Grandstream Networks, Inc.

UCM630X Series

Enterprise-Grade Unified Communication Solutions

User Manual

COPYRIGHT

The latest electronic version of this user manual is available for download here:

http://www.grandstream.com/support

CAUTION

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.

WARNING

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

GNU GPL INFORMATION

UCM630X firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:
http://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download

Table of Content

Table of Tables

Table of Figures

DOCUMENT PURPOSE

The intent of this document is to provide device administrators an overview of the specifications and features of the Grandstream UCM630X IPPBX system. To learn more about the UCM630X, please visit http://www.grandstream.com/support to download additional guides.

This guide covers following main topics:

- Product overview
- Installation
- Getting started
- System settings
- Provisioning
- Extensions
- Extension groups
- Analog Trunks
- VoIP Trunks
- SLA station
- Call routes
- Conference room.
- Conference schedule
- IVR
- Language settings for voice prompt
- Voicemail
- Ring group
- Paging and intercom group
- Call queue
- Pickup groups
- PIN Groups
- Music on hold
- Fax Server
- Busy camp-on
- Presence
- Follow me
- Speed Dial
- DISA
- Callback
- BLF and event list
- Dial by name
- Active calls and monitor
- Call features
- Call recording
- CTI Server
- Asterisk manager interface (AMI)
- CRM integration
- PMS integration
- Wakeup service
- Announcements center
- Status and reporting
- CDR (Call Details Record)
- User Portal
- Upgrading and maintenance
- Backup/restore
- Troubleshooting

CHANGE LOG

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 1.0.5.4

- 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 WebRTC Video Calling & Conferencing]
- 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. [Conference Schedule] [Conference Schedule].
- Support sending post-meeting reports to the host after scheduling a meeting. [Conference Schedule] [Conference 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. [Custom logo]
- Improved push notification for WAVE mobile.
- Added Instant Messaging functionality to Wave Web. [Wave WebRTC Video Calling & Conferencing]
- LDAP phonebook information will now be synchronized when viewing the Contacts page. [Wave WebRTC Video Calling & Conferencing]
- 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 in 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 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/Recordings Storage]
- 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 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 WebRTC Video Calling & Conferencing]
- Added a new command to set same-day wakeup service by dialing *36. [Wakeup Service]

Firmware Version 1.0.2.25

- This is the initial version.

WELCOME

Thank you for purchasing 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. The UCM6301/6302 support 1 x ARM Cortex-A53 Quad-Core CPU and 2GB of memory while UCM6304/6308 support 2 x ARM Cortex-A53 Quad-Core CPU and 2GB for master and 1GB slave memory.

⚠ **Caution:**

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.

⚠ **Warning:**

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

This document is subject to change without notice. The latest electronic version of this user manual is available for download here:
http://www.grandstream.com/support

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 UCM630X series.

Table 1: Technical Specifications

Interfaces	
Analog Telephone FXS Ports	• UCM6301: 1 port with lifeline support • UCM6302: 2 ports with lifeline support • UCM6304: 4 ports with lifeline support • UCM6308: 8 ports with lifeline support Each port supports 3 REN
PSTN Line FXO Ports	• UCM6301: 1 port • UCM6302: 2 ports • UCM6304: 4 ports • UCM6308: 8 ports All ports have lifeline capability in case of power outage
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: USB 3.0, and SD card interface • UCM6302: USB 2.0, USB 3.0, and SD card interface • UCM6304/6308: 2x USB 3.0 and 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-Packet Capabilities	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+, H.265, 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 and Plug-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 local and remote trunk
Network Protocols	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®
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)
Environmental	• Operating: 32 - 113ºF / 0 ~ 45ºC, Humidity 10 - 90% (non-condensing) • Storage: 14 - 140ºF / -10 ~ 60ºC, Humidity 10 - 90% (non-condensing)
Mounting	Wall mount (sold separately) & Desktop for UCM6301/6302 and Desktop & Rack mount for UCM6304/6308.
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, Dutch, Polish, Portuguese, Russian, Swedish, Turkish, Hebrew, Arabic, Netherlands • Customizable language pack to support any other languages
Caller ID	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 – BT, NTT

<table>
<tr><td>Polarity Reversal/ Wink</td><td colspan="2">Yes, with enable/disable option upon call establishment and termination</td></tr>
<tr><td>Call Center</td><td colspan="2">Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/workload, in-queue announcement</td></tr>
<tr><td>Customizable Auto Attendant</td><td colspan="2">Up to 5 layers of IVR (Interactive Voice Response) in multiple languages</td></tr>
<tr><td>Telephony Operating System</td><td colspan="2">Based on Asterisk version 16</td></tr>
<tr><td rowspan="4">Maximum Call Capacity</td><td>UCM6301</td><td>• Users: 500
• Concurrent calls (G.711): 75
• Max concurrent SRTP calls (G.711): 50</td></tr>
<tr><td>UCM6302</td><td>• Users: 1000
• Concurrent calls (G.711): 150
• Max concurrent SRTP calls (G.711): 100</td></tr>
<tr><td>UCM6304</td><td>• Users: 2000
• Concurrent calls (G.711): 300
• Max concurrent SRTP calls (G.711): 200</td></tr>
<tr><td>UCM6308</td><td>• Users: 3000
• Concurrent calls (G.711): 450
• Max concurrent SRTP calls (G.711): 300</td></tr>
<tr><td rowspan="4">Maximum Attendees of Conference Bridges</td><td>UCM6301</td><td>• 4 Video Conference rooms and up to 20 parties with 1080p HD H.264 and Opus (assuming 4 video feeds + 1 screen sharing)
• Voice Conference: Up to 75 parties with G.711</td></tr>
<tr><td>UCM6302</td><td>• 6 Video Conference rooms and up to 30 parties with 1080p HD H.264 and Opus (assuming 4 video feeds + 1 screen sharing)
• Voice Conference: Up to 150 parties with G.711</td></tr>
<tr><td>UCM6304</td><td>• 8 Video Conference rooms and up to 60 parties with 1080p HD H.264 and Opus (assuming 4 video feeds + 1 screen sharing)
Voice Conference: Up to 200 parties with G.711</td></tr>
<tr><td>UCM6308</td><td>• 10 Video Conference rooms and up to 80 parties with 1080p HD H.264 and Opus (assuming 4 video feeds + 1 screen sharing)
• Voice Conference: Up to 300 parties with G.711</td></tr>
</table>

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, 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
Wave Mobile App	Allows Android & iOS users to join UCM-hosted meetings & communicate with other users/solutions registered to the UCM6300
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
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

⚠ **Note:**

UCM630X FXS ports lifeline functionality:
The UCM630X FXS interfaces are metallic through to the FXO interfaces. If there is power outage, 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 installation, connection, and warranty policy of the UCM630X series.

Equipment Packaging

Table 2: UCM630X Equipment Packaging

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

Connect Your UCM630X (UCM6301 as example)

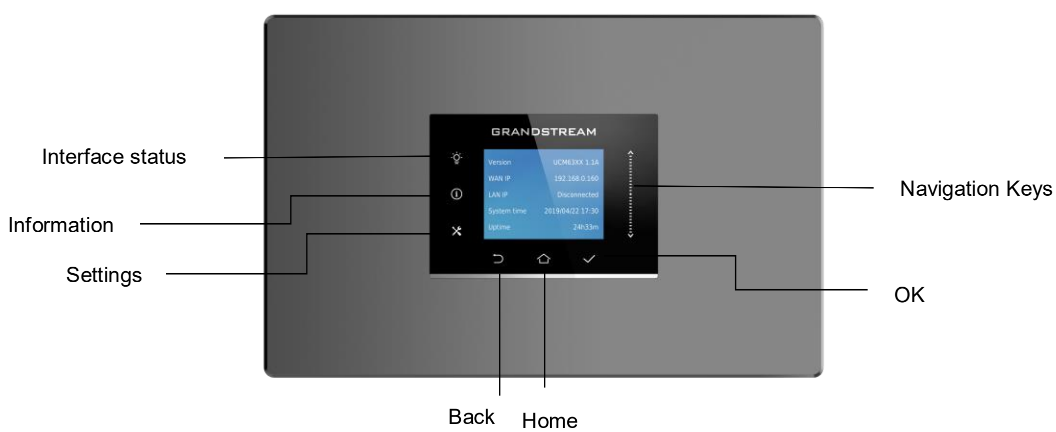


Figure 1: UCM6301 Top View

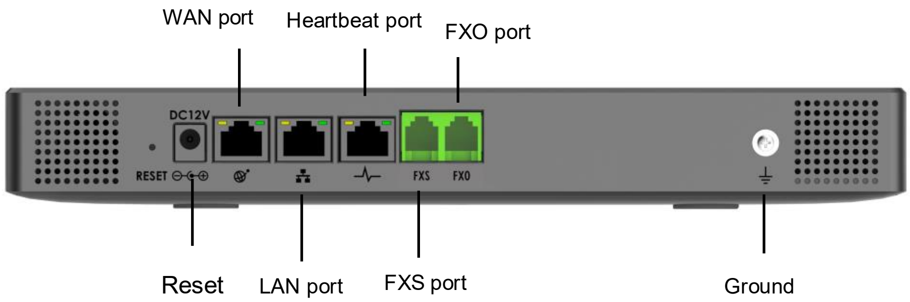


Figure 2: UCM6301 Back View

Figure 3: 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 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.

Note:

