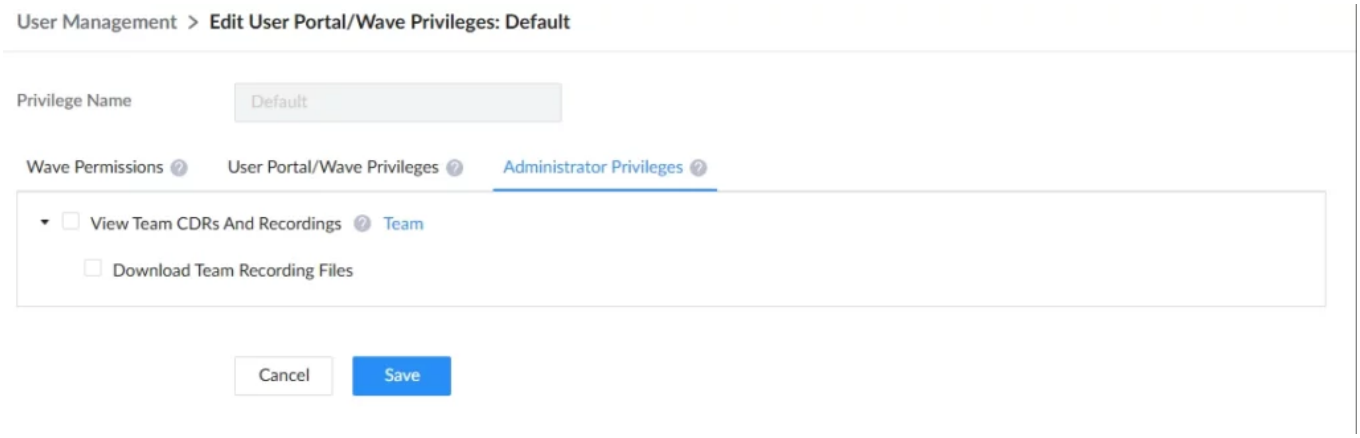
Privilege Option	Description
Account Settings	If unchecked, hides the User Portal -> Basic Information -> Account Settings page and the Wave -> Sidebar -> User -> Account Settings option. Change Email Address: Toggles whether users assigned to this privilege role are allowed to modify their extension email address. If unchecked, the email modification field will be restricted. Note: When Account Settings are enabled users who have not changed their User Portal/Wave password receive a reminder in the User Portal and Wave.
Extension Settings	If unchecked, hides the extension's User Portal -> Basic Information -> Extensions page and the Wave -> Sidebar -> User -> Call Settings option. Do Not Disturb: Toggles the ability to configure Do Not Disturb (DND) status through the User Portal or Wave. SIP/IAX Password & AuthID: Toggles access to view or edit the SIP/IAX Password and AuthID settings under the User Portal -> Basic Information -> Extensions -> Basic Settings page. Configuration Voicemail: Toggles the ability to configure voicemail preferences directly. Note: When SIP/IAX Password & AuthID privilege is enabled, users who have not changed their SIP password receive a reminder in the User Portal.
Manage Recordings	Toggles the ability to view recordings through the User Portal and Wave, including call log recordings, meeting details, and Wave application recordings. Delete Recordings: Toggles the ability to delete recordings through the User Portal and Wave. For Wave, this includes deleting call logs, meeting details, and recording files.

Personal Data	Toggling off parent or sub-privileges hides the corresponding pages and options in the User Portal and Wave: CDR: Toggles access to Call Detail Records. Create or Edit Call Notes: Toggles permission to create, edit, or view notes/tags attached to call records. Follow Me: Toggles access to Follow Me forwarding rules. Voicemail: Toggles access to personal voicemail messages. Recording Files: Toggles access to dedicated recording files. Fax Files: Toggles access to received/sent fax files. SCA: Toggles access to Shared Call Appearance features.
Other Features	Toggling off parent or sub-privileges hides the corresponding pages and options in the User Portal and Wave: Fax Sending: Toggles permission to send faxes. Call Queue: Toggles access to call queue management/wallboard interfaces. Scheduled Call: Toggles permission to create or manage scheduled calls.

*: Features which are marked by an asterisk are a part of RemoteConnect plans.

Administration Privileges

Under Administrator Privileges, the administrator can configure enabling certain extensions to view a designated team's CDR.



Administrator Privileges

- **View Team CDRs and Recordings**: Define whether certain extensions can view each other's CDR. Click on "Team" to designate the extensions.

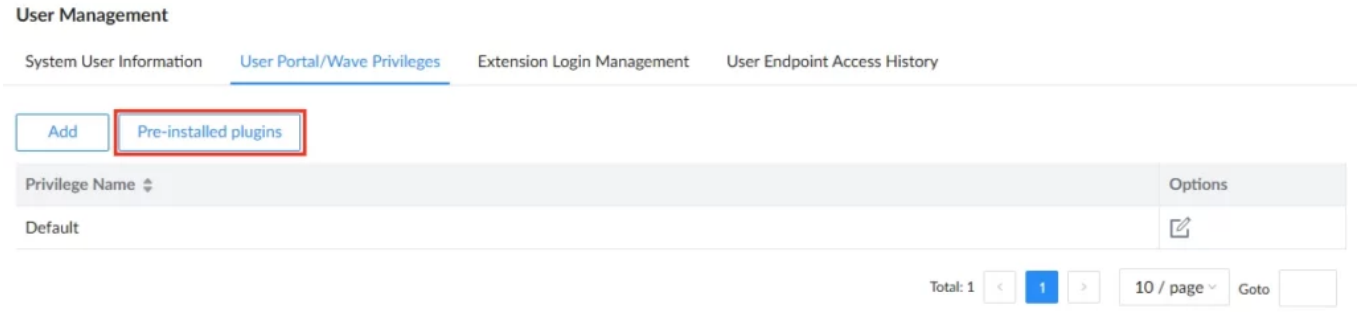
    - **Download Team Recording**: When this option is enabled, the extensions selected in the team will be allowed to access each other's CDR and call recording files.

Pre-intalled Plugins

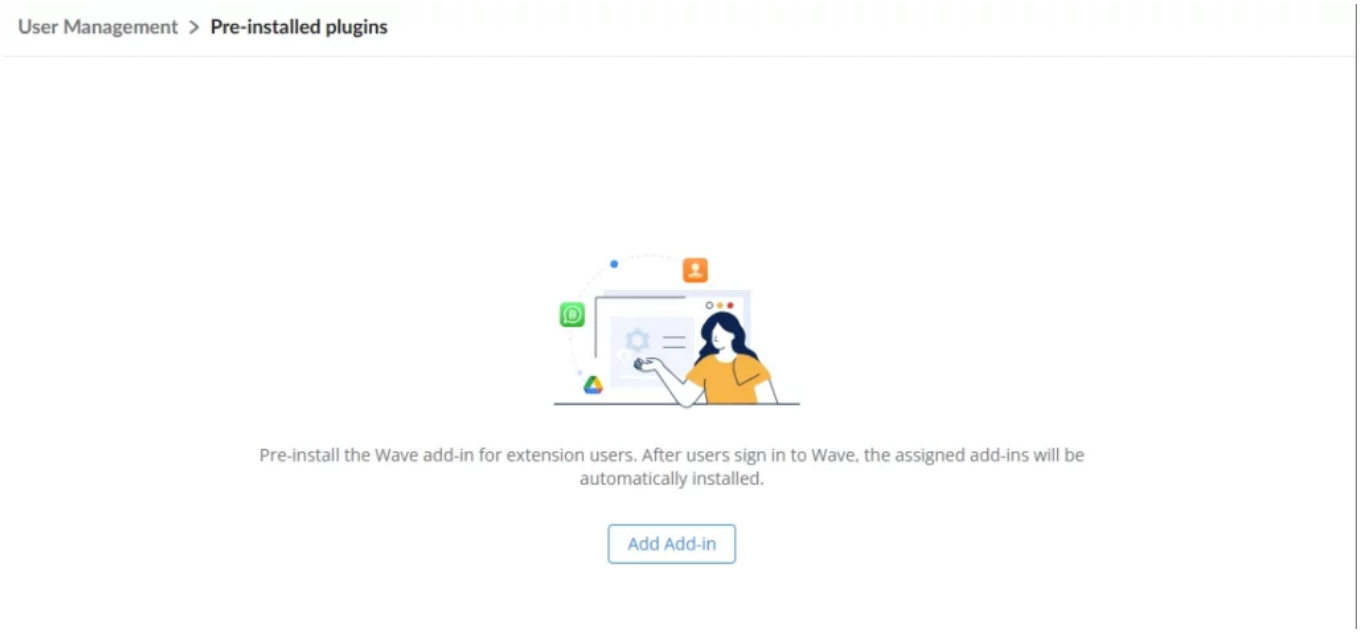
The administrator can set the plug-ins which will be installed when the user logs into Wave Desktop.

To configure the pre-installed plugins, follow the steps below.

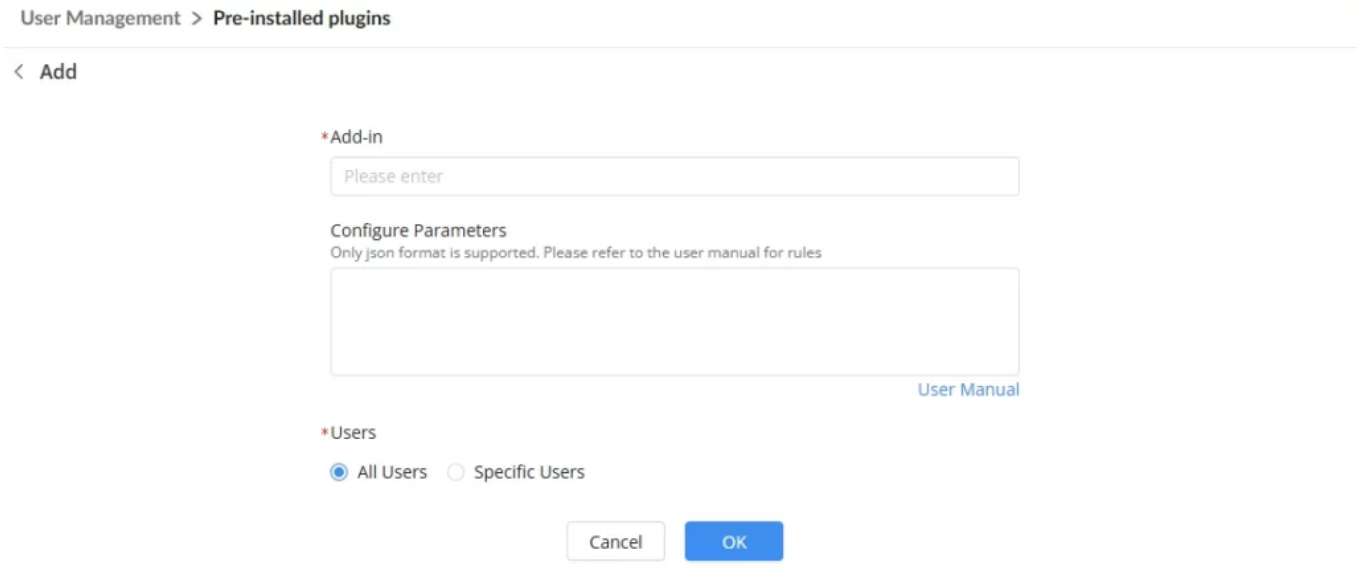
1. Navigate to **Maintenance > User Management > User Portal/Wave Privileges** then click "Pre-installed Plug-ins".



2. Click on "Add Add-in" button.



Pre-installed Plug-ins



Add Pre-installed Plug-ins

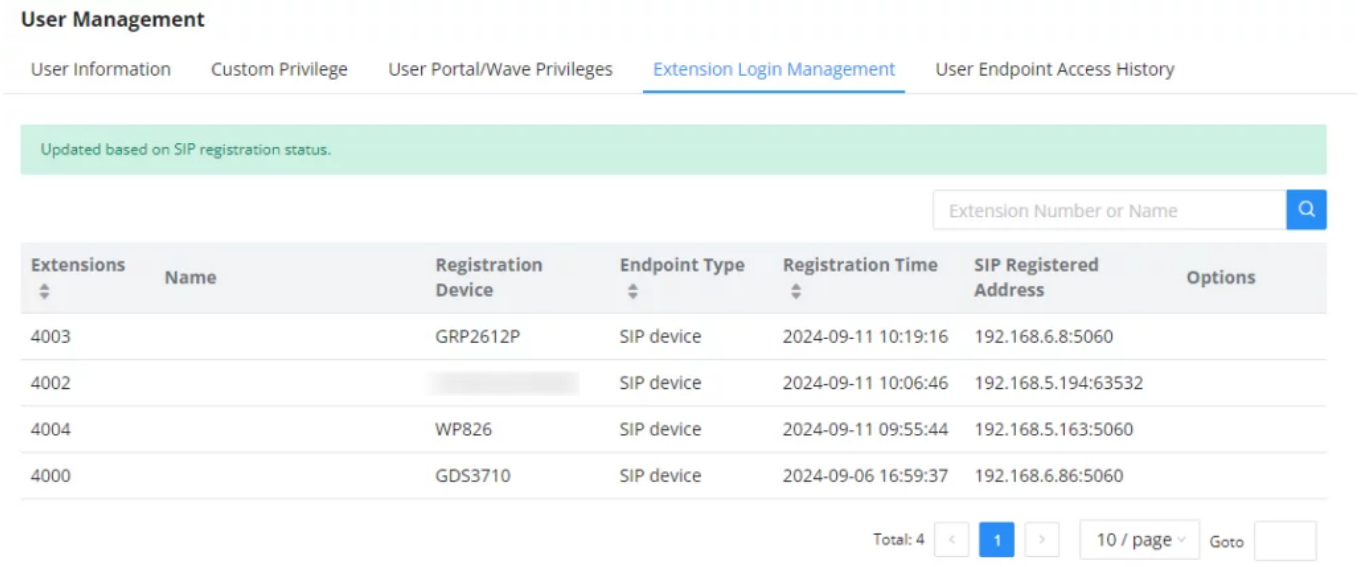
Parameter	Description

Add-in	Select an add-in.Act! CRMBitrix24Capsule CRMDynamics 365FreshdeskGoogle DriveHubspotIPVideoTalkLess Annoying CRMMonday Sales CRMOdoo CRMOffice365OfficeRnD Hybrid WorkOracle NetSuiteSalesforceSugarCRMTelegramVtiger CRMWhatsapp BusinessZendeskZoho CRMZoho Desk
Configure Parameters	Enter the configuration parameters. The configuration parameters consist of authentication information, database name, webhook url etc...Note: Please note that only JSON format is supported.Example: Whatsapp Business{"config": [{"name":"xxxxx","accessToken":"xxxxx","payloadKey":"xxxxx","webhooksUrl":"xxx","phoneNumIDList": ["xxxxx","xxxxx"] }
Users	Select which extension(s) to apply this rule to.All UsersSpecific Users

For the complete steps and information about pre-installing plug-ins, please refer to the following guide: https://documentation.grandstream.com/knowledge-base/pre-install-wave-add-ins-on-the-ucm63xx/

Extension Login Management

Extension Login Management allows the administrator to review the logged-in sessions of SIP devices and Wave.

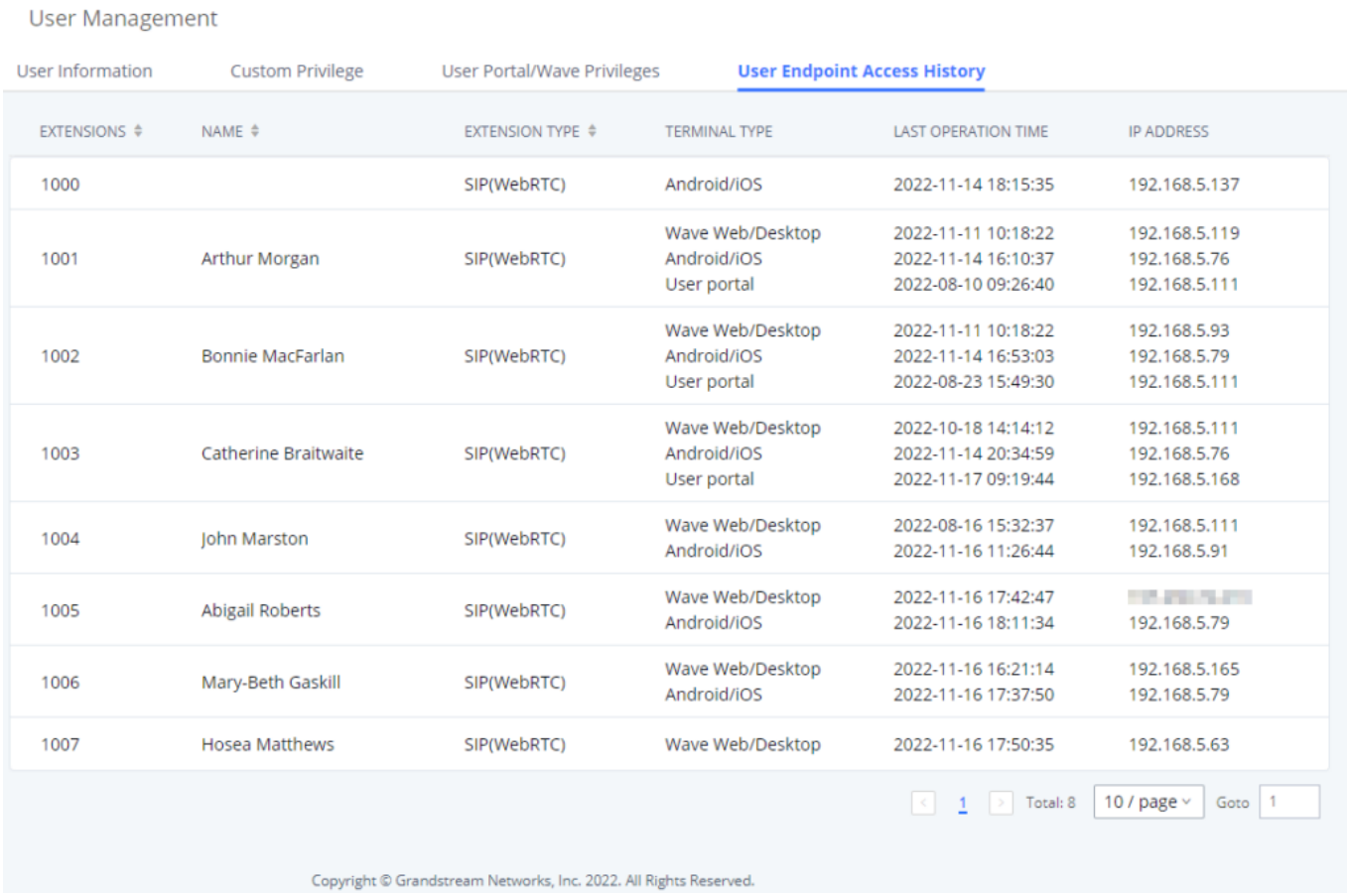


Extension Login Management

For Wave sessions, the administrator can click on to terminate a Wave session. SIP sessions cannot be logged out.

User Endpoint Access History

The User Endpoint Access History tab allows the administrator to view the access history of all extensions, the time on which the access has occurred, the IP addresses from which the extensions were accessed, and whether they were accessed from the User Portal, Wave Web/Desktop, or mobile. Extension access from the SIP endpoints won't be logged in this page.



User Endpoins Access History

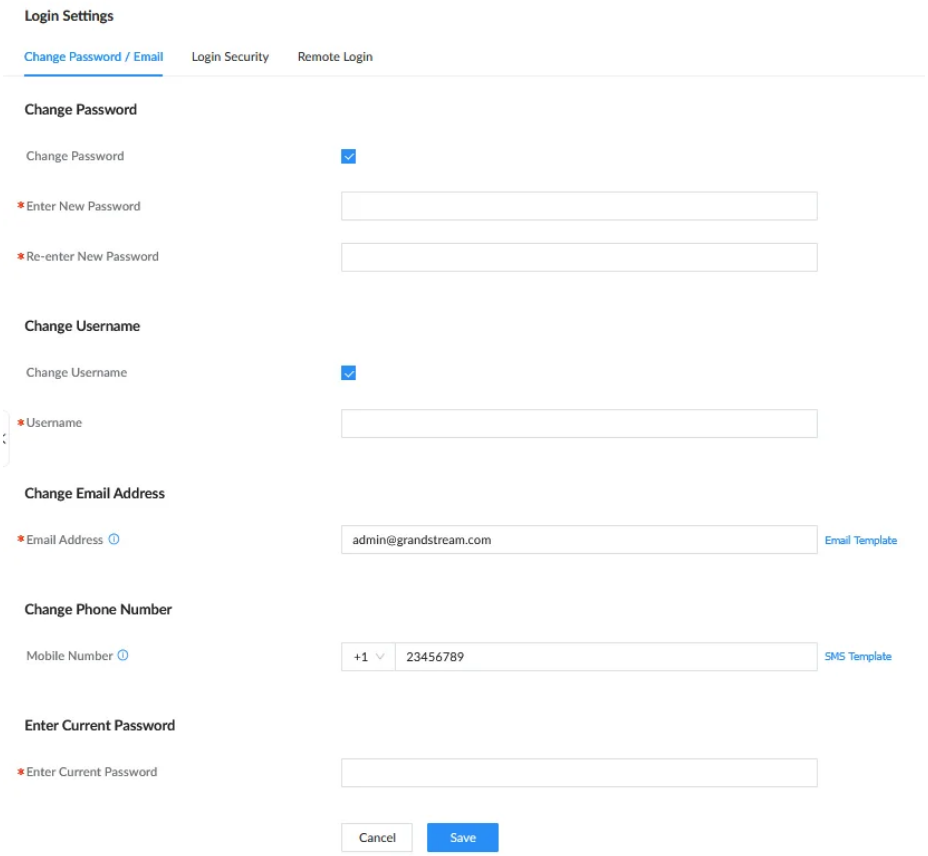
Login Settings

Change Password / Email

Change Password

After logging in the UCM630X Web GUI for the first time, it is highly recommended for users to change the default password to a more complicated password for security purpose. Follow the steps below to change the Web GUI access password.

1. Go to **Maintenance** -> **Login Settings -> Change Password / Email** page.
2. Enter the old password first.
3. Enter the new password and re-type the new password to confirm. The new password has to be at least 4 characters. The maximum length of the password is 30 characters.
4. Configure the Email Address that is used when login credential is lost.
5. Click on "Save" and the user will be automatically logged out.
6. Once the web page comes back to the login page again, enter the username "admin" and the new password to login.

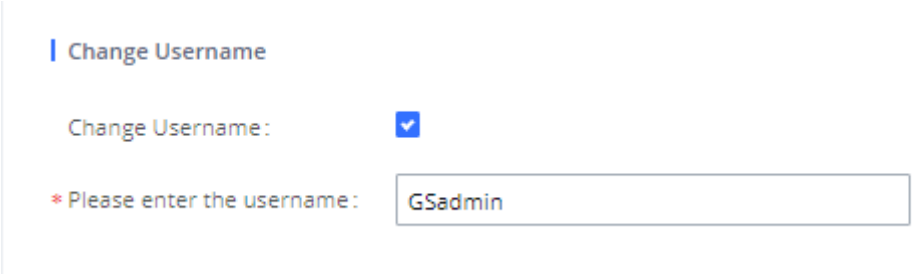


Change Password

Option	Description
Change Password	
Change Password	Check this option to enable modifying the current administrator account login password.
Enter New Password	Enter the new password for the account. Passwords must satisfy length and complexity requirements (e.g., uppercase, lowercase, numbers, and special characters).
Re-enter New Password	Re-type the new password to confirm matching input.
Change Username	
Change Username	Check this option to enable modifying the current account login username.
Username	Enter the new login username for the account.
Change Email Address	
Email Address	Configures the email address associated with the administrator account for receiving password recovery tokens, system event notifications, and two-factor authentication codes. Click Email Template to edit notification formatting.
Change Phone Number	
Mobile Number	Configures the mobile phone number (including country code prefix) for receiving SMS verification codes or SMS alerts. Click SMS Template to manage message formatting.
Enter Current Password	
Enter Current Password	Enter your existing password to authenticate and authorize any changes made on this page before clicking Save.

Change Username

UCM630X allows users now to change Super Administrator username.



Change Username

Change Email Address

UCM630X allows user to configure binding email in case login password is lost. UCM630X login credential will be sent to the designated email address. The feature can be found under **Maintenance > Login Settings > Change Password / Email**



Change Binding Email

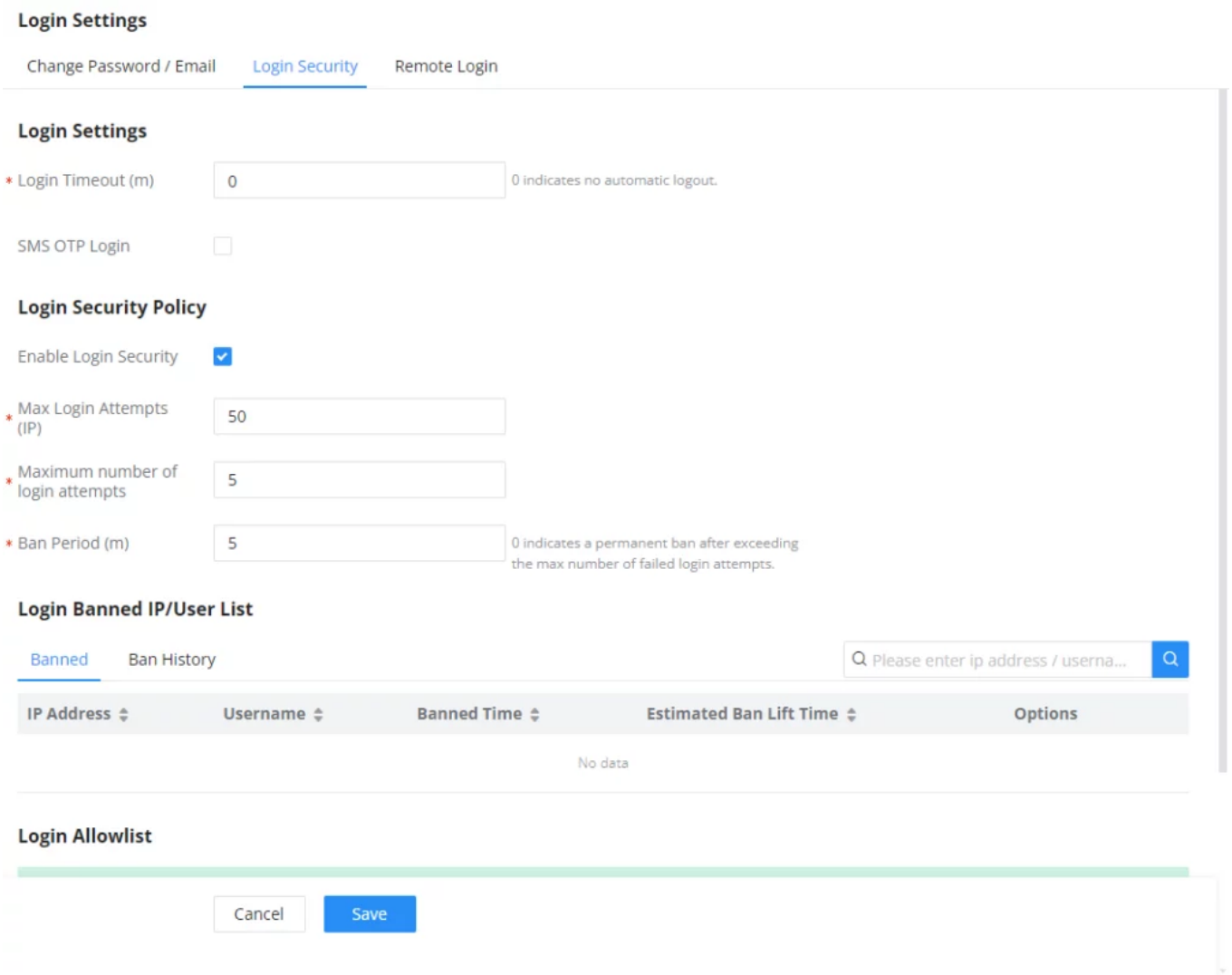
Email Address	Email Address is used to retrieve password when password is lost

Change Binding Email option

Login Security

After the user logs in the UCM630X Web GUI, the user will be automatically logged out after certain timeout, or he/she can be banned for a specific period if the login timeout is exceeded. Those values can be specified under UCM630X **Maintenance** > **Login Settings** > **Login Security** page.

The "**User Login Timeout**" value is in minute and the default setting is 10 minutes. If the user does not make any operation on Web GUI within the timeout, the user will be logged out automatically. After that, the Web GUI will be redirected to the login page and the user will need to enter username and password to log in.



Login Timeout Settings

Login Settings	
Login Timeout (m)	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. If set to 0, the user will not be logged out automatically. Valid range is 0 to 60 and default value is 0.
SMS OTP Login	If enabled, users will be able to log in and reset password via SMS verification code. Mobile phone numbers will need to be configured for administrators and extensions.
Login Security Policy	
Enable Login Security	Enable login security measure to prevent authentication attacks.
Max Login Attempts (per IP address)	The max allowed number of consecutive failed login attempts from an IP address. Once exceeded, no users will be able to log in from that IP address.Note: The valid range is between 5 to 100 attempts.
Maximum number of login attempts (per user)	The maximum number of consecutive failed login attempts. When exceeded, the user will not be able to log in for the amount of time specified in "User ban period".Note: The valid range is between 1 to 100 attempts.
Ban Period (m)	The amount of minutes that a user will be banned for after exceeding the maximum allowed number of consecutive failed login attempts. Note: The valid range is between 0 and 10000 minutes, with 0 indicating a permanent ban.
Login Banned IP/User List	List of IP addresses which are banned from making any further login attempts.

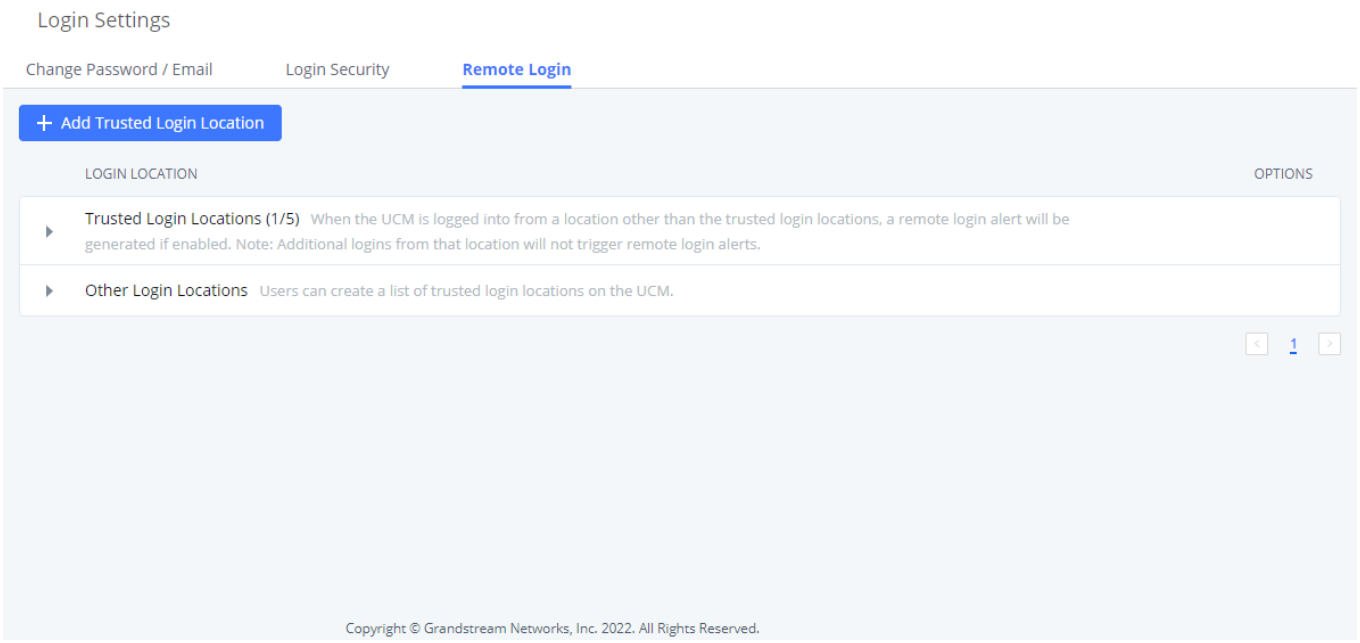
Login Allowlist	List of IP addresses which can make unlimited login attempts.

Remote Login

This feature allows the user to manage trusted login locations, also, verifying where login sessions were initiated from, this is very important since, in this type of scenario, the UCM6300 would be directly connected to the Internet, and the public IP address would be used for the remote login. This feature adds a layer of visibility and control, thus enhacing the security of the UCM.

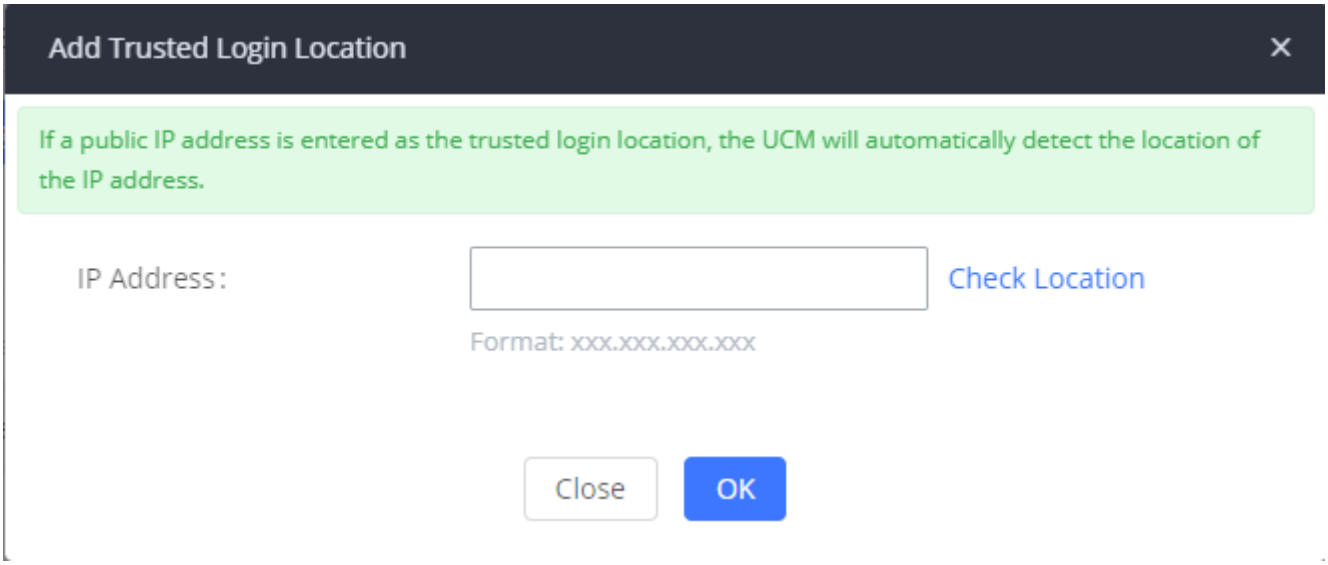
In this tab there are two types of lists of locations:

- Trusted Login Locations: These are the trusted login locations that are added manually by the admin. Any added trusted login location will not generate any remote login alert upon the first time login.
- Other Login Location: This list will show all the remote login locations that are not trusted, logging in for the first time from an untrusted login location will generate an alert, but the subsequent remote logins from the same location will not generate alerts.



Remote Login

To add a trusted login location, the user must click on



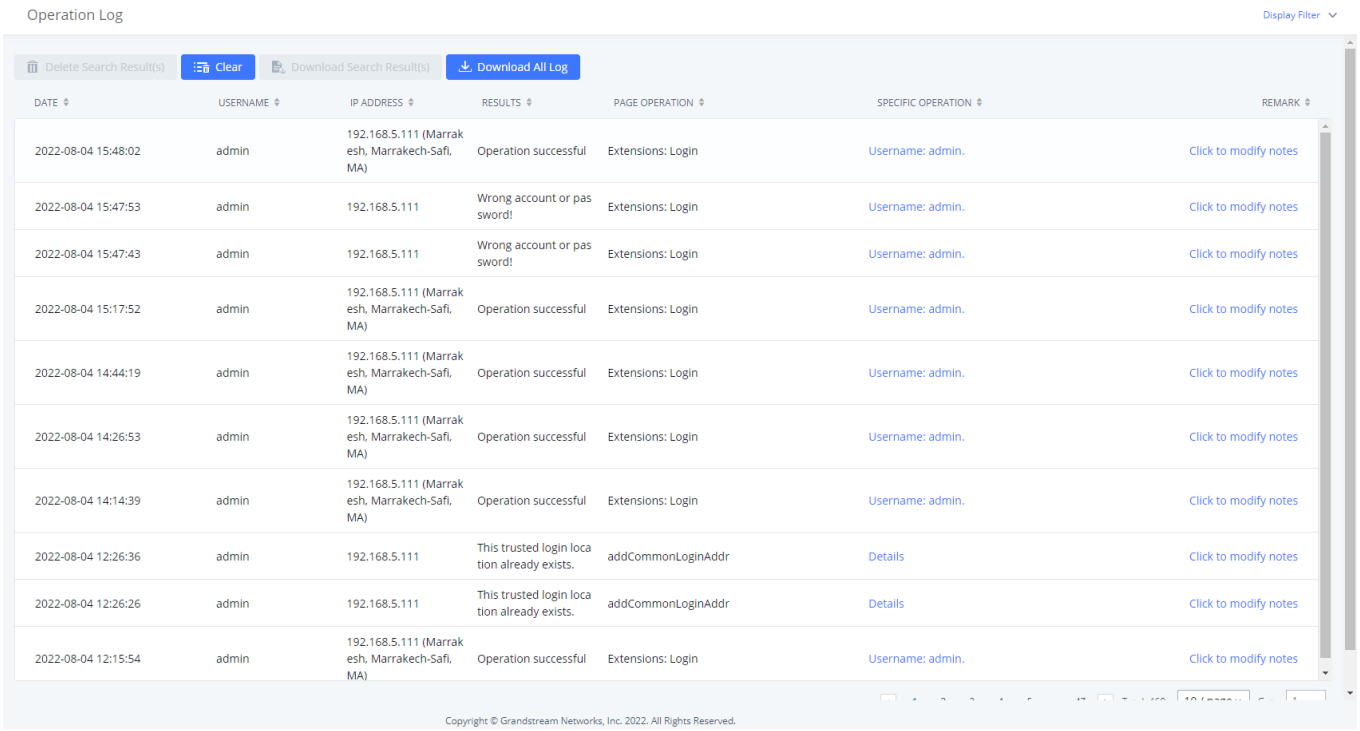
Then add the public IP address of the location, click on "**Check Location**" to verify if it's the correct location

then click "**OK**".

The system administrator can add up to 5 Trusted Login Locations, while Other Login Locations can have an unlimited number of entries.

Operation Log

Super Admin has the authority to view operation logs on UCM630X **Settings** > **User Management** > **Operation Log** page. Operation logs list operations done by all the Web GUI users, for example, Web GUI login, creating trunk, creating outbound rule etc. There are 7 columns to record the operation details "Date", "Username", "IP Address", "Results", "Page Operation", "Specific Operation" and "Remark".

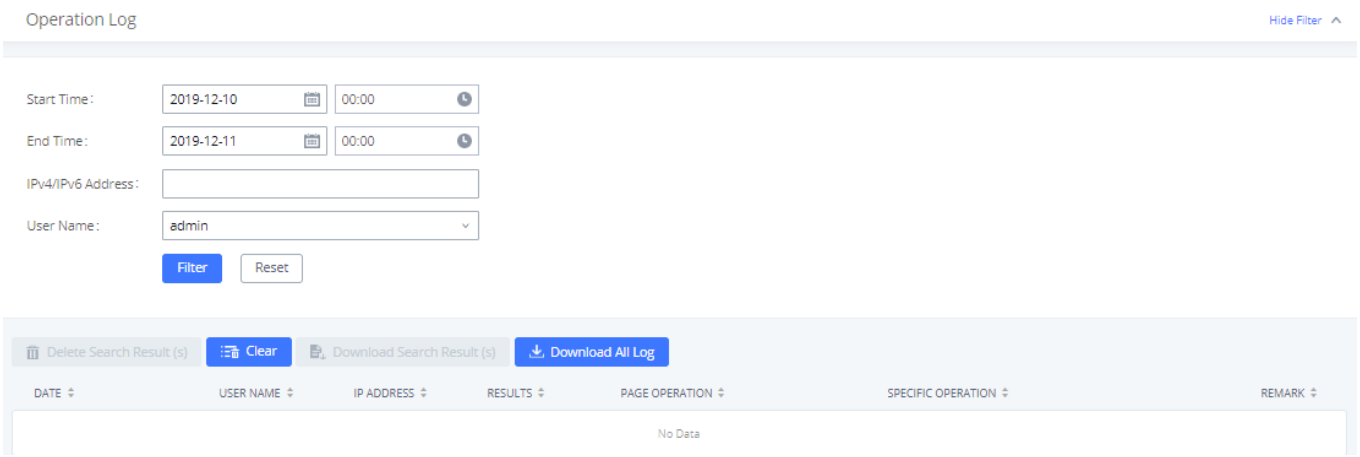


Operation Logs

The operation log can be sorted and filtered for easy access. Click on or at the top of each column to sort. For example, clicking on for "Date" will sort the logs according to newer operation date and time. Clicking on for "Date" will reverse the order.

Date	The date and time when the operation is executed.
Username	The username of the user who peformed the opertation
IP Address	The IP address and geographical location from which the operation has been made.
Results	The result of the operation.
Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
Specific Operation	Click on the hyperlinked operation detail to reveal more details.
Remark	Allows users to add notes and remarks to each operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on "Display Filter".



Operation Logs Filter

The above figure shows an example that operations made by user "support" on device with IP 192.168.40.173 from 2014-11-01 00:00 to 2014-11-06 15:38 are filtered out and displayed.

To delete operation logs, users can perform filtering first and then click on to delete the filtered result of operation logs. Or users can click on to delete all operation logs at once.

Syslog

On the UCM630X, users could dump the syslog information to a remote server under **Maintenance** -> **Syslog**. Enter the syslog server hostname or IP address and select the module/level for the syslog information as well as Process Log Level.

The default syslog level for all modules is "error", which is recommended in your UCM630X settings because it can be helpful to locate the issues when errors happen.

Some typical modules for UCM630X functions are as follows and users can turn on "NOTICE" and "VERBOSE" levels besides "error" level.

- **pbx**: This module is related to general PBX functions.
- **pjsip**: This module is related to SIP calls.
- **chan_dahdi**: This module is related to analog calls (FXO/FXS).

- Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog prints might cause traffic and affect system performance.
- The reserved size for Syslog entries on the cache memory of the UCM is 50M, once this sized is reached the UCM will clean up 2M of the oldest Syslog entries to allow to save new logs.

Syslog

The Syslog feature allows administrators to export and monitor system logs either locally on the UCM or by sending them to a centralized remote Syslog server under **Maintenance -> Syslog**. System logs capture real-time operational events, service warnings, and critical errors across various subsystem modules to assist with diagnostic analysis and troubleshooting.

The table below describes all Web UI options and parameters available on the **Maintenance -> Syslog** page:

Parameter	Description
Syslog Server	Configures the IP address or domain name of a remote Syslog server to receive exported system logs. Note: When an external Syslog server is defined, logs will no longer be stored locally on the UCM.
Write Syslog Into Cache	When enabled, forces the UCM to continuously write Syslog output into local cache memory. Enabled by default.
Time Interval (s)	Specifies the interval in seconds for flushing and updating Syslog cache entries. Default setting is 60 seconds.
Syslog	
Process Log	Selects which system management processes log activity. Checkable options include All Modules, Apply Change Log, Alert Log, ZeroConfig Log, LDAP Log, TR069 Log, HA Log, and Other Log.
Process Log Level	Sets specific logging thresholds (e.g., Disable, Error, All Level) for subsystem services: PBX MID Log: Controls internal middleware logging. (Default: Disable). AVS Log: Controls Audio/Video Service logging. (Default: Error). CGI Log: Controls Web interface CGI script logging. (Default: All Level). IM Log: Controls Instant Messaging service logging. (Default: Disable).
Syslog Level	Selects global logging filters across functional features. Options include All Modules, DTMF, CC (Call Control), FAX, and SECURITY (enabled by default).
PBX Modules	Provides granular logging verbosity levels per PBX module. For each listed module (e.g., pjsip, pbx, chan_dahdi, AGI, AMI, app, etc.), administrators can check one or more logging levels: Error (Default): Logs severe errors and operational failures. Recommended for daily production monitoring. Warn: Logs abnormal conditions or non-fatal warnings. Notice: Logs significant operational state changes. Debug: Logs detailed execution steps for active troubleshooting. Verbose: Logs deep low-level trace information (highest output volume). All Level: Enables all verbosity filters simultaneously for the chosen module.

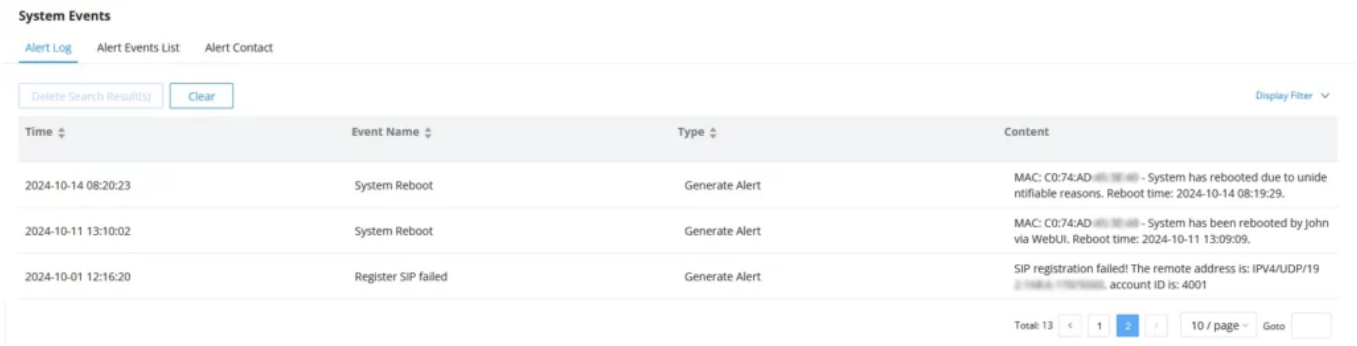
- Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog prints might cause traffic and affect system performance.
- The reserved size for Syslog entries on the cache memory of the UCM is 50M, once this sized is reached the UCM will clean up 2M of the oldest Syslog entries to allow to save new logs.

System Events

The UCM630X can monitor important system events, log the alerts, and send Email notifications to the system administrator.

Alert Log

Under **Maintenance** > **System Events** > **Alert Log**, system messages from triggered system events are listed as alert logs. The following screenshot shows system reboot alert logs.



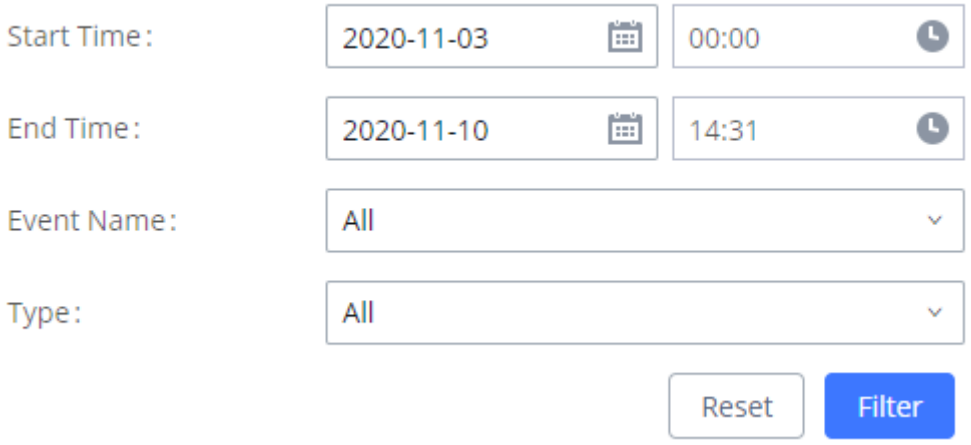
System Events > Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on . Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.

2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

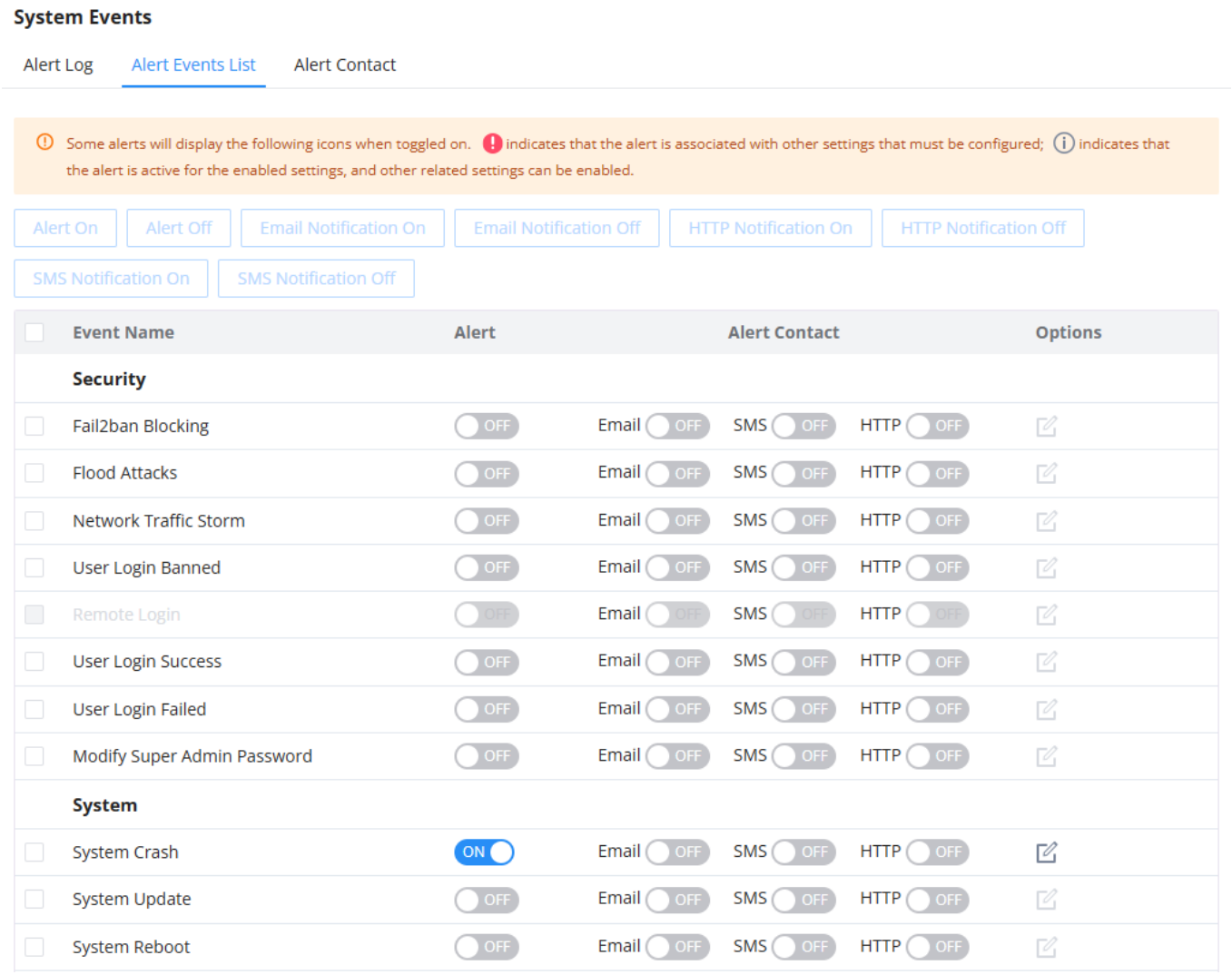
User could filter out alert logs of "Generate Alert" or "Restore to Normal" by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of "Restore to Normal".



Filter for Alert Log

Alert Events List

The system alert events list can be found under **Maintenance -> System Events -> Alert Events List**. The UCM630X supports various system event types that generate alerts and/or email notifications when triggered.



Alert Event List

For users who have purchased a GDMS package, once the option **Alert Events Sync** is enabled under RemoteConnect, triggered system alert events will be pushed automatically to their GDMS platform.

Click on the **Edit** icon next to any event entry to configure its notification parameters. The table below describes the available configuration options for alert events.

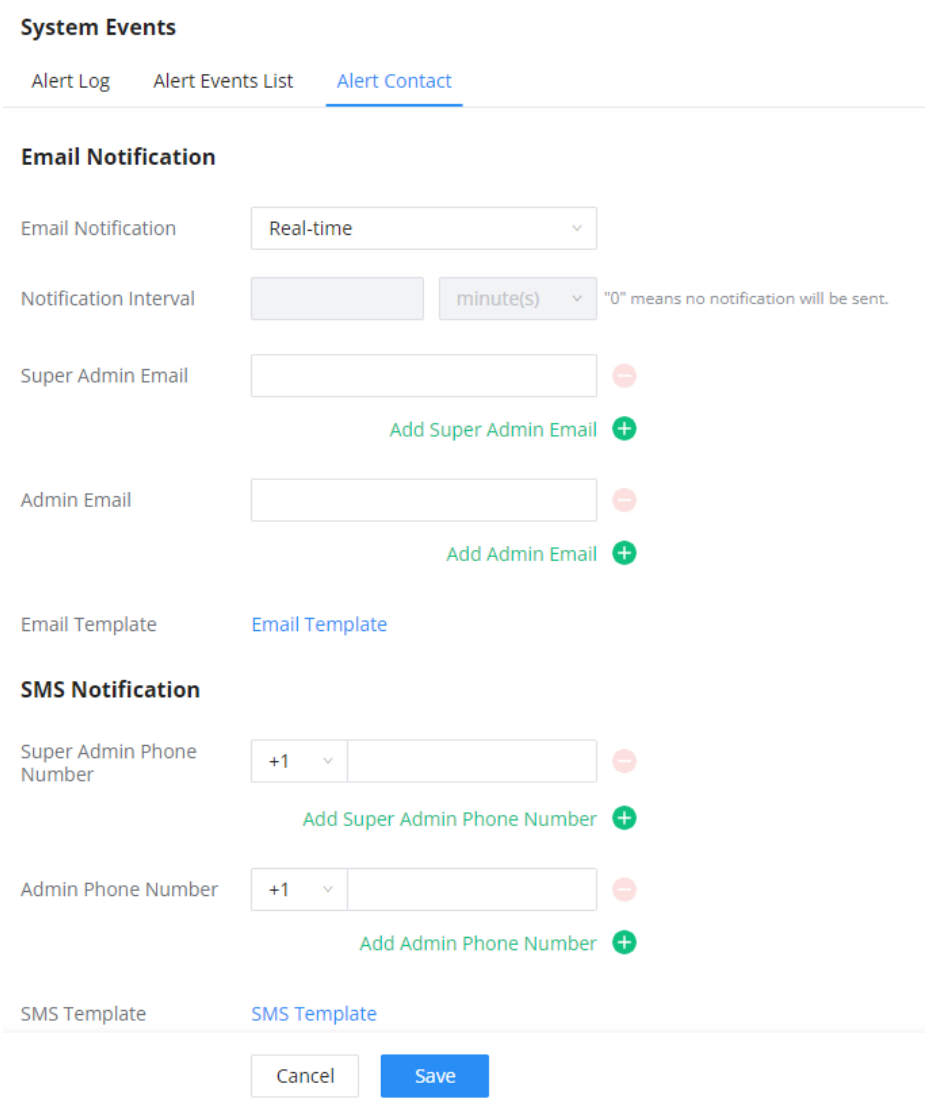
Event	Description
Security	
Fail2ban Blocking	If the system Fail2ban is blocking, the event will be recorded in the alert log.
Flood Attacks	An alert will be generated in case a DDoS attack attempt is detected by the UCM. The event will be registered in the alert log and pushed to GDMS.
Network Traffic Storm	An alert will be generated in case there is an excessive amount of packets on the LAN that consumes network resources and saturates bandwidth. Recorded in alert log and pushed to GDMS.
User Login Banned	If user login is blocked, the event will be recorded in the alert log.
Remote Login	An alert will be generated upon a remote login.
User Login Success	Successful user login events will be recorded in the alert log.
User Login Failed	User login failure events will be recorded in the alert log.
Modify Super Admin Password	An alert will be generated when the super admin password is changed.

System	
System Crash	The UCM will detect system crash events based on a specified cycle time.
System Update	Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
System Reboot	UCM detects system restarts and sends alerts containing MAC address, reboot reason, and initiator. Detects both: Manual restart: Reboot via Web GUI, LCD, or GDMS. Automatic restart: Reboot due to firmware upgrade, HA switchover, factory reset, power failure, or setting changes.
CPU Usage Call Control	Triggered when CPU usage exceeds the threshold configured under System Settings > General Settings (default 90%). Logs the event and prohibits new calls.
Memory Usage	Generates an alert if system memory usage exceeds the configured percentage threshold.
TLS Cert Expiration	Sends daily notifications starting 7 days before HTTP Server TLS certificate expiration, upon expiration, and after uploading a new valid certificate.
Cloud IM Abnormal	An alert message will be generated if Cloud IM encounters issues or exhibits abnormal behavior.
Data Sync Backup	If system data synchronization and backup abnormalities occur, the event will be recorded in the alert log.
Restore Config	Once system configuration is restored, the event is recorded in the alert log.
HA	
HA Failure	Generates an alert when a software or hardware fault occurs in HA dual-system hot backup deployment.
HA Switch	Sends an alert event once a switchover between primary and secondary UCM devices is detected.
HA Data Sync Failure	Generates an alert event in case of Data Sync failure in HA deployment.
Storage	
Local Disk Usage	Performs local disk detection periodically. Generates an alert if usage exceeds the configured percentage threshold. Note: If threshold is exceeded, disk operations (uploads, IM writing, recording, CDR) will be rejected.
External Disk Usage	Generates an alert if external disk usage exceeds the configured threshold percentage.
External Disk Status	Records connection and disconnection events of external disk storage in the alarm log.
Switching File Storage Path	Sends an alert once the file storage path on the UCM device is changed.
GDMS Cloud Storage	Triggered if cloud backup to GDMS fails.
Call Features	
Emergency Calls	If an emergency call is generated by the system, the event is recorded in the alert log.
SIP Outgoing Call through Trunk Failure	If an outgoing call via a SIP trunk fails, the event will be recorded in the alert log.
SIP Internal Call Failure	If an internal extension call fails within the system, the event will be recorded in the alert log.
Remote Concurrent Calls	If a remote concurrent call fails, the event will be recorded in the alert log.
Excessive Outbound Calls	Logged in the alert log and notification pushed when an extension initiates calls frequently.

Outbound Route Per-Call Duration	Triggers an alert notification when single outbound call duration thresholds are exceeded on configured outbound routes.
Outbound Call Duration	Triggered if a call reaches the cumulative duration limit set on an outbound rule.
Trunk Outbound Call Duration Usage	Triggered if a call reaches the duration limit set on a specific trunk.
Trunk Concurrent Calls	Triggered if the maximum allowed concurrent calls threshold is reached on a specific trunk.
Extension/Trunk Status	
Register SIP trunk failed	Detects failure of SIP trunk registration at configured intervals.
SIP Peer Trunk Status	If SIP peer trunk status becomes abnormal, the event will be recorded in the alert log.
Register SIP failed	Configures the notification cycle for SIP registration failures. Immediately alerts on first failure per IP/account, then counts subsequent failures until cycle expiration. Immediate mode if set to 0.
SIP Lost Registration	Records system SIP extension registration loss in the alert log. Note: Clicking the edit button allows enabling or disabling Ignore Wave App Registration Loss.
1+N Media Cluster Connection Status	Sends an alarm when a media resource server in a 1+N cluster goes online or offline.

Alert Contact

This feature allows the administrator to be notified when one of the Alert events mentioned above happens. Users could add administrator's Email address under **Maintenance** > **System Events** > **Alert Contact** to send the alert notification to an email (Up to 10 Email addresses can be added) or also specify an HTTP server where to send this alert.



Alert Contact

Email Notification	
Email Notification	Alert email notification delivery method: Real-time: Notifications will be sent out as soon as the alerts are generated. Periodic: Alerts generated within the configured "Notification Interval" time window will be queued up and sent all at once in a single notification.
Notification Interval	When the notification delivery method chosen is Periodic, this option will be available.? The sending frequency of alert email notifications. All alert events that have occurred within a send cycle will be sent.
Super Admin Email	Configure the email addresses to send alert notifications to.Up to 10 email addresses can be added.
Admin Email	Configure the email addresses to send alert notifications to.Up to 10 email addresses can be added.
Email Template	Please refer to section [Email Templates]
SMS Notification	
Super Admin Phone Number	Send alert notifications via SMS. Multiple phone numbers are supported.
Admin Phone Number	Send alert notifications via SMS. Multiple phone numbers are supported.
SMS Template	Click on the link to access the SMS templates page.
HTTP Notification	

Protocol	Protocol used to communicate with the server. HTTP or HTTPS.Default one is HTTP.
HTTP Server	The IP address or FQDN of the HTTP/HTTPS server.
HTTP Server Port	HTTP/HTTPS port
Warning Template	Customize the template used for system warnings.By default: {"action":"${ACTION}","mac":"${MAC}","content":"${WARNING_MSG}" }
Alarm Notification	Alert notification delivery method: Real-time: Notifications will be sent out as soon as the alerts are generated. Periodic: Alerts generated within the configured "Notification Interval" time window will be queued up and sent all at once in a single notification.
Notification Interval	When Alarm Notification method is set to Periodic, this option will be available. The frequency at which HTTP alert notifications are sent. All alert events that have occurred within a send cycle will be sent.
Resource Usage Notification Template	Customize the notification template to receive relevant alert information.By default: {"action":"${ACTION}","cpu":"${CPU_USED}","memery":"${MEM_USED}","disk":"${DISK_USED}","external_disk":"${EXTERNAL_DISK_USED}"}Note: The notification message with "action:0" will be sent periodically if Notification Interval is set.
Notification Interval	Modifies the frequency at which notifications are sent in seconds.No notifications will be sent if the value is "0". Default value: 20
Template Variables	${MAC} : MAC Address${WARNING_MSG} : Warning message${STATUS} : Alarm Status${TIME} : Current System Time${CPU_USED} : CPU Usage${MEM_USED} : Memory Usage${ACTION} : Message Type${DISK_USED} : Local Disk Usage${EXTERNAL_DISK_USED} : Disk Usage

Task Management

The Task Management feature allows users to schedule various tasks to be performed at a configured date and time. Each task can be set to run either once or repeatedly, depending on user requirements.

The tasks that can be scheduled include:

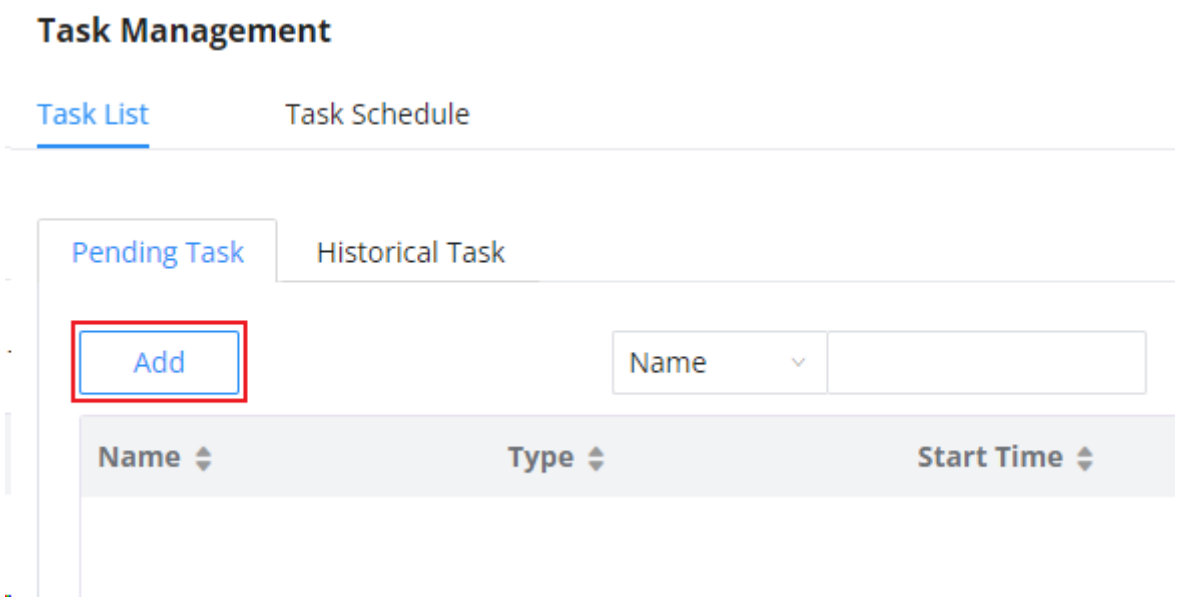
- **Paging/Intercom:** Schedule automated paging or intercom announcements at specific times.
- **Backup:** Schedule automatic backups of system data to USB, SD card, SFTP server, NAS, or Amazon S3. Users can configure multiple backup tasks, each with its own schedule and storage location.
- **Data Sync:** Schedule synchronization of system data with remote servers to ensure data consistency.
- **Cleaner:** Schedule cleaning tasks for system data, such as CDR records, reports, IM messages, and other files, to maintain storage efficiency.
- **Detect New Firmware:** Schedule automatic checks for new firmware versions.
- **Update Country/Region:** Schedule updates for system country/region settings, which are used for Geo-IP Access Control.
- **Update Time Zone:** Schedule updates for the system time zone configuration.

Task List

In the Task List, users can schedule tasks to be performed either once or repeatedly all of the above task types can be scheduled with specific parameters.

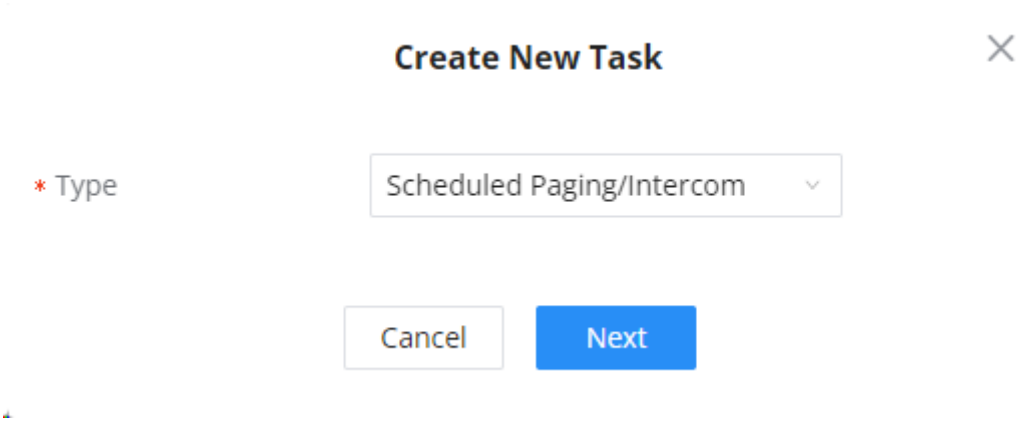
To schedule a task, please follow the steps below:

1. Navigate to **Maintenance->Task Management->Task List->Pending Task**
2. Click on the "Add" button.



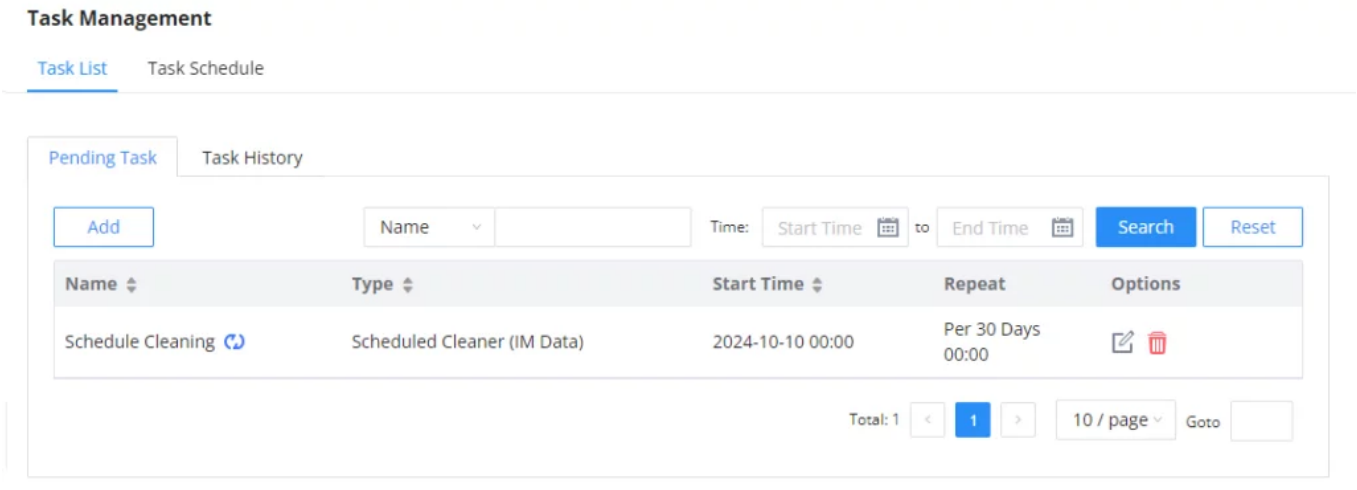
Add Task

3. Select the type of task from the drop-down menu.
4. Click Next and configure the required parameters for the task, such as date, time, frequency, and additional options specific to the task type.



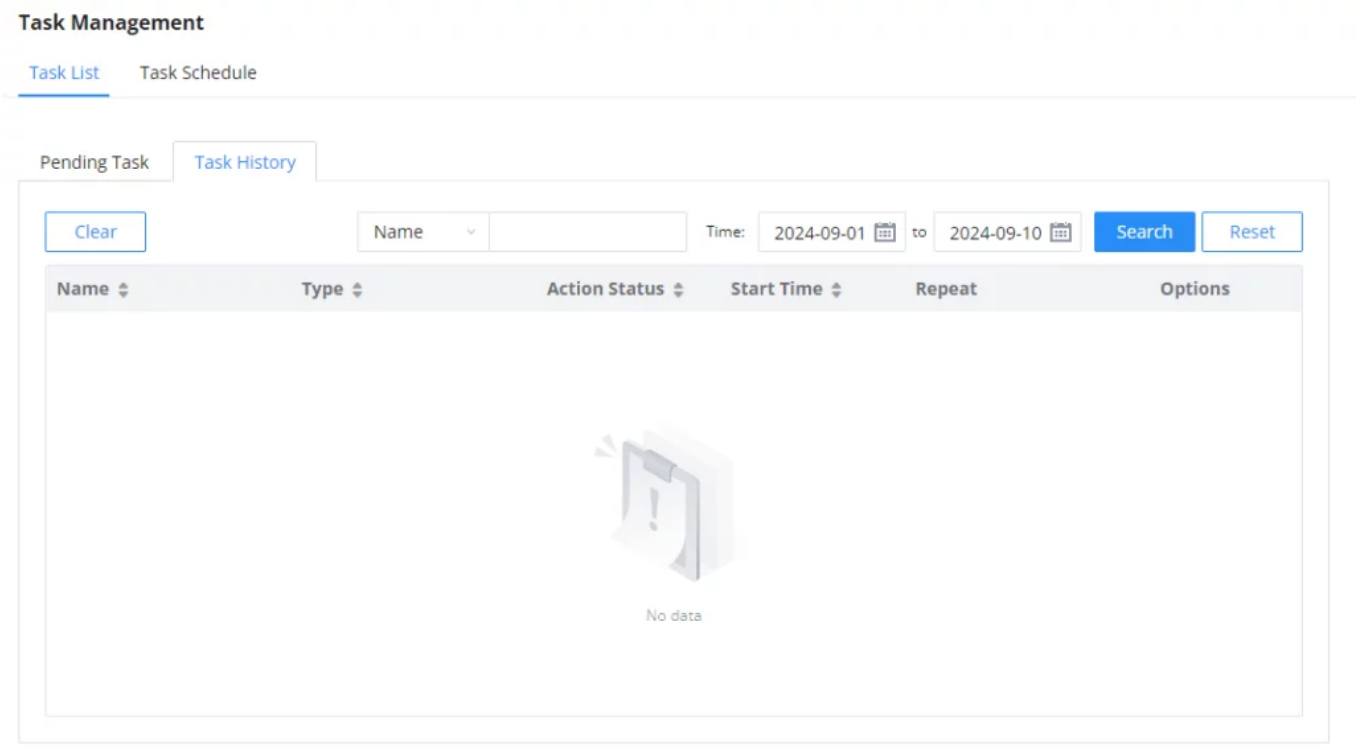
Create New Task

The Pending Tasks section displays all tasks that have been scheduled but not yet executed. Users can review, edit, or delete tasks from this list before execution.



Pending Tasks

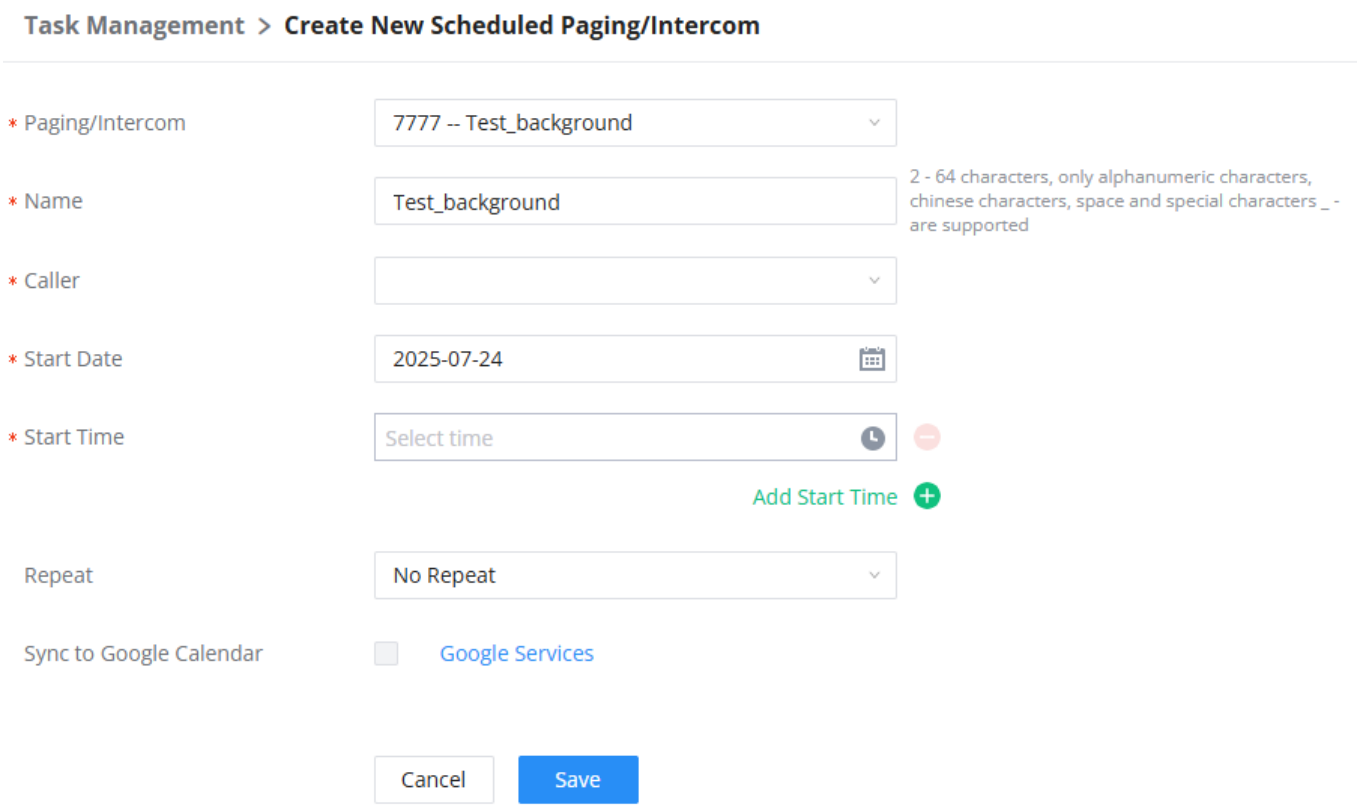
The Task History section logs all tasks that have been performed, including execution time, task type, and status. Users can use this log to verify completed tasks and troubleshoot any issues.



Task History

Scheduled Paging/Intercom

The user can configure a paging or intercom to be initiated automatically according to a schedule. Refer the configuration explained in the table below to be able to configure this feature successfully.