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

UCM6302 front and back view

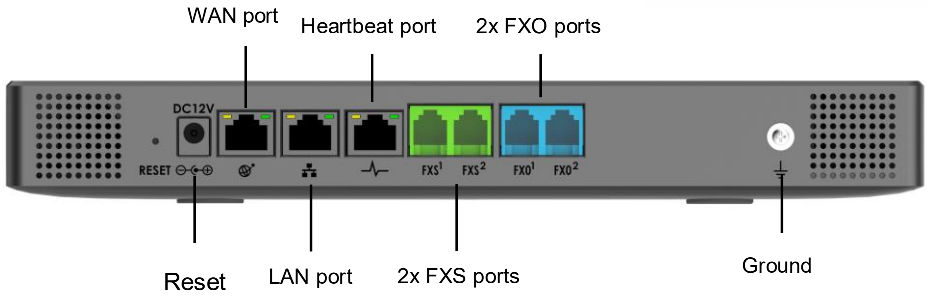


Figure 4: UCM6302 Back View

Figure 5:UCM6302 Front View

UCM6304 front and back view

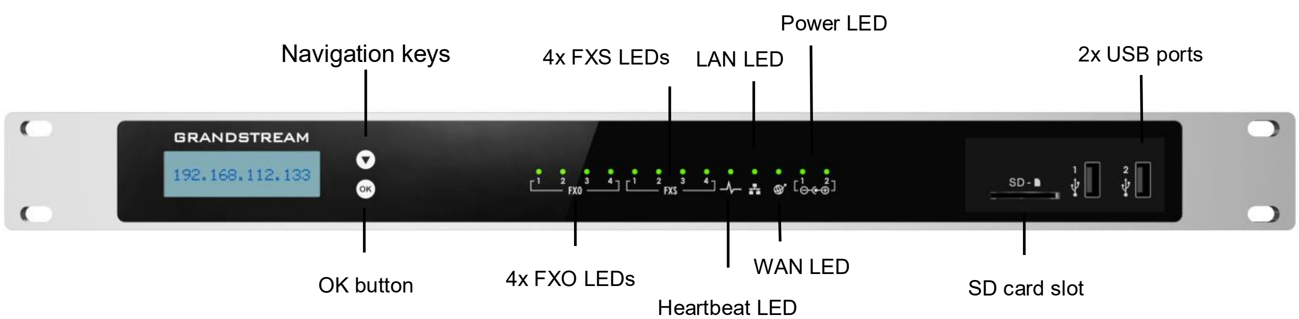


Figure 6: UCM6304 Front View

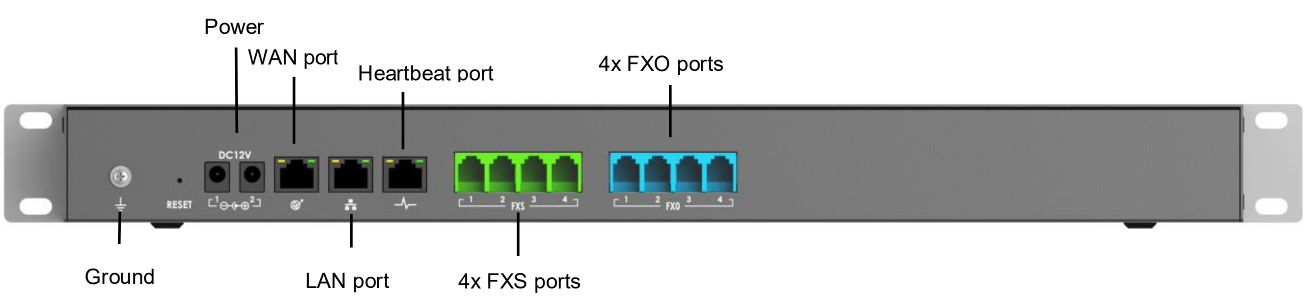


Figure 7: UCM6304 Back View

UCM6308 front and back view

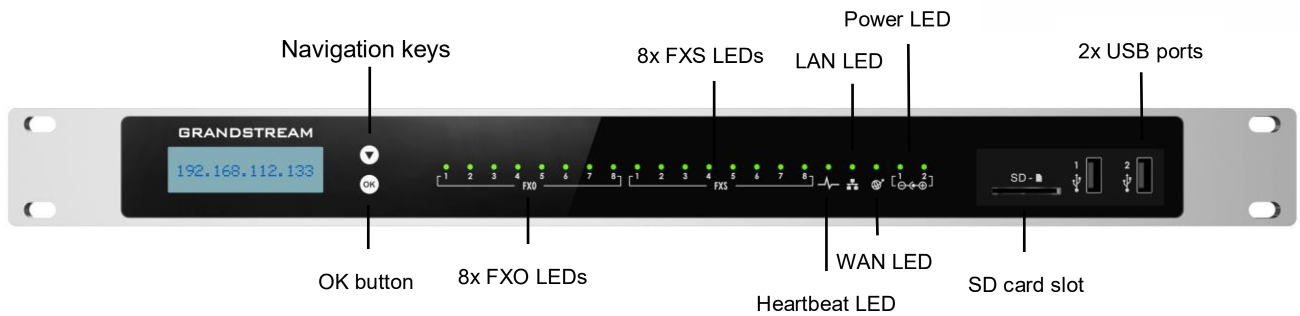


Figure 8: UCM6308 Front View

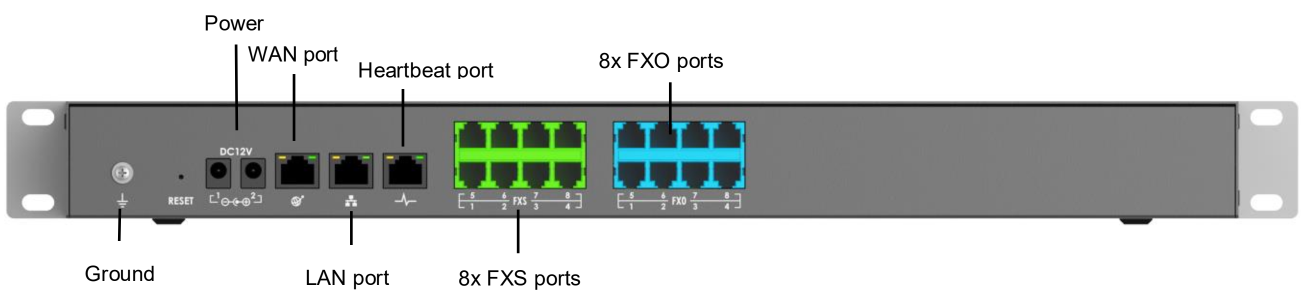


Figure 9: UCM6308 Back View

Safety Compliances

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.

Warranty

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 warranty policy without prior notification.

⚠ **Warning:**

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 *[Table* 3: LCD Menu Options*]*.

- **Menu Navigation**
  Scrolling sown 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.

Table 3: LCD Menu Options

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 back 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 back 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.

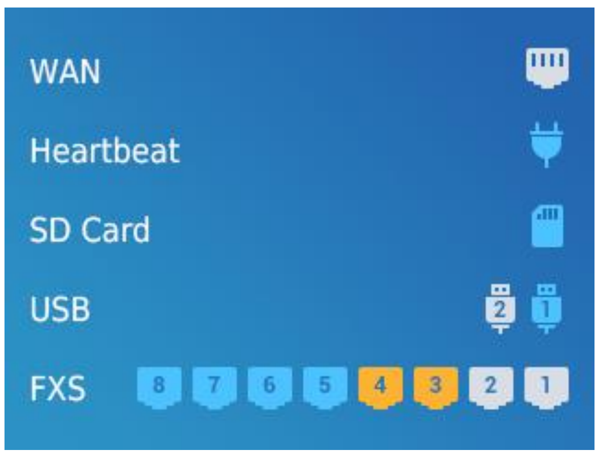


Figure 10: Ports Status

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

Table 4: UCM6304/6308 LED Indicators

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

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 Microsoft IE (version 8+), Mozilla Firefox, Google Chrome, etc. To access the UCM's web portal, follow the steps below:

Figure 11: 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.

⚠ **Note:**

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 Web GUI→**System Settings**→**HTTP Server**.

Setup Wizard

After logging into the UCM web portal for the first time, the setup wizard will guide the user through basic configurations such as time zone, network settings, trunks, and routing rules.

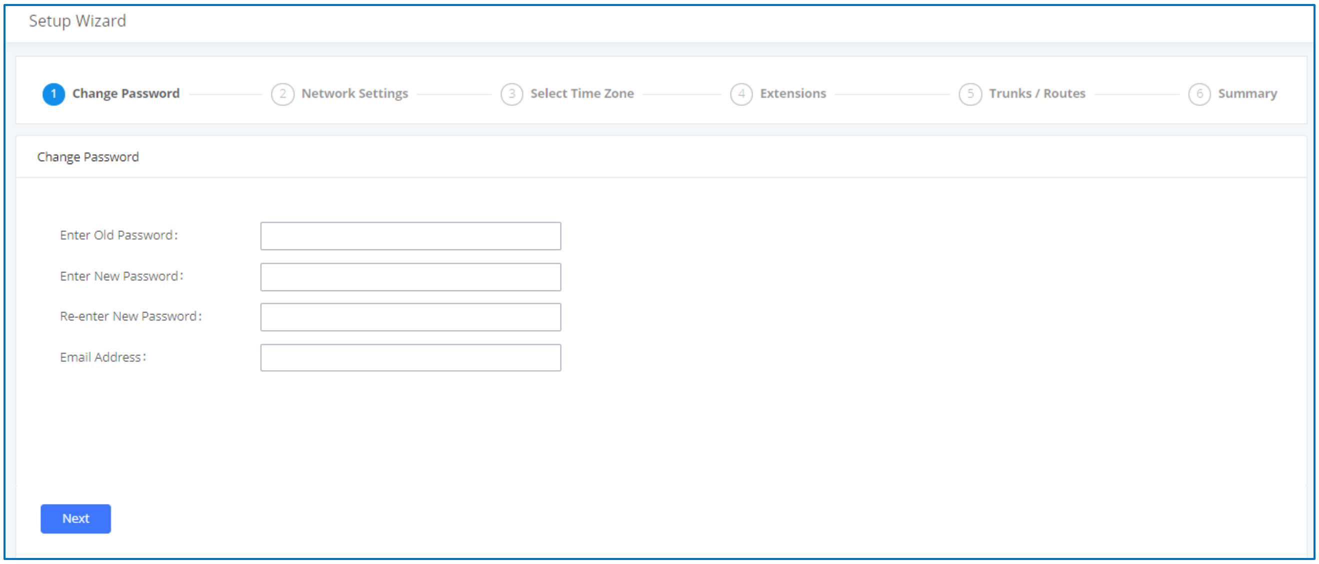


Figure 12: UCM630X Setup Wizard

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.

Main Settings

There are 8 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.
- **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.
- **CDR:** Contains the call detail records, statistics, and audio recordings of calls processed by the UCM.
- **Value-Added Features:** Manages the settings of features unrelated to core PBX functionality such as Zero Config provisioning and CRM/PMS integrations.
- **Maintenance:** Manages settings and logs related to system management and maintenance such as user management, activity logs, backup settings, upgrade settings and troubleshooting tools.

Web GUI Languages

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

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

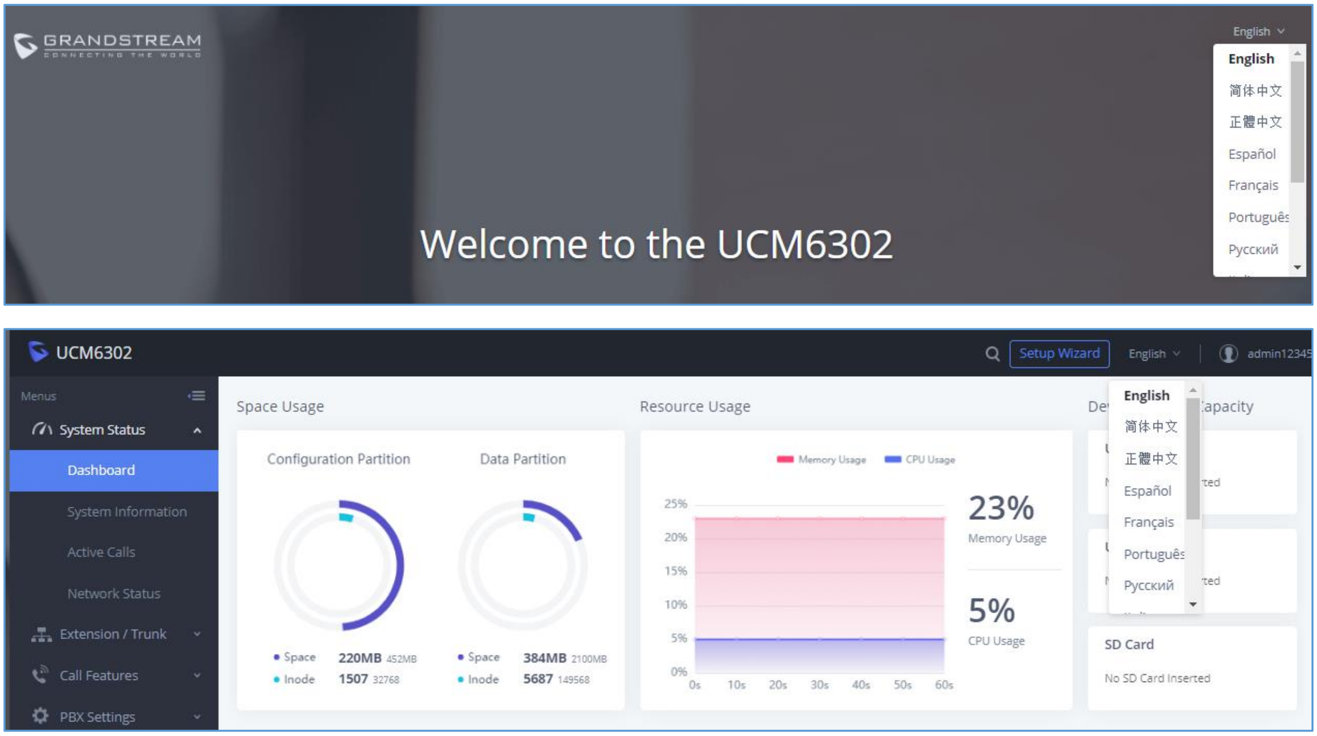


Figure 13: UCM630X Web GUI Language

Web GUI Search Bar

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

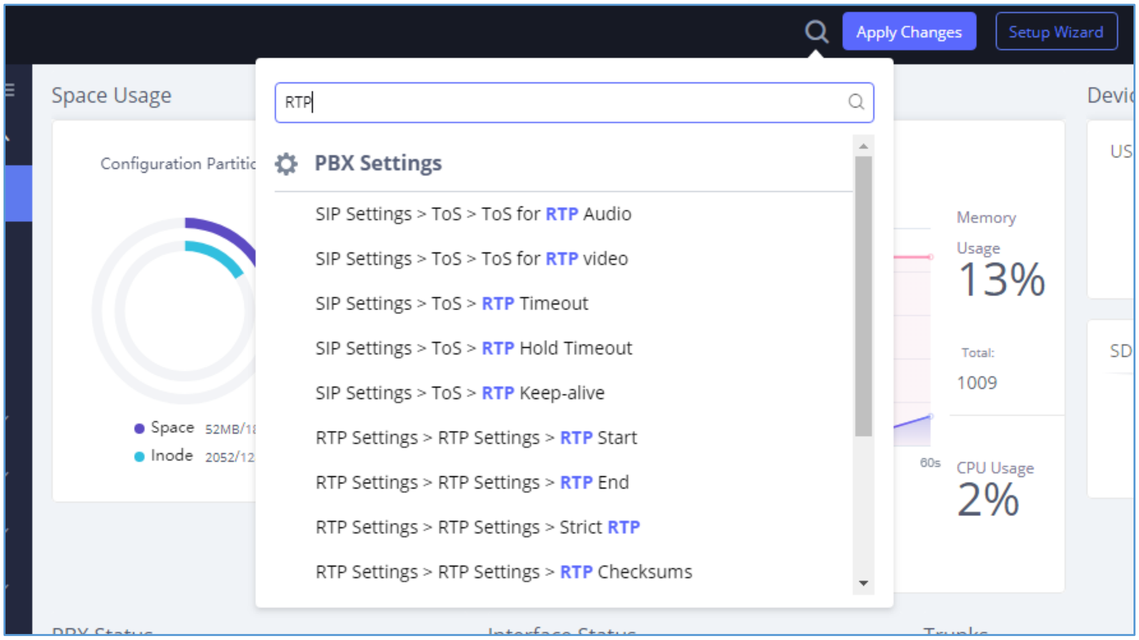


Figure 14: Web GUI Search Bar

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.

Setting Up an Extension

Power on the UCM630X and your SIP endpoint. Connect both devices to the same network and follow the steps below to set up an extension.

1. Log into the UCM web portal and navigate to **Extension/Trunk→Extensions**
2. Click on the "Add" button to start creating a new extension. The Extension and SIP/IAX Password information will be used to register to this extension. To set up voicemail, the Voicemail Password will be required.
3. To register an endpoint to this extension, go into your endpoint's web UI and edit the desired account. Enter the newly created extension's number, SIP user ID, and password into their corresponding fields on the endpoint. Enter the UCM's IP address into the SIP server field. If setting up voicemail, enter *97 into the Voice Mail Access Number field. This field may be named differently on other devices.
4. To access the extension's voicemail, use the newly registered extension to dial *97 and access the personal voicemail system. Once prompted, enter the voicemail password. If successful, you will now be prompted with various voicemail options.
5. You have now set up an extension on an endpoint.

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, 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.

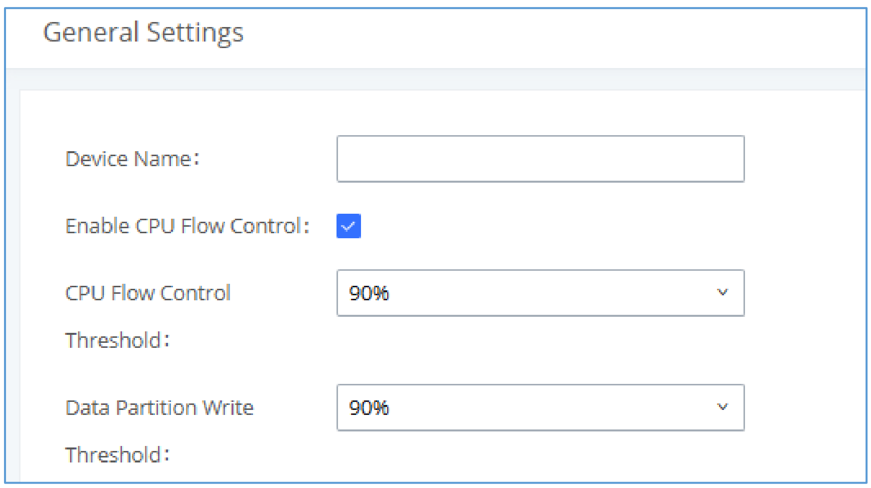


Figure 15: General Settings Interface

Table 5: General Settings Parameters

General Settings	
Device Name	Configure the name of the UCM.
Enable CPU Flow Control	Enables the CPU flow control.
CPU Flow 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. Default value is **90%**.
Data Partition Write 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. 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**.

Table 6: HTTP Server Settings

UCM Web Settings	
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".
Port	Specifies the port number used to access the UCM HTTP server. Default is "8089".
Enable IP Address Whitelist	If enabled, only the server addresses in whitelist will be able to access the UCM's web portal. It is highly recommended to add the IP address currently used to access the UCM web page before enabling this option. Default is "Disabled".
Permitted IP(s)	List of addresses that can access the UCM web portal. Ex: 192.168.6.233 / 255.255.255.255
External Host	Configure a URL and port (optional) used to access the UCM web portal or a public link to the video conference room if the UCM is behind NAT.
GS Wave Settings	
External Host	Configure a URL and port (optional) used to access the UCM web portal or a public link to the video conference room if the UCM is behind NAT.
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	
Certificate 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 Private Key	Uploads the private key for the HTTP server. **Note**: Key file must be under 2MB in file size and in *.pem format. File name will automatically be changed to "private.pem".
TLS Cert	Uploads the certificate for the HTTP server. **Note:** Certificate must be under 2MB in file size and in *.pem format. This will be used for TLS connections and contains private key for the client and signed certificate for the server.
Domain	Enter the domain to request the certificate for and click on Request Certificate to request the certificate.

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 login 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 UCM6301, UCM6302, UCM6304 and UCM6308, respectively.

Table 7: UCM630X Network Settings→Basic Settings

Method	Select "Route", "Switch" or "Dual" mode on the network interface of UCM630X. The default setting is "Route". • **Route** WAN port will be used for uplink connection. LAN port will function similarly to a regular router port. • **Switch** WAN port will be used for uplink connection. LAN port will be used as a bridge for connections. • **Dual** Both WAN and LAN ports will be used for uplink connections labeled as LAN2 and

	LAN1, respectively. The port selected as the Default Interface will need to have a gateway IP address configured if it is using a static IP.
MTU	Specifies the maximum transmission unit value. Default is 1492.
IPv4 Address	
Preferred DNS Server	If configured, this will be used as the Primary DNS server.
WAN (when "Method" is set to "Route")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
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 VLAN tag of the layer 2 QoS packets for WAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for WAN port. The default value is 0.
LAN (when Method is set to "Route")	
IP Address	Enter the IP address assigned to 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	Enable or disable DHCP server capability. 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	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.

LAN (when Method is set to "Switch")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
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 VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.
LAN 1 / LAN 2 (when Method is set to "Dual")	
Default Interface	If "Dual" is selected as "Method", users will need assign the default interface to be LAN 1 (mapped to UCM6302 WAN port) or LAN 2 (mapped to UCM6302 LAN port) and then configure network settings for LAN 1/LAN 2. The default interface is LAN 2.
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings when the port is assigned as default interface. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
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 VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.

IPv6 Address	
WAN (when "Method" is set to "Route")	
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
LAN (when Method is set to "Route")	
DHCP Server	Select Disable, Auto or DHCPv6. • **Disable:** the DHCPv6 server is disabled. • **Auto:** Stateless address auto configuration using NDP protocol. • **DHCPv6:** Stateful address auto configuration using DHCPv6 protocol. The default setting is Disabled.
DHCP Prefix	Enter 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 DNS server 1 address for static settings. Default is (2001:4860:4860::8888)
DNS Server 2	Enter the DNS server 2 address for static settings. Default is (2001:4860:4860::8844)
Allow IP Address From	Configure starting IP address assigned by the DHCP prefix and DHCP prefixlen.
Allow IP Address To	Configure the ending IP address assigned by the DHCP Prefix and DHCP prefixlen.
Default IP Lease Time	Configure the lease time (in second) of the IP address.
LAN (when Method is set to "Switch")	
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
LAN 1 / LAN 2 (when Method is set to "Dual")	
Default Interface	Users will need assign the default interface to be LAN 1 (mapped to UCM630X WAN port) or LAN 2 (mapped to UCM630X LAN port) and then configure network settings for LAN 1/LAN 2. The default interface is LAN 1.
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.

IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.

- **Method: Route**

When the UCM630X has, 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.