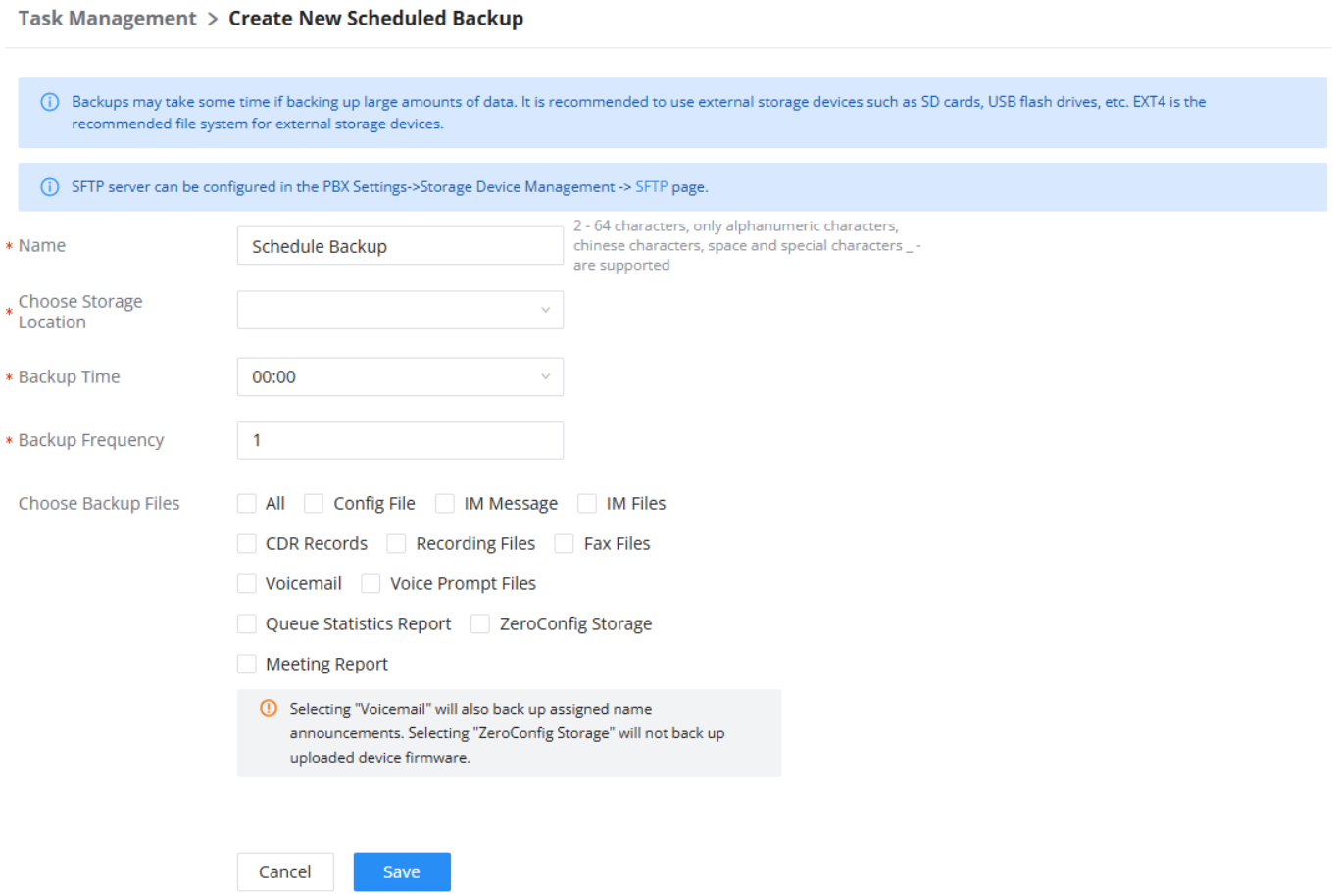


Create New Scheduled Paging

Paging/Intercom	Select pre-existing paging/intercom groups and multicast communities.
Name	Specify the name of the Paging/Intercom schedule.
Caller	When the scheduled time arrives, the system will call this extension. If the call is answered, the paging/intercom will be initiated, if rejected, the paging/intercom will be cancelled.If no caller is specified, the paging/intercom will be directly initiated.
Start Date	Select the start date.
Start Time	Select the start time
Repeat	Select the repeating frequency.No RepeatEvery DayWeeklyMonthly
Sync to Google Calendar	Enabling this option will automatically synchronize the paging/intercom event to the administrator Google Calendar.Note: This requires that the Google Service integration is configured in this specific UCM.

Scheduled Backup

Scheduled backup task management allows the user to schedule regular backups with a specific interval. This provides an efficient and reliable archiving process which can prevent any accidental loss of data.

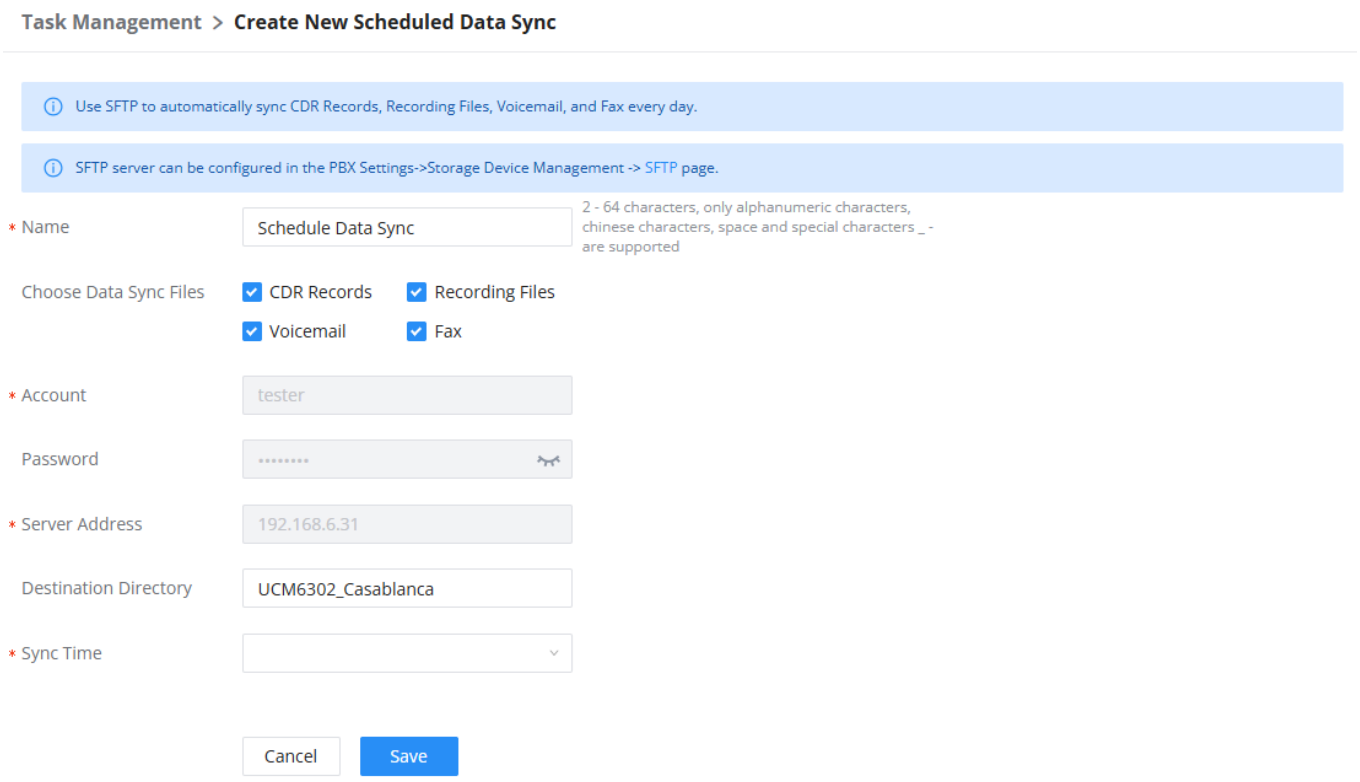


Create New Scheduled Backup

Parameter	Description
Name	Enter the name of the scheduled task.
Choose Storage Location	Choose storage location.NASSFTP ServerUSB DiskSD CardAmazon S3
Date	Specifies the calendar date when the backup task should be executed. Users can select a single date for a one-time backup or a start date for recurring backups.
Time	Defines the exact time of day when the backup task will run. Scheduled backup times must be at least one hour apart from other tasks to avoid conflicts.
Repeat	Determines how often the backup should occur. Options include Every Day, Weekly, Monthly, or Custom for more advanced recurrence settings.
Choose Backup Files	Select the types of files to include in the backup.AllConfig FileIM MessageIM FilesCDR RecordsRecording FilesFax FilesVoicemailVoice Prompt FilesQueue Statistics ReportZero Config StorageMeeting ReportGDS Manager Data

Scheduled Data Sync

Scheduling Data Sync allows the administrator to automate the task of synchronizing the data. When this feature is configured, the UCM will synchronize data to an SFTP server in an incremental way.



Create New Scheduled Data Sync

Parameter	Description
Name	Enter the name of the data sync scheduling.
Choose Data Sync Files	Choose the type of data to synchronize.CDR RecordsRecording FilesVoicemailFax
Account	Enter the username of the account created on the SFTP server.
Password	Enter the password of the account created on the SFTP server.
Server Address	Enter the server address. The port number is not mandatory.
Destination Directory	Enter the directory name on which the data will be store for this specific IPPBX.
Sync Time	Select the time when the synchronization is triggered. We recommend that the synchronization is required outside of the production hours.

Scheduled Cleaner

Scheduled Cleaner allows the user to automate the process of cleaning the files stored in the UCM as well as the attached storage of the UCM.

The following is the list of the types of the cleaner which can be configured for scheduling.

- Scheduled Cleaner (CDR)
- Scheduled Cleaner (Report)
- Scheduled Cleaner (IM Data)
- Scheduled Cleaner (File)

CDR Cleaner

Parameter	Description
Name	Enter the name of the data sync scheduling.
Choose Data Sync Files	Choose the type of data to synchronize.CDR RecordsRecording FilesVoicemailFax

Account	Enter the username of the account created on the SFTP server.
Password	Enter the password of the account created on the SFTP server.
Server Address	Enter the server address. The port number is not mandatory.
Destination Directory	Enter the directory name on which the data will be store for this specific IPPBX.
Sync Time	Select the time when the synchronization is triggered. We recommend that the synchronization is required outside of the production hours.

Report Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (Report) is selected.
Data Type	Select the type of the report to clean automatically.Queue Statistics ReportMeeting Call Statistics ReportMeeting History
Clean Time	Select the time when the cleaning is triggered.
Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the reports which are within this period of time.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

IM Data Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (IM Data) is selected.
Data Type	Select the type of the data to clean automatically.IM FilesIM Message
Clean Time	Select the time when the cleaning is triggered.
Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the files within this period of time.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

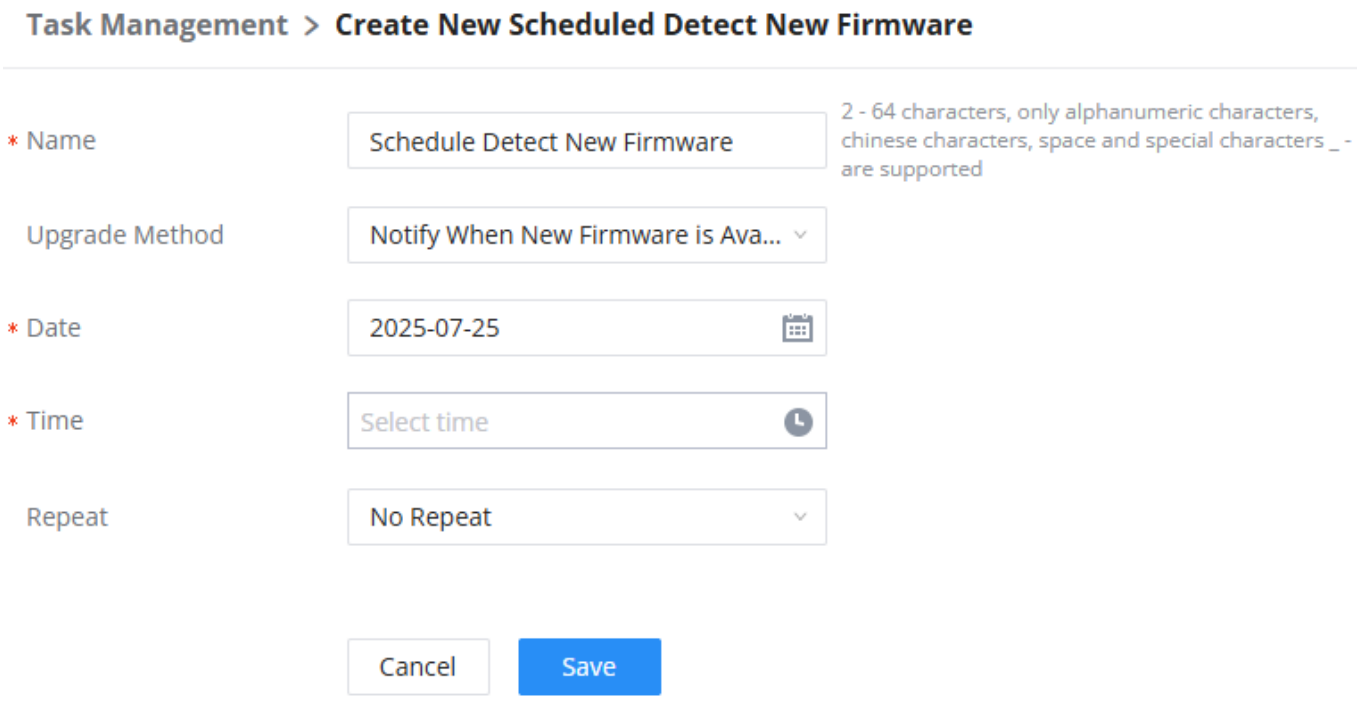
File Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (File) is selected.
Clean Files In External Storage	If enabled, files in the external storage currently being used will be cleaned as configured.

Choose Cleaner Files	Select the file systems for the cleaning.Basic Call RecordingsRecord MeetingMeeting Video RecordingsPaging/Intercom RecordingsPaging/Intercom Video RecordingsQueue RecordingsVoicemail FilesEmergency RecordingsFaxSCA RecordingsBackup Files
Clean Time	Select the time when the cleaning is triggered.
Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the files which are within the period range.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

Scheduled Detect New Firmware

Task scheduling for detecting new firmware allows the user to automate the process of verifying the availability of a new firmware update. Using this feature can ensure that the administrator is notified as soon as there is a new update of the UCM6300 Series software.



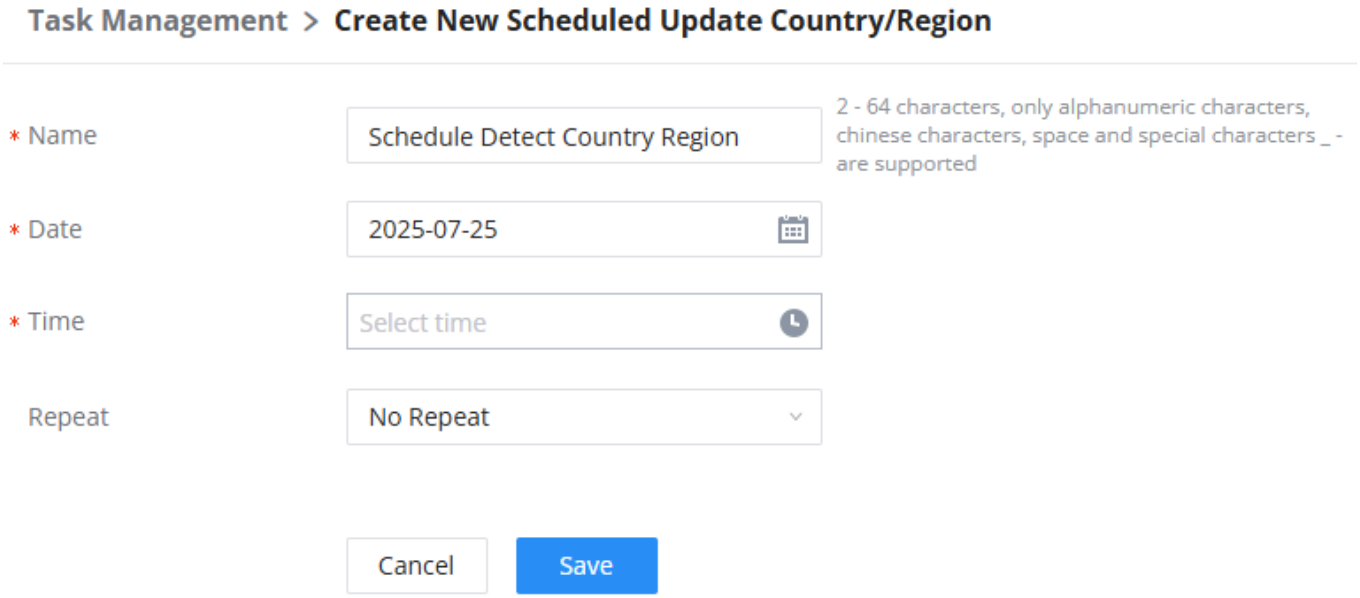
Create New Scheduled Detect New Firmware

Parameter	Description
Name	Configure the name of the scheduled task.
Upgrade Method	Select the action when a new firmware is detected.Notify When a New Firmware is AvailableAuto Download and Upgrade Firmware
Email Reminder Before Upgrade (m)	This option appears when you select Auto Download and Upgrade Firmware.
Date	Select the date when the firmware detection first starts.
Time	Select the time when the firmware is detected.

Repeat	Select the frequency of the detection.No RepeatEvery DayWeeklyMonthly

Scheduled Update of Country/Region List

Scheduling a regular update of the Country/Region List ensures keeping the list for Geo-IP Access Control up to date with any emergence of new countries or name-change of existing countries. This also allows receiving the update without having to wait for a new firmware release.

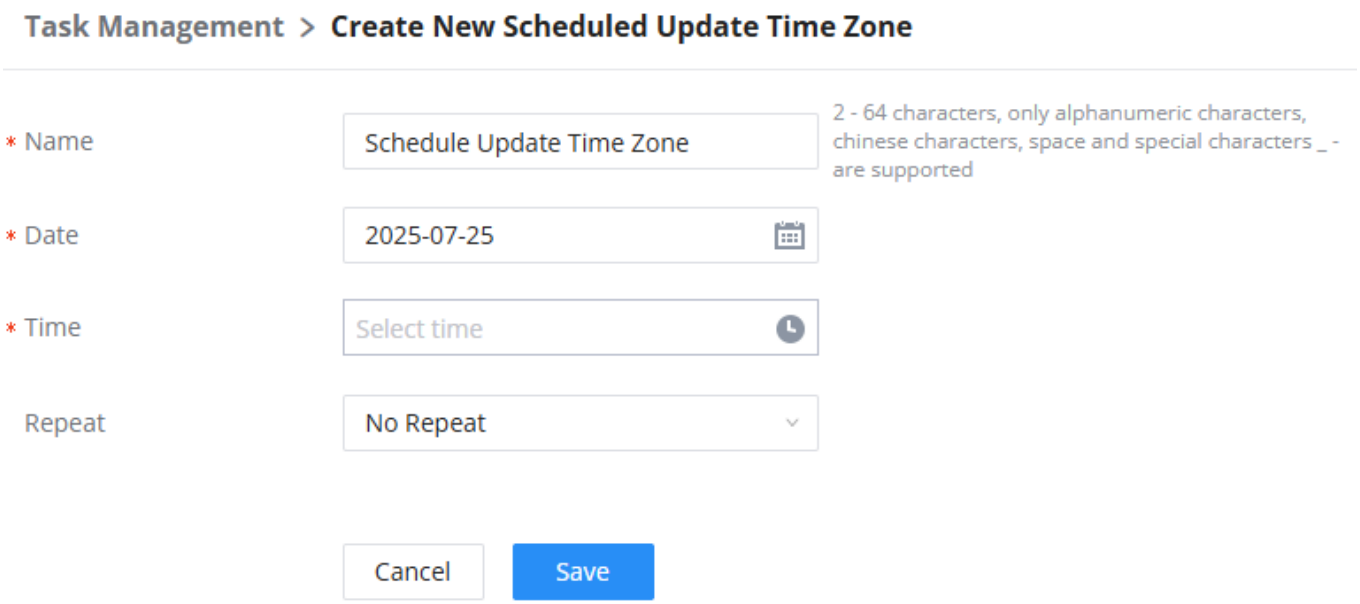


Create New Scheduled Update Country/Region

Parameter	Description
Name	Enter the name of a scheduled task
Date	Enter the date
Time	Enter the time
Repeat	Select the frequency of the updateNo RepeatEvery DayWeeklyMonthly

Schedule Update Time Zone

Scheduling update for timezones ensures that the list can be updated regularly and without the need to wait for a new firmware release.

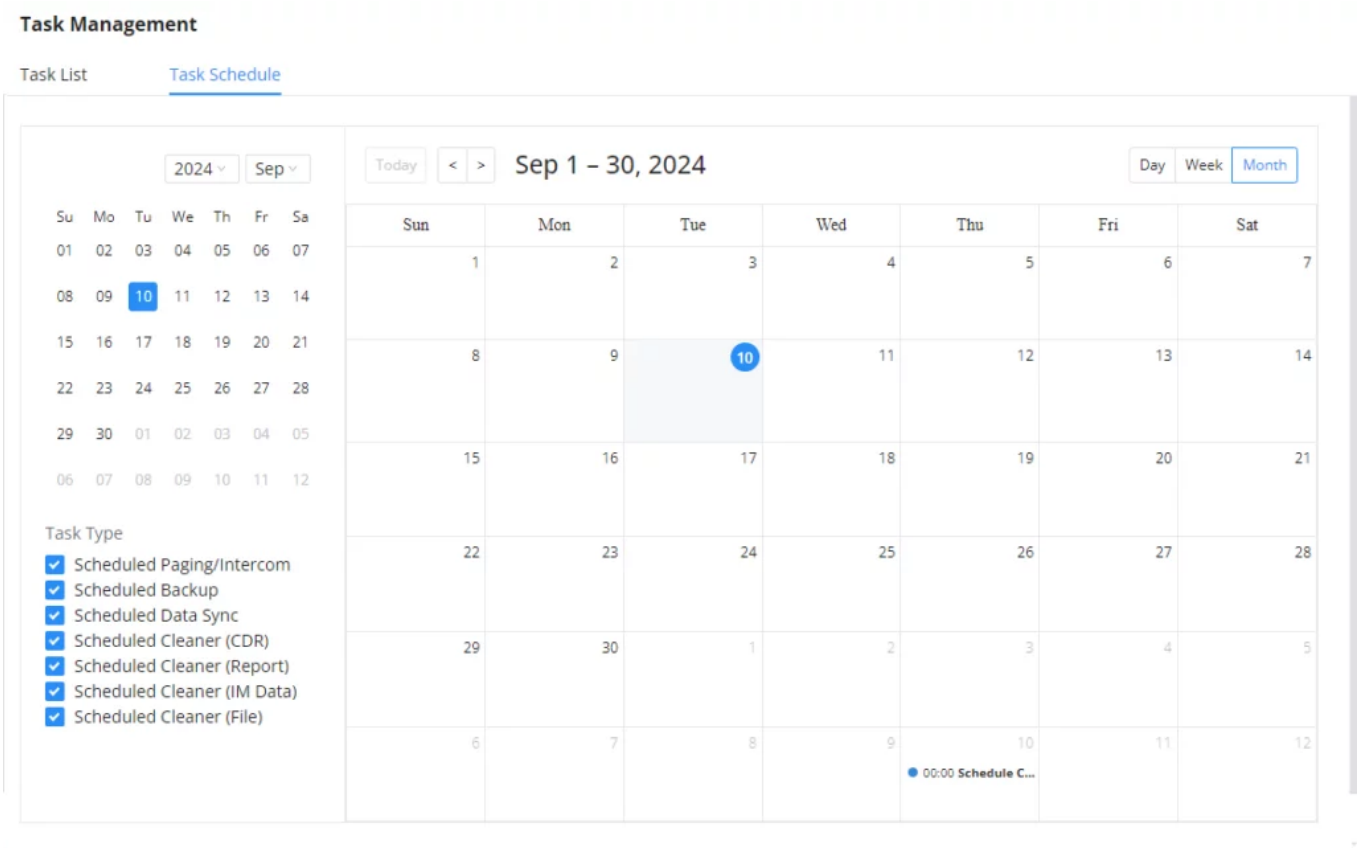


Create New Scheduled Update Time Zone

Parameter	Description
Name	Enter the name of the data sync scheduling.
Choose Data Sync Files	Choose the type of data to synchronize.CDR RecordsRecording FilesVoicemailFax
Account	Enter the username of the account created on the SFTP server.
Password	Enter the password of the account created on the SFTP server.
Server Address	Enter the server address. The port number is not mandatory.
Destination Directory	Enter the directory name on which the data will be store for this specific IPPBX.
Sync Time	Select the time when the synchronization is triggered. We recommend that the synchronization is required outside of the production hours.

Task Schedule

To get an overview about all the tasks which have been scheduled, the user can click on **Task Schedule** tab to view the full schedule.

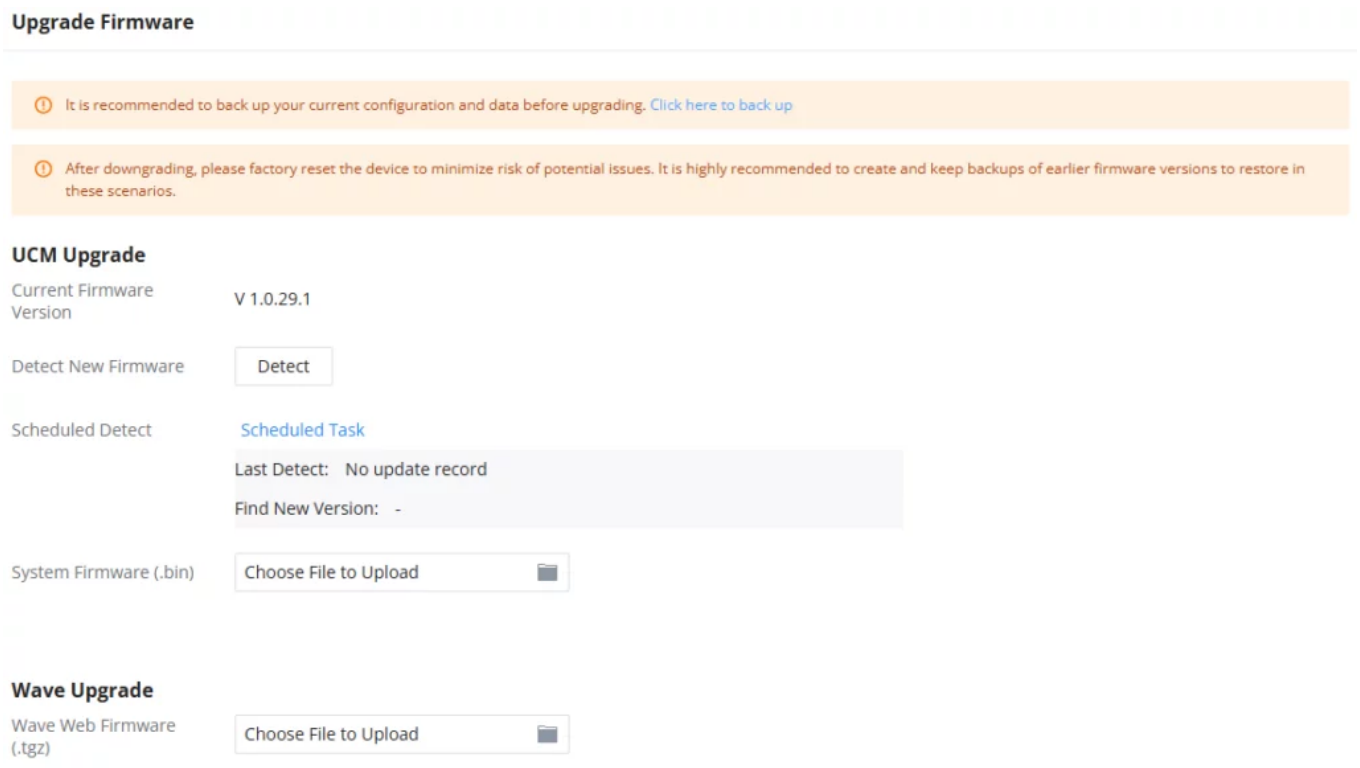


Upgrade

During its lifetime, the UCM6300 Series models will receive regular updates. These updates include new features and functionalities, bug fixes, security patches, and general improvements to the security and performance of the device. It is highly recommended that you keep the firmware of your UCM up to date.

Before proceeding with the firmware upgrade, please visit https://www.grandstream.com/support/firmware and download the latest firmware available for the UCM. Once the file has been download, please decompress the file, you will get a .bin file, that's the file which will uploaded to the UCM.

To upgrade the firmware of the UCM6300 Series, please access the web UI of the UCM, then navigate to **Maintenance > Upgrade**



Upgrade Firmware

On this page, the user can view the firmware version which is installed on the UCM. Clicking "Detect" will initiate firmware version verification, if there is a newer version, a prompt will appear to confirm downloading and installing the firmware.

The user can also schedule detection of the firmware version by clicking on "Schedule Task". For more information regarding scheduling tasks, please refer to [Task Management] section.

1. Click on "Choose File to Upload" field in front of "System Firmware (.bin)"
2. (Optional) To upgrade Wave Web use the field for "Wave Web Firmware (.tgz)"
3. Use the window to navigate to where the firmware file is located then select it.
4. Once the firmware file has been selected, the file will be uploaded to the UCM and the upgrade will begin.
5. A prompt will appear to reboot the device to finalize the upgrade.

Backup

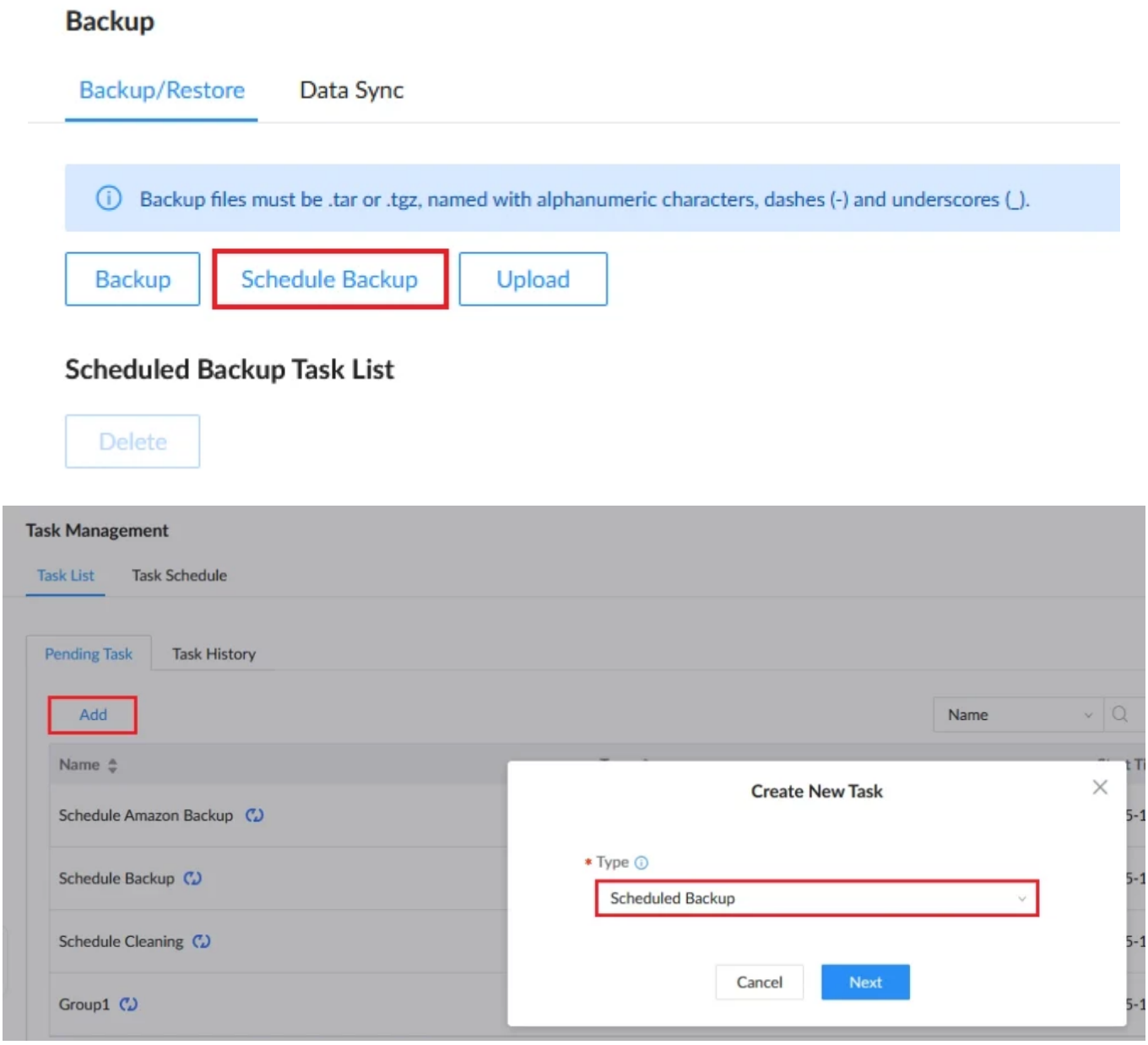
Backup/Restore

Click on "Upload" to upload a backup file from the local device to the UCM630X. The uploaded backup file will be displayed on the web page and can be used to restore the UCM630X.

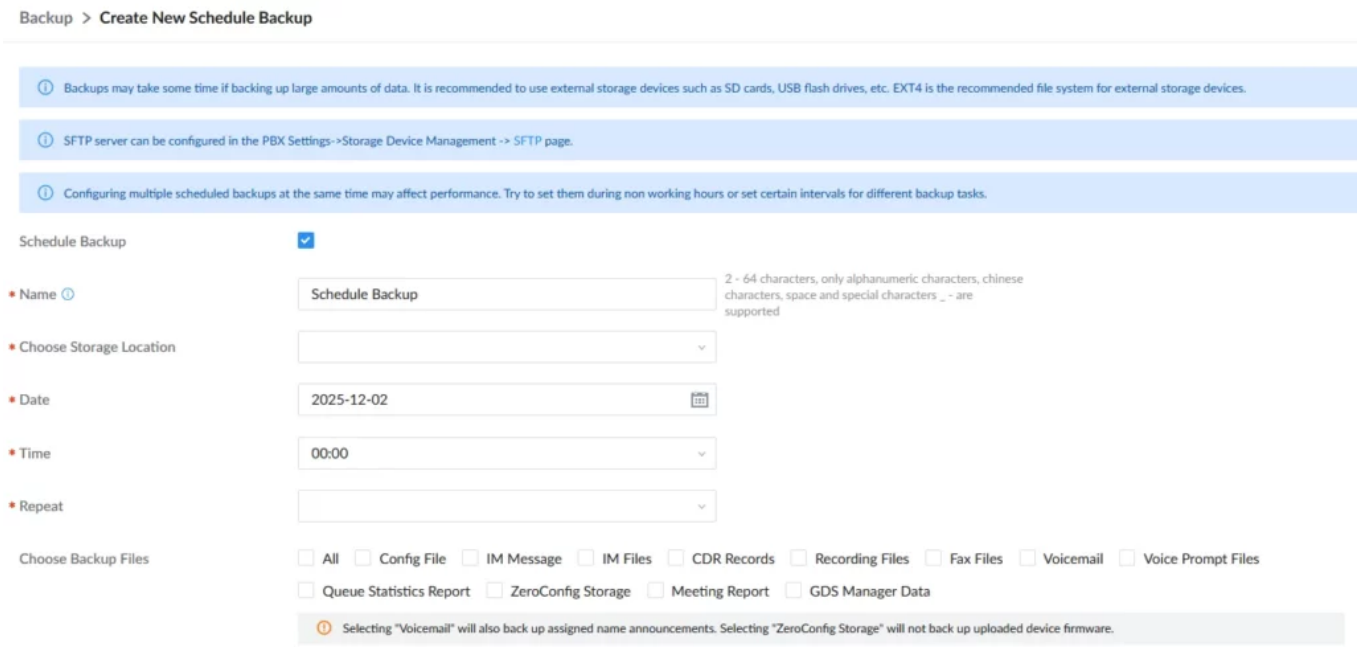
The **Scheduled Backup** feature enables UCM to automatically back up selected data according to defined schedules. Users can configure multiple backup tasks, each with its own schedule and storage destination, while ensuring that no two backups run simultaneously. Supported storage options include USB, SD card, SFTP server, NAS, and Amazon S3 storage.

To configure a scheduled backup, please refer to the steps below:

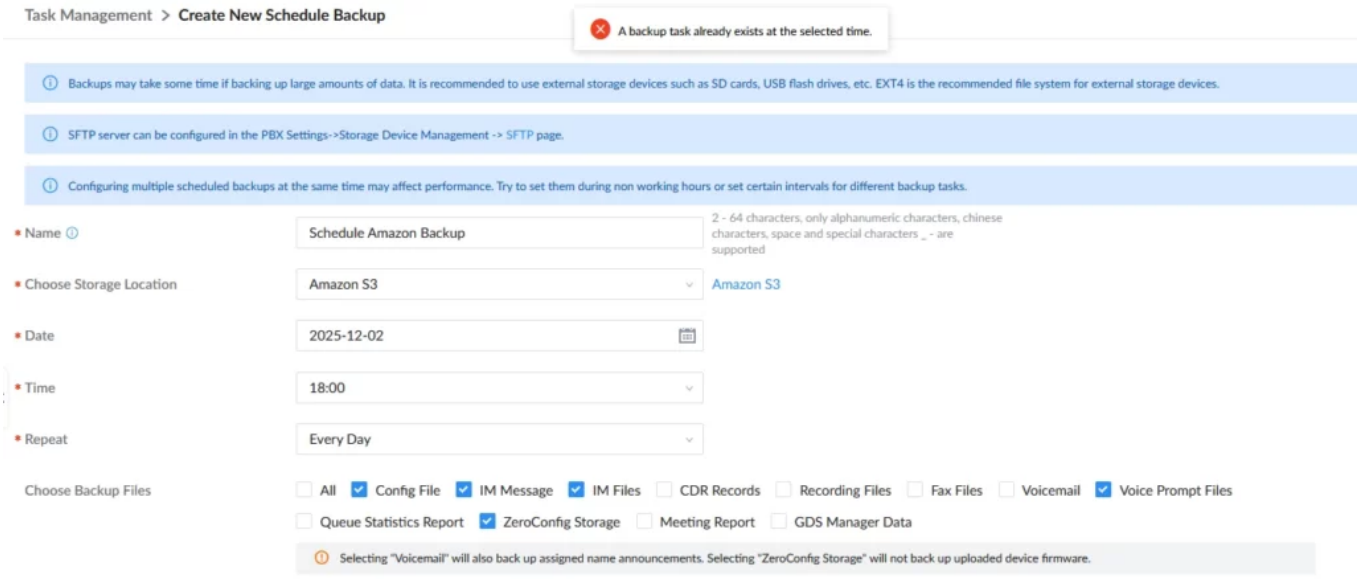
1. Access the Schedule Backup feature either by clicking the "Schedule Backup" button on the **Maintenance->Backup** page or by creating a new task in the **Maintenance->Task Management** page.



2. Check the Schedule Backup option checkbox to activate backup scheduling.
3. Enter a name for the task (should be between 2 and 64 characters. Names can include alphanumeric characters, Chinese characters, spaces, and the special characters _ and -).
4. Select the desired storage destination, such as USB, SD card, SFTP server, NAS, or Amazon S3. The same location can be used for multiple tasks as long as each task is scheduled at a different time.
5. Specify the date and time for the backup. Scheduled backup times must be at least one hour apart.

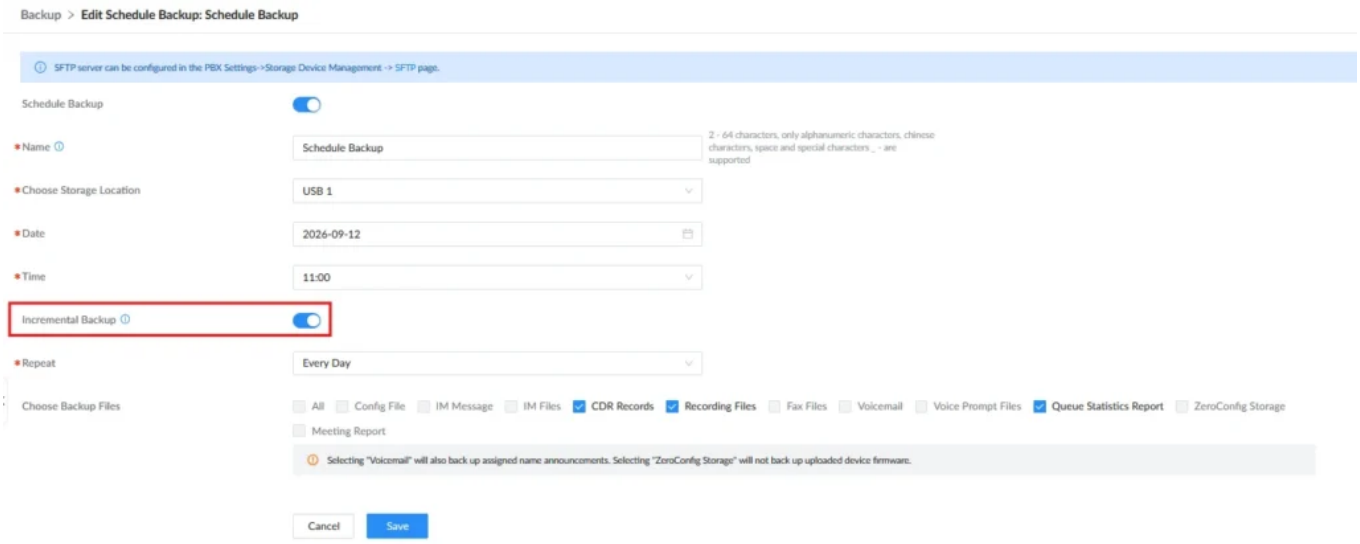


The system does not allow two backup tasks to be scheduled at the same time. If users attempt to create overlapping tasks, the configuration will be blocked because simultaneous backups can affect system performance.



6. Choose how often the backup should occur: Every Day, Weekly, Monthly, or Custom.
7. **Incremental Backup (Optional):** When a supported target storage device (USB, SD Card, or NAS) is selected, users can enable the Incremental Backup option. When enabled, the system automatically backs up data added or modified during the previous cycle (specifically CDR Records, Recording Files and Queue Statistics Reports) rather than creating a full system copy.

- Example: For a monthly incremental backup task running on the 28th, the backup data range will cover from the 28th of the previous month (00:00:00) to the 27th of the current month (23:59:59). If a scheduled day (e.g., 29th, 30th, or 31st) does not exist in a given month, the task automatically executes on the last day of that month.



8. Choose which data to include in the backup. Options include: All, Config File, IM Message, IM Files, CDR Records, Recording Files, Fax Files, Voicemail, Voice Prompt Files, Queue Statistics Report, ZeroConfig Storage, Meeting Report, and GDS Manager Data.
9. Users can view both scheduled backup tasks and completed backup tasks in the **Maintenance->Task Management** page. Within this page, the **Task List** displays all the pending and completed tasks, while the **Task Schedule** shows the timing and recurrence of upcoming backups.

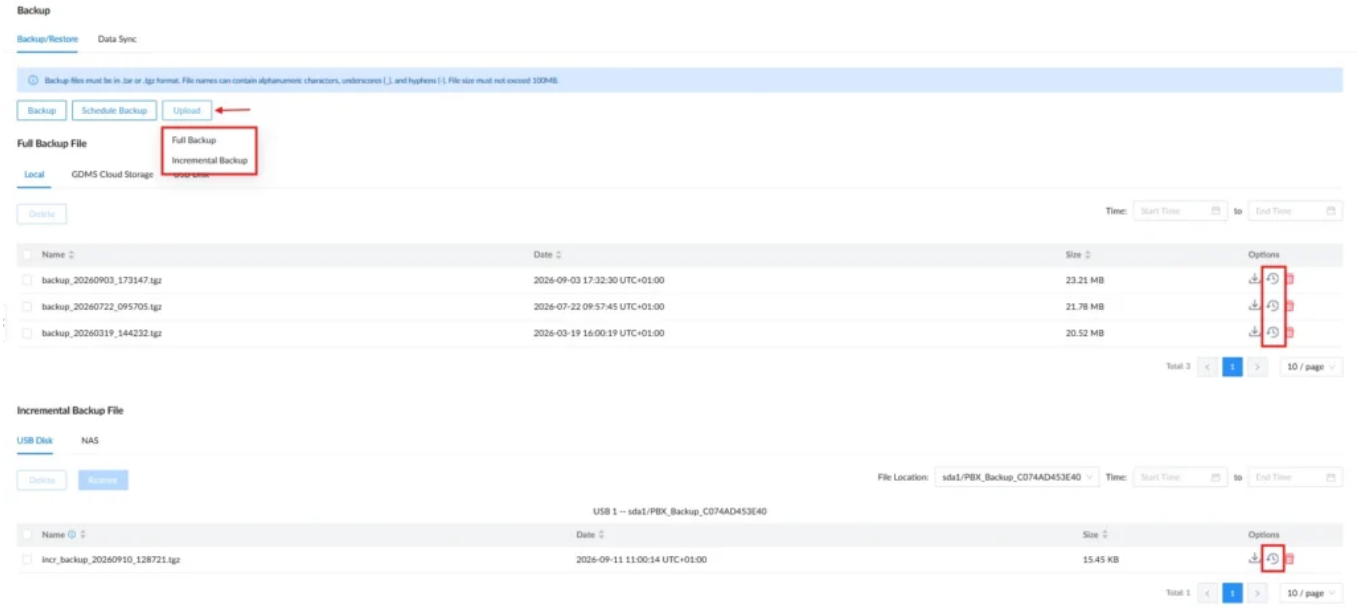
AI transcripts are included in backups as follows:

- AI call transcripts and meeting transcripts are backed up with the **CDR Records**
- AI transcripts generated from recording files are backed up with the **Recording Files**. After restore, the transcripts can be viewed with their recording files.

Restore Configuration from Backup File

To restore the configuration on the UCM630X from a backup file, users can go to **Maintenance**->**Backup**->**Backup/Restore**.

- A list of previous configuration backups is displayed on the web page. Users can click on the "Clock" (Restore) icon of the desired backup file to restore it to the UCM630X.
- If the backup was stored on GDMS, it will be displayed under **Backups GDMS Cloud Storage**, and can be restored by clicking on the "Clock" icon.
- If an active storage target contains incremental backup files, they will be listed under the **Incremental Backup File** section (categorized by storage tab, e.g., NAS, USB, or SD Card). Selecting multiple incremental packages and clicking **Restore** will automatically link and restore them in chronological order up to the target date.
- If users have other backup files on a PC to restore on the UCM630X, click on "Upload Backup File" first and select it from the local PC to upload to the UCM630X. Once the upload is complete, the backup file will be displayed in the list of previous configuration backups for restoration. Click on the "Clock" icon to restore from the backup file.



- The uploaded backup file must be a .tar or .tgz file with no special characters like *,!,#,@,&,$,%,^,(,),/,\,space in the file name.
- The uploaded backup file size must be under 100MB.

Record History

The **Record History** table provides a log of all executed backup tasks on the UCM630X. It allows administrators to review the status, details, and schedules of past backup operations.

Backup packages stored on Amazon S3 or SFTP can only be viewed and downloaded directly from their respective remote servers.

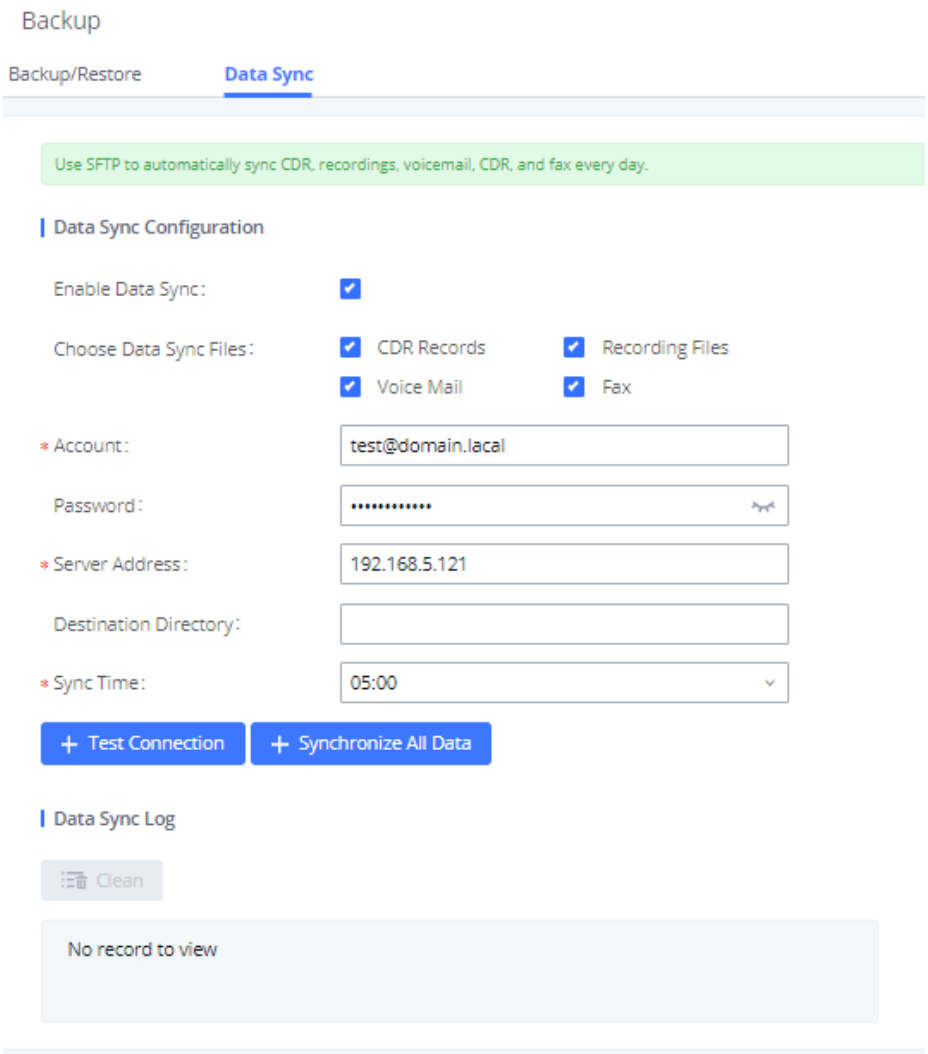
The table below describes the parameters and information displayed in the Record History section:

Option	Description
Name	Displays the name assigned to the backup task (e.g., Realtime Backup).
Storage Location	Indicates the target destination where the backup package was saved (e.g., Local, USB, SD Card, or NAS).
Type	Displays the operation type of the task (e.g., Backup).
Task Status	Displays the execution state of the backup task (e.g., Executed, Failed, or In Progress).
Start Time	Displays the exact timestamp when the backup task began execution.
Repeat	Indicates the recurrence schedule configured for the backup task (e.g., No Repeat, Every Day, Weekly, Monthly).
Options	Allows administrators to manage history entries, such as clicking the Delete (Trash) icon to remove specific records from the log list.

Data Sync

Besides local backup, users could backup the voice records/voice mails/CDR in a daily basis to a remote server via SFTP protocol automatically under **Maintenance > Backup > Data Sync**.

The client account supports special characters such as @ or "." Allowing the use email address as SFTP accounts. It allows users as well to specify the destination directory on SFTP server for backup file. If the directory does not exist on the destination, UCM630X will create the directory automatically



Data Sync

Enable Data Sync	Enable the auto data sync function. The default setting is "No".
Account	Enter the Account name on the SFTP backup server.
Password	Enter the Password associate with the Account on the SFTP backup server.
Server Address	Enter the SFTP server address.
Destination Directory	Specify the directory in SFTP server to keep the backup file. Format: 'xxx/xxx/xxx', If this directory does not exist, UCM will create this directory automatically.
Sync Time	Enter 0-23 to specify the backup hour of the day.

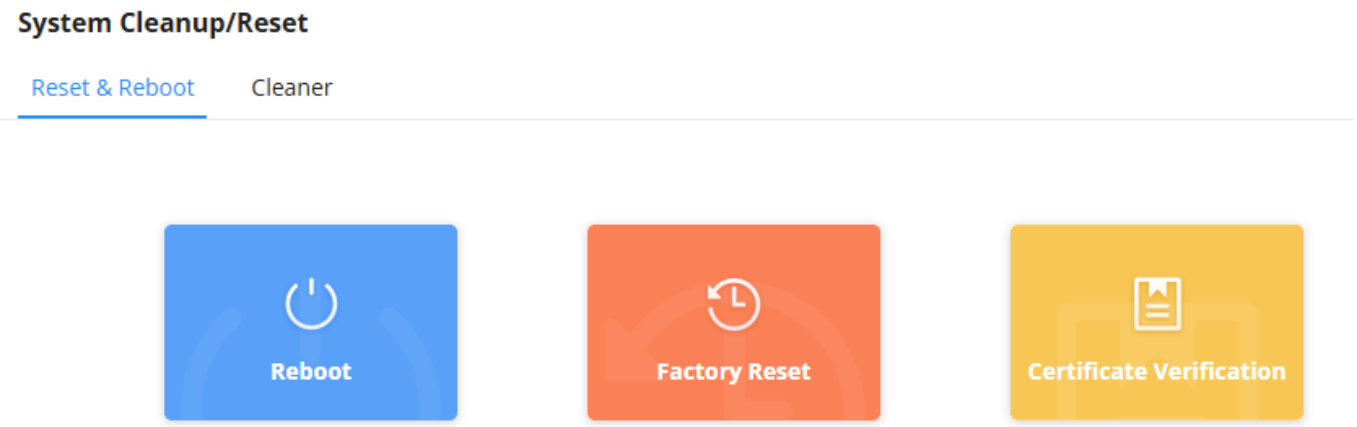
Before saving the configuration, users could click on . The UCM630X will then try connecting the server to make sure the server is up and accessible for the UCM630X. Save the changes and all the backup logs will be listed on the web page. After data sync is configured, users could also manually synchronize all data by clicking on instead of waiting for the backup time interval to come.

System Cleanup/Reset

Reset and Reboot

Users could perform reset and reboot under **Maintenance > System Cleanup/Reset > Reset and Reboot**.

- To reboot the device, click on reboot icon.
- To factory reset the device, click on reset icon, then all the configurations and data will be reset to factory default.



Reset and Reboot

- User can also verify UCM certificate under the same path.

Cleaner

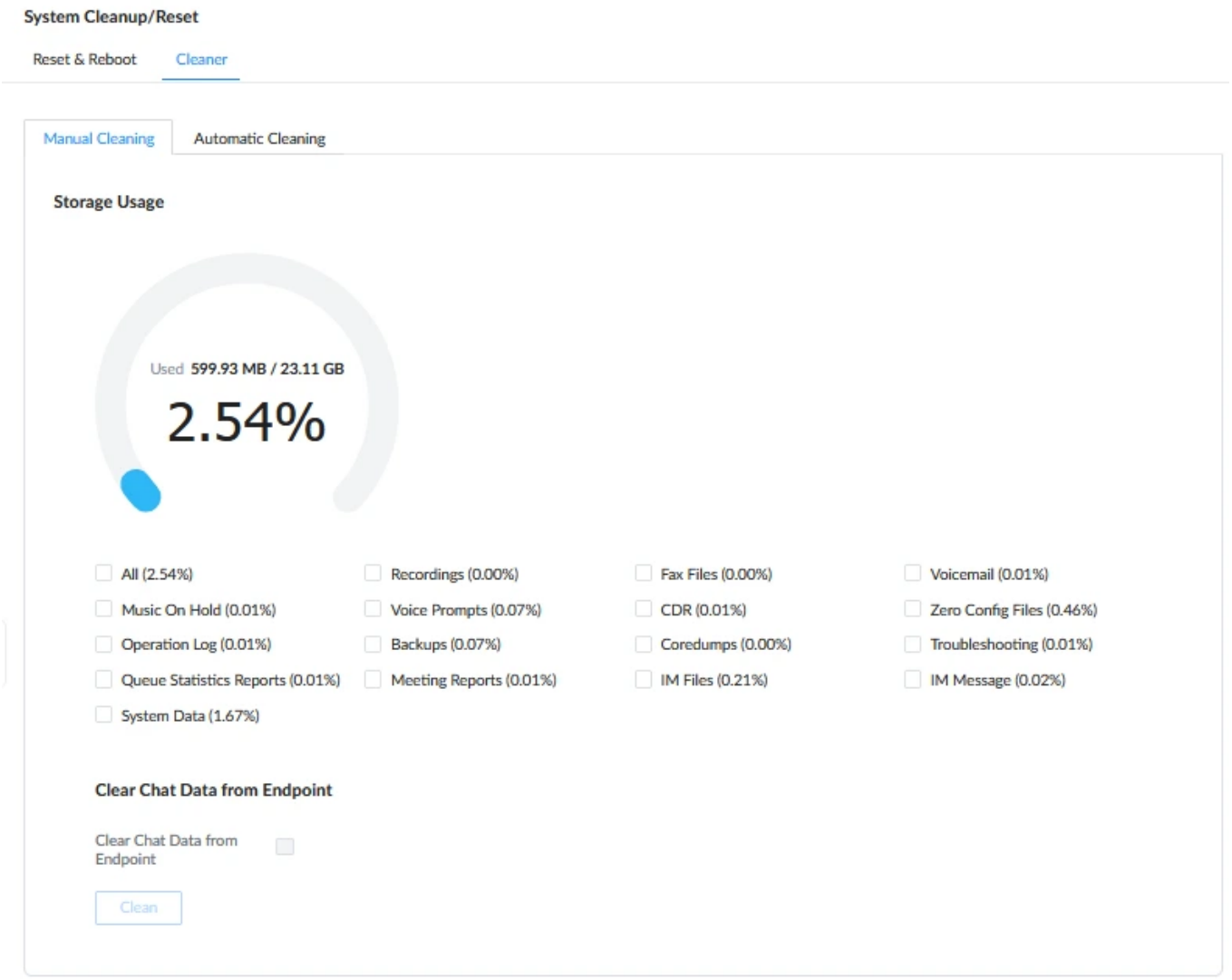
Users can configure the system to clean Call Detail Records (CDRs), voice recordings, voicemails, reports, chat data, meeting history, fax files, backup files, and other stored data either manually or automatically. The Cleaner feature is available under **Maintenance->System Cleanup/Reset->Cleaner**.

UCM provides the ability to manually clean a variety of data types, including CDRs, report data, chat messages and shared files, recording files, meeting history records, voicemails, fax files, and backup files. Report data includes queue statistics reports and conference call statistics, meeting history includes audio and video conference appointment records.

AI Transcripts and Summaries are automatically or manually cleared according to their source:

- **AI Recording Transcripts:** Follow the Recordings and Video Recordings cleanup rules.
- **Call & Meeting Transcripts:** Tied directly to CDR records and are cleared whenever CDR records are cleared.
- **Voicemail Transcriptions:** Follow the Voicemail cleanup rules.

The following screenshot illustrates the settings and parameters available for configuring the Manual Cleaning feature on UCM630X.

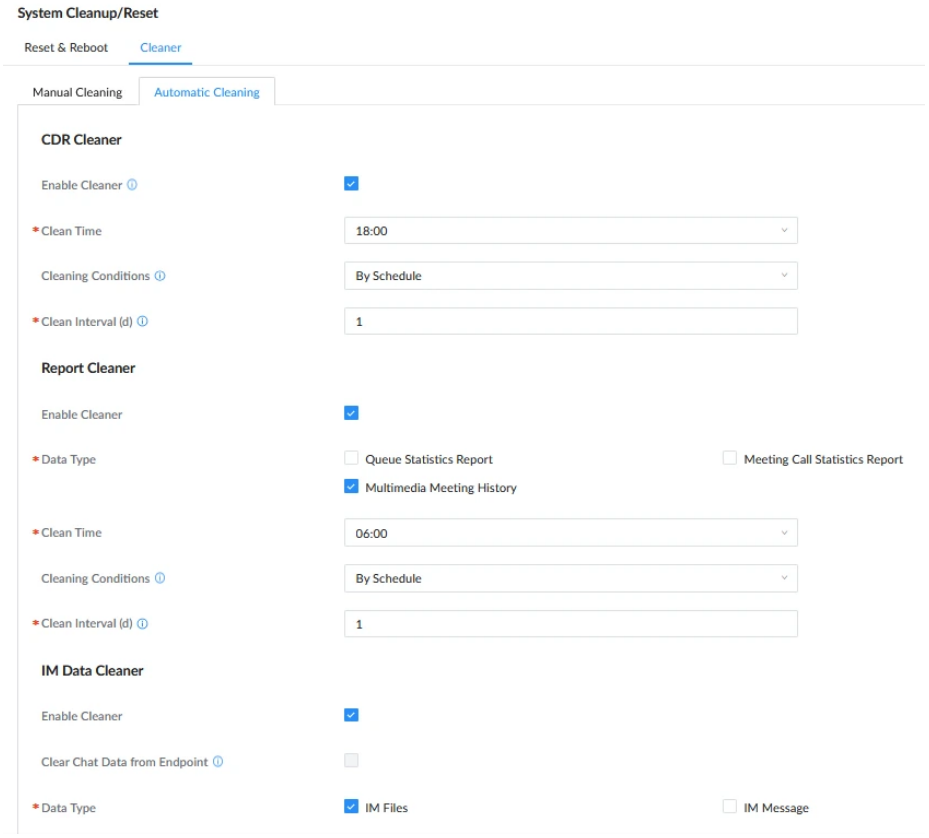


Manual Cleaning Tab

Automatic cleanup is not enabled by default. When configured, automatic cleanup supports scheduled deletion of file data based on parameters such as cleanup time, cleanup conditions, and cleanup intervals.

Users can configure Automatic Cleaning by navigating to **Maintenance->System Cleanup/Reset->Cleaner->Automatic Cleaning,** or by creating an automated cleaning task under **Maintenance->Task Management**.

The following screenshot shows some available parameters for configuring automatic cleanup on UCM630X.



Automatic Cleaning Tab

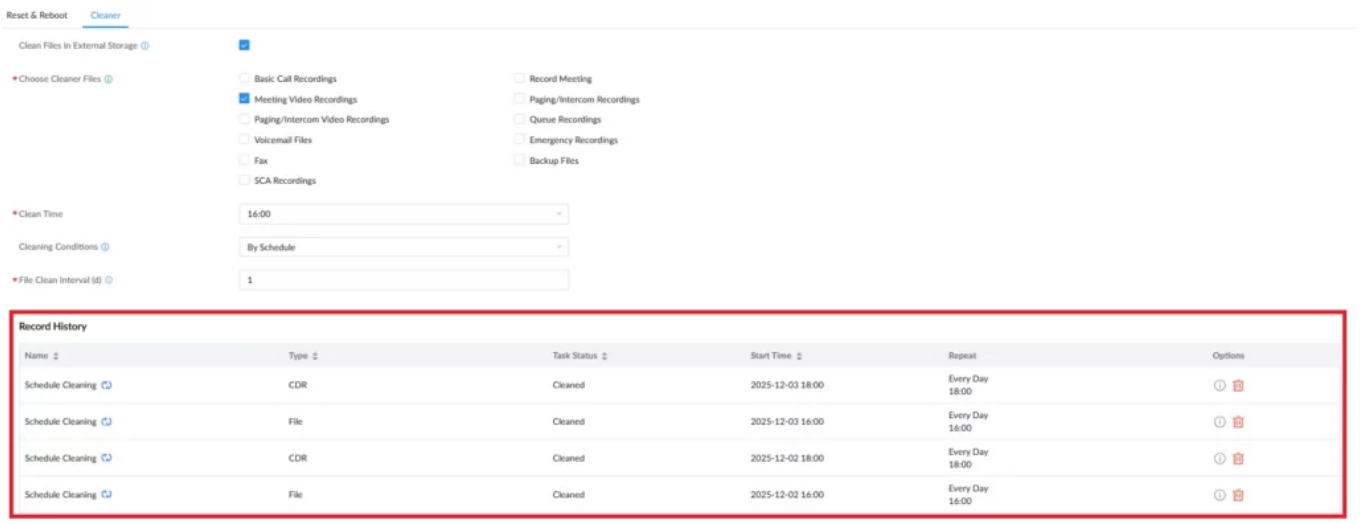
The table below describes all the configurable options that can be configured for automatic cleaning:

CDR Cleaner	
Enable Cleaner	Enable the CDR Cleaner function.Note: AI call and meeting transcript files are removed alongside cleared CDR records
Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated in the past 3 days.Keep Last X Records: If the max number of CDR has been reached, CDR will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval (d)	Enter 1-30 to specify the day of the month to clean up CDR when By Schedule is selected as Cleaning Conditions.
Max Entries	Set the maximum number of CDR entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
Report Cleaner	
Enable Cleaner	Enable scheduled queue log cleaning.
Data Type	Select a type of data to clean. Queue Statistics ReportMeeting Call Statistics ReportMultimedia Meeting History
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.

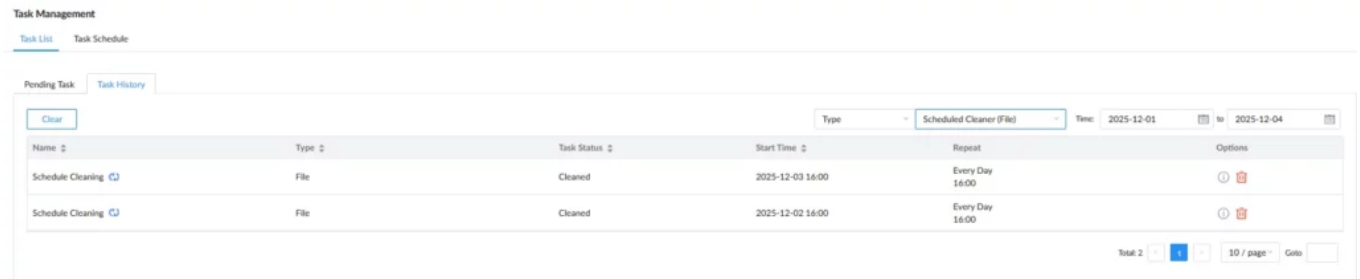
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.Keep Last X Records: If the max number of Queue Statistics Report entries has been reached, Queue Statistics Report entries will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.
Max Entries	Set the maximum number of Queue Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of Queue Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
IM Data Cleaner	
Enable Cleaner	Enable IM data cleaner
Clear Chat Data from Endpoint	This option allows users to clean endpoint chat data and is only available when the selected data type includes IM messages. It is disabled by default.
Data Type	Select a type of file to clean.IM Files IM Messages
Clean time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.Keep Last X Records: If the max number of Conference Call Statistics Report has been reached, Conference Call Statistics Report will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.
Max Entries	Set the maximum number of CDR Conference Call Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of Conference Call Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
File Cleaner	
Enable Cleaner	Enabling files cleaning.
Clean Files in External Device	If enabled the files in external device will be automatically cleaned up as configured.
Choose Cleaner File	Select the files for system automatic clean.Basic Call Recording FilesMeeting Recording FilesMeeting Video Recordings Paging/Intercom Recordings Paging/Intercom Video Recordings Call Queue Recording FilesVoicemail FilesEmergency Calls Recording FilesFax Backup Files SCA Recording FilesNote: The AI recording transcript files are deleted alongside their associated audio/video recording files.
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to delete all files.By Threshold: Check at the configured cleaning time every day to see if the storage threshold has been exceeded and perform cleaning of all files if it has.Keep Last X Days: Delete all files older than X days.
File Clean Interval	Enter 1-30 to specify the day of the month to clean up the files.

File Clean Threshold	Enter the internal storage disk usage threshold (in percent). Once this threshold is exceeded, the file cleanup will proceed as scheduled. Valid range is 0-99.
Keep Last X Days	Automatically delete all recordings older than this x days when the threshold is reached. If not set, all data is cleared. Valid range: 1 - 730.
Record History	
Name	Shows the identifier for the cleanup task.
Type	Specifies the category of cleanup the task performs
Task Status	Shows the final state of the cleanup task.
Start Time	The exact date and time when the cleanup task was triggered.
Repeat	Indicates the schedule for automatic repetition (if enabled).
Options	Provides the available actions for each task, such as Info and Delete. The Delete action removes the task from the record history, while the Info action displays details about the cleaned files.

When automatic cleaning tasks run, the system logs the cleaning results, allowing users to review each task results, including the total size cleaned and number of items removed, by checking either the **Cleaner** page or the **Task Management** sections (**Task History**).



Checking Cleaning Records from the Cleaner Page



Checking Cleaning Records from Task History

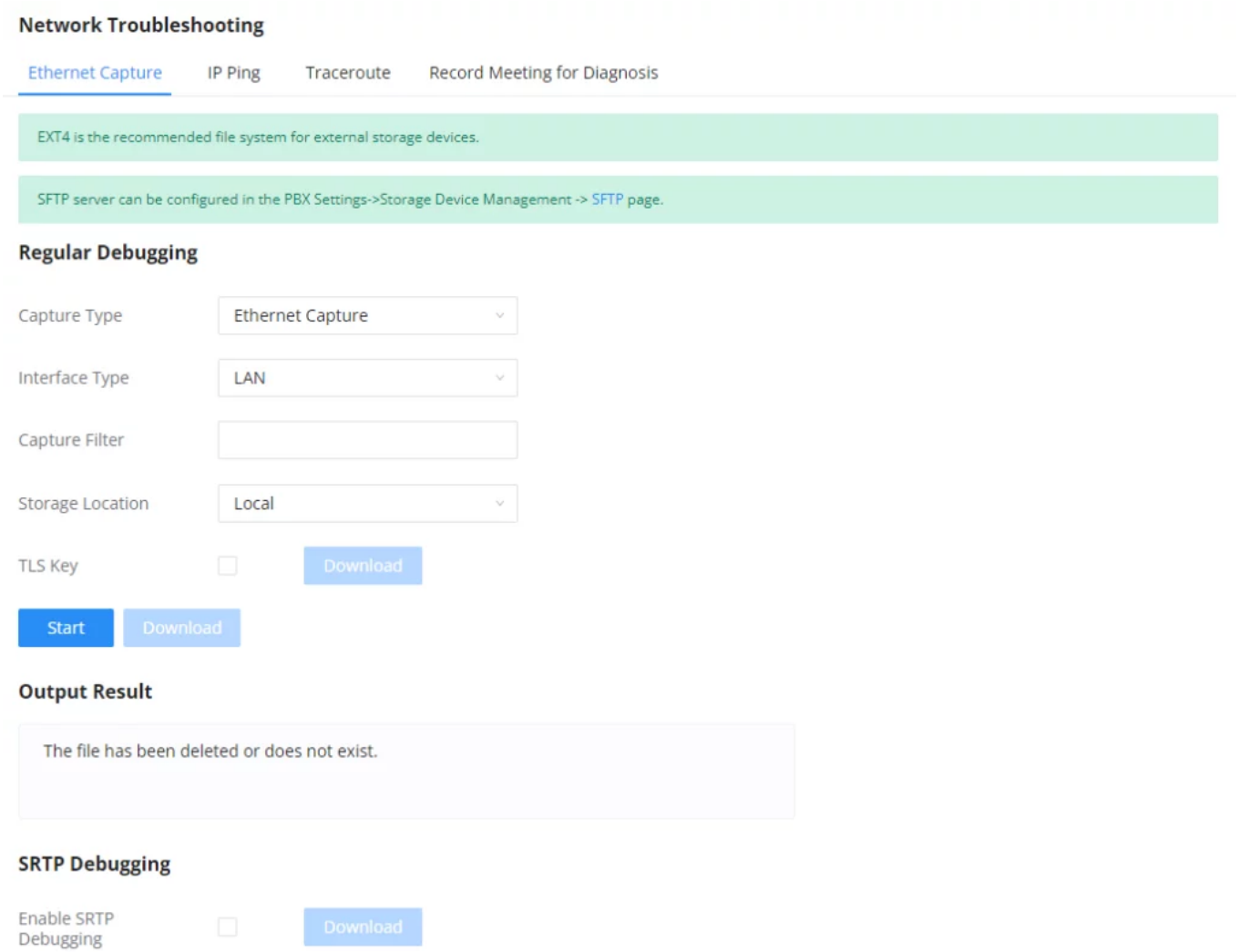
Network Troubleshooting

On the UCM630X, users could capture traces, ping remote host and traceroute remote host for troubleshooting purpose under **Maintenance > Network Troubleshooting**.

The following sections shows the steps to capture different types of traffic traces for analysis purposes.

Ethernet Capture

Ethernet Capture allows capturing the traffic of the UCM for troubleshooting purposes. To access Ethernet Capture feature, please navigate to **Maintenance > Network Troubleshooting > Ethernet Capture**



Ethernet Capture

The capture packets can be stored locally and downloaded for analysis. However, if the user is diagnosing a randomly-occurring issue, he/she can run a continuous packet capture which can be limited by the size of the packet capture and the number of packet capture instances

When the maximum packet capture file size is reached, a new packet capture file will be created. When the maximum number of capture files number is reached, then the UCM will delete the oldest file created file and replace it with the new one.

Parameter	Description
Capture Type	Ethernet Capture: Gets a packet capture of all network traffic going through the device.WebSocket Capture: Gets a packet capture of WebSocket protocol. Mainly used for troubleshooting Wave Web calling and conferencing issues.
Interface Type	Select the network interface to monitor.
Capture Filter	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto...).

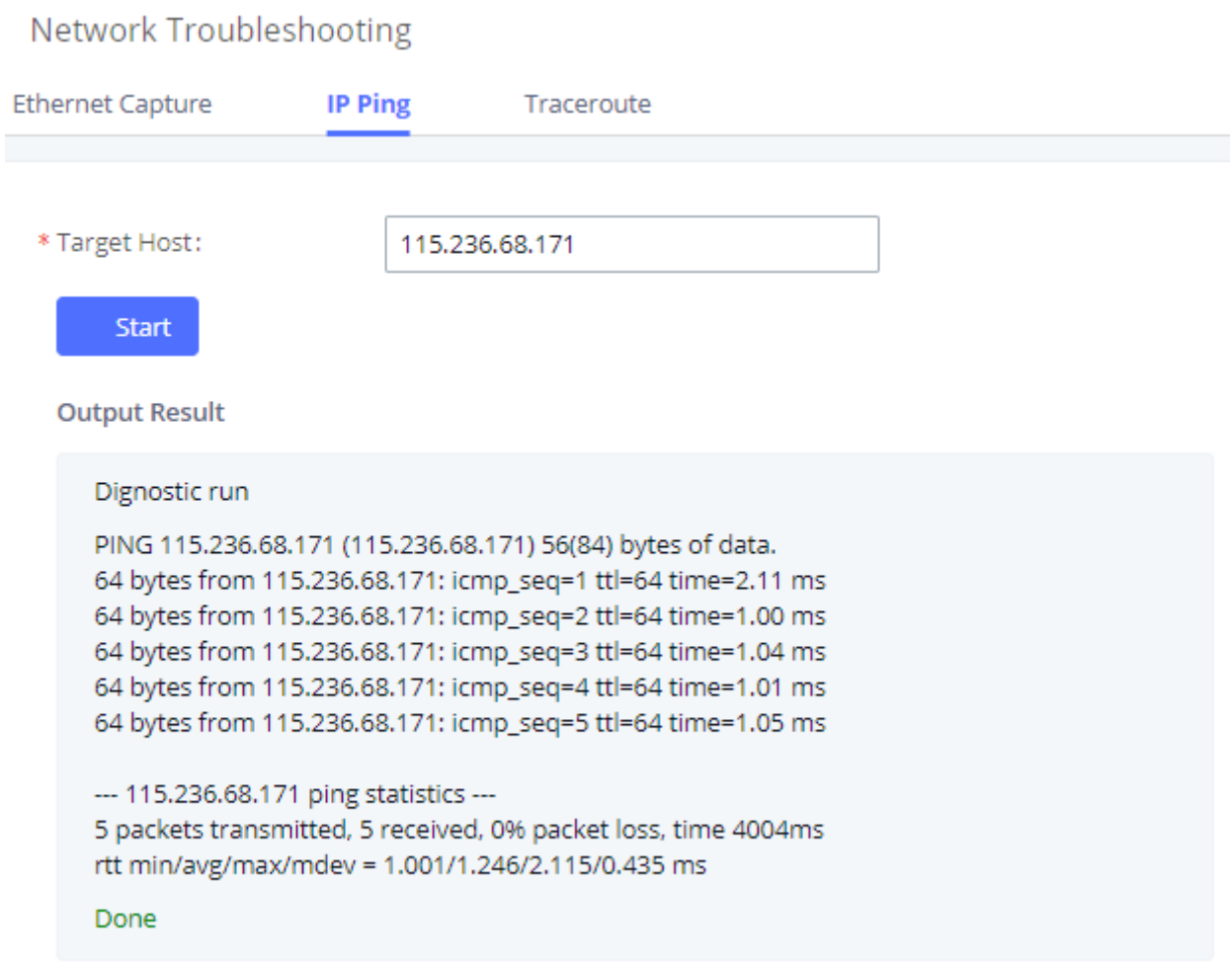
Storage Location	Local: Store the captured packets in the local storage. SFTP Server: Save the capture trace to a SFTP server. Please make sure that SFTP is correctly configured under PBX Settings -> Online Storage -> SFTP Server External Storage: Save the capture trace in a usb flash drive or an SD card. This requires that a USB flash drive or SD card to be plugged into the PBX. File formats supported are FAT32 and ExFat.
Save to External Storage	When or more external storage units are connected to the PBX, the user will be able to pick which one to use.? Note: This option is available only when you choose "External Storage" as the storage destination of the capture trace.
Destination Directory	When SFTP is selected, this option will appear. Please enter the directory path in which you would like to store the captured packets.
Packet Capture Size	This option appears only when "External Storage" or "SFTP" options are selected. Define the packet capture size, the option available are: 50MB, 100MB, and 200MB.
Number of Packet Capture	Define the maximum number of the packets captured. The available options are 5, 10, and 20 packets.
TLS Key	SSL/TLS packets can be decrypted through Wireshark. The packet capture must contain the TLS handshake process.
Start	Start capturing network traffic.
Stop	Stop capturing network traffic.
Download	Download the captured packets. This option can only be used when the captured packets are stored locally.
Enable SRTP Debugging	Check this box to troubleshoot calls encrypted with TLS/SRTP.