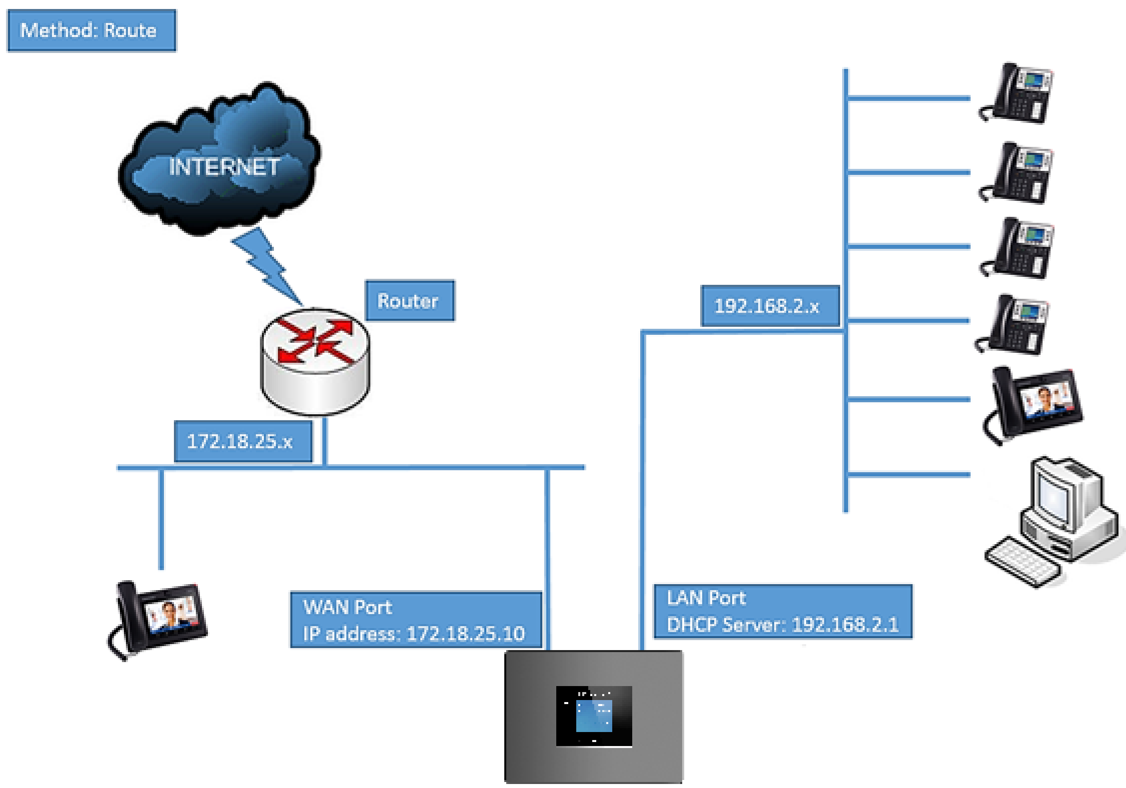


Figure 16: UCM6302 Network Interface Method: Route

- **Method: Switch**

WAN port interface is used for uplink connection; LAN port interface is used as room for PC connection.

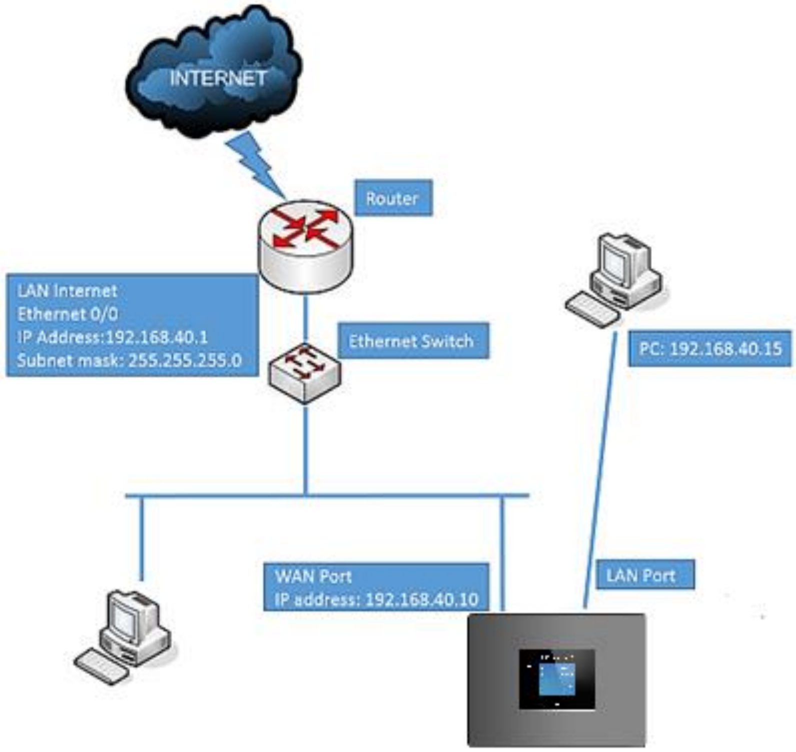


Figure 17: UCM6302 Network Interface Method: Switch

- **Method: Dual**

  Both WAN port and LAN port are used for uplink connection. Users will need 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.

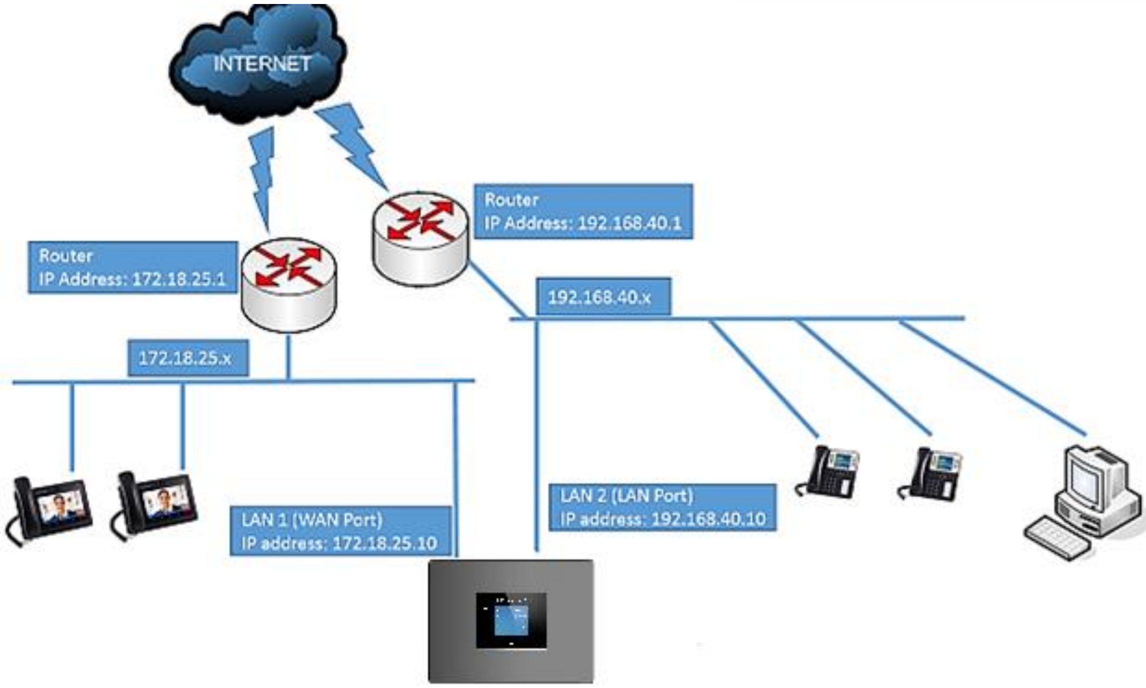


Figure 18: UCM6302 Network Interface Method: Dual

802.1X

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to device before the device can access Internet or other LAN resources. The UCM630X supports 802.1X as a supplicant/client to be authenticated. The following diagram and figure show UCM630X use 802.1X mode "EAP-MD5" on WAN port as client in the network to access Internet.

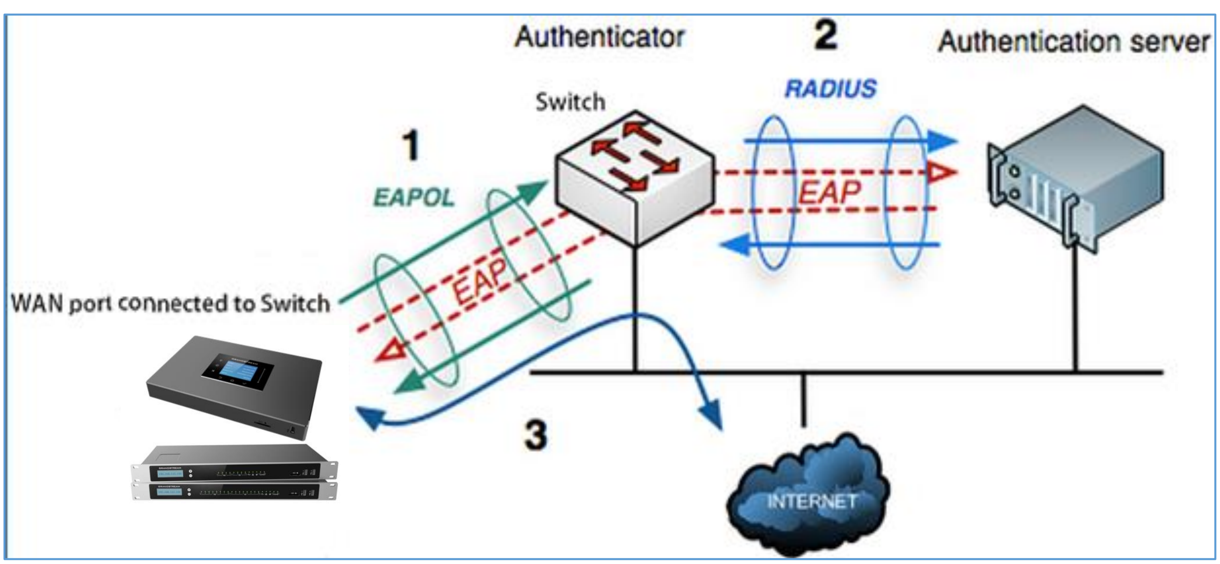


Figure 19: UCM630X Using 802.1X as Client

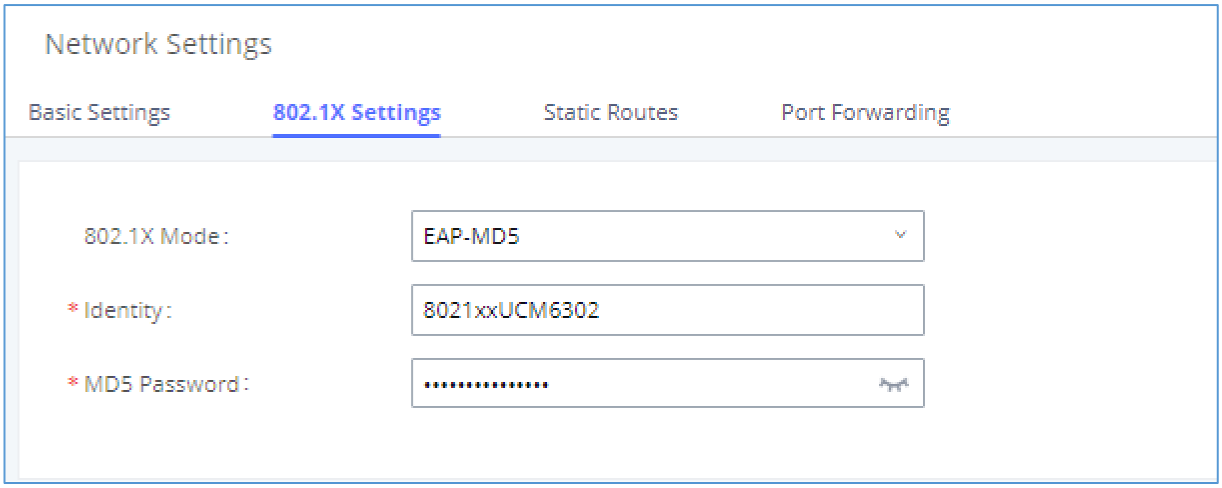


Figure 20: UCM630X Using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on UCM630X. Identity and MD5 password are required for authentication, which should be provided by the network administrator obtained from the RADIUS server. If "EAP-TLS" or "EAP-PEAPv0/MSCHAPv2" is used, users will also need to upload 802.1X CA Certificate and 802.1X Client Certificate, which should be also generated from the RADIUS server.