The output result is in .pcap format. Therefore, users could specify the capture filter as used in general network traffic capture tool (host, src, dst, net, protocol, port, port range) before starting to capture the trace.

Capture files saved on external devices will now have "capture" prepended to file names.

IP Ping

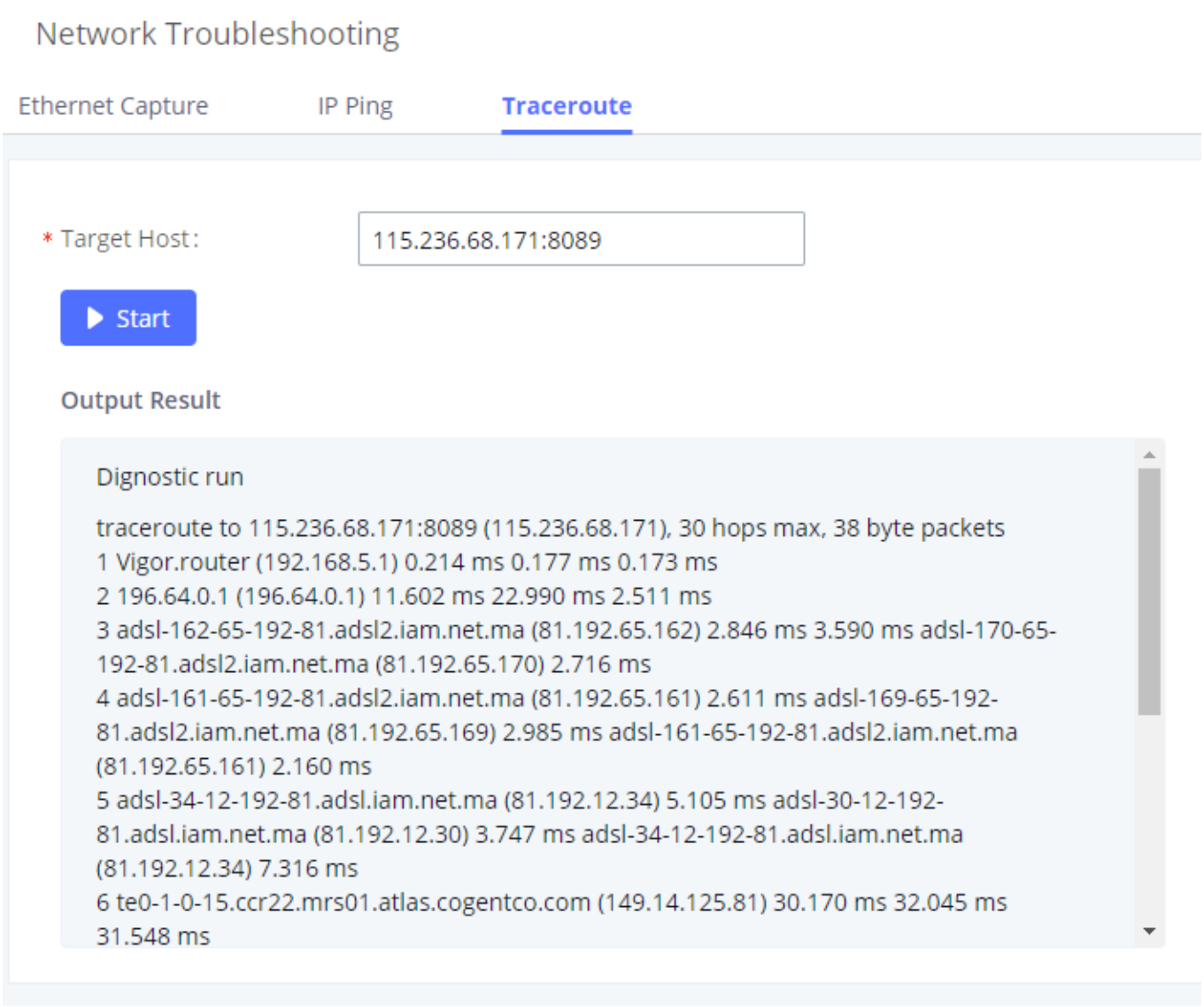
Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



Ping

Traceroute

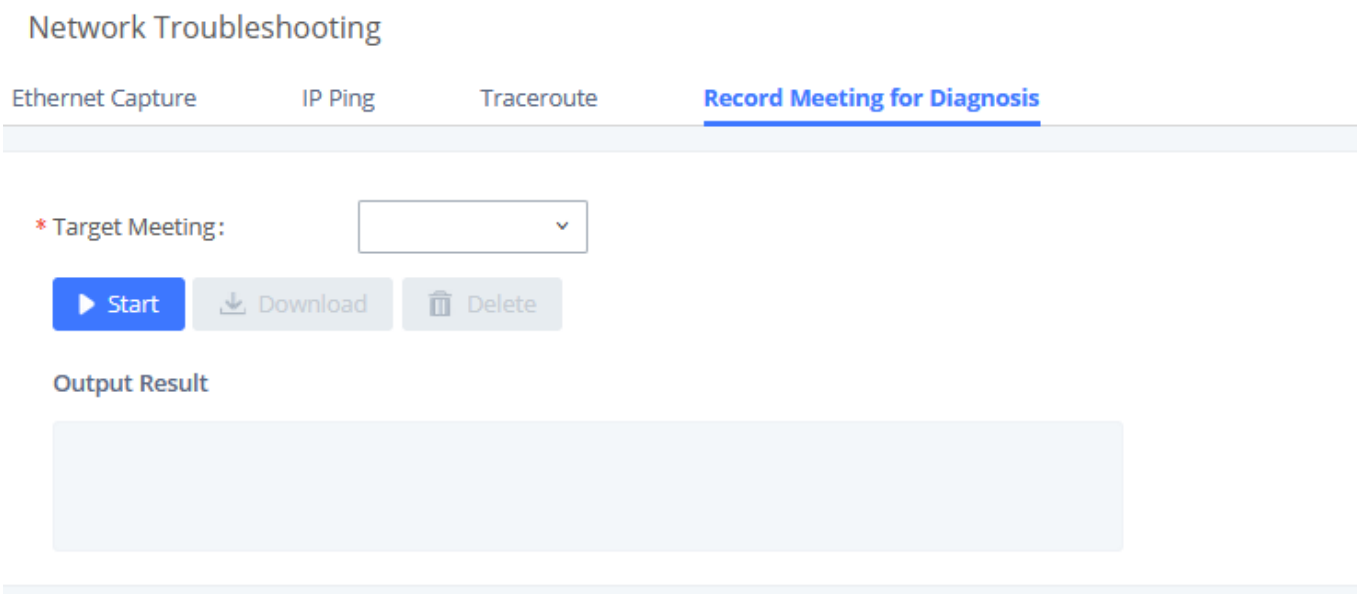
Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



Traceroute

Record Meeting for Diagnosis

Enter the target meeting, support the ongoing meeting, and then click the "Start" button to capture the recording diagnosis of the meeting members in progress. The output result will be automatically displayed below, click the "download" button to download to the local. After the download is complete, immediately click the "Delete" button to clear the system content.



Record Meeting for Diagnosis

Signaling Troubleshooting

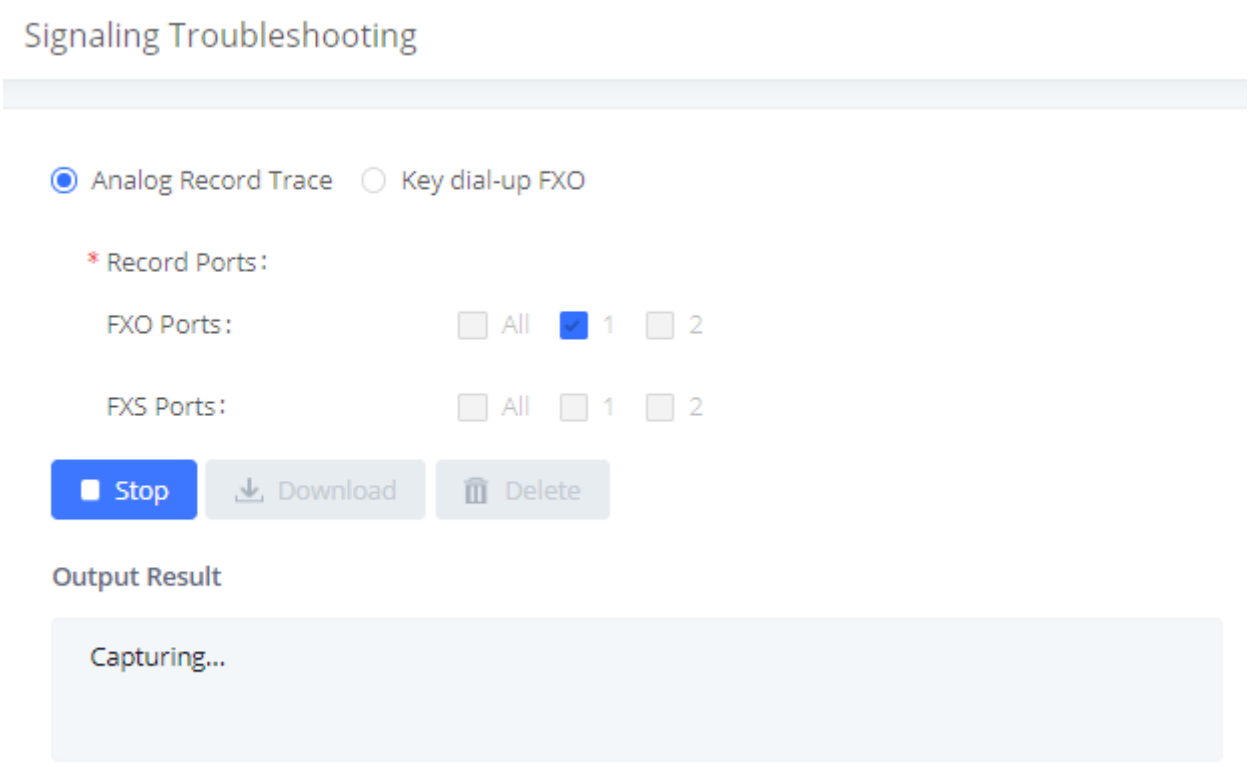
Analog Record Trace

- **Analog Record Trace**

Analog record trace can be used to troubleshoot analog trunk issue, for example, the UCM630X user has caller ID issue for incoming call from Analog trunk. Users can access analog record trance under Web GUI→ **Maintenance→Signal Troubleshooting**.

Here is the step to capture trace:

1. Select FXO or FXS for "Record Ports". If the issue happens on FXO 1, select FXO port 1 to record the trace.
2. Click on "Start".
3. Make a call via the analog port that has the issue.
4. Once done, click on "Stop".
5. Click on "Download" to download the analog record trace.



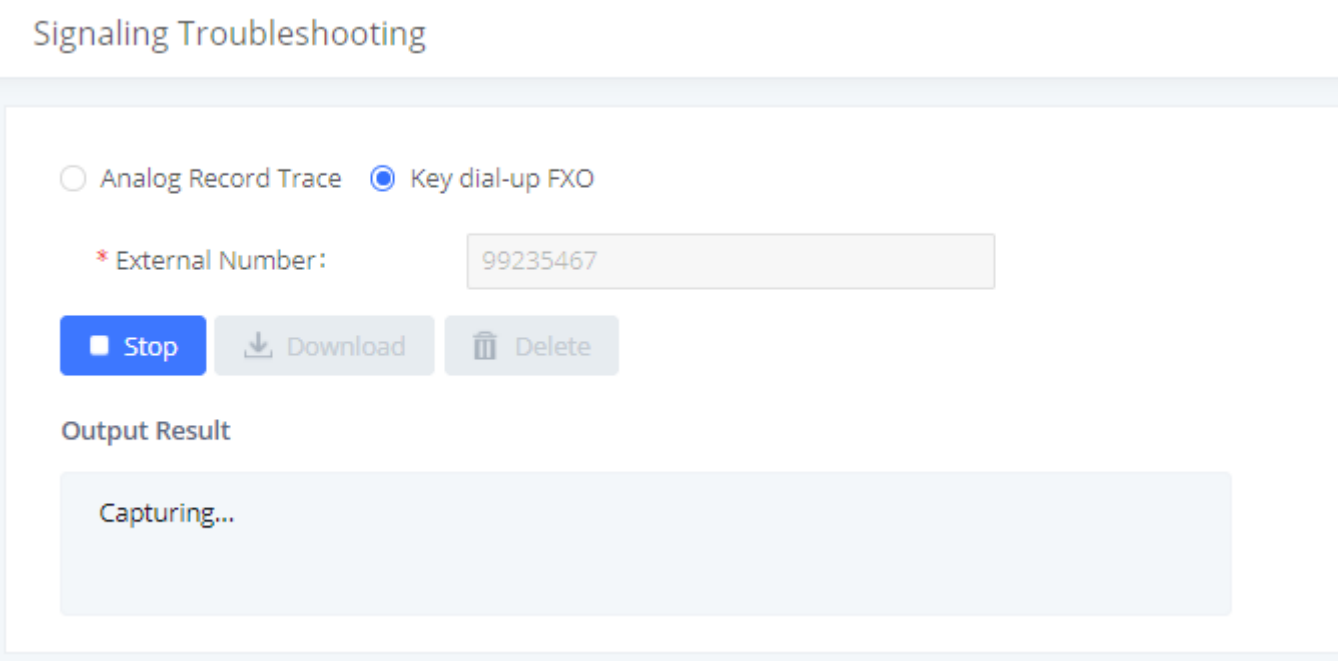
Troubleshooting Analog Trunks

- **A key Dial-up FXO**

Users can directly set a PSTN number on the "**External Extension**" text box to troubleshoot issues related to the analog trunk easily, the following steps shows how to use this feature:

1. Configure analog trunk on UCM, including outbound route.
2. Enter a reachable external number in "**External Extension**".
3. Press "**Start**" button. The call will be initiated to the external number.
4. Answer and finish the call before pressing "Stop" button.

The trace will be available for analysis to download after output result shows "Done! Click on Download to download the captured packets".



A Key Dial-up FXO

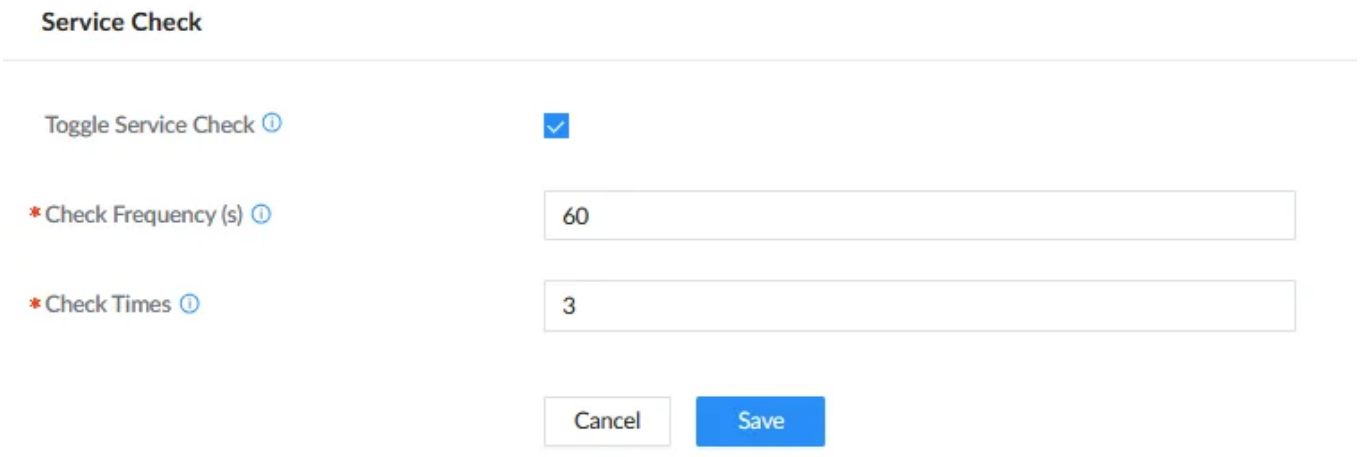
When using a Key Dial-up FXO feature the outbound trunk for the analog trunk need to have internal permission. As well as it should be the trunk with the highest outbound route priority.

After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved.

https://helpdesk.grandstream.com/

Service Check

The Service Check feature enables periodic health checks on the UCM's internal core services. If services become unresponsive after a specified number of failed check attempts, the current system status is saved and internal services automatically restart to maintain system stability.



The table below describes the options available on this page.

Option	Description
Toggle Service Check	Enables or disables periodic service health checks on the UCM.
Check Frequency (s)	Configures the interval between health checks in seconds. The default setting is 60 seconds.

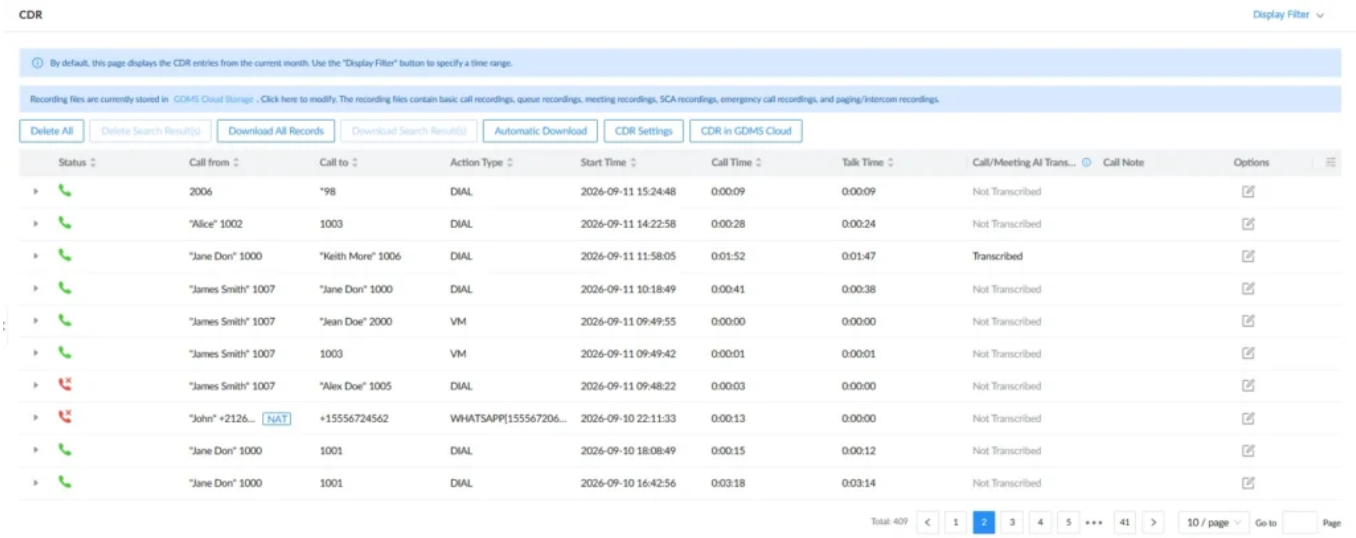
Check Times	Configures the maximum number of consecutive failed checks allowed before restarting internal services. If there is no response from the system after the configured attempts, current status logs are stored and internal services are restarted. The default setting is 3.

CDR

CDR

CDR (Call Detail Record) is a data record generated by the PBX that contains attributes specific to a phone call handled by the PBX. It provides detailed description fields such as the caller number, receiver number, start time, call duration, talk time, and call status.

On the UCM630X, CDRs can be accessed under **CDR -> CDR**. Users can filter the call report by specifying date ranges, call statuses, action types, or specific extension numbers by clicking the **Display Filter** button at the top right of the page.

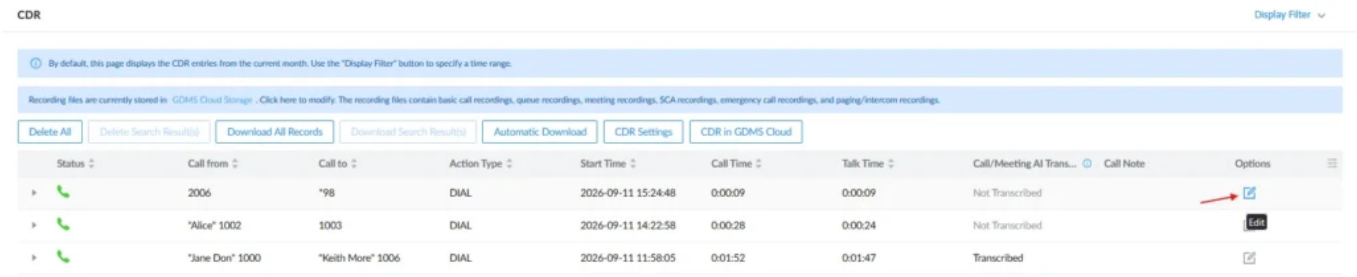


The table below describes the data fields, options, and management features available on the main CDR page:

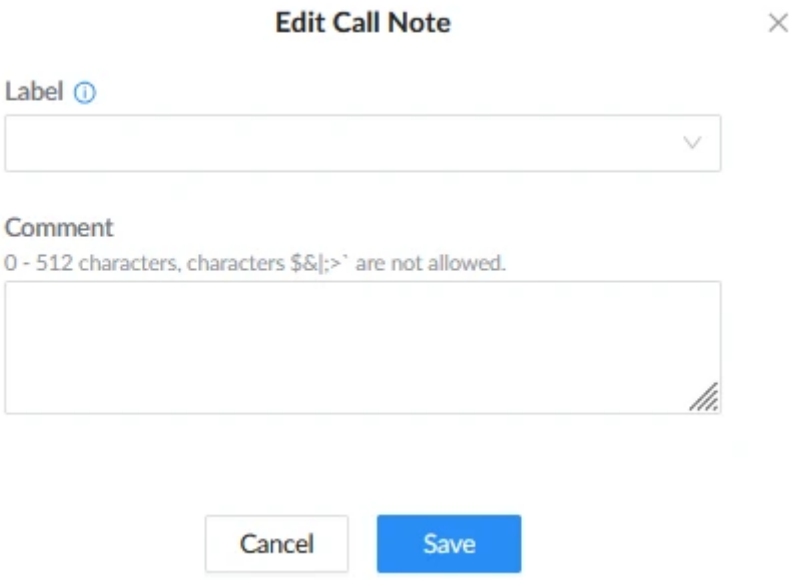
Option / Field	Description
Status	Indicates the final status of the call (Answered, Busy, No Answer, or Failed).
Call From	Displays the caller's name and extension number or external CID (e.g., "Jane Doe" 1005).
Call To	Displays the recipient's name and extension number or external dialed number (e.g., "Robert More" 1006).
Action Type	Displays the mechanism/destination type used for the call (e.g., DIAL, IVR, WAKEUP, MULTIMEDIAMEETING).
Start Time	Timestamp when the call was initiated (Format: YYYY-MM-DD HH:MM:SS). Clicking the column header sorts the list by start time.
Call Time	Total duration of the call from initiation to hang-up (Format: HH:MM:SS).
Talk Time	Connected duration between parties (Format: HH:MM:SS).
Call/Meeting AI Transcription	Displays the status of AI recording transcription (e.g., Transcribed or Not Transcribed).

Call Note	Displays assigned labels or custom comments attached to the call record. Click the Edit Call Note (pencil) icon under the Options column to modify the label or add comments.
Recordings Management	If the call has an associated audio recording, a tape/cassette icon appears in the Options column. Clicking this icon opens the Recordings pop-up dialog to play, download, transcribe, or delete the recording.
Download Search Result(s)	Exports currently filtered CDR records into a .csv file.
Download All Records	Exports all stored system CDR records into a .csv file.
Delete All	Removes all CDR call history entries from the system.
Delete Search Result(s)	Removes only the CDR entries matching the current filter criteria. A secondary prompt asks whether to simultaneously delete associated call recording files.
Automatic Download	Configures scheduled exports of CDR CSV files to email destinations or synced cloud platforms (such as Google Docs).
CDR Settings	Opens global CDR management parameters.

Administrators and authorized users can categorize call records by attaching pre-configured labels or adding custom comments by clicking the Edit icon under **Options** to open the **Edit Call Note** window.



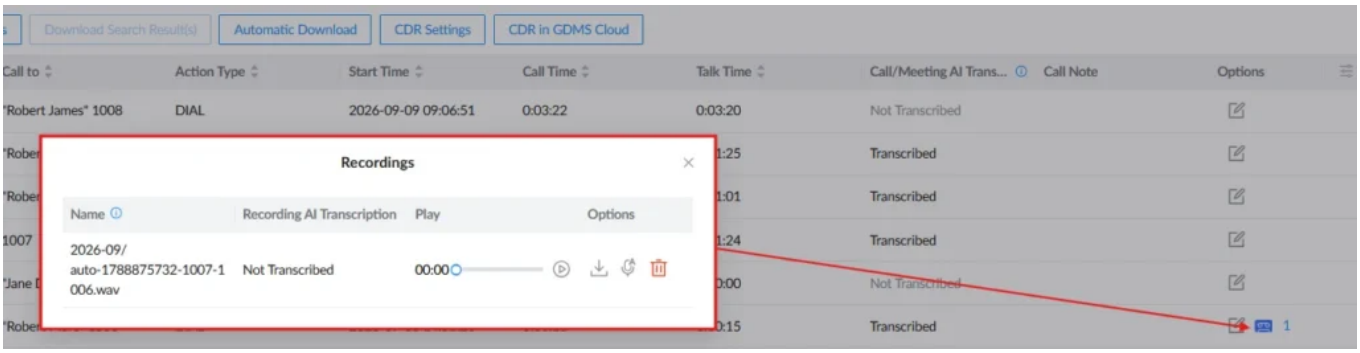
The dialog allows selecting a pre-configured tag from the drop-down menu (configured under **CDR -> Call Note**) or entering a custom note regarding the call (up to 512 characters; special characters $ & | : > ` are restricted).



Clicking the recording icon on a CDR entry opens the **Recordings** pop-up modal, allowing users to preview, manage, or transcribe call recording files. The pop-up dialog provides interactive operations including:

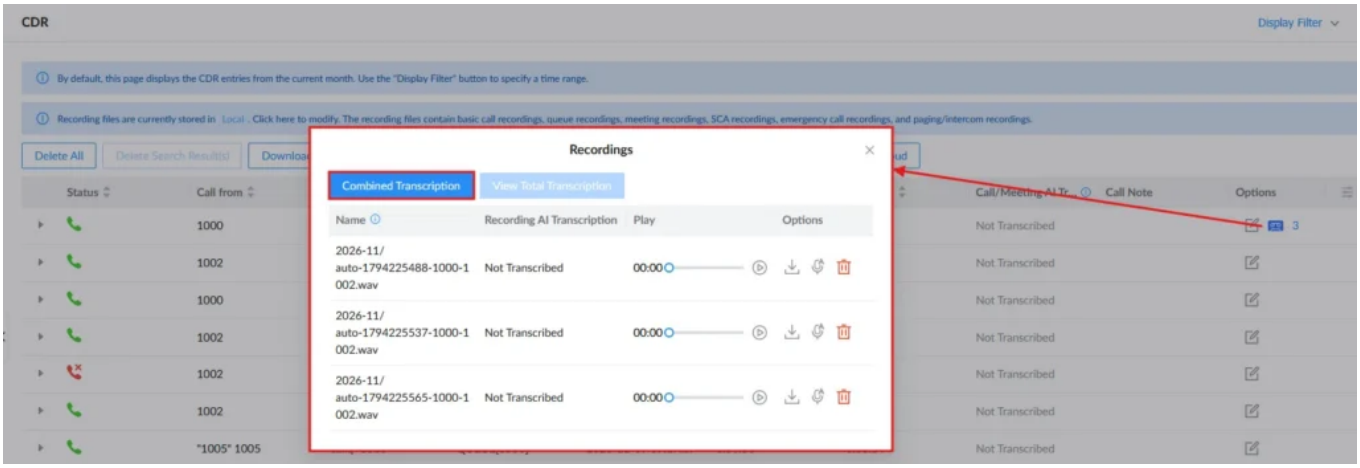
- **Playback** (using the built-in audio player controls to play, pause, or seek)
- **Download** (saving the recording file in .wav format to the local computer)

- **AI Recording Transcription** (initiating AI speech-to-text transcription after selecting the desired language)
- **Delete** (deleting the recording file without removing the CDR call entry).



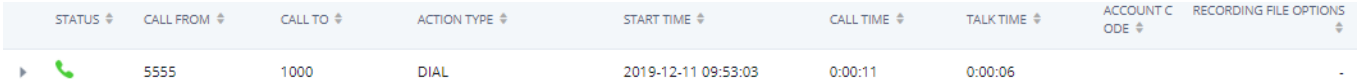
When Merge Same Call Recordings is disabled under **PBX Settings -> General Settings -> Recording Settings**, and recording is started and stopped several times during the same call, the UCM generates a separate recording file each time.

In this case, the Recordings pop-up of a CDR entry lets users transcribe and summarize all recording files of the call together, in addition to transcribing each file individually.

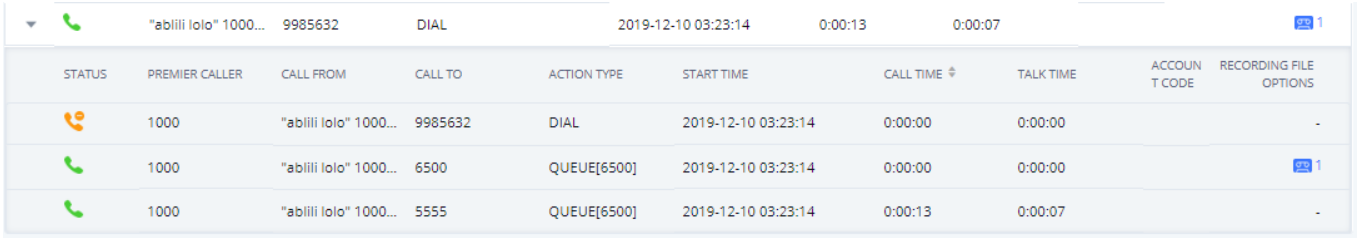


Transferred calls are represented in the CDR log as consolidated entries. Accessing CDR entries under Web GUI -> **CDR -> CDR** allows administrators to review full details for individual call sessions.

Click the **Option** icon next to a specific call record entry to view detailed call flow information, including primary caller IDs, call transfer steps, and timing details.



CDR Report Page

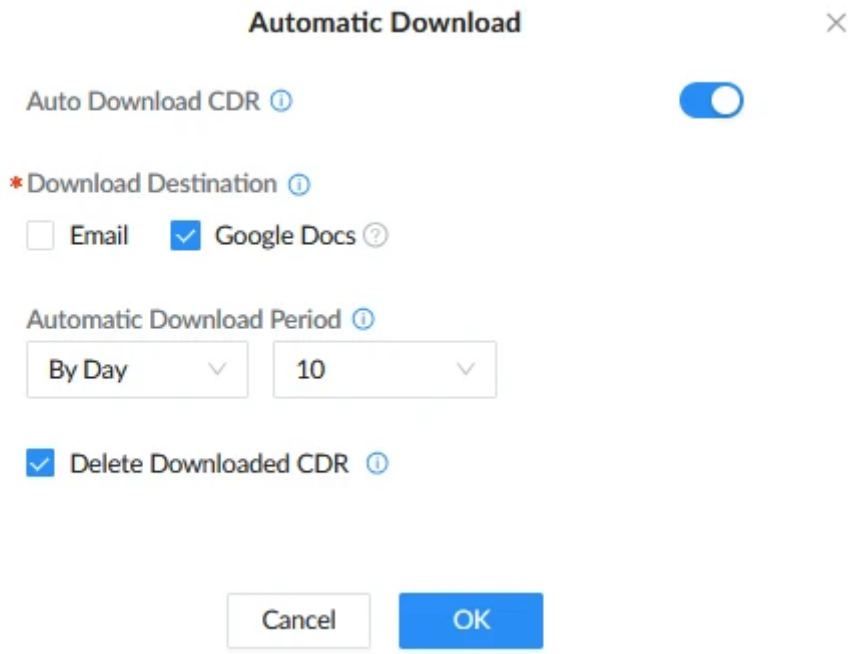


Detailed CDR Log View

CDR Automatic Download

The UCM630x series can be configured to automatically export and transmit CDR records at scheduled intervals. Administrators can deliver CDR files via email or automatically sync them to Google Sheets by

navigating to **CDR -> CDR** and clicking on **Automatic Download Settings**.



The table below describes the parameters available in the Automatic Download configuration dialog:

Parameter	Description
Auto Download CDR	Enables or disables the scheduled automatic downloading and exporting of CDR logs.
Download Destination	Select the delivery method for auto-downloaded CDR records: Email: Transmits exported CDR files as email attachments to designated recipient email addresses. Google Docs: Automatically uploads exported CDR CSV files to Google Drive/Sheets. Note: The Email destination requires configured Email Settings (under System Settings -> Email Settings), while the Google Docs destination requires an active Google Workspace Integration (under Integrations -> Collaborative Office Integration).
Email Address	Displayed when Email is selected as a destination. Enter the email addresses that will receive the CDR records. Multiple email addresses should be separated by commas.
Automatic Download Period	Defines the recurrence schedule and exact hour of the day for automatic CDR exports: By Day: When the configured download hour arrives, the system exports CDR records of the entire previous day. By Week: Select a specific day of the week and hour. When triggered, the system exports records covering the previous 7 days. By Month: Select a specific day of the month and hour. When triggered, the system exports records spanning from the previous month.
Delete Downloaded CDR	When enabled, CDR records that have been successfully generated and sent to the configured destination (Email or Google Docs) will be automatically deleted from local UCM storage to conserve disk space.

Downloaded CDR File

- **Caller number, Callee number**

"Caller number": the caller ID.

"Callee number": the callee ID.

If the "Source Channel" contains "DAHDI", this means the call is from FXO/PSTN line.

caller number	callee number	context	calerid	source channel	dest channel	lastapp
	2009	from-internal	"Wake Up Call" <WakeUp>	Local/2009@from-internal-00000001;2	PJSIP/2009-00000013	Dial
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	Dial
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial
1100	2014	from-did-direct	"1100" <1100>	DAHDI/1-1	PJSIP/2014-00000017	Dial

Downloaded CDR File Sample

- **Context**

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.

ext-did-XXXXX: inbound calls. It starts with "ext-did", and "XXXXX" content varies case by case, which also relate to the order when the trunk is created.

ext-local: internal calls between local extensions.

- **Source Channel, Dest Channel**

Sample 1:

caller number	callee number	context	calerid	source channel	dest channel	disposition
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	ANSWERED

Downloaded CDR File Sample - Source Channel and Dest Channel 1

DAHDI means it is an analog call, FXO or FXS.

For UCM6302, DAHDI/(1-2) are FXO ports, and DAHDI(3-4) are FXS ports.

For UCM6304, DAHDI/(1-4) are FXO ports, and DAHDI(5-6) are FXS ports.

For UCM6308, DAHDI/(1-8) are FXO ports, and DAHDI(9-10) are FXS ports.

Sample 2:

caller number	callee number	context	calerid	source channel	dest channel	lastapp
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial

Downloaded CDR File Sample - Source Channel and Dest Channel 2

"SIP" means it is a SIP call. There are three format:

(a) **PJSIP/NUM-XXXXXX,** where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.

(c) **PJSIP/trunk_X/NUM,** where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.

(c) **PJSIP/trunk_X-XXXXXX,** where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

There are some other values, but these values are the application name which are used by the dialplan.

IAX2/NUM-XXXXXXX: it means this is an IAX call.

Local/@from-internal-XXXXX: it is used internally to do some special feature procedure. We can simply ignore it.

Hangup: the call is hung up from the dialplan. This indicates there are some errors or it has run into abnormal cases.

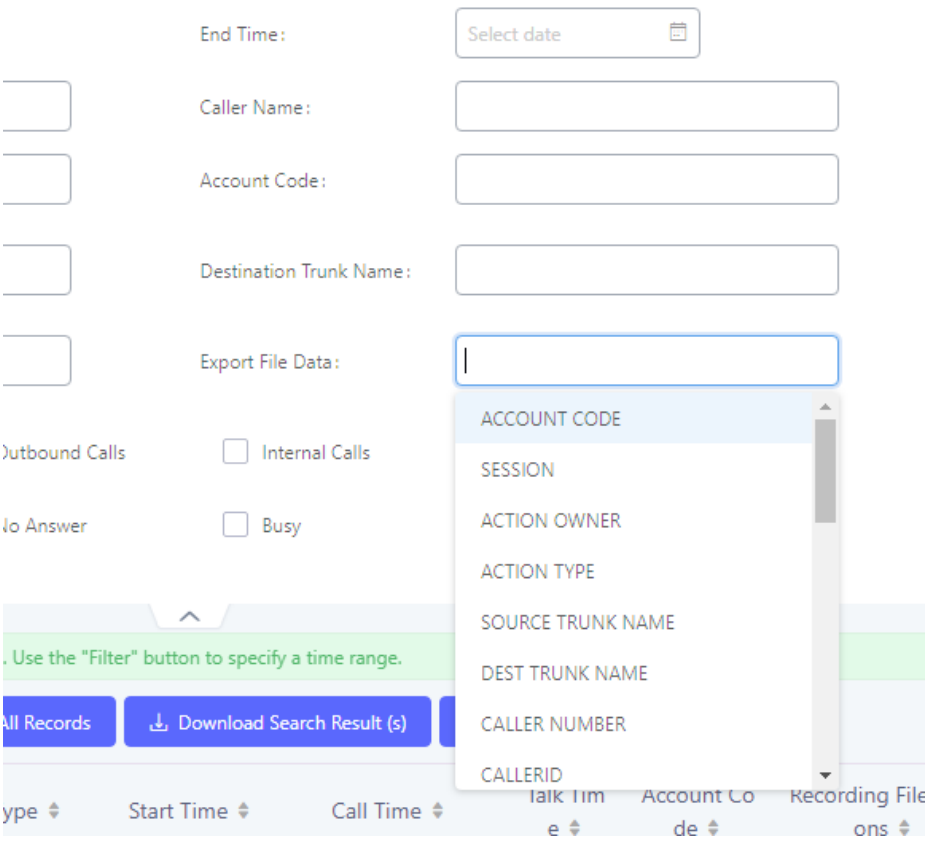
Playback: play some prompts to you, such as 183 response or run into an IVR.

ReadExten: collect numbers from user. It may occur when you input PIN codes or run into DISA

Note: The language of column titles in exported CDR reports and statistics reports will be based on the UCM's display language

CDR Export Customization

Users can select the data they want to see in exported CDR reports by first clicking on the Filter button on the CDR page under **CDR→CDR** and selecting the desired information in the Export File Data field.

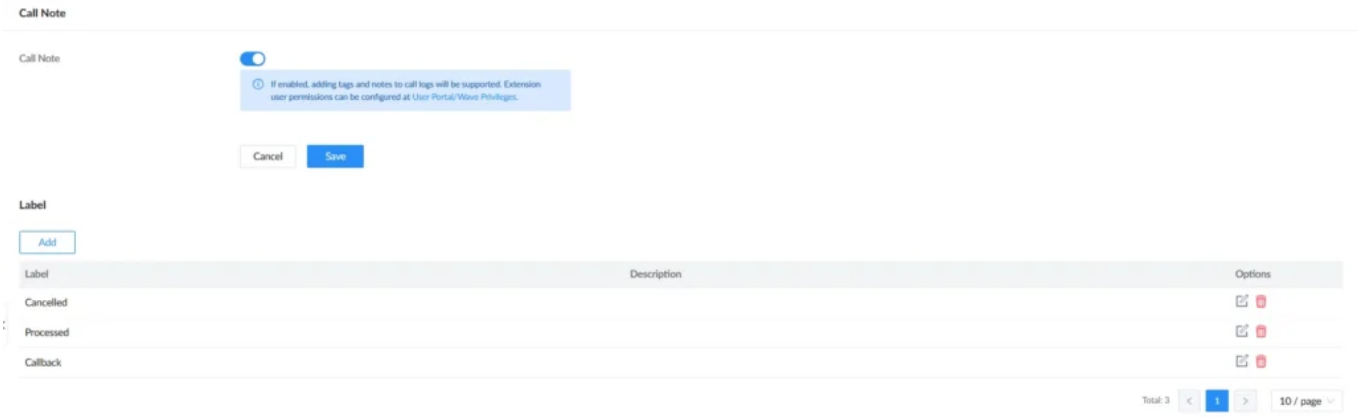


CDR Export File data

Call Note

Under **CDR -> Call Note**, administrators can enable the Call Note feature and define customized call labels (tags) that users can attach to call detail records and call logs across the User Portal and Wave application.

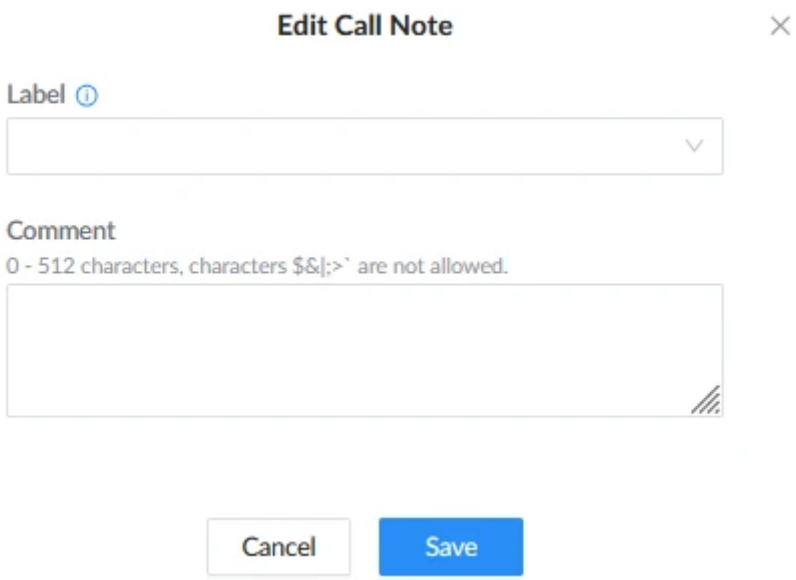
Extension user access permissions for modifying call notes can be configured under Maintenance -> User Management -> User Portal/Wave Privileges.



The table below describes the parameters available on the Call Note configuration page:

Option	Description
Call Note	Toggles the Call Note feature on or off. When enabled, users can add tags, labels, and text comments to call logs and CDR entries.
Label Table	Displays all created call labels along with their descriptions and management options (edit or delete).

To create a new call label tag, click the **Add** button to open the **Add Call Label** window.



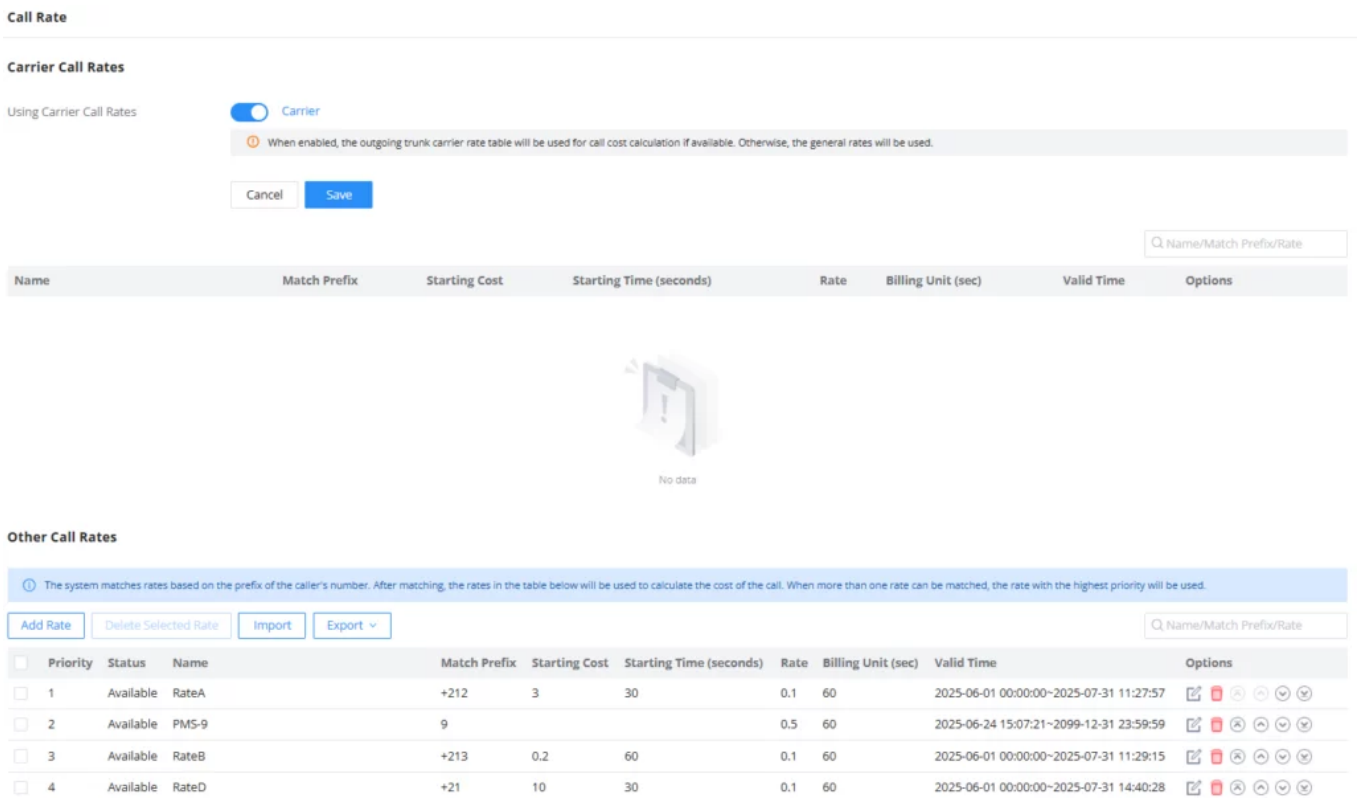
Configure the following fields in the **Add Call Label** dialog:

- **Label:** Enter a unique name for the call tag (1-128 characters; supports numbers, letters, special characters _ -, and Chinese characters).
- **Description:** Enter an optional summary or explanation for the label (0-128 characters; special characters $ & | : > ` are restricted).

Call Rate

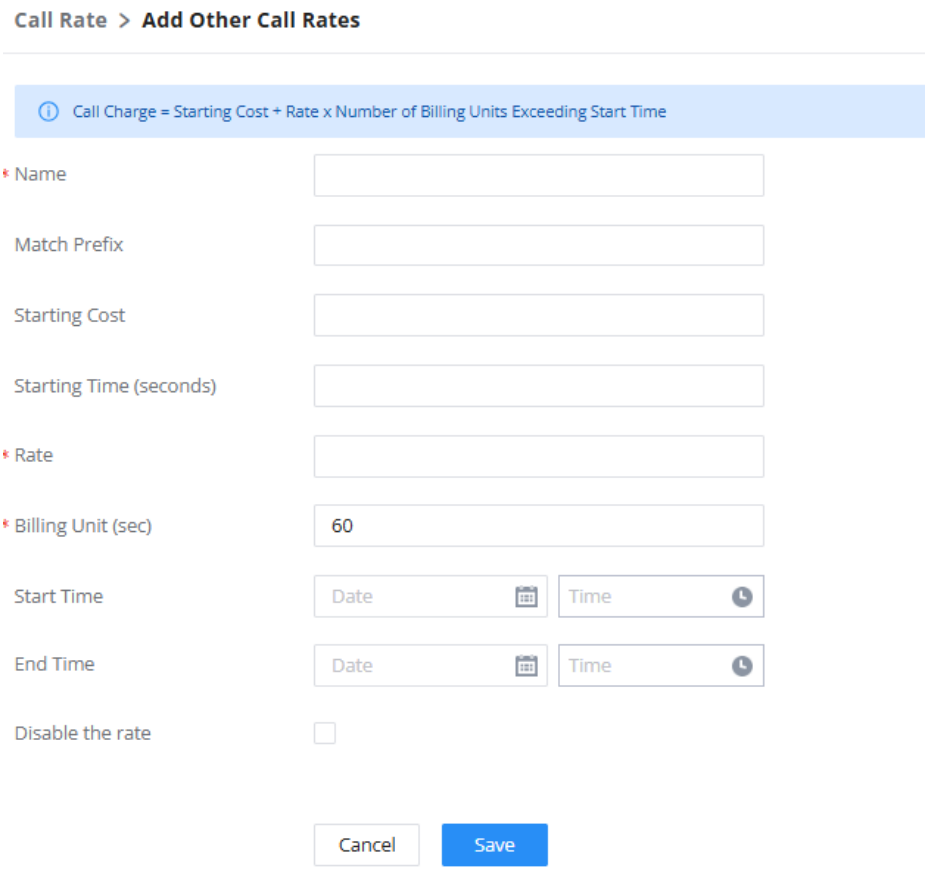
In Call Rate, the user can set call billing for outbound calls. The user can choose to include the call rate onfigured in **Carrier** or configure rates for calls which are identified through a prefix.

If Using Carrier Call Rates has not been enabled, the UCM will fall back to the **Other Call Rates** table.



Call Rate

To add specific rates, click on "Add Rate".



Parameter	Description
Name	Enter the name of the call rate.

Match Prefix	Enter the matching prefix of the outgoing number dialed to match the corresponding rate. The prefix entered must match the outgoing mode of the outgoing route. Leave this field blank if you want to calculate every call using this rate. The matching will be done before any digit stripping or prepending is done.
Starting Cost	Configure the starting flat fee to charge for calls. If the length of the external call does not exceed the start time, only this fee will be charged.
Starting Time (seconds)	Sets the starting time period for call billing. If the length of an external call does not exceed the starting time, only the starting cost amount will be charged.Example 1: If the starting cost is set to 0.2, and the starting time is set to 60, the first 60 seconds of a call will be charged a flat amount of 0.20 dollars (or other currency). If the starting cost is set to 0 instead, the first 60 seconds will be free.Example 2: If the starting cost is set to 0.2 and the starting time is set to 0, the call billing will start upon dialing with an initial cost of 0.2 currency unit.Example 3: If the starting cost is set to 0 and the billing time is set to 0, the billing will start upon dialing with no initial cost.
Rate	Sets the billing rate of a call after the starting time period has ended. This is used with Billing Unit (sec) to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time).
Billing Unit (sec)	Sets the billing unit used after the starting time period has ended. This is used with Rate to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time). Partial units are rounded up (e.g., If the billing unit is set to 60 seconds, and the call lasted 90 seconds (1.5 units), the guest will be billed for 120 seconds (2 units)).
Start Time	Define the starting time. After this time, this rate will be applied.
End Time	Define the end time. After this time, this rate will not be applied.
Disable the rate	Ticking this box will disable this rate. Unticking this box means that this rate will apply.

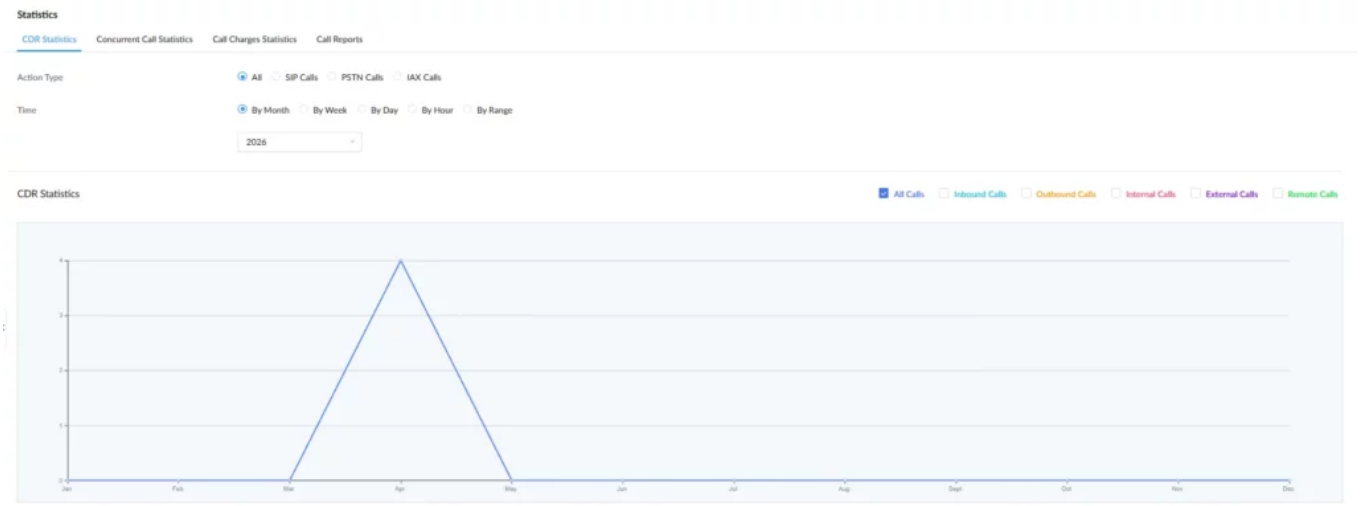
For more information on the UCM6300 built-in billing feature, please refer to the Grandstream Billing System Guide.

Statistics

The UCM provides a comprehensive CDR analytics framework for monitoring, analyzing, and reporting voice traffic across the system. This module is designed to give administrators operational visibility into call patterns, resource utilization, user behavior, and cost distribution.

CDR Statistics

UCM supports the function of concurrent call statistics. This function provides users with statistics on the number of concurrent calls of all VoIP trunks (SIP trunks and IAX trunks). Users can set search criteria to generate custom charts. Select the trunk and time to view the chart of the maximum number of concurrent calls corresponding to the trunk in a certain day or month.

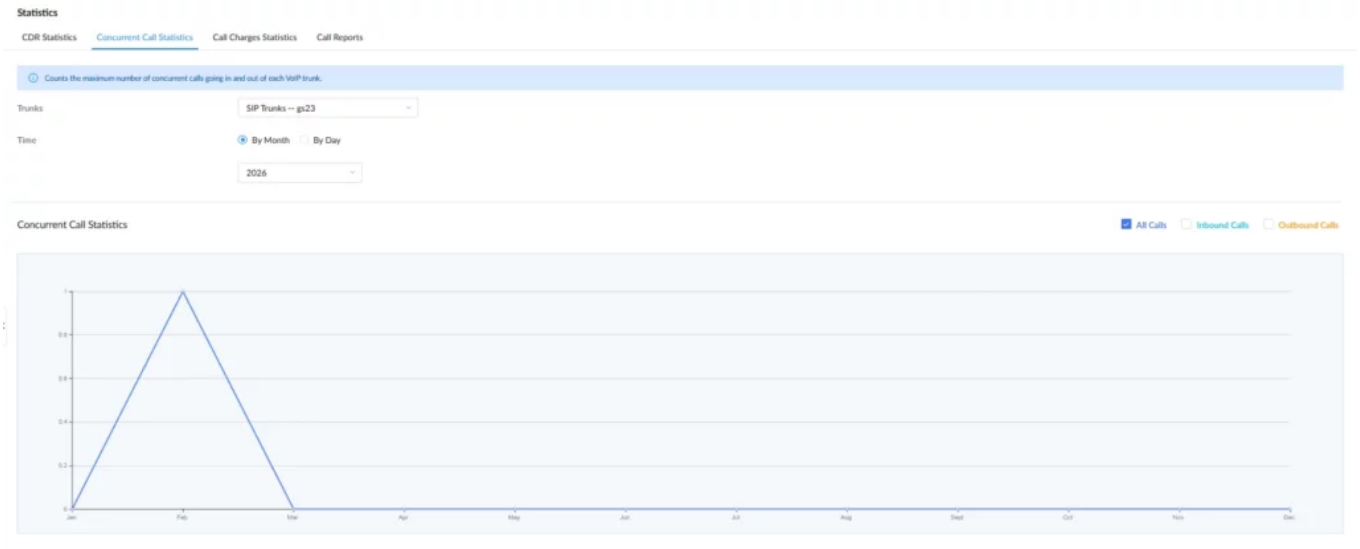


CDR Statistics Tab

Action Type	Select one of the following trunk type All SIP Calls PSTN Calls
Time Range	Select the time period to use for filtering By month (of the selected year) By week (of the selected year) By day (of the specified month for the year) By hour (of the specified date) By range. Example: 2016-01 to 2016-03
Call Type	Select one or more in the following checkboxes. All Calls Inbound Calls Outbound Calls Internal Calls External Calls Remote Calls

Concurrent Call Statistics

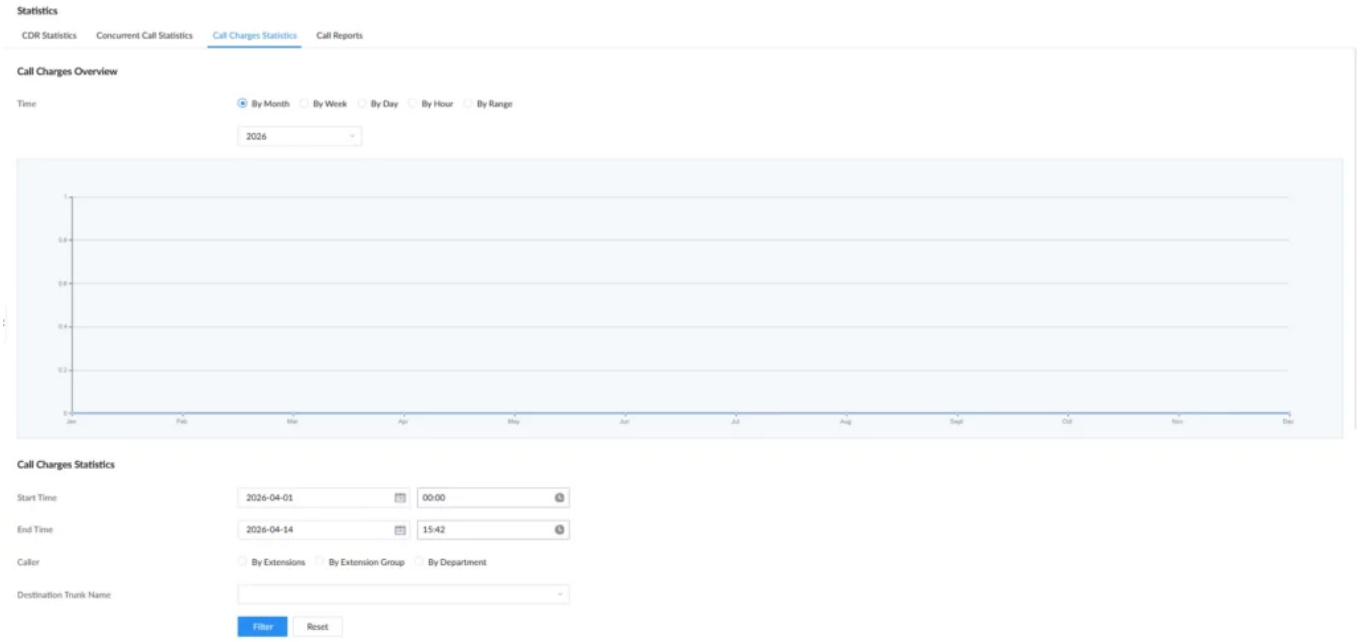
In this tab, the administrator can view the statistics regarding the concurrent calls. The administrator can choose to view the statistics per day, month, and year. The user can also view all calls, inbound calls, or outbound calls; or a combination of all of them together.



Concurrent Call Statistics Tab

Call Charges Statistics

In call Charges Statistics tab, the administrator can view the charges applied to the calls represented in a graph. The administrator can search by time interval, they can also filter per extension, extension group, by department. Once the administrator sets the intended parameters in the filter, they can display and download the filtered statistics.



Call Charges Statistics Tab

Call Reports

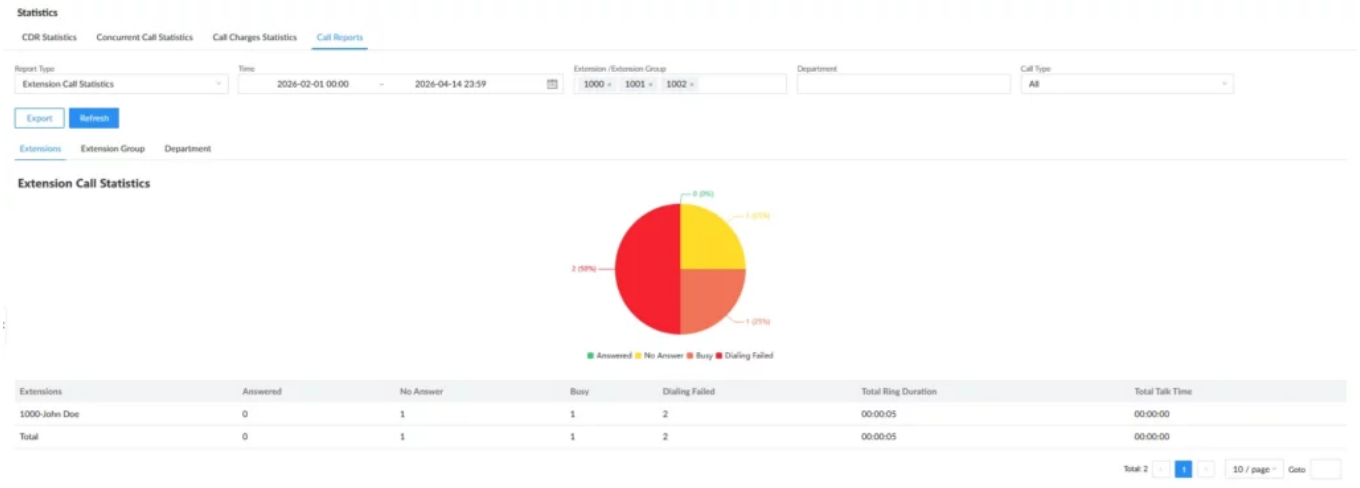
The Call Reports section provides analytics based on different operations within the PBX. These reports allow administrators to analyze how calls are distributed, handled, and processed across extensions, trunks, and system components.

Extension Call Statistics

This report displays insights into call volume associated with selected:

- Extensions
- Extension groups
- Departments

Administrators can filter by time period and call type (inbound, outbound, internal, etc.) to analyze how traffic is distributed across users or organizational units.

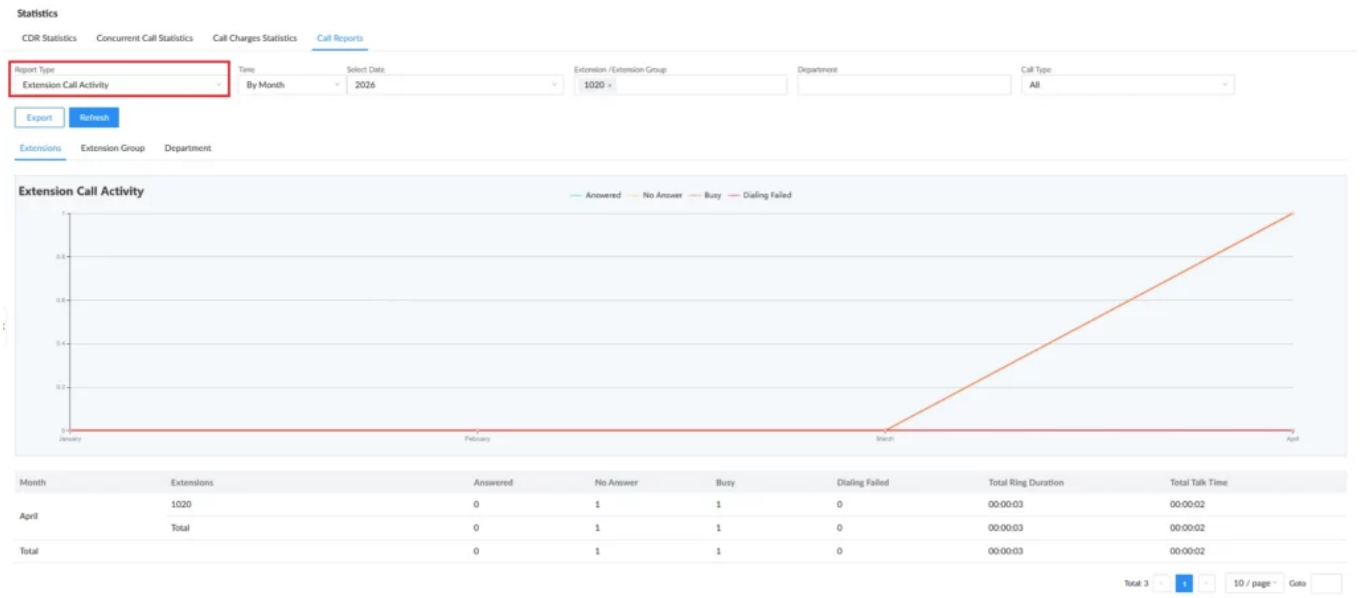


Extension Call Statistics

Extension Call Activity

This report focuses on how calls and selected call types were handled by the specified extensions/extension

groups/departments over the specified time periods.

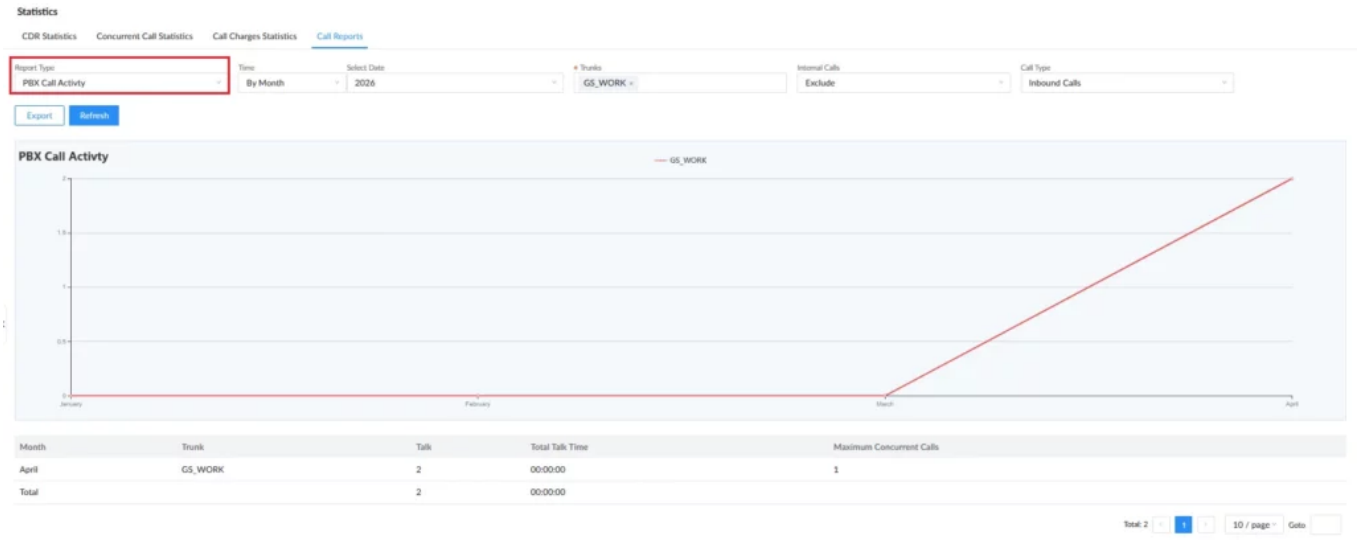


Extension Call Activity

PBX Call Activity

This report provides a system-wide view of call activity across selected trunks, which include or exclude internal calls (extension-to-extension) and can be filtered by call direction.

This enables comparison between internal PBX traffic and external trunk usage, helping identify overall system load distribution and trunk utilization patterns.



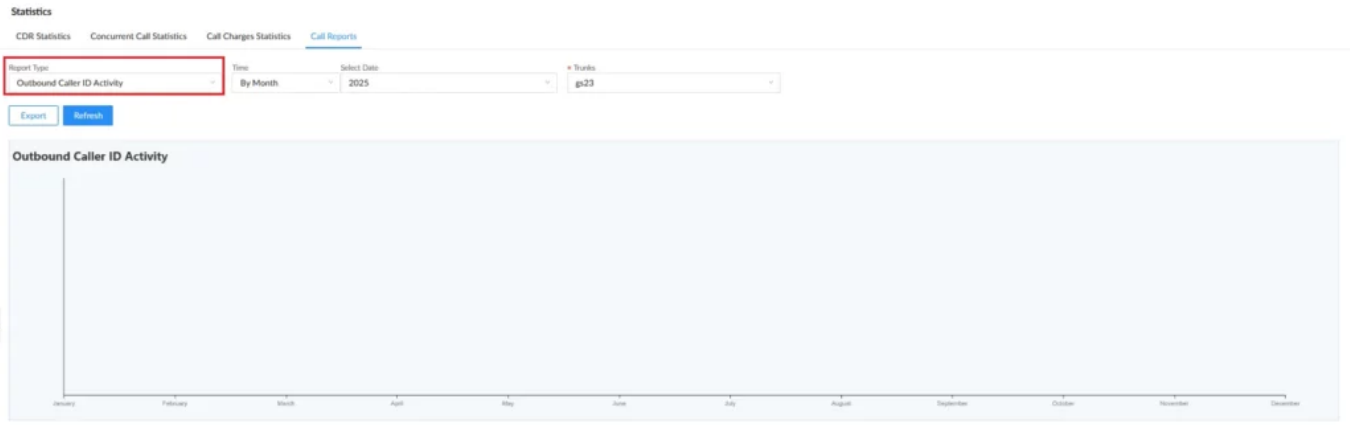
PBX Call Activity

Outbound Caller ID Activity

This report provides visibility into outbound call usage based on the selected trunk and caller ID configuration.

It displays how outbound calls are distributed across:

- Trunks
- Caller IDs

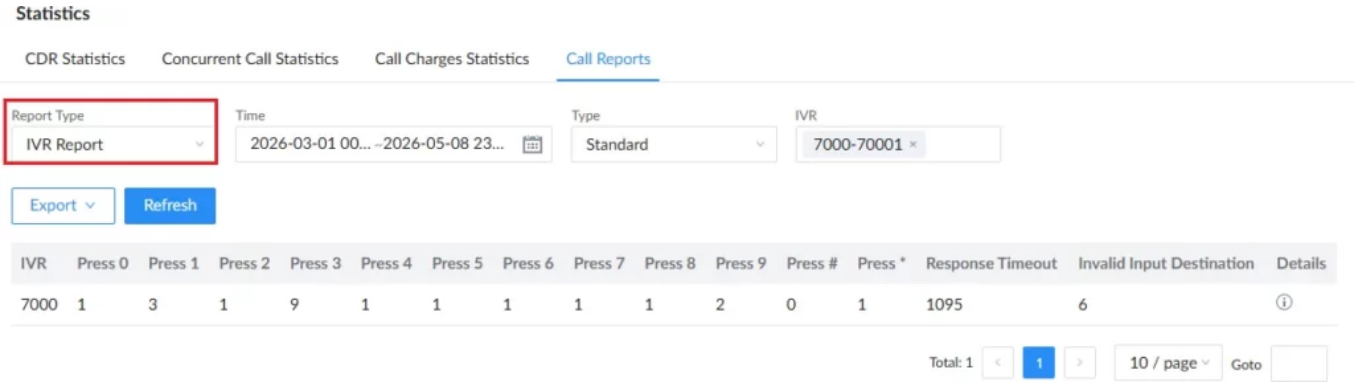


Outbound Caller ID Activity

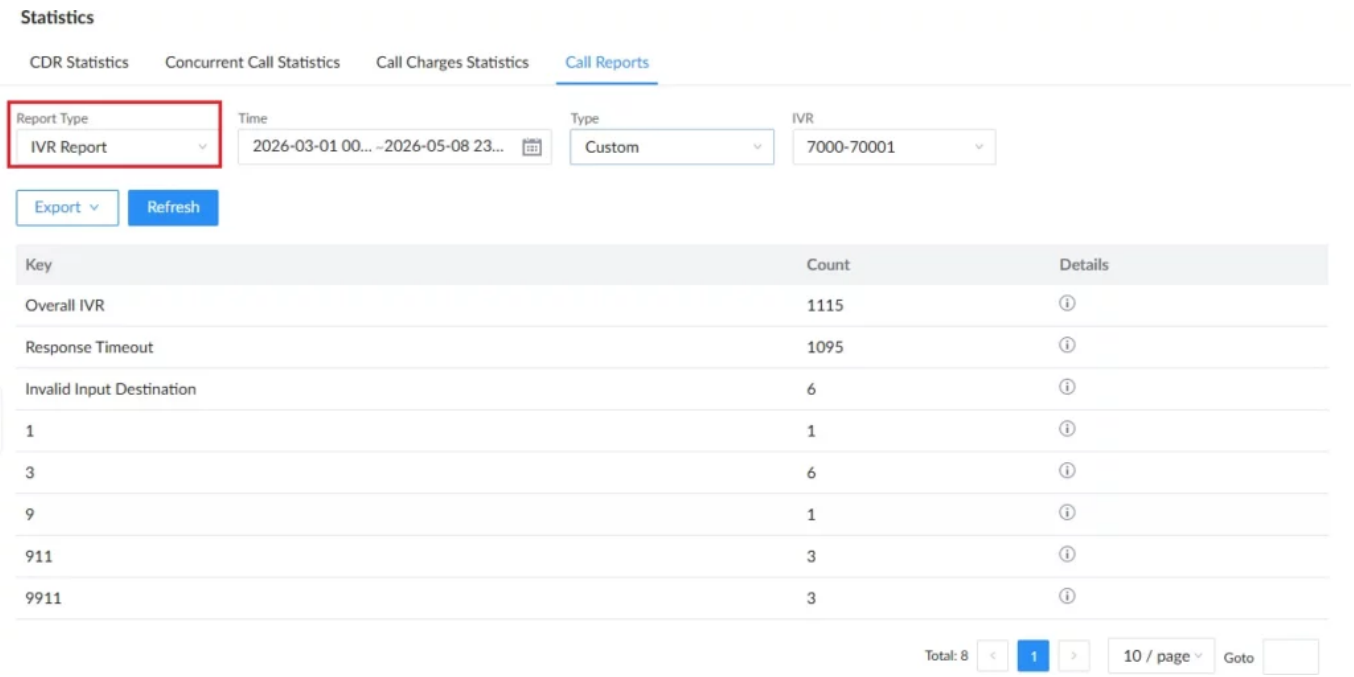
IVR Report

This option provides analysis of IVR interactions over a selected time period and supports two reporting modes:

- **Standard Mode:** Captures key press events (0-9, *, #), including invalid inputs and timeout events, providing detailed per-key interaction statistics.
- **Custom Mode:** Supports multi-digit or combined key inputs. Reports aggregate IVR activity, including total call entries, invalid inputs, and timeouts.



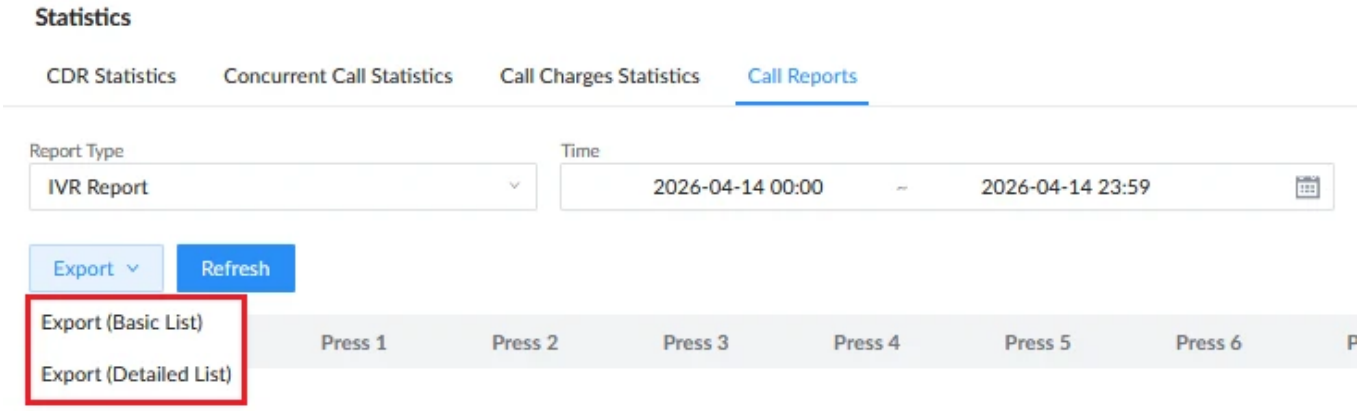
Standard IVR Report



Custom IVR Report

The report can be exported in two formats:

- **Basic List:** Lists all IVRs and the trigger counts of their key press events.
- **Detailed List:** Includes the caller information, triggered key press events, the time of the events, and how long the callers were in the IVRs. In addition to the information in the Basic report

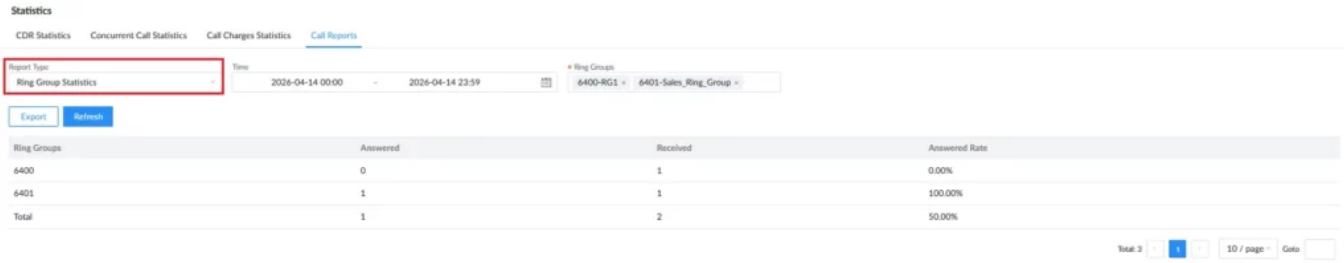


IVR Report Export Types

Ring Group Statistics

This report provides performance metrics for ring groups, including total calls received, answered calls, and answer rate.

It enables evaluation of call distribution efficiency and group responsiveness across configured ring groups.



Ring Group Statistics

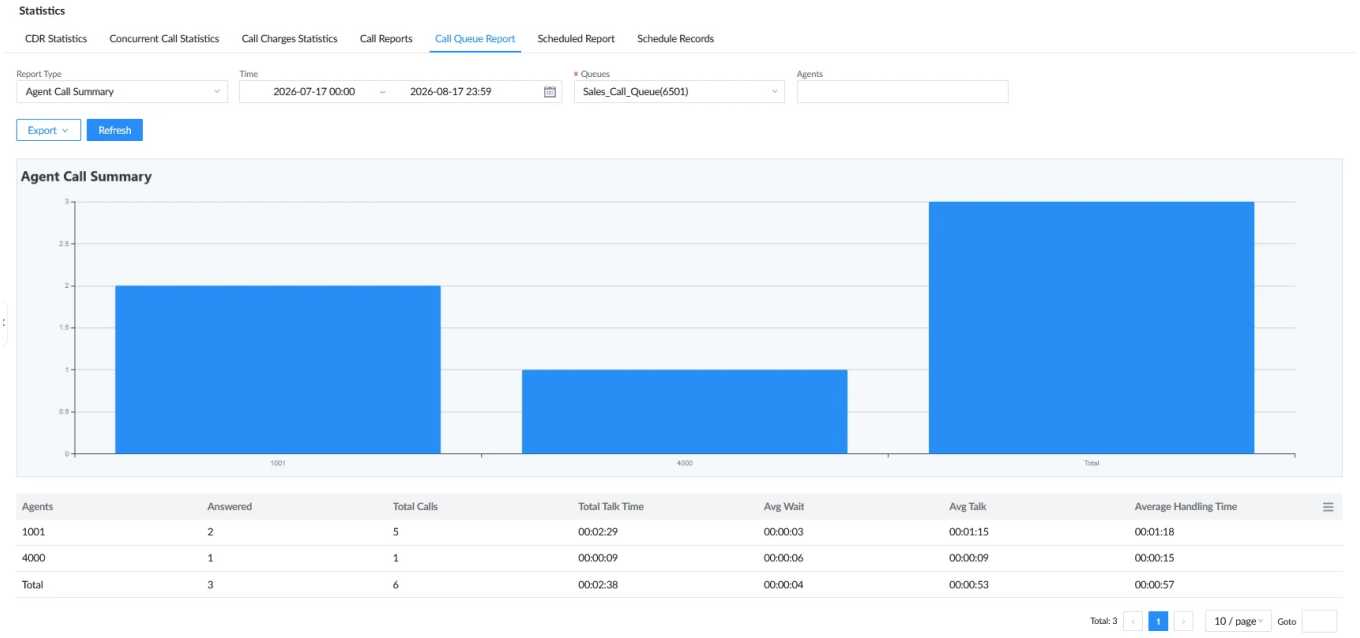
Call Queue Reports

The Call Queue Reports section provides comprehensive, dedicated analytics for call queue performance, agent activities, and queue response metrics across the UCM. Administrators can use these reports to analyze call flow efficiency, monitor agent productivity, and track queue responsiveness over selected time periods.

To access these reports, please navigate to **CDR -> Statistics -> Call Queue Report** and select a report type from the drop-down menu to view its detailed metrics.

Agent Call Summary

Measures individual agent call statistics throughout a specified date range and queue. It displays total calls handled, answered volume, total talk time, average wait time, average talk time, and average handling time per agent.

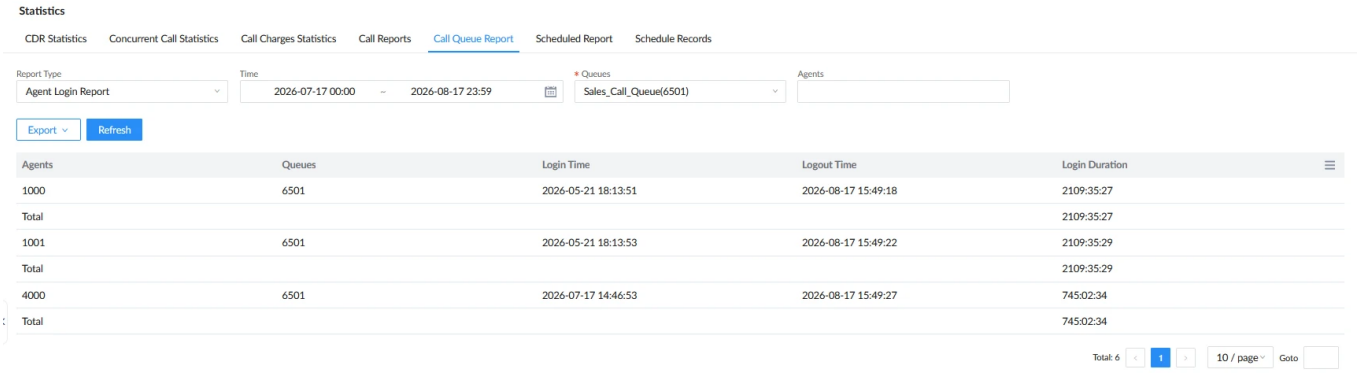


Agents	Answered	Total Calls	Total Talk Time	Avg Wait	Avg Talk	Average Handling Time
1001	2	5	00:02:29	00:00:03	00:01:15	00:01:18
4000	1	1	00:00:09	00:00:06	00:00:09	00:00:15
Total	3	6	00:02:38	00:00:04	00:00:53	00:00:57

Total: 3 1 10 / page Goto

Agent Login Report

Lists individual agent login activity throughout a selected date range for a specific call queue, allowing administrators to track attendance, active duration, and login/logout timestamps.

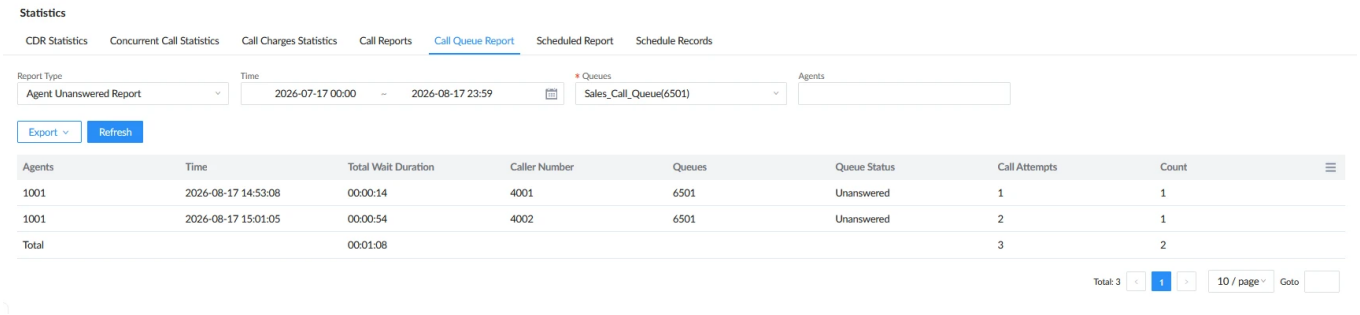


Agents	Queues	Login Time	Logout Time	Login Duration
1000	6501	2026-05-21 18:13:51	2026-08-17 15:49:18	2109:35:27
Total				2109:35:27
1001	6501	2026-05-21 18:13:53	2026-08-17 15:49:22	2109:35:29
Total				2109:35:29
4000	6501	2026-07-17 14:46:53	2026-08-17 15:49:27	745:02:34
Total				745:02:34

Total: 6 1 10 / page Goto

Agent Unanswered Report

Displays individual agent unanswered calls throughout a date range. It provides visibility into the number of missed calls, attempts, and caller number.

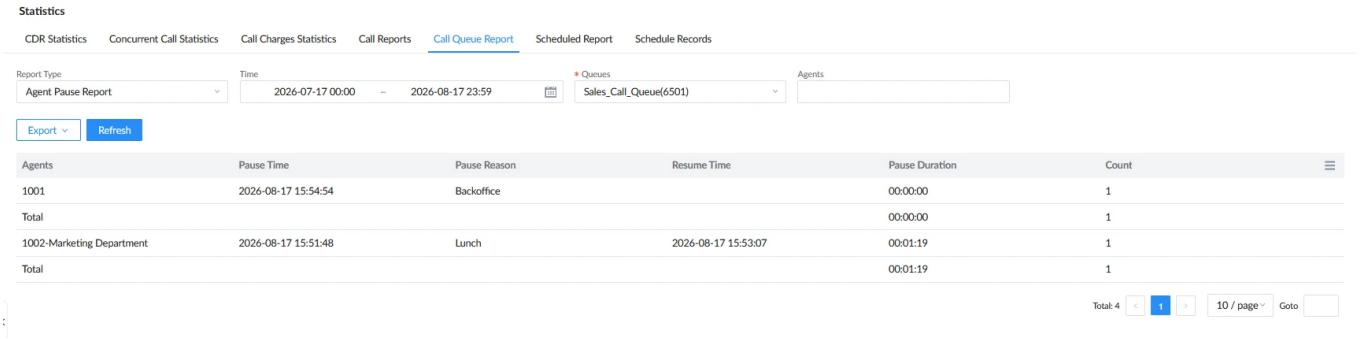


Agents	Time	Total Wait Duration	Caller Number	Queues	Queue Status	Call Attempts	Count
1001	2026-08-17 14:53:08	00:00:14	4001	6501	Unanswered	1	1
1001	2026-08-17 15:01:05	00:00:54	4002	6501	Unanswered	2	1
Total		00:01:08				3	2

Total: 3 1 10 / page Goto

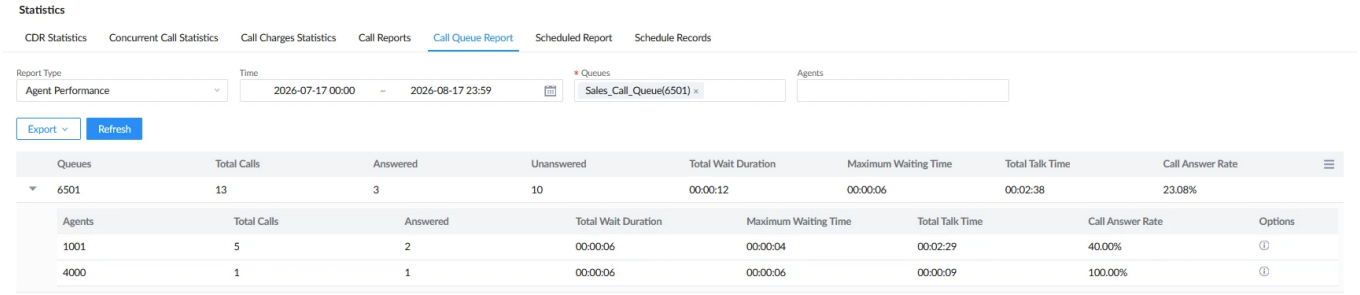
Agent Pause Report

Lists individual agent pausing activity throughout a date range, tracking pause durations, reasons, and total offline time during operational hours.



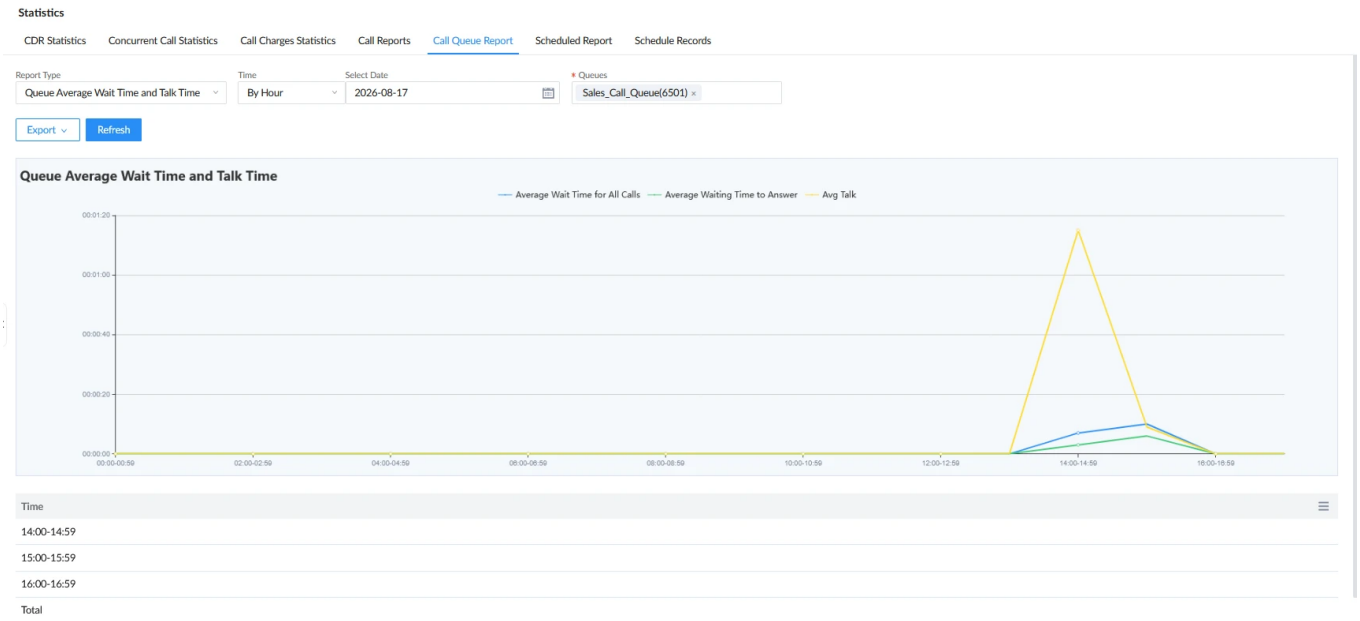
Agent Performance

Measures individual agent performance listed and grouped directly under their respective queues throughout a date range, enabling direct performance comparisons within specific teams.



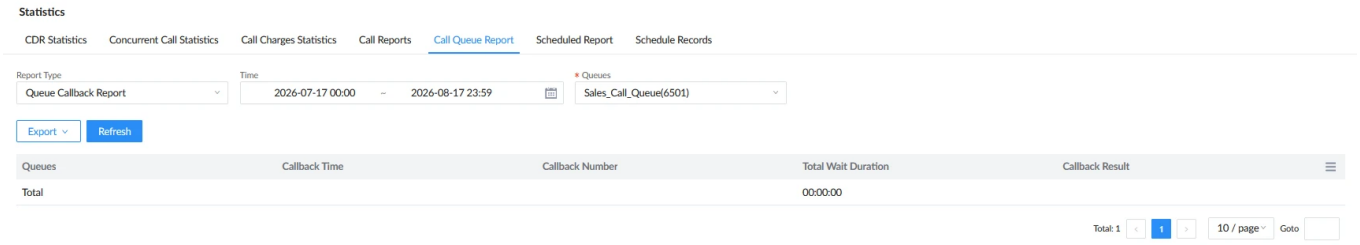
Queue Average Wait Time & Talk Time

Displays a graph showing caller wait time and talk time hourly, daily, or monthly for selected queues, averaging the data across the chosen time frame to help optimize queue staffing levels.



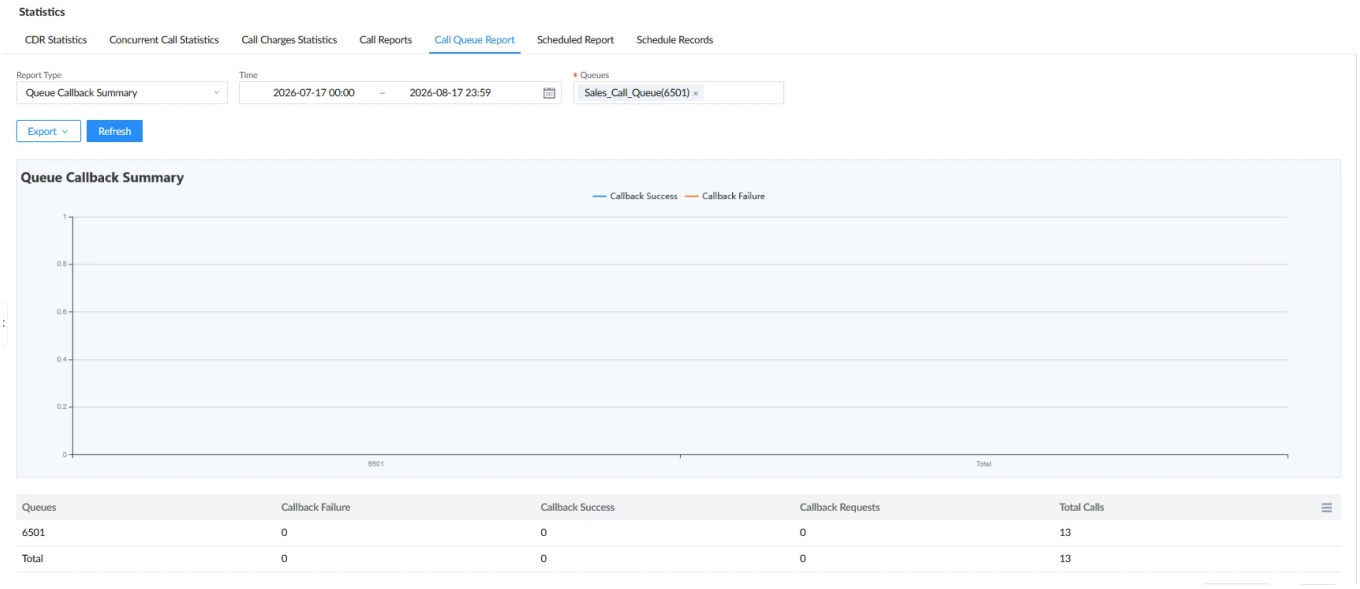
Queue Callback Report

Lists individual queue callback activity throughout a date range and specified queue, detailing requested callbacks, execution timestamps, and call results.



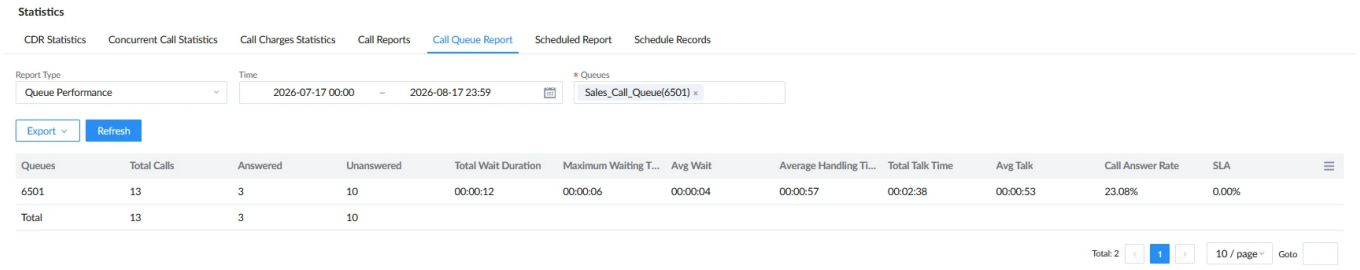
Queue Callback Summary

Displays a graphical representation of queue callback statistics over a specified date range. It provides visual insights into overall callback performance, comparing successful connections against failed callback attempts across the selected queues.



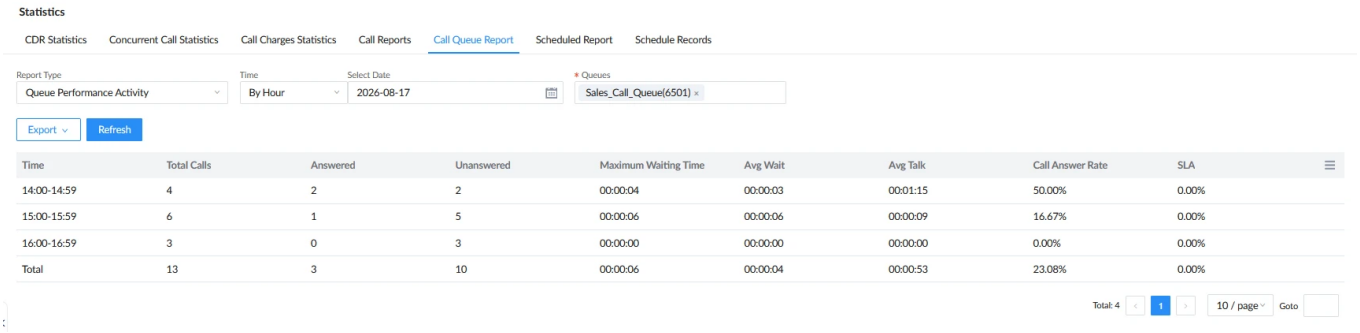
Queue Performance

Measures individual queue performance throughout a date range, focusing on total wait duration, average handling time, and overall service levels per queue.



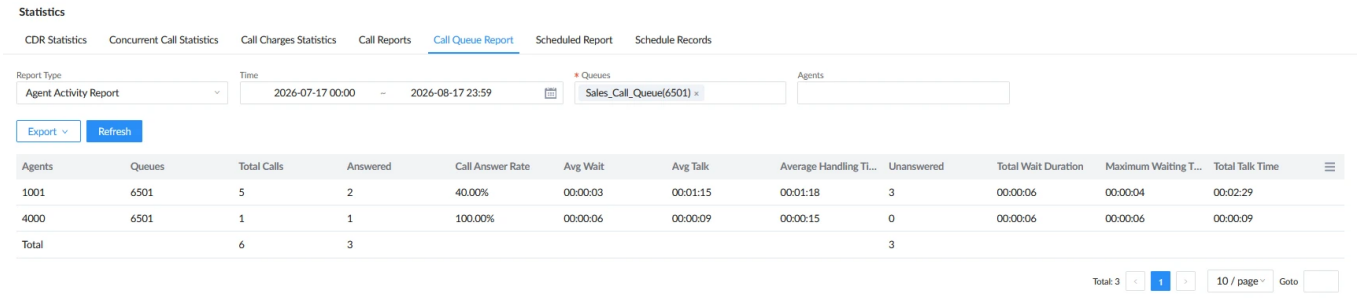
Queue Performance Activity

Provides a time-based breakdown (hourly, daily, or monthly) of call queue activity. Administrators can use this report to evaluate traffic distribution, monitor answer rates and average wait times, and track SLA performance over a selected period.



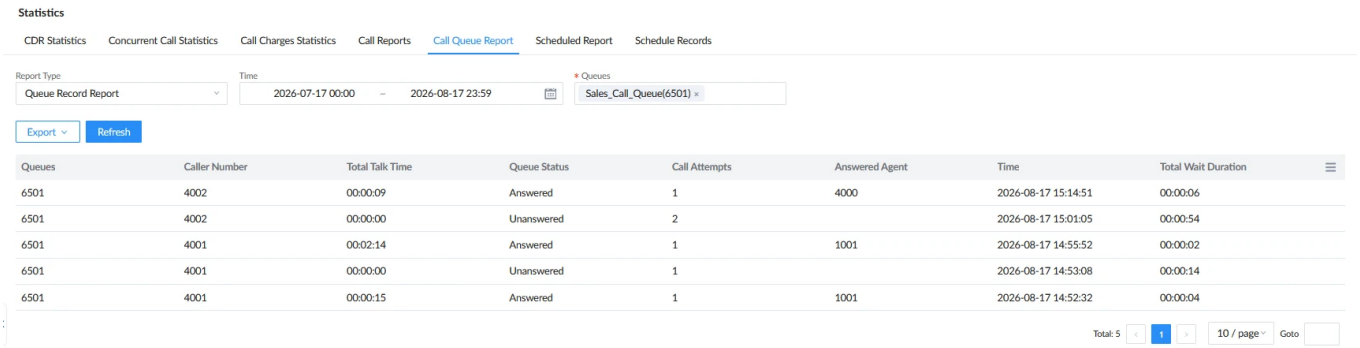
Agent Activity Report

Provides a comprehensive performance breakdown for each agent across selected queues over a specified date range. It details total call volume, answer rates, unanswered calls, wait times, talk duration, and average handling times per agent.



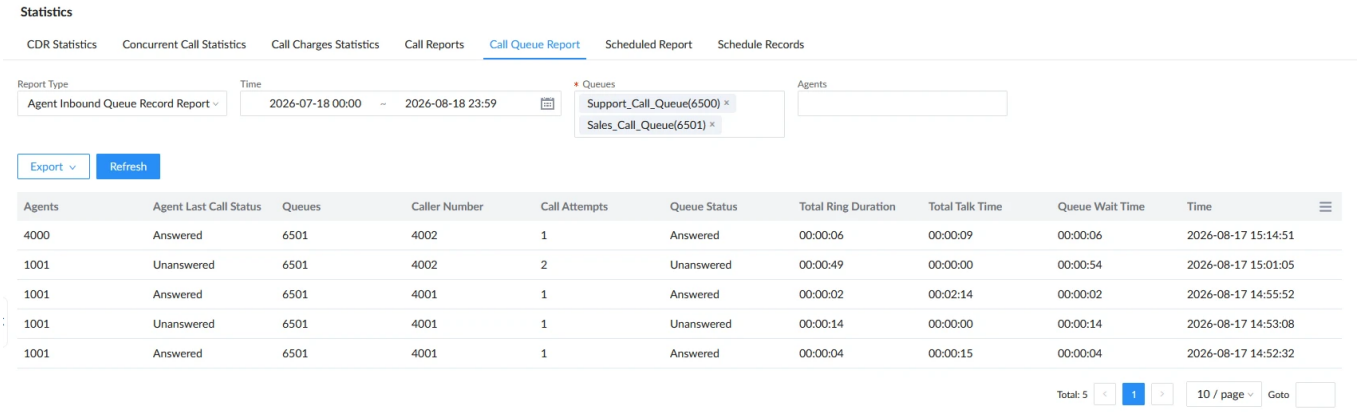
Queue Record Report

Lists every individual call made to the selected queues throughout a specified date range. It details the caller number, queue status, number of call attempts, answering agent, call timestamp, total wait duration, and total talk time.



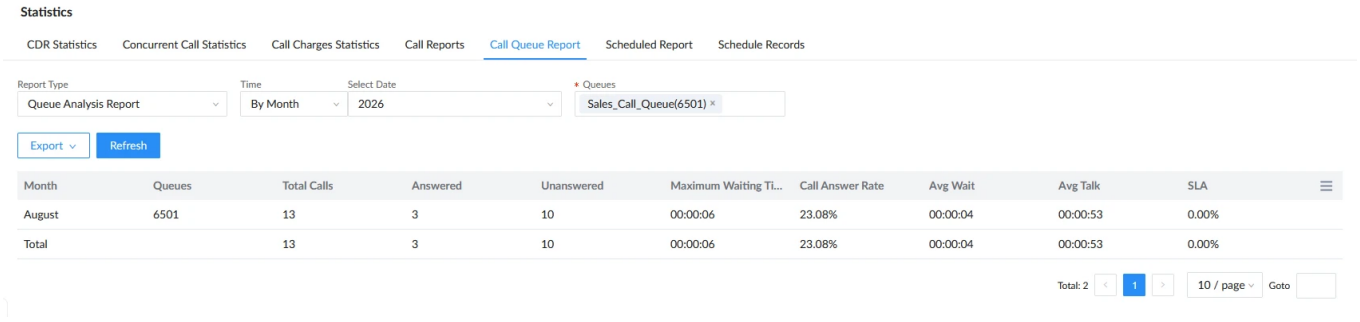
Agent Inbound Queue Record Report

Displays a granular call log for each agent within selected queues over a date range, tracking individual interactions, ring duration, talk time, wait time, and whether the agent answered or missed the call.



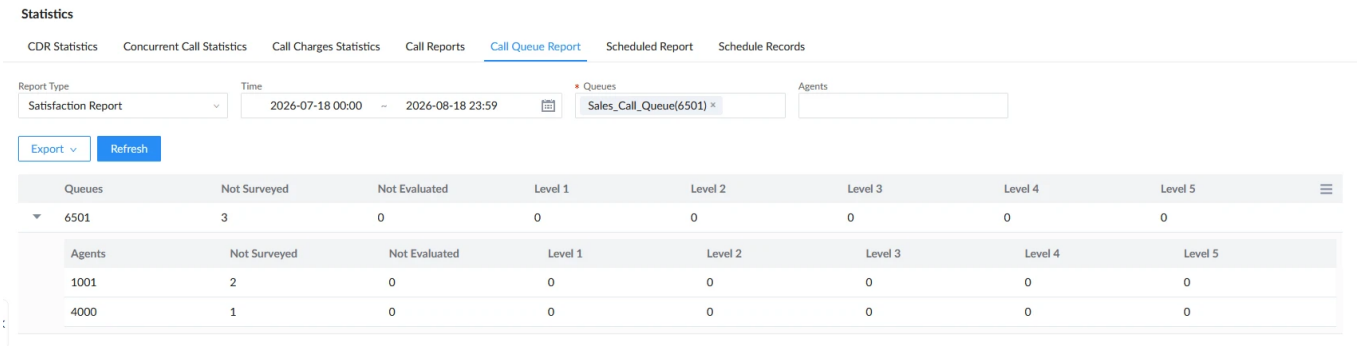
Queue Analysis Report

Sorts and measures call statistics on an hourly, daily, or monthly basis, displaying a dedicated row for each individual queue during every time interval. This provides per-queue trends, unlike Queue Performance Activity, which summarizes total system traffic.



Queue Statistics Report

Generates a satisfaction breakdown for selected queues within a date range, categorizing caller rating scores into levels 1 to 5 alongside counts for non-surveyed calls.



Scheduled Report

The Scheduled Report tab allows administrators to create automated report delivery schedules and have reports sent via email at regular intervals.

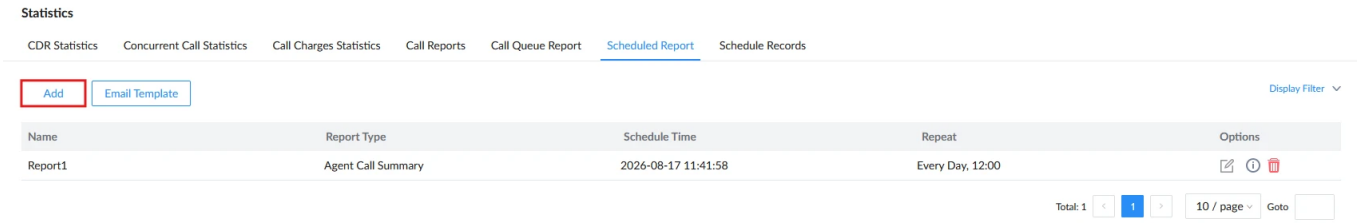
This feature is limited to call queue reports.

In order to receive the scheduled reports, administrators must correctly configure Email Settings.

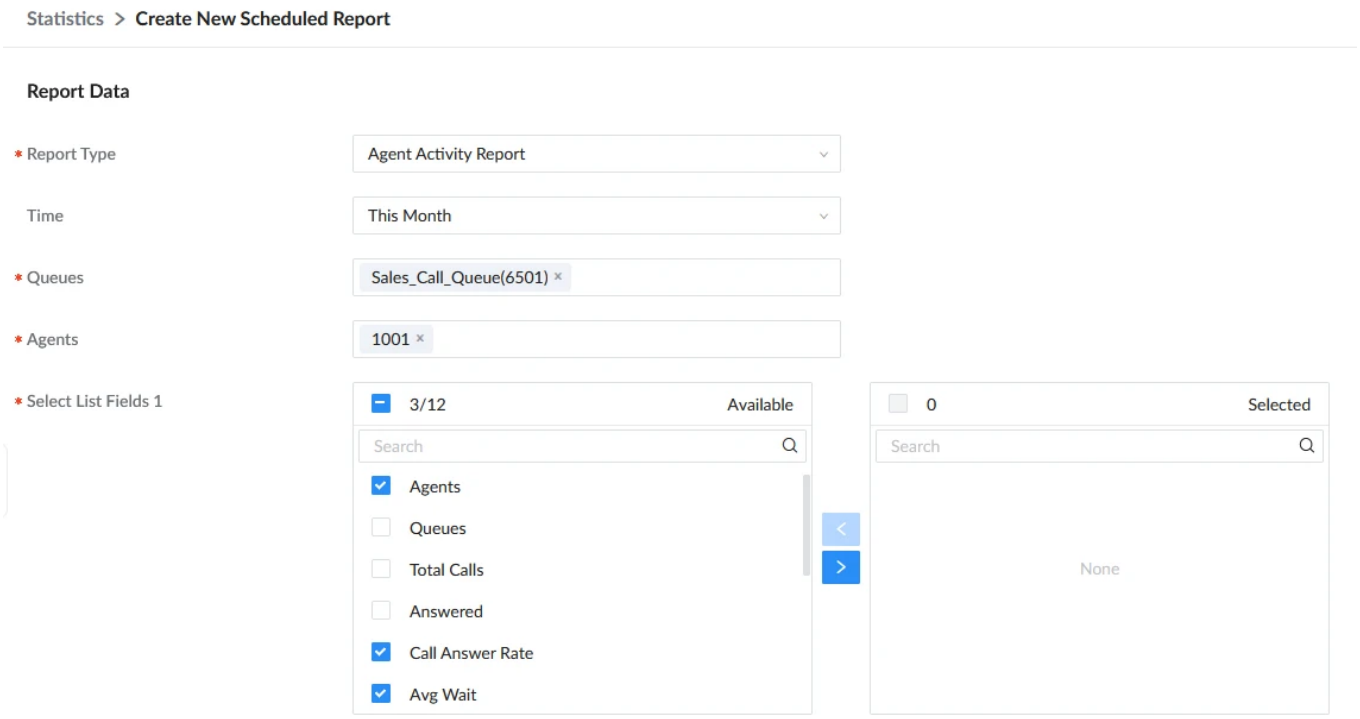
To configure an automated report schedule:

1. Navigate to **CDR -> Statistics -> Scheduled Report**.

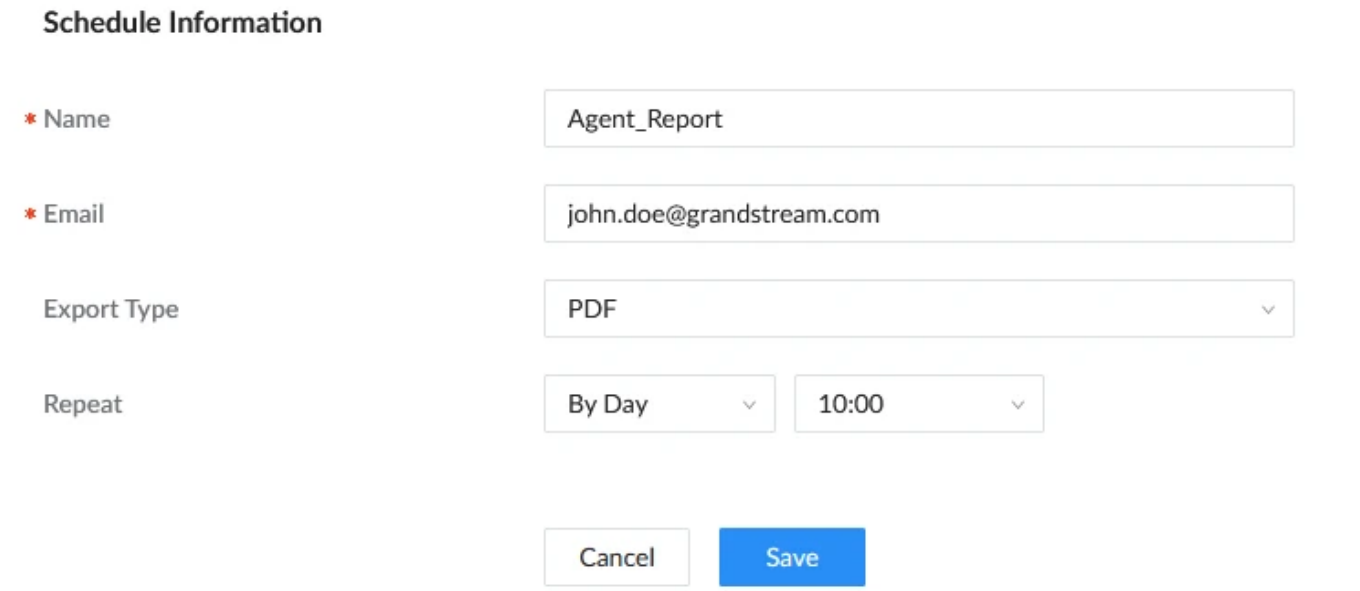
2. Click **Add** to open the creation window (or click **Email Template** to customize the notification layout).



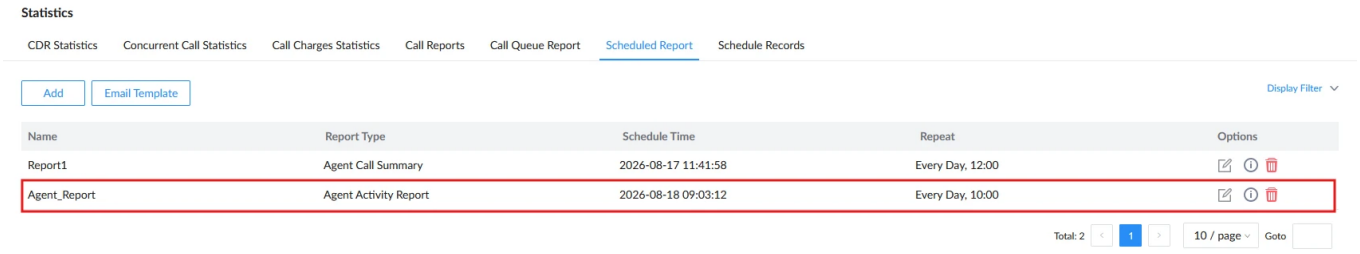
3. Under **Report Data**, select the Report Type, Time frame, target Queues, Agents, and customize the List Fields to include in the output.



4. Under **Schedule Information**, enter the schedule Name, recipient Email, preferred Export Type (XLSX, CSV, PDF), and execution recurrence pattern (Repeat interval and time).



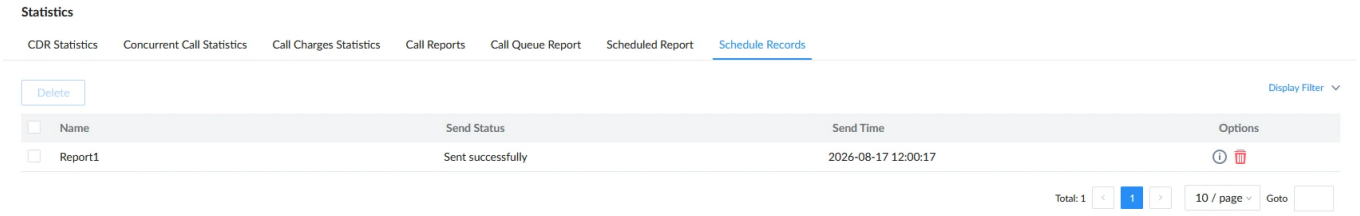
Once configured, all active schedules are listed on this page for quick editing or management.



Schedule Records

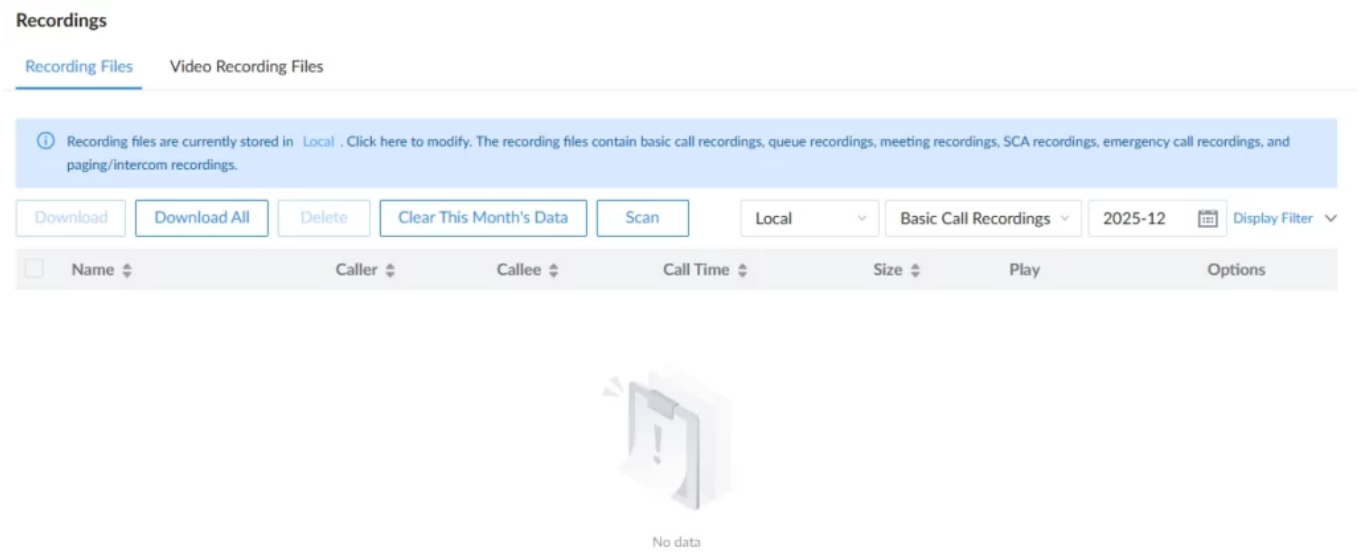
The **Schedule Records** tab provides full historical tracking and audit logging for all automated email report transmissions. On this page users can:

- Review historical entries including the schedule **Name**, transmission **Send Status** (e.g., Sent successfully), and exact **Send Time**.
- Click the **Info icon (i)** under the Options column to preview the sent report in a different tab.
- Select individual or multiple log entries to delete historical records as needed.



Recordings

This page lists all the recording files recorded by "Auto Record" per extension/ring group/call queue/trunk, or via feature code "Audio Mix Record". If external storage device is plugged in, for example, SD card or USB drive, the files are stored on the external storage. Otherwise, internal storage will be used on the UCM630X.



CDR > Recording Files

- Click on "**Download**" to batch-download the selected recording files.
- Click on "**Download All**" to download all the recording files.
- Click on "**Delete**" to batch-delete the selected recording files.

- Click on "**Clear**" to delete all the recording files.
- Click on "**Scan**" to retrieve the file information and display all the recording files on external storage. The UCM automatically retrieves the info of the first 5000 files from external storage already. This button can be used when the number of files stored on the external storage exceeds 5000 files and it requires manual file scanning.
- Select either "**USB Disk**" or "**Local**" to show recording files stored on external or internal storage, depending on selected storage space.
- Select whether to show call recordings, queue recordings or conference recordings.
- Click on to download the recording file in .wav format.
- Click on to delete the recording file.
- To sort the recording file, click on the title "Caller", "Callee" or "Call Time" for the corresponding column. Click on the title again can switch the sorting mode between ascending order or descending order.

If Data/File encryption is enabled for audio/video call recordings, scanning the external storage for recordings via the Scan button will automatically encrypt all the found recordings.

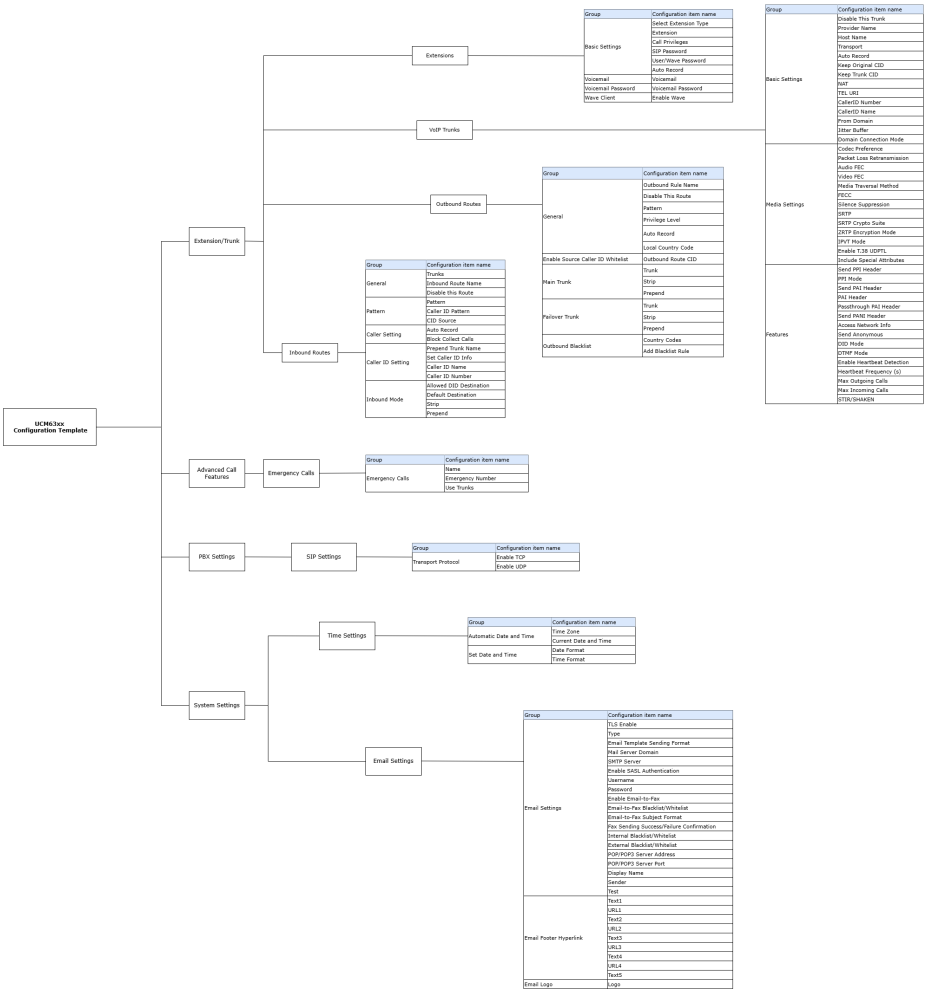
PROVISIONING

UCM6300 Series supports configuration provisioning via GDMS, enabling users to configure a single UCM6300 Series device or perform batch configurations using predefined templates to ensure consistency and increase efficiency.

This section describes in detail how UCM6300 Series leverages GDMS to facilitate efficient configuration provisioning for both individual devices and large-scale deployments.

Configuration Parameters

To give users a better understanding of the configuration possibilities, the following diagram outlines the key configuration parameters available in UCM6300 through GDMS.



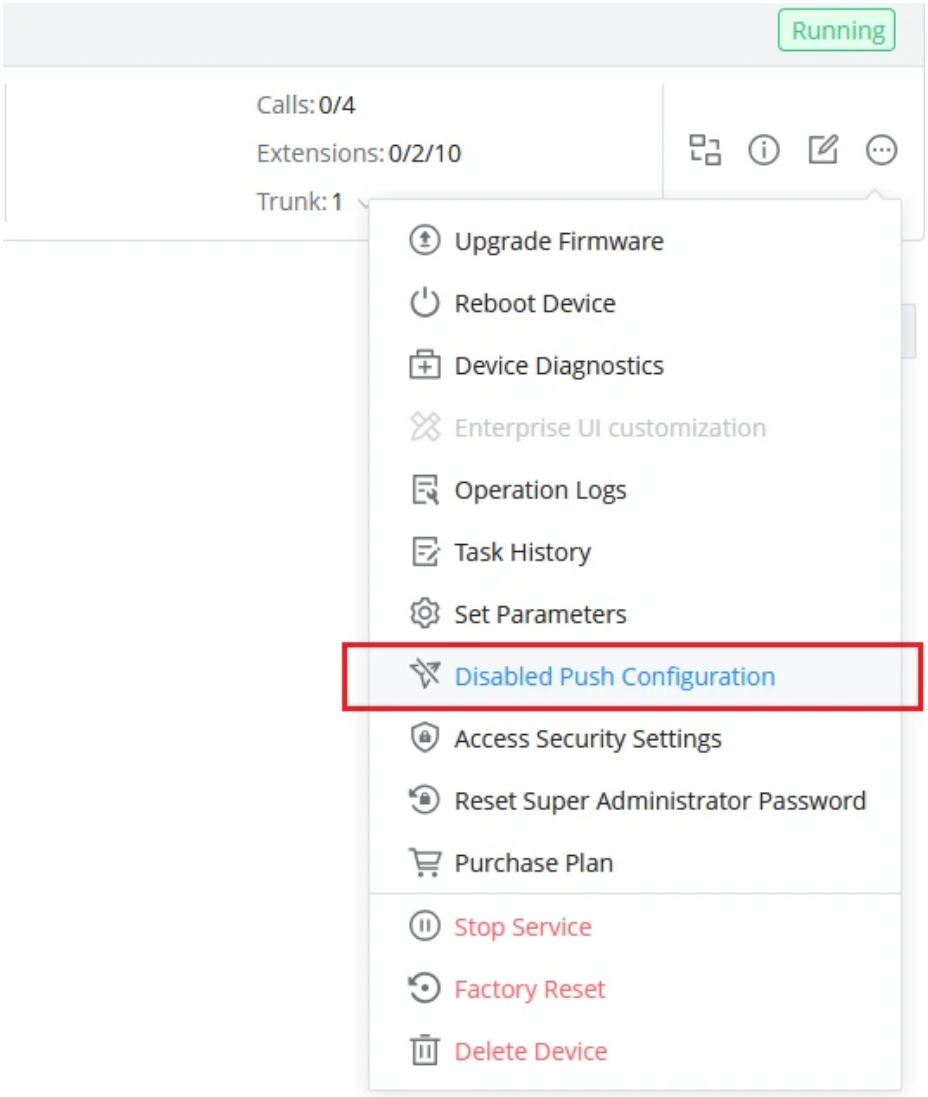
UCM6300 Series Configuration Template Parameters

Creating UCM6300 Configuration Template

UCM6300 Series supports provisioning using two types of templates:

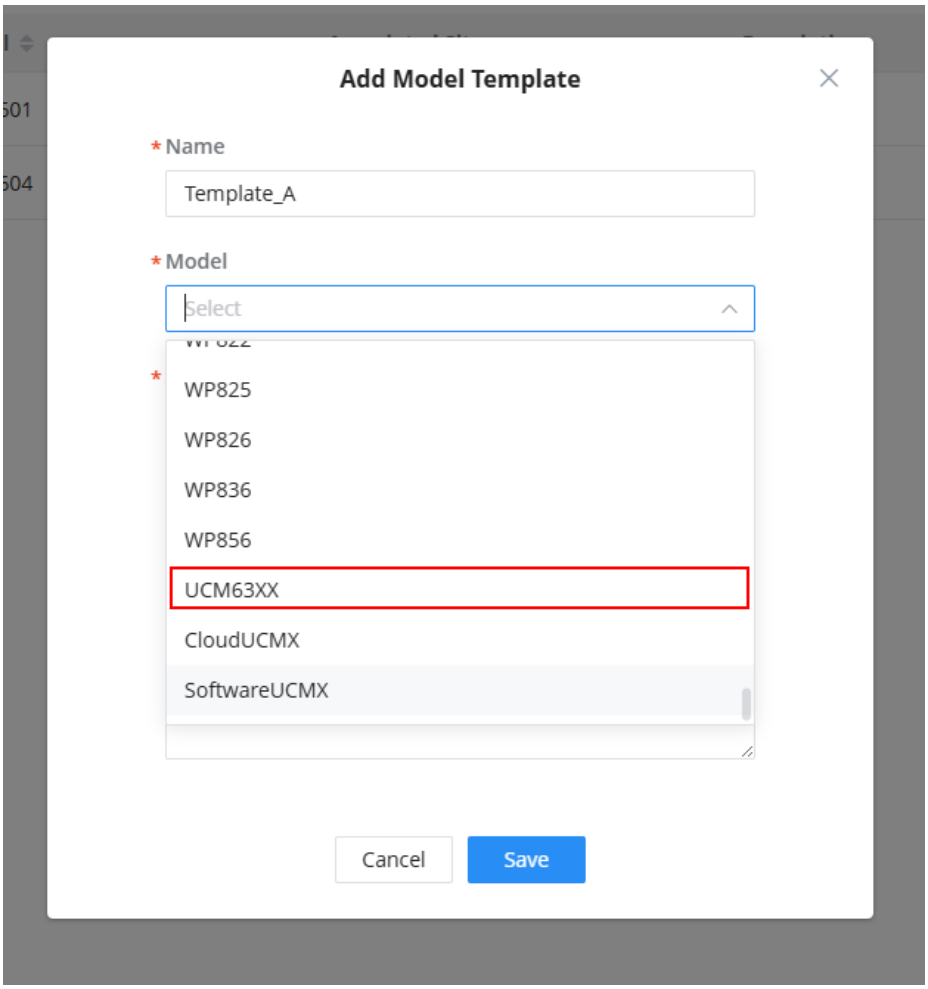
Model Template

After adding a UCM6300 model template, the configuration will be pushed to the selected site automatically, except for UCM6300 series where push configuration has been disabled. (See image below)



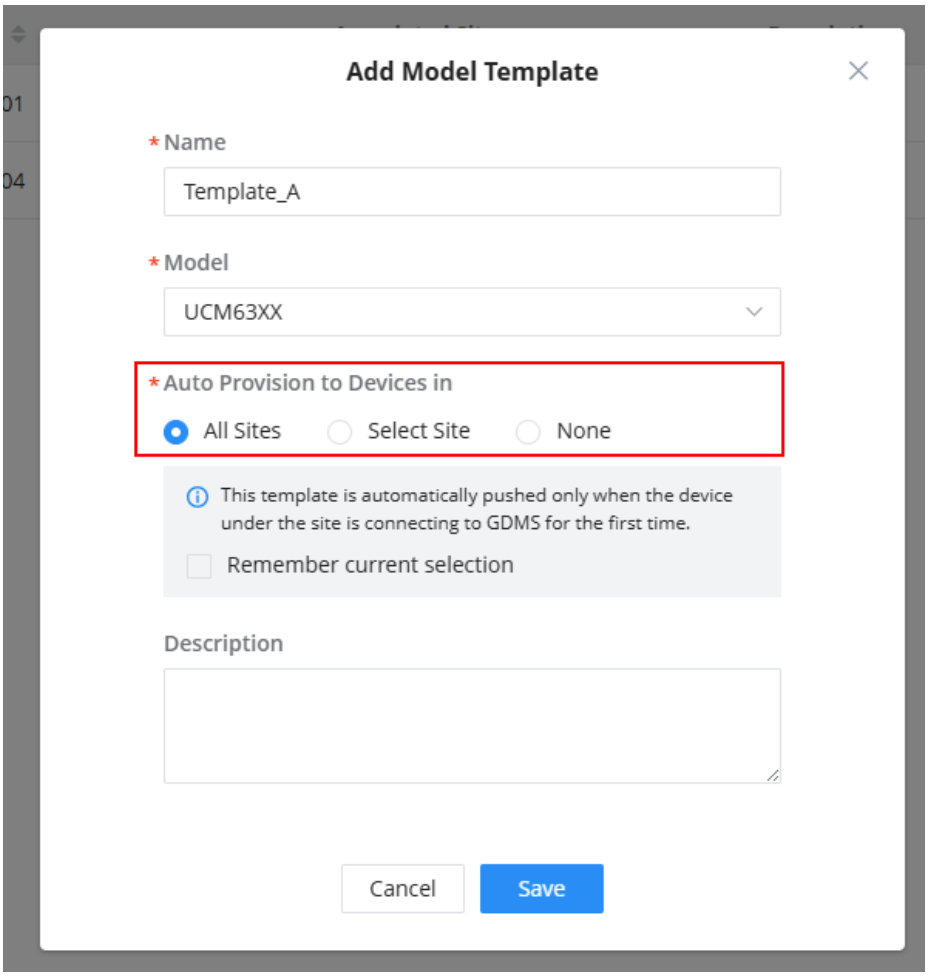
In order to add a UCM6300 model template, please follow these steps:

1. Go to **Organization -> Device Template -> By Model** and click on
2. Enter a name for this template and select UCM6300 from the Model list.



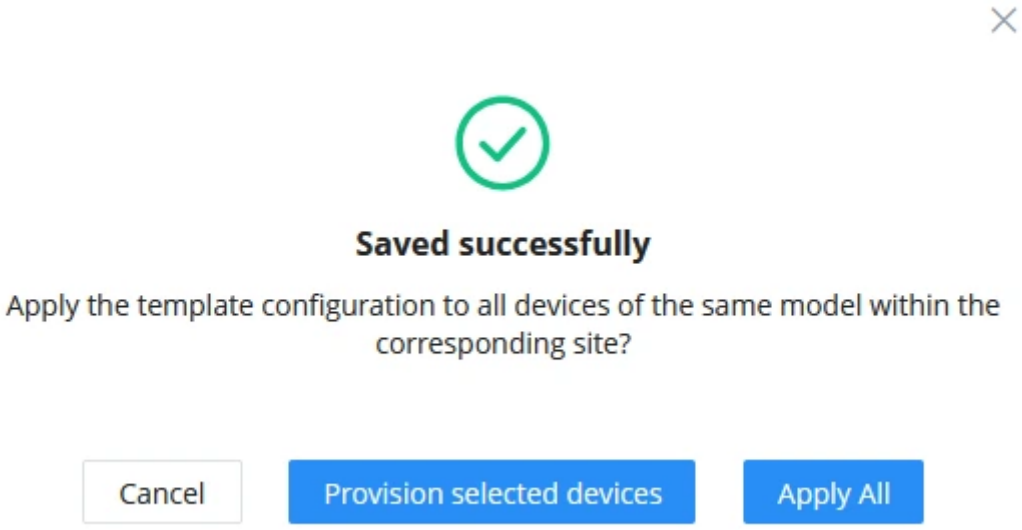
Select The Model

3. Choose whether to automatically push this template to a specific site, all sites or none. Users can also add a description for this template (optional).



Select Sites

4. Configure the model template parameters and click **Save**. A prompt will appear, confirming the change and offering the option to push the configuration to the entire site or to specific devices.

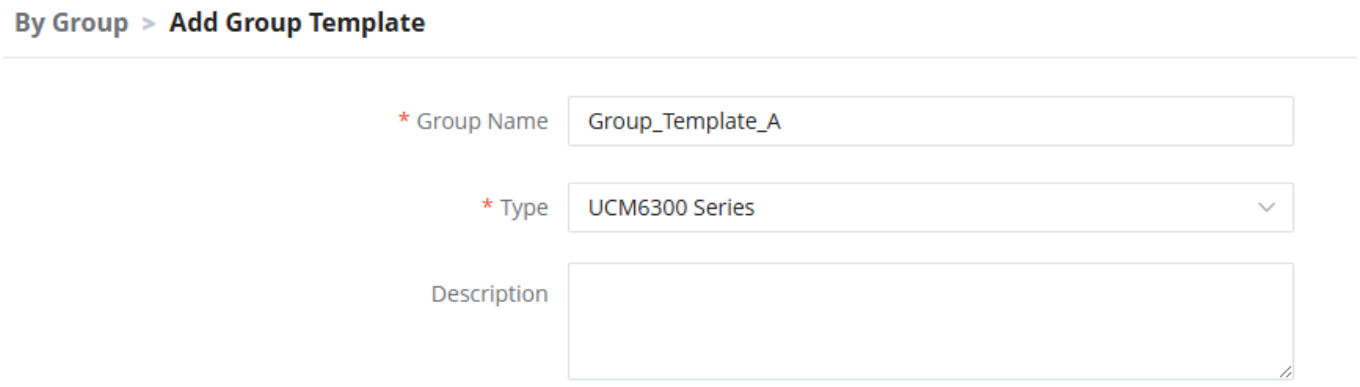


Group Template

Users can configure a group of UCM6300 devices and apply settings to the entire group simultaneously by following the instructtions below:

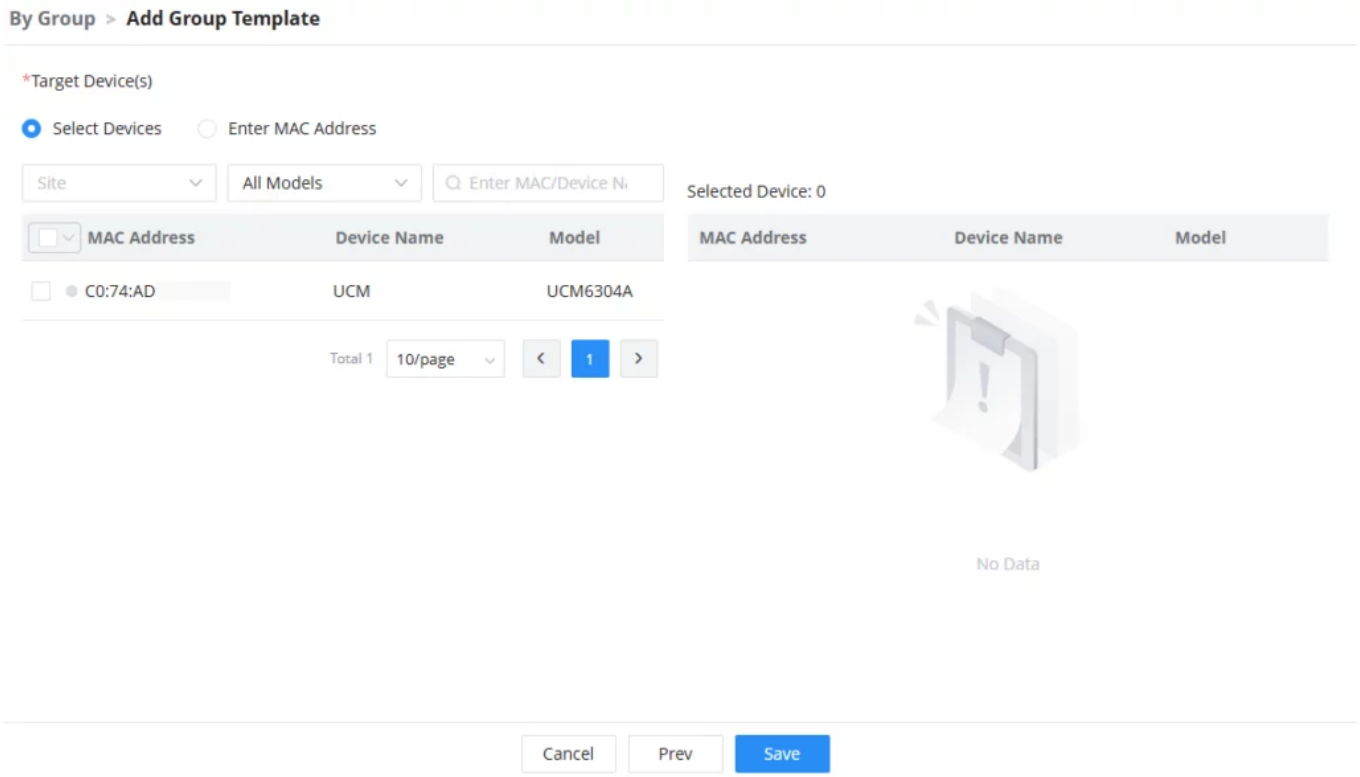
1. Under Organization -> Device Template -> By Group, click on

2. Name the group and choose the UCM6300 series from the Type dropdown list. Writing a description is optional.



Add Group Template

3. Select the target devices by checking the boxes or by entering their MAC Address.



Add Devices To The Group Template

Pushing Configuration For UCM6300 Series

There are several methods available for users to push configurations to a UCM6300 device. This section will explain each method in detail, but first, it is important to highlight some important notes.

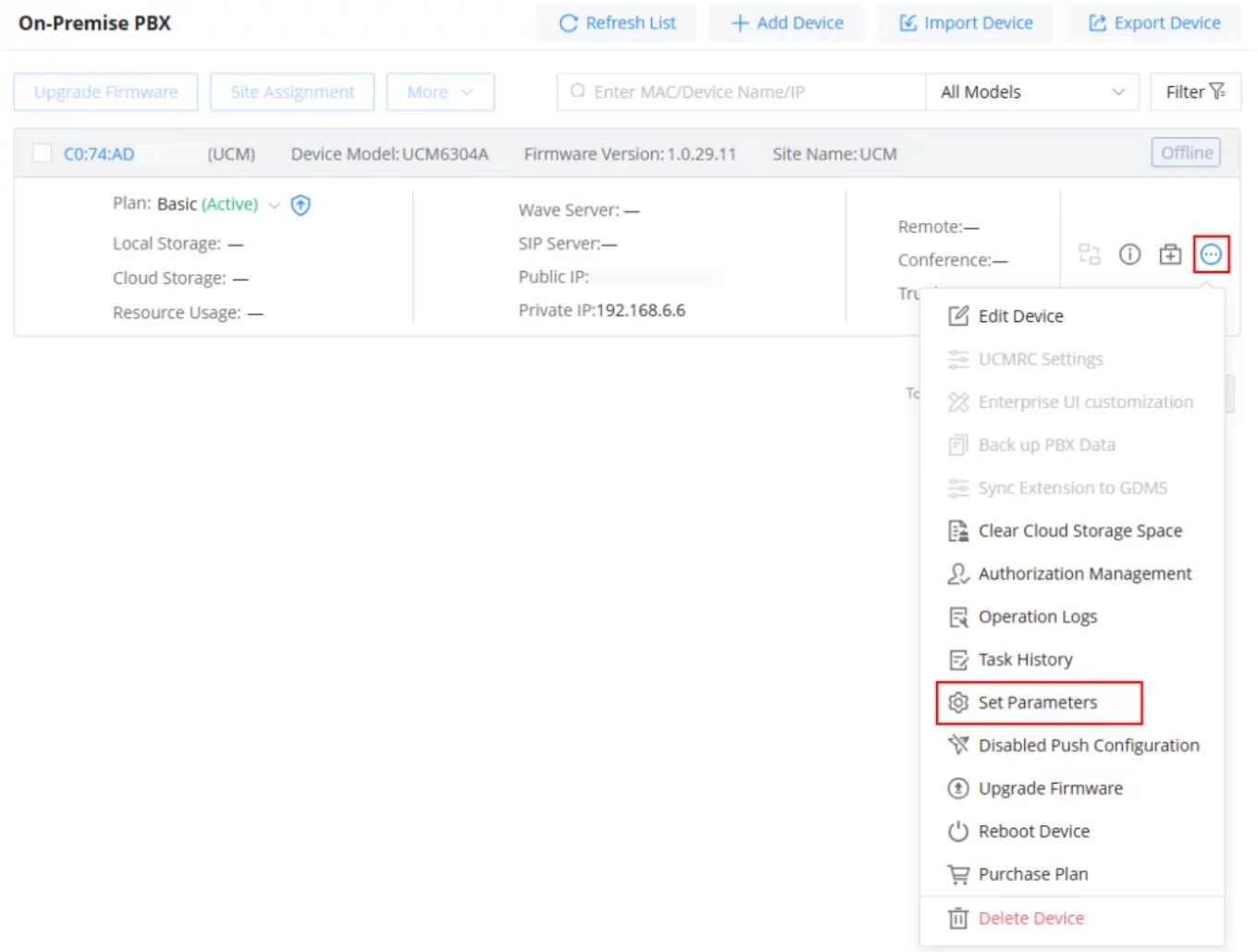
- If a required configuration parameter fails (e.g. invalid voicemail password), the configuration will be considered unsuccessful.
- If a restart is needed, it will be performed immediately.
- When using a configuration template for a new UCM6300 Series device, the setup wizard will still appear upon the first login and cannot be skipped.

The enabled fields in template configuration will override the configuration configured on the UCM. Reviewing your configuration before pushing it to the UCM is mandatory to avoid any misconfiguration.

Setting Parameters for a Single UCM6300 Series

The user can edit the configuration for a single UCM6300 by going to **UCMRC > On-Premise PBX**.

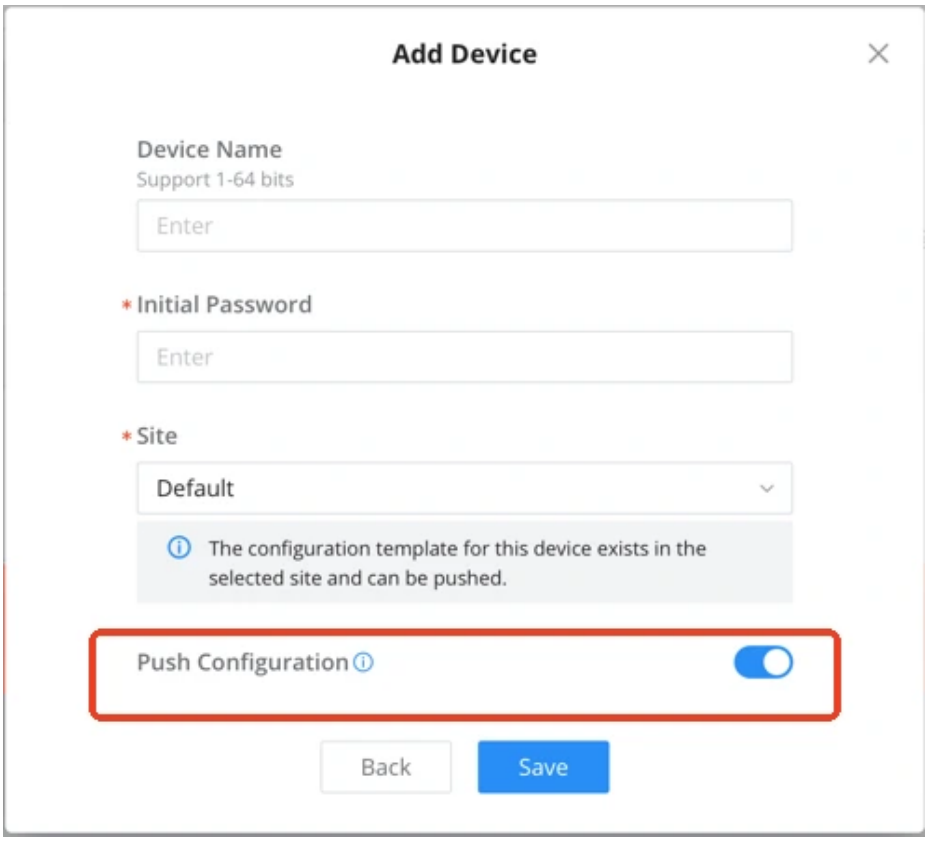
Then click on then click on "Set Parameters" as shown below in the screenshot.



UCM6300 Series Set Parameters

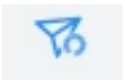
Automatically Pushing the Configuration

When adding a UCM6300 Series device and the selected site has an associated UCM6300 Series model template, a prompt will appear with the option to allow the automatic push configuration.



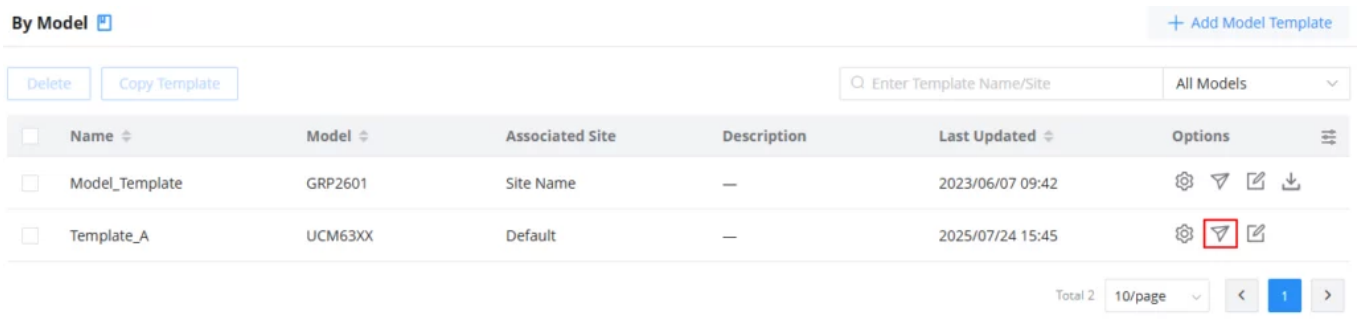
Push Configuration When Adding a New Device

As mentioned previously, users can disable/enable push configuration anytime for a specific UCM6300 Series. The following table includes the icons related to automatic push configuration:

Icon	Description
	Push configuration is prohibited.
	Configuration is being pushed.
	Last push configuration has failed. (Users can click on this icon to try again)

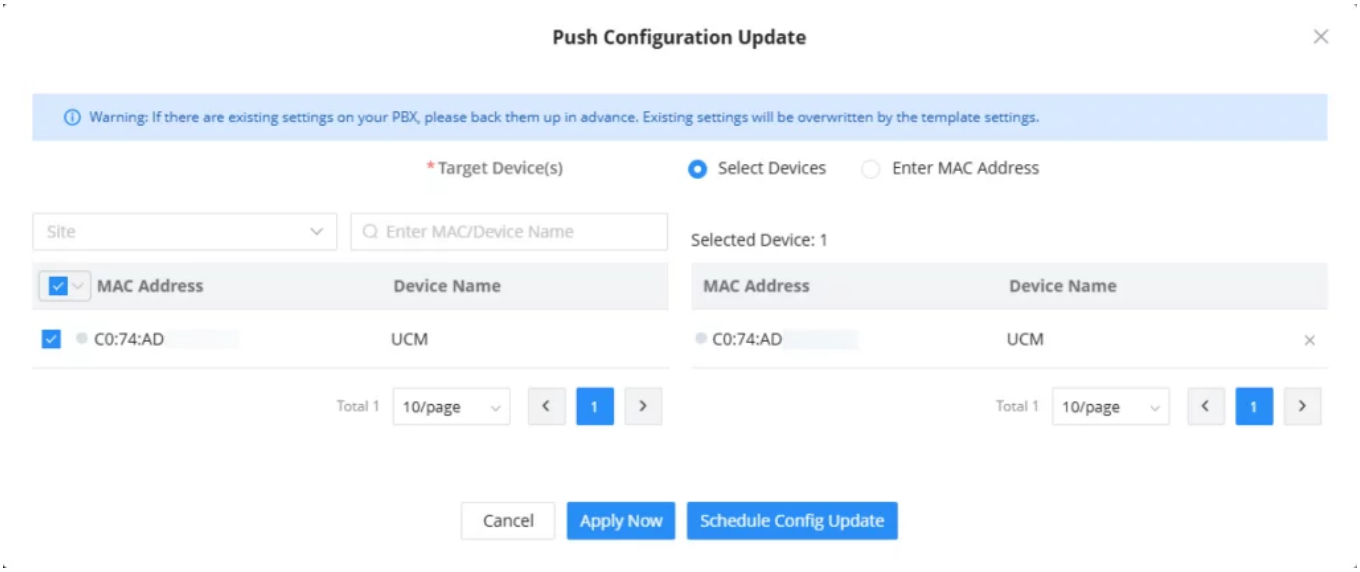
Manually Pushing The Configuration

It is possible to manually push model configuration templates or group configuration templates to multiple UCM6300 Series. This can be done by clicking on the Push Configuration Update icon that can be found under **Organization > Device Template > By Model/By Group**.



Push Configuration Manually

Select the device from the list, as shown in the screenshot below, or select Enter MAC Address to type the MAC address of the target device.



Choose a Device

REMOTECONNECT

An integrated and essential component of Grandstream's GDMS cloud-based device management service, UCM RemoteConnect runs on Amazon Web Services (AWS) and provides high-availability remote communication and collaboration services.

UCM RemoteConnect enables work from home and mobile users to securely access UCM services using Grandstream Wave softphones, with license-free WebRTC-based communication, automatic NAT traversal, and centralized cloud-based management. In addition, RemoteConnect provides GDMS cloud storage, Cloud IM, AI Services, and other collaboration and management features.

The RemoteConnect service can be configured from the UCM Web GUI under the **RemoteConnect** tab.

For more information about the UCM RemoteConnect services, please refer to the UCM RemoteConnect - User Guide.