Table 8: UCM630X Network Settings→802.1X

802.1X Mode	Select 802.1X mode. The default setting is "Disable". The supported 802.1X mode are: • EAP-MD5 • EAP-TLS • EAP-PEAPv0/MSCHAPv2
Identity	Enter 802.1X mode Identity information.
MD5 Password	Enter 802.1X mode MD5 password information.
802.1X CA Certificate	Select 802.1X certificate from local PC and then upload.
802.1X Client Certificate	Select 802.1X client certificate from local PC and then upload.

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 on **"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.

Table 9: UCM630X Network Settings→Static Routes

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 subnet - ***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. 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 LCD menu→Network Menu.

The following diagram shows a sample application of static route usage on UCM6304.

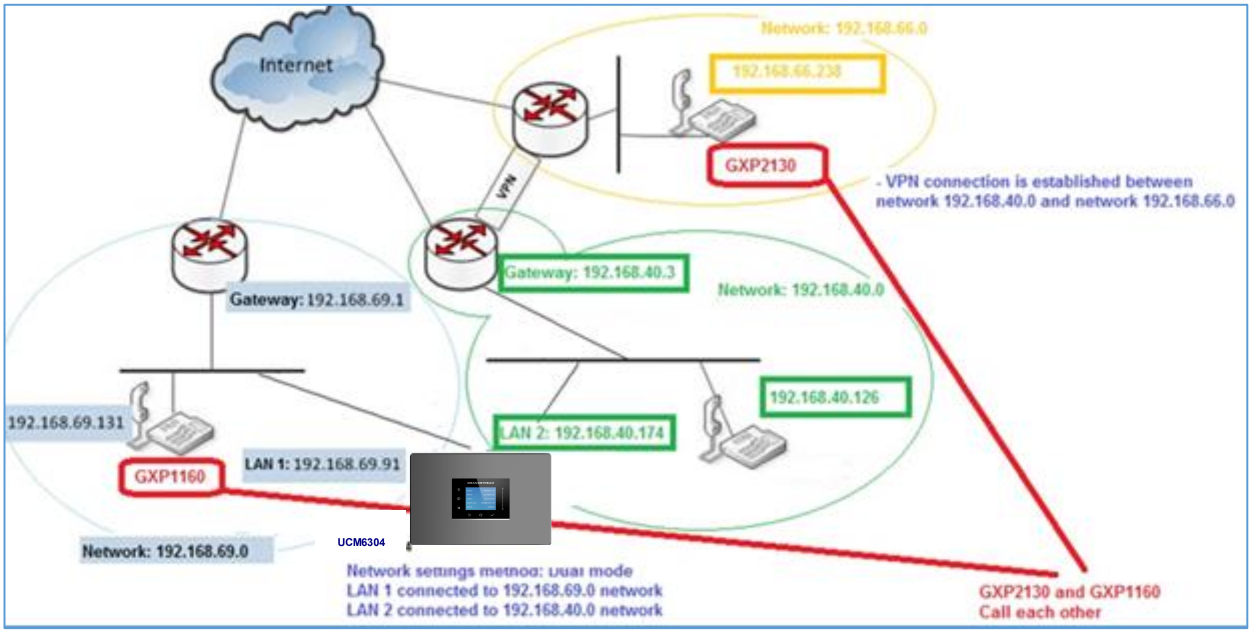


Figure 21: UCM6304 Static Route Sample

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 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 configure a static route on the UCM6304 so that the phones in isolated networks can make calls between each other.

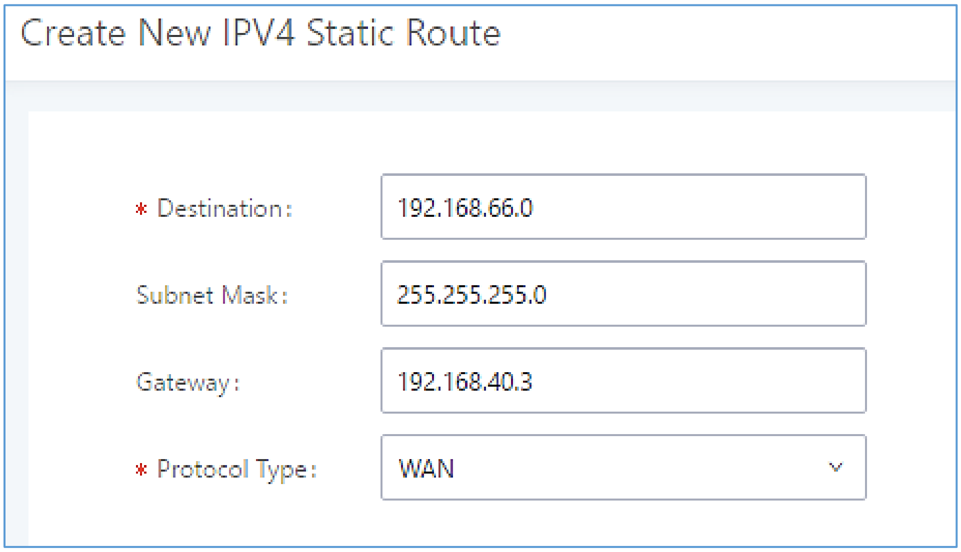


Figure 22: UCM6304 Static Route Configuration

Port Forwarding

The UCM network interface supports 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.

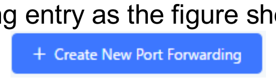
The port forwarding configuration is under Web GUI→**System Settings**→**Network Settings**→**Port Forwarding** page. Please see related settings in the table below.

Table 10: UCM630X Network Settings→Port Forwarding

WAN Port	Specify the WAN port number or a range of WAN ports. Unlimited number of ports can be configured. **Note:** When it is set to a range, 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 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, 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 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".

The following figures demonstrate a port forwarding example to provide phone's Web GUI access to public side.

- UCM630X network mode is set to "Route".
- UCM630X WAN port is connected to uplink switch, with a public IP address configured, e.g. 1.1.1.1.
- UCM630X LAN port provides 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 UCM630X DHCP pool.
- On the UCM630X Web GUI→**System Settings**→**Network Settings**→**Port Forwarding**, configure a port forwarding entry as the figure shows below.
- Click on 

  WAN Port: This is the port opened on the WAN side for access purpose.

  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 purpose.

  Protocol Type: We select TCP here for Web GUI access using HTTP.

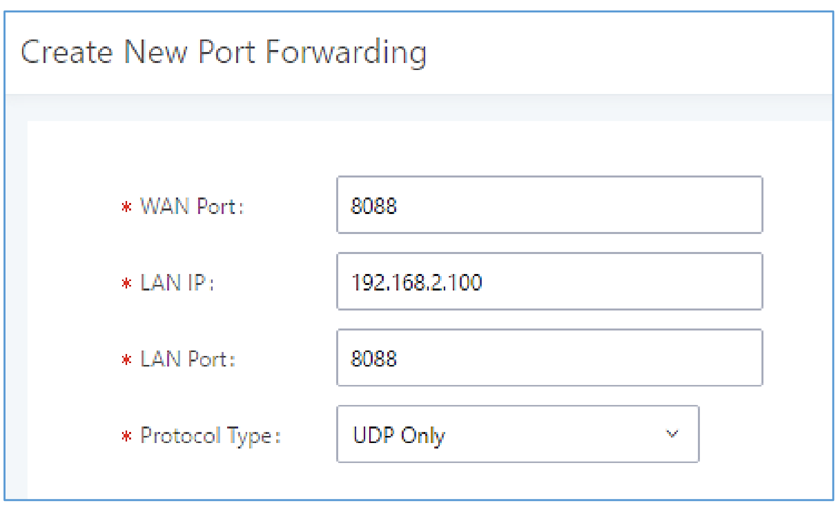


Figure 23: Create New Port Forwarding

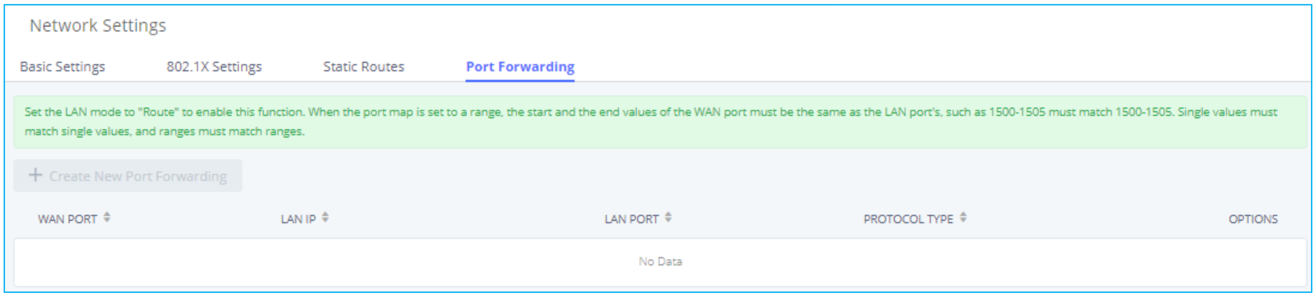


Figure 24: UCM630X Port Forwarding Configuration

This will allow users to access the GXP2160 Web GUI from public side, by typing in public IP address (example: 1.1.1.1:8088).