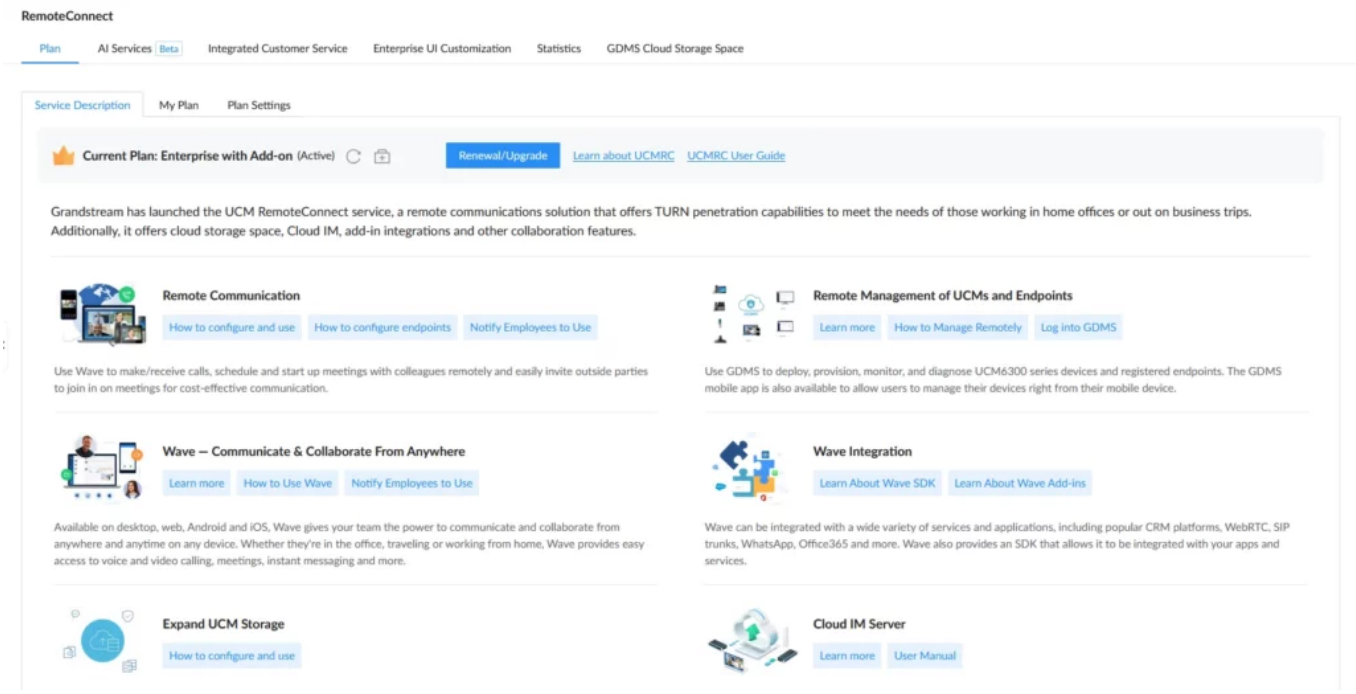
Plan

This section provides an overview of the RemoteConnect service associated with the UCM, including service description, current subscription status, and configurable plan options.

Service Description

After the UCM is added to GDMS, RemoteConnect enables automated SIP extension synchronization, Media NAT Traversal, and basic statistics without requiring manual configuration. These services allow remote users and devices to connect reliably through the cloud.

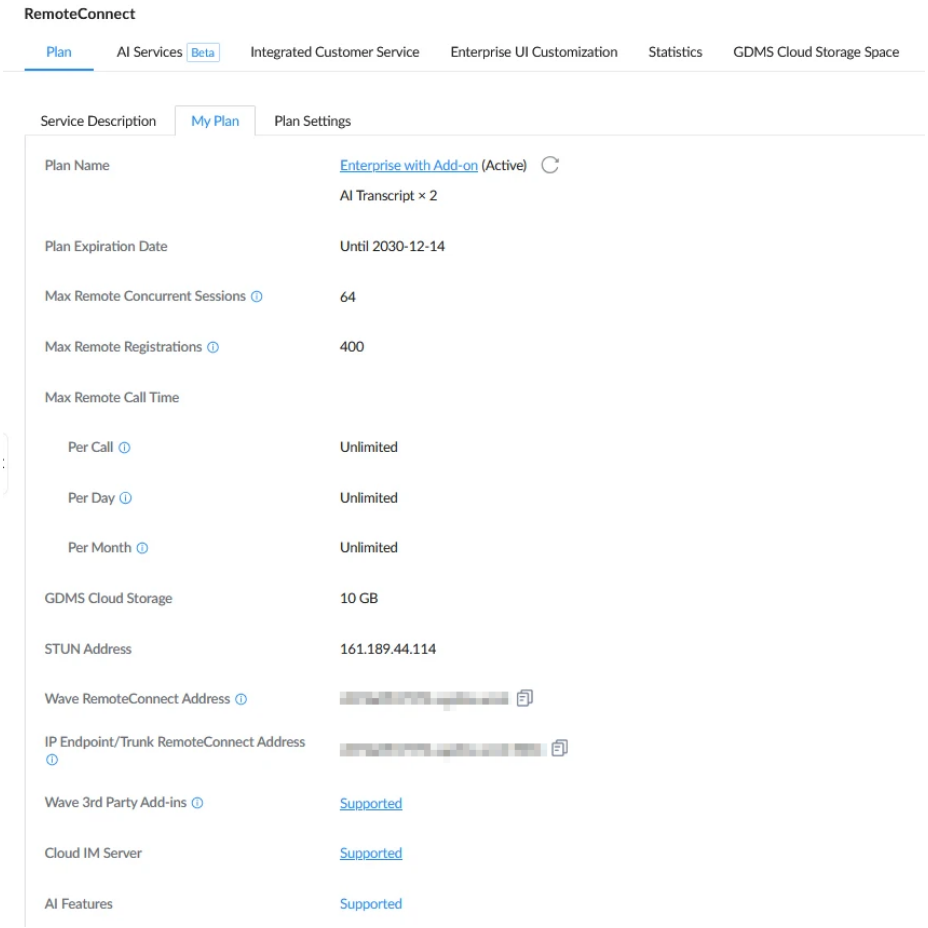
This tab provides an overview of the UCMRC services and displays the current subscription plan, as well as related links and learning resources for the services supported by RemoteConnect.



RemoteConnect Service Description Tab

My Plan

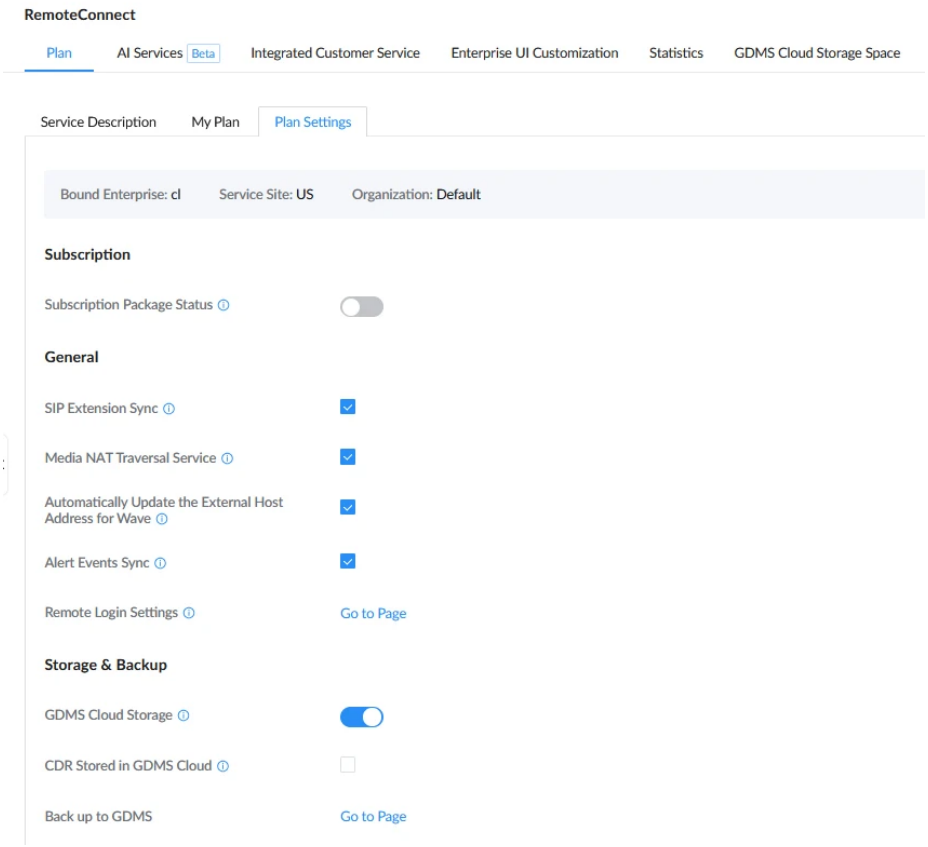
This page displays detailed information about the currently active RemoteConnect subscription, including plan name, expiration date, concurrent session limits, remote registration limits, call time limits, allocated GDMS cloud storage space, Wave RemoteConnect addresses, and support status for Wave add-ins, Cloud IM Server, and AI features.



RemoteConnect My Plan Tab

Plan Settings

This tab allows administrators to configure how the UCM interacts with UCMRC services, including SIP synchronization, NAT traversal, cloud storage, backups, and remote access behavior. All settings on this page take effect immediately after saving and directly impact how the UCM integrates with GDMS and cloud services.



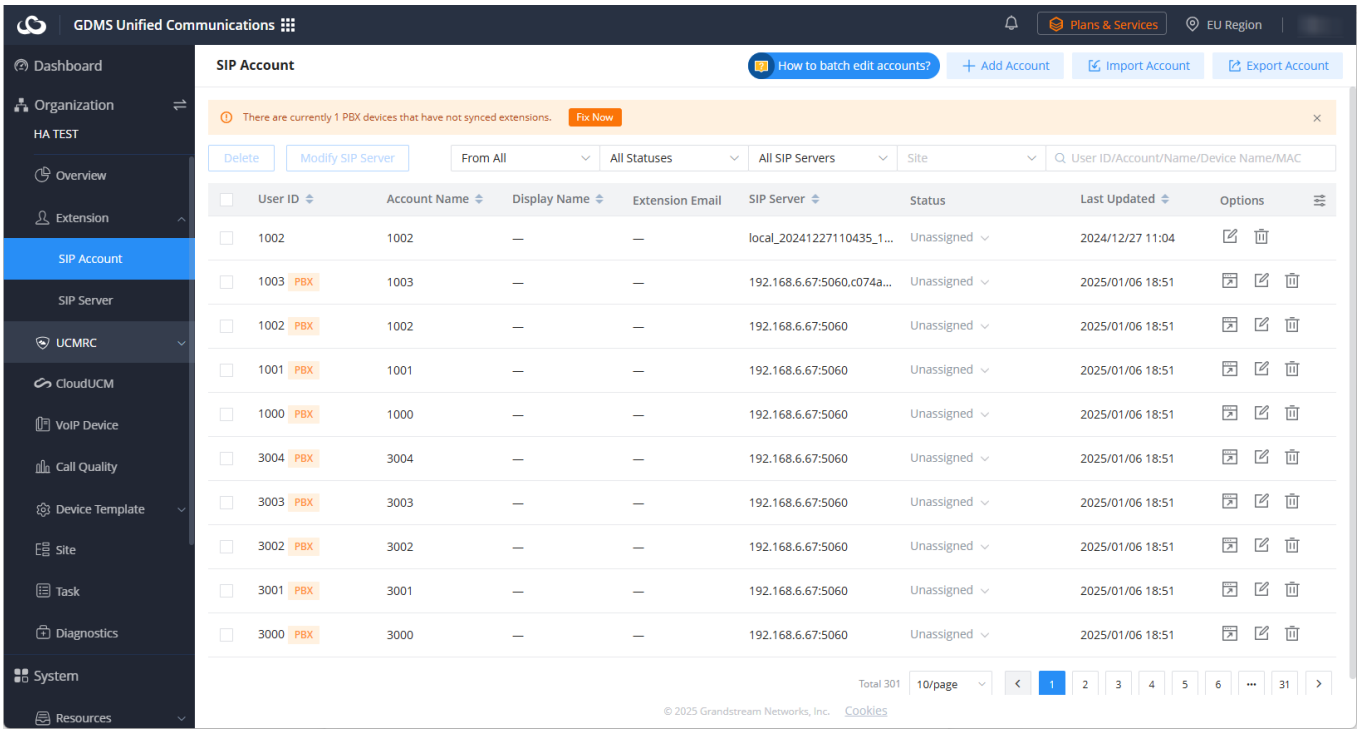
RemoteConnect Plan Settings Tab

The table below describes the configurable parameters on this page.

Subscription	
Subscription Package Status	Once enabled, the configured email address will receive notifications about the UCMRC package status such as expiration or low balance.
Email	The email entered in this field will receive updates regarding subscription status.
General	
SIP Extension Sync	Enables synchronization of SIP extensions between the UCM and GDMS. When enabled, all SIP extensions on the UCM are automatically exported to GDMS.
Media NAT Traversal Service	Enables automatic TURN based NAT traversal for remote users and devices. When enabled, any defined NAT traversal or TURN settings configured locally on the UCM are overridden.
Automatically Update the External Host Address for Wave	Controls whether the Wave external host address is automatically synchronized from UCMRC. Disable this option to retain a user defined Wave domain or external address.
Alert Events Sync	Synchronizes alarm and event information generated on the UCM to the GDMS platform.
Remote Login Settings	Opens the configuration page for managing passwordless remote access to the UCM.

Storage & Backup	
GDMS Cloud Storage	Enables cloud storage services provided by GDMS. This option must be enabled to use cloud-based storage features. Notes:Even if this option is disabled, users will still be able to retrieve data/files stored on GDMS.The UCM will automatically turn on the GDMS Cloud Storage alert event option if this feature is enabled.
CDR Stored in GDMS Cloud	If enabled, UCM CDR data will be synced to the GDMS server at 2 AM on the 1st of each month based on the UCM's system time.
Back up to GDMS	Opens the backup configuration page, allowing UCM configuration backups to be stored in GDMS cloud storage.
Recordings Stored in GDMS Cloud	Opens the file manager configuration page, where administrators can control if call recordings are stored in GDMS cloud storage.
Chat Data Cloud Storage	Opens the file manager configuration page, where administrators can control the chat data storage, allowing instant messaging data to be stored in GDMS cloud storage.
Passwordless Remote Access	
Enable Passwordless Remote Access	Allows authorized GDMS users to access the UCM without entering the local UCM account password.

When "SIP Extension Sync" is enabled, the accounts synchronized to GDMS platform can be viewed on the **GDMS->VoIP Account->SIP Account** page. As shown in the figure below:



UCM SIP Extensions synchronized to GDMS

- Deleting an account on GDMS only removes the association between the account and the device, and does not delete the SIP account information on UCM.
- Any creation, deletion or modification of the SIP account on UCM will be automatically synchronized to the GDMS cloud platform.

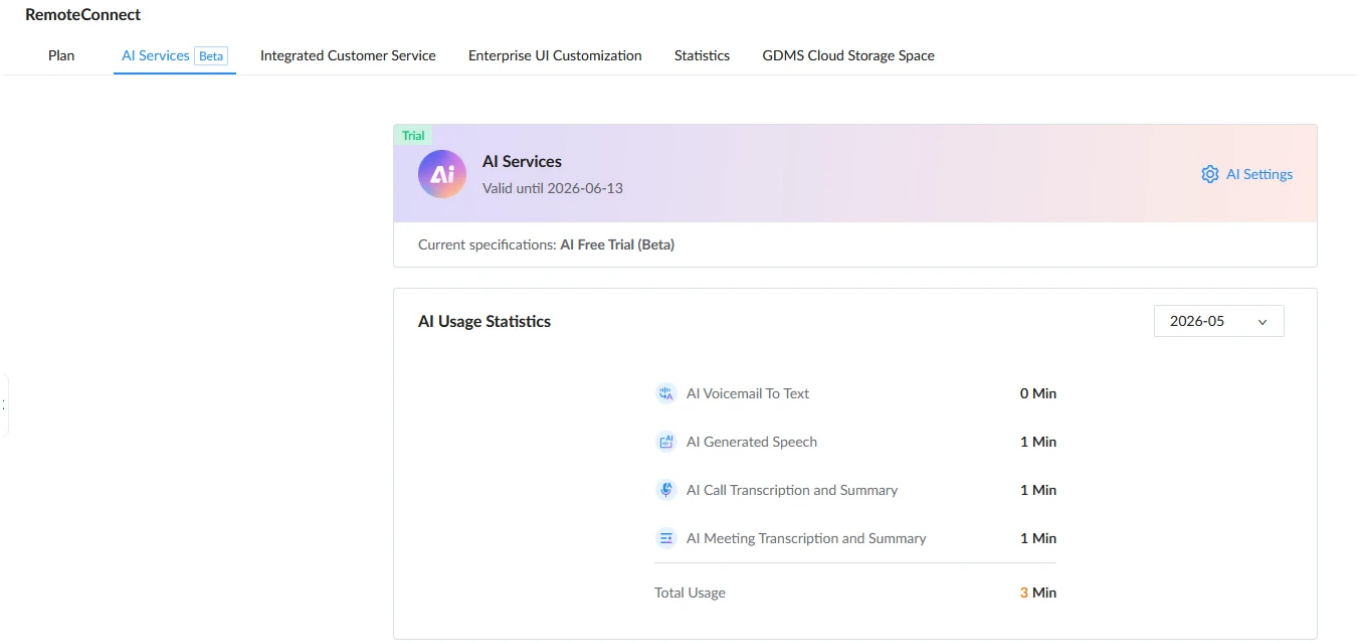
AI Services

This section displays AI related service status and usage information for the UCM. It provides visibility into the active AI plan, its validity period, and detailed usage statistics. Users can also jump to configure AI Settings from this page.

Supported AI features include:

- AI Voice Message to Text
- AI Generated Speech (Text-to-Speech)
- AI Call Transcription and Summary
- AI Conference Transcription and Summary

Usage statistics show monthly consumption per feature and total usage versus the available quota, helping administrators monitor AI resource usage.



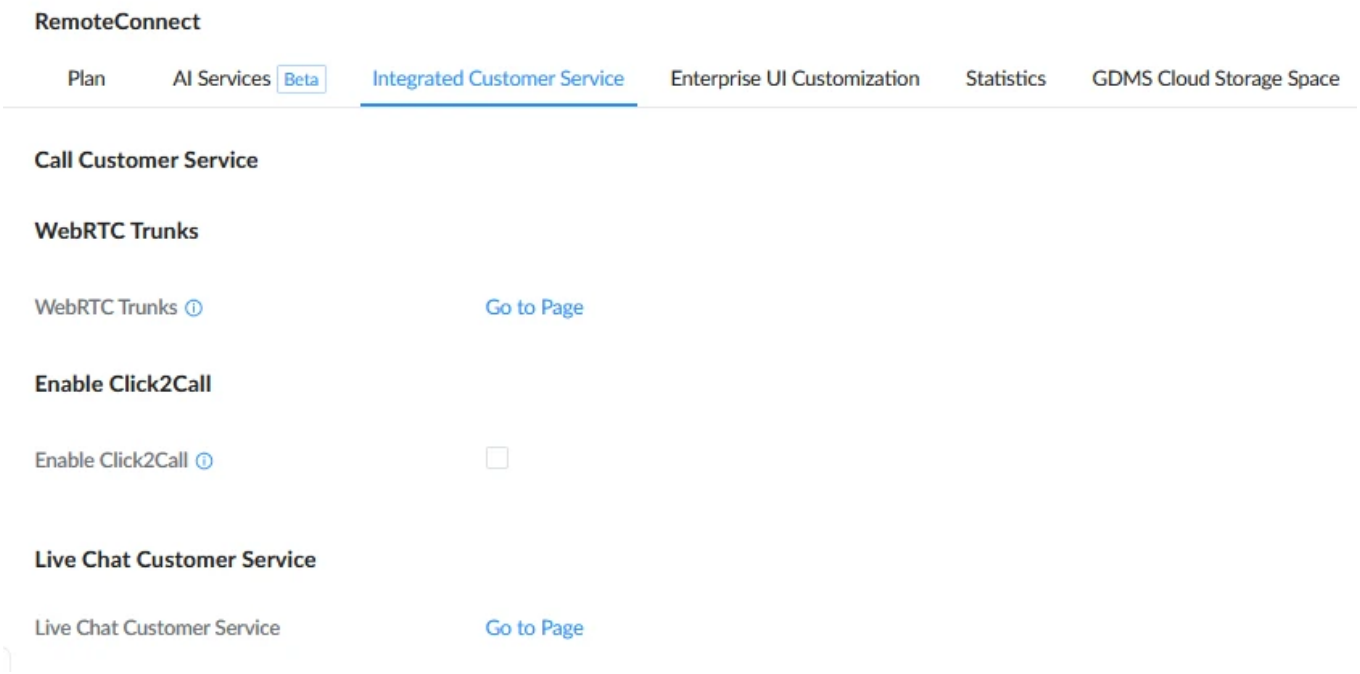
RemoteConnect AI Services Page

Integrated Customer Service

This section allows administrators to configure web-based customer service features that integrate communication tools into websites. Under the **Integrated Customer Service** tab, administrators can access options for WebRTC Trunks, Enable Click2Call, and Live Chat Customer Service.

Through this section, administrators can navigate directly to the configuration pages for WebRTC Trunks and Live Chat Customer Service to manage web-based customer interactions.

The Click2Call feature has been retired for new setups. However, users who had Click2Call enabled prior to this update will still see the configuration options in the Web GUI to ensure existing configurations remain functional without interruption.



RemoteConnect Integrated Customer Service Page

Enterprise UI Customization

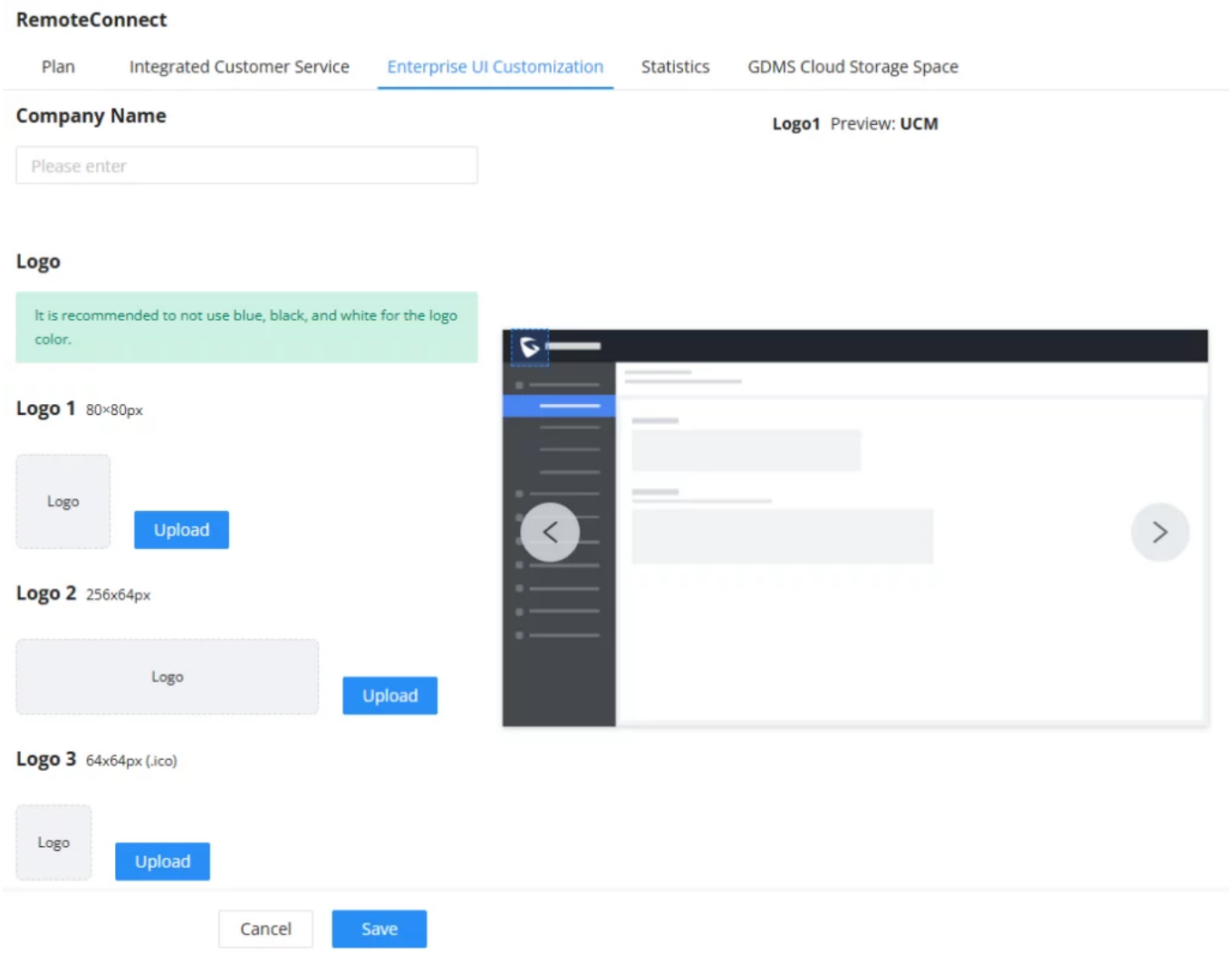
With a RemoteConnect plan, the Enterprise UI Customization page allows administrators to apply customized branding across the UCM and Wave interfaces. From this page, the company name can be configured and multiple logo images can be uploaded to replace the default branding in supported system interfaces.

The system supports different logo sizes and formats to ensure proper rendering in various locations as described below

- **Logo 1 (80x80px):** Replaces the Grandstream logo on the top left corner of the Wave Web interface and UCM management interface. The recommended format is PNG, and the maximum file size is 2 MB.
- **Logo 2 (256x64px):** Replaces the Grandstream banner on the top left corner of the login page and emails. The recommended format is PNG, and the maximum file size is 2 MB.
- **Logo 3 (64x64px):** Replaces Browser tab icon. The recommended format is .ico, and the maximum file size is 2 MB.

A built-in preview panel is provided on the right side of the page, allowing administrators to review how the configured company name and logos will appear in different interfaces.

To ensure optimal visibility and contrast with the system UI, it is recommended not to use blue, black, or white as the primary logo color.

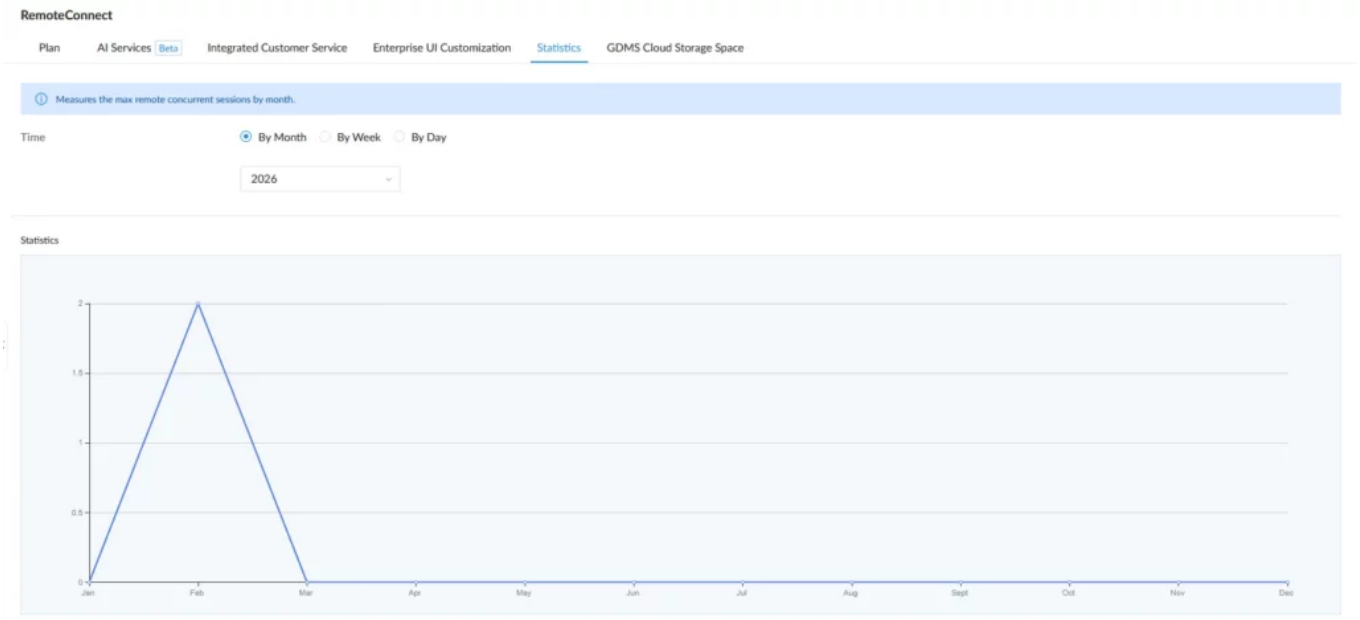


RemoteConnect Enterprise UI Customization Page

Statistics

The Statistics page provides an overview of RemoteConnect usage by displaying historical data on maximum concurrent remote sessions. This information helps administrators monitor RemoteConnect capacity usage and understand how remote access services are consumed over time.

Usage statistics can be viewed by month, week, or day. When viewing data by month, the system displays the highest number of concurrent remote sessions recorded during each month of the selected year.



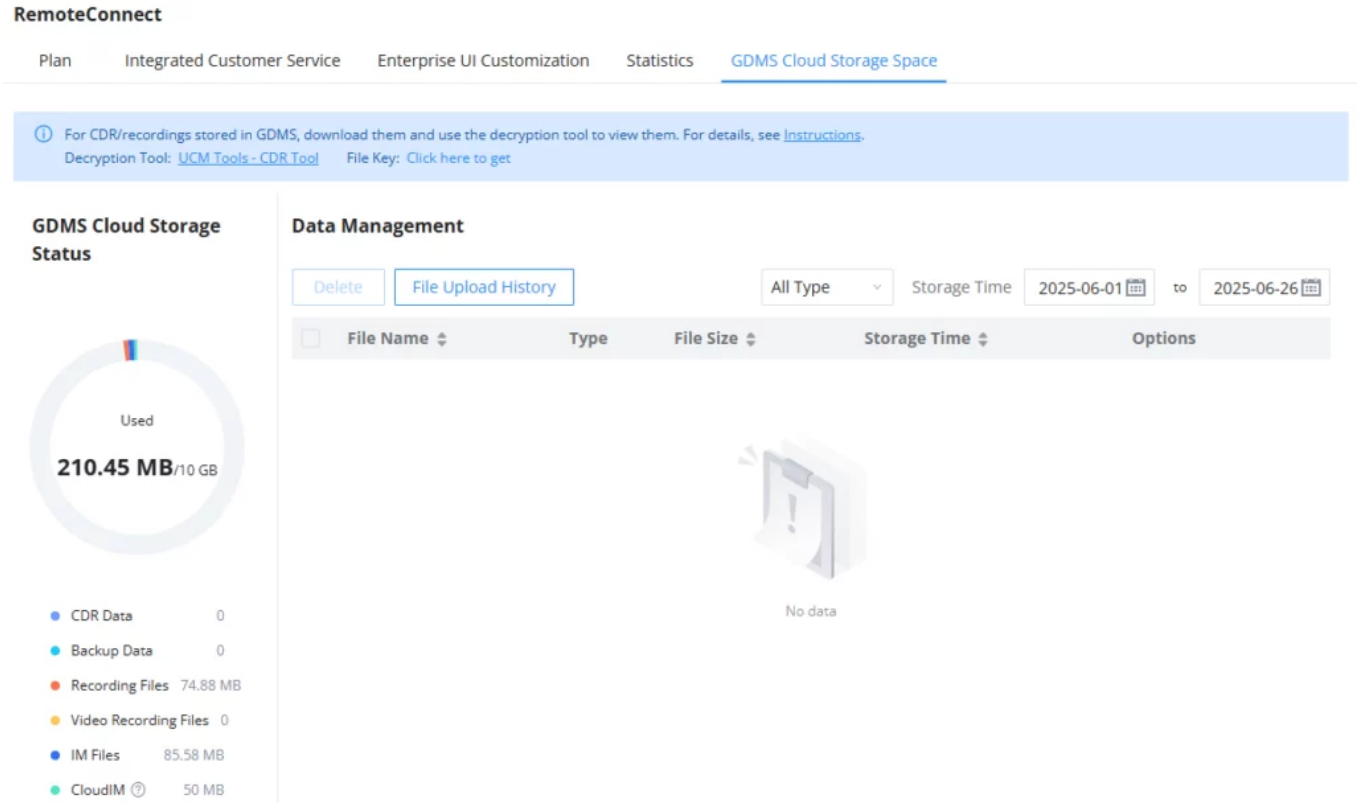
RemoteConnect Statistics Page

For more information, please visit the following website: https://ucmrc.gdms.cloud/home and check the UCM63XX RemoteConnect Guides.

GDMS Cloud Storage Space

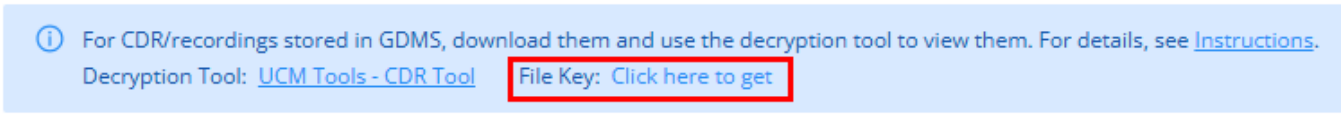
When the correspondent RemoteConnect plan is active, the user can access to a GDMS Cloud Storage Space to get an overview about how the storage space is being used. The data is represented in four categories of file types: CDR Data, Backup Data, Recording Files, and IM Files.

The user is also able to see the names of all the files stored in the GDMS Cloud Storage Space.



RemoteConnect GDMS Cloud Storage Space Page

On this page the user can obtain the file key by clicking on the following hyperlink.



To decrypt the files, please refer to the following guide: UCM6300/A Series IP PBX - CDR Tool Guide.

INTEGRATIONS

AI Settings (Beta)

The AI Settings page allows administrators to configure the usage of AI services provided through the RemoteConnect AI service. These features enable automatic speech recognition, transcription, translation, voice control, summarization, and text-to-speech processing for calls, conferences, recording files, and voice messages.

AI services are a purchaseable add-on and subject to usage limits defined by the active RemoteConnect plan. The administrator can enable each AI feature independently under four primary categories:

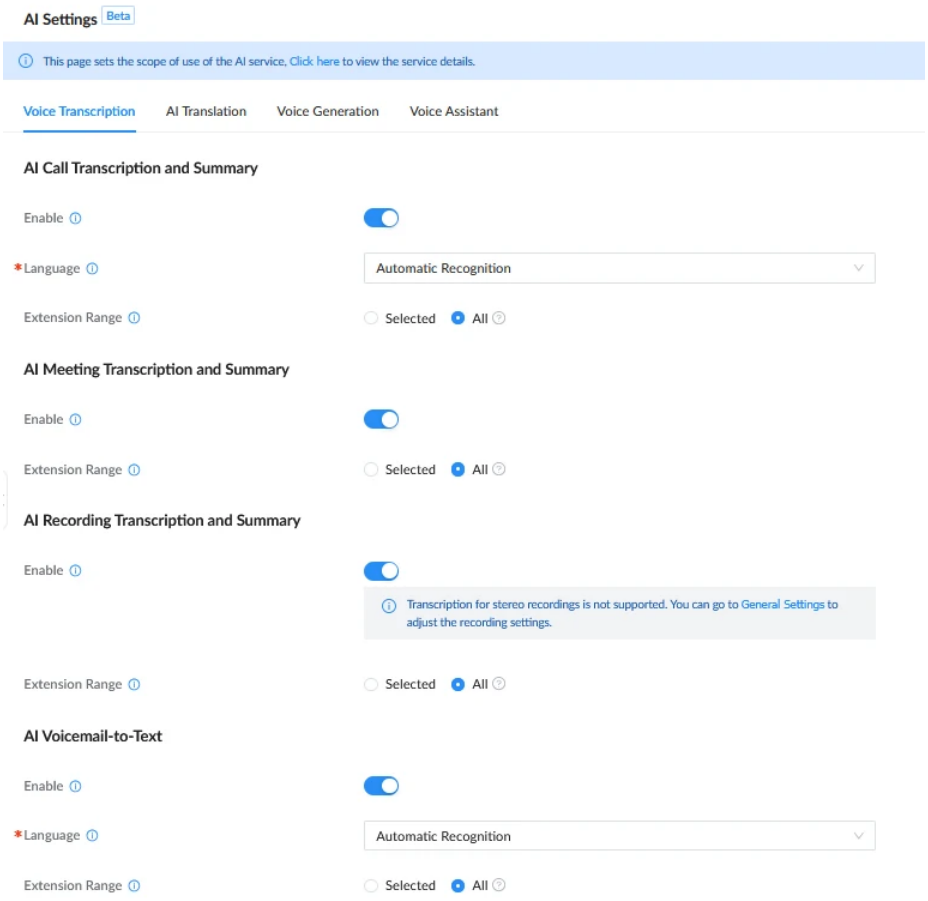
- **Voice Transcription**
- **AI Translation**
- **Voice Generation**
- **Voice Assistant**

For more information about configuring Voice Transcription and other AI functionalities, refer to GS AI Features Guide.

In order to use AI features on the UCM6300 series, an active **GS AI Free Trial** is required. Please note that applications for the GS AI Free Trial are currently closed and new trial applications can no longer be submitted at this time.

The following AI capabilities are supported on the UCM:

- **AI Call Transcription and Summary**
- **AI Meeting Transcription and Summary**
- **AI Recording Transcription and Summary**
- **AI Voicemail to Text**
- **AI Translation**
- **AI Generated Speech**
- **AI Voice Assistant**

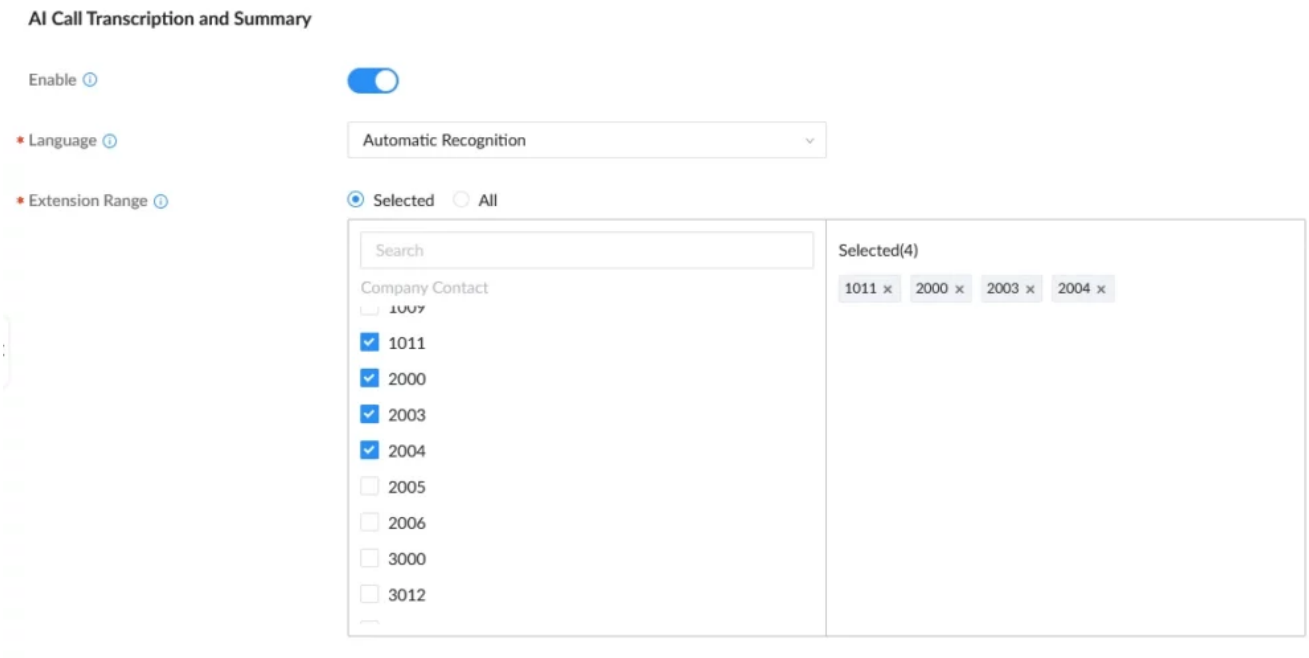


Voice Transcription

The **Voice Transcription** tab consolidates configuration for all speech-to-text features, including calls, meetings, media recording files, and voicemails.

AI Call Transcription and Summary

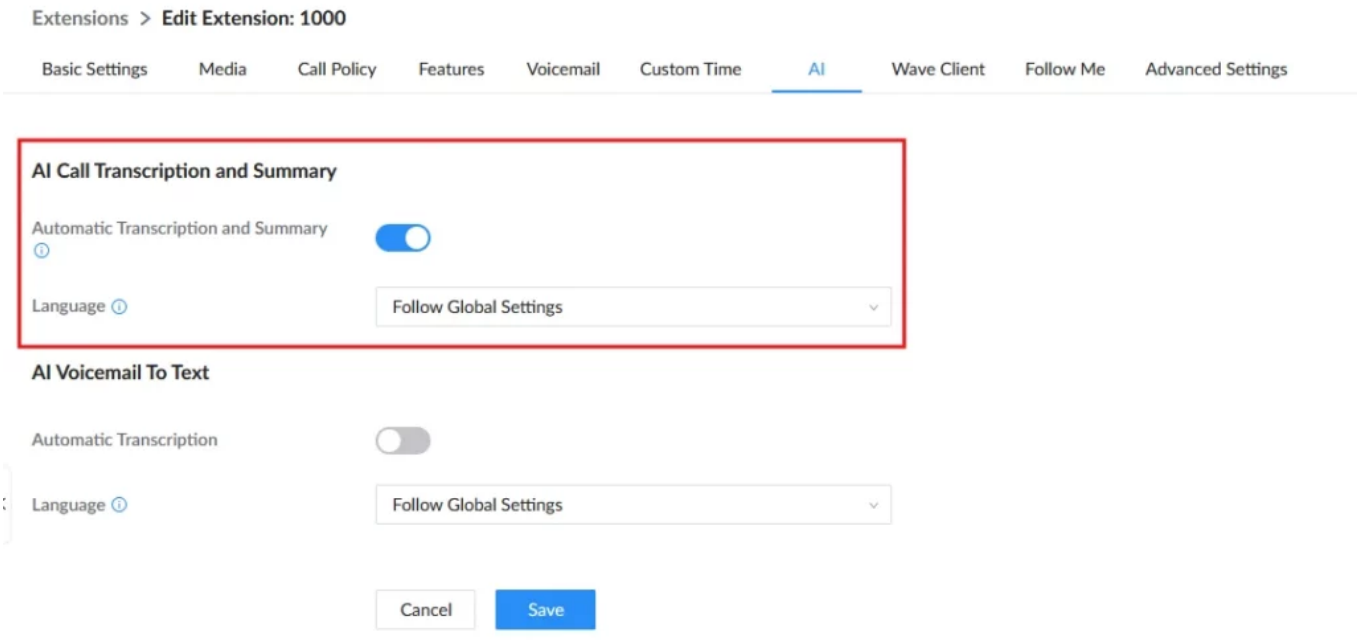
This feature enables AI-based transcription and summarization for one-to-one calls. When enabled globally, the administrator defines whether the feature applies to all extensions or only selected extensions. Only extensions included in this scope are eligible for call transcription and summarization.



AI Call Transcription and Summary General Setting

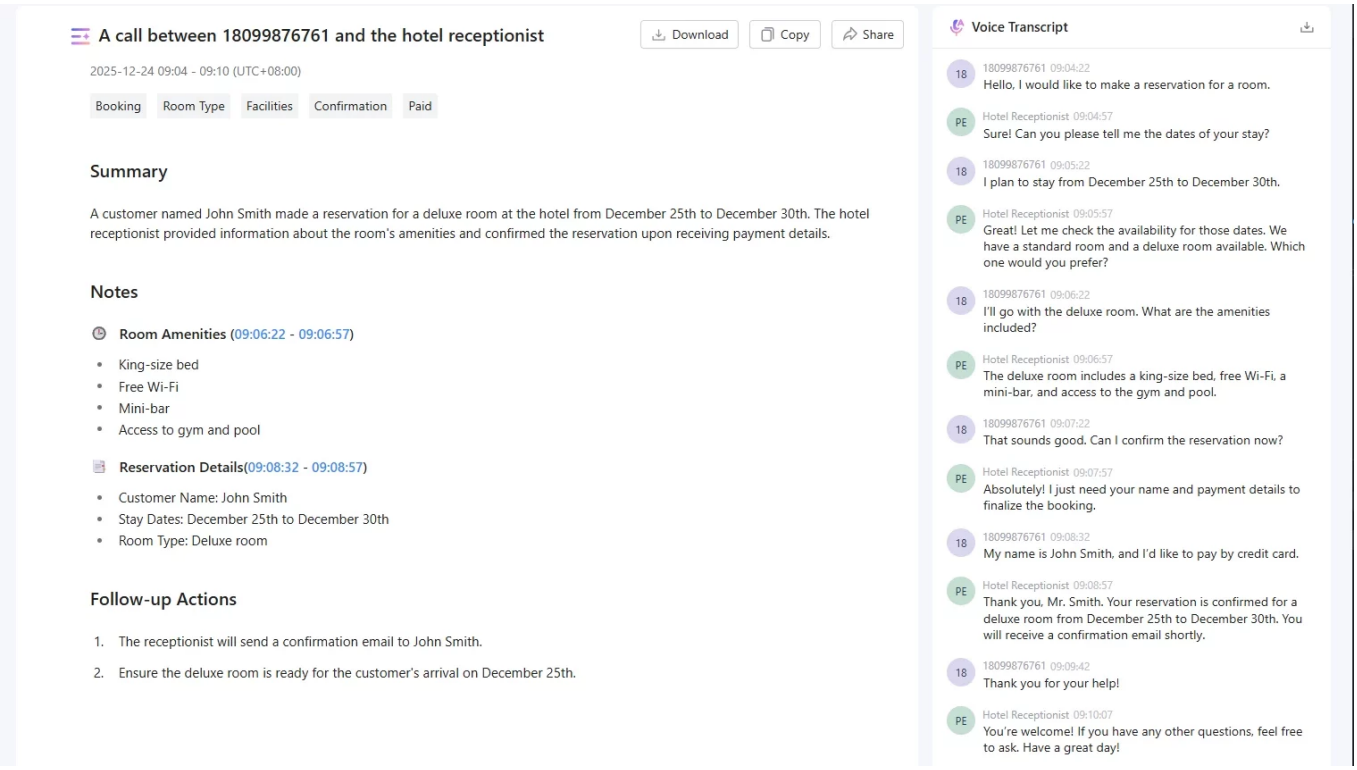
At the extension level, the Automatic Transcribing and Summarizing option determines whether calls for that extension are processed automatically. When enabled, all calls made or received by the extension are automatically transcribed and summarized.

The recognition language can be configured globally under **AI Settings (Beta)->Voice Transcription->AI Call Transcription and Summary** and followed by the extension, or explicitly set per extension.



Extension Automatic Call Transcription

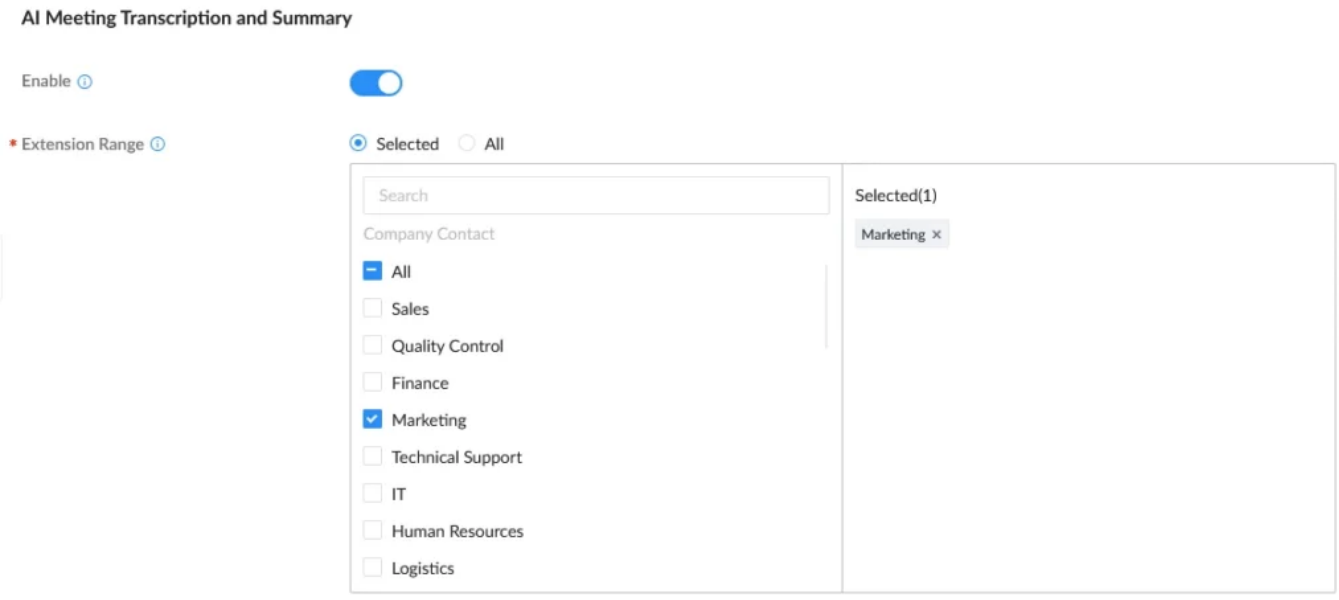
Generated transcripts and summaries can be viewed by users through the **Wave client**, as shown below.



Call Transcript on Wave

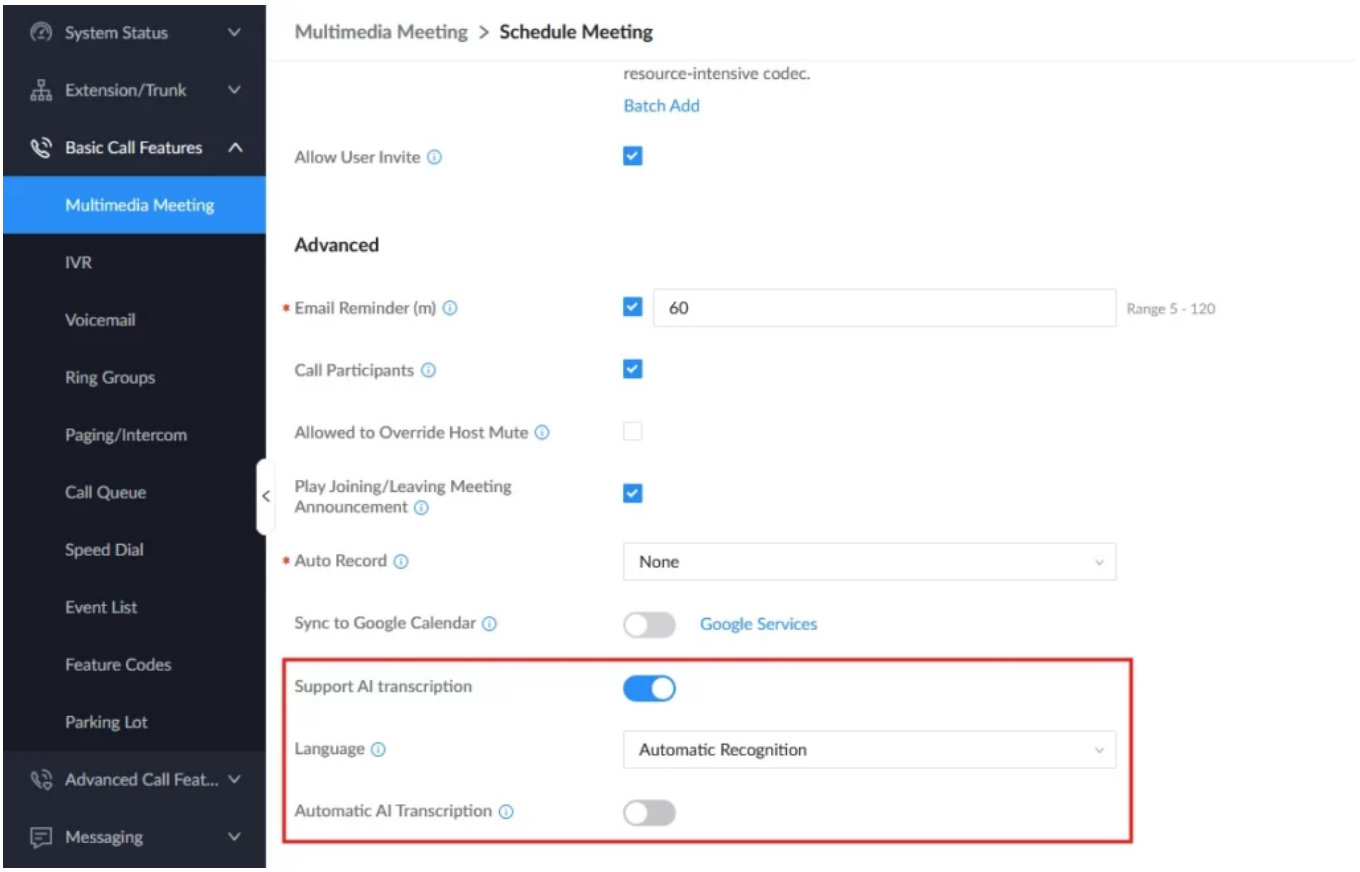
AI Meeting Transcription and Summary

This feature enables AI-based transcription and summarization for conference calls and meetings. When enabled, meeting audio is processed by the AI service and a transcript and summary are generated after the meeting ends. The administrator can define whether the feature applies to all extensions or only selected extensions participating in conferences.



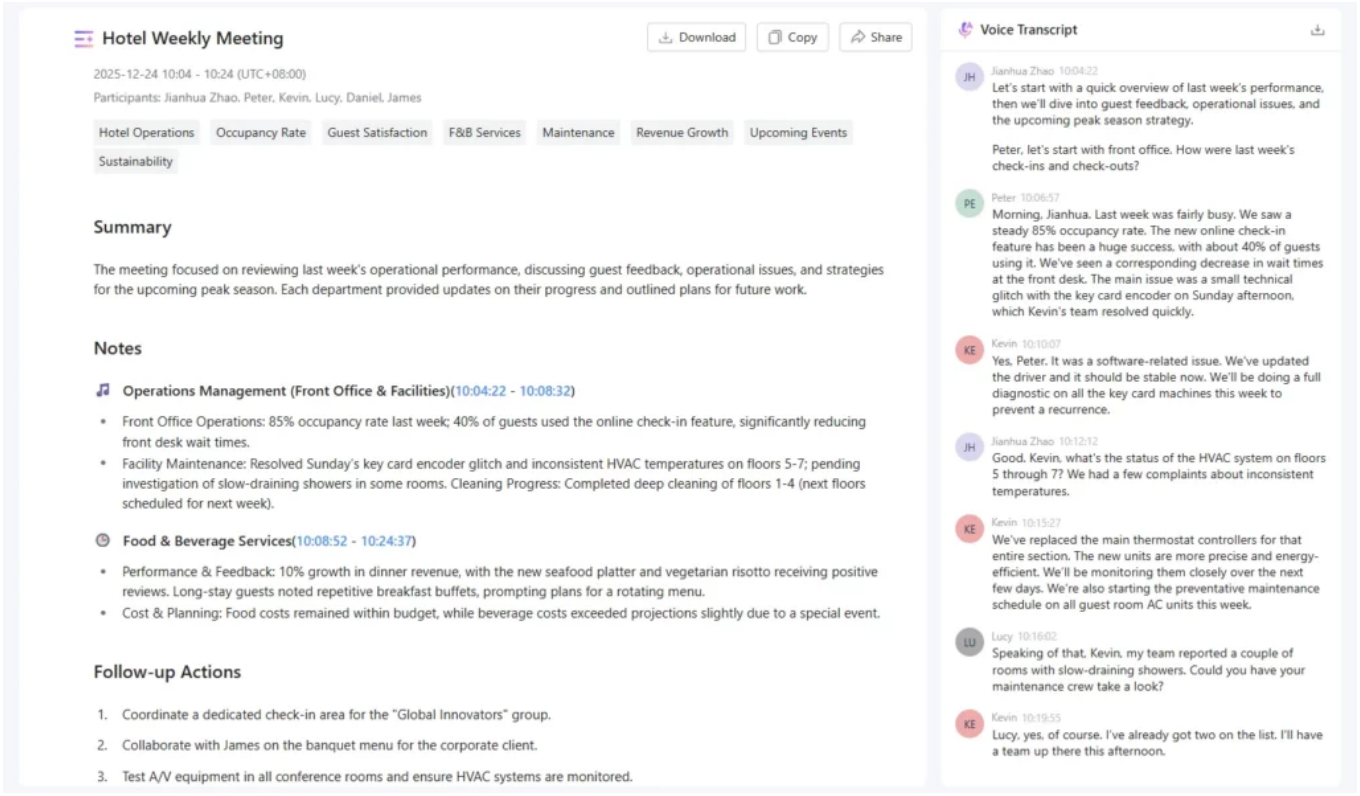
AI Meeting Transcription and Summary Setting

When scheduling a meeting, the meeting organizer can explicitly choose whether the conference will be transcribed or not. This selection applies only to the scheduled meeting and does not affect global or extension-level AI settings.



AI Transcription Support for Scheduled Meeting

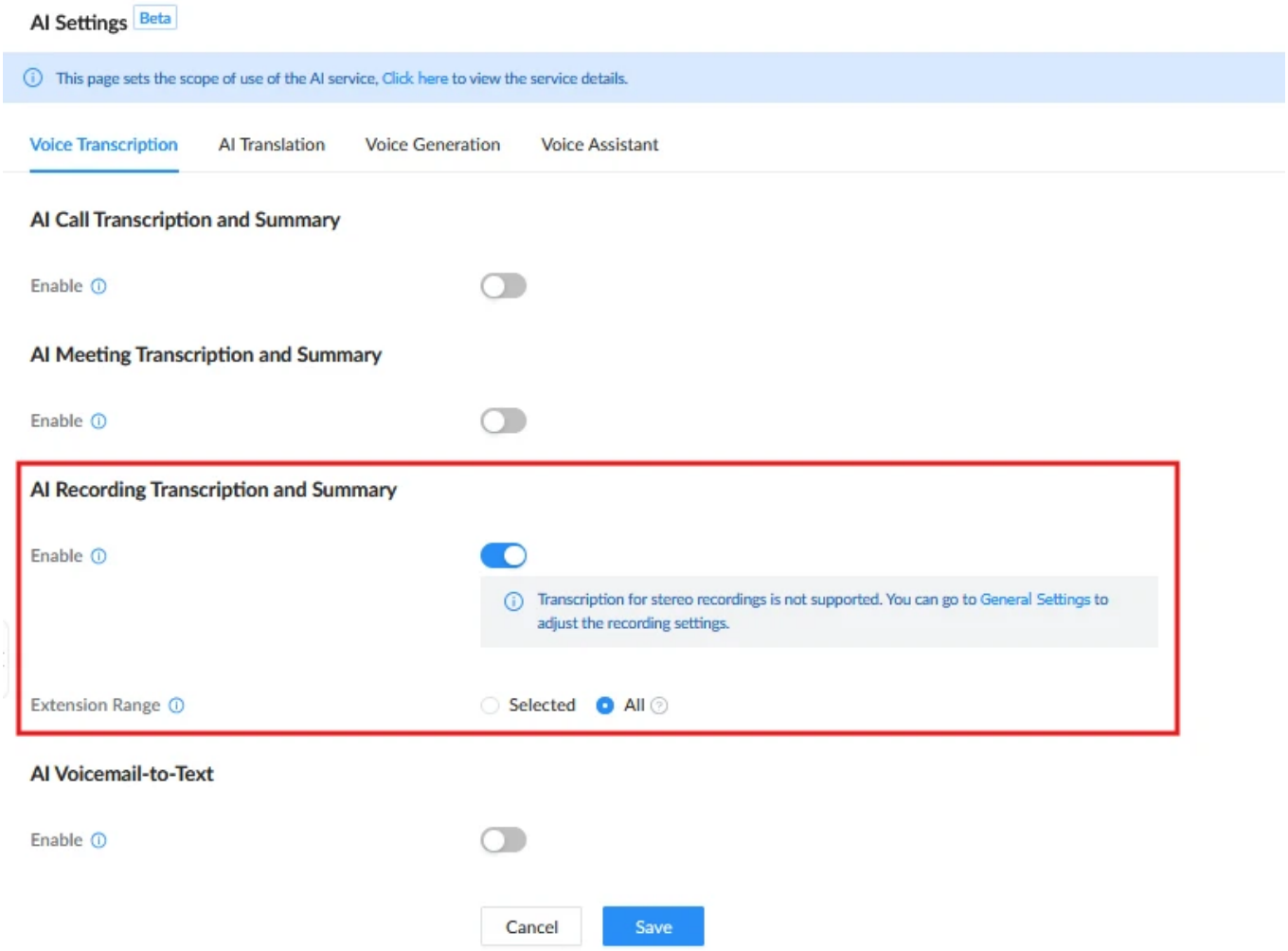
Meeting transcripts and summaries can be accessed by participants through supported Wave clients and user portals.



Meeting Transcript on Wave

AI Recording Transcription and Summary

This feature allows audio and video recording files stored on the UCM to be transcribed and summarized using AI. When enabled globally, the administrator specifies whether the scope applies to all extensions or selected extensions.

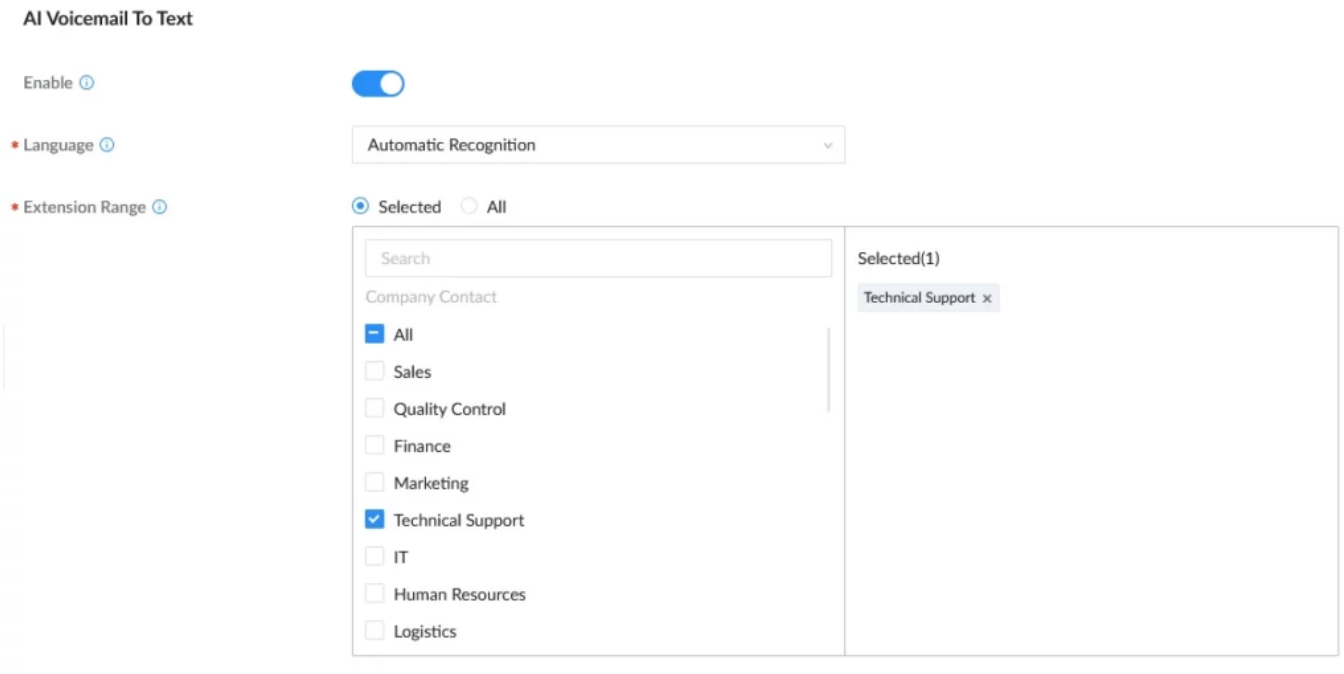


Transcription for stereo recordings is not currently supported. Administrators can adjust recording audio channel modes under **PBX Settings->General Settings**.

Once transcribed, users can review recording transcripts with interactive synchronization. Clicking a text segment automatically seeks media playback progress to that timestamp, and active media playback dynamically highlights the corresponding transcript text.

AI Voicemail to Text

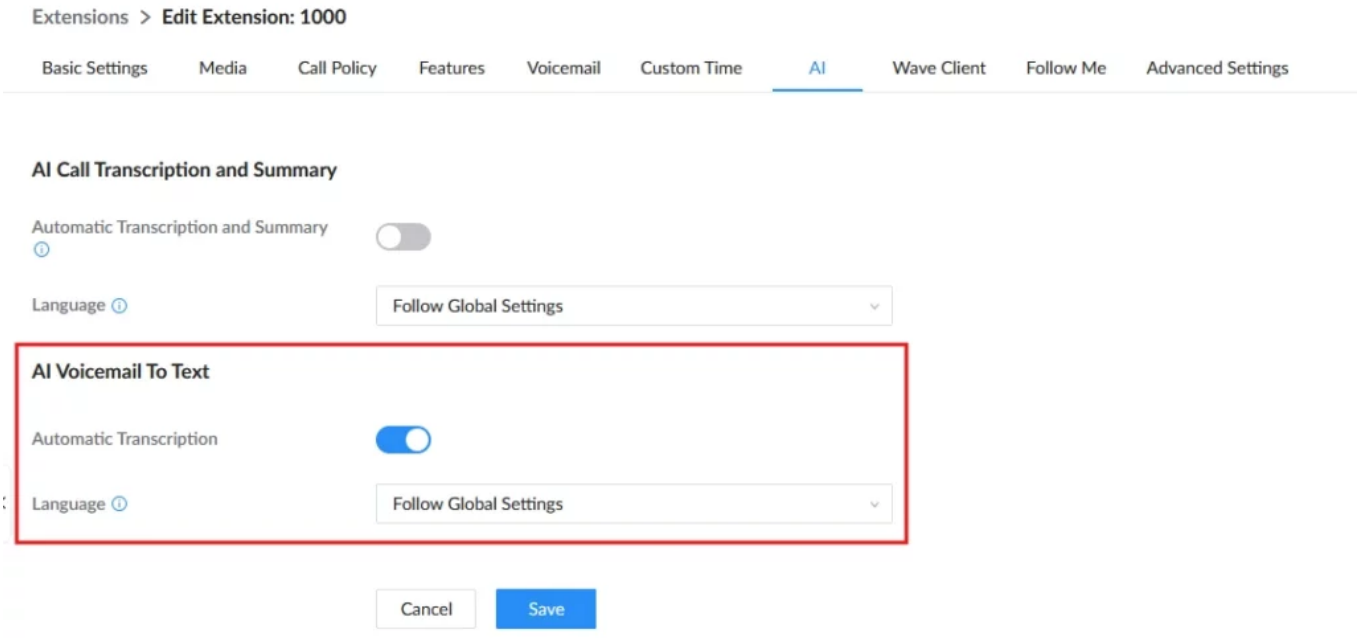
This feature converts voice messages (voicemail) into text using AI speech recognition. When enabled globally, voice messages left for eligible extensions can be transcribed.



AI Voice Message to Text General Setting

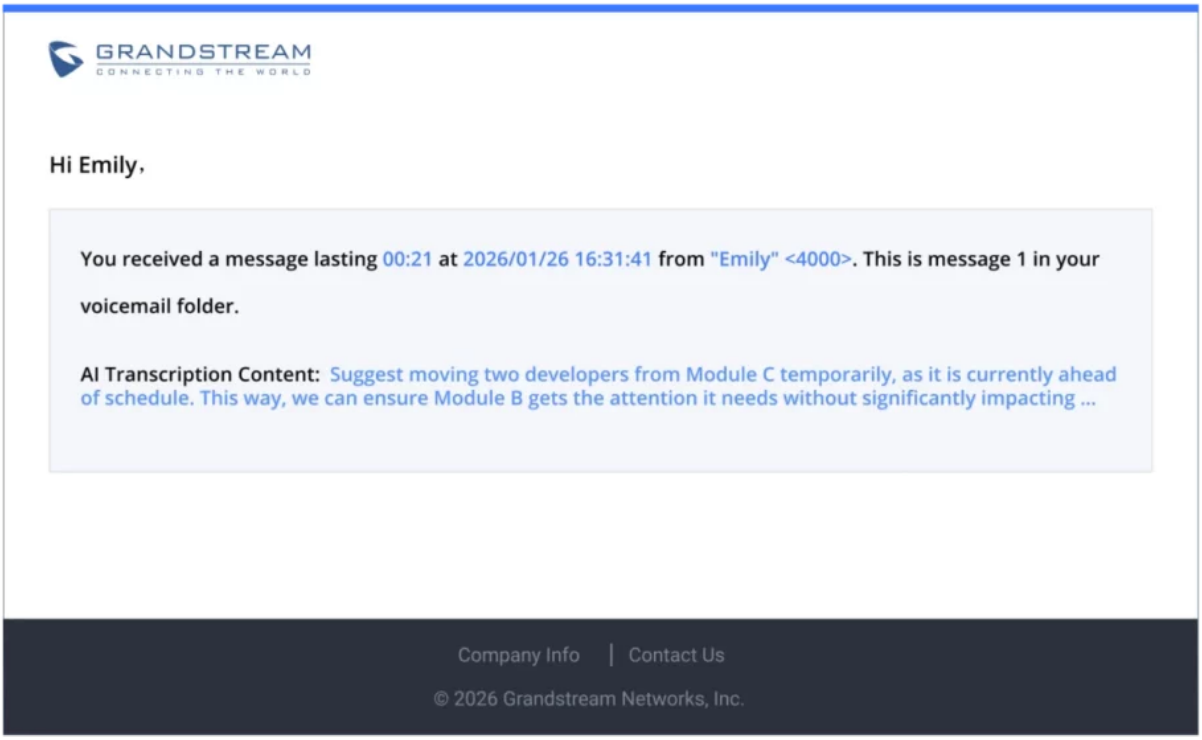
At the extension level, the Automatic Transcription option determines whether voice messages for that extension are automatically converted into text.

The recognition language can follow the global configuration or be explicitly specified for the extension.

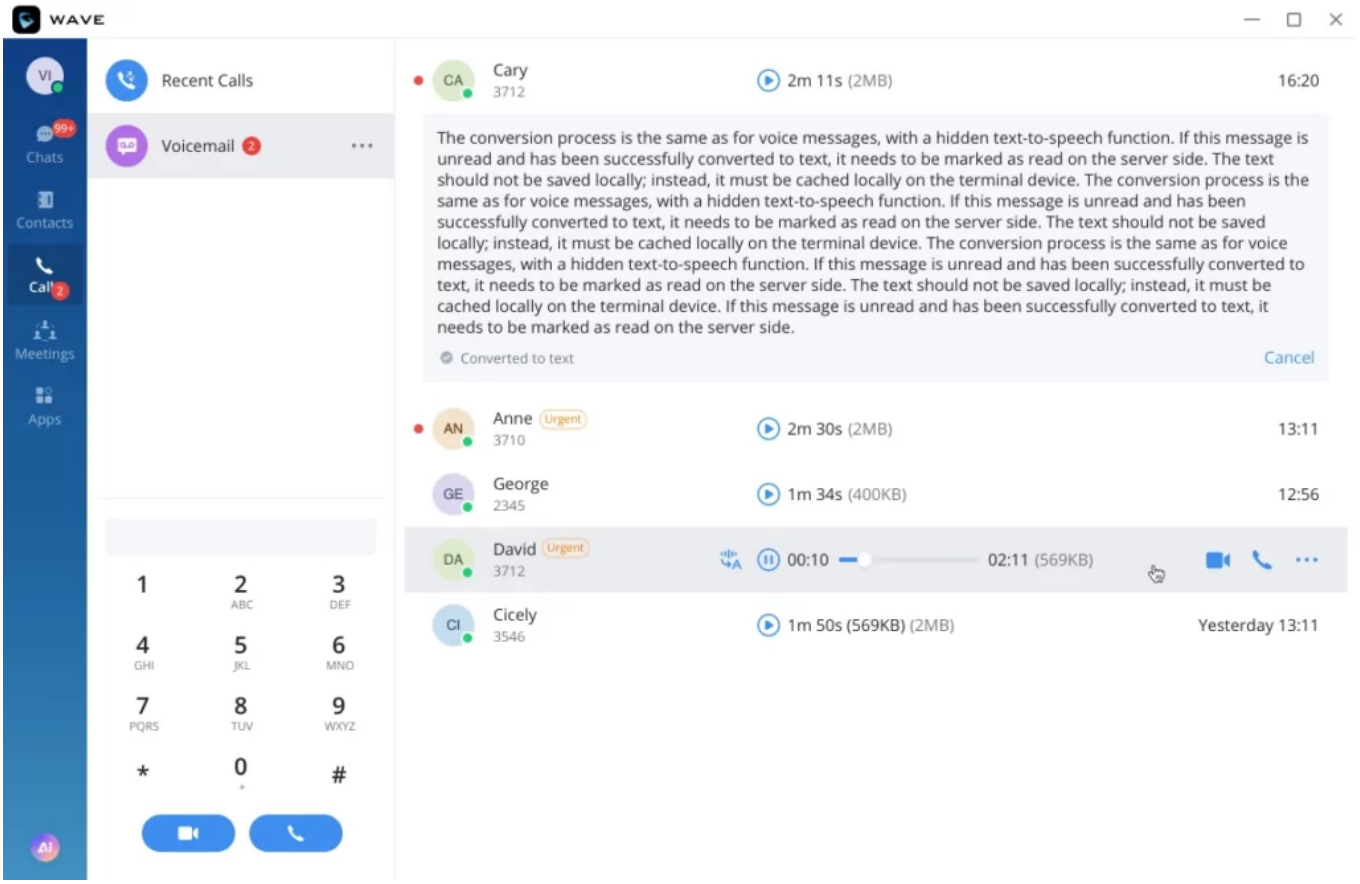


Extension Automatic Voicemail Transcription

Transcribed voicemail content can be viewed in supported Wave clients, through the User Portal (where accessing or playing the voicemail marks it as read), and may also be included in voicemail email notifications depending on system configuration.



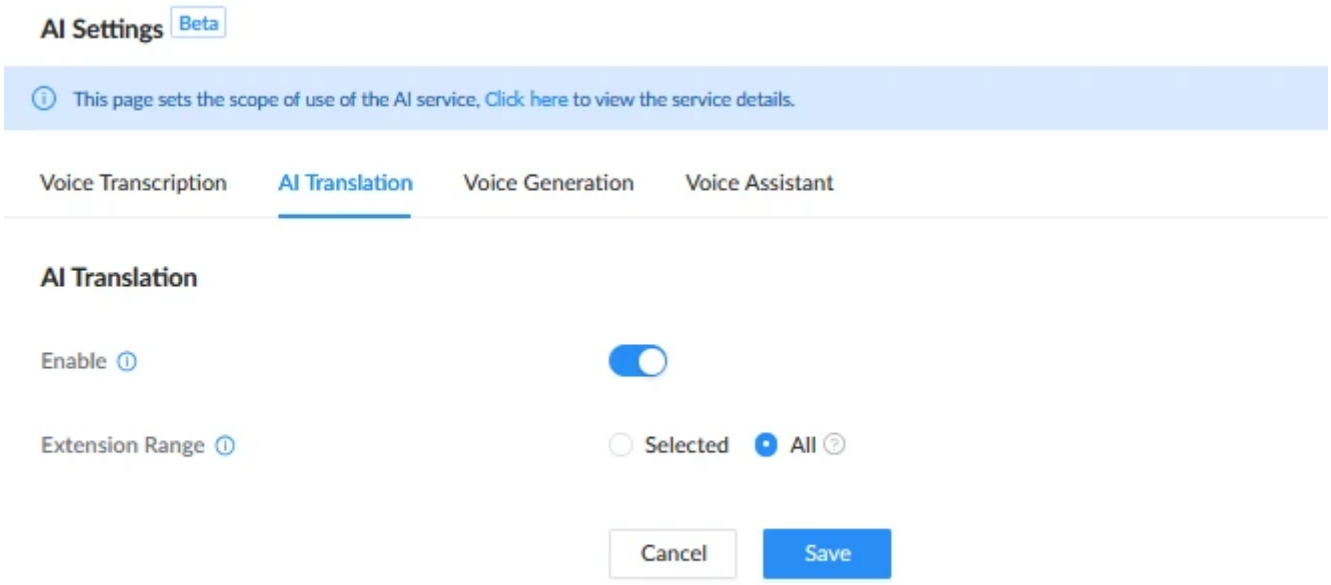
Voicemail Transcript Email



Voicemail Transcript on Wave

AI Translation

The **AI Translation** feature provides real-time translation capabilities for call transcripts, conference transcripts, and chat messages across Wave endpoints. When enabled globally, the administrator defines the extension scope (All Extensions or Selected Extensions) authorized to use AI Translation.

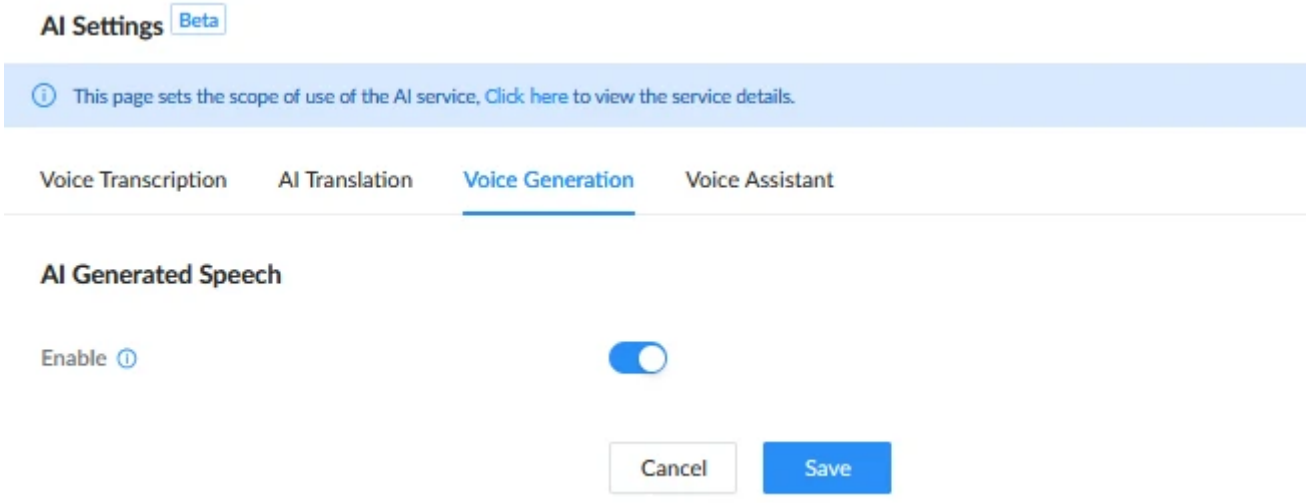


Once granted permission, users can translate live speech-to-text transcripts during active calls/meetings or translate instant chat messages on-demand.

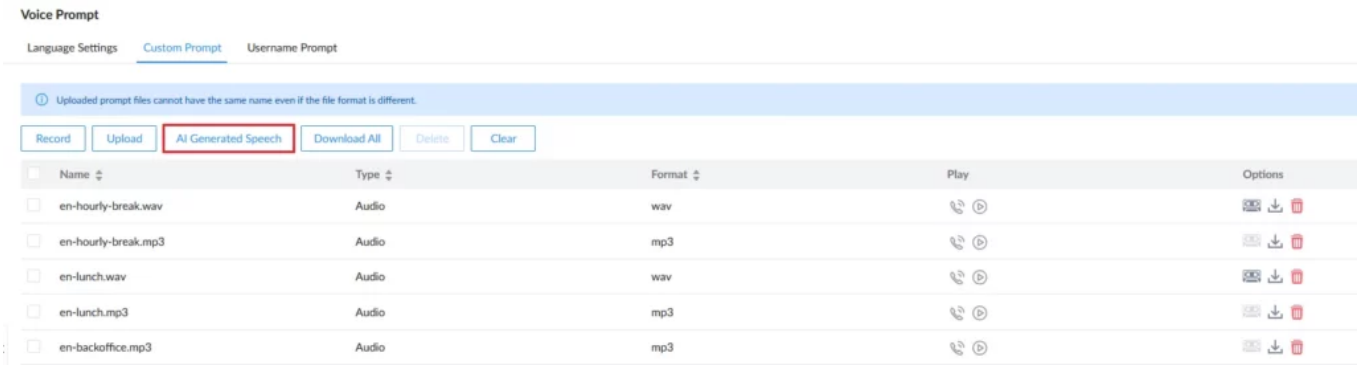
AI Voice Generation

The **Voice Generation** tab manages AI Generated Speech capabilities. This feature provides text-to-speech (TTS) processing powered by the AI service, allowing administrators to generate voice prompt audio directly from text. This feature is primarily used for IVR prompts, queue announcements, and other system voice prompts, eliminating the need to manually record or upload audio files.

Before using this feature, AI Generated Speech must be enabled on the **Voice Generation** tab under **AI Settings**. Once enabled, administrators can generate AI-based voice prompts from multiple entry points in the system.

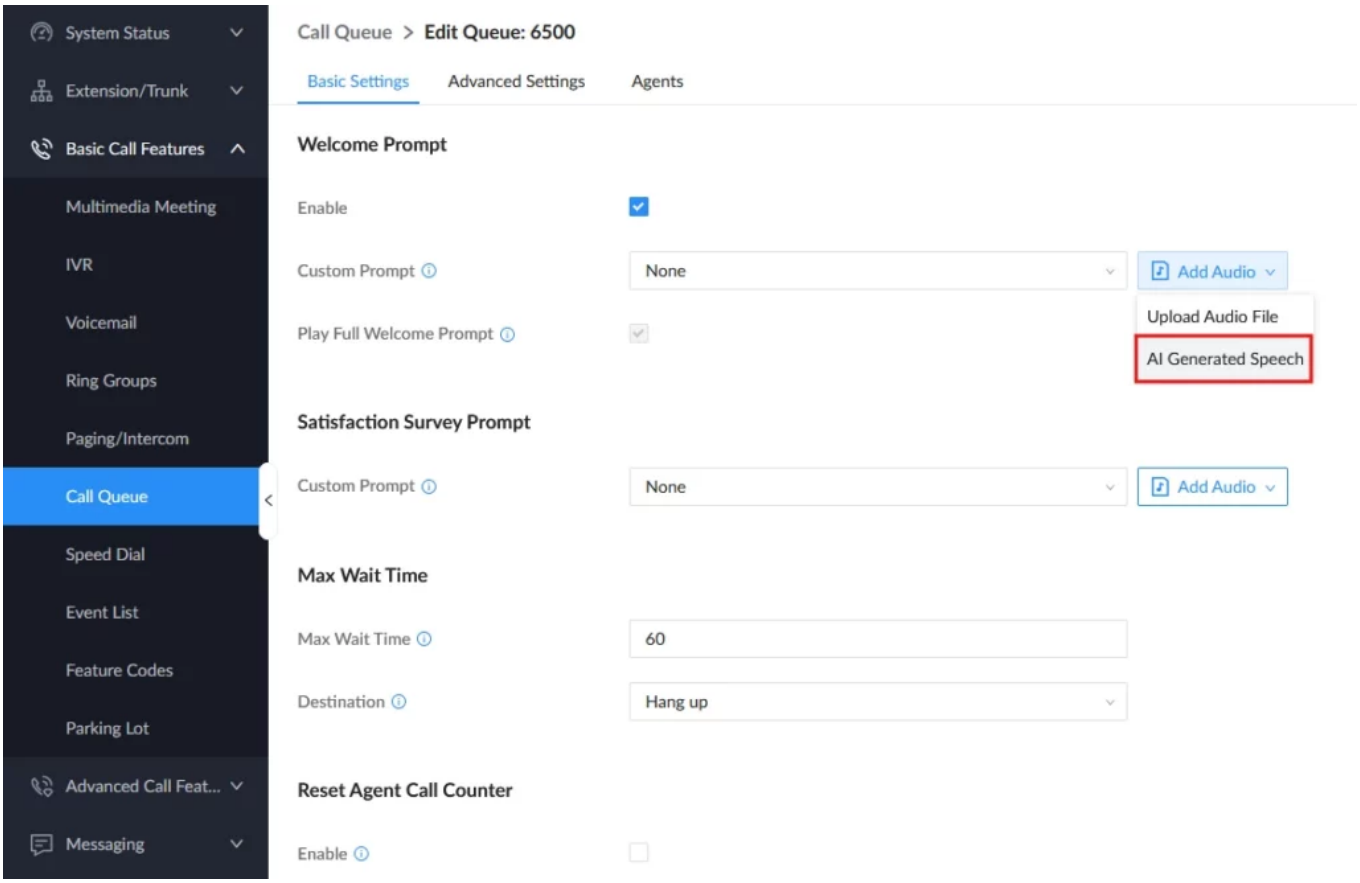


The feature can be accessed from **PBX Settings->Voice Prompt->Custom Prompt** by clicking the AI Generated Speech button, which opens the AI generation window.



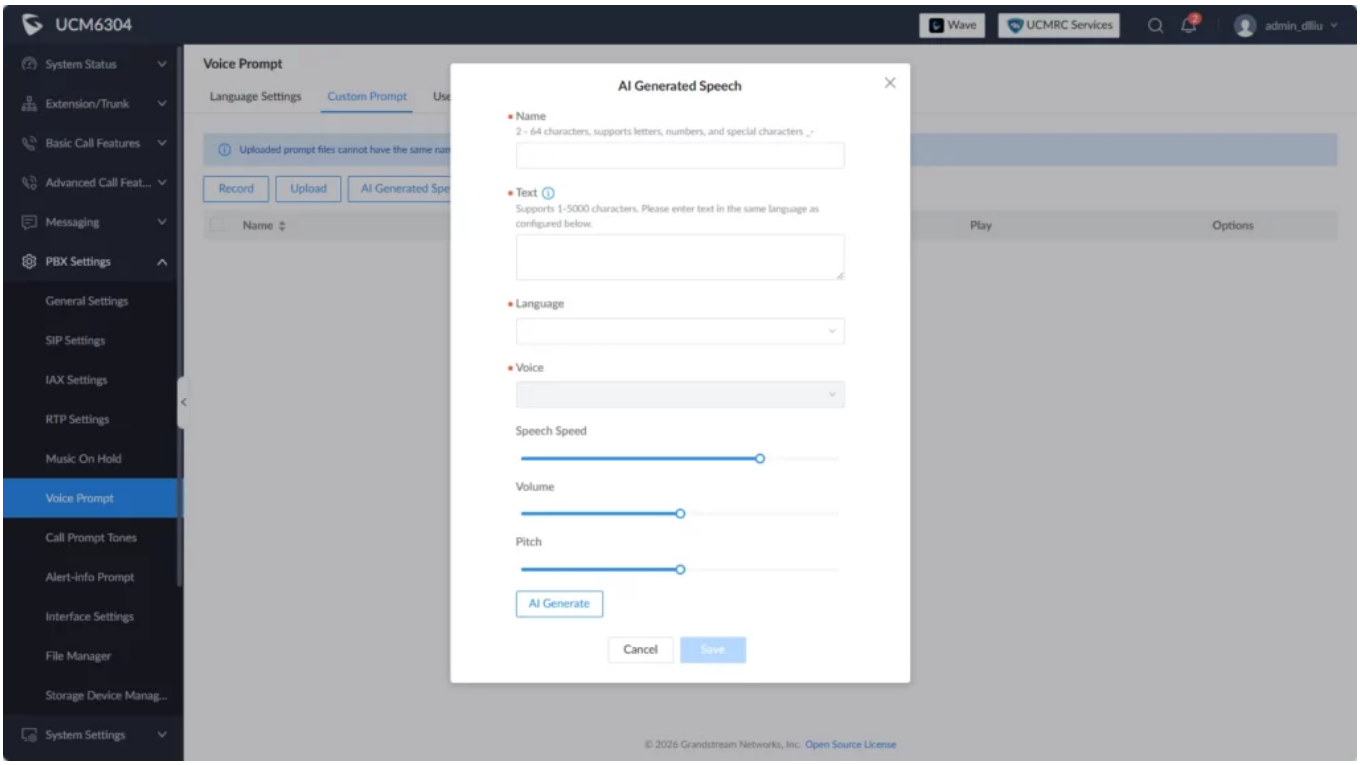
AI Generated Speech Option in Custom Prompt

It is also accessible while configuring features that require voice prompts (such as call queues). In those cases, selecting AI Generated Speech from the prompt selection dropdown redirects the user to the same AI generation window used in the Voice Prompt page.



Call Queue AI Generated Prompt Option

When creating an AI-generated voice prompt, the following settings are available:



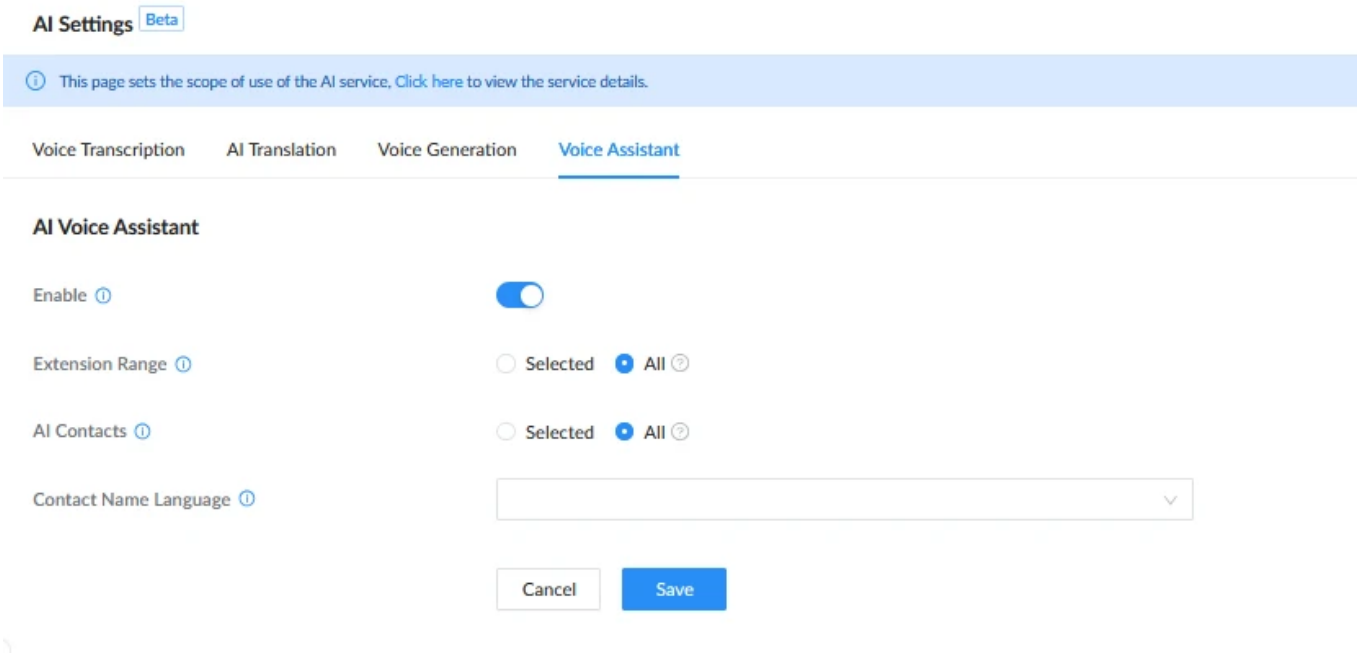
AI Generated Speech Configuration Options

Name	Defines the name of the generated voice prompt. This name is used to identify the prompt in the system and must be unique. The field supports 2-64 characters, including letters, numbers, and special characters.
Text	Specifies the text content that will be converted into speech. The text length supports up to 5,000 characters.
Language	Specifies the language used for text-to-speech processing.
Voice	Selects the voice profile used to generate the speech. Different voice options may be available depending on the selected language.A preview option is provided, allowing administrators to listen to the voice style before generating the prompt.
Speech Speed	Controls the playback speed of the generated speech. The speed can be adjusted from slower to faster relative to normal speaking speed.
Volume	Adjusts the output volume level of the generated audio. The value can be set from 0 to 100 to accommodate different playback environments.
Pitch	Controls the pitch of the generated voice. Higher values produce a higher-frequency voice, while lower values produce a deeper tone. The pitch range can be set from 0 to 100.

After configuring the parameters, clicking AI Generate produces the audio preview. Once satisfied, the generated prompt can be saved and reused like any other system voice prompt.

AI Voice Assistant

The **Voice Assistant** tab allows administrators to configure natural voice command controls for endpoints. When enabled globally, extension users within the configured scope can issue spoken commands to perform actions such as making calls, transferring calls, initiating meetings, or sending messages.



Administrators can configure the following settings under **AI Settings->Voice Assistant**.

- **Enable:** Toggles the AI Voice Assistant service on or off.
- **Extension Range:** Controls which extensions are permitted to speak commands to the AI Voice Assistant (e.g., Only allow Extensions 1000-1005 to use the Voice Assistant feature).
- **AI Contacts:** Controls which contacts/directory entries the AI can look up when executing a voice command (e.g., Allow to search the entire contacts when an extension user asks "Call John").
- **Contact Name Language:** Defines the language rules used to recognize and match spoken names in the directory.

API Configuration

The UCM630X supports third party billing interface API for external billing software to access CDR and call recordings on the PBX. The API uses HTTPS to request the CDR data and call recording data matching given parameters as configured on the third-party application.

API Configuration Parameters

Before accessing the API, the administrators need enable API and configure the access/authentication information on the UCM630X first under **Integrations→API Configuration**. The API configuration parameters are listed in the tables below.

You can create multiple users with different login credentials to access to the HTTPS API.

The old version of the API interface only supports cdrapi, recapi and pmsapi functions, and will be removed, please use the new HTTPS API instead.

Username	The username for API Authentication.
Password	The password for API Authentication.
IP Address Allowlist	If enabled, only addresses in the list below will be allowed access.If disabled, geo-ip access control will be used instead.

API Interface Permissions	Select the API interface permissions. The permissions which can be selected with their respective parameters are listed below.Call ControlCDRContactsDevice ManagementExtensionsExtension GroupFilesInbound RoutesIVRMultimedia MeetingOutbound RulesPaging/IntercomPIN GroupsPMSQueuesRecordingsStatusTrunkUser Information

HTTPS API Settings (Old)	
Basic Settings	
Enable	Enable/Disable API. The default setting is disabled.
TLS Bind Address	Configure the IP address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 8443. The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses. The default setting is 0.0.0.0:8443.
Username	Configure the username for TLS authentication.
Password	Configure the password for TLS authentication.
Permitted IP(s)	Specify a list of IP addresses permitted to use the API. This creates an API-specific access control list. Multiple entries are allowed. For example, "192.168.40.3/255.255.255.255" denies access from all IP addresses except 192.168.40.3. By default, this is blank, which indicates that no IP addresses are allowed to use this API.
Other Settings	
TLS Private Key	Upload TLS private key. The size of the key file must be under 2MB. This file will be renamed as 'private.pem' automatically.
TLS Cert	Upload TLS cert. The size of the certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection. This file will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.
API Module	
CDR API	Enable/disable CDR API module.
REC API	Enable/disable REC API module.
PMS API	Enable/disable PMS API module.

Configuration Parameters (Old)

For more details on CDR API (Access to Call Detail Records), REC API (Access to Call Recording Files) and PMS API, please refer the document in the link here:

- https://documentation.grandstream.com/knowledge-base/cdr-rec-api/

- https://documentation.grandstream.com/knowledge-base/cdr-rec-api/

- PMS API

API Queries Supported

The new API supports now new queries listed below which will accomplish certain requests and get data about different modules on UCM630X.

getSystemStatus	addInboundRoute	listPaginggroup
getSystemGeneralStatus	getInboundRoute	addPaginggroup
listAccount	updateInboundRoute	getPaginggroup

getSIPAccount	deleteInboundRoute	updatePaginggroup
updateSIPAccount	playPromptByOrg	deletePaginggroup
listVoIPTrunk	listBridgedChannels	MulticastPaging
addSIPTrunk	listUnBridgedChannels	MulticastPagingHangup
getSIPTrunk	Hangup	listIVR
updateSIPTrunk	Callbarge	addIVR
deleteSIPTrunk	listQueue	getIVR
listOutboundRoute	getQueue	updateIVR
addOutboundRoute	updateQueue	deleteIVR
getOutboundRoute	addQueue	cdrapi
updateOutboundRoute	deleteQueue	recapi
deleteOutboundRoute	loginLogoffQueueAgent	pmsapi
listInboundRoute	pauseUnpauseQueueAgent	queueapi
mute	Unmute	hold
unhold	dialExtension	dialOutbound
callTransfer	transferNumberInbound	transferNumberOutbound
dialIVR	dialIVROutbound	dialQueue
dialRinggroup	dialOutboundTwo	listUser
getUser	updateUser	listExtensionGroup
listPinSets	refuseCall	acceptCall
applyChanges	addAnalogTrunk	getAnalogTrunk
listAnalogTrunk	updateAnalogTrunk	deleteAnalogTrunk
addSLATrunk	updateSLATrunk	deleteDigitalTrunk
addDigitalTrunk	getDigitalTrunk	listDigitalTrunk
updateDigitalTrunk	listDepartment	addContact
updateContact	deleteContact	

CDR Real-time Output Settings	
Enable	Enables real-time CDR output module. This module connects to selected IP addresses and ports and posts CDR strings as soon as it is available.
Server Address	CDR server IP address
Port	CDR server IP port
Upload Prompts User Configuration	
Username	Username used to upload prompts.
Password	Password used to upload prompts.

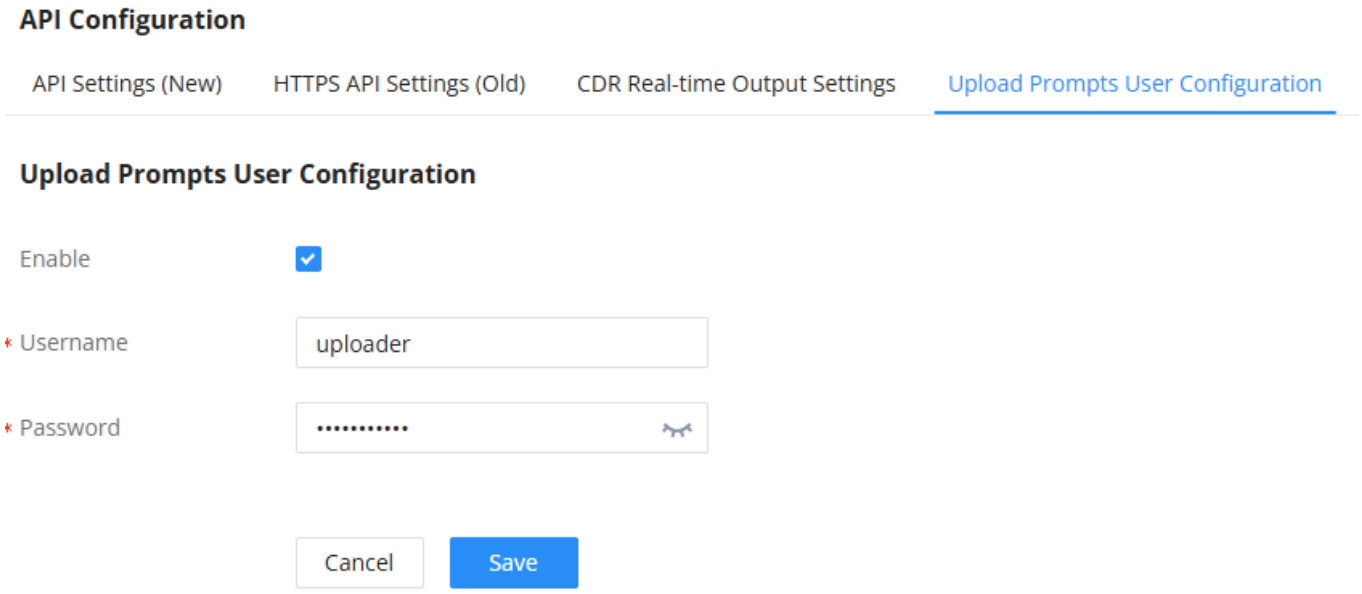
Upload Voice Prompt via API

Customers now can use the "Upload Prompts User Configuration" to upload/replace voice prompt files as an alternative method to the manual upload method on UCM **PBX Settings→ Voice Prompt→ Custom Prompt.**

The workflow of the prompt file upload goes as:

An HTTP/HTTPS request is sent to the UCM to upload/replace a voice prompt file, the request should include authentication details to the UCM and the name of the file to be uploaded. Then the UCM will contact an FTP server that should be hosted on the same IP address of the HTTP/HTTPS requester and download the prompt file from the FTP server.
The steps and conditions to upload the voice prompt via API are listed below:

1. Configure the prompt User under **Integrations → API Configuration → Upload Prompts User Configuration.** By default, the username and password for voice prompt user are "Username: uploader; Password: uploader123".



Upload Prompt User Configuration

2. Hash the password of the user configured to an MD5 Encryption format.
3. Set the permission on the FTP server to Anonymous on the local computer hosting the FTP server and make sure that the default FTP port 21 is used.
4. Send an HTTP/HTTPS command to trigger the Prompt file upload on the UCM. If UCM's HTTP server is set to HTTPS, the example of the request sent to the UCM is:

https://192.168.124.89:8089/cgi?action=uploadprompt&username=uploader&password=9191a6394c21b3aabd779213c

If UCM's HTTP server is set to HTTP, the example of the request sent to the UCM is:

https://192.168.124.89:8089/cgi?action=uploadprompt&username=uploader&password=9191a6394c21b3aabd779213c

If the File name on the HTTP/HTTPS request exists already on the UCM's Custom voice prompts list the existing file will be overwritten by the new file downloaded from the FTP server.

For more details on CDR API (Access to Call Detail Records) and REC API (Access to Call Recording Files), please refer the document in the link here:

AMI (Asterisk Manager Interface)

The UCM630X supports AMI (Asterisk Manager Interface) with restricted access. AMI allows a client program to connect to an Asterisk instance commands or read events over a TCP/IP stream. It is particularly useful when the system admin tries to track the state of a telephony client inside Asterisk.

User could configure AMI parameters on **Integrations** > **AMI**. For details on how to use AMI on UCM630X, please refer to the following AMI guide:

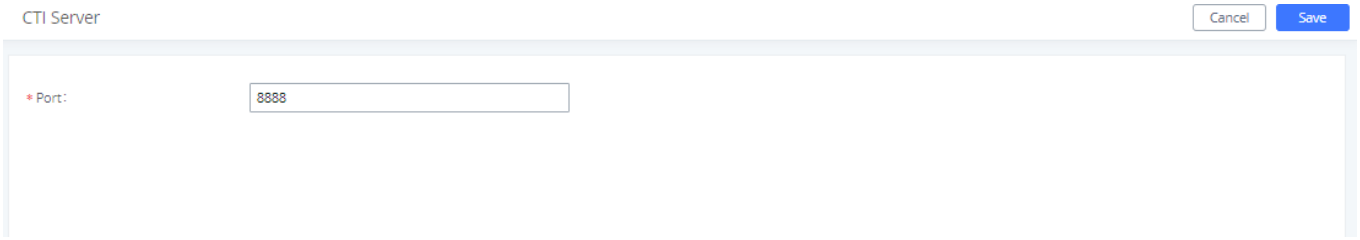
Please do not enable AMI on the UCM630X if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM630X system. Please be cautious when enabling AMI access on the UCM630X and restrict the permission granted to the AMI user. By using AMI on UCM630X you agree you understand and acknowledge the risks associated with this.

CTI Server

UCM does support CTI server capabilities which are designed to be a part of the CTI solution suite provided by Grandstream, including GXP21XX and GXP17XX enterprise IP phones along with GS Affinity app.

Mainly the UCM will by default listening on port TCP 8888 for the connections from GS affinity application in order to interact, modify and serve data requests by the application which includes setting call features for the connected extension as call forward and DND.

Users can change the listening port under the menu page, **Integrations** > **CTI Server** as shown on below screenshot:



CTI Server Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link:

CRM

Customer Relationship Management (**CRM**) refers to practices, strategies, and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers.

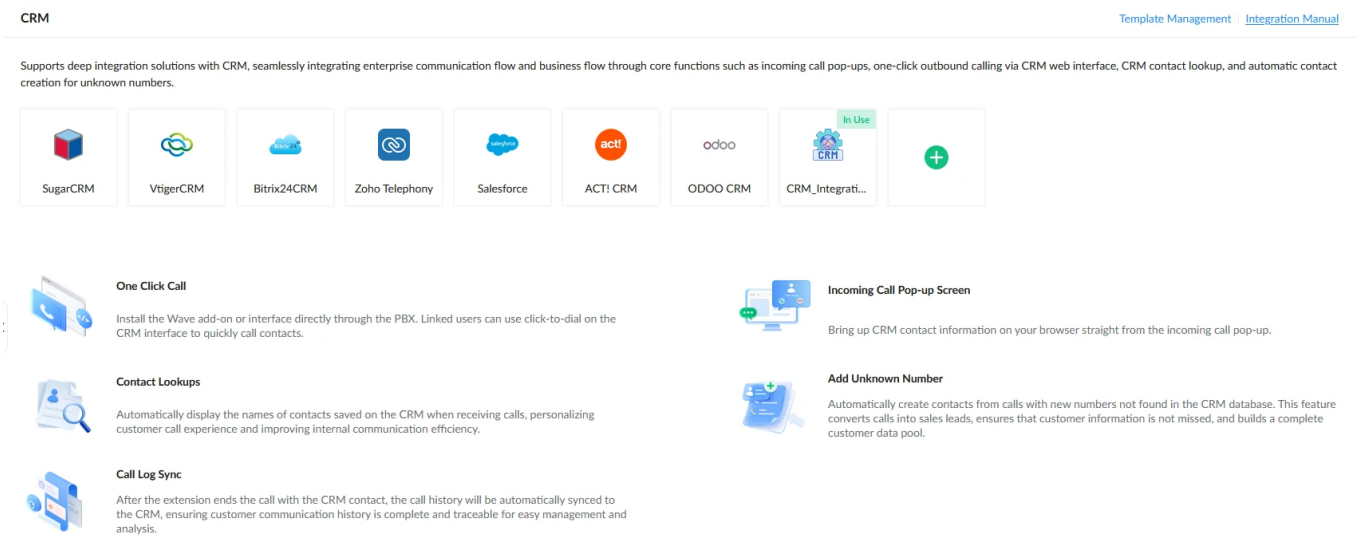
The UCM630X supports seamless integration with various CRM systems, allowing users to look up contact information in the Contacts, Leads, and Accounts tables, display contact records directly in the CRM web interface during incoming calls, perform one-click outbound calling, and automatically synchronize call history into the contact's activity history.

To accommodate different business environments, the UCM630X provides two flexible integration approaches:

- **Default Built-in Integration Templates:** Pre-configured, out-of-the-box integration solutions for widely used CRM platforms, including SugarCRM, VtigerCRM, Bitrix24CRM, Zoho Telephony,Salesforce, ACT! CRM, and ODOO CRM.
- **Custom CRM Templates:** Designed for proprietary or third-party CRM platforms not included in the default list. Administrators can create, import, export, or edit custom CRM templates.

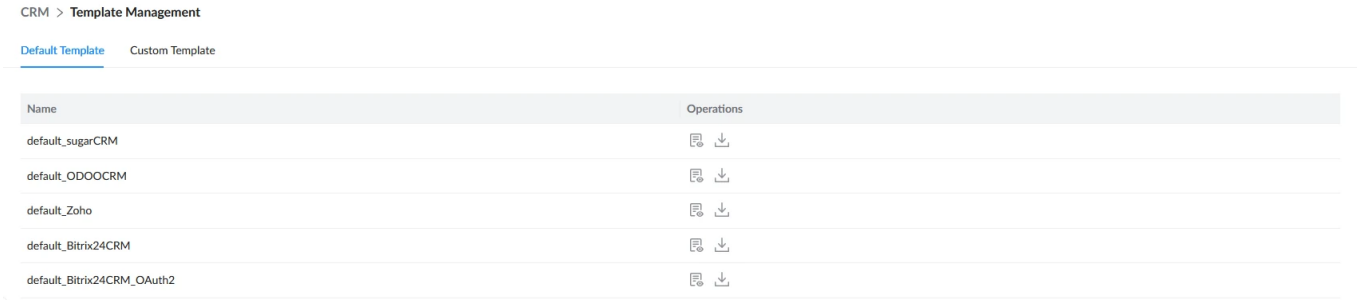
For step-by-step instructions on creating, importing, exporting, and managing custom CRM integration templates, please refer to the Custom Template Configuration Guide.

The main **CRM** page serves as the central hub for selecting and managing integrated CRM platforms. Here, administrators can view all available default and custom CRM modules, activate or switch the active CRM instance.



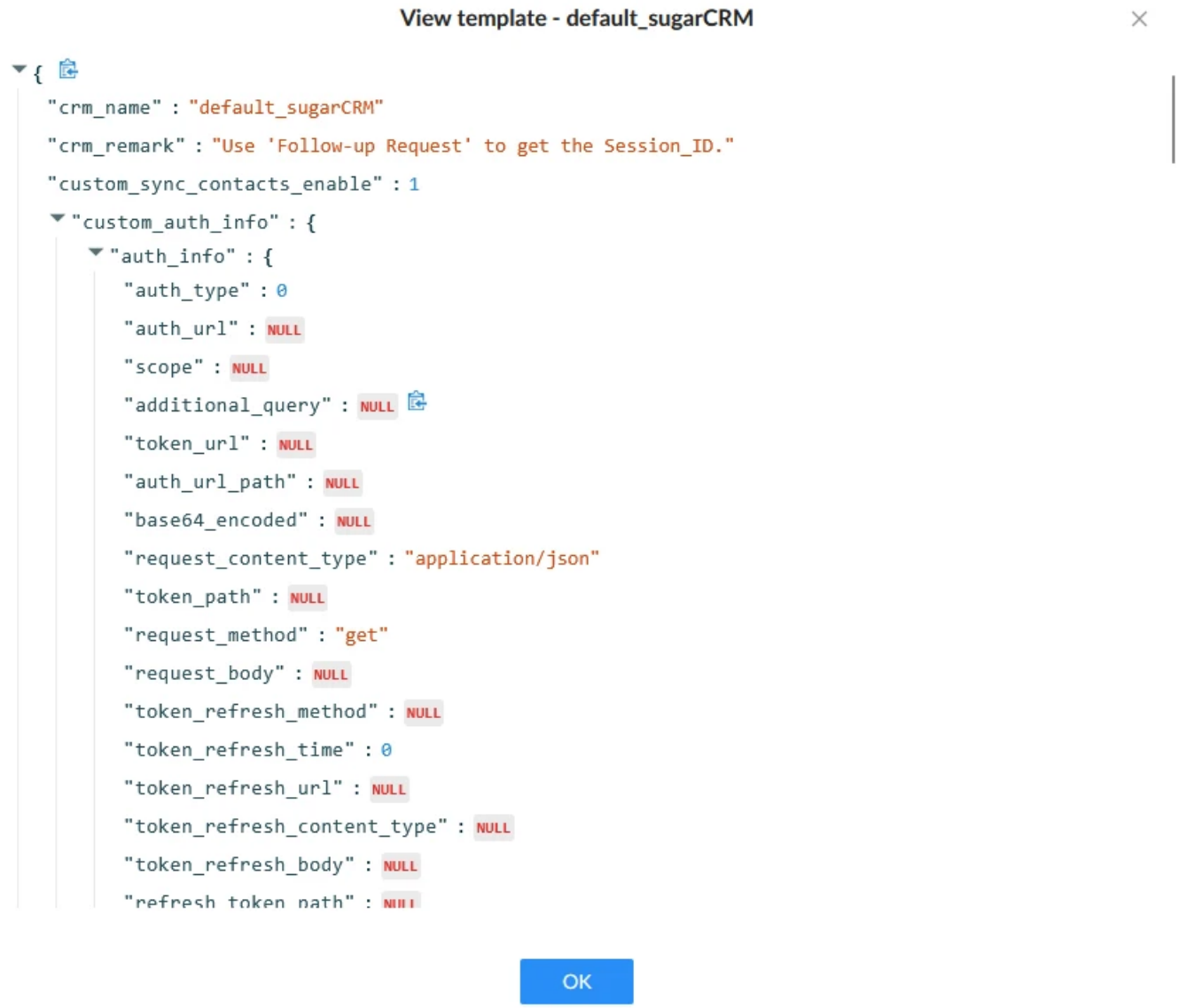
CRM Integration Main Page

Navigating to **Template Management -> Default Template** displays the list of pre-configured CRM templates built into the system. From this page, administrators can inspect the structure of default templates or download them as JSON configuration files to serve as reference models when building custom integrations.



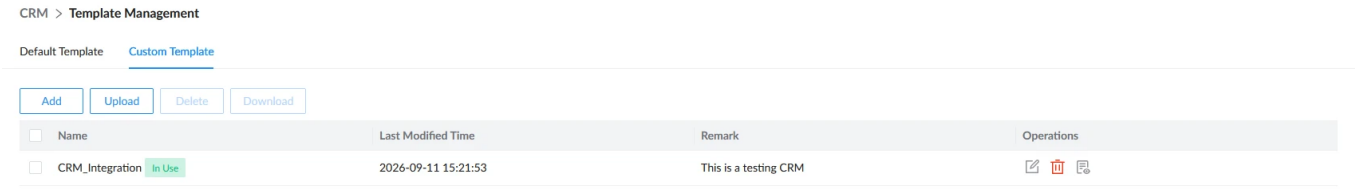
Default CRM Templates Management

Clicking the **View Template** icon on any default template opens a pop-up window displaying its underlying JSON schema. This view reveals the exact REST API endpoints, request methods, authentication structure, token refresh URLs, and parameter definitions used by the platform.



View Default CRM Template Details

The **Template Management -> Custom Template** page allows administrators to manage user-defined CRM templates. From this tab, administrators can create new templates manually by clicking **Add**, batch-upload existing JSON template files, export custom templates for deployment across other UCM systems.



Custom CRM Templates List

When creating or editing a custom CRM template, the **Edit Custom Template** interface provides sections to upload a custom CRM logo, set general metadata (Name and Remarks), and configure detailed REST API request parameters.

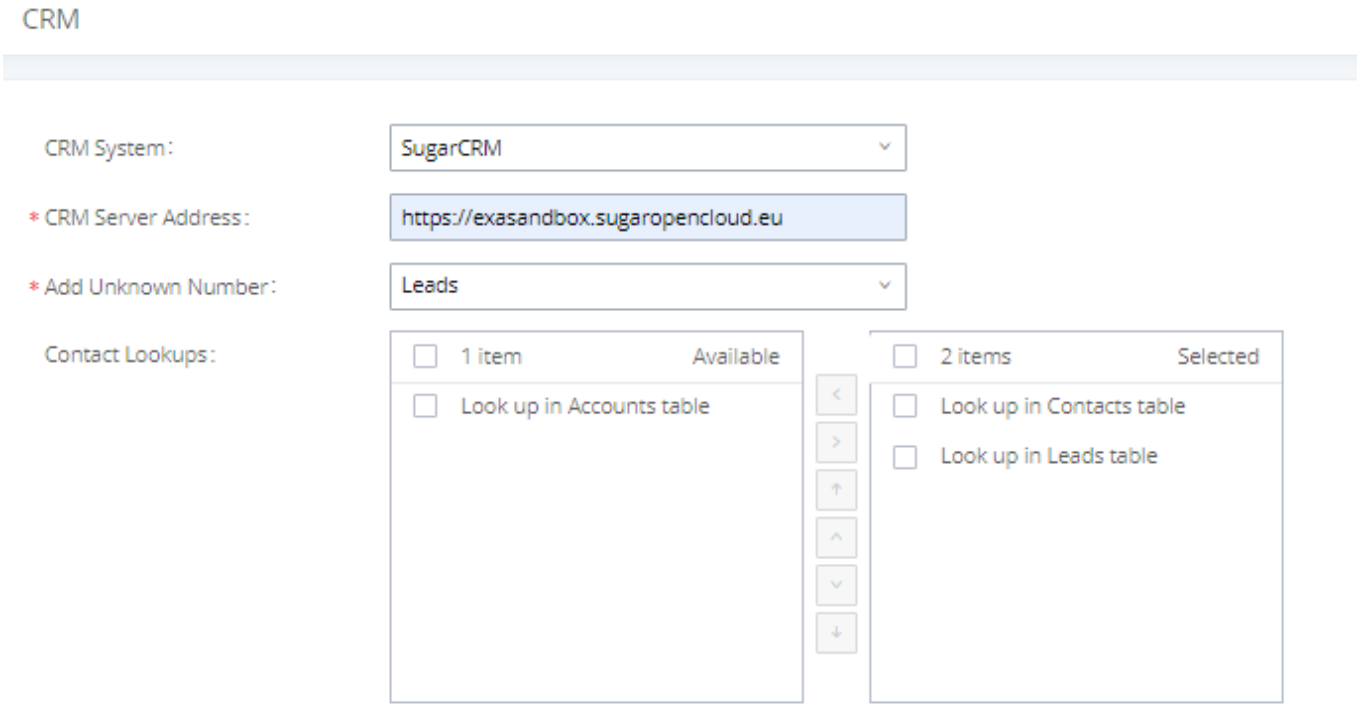
This includes selecting authentication protocols (Basic, Bearer Token, OAuth 2.0), providing certificates or tokens, and defining custom fields that prompt users for required credentials during initial CRM pairing



Edit Custom CRM Template Configuration

Sugar CRM

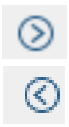
Configuration page of the SugarCRM can be accessed via admin login, on **Integrations > CRM**.



SugarCRM Basic Settings

1. Select "SugarCRM" from the CRM System Dropdown in order to use SugarCRM.

CRM System	Select a CRM system from the dropdown menu.
CRM Server Address	Enter the IP address of the CRM server.

Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	 Select from the "Available" list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

SugarCRM Settings

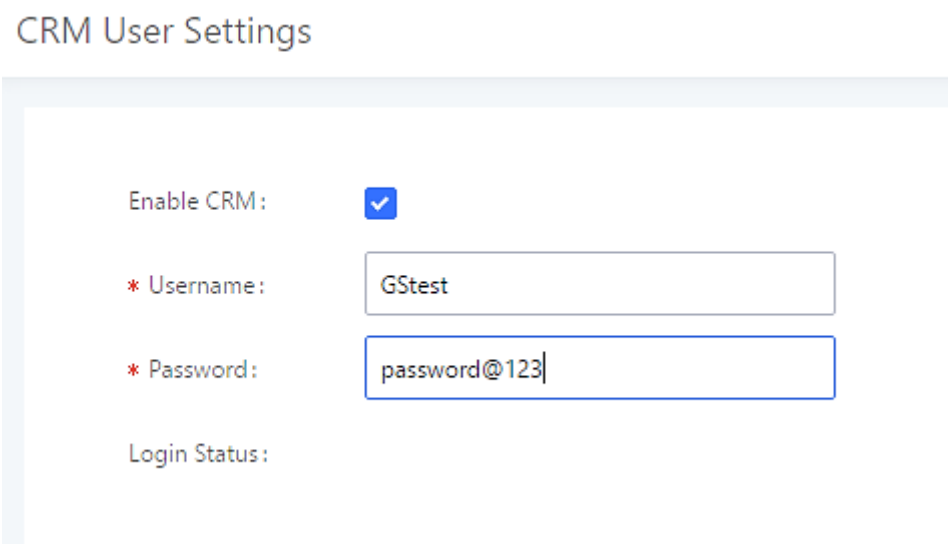
Once settings on admin access are configured:

2. Click on and .
3. Logout from admin access.
4. Login to the UCM as user and navigate under "**User Portal→Other Feature→CRM User Settings**".

Click on "**Enable CRM**" and enter the username/password associated with the CRM account then click on

and

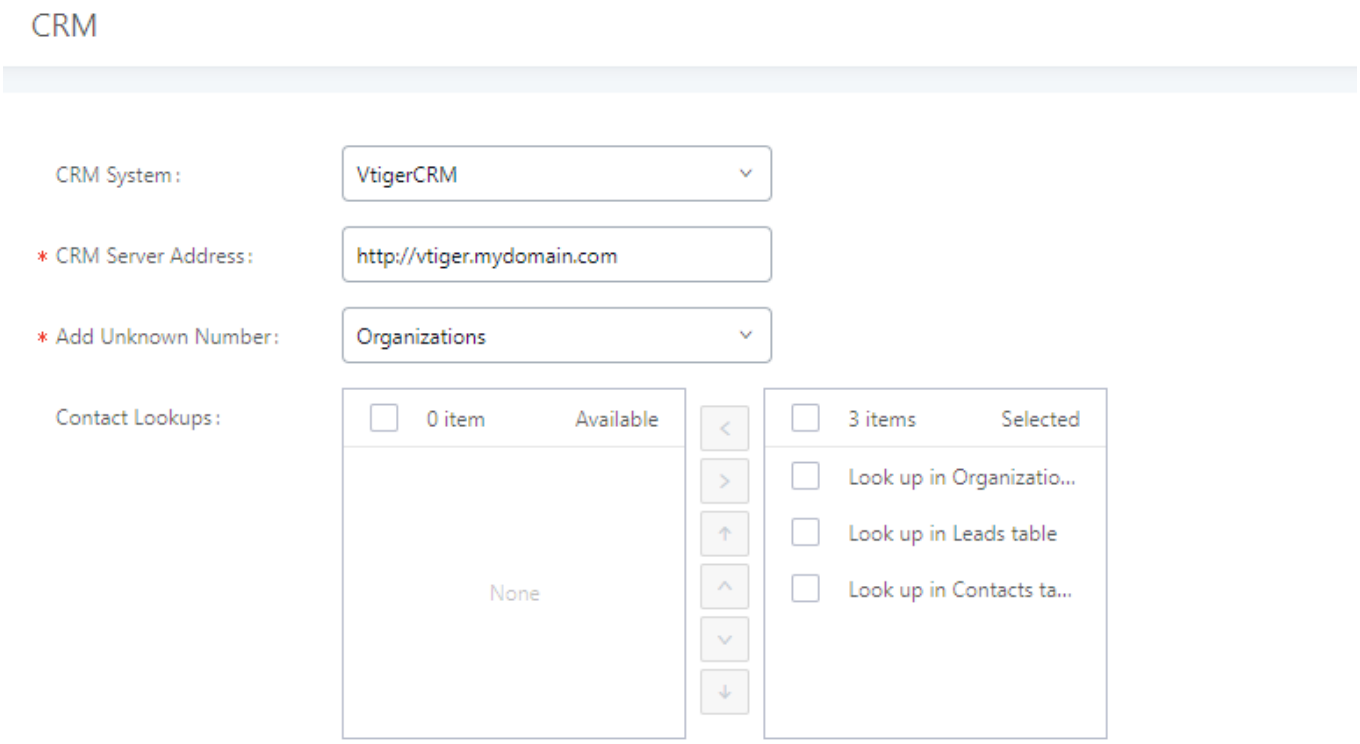
. The status will change from "Logged Out" to "Logged In". User can start then using SugarCRM features.



CRM User Settings

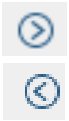
Vtiger CRM

Configuration page of the VtigerCRM can be accessed via admin login, on the UCM WebGUI→**Integrations →CRM**.



VtigerCRM Basic Settings

1. Select "Vtiger CRM" from the CRM System Dropdown in order to use Vtiger CRM.

CRM System	Select a CRM system from the dropdown menu.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	 Select from the "Available" list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.

VtigerCRM Settings

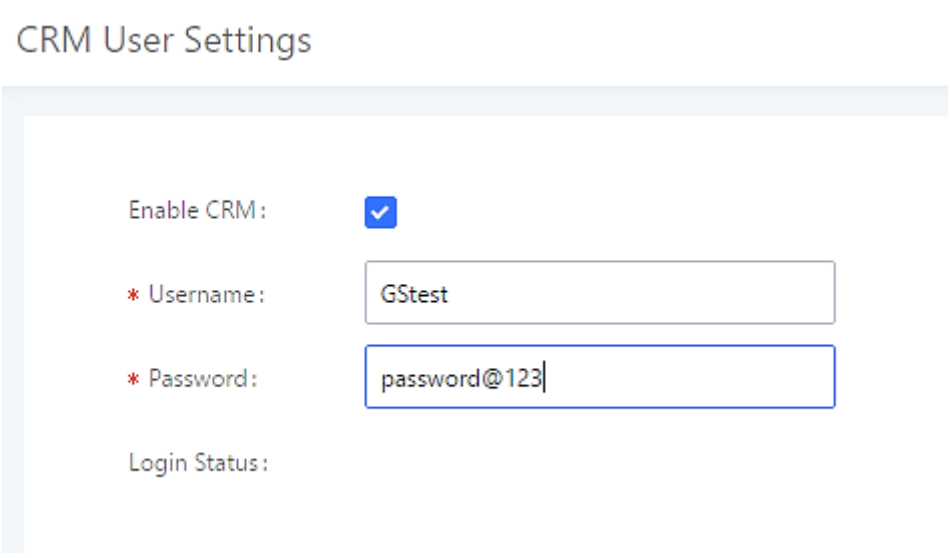
Once settings on admin access are configured:

2. Click on and .

3. Logout from admin access.

4. Login to the UCM as user and navigate under "**User Portal→Other Features→CRM User Settings**".

Click on "**Enable CRM**" and enter the username/password associated with the CRM account then click on and . The status will change from "Logged Out" to "Logged In". User can start then using SugarCRM features.

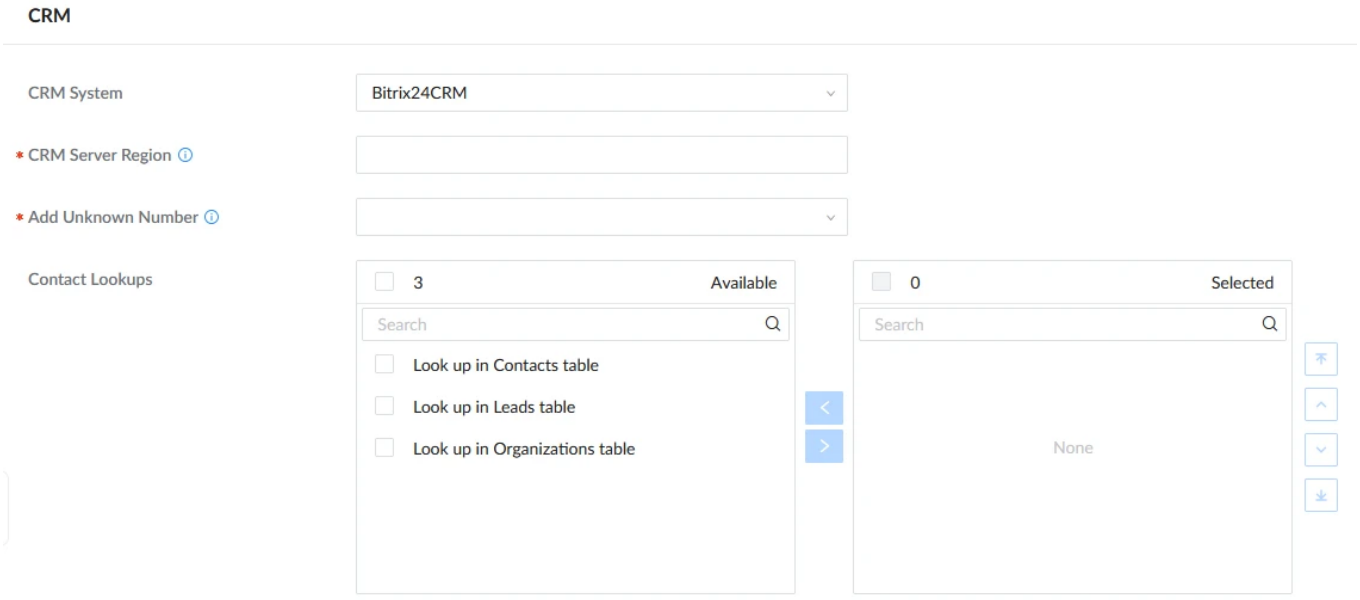


CRM User Settings

Bitrix24 CRM

The UCM6300 Series supports integration with Bitrix24 CRM, allowing the system to query CRM records during calls, display contact information, and automatically create CRM records for unknown numbers based on configuration.

For detailed step-by-step instructions on preparing the Bitrix24 account, generating webhooks, and completing the integration, refer to the Bitrix24 CRM Configuration Guide.



Bitrix24 CRM Settings

The table below describes the configurable parameters for this integration.

CRM System	Select "Bitrix24CRM" from the CRM System dropdown menu to enable Bitrix24 integration.
CRM Server Region	Specify the Bitrix24 server region or domain associated with the Bitrix24 account. This value must match the region or URL used when configuring the Bitrix24 webhook.

Add Unknown Number	Specifies how the UCM handles incoming or outgoing calls from phone numbers that do not exist in Bitrix24 CRM.None: No CRM record is created when an unknown number is detected.Contacts: Automatically creates a new Contact record in Bitrix24 when the number is not found in existing CRM records.Leads: Automatically creates a new Lead record in Bitrix24 when the number is not found.Accounts: Automatically creates a new Account record in Bitrix24 when the number is not found.
Contact Lookups	Select from the "Available" list and move items to the "Selected" list to define where the UCM performs contact lookups in Bitrix24. Supported lookup tables include Contacts, Leads, and Organizations. When multiple tables are selected, the lookup order determines the priority of the search.

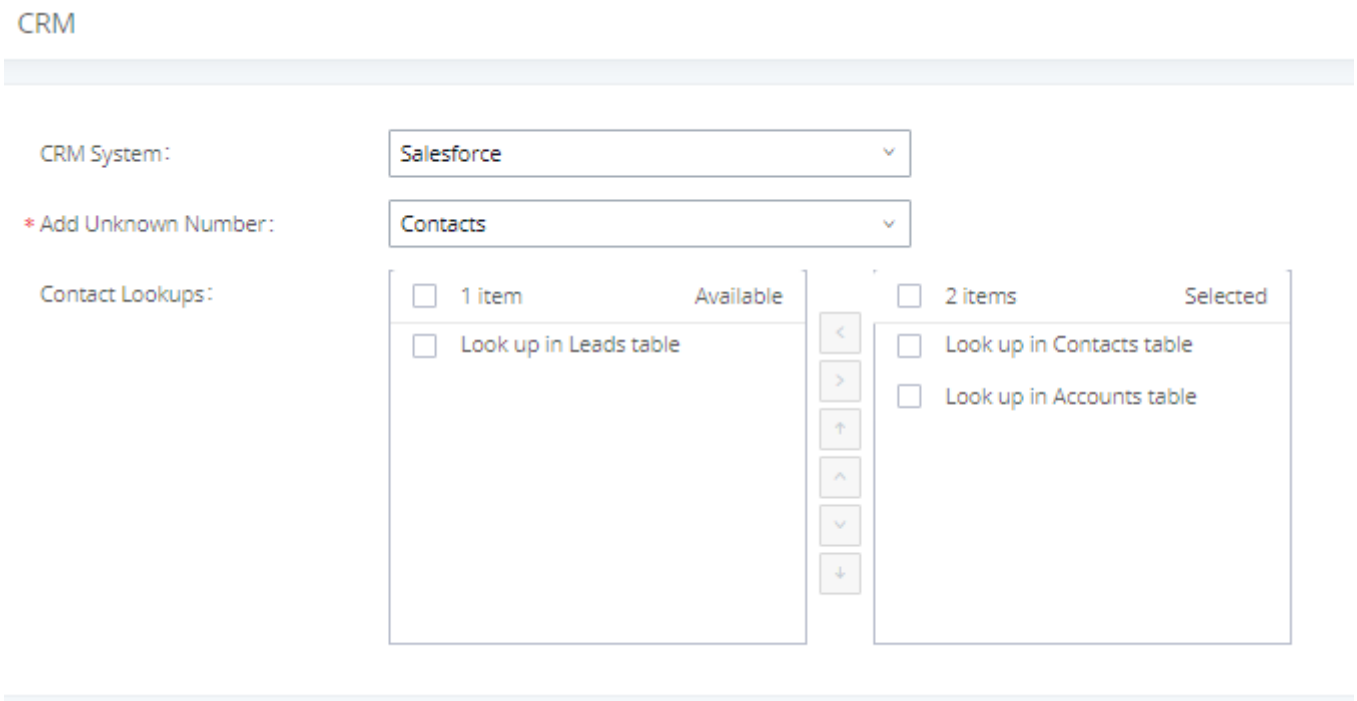
Once the Bitrix24 CRM settings on the admin interface are configured:

1. Click Save and Apply Changes.
2. Log out from the admin account.
3. Log in to the UCM as a user and navigate to **User Portal->Other Features->CRM User Settings**.
4. Enable CRM and enter the Bitrix24 account credentials information as required.
5. Click Save to complete the login process.

After successful login, the CRM status will change from Logged Out to Logged In, and the user can start using Bitrix24 CRM features during calls.

Salesforce CRM

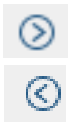
Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI→ **Integrations→CRM**".



Salesforce Basic Settings

1. Select "Salesforce" from the CRM System Dropdown in order to use Salesforce CRM.
2.

CRM System	Select a CRM system from the dropdown menu.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.

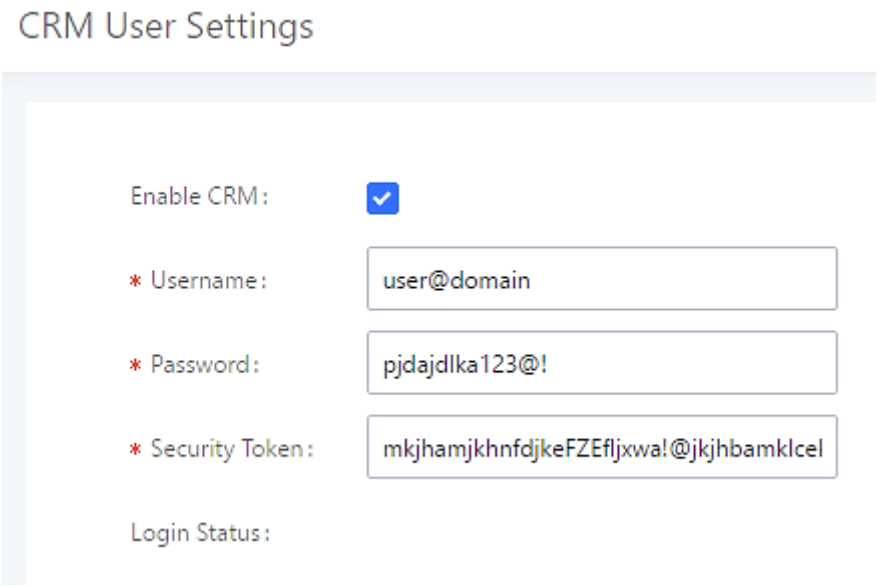
Contact Lookups	 Select from the "Available" list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Salesforce Settings

Once settings on admin access are configured:

2. Click on and .
3. Logout from admin access.
4. Login to the UCM as user and navigate under "**User Portal→Other Features→CRM User Settings**".

Click on "**Enable CRM**" and enter the **username**, **password** and **Security Token** associated with the CRM account then click on and . The status will change from "Logged Out" to "Logged In". User can start then using Salesforce CRM features.



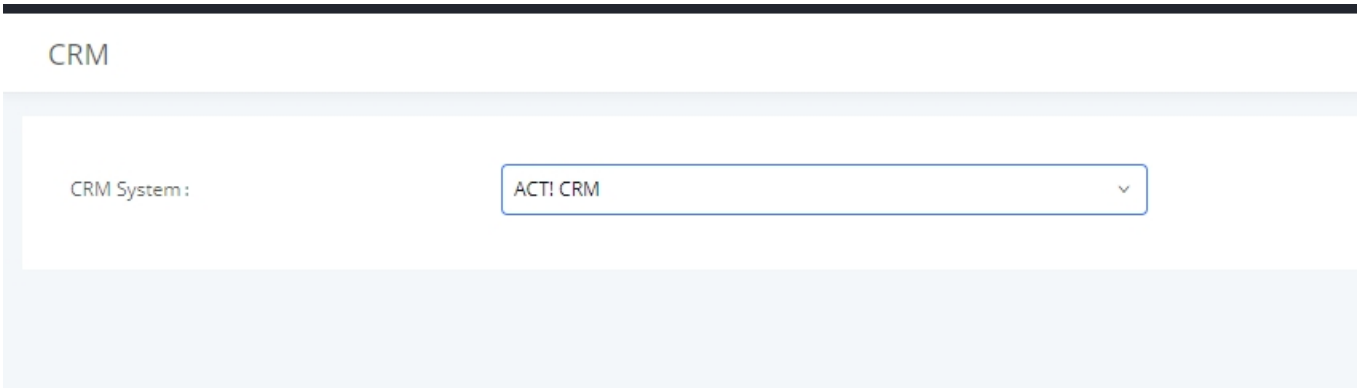
Salesforce User Settings

ACT! CRM

Configuration page of the ACT! CRM can be accessed via admin login, on **Integrations** > **CRM**".

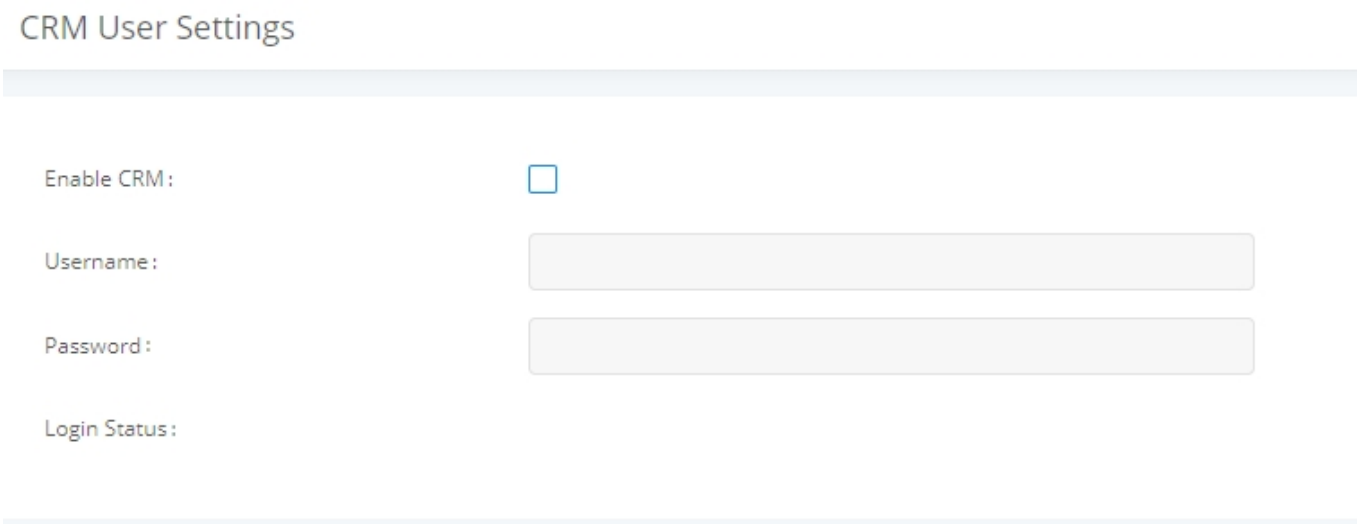
The configuration steps of the ACT! CRM are as follows:

1. Navigate to **Integrations** > **CRM** and select the "ACT! CRM" option.



Enabling ACT! CRM

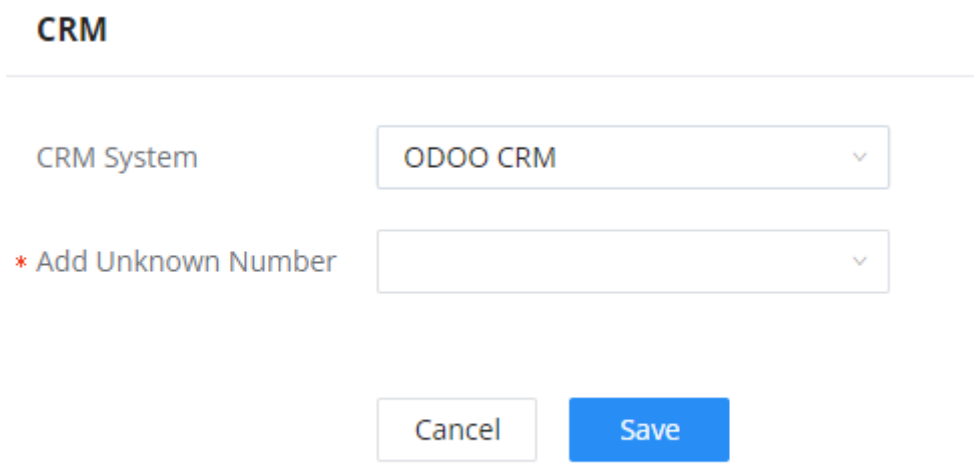
2. Log into the UCM as a regular user and navigate to **Integrations** > **CRM User Settings** and check "Enable CRM" option and enter the username and password, which will be the ACT! CRM account's **API Key** and **Developer Key,** respectively. To obtain these, please refer to the ACT! CRM API developer's guide here: https://www.act.com/



Enabling CRM on the User Portal

Odoo CRM

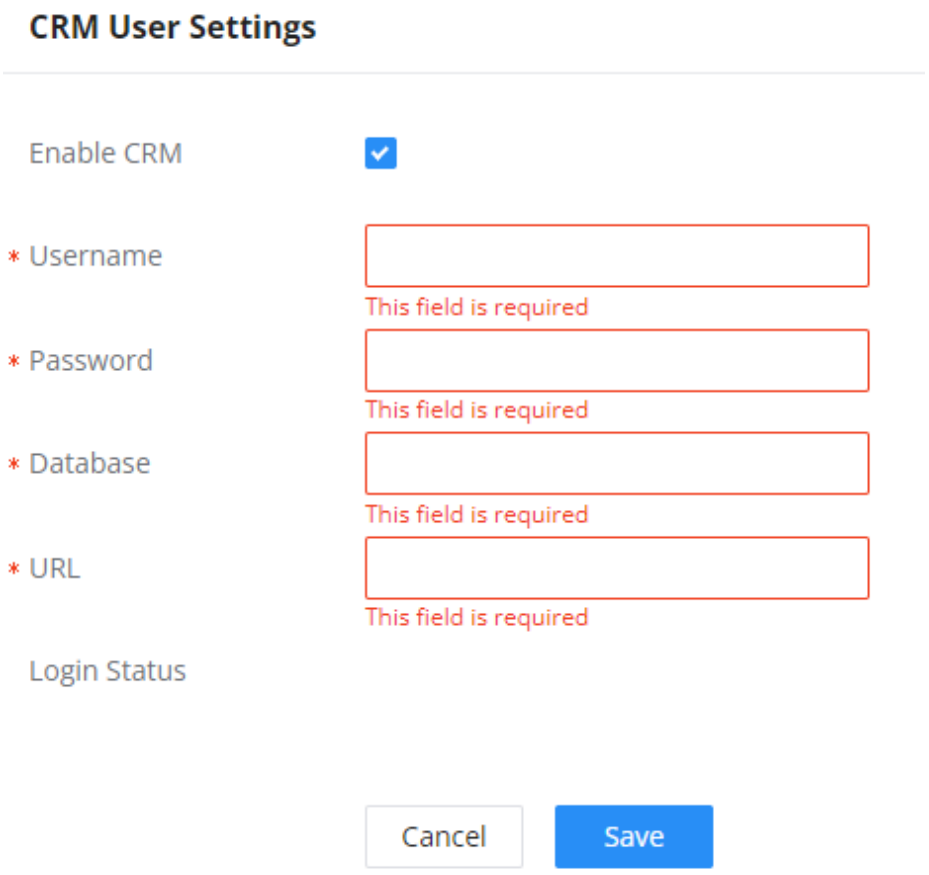
The UCM6300 Series supports integration with Odoo CRM. To enable Odoo CRM, please access the UCM's web UI then navigate to **Integration > CRM**.



Odoo CRM

Click "Save" then "Apply Changes".

Once Odoo CRM is enabled, the user can log into the user portal by access the UCM web UI and entering their username and password, then they can navigate to **Other Features > CRM User Settings**, then they configure their account using username and password created on Odoo platform.



CRM User Settings

PMS (Property Management System)

UCM630X supports Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI->**Integrations→PMS.**

The PMS integration on UCM is currently supported only with one of the five following solutions.

The PMS module built-in the UCM supports the following features based on each solution:

Feature	Mitel	char pmslink	HSC	IDS	Oracle OPERA
Check-In	Yes	Yes	No	Yes	Yes
Check-out	Yes	Yes	No	Yes	Yes
Wake-up Call	Yes	Yes	No	Yes	Yes
Name Change	Yes	No	No	No	Yes
Update	No	Yes	No	Yes	Yes
Set Credit	Yes	No	No	No	No
Set Station Restriction	Yes	No	No	No	No

Room Status	No	Yes	No	Yes	Yes
Room Move	No	Yes	No	Yes	Yes
Do Not Disturb	No	Yes	Yes	No	Yes
Mini Bar	No	Yes	No	Yes	Yes
MSG	No	Yes	No	No	No
MWI	No	No	Yes	No	No
Unconditional Call Forward	No	No	Yes	No	No

Char pmslink

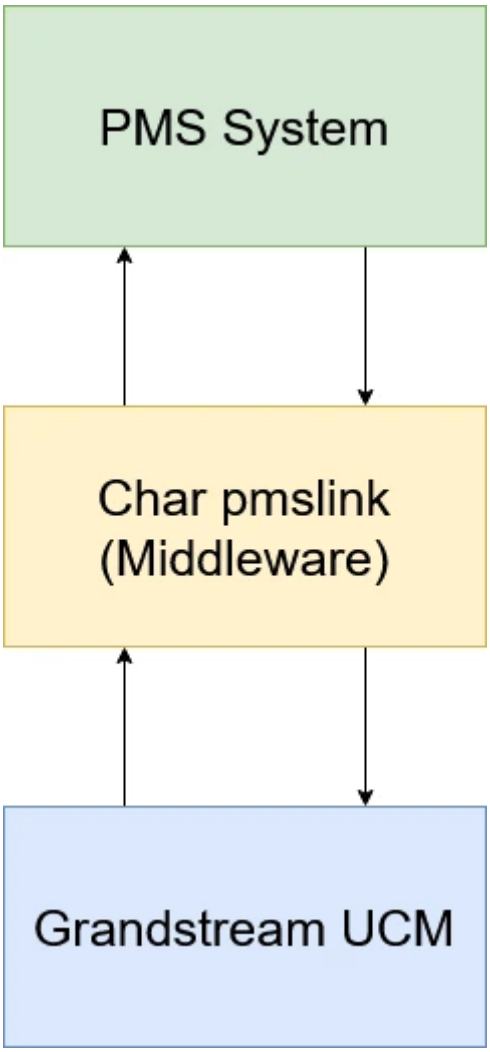
In this mode, the system leverages the **char pmslink** cloud middleware to integrate the UCM with a wide variety of Property Management System (PMS) software.

The communication flow is divided into three parts:

- **PMS (Property Management System):** Your hotel's management software.
- **charpmslink (Middleware):** Acts as the universal interface, translating messages between the PMS and the PBX.
- **PBX (UCM6300):** The Grandstream UCM, which receives commands from the PMS via charpmslink to execute hospitality features.

This integration enables a large variety of hotel features such as: Check-in, Check-out, set Room Status, Wake-up call, and more.

The following figure illustrates the communication flow between the UCM and PMS software, which is done through a middleware system (char pmslink) acting as an interface between both parties.



UCM & Char pmslink interaction

HSC PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series has integrated HSC PMS providing the following features:

- Changing Display Name
- Set Station Restriction
- Call forwarding
- DND
- Name Change
- MWI

Notes:

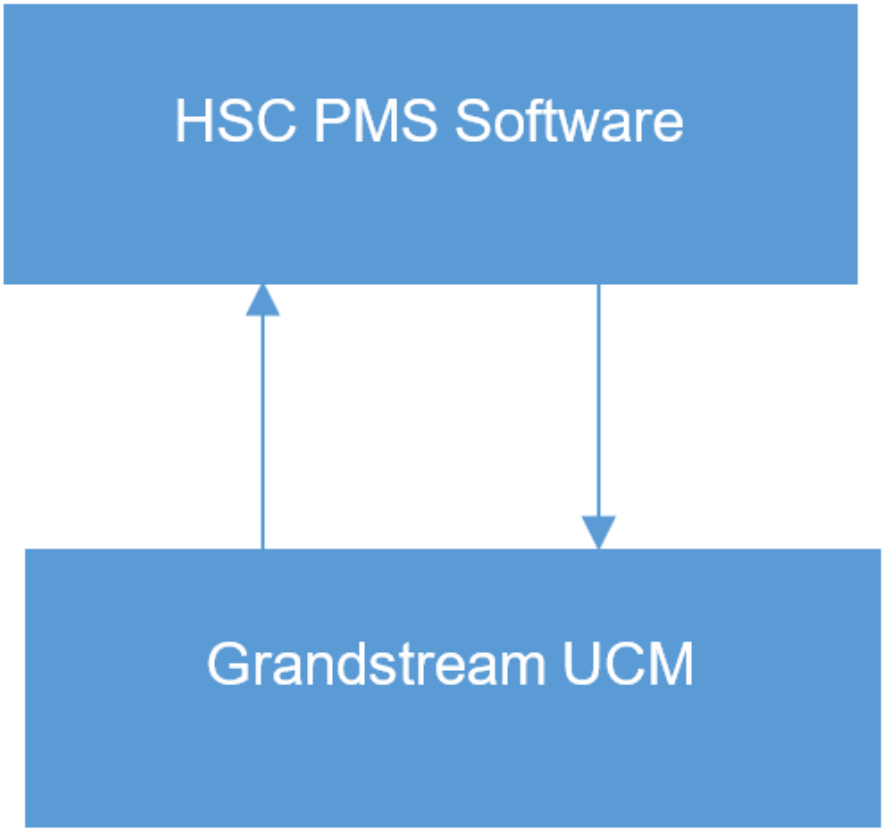
1. Added support for receiving HTTP GET keep-alive messages from HSC PMS. This will allow the PMS to be aware of its connection to the UCM and take the appropriate actions such as raising alarms, sending notifications, etc.
2. Added support for HTTP GET requests from HSC PMS to retrieve UCM extension information. UCM can provide the following information:

- extension - UCM extension number
- name - extension display name / CID name
- mwi - MWI state
- permission - permission level of the extension
- cfwt - call forwarding always number
- dnd - DND state
- language - display language of the extension in ISO 639-1 format

The UCM should respond with either 200 OK or 404 responses.

3. Added HTTPS support

The following figure illustrates the communication flow between the PBX (Grandstream UCM630x Series) and PMS software (HSC). The communication between both parties is direct with no middleware.



UCM & HSC PMS interaction

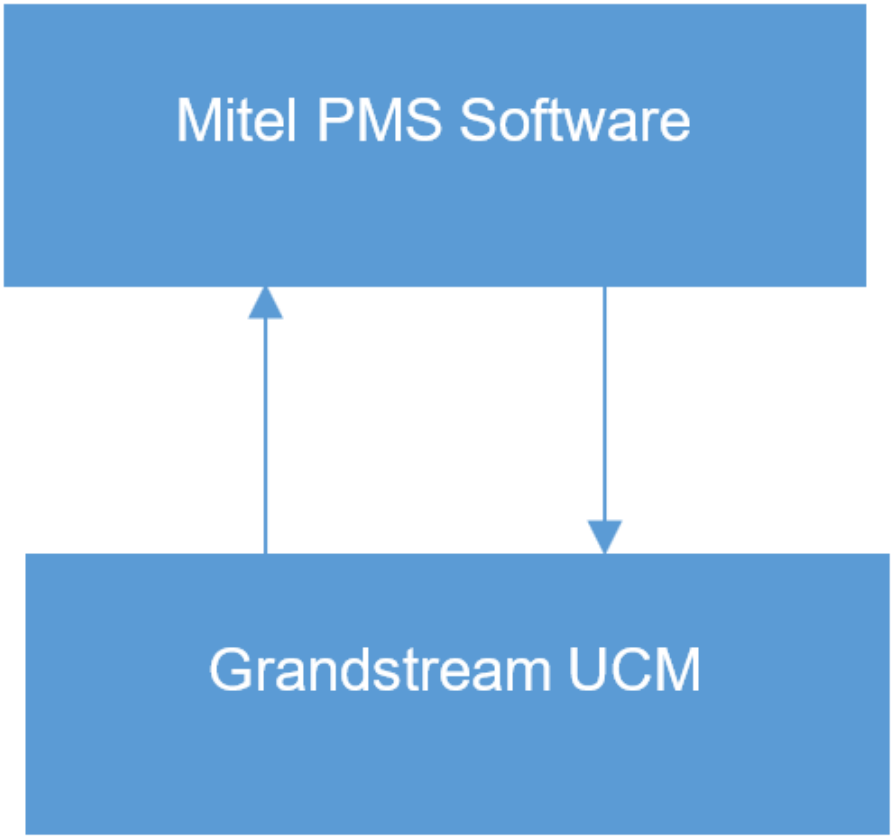
Mitel PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

Grandstream UCM630x series has integrated Mitel PMS providing the following hospitality features: Check-in, Check-out, set Room Status, Wake-up call, and more.

The following figure illustrates the communication flow between the PBX (Grandstream UCM630x Series) and PMS software (Mitel). The communication between both parties is direct with no middleware.



UCM & Mitel PMS interaction

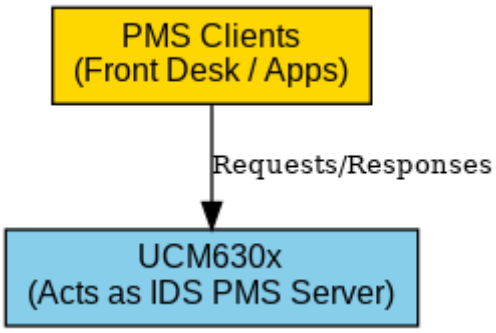
IDS PMS

In this mode, the system can be divided into two parts:

- **PMS Clients** - These are the hotel management applications such as the front desk system, reservation software, or any client that normally communicates with a PMS server.
- **UCM PBX** - Instead of acting as a client or middleware, the UCM directly emulates an IDS PMS server.