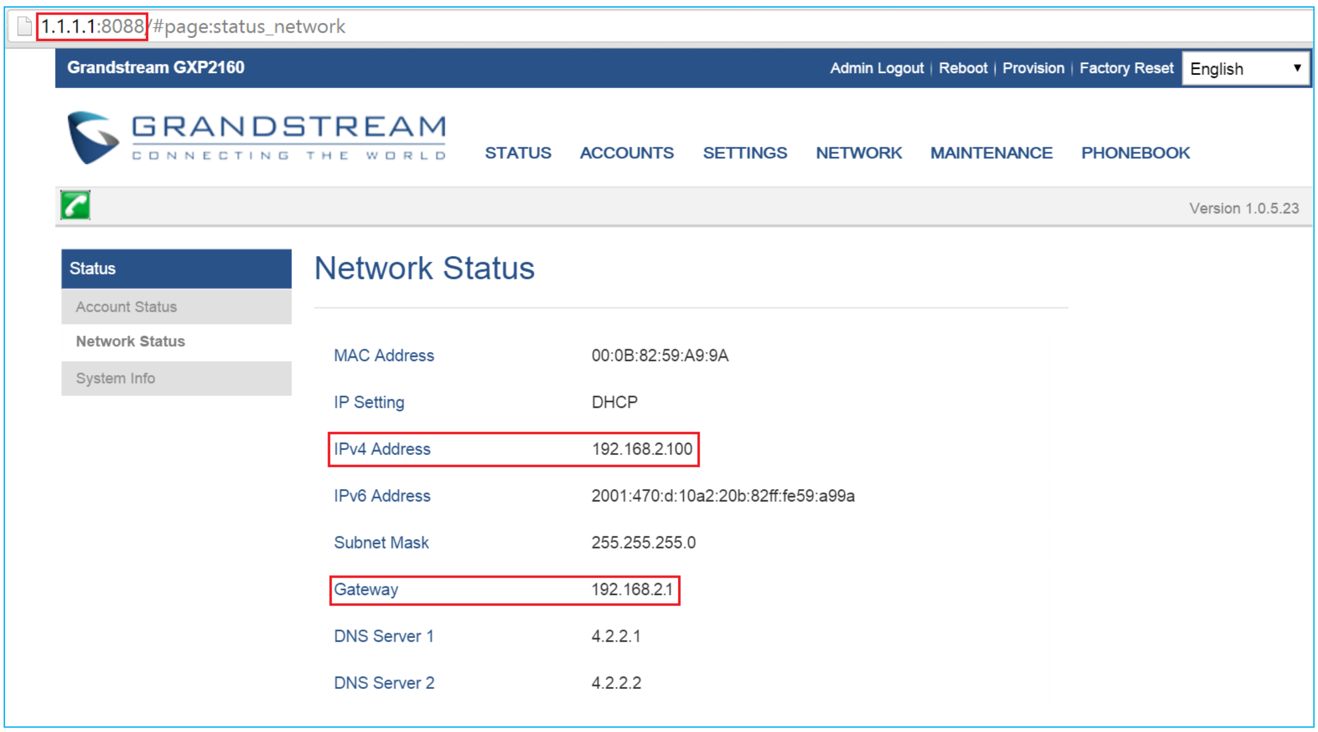


Figure 25: GXP2160 Web Access using UCM6302 Port Forwarding

ARP Settings

The ARP settings can be configured under Web GUI→**System Settings→Network Settings→ARP Settings**

Table 11: ARP Settings

ARP GC Threshold 1	Minimum number of entries to keep. 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	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.

OpenVPN®

OpenVPN® settings allow the users to configure UCM630X to use VPN features, the following table gives details about the various options in order to configure the UCM as OpenVPN Client.

Table 12: UCM630X System Settings→Network Settings→OpenVPN®

OpenVPN® Enable	Enable / Disable the OpenVPN® feature.
Configuration Method	Select OpenVPN® configuration method. **Manual Configuration:** Allows to configure OpenVPN® settings manually. **Upload Configuration File:** Allows to upload. ovpn and *.conf* files to the UCM and to automatically configure OpenVPN® settings.
OpenVPN® Server Address	Configures the hostname/IP and port of the server. For example: 192.168.1.2:22
OpenVPN® Server Protocol	Specify the protocol user, user should use the same settings as used on the server
OpenVPN® 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® 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® Encryption Algorithm	Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server.
OpenVPN® CA Cert	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
OpenVPN® Client Cert	Upload a client certificate. This file will be renamed as 'cliend.crt' automatically.
OpenVPN® Client Key	Upload a client private key. This file will be renamed as 'client.key' automatically.

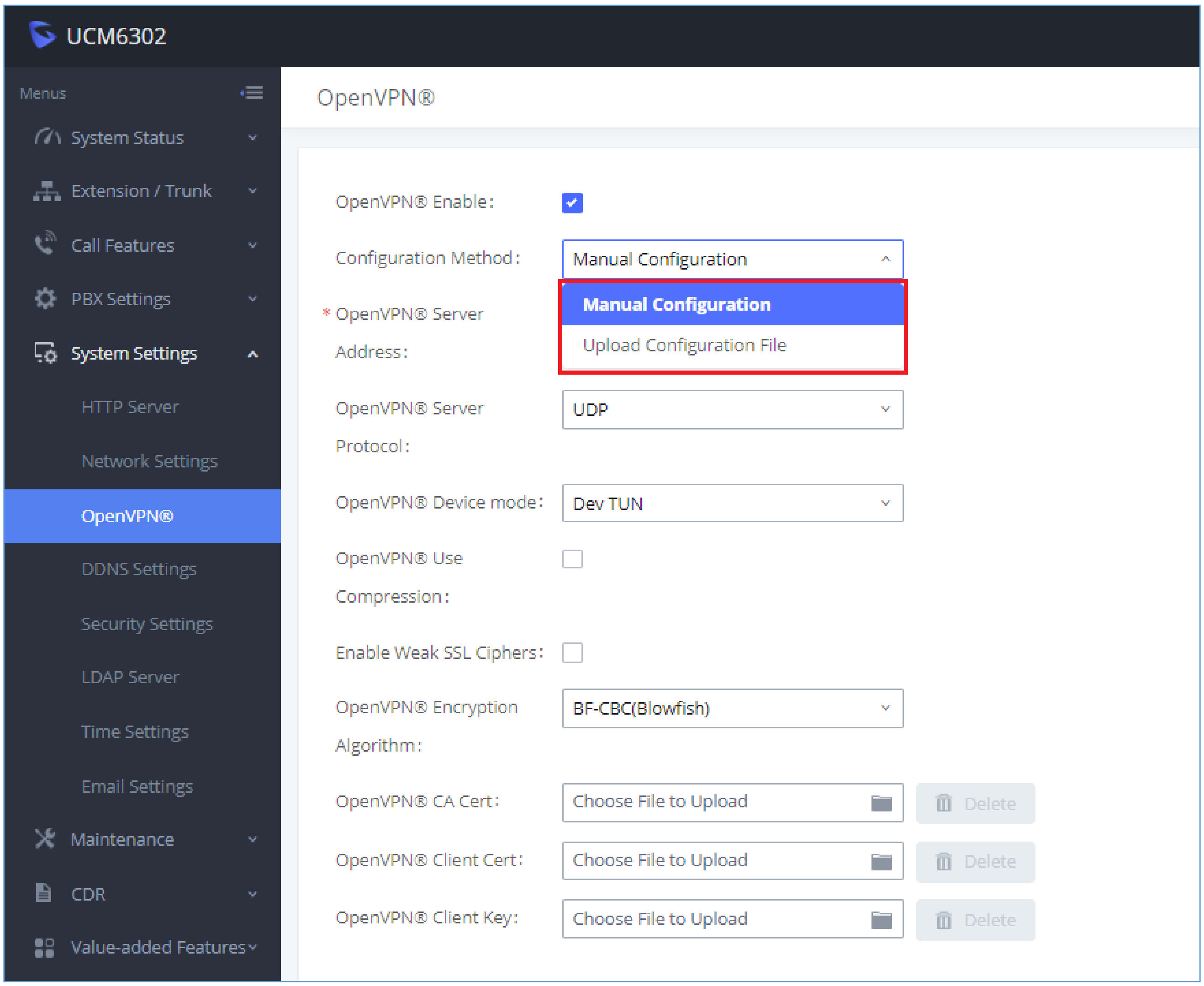


Figure 26: Open VPN® Feature on the UCM630X

DDNS Settings

DDNS setting allows user 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.

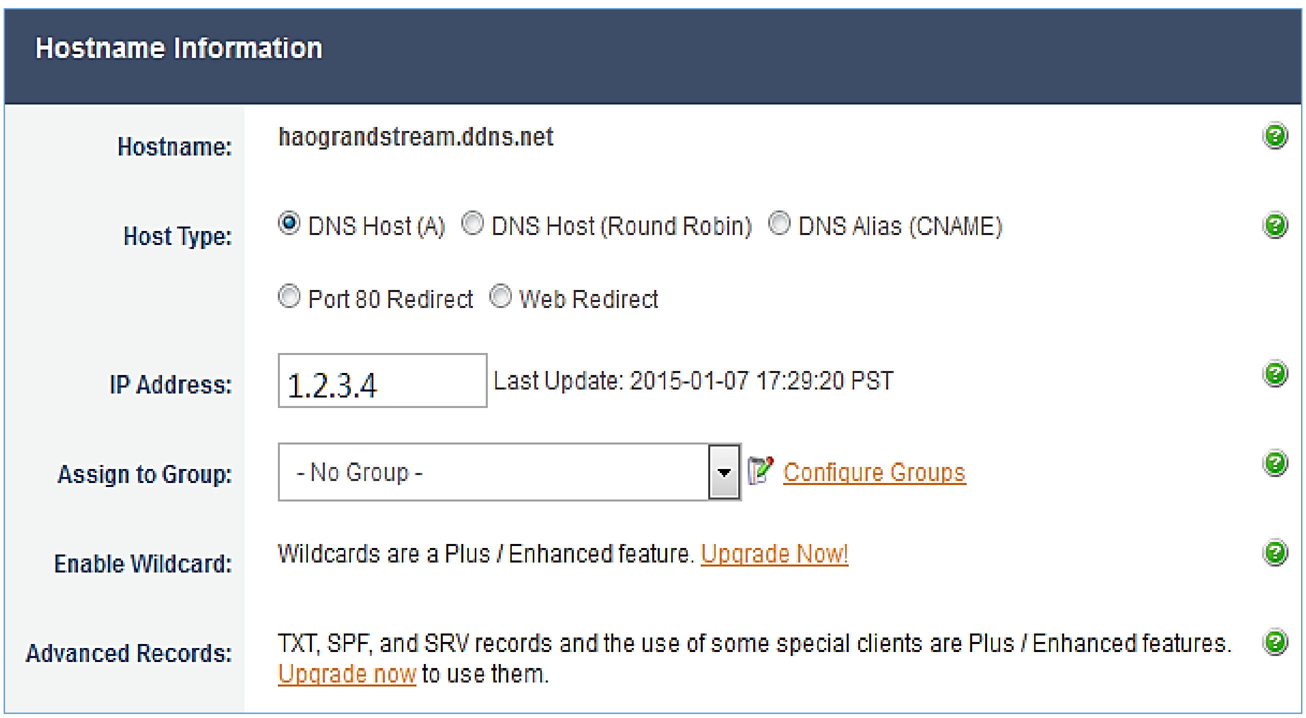


Figure 27: Register Domain Name on noip.com

2. On Web GUI→**System Settings→Network Settings→DDNS Settings,** enable DDNS service and configure username, password, and host name.