With this setup, PMS clients connect directly to the UCM through its PMS port. The UCM listens for incoming requests and responds as if it were the IDS PMS server. This allows hotel staff to perform operations such as setting room status (clean, occupied, available), posting Mini Bar charges, scheduling and managing wake-up calls, or enabling and disabling dialing permissions.

By integrating IDS PMS in this way, the UCM simplifies deployment since no external IDS PMS server or additional middleware is required-the PBX itself provides the PMS server functionality.



UCM & IDS PMS interaction

PMS API

The PMS API allows users to use their middleware to work with PMS systems instead of currently supported integrations.

Additionally, this API allows access to read and modify certain UCM parameters that current supported PMS integrations cannot. To use this, users must first enable and configure the HTTPS API settings.

For more details, please refer to the online https://documentation.grandstream.com/knowledge-base/https-api/, Pmsapi section.

Oracle Hospitality OPERA

The UM603x series integrates directly with Oracle Hospitality OPERA PMS to manage room statuses and extensions from within the OPERA interface. This connection is established using the IFC_PBX interfacing protocol.

To configure the integration, first select the pre-built interface, "Oracle Hospitality OPERA TMS Interface for UCM Series PBX by Grandstream Networks," within the OPERA software. Once enabled, you can complete the setup from the CloudUCM admin portal.

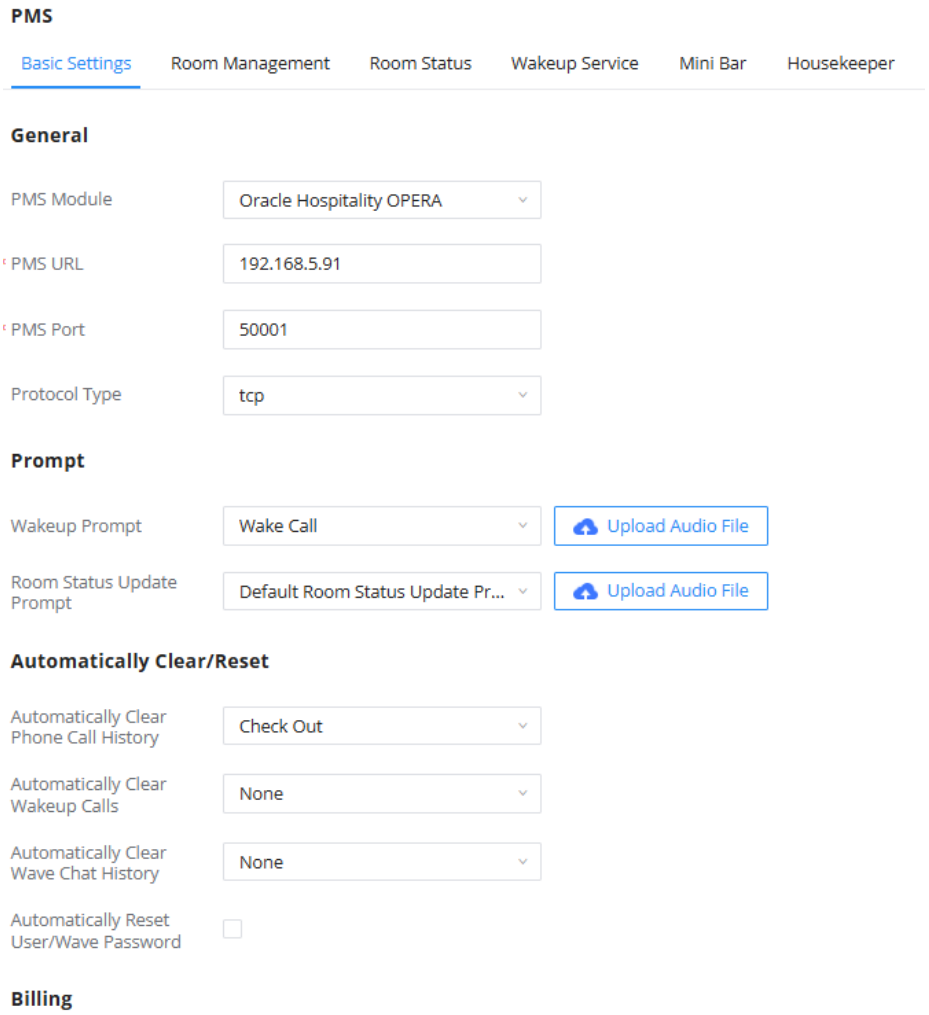
Data exchange between the UCM and the OPERA server is handled by the Fidelio Interface Application Specification (FIAS) protocol. FIAS uses specific attributes to define the data being transmitted. For example:

- "**RN**" represents the Room Number.
- "**RS**" represents the Room Status.
- "**RU**" is used as an update indicator to initiate a room status change.

A typical FIAS message to update a room's status would be formatted as follows: **RU|RN211|RS3**

In this example, room 211 is updated to status code 3.

In addition, The UCM630x supports Oracle OPERA's Youth Hostel Mode. This feature allows a single room to be partitioned into multiple independent units, enabling management of separate groups with distinct extensions and individual billing records within the same physical room.



Oracle Hospitality OPERA

General	
PMS Module	Select "Oracle Hospitality OPERA"
PMS URL	Enter the URL of the Oracle Hospitality Opera server.
PMS Port	Enter the PMS server port.Note: The allowed range 1 - 65535.
Protocol Type	Select the transport protocol to use. TCP: The connection is established using only TCP handshake. Simple SSL: Authentication is required to establish the connection. The identity is verified only on the Oracle OPERA Hospitality server. Mutual SSL: Authentication is required to establish the connection. The identity of both parties is verified by having both parties exchanging their certificates. This reinforces the security by ensuring that only the authorized parties are allowed to contact the server.
Prompt	
Wakeup Prompt	Upload the prompt to play when a wakeup call is answered, or used the default prompt.The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate.Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size.File name can only contain alphanumeric characters and special characters -_Mp3 and WAV formats are supported. If the user uploads an mp3 recording, it will be converted to WAV.

Room Status Update Prompt	Select the prompt to play when the room status is updated, or use the default prompt.The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate.Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size.File name can only contain alphanumeric characters and special characters -_
Automatically Clear/Reset	
Automatically Clear Phone Call History	Select when to clear phone call history. None: The phone call history will not be cleared. Check Out: The phone call history of the guest will cleared upon checking-in. Check In: The phone call history will be cleared when checking-in a new guest.
Automatically Clear Wake Up Calls	Select when to clear scheduled Wakeup calls. None: The wake-up call configuration will not be cleared. Check In/Out: The wake-up call configuration will cleared upon either checking-in or checking-out. Check Out: The wake-up call configuration will cleared upon checking-out. Check In: The wake-up call configuration will cleared upon checking-in.
Automatically Clear Wave Chat History	Select when to clear Wave chat history. None: Wave chat history will not be cleared. Check Out: Wave chat history will cleared upon checking-out. Check In: Wave chat history will cleared when checking-in a new guest.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
Billing	
Type of Call Billing	Select the type of billing the call fees for the guests. Send to Oracle PMS: The call details will be sent and calculated on Oracle Opera. PBX Direct Billing: The billing will be calculated by the UCM and synchronized with Oracle Opera.
Minibar Billing Type	Select the type of billing the mini bar Send to Oracle PMS: The consumed mini bar goods will be pushed to Oracle Opera where they will be processed for the billing. PBX Direct Billing: The consumed mini bar goods will be processed for billing on the UCM, and the bill will be synchronized with Oracle Opera.
Other	
Back Up Voicemail Recordings	Back up voicemail recordings to external storage after check-out. When this option is enabled, the user can select the storage location option, SD Card, USB 1, USB 2, NAS, or SFTP Server.The user can also specify an email address to send voicemail recordings for archiving purpose.
Sync Guest Name to Phone	Provisions the name of checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisionable by Zero Config.

Local PMS

The UCM6300 series includes an integrated on-premise Property Management System (PMS), providing essential hospitality management capabilities directly from the Web GUI under **Integrations -> PMS** without requiring external software licenses.

The local PMS solution manages core hotel operations including Room Management, Reservation and Check-in/Check-out management, Hourly Room rentals, Minibar consumption tracking, Wake-up Services, and more.

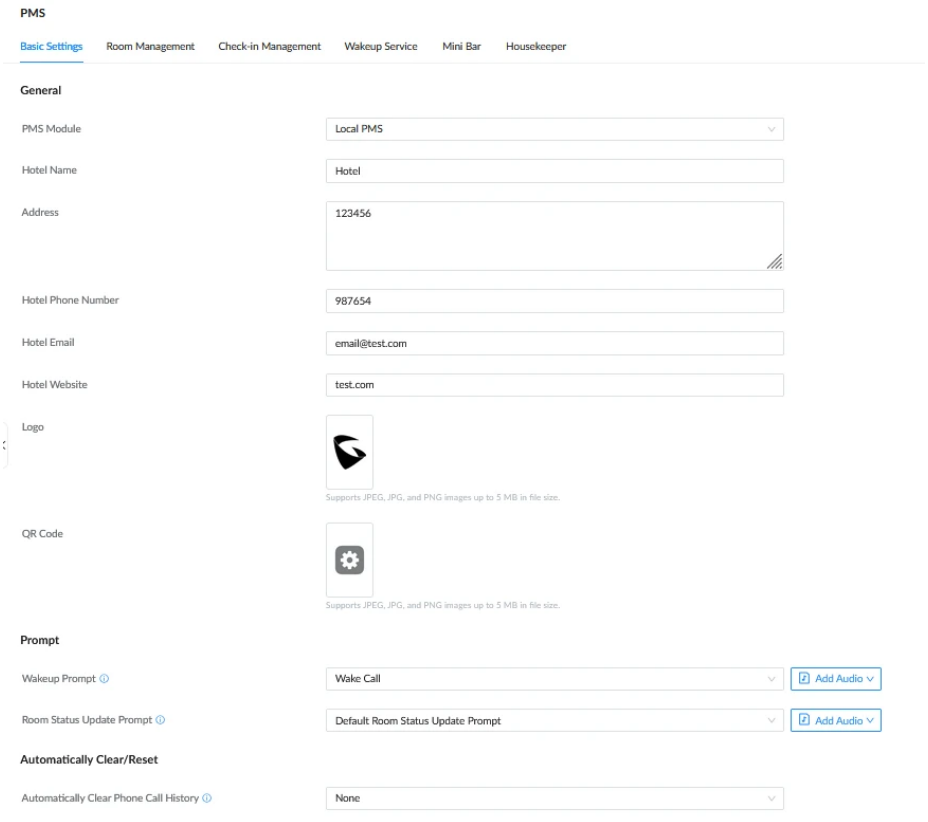
Key highlights and features supported by the Local PMS include:

- **Custom Hotel Branding:** Configure hotel logos, contact phone numbers, website, and a QR code to customize printed bills and automated self-check-in/check-out emails.
- **Self Check-in and Check-out:** Guests can check in and check out using emails automatically sent by the UCM for reservations.

- **Room & Calendar Management:** Real-time Room Availability Calendar, itemized bill printing (breakdowns for taxes, room charges, and minibar items), and hourly room options.
- **Guest List:** Stored database of guests which helps with future bookings and retains guest information for quick reference.

For detailed step-by-step configuration guides and operational workflows, refer to the Local PMS Guide.

https://documentation.grandstream.com/knowledge-base/ucm63xx-local-pms-guide



The configuration parameters available under Local PMS Basic Settings are explained in the table below:

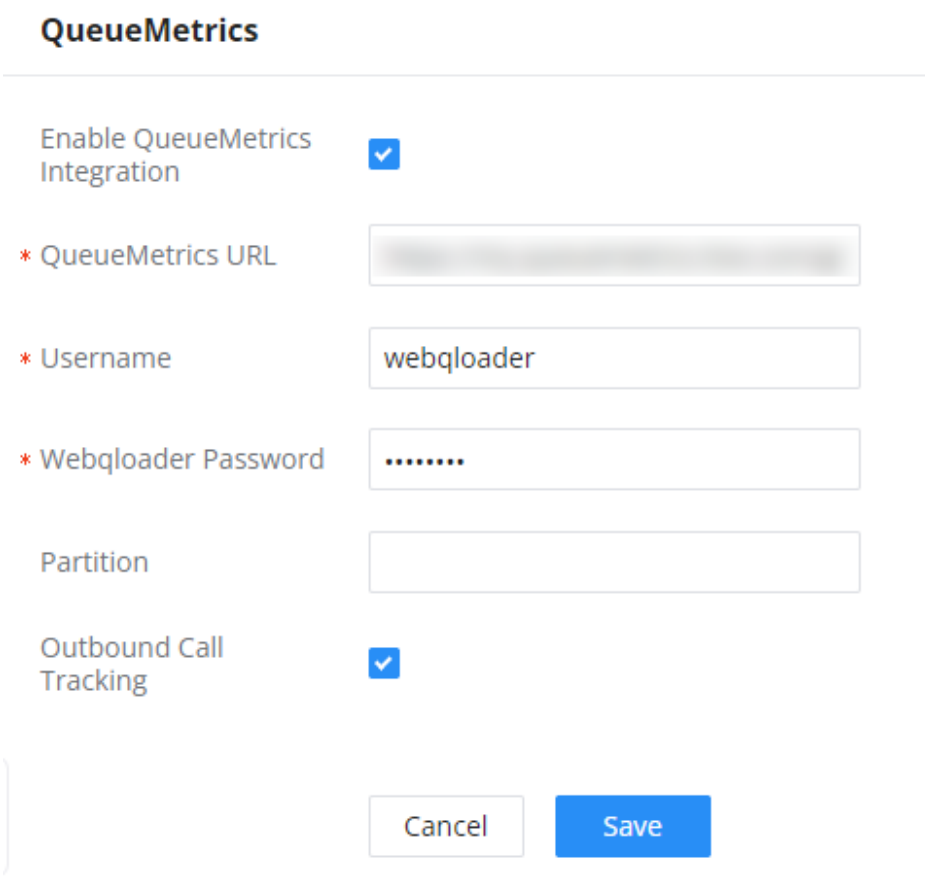
Parameter	Description
General	
PMS Module	Selects the Local PMS module functionality.
Hotel Name	Configures the official hotel name to be displayed on guest bills, and emails.
Address	Configures the hotel physical address displayed on bills and emails.
Hotel Phone Number	Configures the contact phone number printed on bills and emails.
Hotel Email	Configures the official hotel email address used for bills and emails.
Hotel Website	Configures the hotel website URL printed on guest bills and emails.
Logo	Uploads a custom hotel logo for printed bills and automated emails. Supports JPEG, JPG, and PNG formats up to 5 MB.
QR Code	Uploads a custom QR code (e.g., for online hotel guides) displayed on printed bills and automated emails. Supports JPEG, JPG, and PNG formats up to 5 MB.
Prompt	
Wakeup Prompt	A customized prompts that can be played when the wakeup call is answered. To customize it please navigate to PBX Settings->Voice Prompt->Custom Prompt.

Room Status Update Prompt	Choose a previously uploaded prompt or upload the prompt which will be played when the room status is changed. If the room status codes have been change, please update the Room Status accordingly.
Automatically Clear/Reset	
Automatically Clear Phone Call History	Configures whether or not the call history of phones will be automatically cleared upon check-in or check-out. Currently only supported on Grandstream phones. None: Call history will not be deleted after checking-in or checking-out. Check Out: Call history will be delete when the guest checks-out. Check In: Call history will be delete when a new guest checks-in.
Automatically Clear Wakeup Calls	Scheduled wakeup calls for rooms can be cleared upong checking in or checking out. None: The wakeup calls won't be automatically cleared. Check out: The wake up calls assigned to the guest will be cleared when they check out. Check In: The wake up calls assigned to a guest will be cleared when a new client checks in.
Automatically Clear Wave Chat History	If enabled, room Wave chat history will be automatically cleared upon check-in or check-out.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
Self-service Settings	
Self Check-in via Email	Enables the system to automatically send a self check-in email with a link prior to the guest's arrival.
Check-in Email Template	Selects the email template used for sending automated self check-in notifications.
Send in Advance (hrs)	Defines how many hours before the scheduled check-in time the self check-in email will be sent. (Range: 0 - 6 hours).
Self Check-out via Email	Allows the system to automatically send a self check-out email with a link prior to departure.
Check-out Email Template	Selects the email template used for sending automated self check-out notifications.
Send in Advance (hrs)	Defines how many hours before the scheduled check-out time the email will be delivered. (Range: 0 - 6 hours).
Allow Check-out with Unsettled Bill	Controls whether guests are allowed to complete self check-out even if their bill is not fully paid. Enabled: The guest may check out before completing the payment. Disabled: Payment must be settled before self-check-out is allowed. This option is disabled by default.
Other	
Back Up Voicemail Recordings	Configures automatic backup of voicemail recordings to external storage after check-out. When this feature is enabled, users can specify the storage destination.
Storage Location	Select the storage location for voicemail recordings. The available options are: SFTP Server NAS USB SD Card Note: To configure storage devices, go to PBX Settings->Storage Device Management.
Email Address	Enter the destination email address where the system will deliver backup files.
Sync Guest Name to Phone	Provisions the name of the checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisinable by Zero Config.
Review Bill at Check-Out	If enabled, a pop-up window with all the charges will appear during guest check-out for reviewing purposes.
Call Billing	
Call Rate	Configures call charge rates for outbound calls made from guest room extensions.

Currency Unit	The currency unit for the call rate. These are the supported options which you can choose from: American Dollar Euro Sterling Pound Yen Won Hong Kong Dollar Australian Dollar Canadian Dollar Baht Singapore Dollar Swiss Franc Swedish Krona Danish Krone Norwegian Krone New Zealand Dollar South African Rand Brazilian Rial Indian Rupee Russian Ruble Vietnamese Dong Polish Zolty Czech Koruna Turkish Lira Custom: Enter the currency unit.
Periodically Send Records to Email	If enabled, new recordings will be automatically sent to the specified email inbox periodically at the specified intervals.
Type	Configures the type of recordings that should be sent periodically: Wakeup Service Check-in/Check-out History CDR Records
Period	Specifies the automatic download period. The default option is "By Day". At the specific time of each day, week or month, the last cycle of new records will be sent to the user. By Day By Week By Month
Email	Specifies the automatic download period. The default option is "By Day". At the specific time of each day, week or month, the last cycle of new records will be sent to the user.
Guest Email	
Customer Email	Enables the system to send automated emails to guests. This includes reservation updates and billing information. Note: Email notifications will not be sent if the customer's email address is missing.
Reservation Notification	When enabled, the guest will automatically receive an email whenever a reservation is created, modified, or cancelled.
Billing Notification	If enabled, billing-related emails will be sent automatically to the guest.
Email Template	Selects or edits custom email templates used for reservation and billing notifications.

QueueMetrics

The QueueMetrics docking tool provides an interface for UCM system and QM docking. Pass the UCM call queue report to QueueMetrics in a richer form. QueueMetrics is a call center control platform that supports login and logout of frequently used agents in the call center, provides call reports, real-time queue monitoring and other functions.



QueueMetrics

Parameter	Description?
Enable QueueMetrics Integration	Tick this box to enable QueueMetrics integration module.
QueueMetrics URL	Enter the URL of the QueueMetrics on-premise server you have installed. (i.e. http://xxx.xxx.xxx.xxx:8080/queuemetrics.).
Username	Please enter the username used to interface with QueueMetrics. This is typically the QueueMetrics webqloader user. Please confirm that the user is enabled to avoid connection failure.
Webqloader Password	Please enter the webqloader password.
Partition	Enter the data storage partition identifier
Outbound Call Tracking	If enabled, QueueMetrics will track the outgoing calls of all extensions. Note: Outbound Call Tracking is available only on the PBX.

For step-by-step configuration of QueueMetrics integration with the UCM6300 Series, please refer to the following guide: https://documentation.grandstream.com/knowledge-base/queuemetrics-integration/

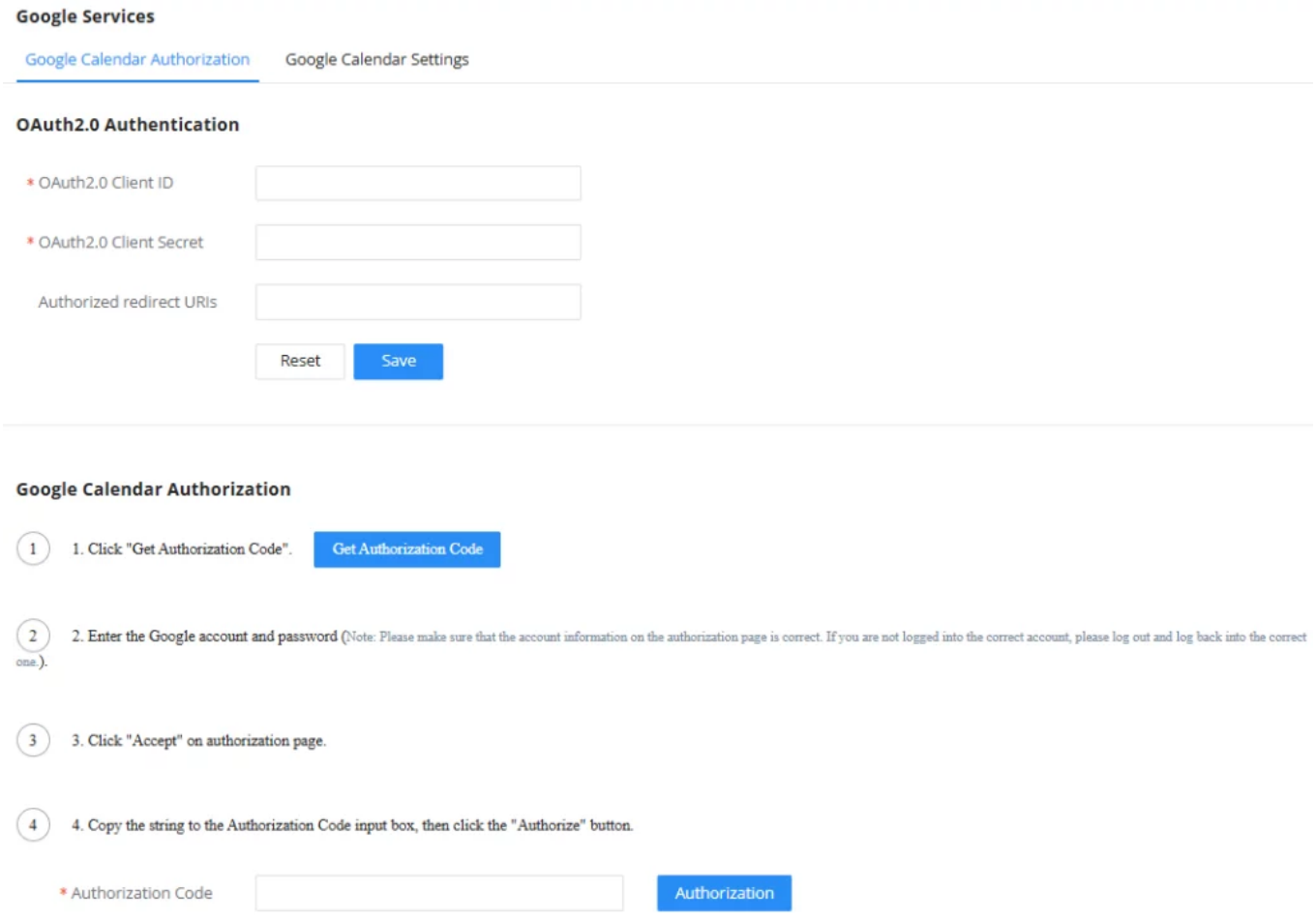
Google Services

Configuring the Google Services integration allows the user to automatically and synchronously events, such as, scheduled meeting and scheduled paging, on Google Calendar of the user upon creating one of the aforementioned events.

Google Calendar Authorization

In this page, the user can configure the OAuth2.0 authentication information to establish the integration successfully. The user can create the authentication ID and the client secret in Google API console, then use

them on the UCM.



Google Calendar Authorization

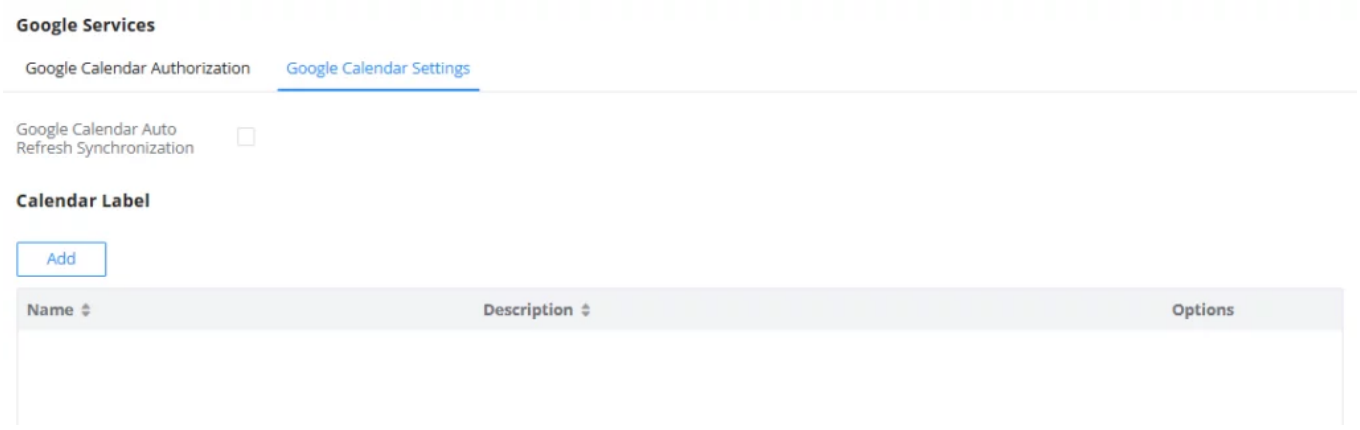
The table below describes the configuration parameters and action steps required to authorize and integrate Google Calendar services.

Parameter	Description
OAuth2.0 Authentication	
OAuth2.0 Client ID	Enter the Client ID generated from your Google Cloud Platform API & Services console.
OAuth2.0 Client Secret	Enter the Client Secret generated from your Google Cloud Platform API & Services console.
Authorized redirect URIs	Displays the URI required to be added under Authorized Redirect URIs in your Google API project settings.
Google Calendar Authorization Steps	
Get Authorization Code	Step 1: Click the Get Authorization Code button to open the Google Account login and authorization window.
Account Authentication	Step 2: Enter your Google account credentials. Ensure you log into the correct Google account associated with the calendar.
Grant Permissions	Step 3: Click Accept on the authorization page to grant the system access to manage calendar events.
Authorization Code	Step 4: Copy the generated token string from Google into the Authorization Code input field, then click the Authorization button to complete the process.

Google Calendar Settings

On this page, the user can configure the refresh interval of the information in Google Calendar. Periodically, the UCM will send the updated/created information to Google Calendar.

The user can also create calendar labels which are use to distinguish the different kinds of events which are synchronized. For example, the user can choose to give different labels to scheduled meetings and to scheduled paging, to easily distinguish the type of event synchronized to Google Calendar.



Google Calendar Settings

For a step-by-step configuration guide for Google Services configuration, please refer to the following guide: https://documentation.grandstream.com/knowledge-base/google-calendar-api-integration/

3rd Party Database Integration

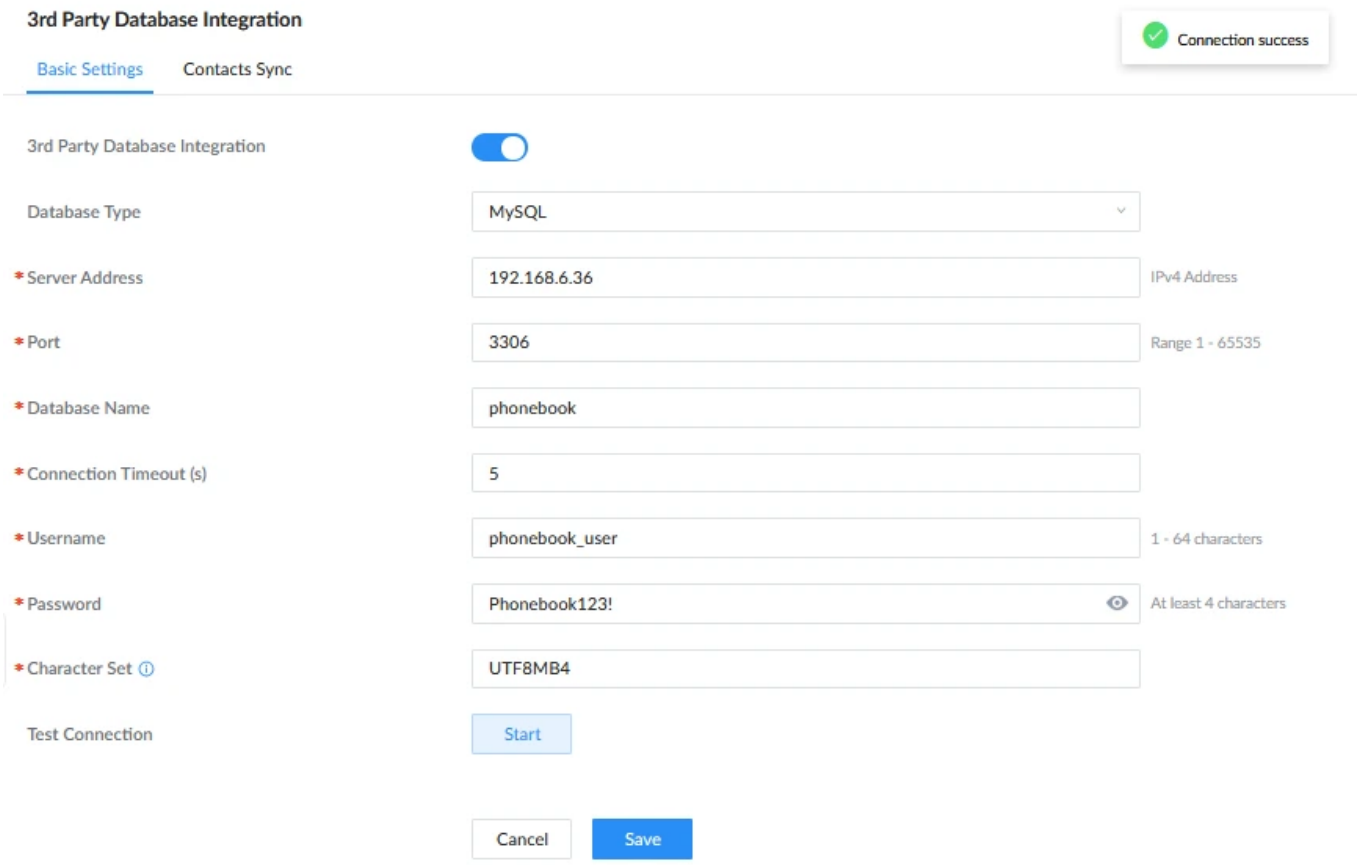
The Third-Party Database Integration feature allows the UCM to connect to external databases (such as MySQL) to query contact information when calls are received. When a matching record is found, the caller name is displayed. Optionally, contacts can be synchronized into the UCM LDAP phonebook for centralized management.

For comprehensive details on this integration, its workflows, and configuration steps, please refer to the following guide.

https://documentation.grandstream.com/knowledge-base/third-party-sql-database-integration-guide/

LDAP phonebooks synced from third-party databases support up to 500,000 contacts.

This feature is configured under **Integrations->3rd Party Database Integration**.

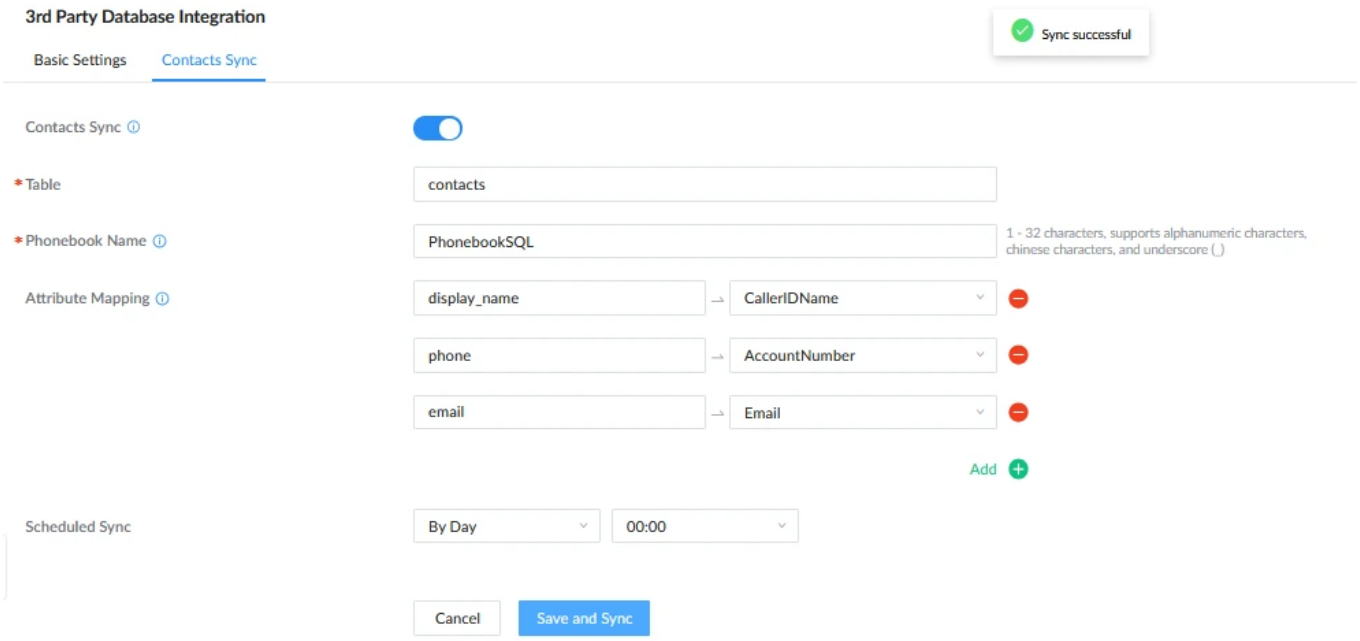


3rd Party Database Integration Basic Settings

The Basic Settings tab is used to configure and enable the database connection. The table below describes the parameters on this page:

3rd Party Database Integration	Enable or disable 3rd party database integration. When enabled, the UCM queries the configured database for contact information.
Database Type	Select the database engine: SQL Server MySQL
Server Address	Enter the IPv4 address of the database server.
Port	Enter the port used by the database service. Valid range: 1-65535
Database Name	Enter the name of the database used for establishing the connection.
Connection Timeout (s)	Set the time (in seconds) to wait before a connection attempt times out. Please enter a value between 1 and 300. The default value is 5.
Username	Enter the username used to connect to the database.
Password	Enter the password for the specified username.
Character Set	Specifies the character set for MySQL connections. ASCII UTF-8 GBK GB2312 UTF8MB4
Test Connection	Click to test connectivity and authentication to the configured database.

After the database connection is successfully established, an additional Contact Synchronization tab becomes available, which enables synchronization of database contacts into the UCM LDAP phonebook.



3rd Party Database Integration Contacts Sync

The configurable parameters on this page are described in the table below:

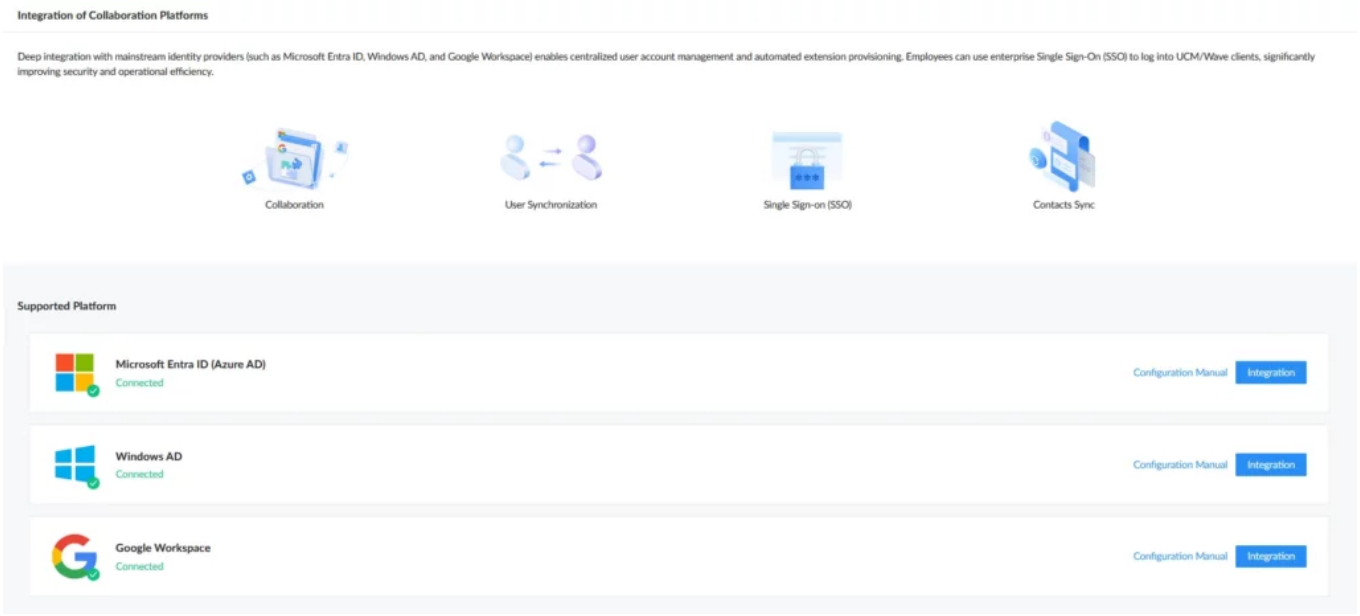
Contacts Sync	Enables synchronization of database contacts into the UCM LDAP phone book. When disabled, real-time caller lookup remains available, but contacts are not synchronized.
Table	Enter the database table containing contact records.
Phonebook Name	Choose the display name of the LDAP phone book created on UCM.
Attribute Mapping	Maps the 3rd party database fields to UCM LDAP attributes (max 10).
Scheduled Sync	Defines automatic synchronization schedule.

Integration of Collaboration Platforms

The UCM6300 Series supports integration with enterprise collaboration and identity platforms to centralize user management, authentication, and directory synchronization. These integrations allow administrators to synchronize user identity information from external platforms into the UCM, associate users with extensions or system accounts, and enable Single Sign-On for simplified and secure access to the UCM web interface.

Supported platforms include:

- **Microsoft Entra ID (Azure AD)**
- **Windows Active Directory**
- **Google Workspace**



Integration of Collaboration Platforms Page

Each integration provides configurable options for user synchronization scope, user linking behavior, LDAP directory integration, and authentication methods. The following sections describe the configuration and usage of each platform.

Microsoft Entra ID (Azure AD)

Microsoft Entra (formerly Azure Active Directory) is a cloud platform which provides access management and identity provision. When integrated with the UCM6300 Series, it allows synchronizing the identity information with the UCM which can be used to log into the UCM's user interface.

For step-by-step configuration guide for Microsoft Entra, please refer to the following link: https://documentation.grandstream.com/knowledge-base/microsoft-entra-id-azure-ad-configuration-guide/

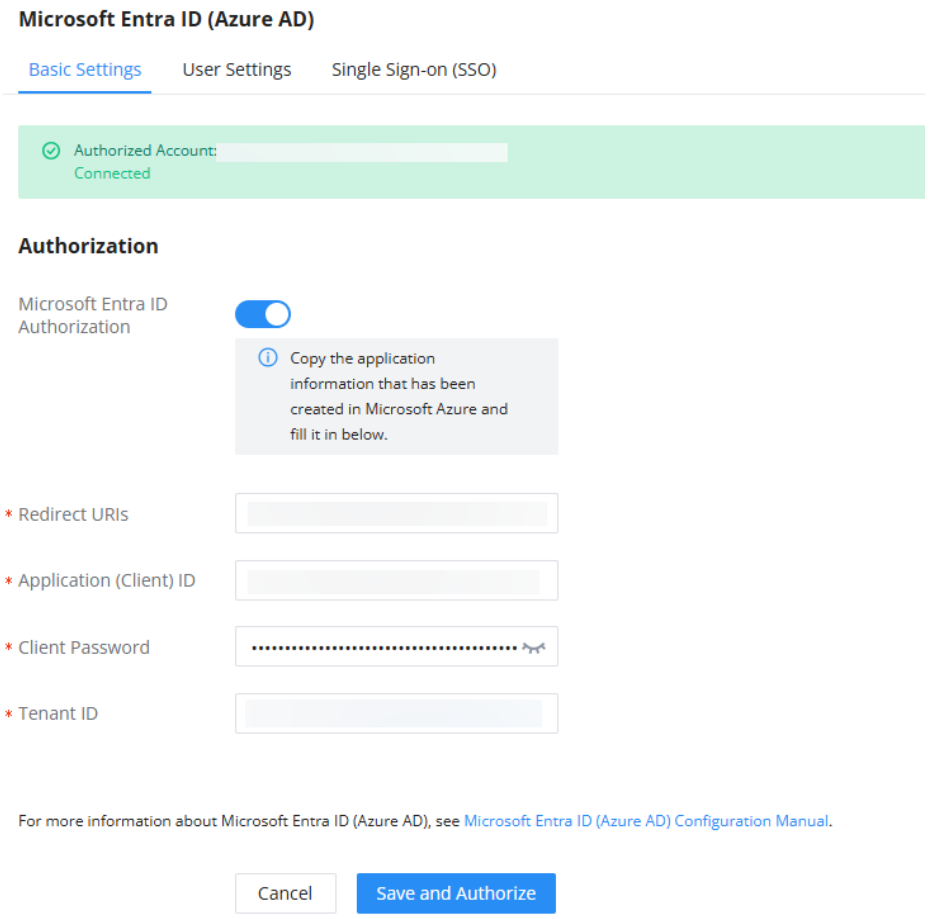
The Microsoft Entra ID configuration page consists of the following tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-On (SSO)**

Each tab is described below.

Basic Settings

This tab defines the connection between the UCM and Microsoft Entra ID.

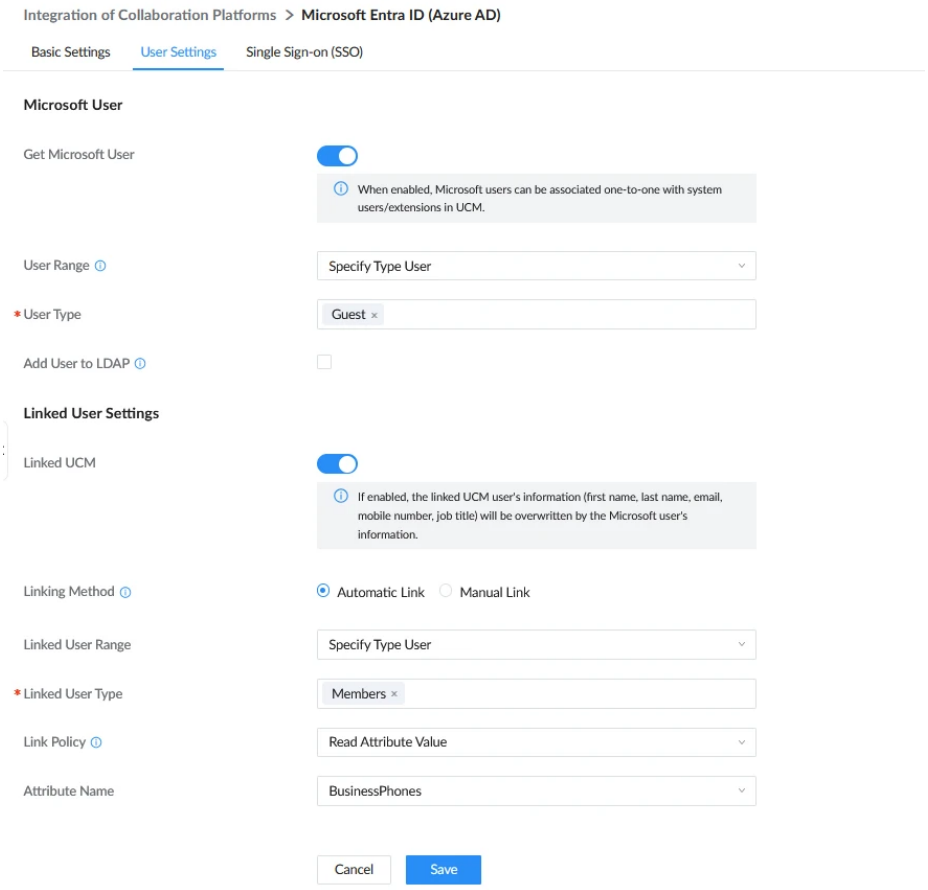


Microsoft Entra ID Basic Settings

Parameter	Description
Microsoft Entra ID Authorization	Enable Microsoft Entra ID
Redirect URIs	Enter a URI to return Microsoft tokens.
Application (Client) ID	Enter the application ID
Client Password	Enter the client password. If the client's password expires, this will interrupt Microsoft user synchronization. Ensure that the password is updated in a timely manner.
Tenant ID	Enter the tenant ID provided by Microsoft. This can be found in the admin center of Microsoft Entra ID.

User Settings

This tab controls how Microsoft users are synchronized to the UCM.



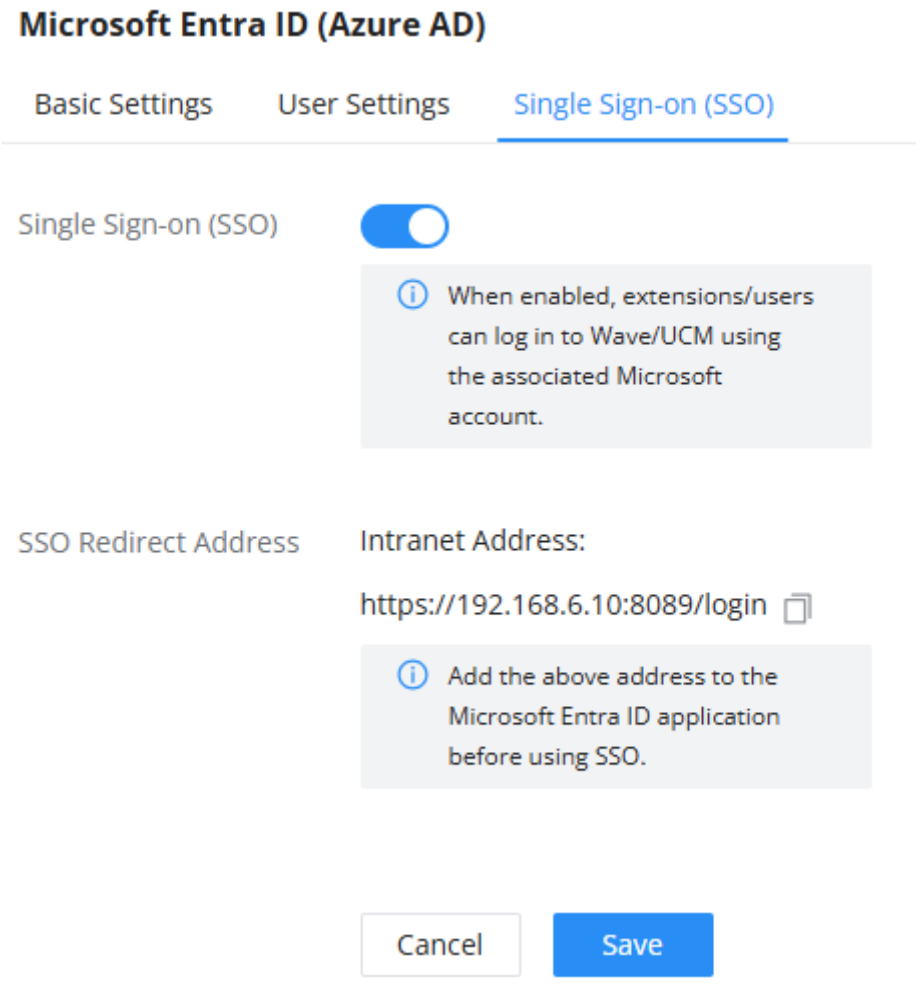
The table below describes the parameters available on this tab

Get Microsoft User	
Get Microsoft User	Enable to retrieve users from Microsoft Entra ID. When enabled, Microsoft users can be associated with UCM users/extensions. When disabled, synchronization is stopped.
User Range	Defines the scope of Microsoft users to retrieve. Options include retrieving all users or specifying user types.
User Type	Available when "Specify Type User" is selected. Defines which Entra user types (e.g., Members, Guest) will be retrieved. Only selected types are synchronized.
Add User to LDAP	When enabled, synchronized Microsoft users are added to the UCM LDAP directory, allowing them to appear in LDAP searches and dialing features.
Linked User Settings	
Linked UCM	Enable to associate Microsoft Entra users with existing UCM users/extensions. When enabled, the linked UCM user's information will be overwritten by the Microsoft user's information.
Linking Method	Defines how Microsoft users are linked to UCM users.Automatic Link: The system automatically matches Microsoft users to UCM users based on defined matching rules.Manual Link: Administrator must manually associate users.
Linked User Range	Specifies which UCM users are eligible for linking. Options include linking all users or only selected user types.
Linked User Type	Available when "Specify Type User" is selected. Defines the Entra user categories (e.g., Members) that are eligible for linking.
Link Policy	Defines how the extension number is assigned during automatic linking. Available options are:Automatic Allocation: assigns extensions sequentially, starting from a specified number.Read Attribute Value: The extension number is taken from a specified Microsoft Entra user attribute.

Starting Extension	Specifies the initial extension number used when Automatic Allocation is enabled under the linking policy.
Attribute Name	Available when Read Attribute Value is selected. Specifies which Microsoft Entra attribute will be used to determine the extension number.
Microsoft User	
Sync Now	Manually triggers immediate synchronization with Microsoft Entra ID based on the defined User Range.
Sync Settings	Opens synchronization configuration options.
Microsoft User List	Displays all retrieved Microsoft Entra users with the following fields:Microsoft Entra username (typically UPN).Display NameFirst NameLast NameJob TitleEmail (Entra ID Contact Email)Mobile NumberBusiness PhoneLink UCM User

Single Sign-on (SSO)

The SSO tab allows users to log into the UCM Web UI and Wave using Microsoft Entra authentication.



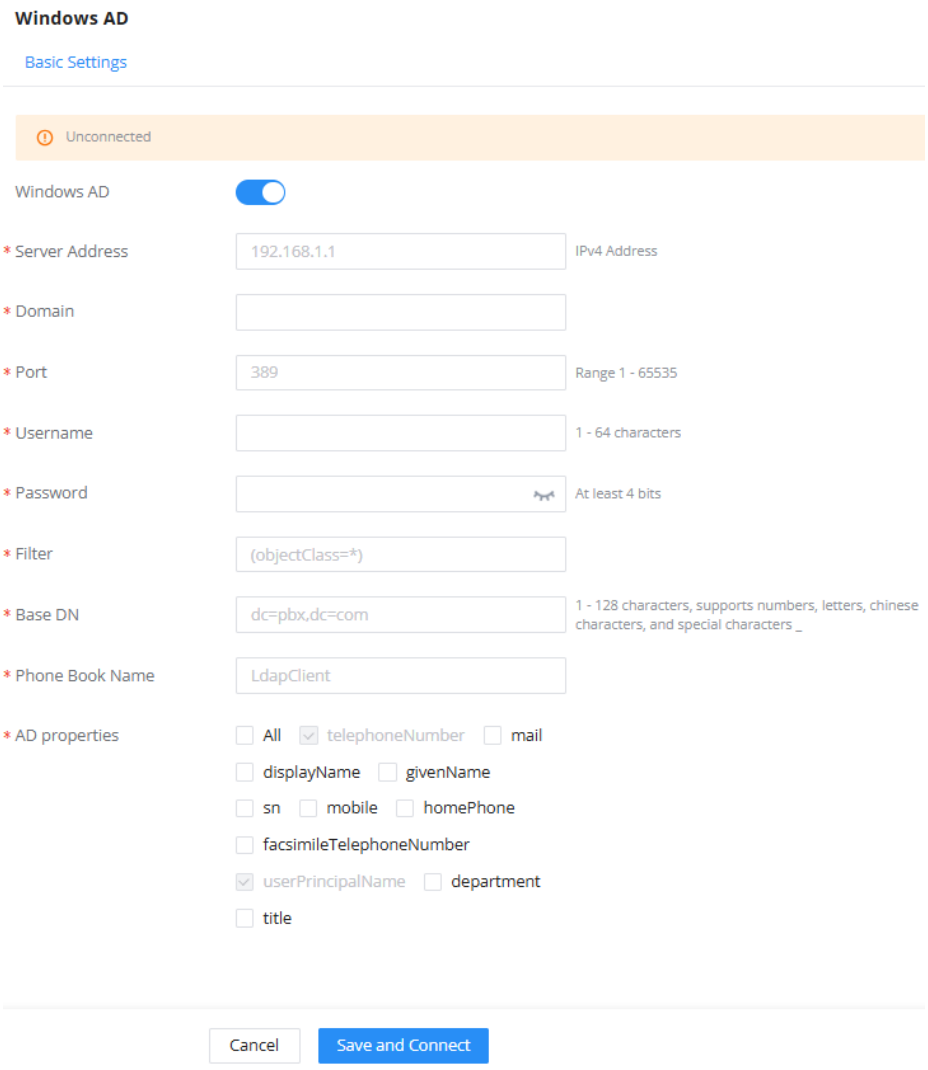
Windows AD

Integrating AD with the UCM allows the system to fetch and manage user data directly from the AD server, making it easier to maintain consistent user information across platforms. Contacts can be imported into the UCM's LDAP phonebook, and AD users can be linked to UCM extensions or system accounts for unified user administration. The integration also supports automatic and scheduled synchronization, reducing manual workload and keeping user records up to date.

Additionally, enabling Single Sign-On (SSO) allows AD users to log in to the UCM web interface using their

domain credentials, enhancing security and simplifying password management.

For step-by-step configuration guide for Windows AD, please refer to the following link: https://documentation.grandstream.com/knowledge-base/windows-ad-configuration-guide/

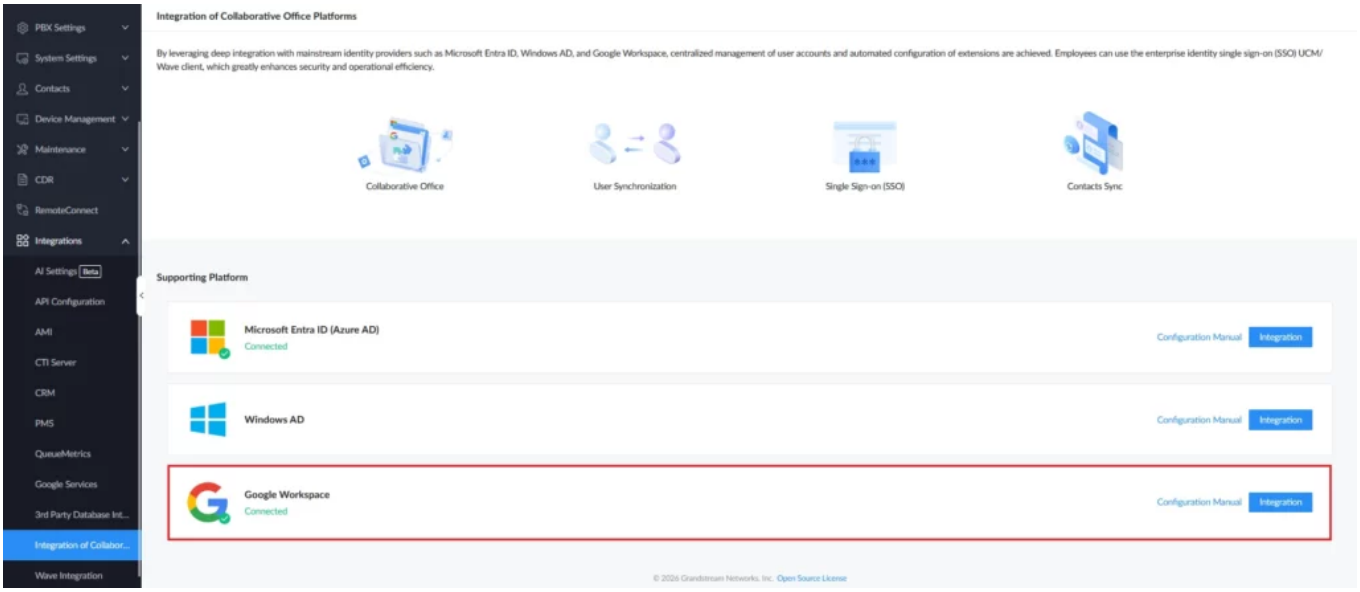


Parameter	Description
Windows AD	Toggle on/off the Windows AD integration
Server Address	Enter the AD server address.
Domain	Enter the domain
Port	Enter the port to use. The port number must be within the range 1 - 65535
Username	Enter the username.
Password	Enter the password.
Filter	Enter the filter which can be an object class.
Base DN	Information about the AD node to be pulled, for example,dc= pbx,dc=com.
Phonebook Name	Enter the phonebook name.
AD Properties	Select the AD properties which can be used by the UCM.

Google Workspace Integration

The Google Workspace Integration allows the UCM Series to connect with a Google Workspace domain in order to synchronize user identity information, enable Single Sign-On (SSO), and synchronize Google Calendar schedules with extension presence statuses. When enabled, Google users can be associated with UCM system users or extensions, optionally synchronized into the UCM LDAP directory, and used for authentication when accessing the UCM web interface.

This feature is configured under **Integrations->Integration of Collaborative Office Platforms->Google Workspace**.



Integration of Collaborative Office Platforms Page

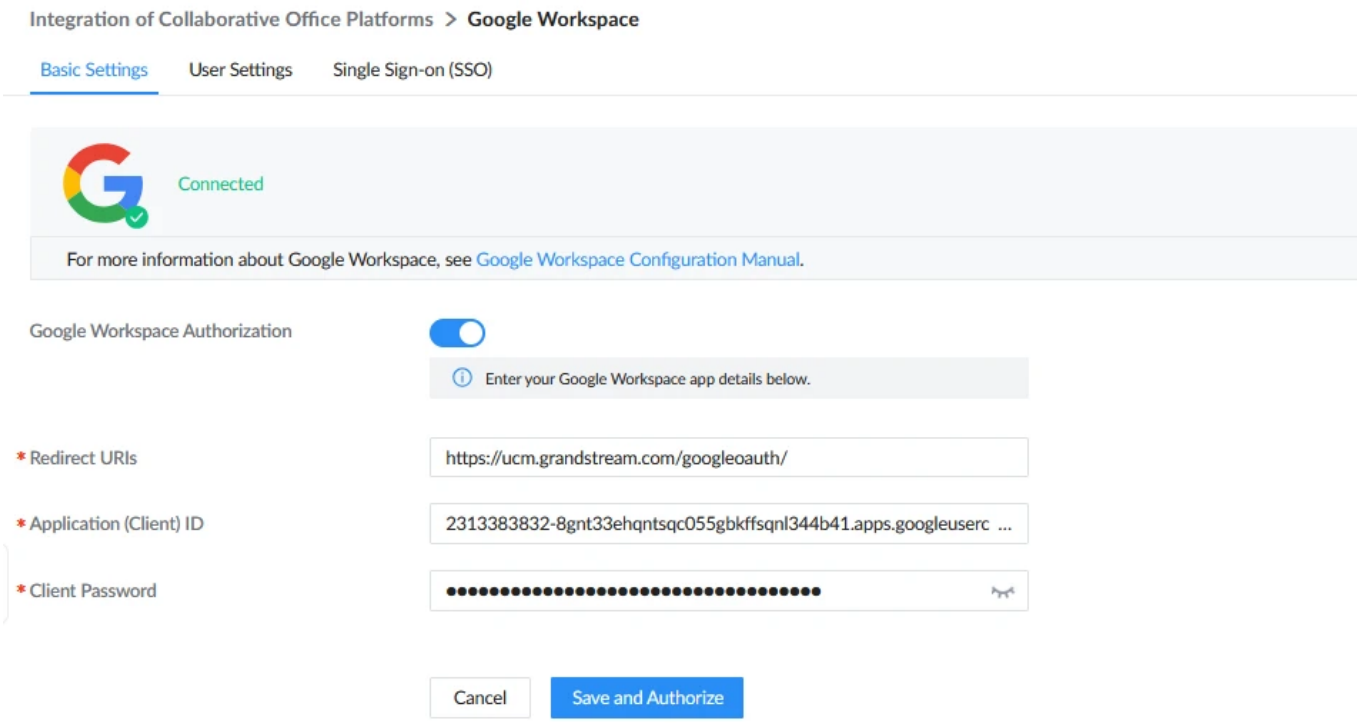
The Google Workspace integration module consists of four tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-on (SSO)**
- **Google Calendar**

For detailed configuration procedures refer to the **Google Workspace Integration Guide**.

Basic Settings

The Basic Settings tab is used to configure OAuth authorization between the UCM and Google Workspace. This step is mandatory before any user synchronization, SSO, or calendar functionality can be enabled.



Google Workspace Basic Settings Tab

The table below describes the parameters of this page:

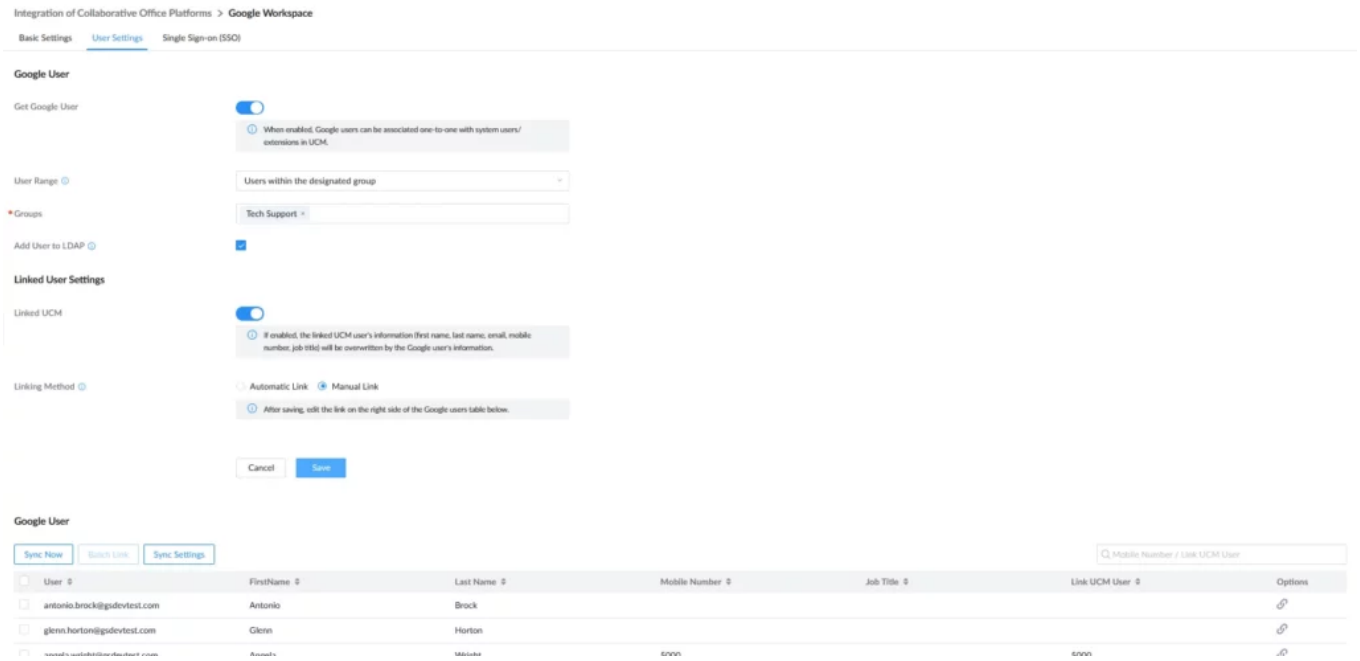
Parameter	Description
Google Workspace Authorization	Enables or disables Google Workspace integration on the UCM.
Redirect URIs	OAuth redirect URI used to receive authorization tokens from Google. This value must exactly match the redirect URI configured in the Google Cloud Console application.
Application (Client) ID	OAuth Client ID generated in Google Cloud Console for the Workspace application.
Client Password	OAuth Client Secret associated with the Client ID. If the client secret expires or is regenerated, it must be updated here to avoid authorization failure.

User Settings

The User Settings tab controls how Google Workspace users are retrieved, synchronized, and linked to UCM users or extensions. The settings on this page are grouped into three categories:

1. **Google User**
2. **Linked User Settings**
3. **Google User Management**

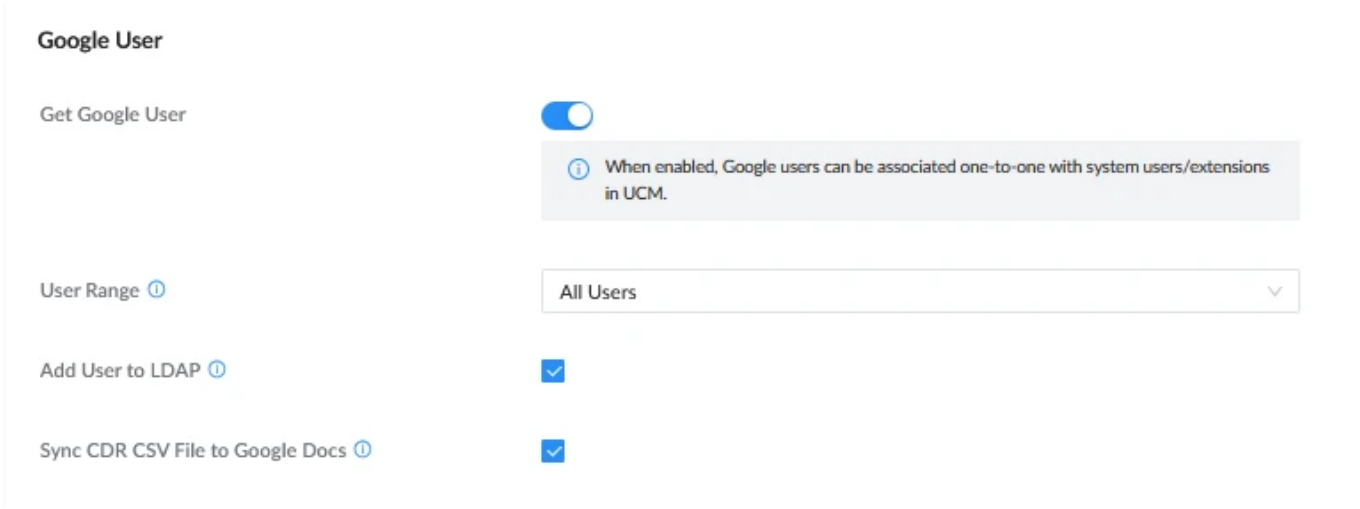
The sections below describe each of the Google Workspace user settings tab categories.



Google Workspace User Settings Tab

Google User

This section defines how Google Workspace users are retrieved from the domain and whether they are synchronized into the UCM system.

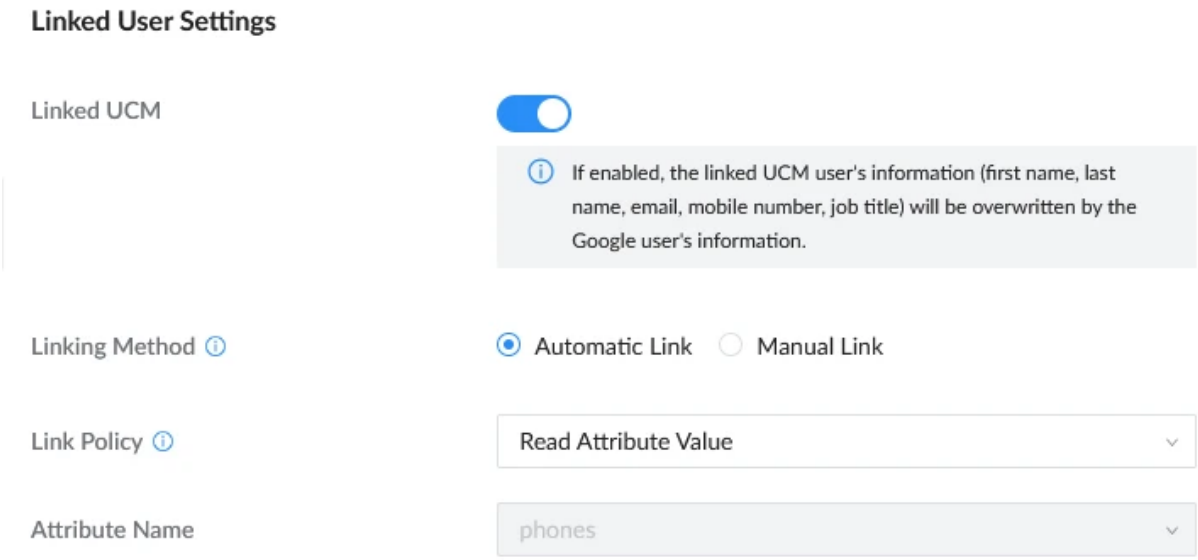


Parameter	Description
Get Google User	Enables/disables retrieval of users from the connected Google Workspace domain. When enabled, Google users can be listed and managed on the UCM.
User Range	Specifies the scope of Google Workspace users to retrieve. The available options are: All Users: Retrieves all users from the Google Workspace domain. Users within the designated organizational unit: Retrieves users from a specific Google Workspace organizational unit. Users within the designated group: Retrieves only users who belong to one or more specified Google Workspace groups.
Organizational Unit	Specify the Google Workspace Organizational Units whose users will be retrieved.
Groups	Specify the Google Workspace Groups whose users will be retrieved.
Add User to LDAP	When enabled, retrieved Google Workspace users are synchronized into the UCM LDAP directory under the "ou=google,dc=pbx,dc=com" phone book.

Sync CDR CSV File to Google Docs	When enabled, call detail records (CDR) exported as CSV files will automatically be synchronized and saved to Google Drive/Sheets.

Linked User Settings

This section controls how Google Workspace users are associated with UCM users or extensions.

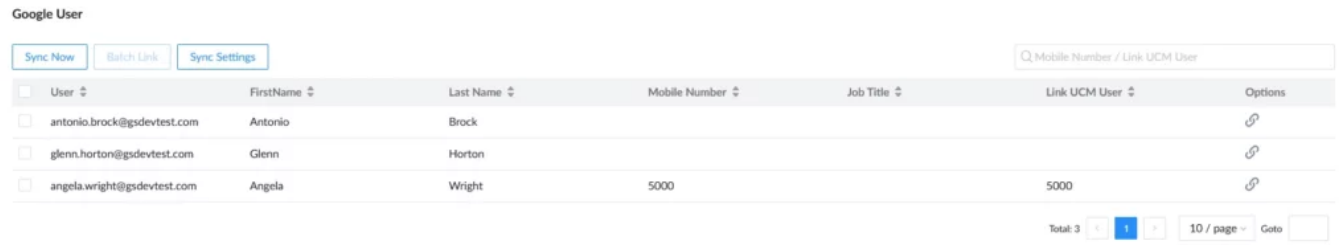


User Settings - Linked User Settings

Parameter	Description
Linked UCM	Enables linking between Google Workspace users and UCM system users or extensions. When enabled, selected Google user attributes (such as first name, last name, email address, mobile number, and job title) can be applied to the linked UCM user.
Linking Method	Defines how the association between Google users and UCM users is performed: Automatic Link: The UCM automatically links Google users to existing UCM users or extensions based on the selected link policy. Manual Link: Administrators manually associate Google users with UCM users or extensions from the Google User list.
Link Policy	Defines how the UCM determines the target UCM user or extension when Automatic Link is selected. Available options include: Automatic Allocation: The UCM automatically assigns available UCM users or extensions to Google users. Read Attribute Value: The UCM reads a specific Google user attribute (such as extension number or mobile number) and uses it to match an existing UCM user or extension.
Starting Extension	This field is displayed when Link Policy is set to Automatic Allocation. It defines the starting extension number that the UCM uses when automatically assigning extensions to Google Workspace users.
Attribute Name	Displayed when Read Attribute Value is selected. Specifies the Google Workspace user attribute that the UCM will use for automatic matching. Note: When Read Attribute Value is used for automatic linking, the UCM only evaluates the Work Number attribute from Google Workspace users. Mobile and Home numbers are ignored for automatic binding.

Google User List

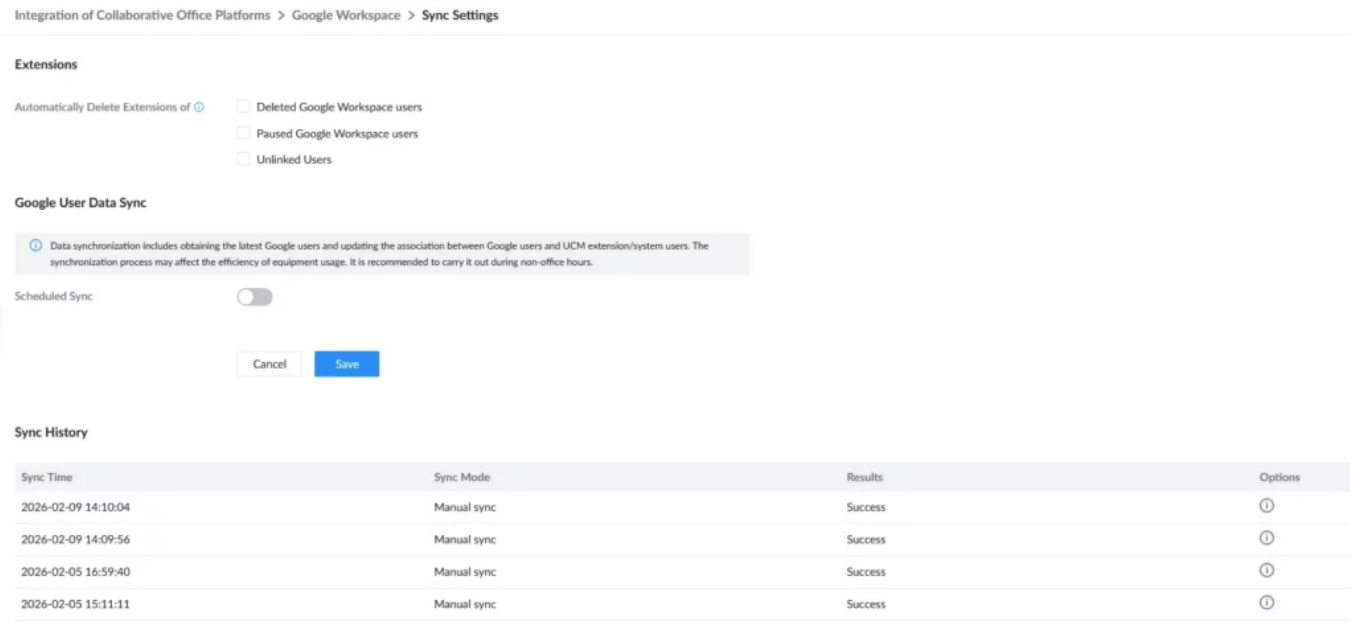
This section displays the list of retrieved Google Workspace users and provides controls for synchronization and user linking.



User Settings - Google User List

Parameter	Description
Sync Now	Immediately retrieves the latest user information from Google Workspace based on the current User Settings configuration.
Sync Settings	Opens the Google Workspace Sync Settings page, which allows configuration of automatic extension deletion policies (for deleted, paused, or unlinked Google users), scheduled synchronization, and provides visibility into synchronization history.
Batch Link	Available when Manual Link is selected. Allows multiple Google users to be linked to UCM users or extensions in a single operation.
Google User List Table Columns	User (email address) First Name Last Name Mobile Number Job Title Linked UCM User Note: For manually linked users, the Options column provides controls to link, modify, or remove the association with a UCM user or extension.

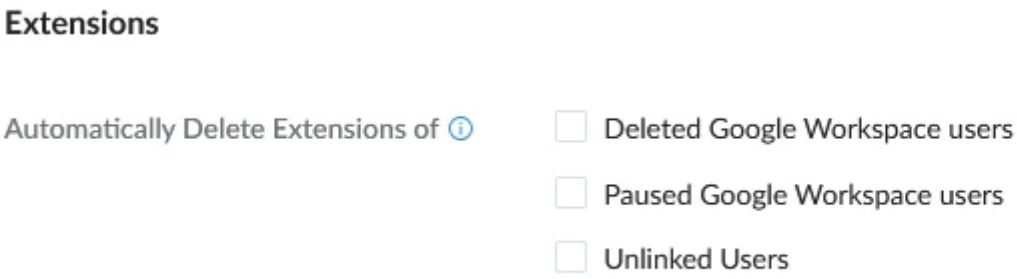
The **Sync Settings** page is used to define how Google Workspace user data is synchronized with the UCM and how linked extensions are handled during synchronization events. This page is accessed by clicking Sync Settings from the Google User List section.