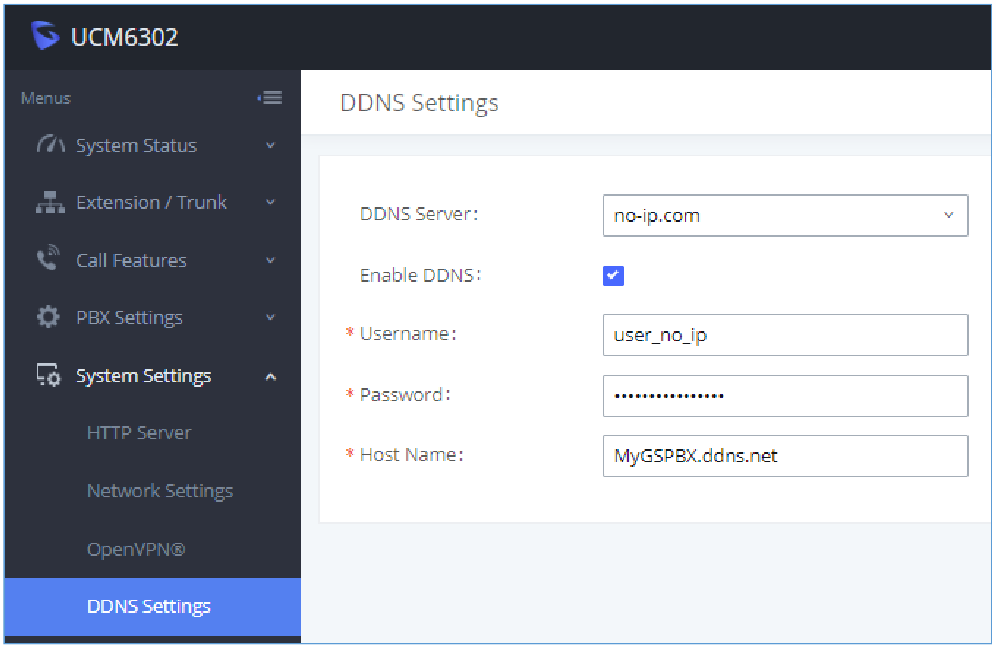


Figure 28: UCM630X DDNS Setting

3. Now you can use domain name instead of IP address to connect to the UCM630X Web GUI.

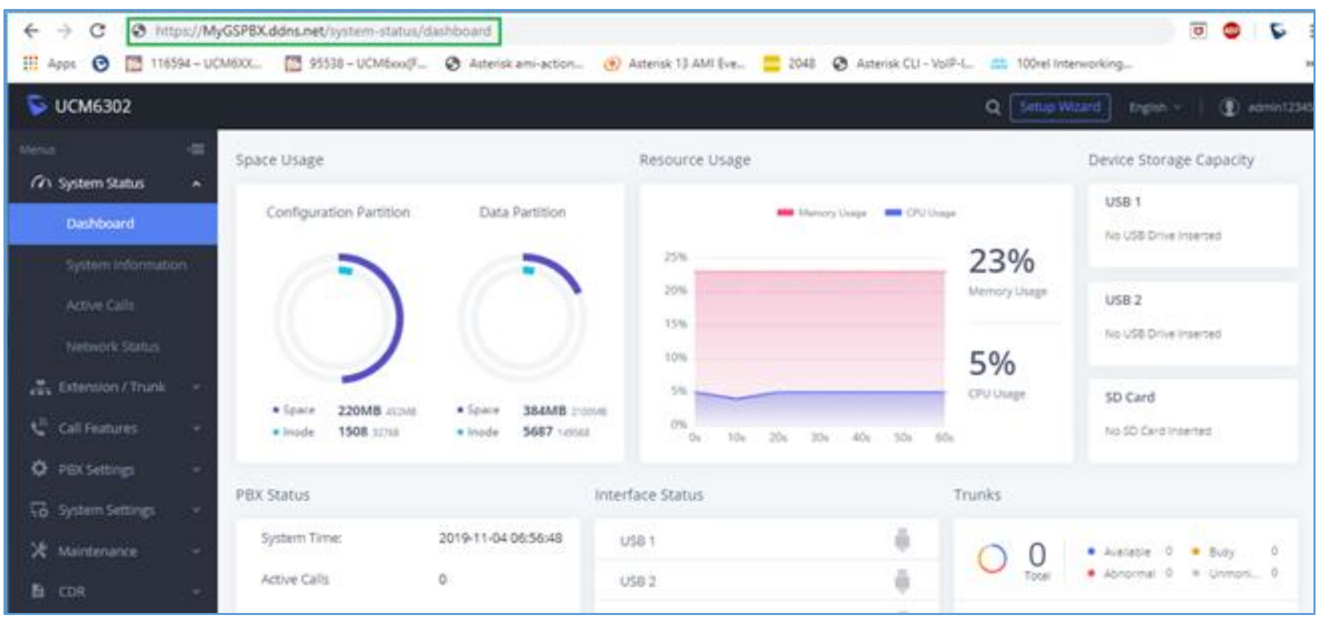


Figure 29: Using Domain Name to Connect to UCM630X

Security Settings

The UCM630X provides users firewall security configurations to prevent certain malicious attack 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 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.

Table 13: UCM630X Firewall→Static Defense→Current Service

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	SIP
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

For typical firewall settings, users could configure the following options on the UCM630X.

Table 14: Typical Firewall Settings

Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping request. 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.

Under "Custom Firewall Settings", users could create new rules to accept, reject or drop certain traffic going through the UCM630X. To create new rule, click on "Create New Rule" button and a new window will pop up for users to specify rule options.

Right next to "Create New Rule" button, there is a checkbox for 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"
- Destination port is set to the system login port (e.g., by default 8089)
- Protocol is not UDP

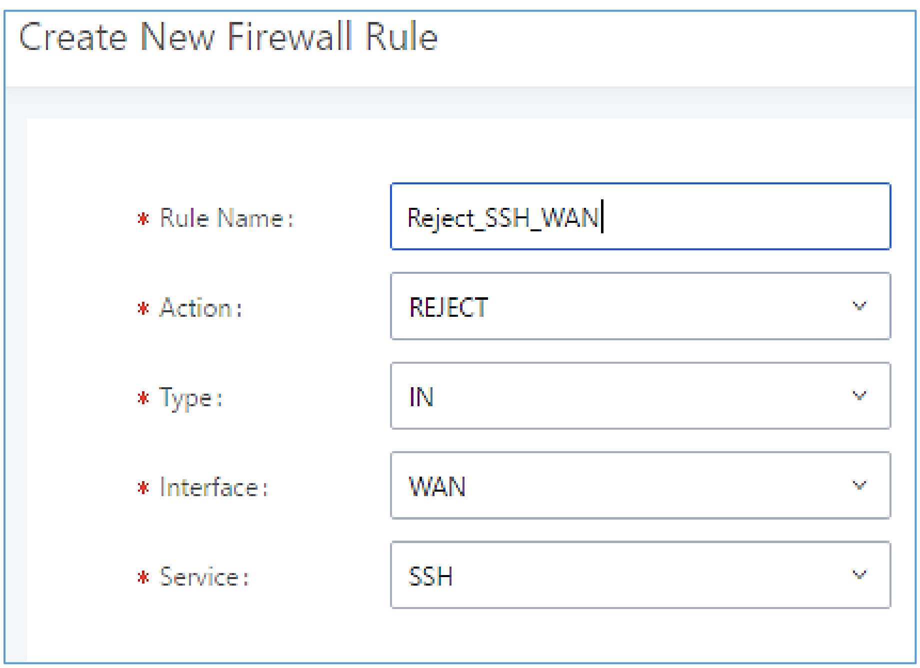


Figure 30: Create New Firewall Rule

Table 15: Firewall Rule Settings

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 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 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 "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 below:

- Click on to edit the rule.
- Click on 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 in the web page. Please refer to the following table for dynamic defense options on the UCM630X.

Table 16: UCM630X Firewall Dynamic Defense

Dynamic Defense Enable	Enable dynamic defense. The default setting is disabled.
Blacklist Update Interval	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 into the blacklist. The default setting is 100.
Dynamic Defense Whitelist	Allowed IPs and ports range, multiple IP addresses and port range. For example: ***192.168.2.100-192.168.2.105, 1000:9999***

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 into 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 whitelist, if a host initiates more than 20 TCP connections to the UCM630X it will not be added into UCM630X blacklist. It can still establish TCP connection with the UCM630X.

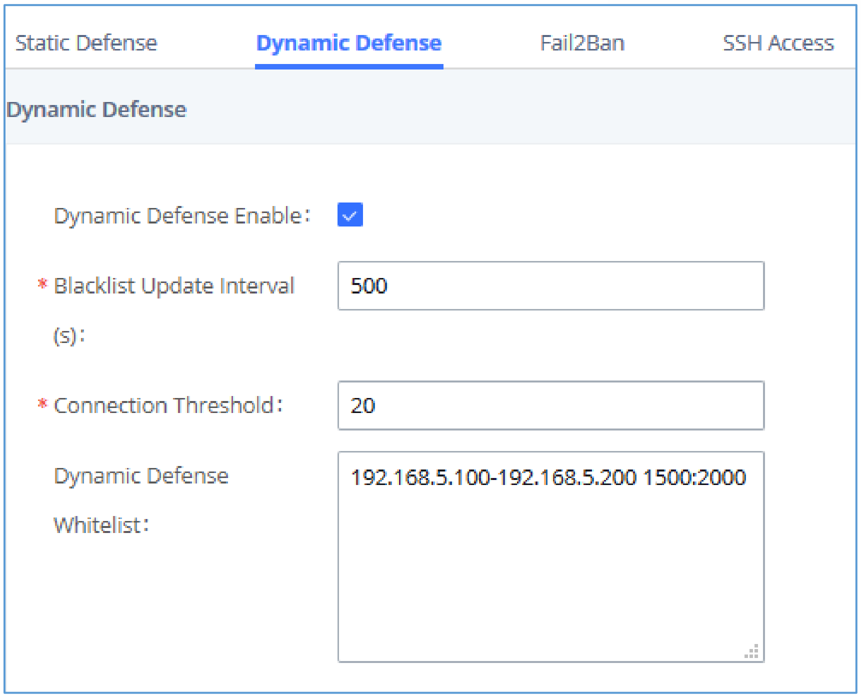


Figure 31: Configure Dynamic Defense

Fail2ban

Fail2Ban feature on the UCM630X provides intrusion detection and 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 certain period as defined in "Banned Duration". This feature helps prevent SIP brute force attacks to the PBX system.