Google Workspace Sync Settings

The **Extensions** section controls automatic cleanup behavior for UCM extensions based on Google Workspace user status:

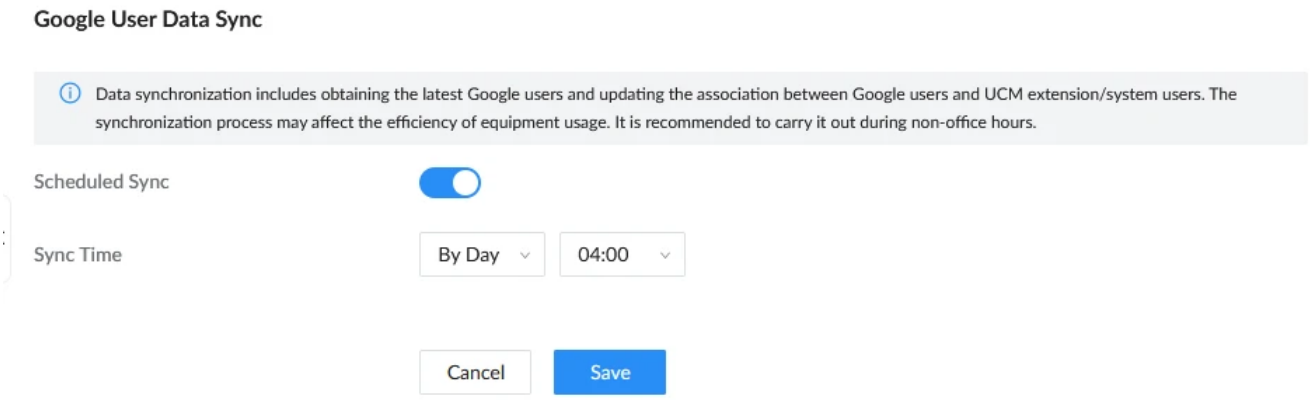
- **Deleted Google Workspace users:** Automatically deletes the linked UCM extension when the corresponding Google Workspace user is deleted.
- **Paused Google Workspace users:** Automatically deletes the linked UCM extension when the corresponding Google Workspace user is suspended or paused.
- **Unlinked Users:** Automatically deletes UCM extensions that are no longer linked to any Google Workspace user.



Extensions Sync Settings

The **Google User Data Sync** section controls how and when Google Workspace user data is synchronized. When **Scheduled Sync** is enabled, the UCM automatically retrieves the latest Google Workspace users and updates the association between Google users and UCM users or extensions according to the current configuration.

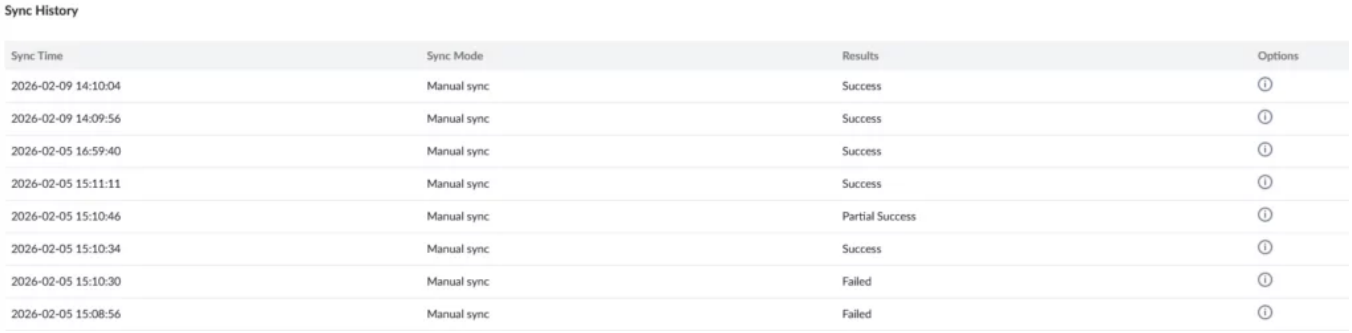
Data synchronization may temporarily impact system performance. It is recommended to perform synchronization during non-office hours.



Google User Data Sync Settings

The **Sync History** section displays historical records of Google Workspace synchronization activities. The following information is shown for each synchronization event:

- **Sync Time:** Date and time when the synchronization was executed.
- **Sync Mode:** Indicates whether the sync was triggered manually or by schedule.
- **Results:** Displays the synchronization result (Success, Partial Success, or Failed).
- **Options:** Provides access to detailed synchronization logs for troubleshooting purposes.



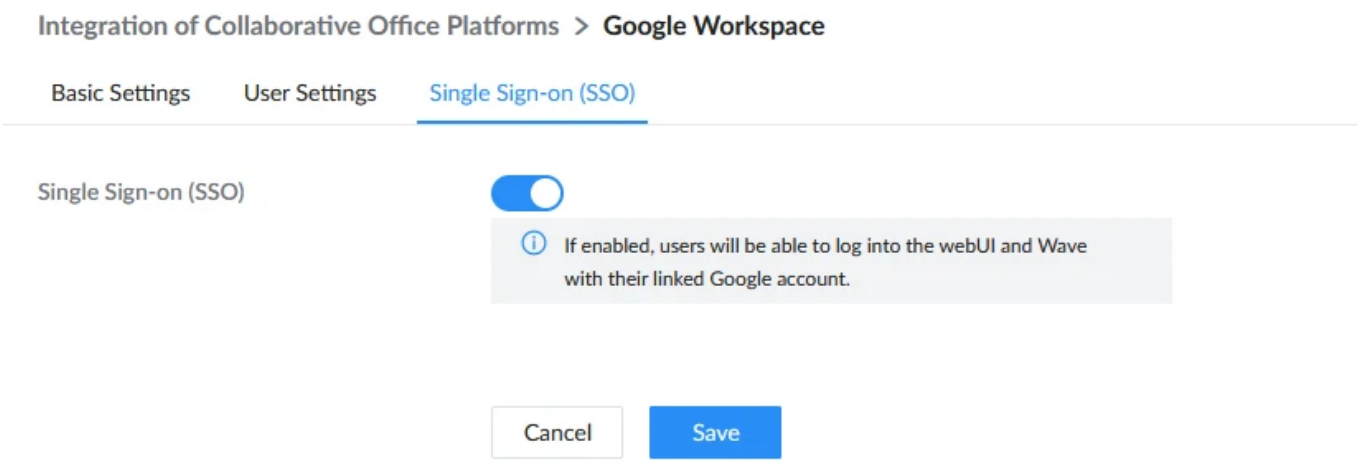
Google Workspace Sync History

Single Sign-On (SSO)

The Single Sign-On (SSO) tab controls Google-based authentication for accessing the UCM web interface.

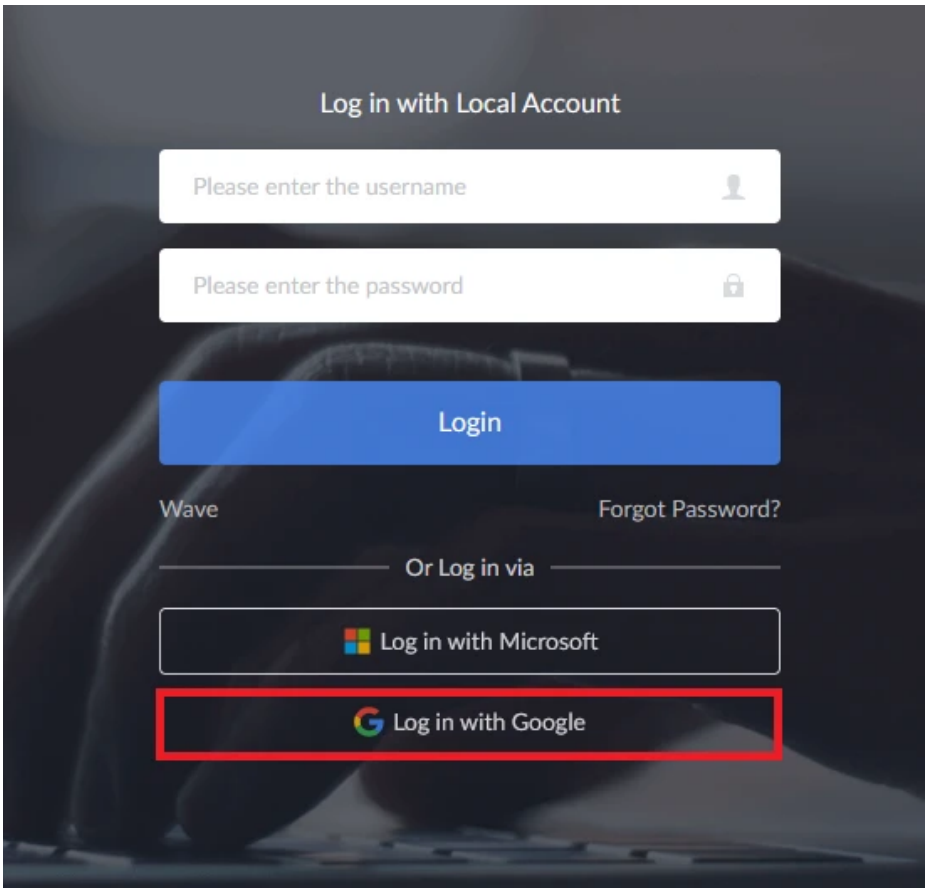
This page is used to enable or disable Google Workspace SSO and define how Google-authenticated users are mapped to UCM system users.

- For Google Workspace SSO to function, **at least one Google Workspace** user must be successfully linked to a UCM system user. SSO authentication will fail if no linked user exists.
- Google Workspace SSO requires the UCM to be accessed using **a valid domain name (FQDN)**. Accessing the UCM via a private IP address is not supported and will trigger a warning during OAuth authorization.



Google Workspace Single Sign-on (SSO) Tab

If SSO is enabled, the Sign in with Google option will appear on the UCM login page.

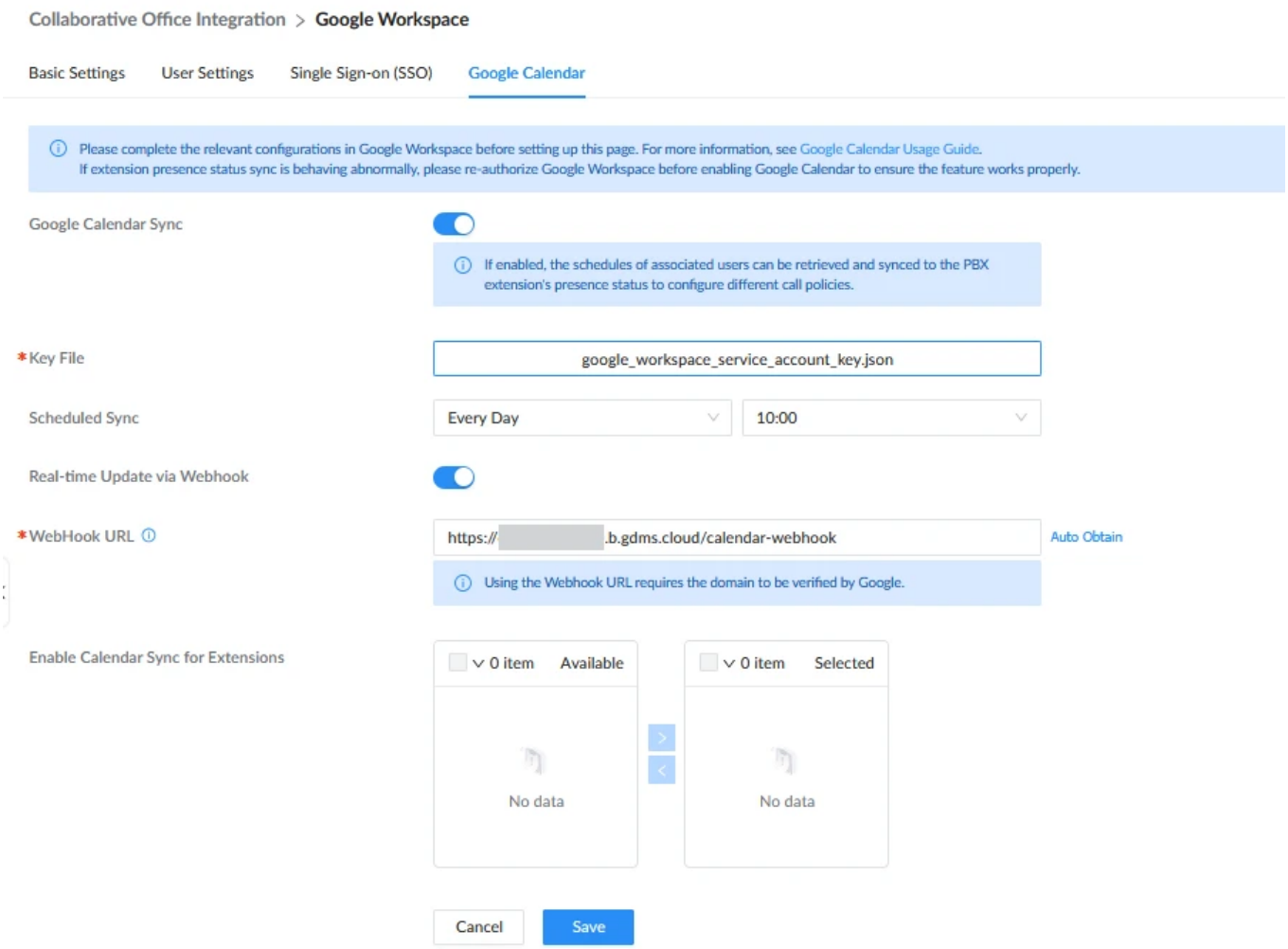


Log in with Google Option for UCM

Google Calendar

The Google Calendar tab allows administrators to synchronize Google Calendar schedules with PBX extension presence statuses, enabling automated call routing policies based on a user's calendar availability.

- Please complete the relevant configurations in Google Workspace before setting up this page. For more information, see the Google Workspace Integration Guide.
- If extension presence status sync is behaving abnormally, please re-authorize Google Workspace before enabling Google Calendar to ensure the feature works properly.



The table below describes the parameters available on the Google Calendar tab:

Parameter	Description
Google Calendar Sync	Enables or disables Google Calendar synchronization. When enabled, the schedules of associated users are retrieved and synced to PBX extensions' presence status to apply dynamic call policies.
Key File	Upload or select the service account JSON key file generated in Google Cloud Console for API authentication.
Scheduled Sync	Configures the periodic sync schedule (e.g., Every Day at a specified time) to fetch calendar updates.
Real-time Update via Webhook	Enables real-time event updates via Google push notifications using a Webhook URL.
WebHook URL	Specifies the Webhook URL used to receive real-time calendar updates. Clicking the Auto Obtain button automatically populates it with the UCMRC domain URL. Note: Using the Webhook URL requires domain verification in Google Console.
Enable Calendar Sync for Extensions	Select extensions from the Available list and move them to the Selected list to enable calendar-based presence sync for specific extensions.

Using the Real-time Update via Webhook feature requires domain verification in Google Search Console:

- **Custom Domain:** If using your own domain, follow the Google Search console instructions to to complete verification.
- **UCMRC Subdomain:** If using UCMRC domain, please contact Technical Support to assist with the verification.

When a scheduled event occurs on a linked user's Google Calendar, the UCM automatically updates the extension's SIP presence status to Do Not Disturb (DND) for the duration of the event window. Any call routing rules or forwarding policies configured for the DND status will apply automatically during the event.

SAML SSO

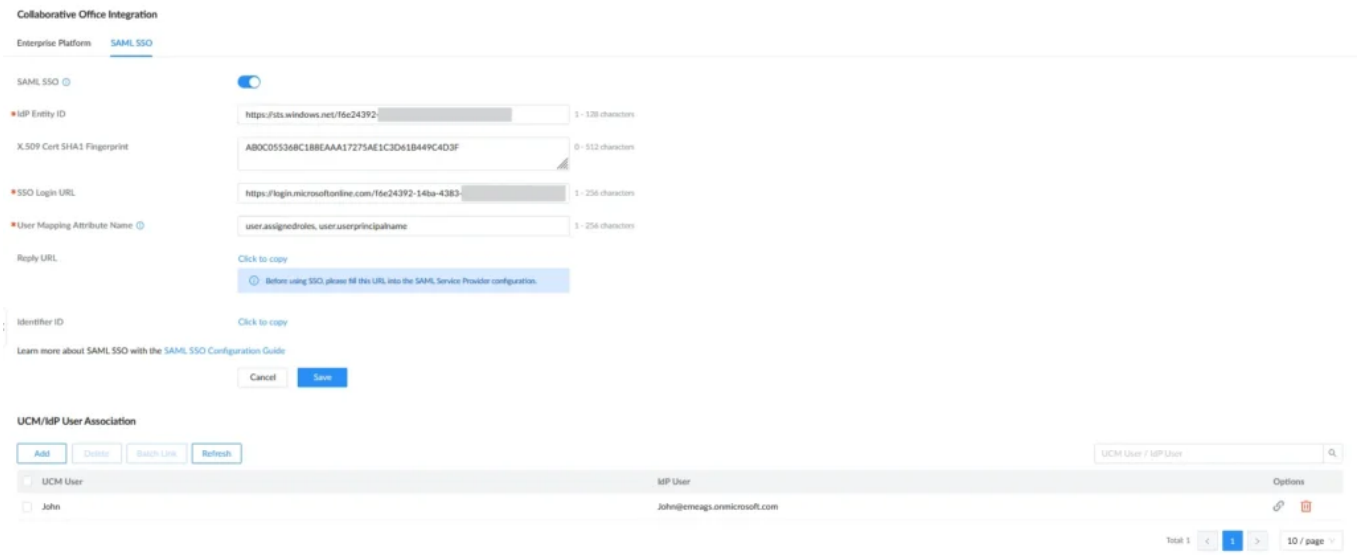
SAML Single Sign-On (SSO) is an enterprise-grade identity authentication solution that allows the UCM6300 series to integrate with external Identity Providers (IdP) such as Microsoft Entra ID, Okta, OneLogin, or AD FS. Once configured, users can authenticate via their organization's centralized identity provider to access the UCM Web UI without managing separate local credentials.

This feature is configured under **Integrations -> Integration of Collaborative Office Platforms -> SAML SSO**.

For step-by-step instructions on configuring external Identity Providers (Entra ID, AD FS, etc.) to pair with the UCM, please refer to the **SAML SSO Configuration Guide**.

SAML SSO Configuration

To enable SAML SSO, configure the Identity Provider credentials, Service Provider details, and user mapping rules under the SAML SSO tab.



SAML SSO Configuration Page

The table below describes the parameters available on the SAML SSO page:

Parameter	Description
SAML SSO	Enables or disables SAML Single Sign-On integration on the UCM.
IdP Entity ID	Enter the unique entity identifier (Issuer URL) provided by your Identity Provider. Used as a mechanism to validate SAML responses.
X.509 Cert SHA1 Fingerprint	Enter the SHA1 fingerprint of the IdP's X.509 signing certificate for response validation.
SSO Login URL	Enter the Single Sign-On service endpoint URL provided by your IdP where UCM will redirect authentication requests.
User Mapping Attribute Name	Specifies the attribute name on the IdP side used for user mapping. The value of this attribute for the IdP user must have a one-to-one correspondence with the UCM user/extension (it is recommended that the value be unique on the IdP side). Example: userName, email.

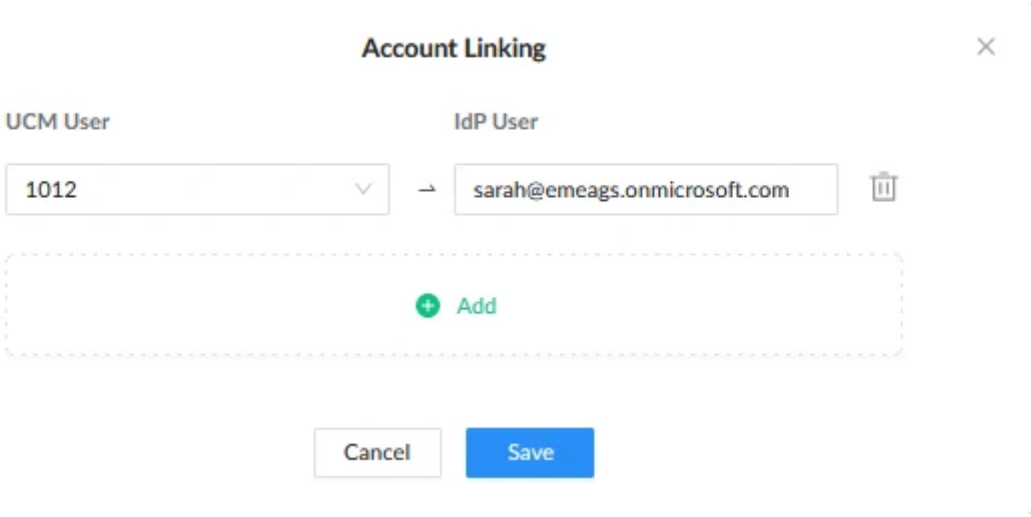
Reply URL	Use Click to copy to copy the Assertion Consumer Service (ACS) URL of the UCM and paste it into the SAML Service Provider configuration on the IdP side.
Identifier ID	Use Click to copy to copy the SP Entity ID of the UCM and paste it into the SAML Service Provider configuration on the IdP side.

Account Linking

Before users can log in via SAML SSO, their enterprise IdP attribute value must be mapped to a corresponding UCM user account.

To associate accounts:

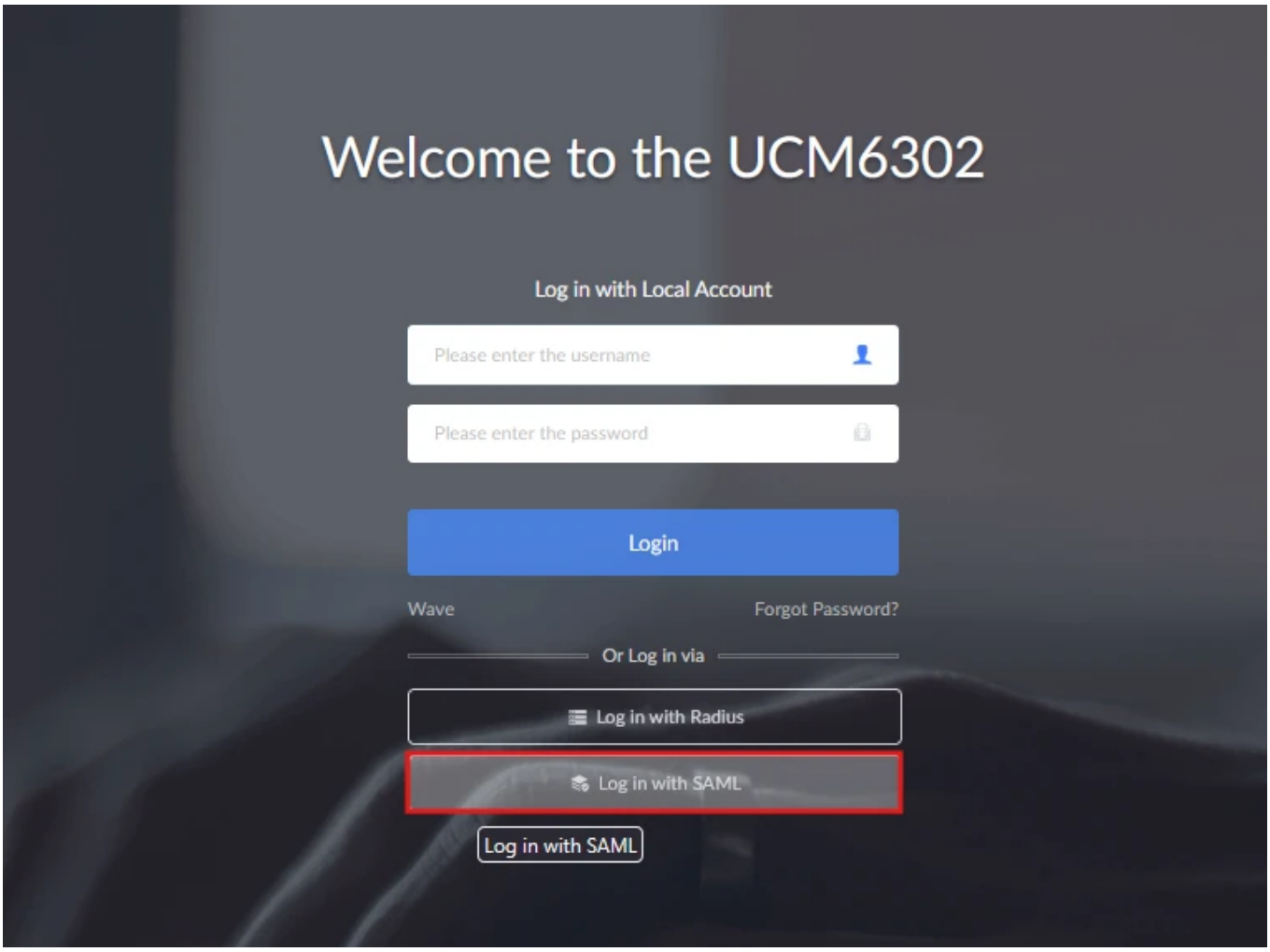
1. Click **Add** to open the Account Linking dialog.
2. Select the target **UCM User** from the drop-down menu.
3. In the **IdP User** field, enter the exact attribute value (e.g., user email address or username) corresponding to the configured User Mapping Attribute Name.
4. Click **OK** to save the association.



Account Linking Dialog

Logging in with SAML SSO

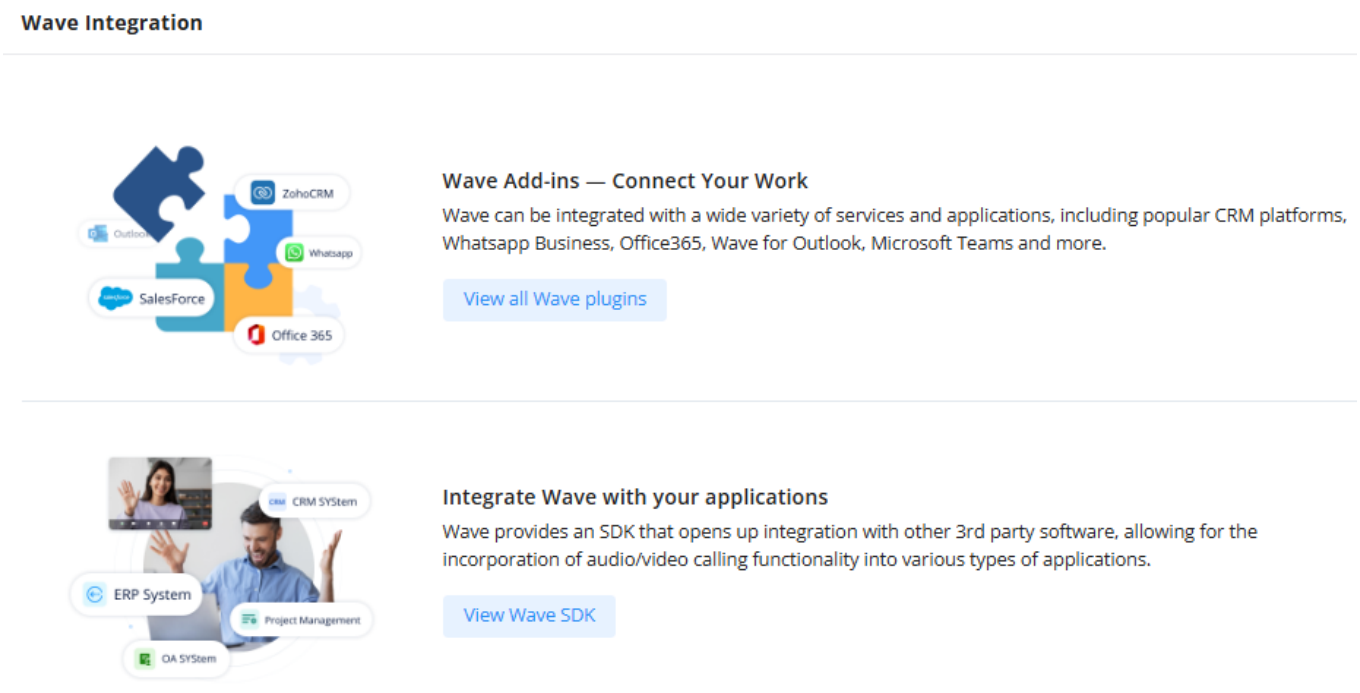
Once SAML SSO is enabled and user accounts are linked, a **Log in with SAML** option will appear on the UCM Web UI login page. Clicking this option redirects the user to the configured Identity Provider login page. Upon successful authentication, the user is redirected back to the UCM Web UI and logged in automatically.



UCM Login Page with SAML SSO

Wave Integration

In this page, the user can refer to links which include features and add-ons which provide powerful tools for communication and collaboration.



APPENDIX A: RFC STANDARDS USED IN UCM6300 SERIES

- **RFC 3261** SIP: Session Initiation Protocol
- **RFC 3262** Reliability of Provisional Responses in SIP
- **RFC 3263** Session Initiation Protocol (SIP): Locating SIP Servers
- **RFC 3264** An Offer/Answer Model with the Session Description Protocol
- **RFC 3515** The Session Initiation Protocol (SIP) Refer Method
- **RFC 3311** The Session Initiation Protocol (SIP) UPDATE Method
- **RFC 4028** Session Timers in the Session Initiation Protocol (SIP)
- **RFC 2976** The SIP INFO Method
- **RFC 3842** A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- **RFC 3892** The Session Initiation Protocol (SIP) Referred-By Mechanism
- **RFC 3428** Session Initiation Protocol (SIP) Extension for Instant Messaging
- **RFC 4733** RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
- **RFC 4566** SDP: Session Description Protocol
- **RFC 2617** HTTP Authentication; Basic and Digest Access Authentication
- **RFC 3856** A Presence Event Package for the Session Initiation Protocol (SIP)
- **RFC 3711** The Secure Real-time Transport Protocol (SRTP)
- **RFC 4582** The Binary Floor Control Protocol (BFCP)
- **RFC 4583** Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- **RFC 5245** Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- **RFC 5389** Session Traversal Utilities for NAT (STUN)
- **RFC 5766** Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- **RFC 6347** Datagram Transport Layer Security Version 1.2
- **RFC 6455** The WebSocket Protocol
- **RFC 8860** Sending Multiple Types of Media in a Single RTP Session
- **RFC 4734** Definition of Events for Modem, Fax, and Text Telephony Signals
- **RFC 3665** Session Initiation Protocol (SIP) Basic Call Flow Examples
- **RFC 3323** A Privacy Mechanism for the Session Initiation Protocol (SIP)
- **RFC 3550** RTP: A Transport Protocol for Real-Time Applications

CHANGELOG

This section documents significant changes from previous versions of the UCM630X user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.35.12

- No major change.

Firmware Version 1.0.35.8

- **Call Flow Design**
  - Added Visual Call Flow Design (Call Flow Design) to build complex call routing using drag-and-drop components. [Call Flow Design]
- **WhatsApp Trunk**
  - Added support for WhatsApp SIP Trunk integration and Wave WhatsApp calling support. [WhatsApp Trunk]
- **AI Features**
  - Added AI Translation feature for real-time translation of call/meeting transcripts and chat messages. [AI Translation]
  - Added AI Voice Assistant (Beta) support for controlling endpoints via voice commands. [AI Voice Assistant]
  - Added option to allow meeting summaries to be shared with all participants. [Schedule Meeting]
  - Added AI Recordings Transcription and Summary support for audio/video recording files. [AI Recording Transcription and Summary]
  - Added interactive synchronization between recording playback progress and AI transcript text. [AI Recording Transcription and Summary]
  - Added automated and manual cleanup options as well as backup and restore support for AI transcript files. [Cleaner][Backup/Restore]
  - Added feature code to start or stop AI call transcription during an active call. [Feature Codes]
  - Added User Portal support for playing and accessing AI transcriptions of voicemails. [AI Voicemail to Text]
  - Added noise suppression configuration for AI meeting transcriptions. [Schedule Meeting]
- **Collaborative Office Integration**
  - Added support for automatically syncing CDR CSV files to Google Docs via Google Workspace integration. [Google User][CDR Automatic Download]
  - Added support for SAML SSO authentication. [SAML SSO]
  - Added Google Workspace Calendar integration to dynamically map user calendar events to extension status. [Google Calendar]
- **Messaging**
  - Added support for Voxtelesys SMS provider integration. [SMS Configuration]
  - Added support for VoiceMeUp SMS provider integration. [SMS Configuration]

- Added Smart Call SMS Link Service to trigger automatic SMS messages with links via IVR key presses. [SMS Template]
- Added Message Edit/Delete Period option to the IM settings page. [IM Settings]

- **Call Queue**

- Added Wallboard feature to display real-time call queue metrics and agent status. [Queue Board]
- Added Queue Panel for interactive call management, agent status changes, and real-time monitoring. [Queue Operation Panel]
- Added dedicated Queue Permissions configuration to restrict control operations for chairmen and agents. [Queue Permissions]
- Added Queue CDR management with support for viewing, calling back, and tracking missed call processing status. [Queue Permissions]
- Added Priority Queue feature to dynamically assign call weights and route high-priority calls first. [Call Queue Configuration]
- Added time-based condition routing for call queues during out-of-office hours or holidays. [Call Queue Configuration]
- Optimized virtual queue timeout triggering logic and updated user interface. [Call Queue Configuration]
- Added "Skip Busy Agents" option to allow or prevent ringing call queue agents who are currently in a call. [Call Queue Configuration]
- Removed Queue Switchboard to be replaced with Queue Operation Panel. [Queue Operation Panel]
- Added custom user permissions for Queue Wallboard and Queue Operation Panel. [Add Custom Privilege]

- **PMS**

- Added Local PMS unique order ID generation for reservation tracking across lists and invoices. [Local PMS]
- Added Local PMS read-only historical reservation views to prevent accidental data changes. [Local PMS]
- Added Local PMS overdue reservation filtering to identify guests who failed to check in on time. [Local PMS]
- Added global Local PMS reservation time settings to configure default daily check-in/check-out times and set allowed thresholds for earliest check-in and latest check-out. [Local PMS]
- Updated Local PMS multi-room reservations to preserve checked-in room rates when reservation prices are modified. [Local PMS]
- Added a dedicated refresh button to the Local PMS Room Availability Calendar for real-time updates. [Local PMS]
- Added tax-inclusive rate displays for active bookings on the Local PMS Room Availability Calendar. [Local PMS]
- Added Local PMS hour-room management rules restricting room changes after check-in. [Local PMS]
- Added mandatory base price requirement when enabling Local PMS hourly rental option. [Local PMS]
- Added customizable hotel branding logo, phone numbers, and websites to Local PMS bill printing. [Local PMS]
- Added Local PMS auto-assign room button for automated room selection during reservation creation. [

Local PMS]
  - Added itemized tax, room charge, and minibar breakdowns to Local PMS bill printing. [Local PMS]
  - Added Local PMS support for custom hotel branding (logo, phone number, website, and QR code) in self-check-in and self-check-out emails. [Local PMS]
  - Added custom permission controls for PMS Basic Settings and Minibar management. [Add Custom Privilege]
- **Zero Config**

  - Added support for batch local firmware upgrades via Zero Config. [Firmware]
  - Added Zero Config support for Avaya IP phones. [Zero Config Supported Devices]
  - Added Zero Config multi-account configuration support for Poly Edge B Series IP phones. [Zero Config Supported Devices]
  - Added Zero Config support for Grandstream HT and GXW gateways. [Zero Config Supported Devices]
  - Added support for Cisco phone DND and Conference features. [Zero Config Supported Devices]
  - Added support for Cisco CP-6921 and CP-3905 IP phones. [Zero Config Supported Devices]
- **CRM**

  - Added Custom CRM Integration interface, custom templates, OAuth2/Bearer Token options, and import/export capabilities. [CRM]
- **VoIP Trunk**

  - Added option to select whether to use DOD numbers when "Keep Original CID" is enabled on SIP trunks. [VoIP Trunks]
  - Added "Not Passthrough" option and refined configuration for Diversion headers on SIP trunks. [VoIP Trunks]
- **Inbound Routes**

  - Added support for custom Inbound Mode names and audio prompts for mode switching. [Inbound Route: Multiple Mode]
- **Outbound Routes**

  - Added Diversion ID Manipulation settings (strip and prepend) for outbound routes. [Configuring Outbound Routes]
- **User Management**

  - Added global configuration option to restrict users from modifying their extension email addresses. [User

Portal/Wave Privileges]

  - Added Multi-Factor Authentication (MFA) login support for User Portal. [Create New SIP Extension]
- **Upgrade**

  - Added interactive feature highlights guide on new system updates for administrators. [New Feature Guide]
- **Backup**

  - Added support for incremental backup tasks for CDR, queue statistics, and recording files. [Backup/Restore]
- **Storage Device Management**

  - Added support for SMB 3.0 protocol for network disk storage. [NAS]
- **System Cleanup/Reset**

  - Increased maximum automatic cleanup retention period to 730 days. [Cleaner]
- **System Events**

  - Added alert notifications when outbound call duration thresholds are exceeded on outbound routes. [Alert Events List]
- **System Events**

  - Added CISA security reminders for users to change SIP and User Portal/Wave passwords and to enable MFA. [User Portal/Wave Privileges][Multi-Factor Authentication]
- **Voicemail**

  - Optimized voicemail audio encoding format terminology in the web interface. [Configure Voicemail]
- **Fax/T.38**

  - Added support for configuring a unified administrator email address for failed Email-to-Fax notifications. [Email Settings]
- **Meeting**

    - Added support for including UCM Station IDs in random meeting room numbers for cross-PBX routing. [General Settings][Meeting Settings]
- **CDR**

    - Added Call Notes and Labels feature for tagging and adding comments to call records. [CDR][Call Note]
- **IVR**

    - Added support for configurable IVR end keys (including #). [Key Pressing Events]
- **Emergency Calls**

    - Added option to configure whether Geolocation-Routing headers are included in emergency call location mapping. [Emergency Location Mapping]
- **Voicemail**

    - Added support for feature code *99 to record and modify Voicemail Group prompts. [Feature Codes][Voicemail Groups]
- **Announcement**

    - Added call permission configuration for Announcements when the destination is set to an external number. [Announcement]
- **Time Settings**

    - Added custom prompt support for holiday events in Time Settings. [Holiday]
- **SIP Settings**

    - Added option to enable blind transfers while the callee's phone is still ringing. [Misc]
- **WebRTC Trunk**

    - Added WebRTC Trunk one-click dialing mode and script-based integration code. [WebRTC Trunks]
- **Dashboard**

    - Added Storage Health display to dashboard. [Dashboard]
- **RemoteConnect**

    - Retired Click2Call option while preserving existing configurations for legacy setups. [Integrated Customer Service]
- **PBX Settings**

    - Moved Enterprise Contact Number field to PBX Settings->General Settings. [General Settings]

Firmware Version 1.0.33.42

- Added support for call queue reports. [Call Queue Reports]
- Added support for scheduling call queue reports. [Scheduled Report]

Firmware Version 1.0.33.32

- No major changes.

Firmware Version 1.0.33.30

- Added AI configuration tab to SIP extensions, allowing per-extension control of Automatic AI Transcription. [Create a New SIP Extension]
- Added scheduled meeting configuration with AI transcription option, allowing organizers to enable or disable AI transcription per meeting. [Schedule Meeting]
- Added AI Settings (Beta) page to centrally manage AI services. [AI Settings (Beta)]
- Added RemoteConnect AI Services page to display AI service status, plan validity, and detailed usage statistics [AI Services]
- Added support for AI Call Transcription & Summary. [AI Call Transcription and Summary]
- Added support for AI Conference Transcription & Summary. [AI Meeting Transcription and Summary]
- Added support for AI Voice Message to Text. [AI Voice Message to Text]
- Added AI Generated Speech (TTS) feature for creating voice prompts directly from text. [AI Generated Speech]

Firmware Version 1.0.33.22

- No major changes.

Firmware Version 1.0.33.21 (BETA Only)

- Added several new call report types for various call scenarios [Call Reports]
- Added support for Cisco CP69xx/78xx/88xx endpoints DND. [Extensions]

Firmware Version 1.0.33.7 (BETA Only)

- Added Strict Defend Mode option to Geo-IP Access Control [Geo-IP Access Control]
- Added unified Integration tab for collaboration and identity platforms. [Integration of Collaboration Platforms]
- Added support for Google Workspace integration to synchronize user identity information between Google Workspace and the UCM Series. [Google Workspace Integration]
- Added Google Workspace Single Sign-On (SSO) support for UCM web interface authentication. [Google Workspace Integration]
- Added support for configuring Microsoft Entra ID user synchronization scope. [Microsoft Entra ID (Azure

AD)]

- Added support for configuring holidays by date or by week. [Holiday]
- Increased the maximum size limit for backup files uploaded to the UCM via the Web GUI. [Restore Configuration from Backup File]
- Added Zero Config support for Yealink IP phones. [Zero Config Supported Devices]
- Updated the Local PMS wake-up service prompt to dynamically use the language configured during room check-in. [Local PMS]
- Optimized Local PMS check-in and check-out actions to take effect immediately without requiring "Apply Changes". [Local PMS]
- Added option to control Wave app Screenshot and Screen Recording permission. [Wave Permissions]
- Added support for configuring whether the Wave external host address is automatically synchronized from UCMRC. [Plan Settings][HTTP Server]
- Added support for Bitrix24 CRM integration. [Bitrix24 CRM]
- Added support for network abnormality HA switchover. [HA Settings]

Firmware Version 1.0.31.7

- Added support for third-party SQL database integration for phonebook lookup and synchronization. [3rd Party Database Integration]
- Updated the Inbound Routes->3rd Party Database Search page to align with the new third-party SQL database integration feature. [Inbound Routes: 3rd Party Database Search]
- Added support for enabling local HA while operating in Dual network mode. [HA Settings]
- Added third-party SIP Phone support (Cisco/Poly). [Zero Config Supported Devices]
- Added vendor and model search capability when downloading model templates. [Model Update]
- Increased maximum Zero Config firmware upload size to support larger GXV series firmware packages. [Firmware]
- Added configurable room types with support for day-based pricing, holiday pricing, tax rates, and hourly pricing. [Local PMS]
- Added reservation management. [Local PMS]
- Added a guest list for centralized customer profile management, including search, import/export. [Local PMS]
- Added email templates for reservation notifications, cancellation notices, and billing emails. [Email Template]
- Added multiple check-in workflows, supporting check-in from reservation list, from room list (immediate check-in), and hourly or full-day room selection. [Local PMS]
- Added room change (house switch) functionality to move checked-in guests to another available room while preserving guest and billing data. [Local PMS]
- Added a room availability calendar with visual status indicators, booking and check-in actions, hover-based detail display. [Local PMS]
- Added bill printing with detailed room charges, minibar costs, call charges, tax breakdowns, and prepayment deductions. [Local PMS]
- Added wake-up service management with support for room group based scheduling. [Local PMS]
- Added support for self-service check-in and chek-out via email for guests with valid reservations. [Local PMS]
- Added configurable email delivery timing for self-service check-in and check-out messages relative to arrival and departure times. [Local PMS]
- Added tracking of check-in and check-out methods, distinguishing between front-desk and self-service operations in history records. [Local PMS]
- Added automatic room assignment during self-service check-in when reservations are not pre-assigned to

specific rooms. [Local PMS]

- Added support for DOD numbers batch deletion. [Direct Outward Dialing (DOD)][Outbound Routes DOD]
- Added support for inbound and outbound routes batch deletion. [Configuring Inbound Routes][Configuring Outbound Routes]
- Added outbound route total call duration limit setting. [Configuring Outbound Routes]
- Added display of trunk status and current call count display on the VoIP Trunk page [VoIP Trunks]
- Added Caller ID Manipulation feature on outbound routes [Configuring Outbound Routes]
- Added support for data backup and archiving to third-party cloud storage (Amazon S3). [Amazon S3]
- Add the ability to play/hear the uploaded Prompts directly from the WebGUI. [Custom Prompt]
- Added support for manual addition of Fail2Ban blocklist entries. [Fail2Ban]
- Added Cleaner Record and Details [Cleaner]
- Added the ability to have multiple Scheduled Backup tasks on different storage locations. [Scheduled Backup][Backup/Restore]
- Added ability to modify LDAP phonebooks through API. [API Queries Supported]
- Added support for adding LDAP contacts as members of paging/intercom groups to 2-way intercom and 1 way paging. [LDAP Members]
- Added support for proficiency-based routing as a routing strategy in the call queue. [Proficiency Routing]
- Added selecting the dynamic agents which can be added to a specific call queue. [Dynamic Agents]
- Added recording file and CDR access permission. [View Team CDRs and Recordings]
- Added Wave recording indicator appearance permission. [Recording Status]
- Added support for configuring the pre-installed Wave add-ins. [Pre-intalled Plugins]
- Added support for multifactor authentication using email for Wave. [Multifactor Authetication]

Firmware Version 1.0.29.21

- Some general call failure prompt tones (e.g., no-answer, user-busy, no-permission, wrong-number, general-failed) can now be used for SIP trunk call failure messages. [SIP Trunk Prompt Tone]

Firmware Version 1.0.29.19

- Added Advanced Messaging page under the Sidebar->Messaging section. [Advanced Messaging]
- Added option to the PBX->General Settings page to set prefixes that will allow the UCM to distinguish and definitively label different types of calls (i.e., local calls, long-distance calls, and international calls) for call billing purposes (Only applicable for Oracle Hospitality's OPERA PMS). [International Call Prefix] [Domestic Long Distance Call Prefix] [Local Area Code]
- Added support for Oracle Hospitality OPERA's Youth Hostel Mode, which divides individual rooms into multiple units to account for multiple different groups and separate billing within the same room. [Oracle Hospitality OPERA]

Firmware Version 1.0.29.11

- UCM6300 Series now support provisioning through GDMS Unified Communications. [PROVISIONING]
- Added Least Cost Routing policy to Outbound Routes [Carrier]
- Added support for call billing [Call Rate]
- The administrator can choose to prioritize call pattern matching or outbound route priority order as the criteria for call routing [Outgoing Routing Priority]
- Added a configuration field to enter maximum concurrent calls allowed by a SIP trunk. [VoIP Trunks]
- Added ability to select the error message to display when the number of maximum concurrent calls is achieved. [VoIP Trunks]
- Added support for enabling/disabling sending the diversion header on a particular trunk. [VoIP Trunks]
- Added support for Microsoft Entra ID integration, this allows synchronizing SIP accounts from LDAP or

Active Directory for single sign-on. [Microsoft Entra ID (Azure AD)]

- Added support for Active Directory to synchronize user accounts (user portal and Wave login) and admin accounts. [Windows AD]
- Added support for detecting new firmware directly from the web UI, regular firmware version checking can be scheduled on the webUI. [Upgrade]
- Added country-specific restriction in ACL [Country/Region IP Defense]
- Added support for automatic update of the timezone list [Automatic Date and Time]
- Service ports can now be configured. [Port Management]
- Added a link to the Open Source Software License Agreement [Open Source License]
- Administrator password, user password, and SIP password now require at least 10 characters [Create New SIP Extension][User Management]
- Added TLS compression for LDAP server [LDAP Server Configurations]
- Backup allows now excluding instant messages [Backup]
- The dashboard now displays the physical port name [Dashboard]
- Added Call Policy [Create New SIP Extension]
- Added name configuration in Speed Dial [Speed Dial]
- Added "First Answer Termination" in Paging configuration [Paging/Intercom Groups]
- Added Call Privilege to Announcement Center [Announcement Center Settings]
- Increased voicemail group members number to 150 [Configure Voicemail Group]
- CDR now displays the name of the callee
- Added prompt language configuration in Call Queue [Add Call Queue]
- Call Queue Chairman can now view the CDR of their queues
- Added option to disable RPID in the Call Queue [Add Call Queue]
- ELIN field in Emergency calls now can be configured with more character, letters and numbers [Emergency Location Mapping]
- Add the ability to support Emergency Location Mapping based on a single Extension approach for the Emergency calls feature [Emergency Location Mapping]
- Added default emergency callID field for Extension's autopopulate [Emergency Location Mapping]
- Added ability to customize PAI for Emergency Calls in multi-site environment [Emergency Location Mapping]
- Added Oracle Hospitality OPERA PMS integration [Oracle Hospitality Opera]
- PMS parameters have been added to list of privileges for admins [Custom Privilege]
- Added ability to use key pressing events when receiving a wake up call. [Wakeup Service]
- Added support for configuring the allowed API modules when adding a user [API Configuration Parameters]
- The administrator can now configure up to 10 subnets on Zero Config whitelist [Zero Config Settings]
- Administrator can now use MAC OUI to scan only certain manufactorer devices. [Discovery]
- Updated email template for "new messages to inactive user notification" [Email Template]
- Added "Delete message" Wave permission. [User Portal/Wave Privileges]
- Added "Allow Simultaneous Logins from the Same Client Type" Wave permission [User Portal/Wave Privileges]
- Added "Play Joining/Leaving Meeting Announcement" which enables/disables the sound played when a user joins/leave [Schedule Meeting]
- Added end time for scheduled meetings [Schedule Meeting]
- Meeting will now end when a GDS or GSC extensions are the only ones left in the meeting
- Added event alert in case synchronizing files to cloud storage fails [Alert Events List]

- GDMS cloud storage security key is now hidden by default and can be revealed after clicking on the corresponding button [GDMS Cloud Storage Space]
- Added compatibility for GDMS configuration template for the UCM6300 Series
- Import and export functions now support XLSX file format
- Backup packages now use TGZ format by default instead of TAR
- Restore feature now supports TGZ file format
- Added support for triggering webhooks via an IVR [Configure IVR]
- Added Background Sound to Multicast Community [Multicast Community]
- Added LinkedID to CDR AMI event reporting for improved call tracking and management
- Added Premium Code and and Premium Code Prompt option to Advanced Settings page. The user can use the premium code to increase their priority in the queue. [Add Call Queue]
- Administrators can now choose either dial plan accuracy or outbound route priority list as the criteria for call routing. [Outgoing Routing Priority]
- Added support for backing up video files to GDMS [File Manager]

Firmware Version 1.0.27.20

- Added support for Microsoft Outlook SMTP OAuth2 authentication. [Email Settings]

Firmware Version 1.0.27.15

- No major change

Firmware Version 1.0.27.10

- Added QR code to email template for quick SIP registration [Email Template]
- Added Account SIP Trunk [Account SIP Trunk]
- Added VoIP VLAN [Network Settings]
- Added support for searching CallerID in a third-party MySQL database [Inbound Route: Third-party Database Search]
- Added support for integration with Don't Call Me database [Don't Call Me Blacklist Integration]
- Added support for ZRTP on the extensions level [Create New SIP Extension]
- Added support for ZRTP on the trunk level [VoIP Trunk Configuration]
- Added support for enabling multiple Wave session on the same platform [Create New SIP Extension]
- Added support for verifying ACS [TR-069]
- Added support for Tx and Rx Noise Cancellation in Analog Trunks [Analog Trunk Configuration]
- Added Task Management feature [Task Management]
- Added support for search function in LDAP server phonebooks [LDAP Phonebook]
- Added support for data encryption on the local storage and attached storage [Data/File Encryption]
- Password Visibility Toggle has been added to the Admin privilege [Super Administrator]
- Added Merge Same Call Recordings setting [PBX SETTINGS]
- Added support for adding suffix to Call Forward Enable/Disable feature [Feature Codes]
- Added icons next to feature codes to indicate whether or not they can be nested by other feature codes [Feature Codes]
- Added support for Time Condition Routing [TIME CONDITION ROUTING]
- Added support for Custom Time Groups [Custom Time Groups]
- Added support for custom announcement for Call Queue [Configure Call Queue]
- Added Reset Agent Call Counter to Call Queue [Configure Call Queue]
- Added number and percentage of transferred calls in the Call Queue Switchboard [Configure Call Queue]
- Added Call Memory in Call Queue [Configure Call Queue]

- Updated Wake-up Service by adding call failure notification [Wakeup Service]
- Added Wake-Up Call Service Failure email template. [Email Template]
- Room status can now be modified using the API [API CONFIGURATION]
- Odoo CRM integration has been added [Odoo CRM]
- Added custom repeating setting when scheduling meetings [Schedule Meeting]
- Added Extension Login Management module [Extension Login Management]
- Added Wave Administrator privilege [Create New SIP Extension][Custom Privilege]
- Added Download Chat Logs privilege [User Portal/Wave Privileges]
- Added Remote Logout Wave Privilege [User Portal/Wave Privileges]
- Added API support to retrieve recording filename [API CONFIGURATION]
- Added enable/disable setting for Paging/Intercom [Paging/Intercom]
- Added the option to synchronize RTP and media NAT setting in 1+N cluster deployment [1+N Media Cluster Synchronization]
- Added 1+N Media Cluster Connection Status Alarm [1+N Media Cluster Connection Status]
- Added support for configuring custom agent pause reason with a custom prompt [Global Queue Settings]
- Added support for allowing multiple login session from the same platform for Wave [Create New SIP Extension]
- Added TLS key download in Ethernet Capture diagnosis tool [Ethernet Capture]
- Login Security options have been improved [Login Security]
- External Host address will be automatically pushed to Wave clients when the UCM is deployed in a Remote Disaster Recovery setup [HTTP Server]
- UCM reboot event alerts and logs will now contain the reboot reason and the name of the user who initiated the reboot (if applicable) [System Reboot]
- Increased members notified for Emergency Calls from 10 to 30 [Emergency Calls]

Firmware Version 1.0.25.9

- Add Portugal Portuguese voice prompt support. [LANGUAGE SETTINGS FOR VOICE PROMPT]
- Added Wi-Fi related settings to GHP-W series template.

Firmware Version 1.0.25.7

- Added support for media resource clustering for UCM6304 and UCM6308. [Cluster]
- Multicast Community has been added. [Multicast Community]
- Scheduled Paging UI has been reworked. [Scheduled Paging/Intercom]
- Added support for playing MP3 files over GSC35XX devices. [Upload Custom Prompt]
- Added support for PMS billing system for Local PMS. [Call Rate]
- Mini bar has been improved. [Mini Bar]
- Added ability to set a Feature Code as a the Default Destination. [Speed Dial]
- Added ability to add External Number and LDAP numbers on Announcement Center. [Announcement Center]
- Added Fax Sending privilege when creating custom privileges. [Custom Privilege]
- Added enabling TURN Relay for a specific extension. [Create New SIP Extension]
- HA Data Sync Failure alert event has been added to the Alert Events List. [Alert Events List]
- SIP endpoints firmware can now be updated using the Zero Config page. [Managing Discovered Devices]
- Clearing the call history upon guest check-in or check-out has been added. [Local PMS]
- Onsite Meetings email invitations will include now an ics file. [Onsite Meeting]
- "Send File" Wave privilege has been added. [User Portal/Wave Privilege]

Firmware Version 1.0.23.17

- No major change.

Firmware Version 1.0.23.15

- Increased Fail2Ban list limit to 50 entries. [Fail2ban]
- NAS password field now supports special characters "&$'^`>|, [NAS]
- Speed Dial limit has been increased to 1000. [Speed Dial]

Firmware Version 1.0.23.12

- Added support for limiting chat history viewing for newly added participants. [Meetings Settings]
- Added support for including company number when scheduling a meeting. [Meetings Schedule]
- Added support for tracking outbound calls for QueueMetrics. [QueueMetrics]
- Added support for displaying call queue names on GRP phones.
- Added support for auto answer on inbound route level to detect fax call. [Inbound Rule Configurations]
- Added support for updating the call forwarding status when enabled via feature code. [Feature Codes]
- Added support for controlling diversion header. [SIP Settings]
- Added "Extension Group" as a custom privilege. [Custom Privilege]
- Added ability to retrieve recording files saved on NAS/GDMS cloud through API.
- Added support for manually backing up the UCM configuration to SFTP. [Backup/Restore]
- Added disaster recovery for High Availability. [HA]
- Added feature code to blacklist last called number. [Feature Codes]
- Added ability to share voicemail to group members. [VOICEMAIL]
- Added ability to delete voicemails for all voicemail group from one member. [VOICEMAIL]
- Added ability to monitor voicemail groups with voicemail key on endpoints. [VOICEMAIL]
- Added "Ignore Safe Operational Flow" to Network Port Traffic Control. [Network Settings]
- Added support for domains in API ACL.
- Added support for configuring chat file size limit. [IM Settings]
- Added support for "announce message caller-ID" in Announcement Center. [Announcement Center Settings]
- Added support for preventing Wave chat deletion. [User Portal/Wave Privilege]
- Added "Priority Call" feature code. [Feature Codes]
- Added support for updating time zones under Time Settings. [Time Settings]
- Added Live Chat feature. [Live Chat]
- Added Message Broadcast feature. [Message Broadcast]

Firmware Version 1.0.21.9

- Added SMS service support. [SMS Settings]
- Added support for creating shared departments. [Department Management]
- Added support for RADIUS login. [RADIUS]
- Added support for private intercom. [Configure Private Intercom]
- Added support for setting an extension as the default destination in Click2call. [Integrated Customer Service]
- Added support for SIP TLS cipher suite. [TCP & TLS]
- Added size and packet number limit for continuous packet capture when using USB/SD card storage or SFTP. [Ethernet Capture]
- Added support for resetting TLS certifcates to the default ones. [TCP & TLS]

- Added support for SSH token. [SSH Access]
- Added support for subscribing to a voicemail group. [Configure Voicemail Group]
- Added support for setting separate call forwarding conditions for external and internal calls. [Create New SIP Extension]
- Added support for forwarding calls to a custom prompt. [Create New SIP Extension]
- Added support for external numbers to opt out of being recorded when calling into the UCM. [PBX Settings]
- Added support for caller name look up. [Inbound Routes]
- The name of the agent will now be displayed in the switchboard. [Switchboard]
- Agent pause can now be performed quickly by dialing the respective feature code and the corresponding pause reason without having to interact with the IVR. [Configure Call Queue]
- Agent pause reason will now be displayed in the switchboard. [Switchboard]
- Added support for enabling the welcome prompt to be played simultaneously with background music while the agent phone is ringing. [Configure Call Queue]

Firmware Version 1.0.19.10

- Specific time configuration is now included in extension exports

Firmware Version 1.0.19.9

- Optimized various system processes
- Added Onsite Meetings feature. [Onsite Meeting]
- Added ability to customize extension call waiting tone [General Call Prompt Tones]
- {VM_DATE} date value format has been changed to MM/dd/yyyy hh:mm:ss from DDD yyyy MMM hh:mm:ss. [Configure Fax/T.38] [Voicemail Email Settings]
- Added Device Name ${DEVICE_NAME} variable to Alert Events and Emergency Calls email templates
- Added Geolocation header support [Emergency Location Mapping]
- Added P-Called-Party-ID header option to the Add/Edit Extension -> Features page [Create New SIP Extension]
- Added Allow Operator Panel Monitoring extension option to toggle whether the Operator Panel can monitor the extension. [Create New SIP Extension]
- Added Basic extension export option [Export Extensions]
- Allow Call-barging Extension List option changed to Call Monitoring Whitelist [Create New SIP Extensions] [Create New IAX Extension]
- Added Silence Suppression option to Extensions/VoIP Trunks page [Create New SIP Extension] [VoIP Trunk Configuration]
- If a storage device is full, the UCM will mark it as unavailable and automatically change file storage path to the next available location based on the Storage Path Priority. Previously, UCM would change the file storage path to its own local storage if external storage was full. [File Manager]
- Added new commands related to call queue and Wave [API Configuration Parameters]
- Added support for multiple API (new) users [API Configuration Parameters]
- Added the Default Certificate Auto Renewal option. If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected. [HTTP Server]
- Added ability to sync local IM data to Cloud IM [Cloud IM Service]
- Added ability create custom IVR key presses [Custom Key Event]
- Added Chat Data from Endpoint option to the Maintenance -> System Cleanup/Reset -> Cleaner page. If enabled, this option will clean out chat data from Wave clients at the same time as the UCM's server-side automatic/manual cleaning of chat data. [Cleaner]

- Added support for meeting room passwords. However, meetings cannot be scheduled for rooms with meeting password enabled. [Multimedia Room Configurations]
- Meeting kick warning interval has been changed from 30 mins to 20 mins. Note: This kick warning will only play when there is only 1 person in a meeting room, and if they do not opt to stay in the meeting room after the warning, they will be removed from the meeting room after 5 minutes.
- ARP will now be used instead of ping to check NAS connectivity.
- Upgrade logs will now contain firmware version information.
- Queue chairmen can now log out dynamic agents
- Added video paging support. [Configure 1-way Paging]
- Added option to automatically reset user/Wave password upon check-in/check-out. [Local PMS]
- Added option to clear Wave chat history automatically upon check-in or check-out. [Local PMS]
- Added Local PMS functionality [Local PMS]
- Check-out will no longer reset the "Skip Voicemail Password Verification" extension setting
- Added ability to assign two extensions to a room [Room Management]
- Added option to clear scheduled wakeup calls on both check-in and check-out. [Local PMS]
- Added the ability to change the default call privilege of a room. A room's privilege will be reset to this value after a guest checks out of it.
- Added support for stereo audio recording [General Settings]
- Added option to route calls based on a caller's Diversion header value [Inbound Rule Configuration]
- Added ability to control whether to use failover trunks based on the call response codes [Failover Trunk Toggles]
- Added support for H.264 with multiple payload types in SDP
- When receiving an INVITE with no SDP, following INVITEs with SDP will offer H.264 1080p resolution by default.
- In the scenario where an inbound external call is forwarded from an extension to an external number, the Contact header will now use the CID of the forwarding extension instead of the caller's CID.
- Removed External Device Usage Threshold option. If a connected NAS has only 1GB remaining available storage space, it will be considered unavailable and trigger the external disk usage alert. [NAS]
- Added User Endpoint Access History page [User Endpoint Access History]
- Added User Portal/Wave privilege control [User Portal/Wave Privilege]
- Dial Trunk option has been renamed to Dial External Number and moved to the Dial Other Extensions section
- The Wave Welcome email will now use the port number configured in System Settings->HTTP Server->Wave Settings->Port if the Wave Settings->External Host value is not a RemoteConnect address or does not contain a port number.
- Added links to relevant online documentation to various pages of the UCM webUI.
- Added Phonebook VMPK mode to GRP261x template
- Added Firmware tab for improved firmware management [Firmware]
- Added ability delete downloaded base model templates in the Model Update page
- Added ability to search for templates via the device model name
- Added ability to select either LAN1 or LAN2 to scan for devices on when using dual network method

Firmware Version 1.0.17.11

- Several system process optimizations

Firmware Version 1.0.17.8

- Updated python version to 3.8 and related processes.

- Improved speed of applying changes
- Updated lighttpd version to 1.4.61
- The Privilege Name field now supports parenthesis ()
- The Contacts page has been moved to its own category in the sidebar
- Added Channel Path option for accessing specific IP camera channels via URL [Device Management]
- Improved alert email sending process
- Updated Remote Registration email template
- Emergency calls will no longer be restricted by the RemoteConnect call limit.
- The default highest priority codec is now G.722.
- Added Remote Extension Privilege Update feature code and Remote Extension Privilege Update Whitelist field to allow specified users to remotely change extensions' privileges. [Feature Codes]
- Automatic file migration after file storage path failure to the next storage location in the storage priority path.
- Users can now customize the storage path priority for recordings, video recordings, and IM files. [File Manager]
- FXO FSK CID detection now uses spandsp.
- If SIP extensions synced from UCMs are deleted on GDMS, they will no longer be synced again.
- If HA is enabled, the HA cluster IP address will now be provisioned as the config server to endpoints instead of the active UCM's IP address.
- Added support for configuring inbound route blacklist via HTTPS API.
- If dialing into a Dial by Name directory, the call will end automatically after failing 3 times.
- Added Server Type option to the LDAP Server->LDAP Phonebook->Phonebook Download Configurations page. Users can select between LDAP and Active Directory. [LDAP Server]
- Added Department field to LDAP phonebook contacts. [LDAP Server]
- Added meeting room extensions to LDAP phonebooks. [LDAP Server]
- External Contacts created from the Contacts page will now be added to the system's internal LDAP phonebook. [LDAP Server]
- Added Remote Login tab to the Maintenance->Login Settings page. [Maintenance]
- Created new Meetings Settings page under the Multimedia Meetings page and moved several meeting-related options to it. [Multimedia Meeting]
- Regular meeting participants can now invite other members to join the meeting by dialing 1 if "Allow User Invite" is enabled. [Multimedia Meeting]
- Meetings will become "Pending" after rescheduling.
- Pending meetings are now sorted by start time by default.
- Added the Allowed to Override Host Mute option to the Edit Meeting Room and Schedule Meeting pages to allow participants to unmute themselves even after the meeting host mutes them. [Multimedia Meeting]
- Added support for user authentication. [OpenVPN]
- Operation Log entries will now contain the IP address and location information from which the operation originated. [Operation Log]
- Added option Automatically Clear Wakeup Calls for deleting scheduled wakeup calls after either guest check-in and check-out. [PMS Features]
- Users can now dial the Update PMS Room Status feature code, the maid code, and the room status code all at once to change room status. [PMS Features]
- Added a Scan button to manually retrieve the list of recordings on external storage. The UCM automatically displays up to 5000 recordings on attached external storage, but pressing this button will allow the UCM to display more. [Recordings Files]
- Added ability to batch delete cloud storage files.

- If IP endpoints cannot connect to the GDMS TURN server via UDP, UCM will use TCP to connect them.
- Added Trunk Registration Period (s) option to SIP Settings->Misc. [SIP Settings]
- Added option Special Attributes to the Extension/Trunk->VoIP Trunks->Edit SIP Trunk->Advanced Settings page. If enabled, the following attributes will be included in the SIP SDP: ssrc, msid, mid, ct, as, tias, record. Enabling this may cause compatibility issues with non-Grandstream devices. [VoIP Trunk Configuration]
- Added CEI msid for audio calls.
- Added trickle-ice param to SIP OPTION's 200 OK.
- profile-level-id will be added to 200 OK when receiving INVITEs without SDP.
- Added ability to import/export speed dials. [Speed Dial]
- Improved processes to avoid duplicate alerts for the following events: Registered SIP Trunk failed, Local Disk Usage and External Disk Usage.
- Separated Allow Deletion of CDR and Recordings option to Allow Deletion of CDR and Allow Deletion of CDR Recordings. [User Management]
- Added the Call Waiting option to the User Portal.
- Added support for voicemail message seeking. When listening to voicemail, users can press star (*) to rewind 3 seconds or pound (#) to fast forward 3 seconds. [Voicemail]
- Added Line Selection Strategy option for Trunk Groups. [VoIP Trunks]
- Changed register trunk Username field name to Trunk Registration Number. [VoIP Trunks]
- General web UI improvements
- Added Help option under the username dropdown menu that will redirect to the UCM6300 Series FAQ.
- Updated some tooltips.
- Optimized search functionality
- Added GMT+2:00 (Israel) option to Time Zone drop down list in all Zero Config pages.
- Added support for WP22 and WP825 model templates.

Firmware Version 1.0.15.13

- Added SNMP monitoring feature. [SNMP]
- Added support to configure the time of a holiday. [Holiday]
- Added ability to determine the maximum total call duration per trunk for outbound calls.
- Added contact viewing privilege (independent from Department Contact Privilege). [Contacts]
- Added support for agent ID announcement. [Call Queue]
- Added support for Service Level Agreement for Call Queue. [Service Level Agreement]
- Added support for changing the Meeting room's name.
- Added WebRTC Trunk feature. [WebRTC Trunks]
- Extension data cleaning has been improved. [Search and Edit an Extension]
- Added support for SRTP Crypto Suite. [Create New SIP Extension]
- STIR/SHAKEN has been improved. [STIR/SHAKEN]
- Added support for displaying the extension that initiated an emergency call in the emergency email notification.
- Added support for collecting ICE candidates when an RTP connection is requested. [RTP Settings]
- Added support for recording a Multimedia Meeting shared screen only with the audio of the participants.
- Flood Attacks and Network Traffic Storm alerts have been added to the Alert Events List.
- Added support for Network Port Traffic Control for the ports of the UCM63xx.
- Added Support for limiting the frequency of calls that can be made in a period of time.
- Added support for storing the local chat files in the GDMS.

- UCM RemoteConnect plan expiry screen has been improved.
- GDMS Cloud Storage Space details can now be viewed in the RemoteConnect menu.

Firmware Version 1.0.13.9

- Added option to enable/disable DND status remotely for an extension. [CALL FEATURES]
- Added local proxy in IM settings. [Cloud IM]
- Added support for enabling/disabling auto audio/video recording for meeting. [Multimedia Meeting Configurations]
- Added privilege management for contacts. [Privilege Management]
- Improved fail2ban blacklist display. [Blacklist]
- Improved email template for scheduling meeting. [Email Templates]
- Contacts sync-up between UCM and end points (wave/IP phones). [LDAP Settings]
- Added ability to specify DOD number based on outbound route. [Outbound Routes DOD]
- Fixed an issue where updating model templates will result in deleting the existing ones.
- Added support to use TURN Relay as an option to allow hosts behind NAT firewalls to communicate. [VoIP Trunk Configuration]

Firmware Version 1.0.11.10

- Combined audio meeting and video meeting to multi-media meeting. [MULTIMEDIA MEETING]
- Updated UCM6301 public meeting room number from 3 to 4. [MULTIMEDIA MEETING]
- Added operator panel. [OPERATOR PANEL]
- Added time condition support for IVR key events. [Key Press Event]
- Supported adding comments for fail2ban whitelist. [Fail2Ban Whitelist]
- Added Call Flip feature code. [Call Flip]
- Added cloud IM abnormal alert event. [Cloud IM abnormal]
- Added option "Play Follow Me Prompt". [Play Follow Me Prompt]
- Add option "Ignore 180 Response". [Ignore 180 Response]
- Added Multi-Factor Authentication for UCM login. [Multi-Factor Authentication]
- Added support for IoT device management. [DEVICE MANAGEMENT]
- Added remark for UCM system status. [Remark]
- Added option to enable and disable passwordless for remote access. [UCM RemoteConnect Plan Settings]
- Added option to enable and disable virtual queue call back keys settings. [Virtual Queue Callback Key]
- Added option to enable IPv6 for HA settings. [Enable IPv6]
- Added Address Book Management section. [Address Book Management]
- Added option "Stop Ringing". [Stop Ringing]
- Add option "Email Missed Call Log". [Email Missed Call Log]
- Add option "Security Mode" for NAS settings. [Security Mode]
- Removed display for consumer users on the user management page. [Create New User]

Firmware Version 1.0.9.10

- Added support for import/export Zero Config. [Figure 68: Global Policy Categories]
- Added support for Enable Wave and Sync Contact under the extension. [Enable Wave][Sync Contact]
- Added support for Custom time supplement time conditions. [Time Condition]
- Added support for Call Restriction. [RESTRICT CALLS]
- Added support for QueueMetrics. [QUEUEMETRICS]

- Added support for CDR API whitelist. [API Configuration Parameters]
- Added support for Call queue satisfaction survey. [Call Queue Statistics]
- The old API Configuration is reopened for use.
- Custom permissions support the function of deleting CDR and recording files. [delete CDR and recording files]
- Added support to adjust the recording file storage path. [File Manager]
- High Availability feature on UCM6300 series. [HA]
- Paging/Intercom supports delayed paging. [Configure Multicast Paging]
- UCMRC remote service diagnosis. [RemoteConnect]
- Support LDAP to automatically update the phone book. [LDAP Client Configurations]
- Support meeting room automatic gain control. [Meeting Settings]

Firmware Version 1.0.7.12

- Added support for an email reminder when editing the time of a scheduled meeting. [Email Reminder (m)]
- Improved extension status syncing process to the IM server.

Firmware Version 1.0.7.9

- Statistics and alarm settings of the maximum number of concurrent calls on the trunk. [Enable Concurrent Call Alert] [Enable Concurrent Call Alert]
- Add ability to enable/disable Ring Group Voicemail and make Ring Group Voicemail have configurable voicemail prompts. [Voicemail]
- Add ability to import/export pickup groups and time settings. [PICKUP GROUPS]
- Add option to set a holiday as fixed. [Year]
- Support DOD digit manipulation based on extension. [Direct Outward Dialing (DOD)]
- Support to join the scheduled meeting 10 minutes in advance and is controlled by conference resources. [Meeting Schedule]
- Clean up the history of audio and video schedule meetings regularly. [Cleanup Type]
- Record the actual member information in the meeting history details.
- Support to initiate a random meeting in a scheduled/instant-meeting room. [Meeting Schedule]
- The host password for the scheduled meeting is randomly generated. [Meeting Schedule]
- Add the "Download Client" link to the extension email template and add the Wave promotion guide in the setup wizard. [Email Templates] [Setup Wizard]
- Added support for Integrated Customer Service SDK. [Integrated Customer Service SDK]
- Support customer service system call (Click2Call) service provides SDK download for customers to integrate into the website and set up security defense Fail2ban. [Customer Service System Call Defense]
- Support to use Cloud IM service. [IM]
- Add email reminder configuration in the audio meeting room. [Email Reminder (m)]
- Added support for custom prompts under Voicemail Group. [Busy Prompt][Greet Prompt][Temporary Prompt][Unavailable Prompt]
- The dashboard shows eMMC lifetime and the number of public/random video meetings. [PBX Status]
- Added some System Alert Events. [Alert Events List]

Firmware Version 1.0.5.4

- Added support for v-Fax, Fax-sending, Email2Fax. [FAX SERVER]
- Added ability to restore backups remotely stored on GDMS [Restore Configuration from Backup File]

- Added support for STIR/SHAKEN. [SIP Settings/STIR/SHAKEN] [VoIP Trunk Configuration]
- Added ability to restrict calls and features based on CPU usage and data partition usage. [General Settings]

- Added NAT option to the Export File Data filtering option. [Export File Data]
- Wave desktop client is now supported. [Wave Desktop]
- Added support for IAX. [IAX SETTINGS] [EXTENSIONS] [VoIP Trunk Configuration]
- Improved audio and video conference pages. A list of the meetings that have not started and a meeting history list have been added. [Meeting Schedule]
- Support sending post-meeting reports to the host after scheduling a meeting. [Meeting Schedule]
- Added the SRTP Debugging option to the Ethernet Capture page. [Enable SRTP Debugging]
- Updated the System Cleanup/Reset page interface. [System Cleanup/Reset]
- Added manual cleaning. [Cleaner]
- Added ability to add a custom browser tab icon and custom logos on various pages of the web management portal and Wave Web portal. [UI Customization]
- Improved push notification for Wave mobile.
- Added Instant Messaging functionality to Wave Web. [Wave Web]
- LDAP phonebook information will now be synchronized when viewing the Contacts page. [Wave Web]
- UCM can now synchronize system event alerts to GDMS. [Plan Settings]
- Added threshold-based Call Control & Data Write Control. [General Settings]
- Added Layer 3 QoS for SIP and Layer 3 QoS for RTP options to global policy and relevant templates. [Layer 3 QoS For RTP] [Layer 3 QoS For SIP]
- Improved device list import support and added the ability to export devices on the ZeroConfig Device List page. [Managing Discovered Devices]

Firmware Version 1.0.3.10

- Added RemoteConnect Mode option in SIP trunk. [RemoteConnect Mode]
- Cloud Storage for CDR Backup and Record. [CDR in GDMS Cloud]
- Add support for IDS PMS interface. [IDS PMS]
- Add ability to enable PMS Wakeup call from remote extensions. [PMS Remote Wakeup Service]
- Add ability to configure local country code for an outbound route. [Local Country Code]
- Add support for Pattern and Leading digit filtering options in Callee Number. [Callee Number]
- Added description of SSH switch options in LCD menu. [Use the LCD Menu]
- Add the ability to import/export DOD. [Direct Outward Dialing (DOD)]
- Add the ability to enable auto record per inbound/outbound route. [Auto Record] [Auto Record]
- Add the ability to Enable Recording Whitelist. [Enable Recording Whitelist]
- Add the ability to select missed call type to be sent via email. [Missed Call Type]
- The Filter action is now supported in AMI sessions. [ASTERISK MANAGER INTERFACE]
- Added command to delete call recordings after downloading them. [recapi]
- Added commands to add, edit, and delete PIN groups. [addPinSets] [getPinSets] [updatePinSets] [deletePinSets]
- Added External Disk Status alert event for monitoring external storage connection status. [Alert Events List]
- The language of column titles in exported CDR reports and statistics reports will now be based on the UCM's display language. [Downloaded CDR File]
- Added Parking Lot Timeout Alert-Info option. This will add the specified alert-info header value to parking timeout callbacks. [Parking Lot Timeout Alert-Info]

- Updated HMobile check-in request format. [HMobile PMS Connector]
- Updated HMobile Mini Bar request. [HMobile PMS Connector]
- Added several updates to HSC PMS. [HSC PMS]
- Added the ability to specify the reason for agent pause (*83 by default). [Agent Pause]
- Added CDR Stored in GDMS Cloud option for RemoteConnect Plan Settings. [UCM RemoteConnect]
- GDMS Cloud Storage has been added as a recording storage location in the PBX. [PBX Settings/]
- After adding a UCM to GDMS, its RemoteConnect address will automatically be added as a SIP server to the GDMS account. [UCM RemoteConnect]
- Added the Ringback Tone option. Users can now select a custom prompt to play as a ringback tone for callers dialing in via the selected inbound route. [Ringback tone]
- Ring Group Voicemail can now be set as a routing destination and an IVR key press destination. [Default Destination]
- Added the following custom privileges: LDAP Server, UCM RemoteConnect, and Announcement. [Custom Privilege]
- Added a Forgot Password option to the Wave Web login page. [Wave Web]
- Added a new command to set the same-day wakeup service by dialing *36. [Wakeup Service]

Firmware Version 1.0.2.25

- This is the initial version.