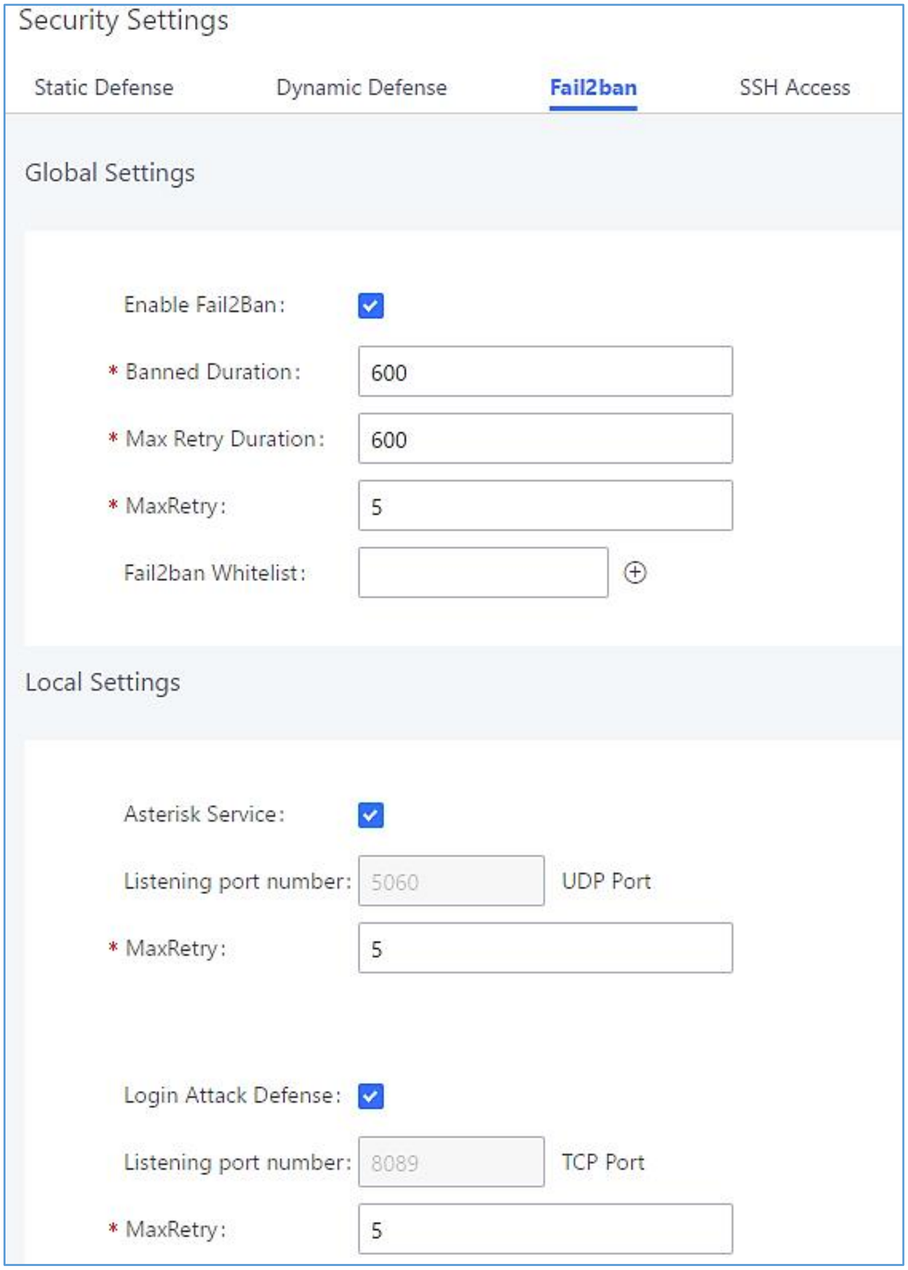


Figure 32: Fail2ban Settings

Table 17: Fail2Ban Settings

Global Settings	
Enable Fail2Ban	Enable Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on to use Fail2Ban for SIP authentication on the UCM630X.
Banned Duration	Configure the duration (in seconds) for the detected host to be banned. The default setting is 600. If set to 0, the host will be always banned.

Max Retry Duration	Within this duration (in seconds), if a host exceeds the max times of retry as defined in "MaxRetry", the host will be banned. The default setting is 600.
MaxRetry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5.
Fail2Ban Whitelist	Configure IP address, CIDR mask or DNS host in the whitelist. Fail2Ban will not ban the host with matching address in this list. Up to 20 addresses can be added into the list.
Local Settings	
Asterisk Service	Enable Asterisk service for Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on to use Fail2Ban for SIP authentication on the UCM630X.
Listening Port Number	Configure the listening port number for the service. By default, port 5060 will be used for UDP and TCP, and port 5061 will be used for TCP.
MaxRetry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5. Please make sure this option is properly configured as it will override the "MaxRetry" value under "Global Settings".
Login Attack Defense	Enables defense against excessive login attacks to the UCM's web GUI. The default setting is disabled.
Listening Port Number	This is the Web GUI listening port number which is configured under **System Settings→HTTP Server→Port**. The default is 8089.
MaxRetry	When the number of failed login attempts from an IP address exceeds the MaxRetry number, that IP address will be banned from accessing the Web GUI.
Blacklist	
Blacklist	Users will be able to view the IPs that have been blocked by UCM.

SSH Access

SSH switch now is available via Web GUI and LCD. User can enable or disable SSH access directly from Web GUI or LCD screen. For web SSH access, please log in 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 also requires the username and password of the super administrator. This option is turned off by default. It is recommended to turn off this option when debugging is not required.

Enable the "Enable remote SSH (via GDMS)" 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.

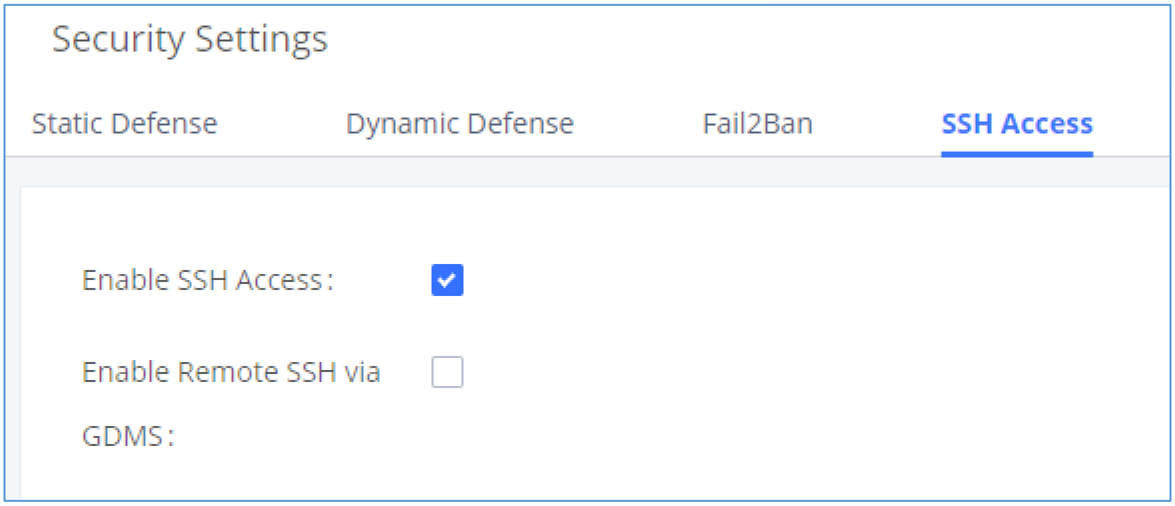


Figure 33: SSH Access

Table 18: SSH Access

Enable 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.
Enable Remote SSH via GDMS	If this option is enabled, remote SSH access will be allowed through the GDMS platform. It is strongly recommended to keep this disabled unless remote troubleshooting is necessary.

LDAP Server

The UCM630X has an embedded LDAP/LDAPS server for users to manage 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 a LDAP client to download phonebook entries from another LDAP server.
To access 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.

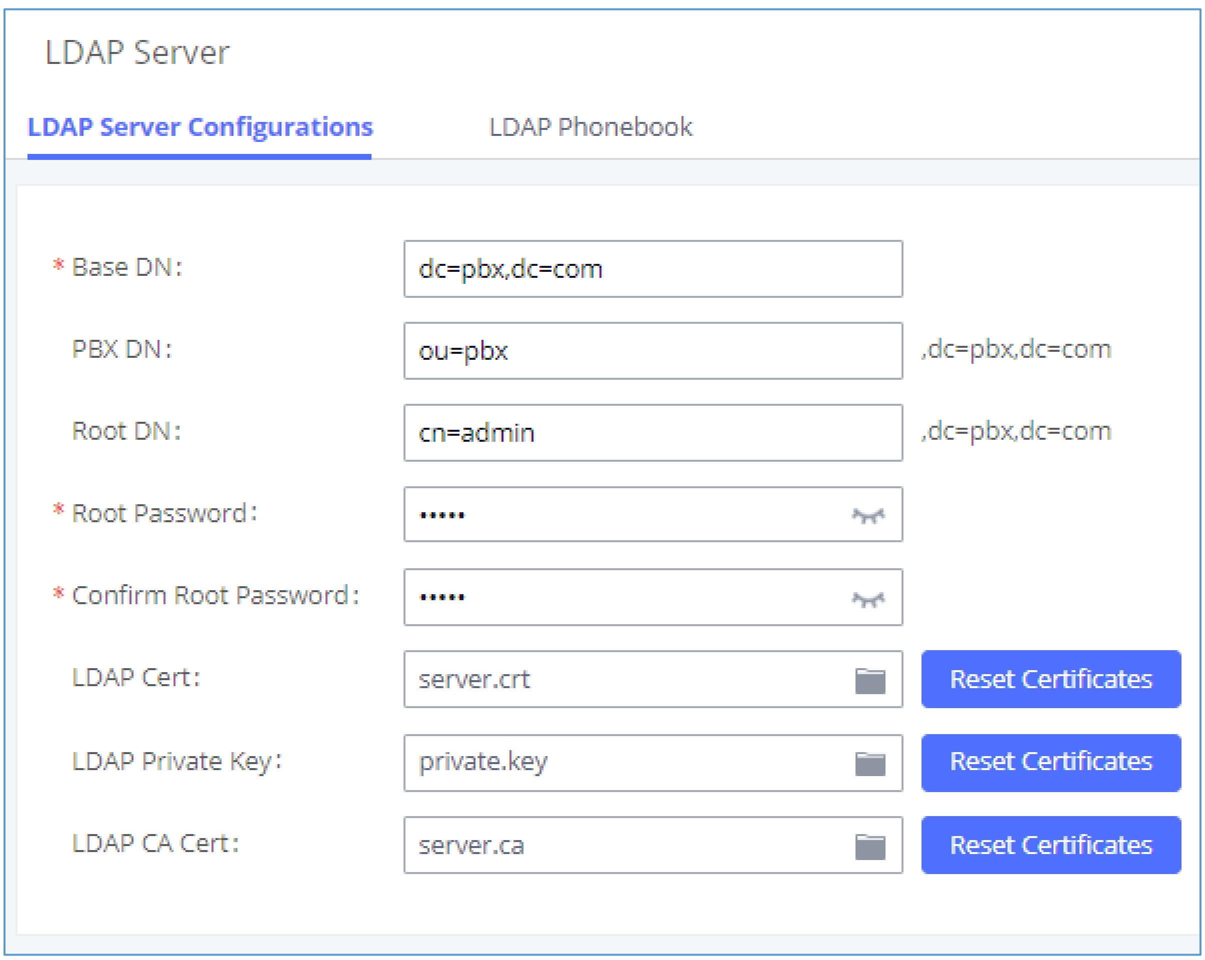


Figure 34: LDAP Server Configurations

The UCM630X LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client does not have to configure 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 provide for authentication purpose 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.

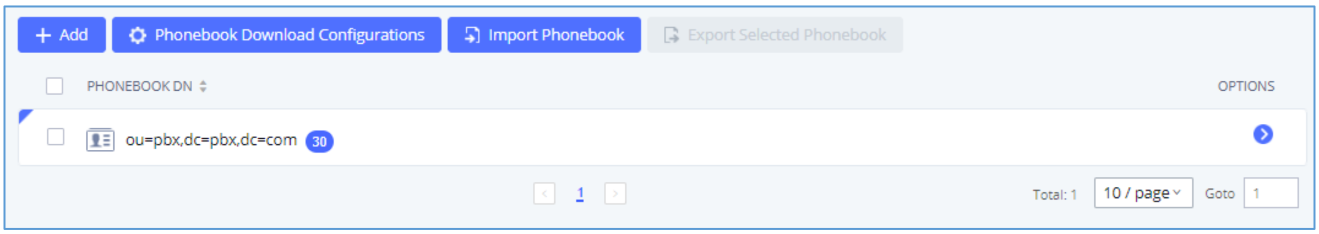


Figure 35: Default LDAP Phonebook DN

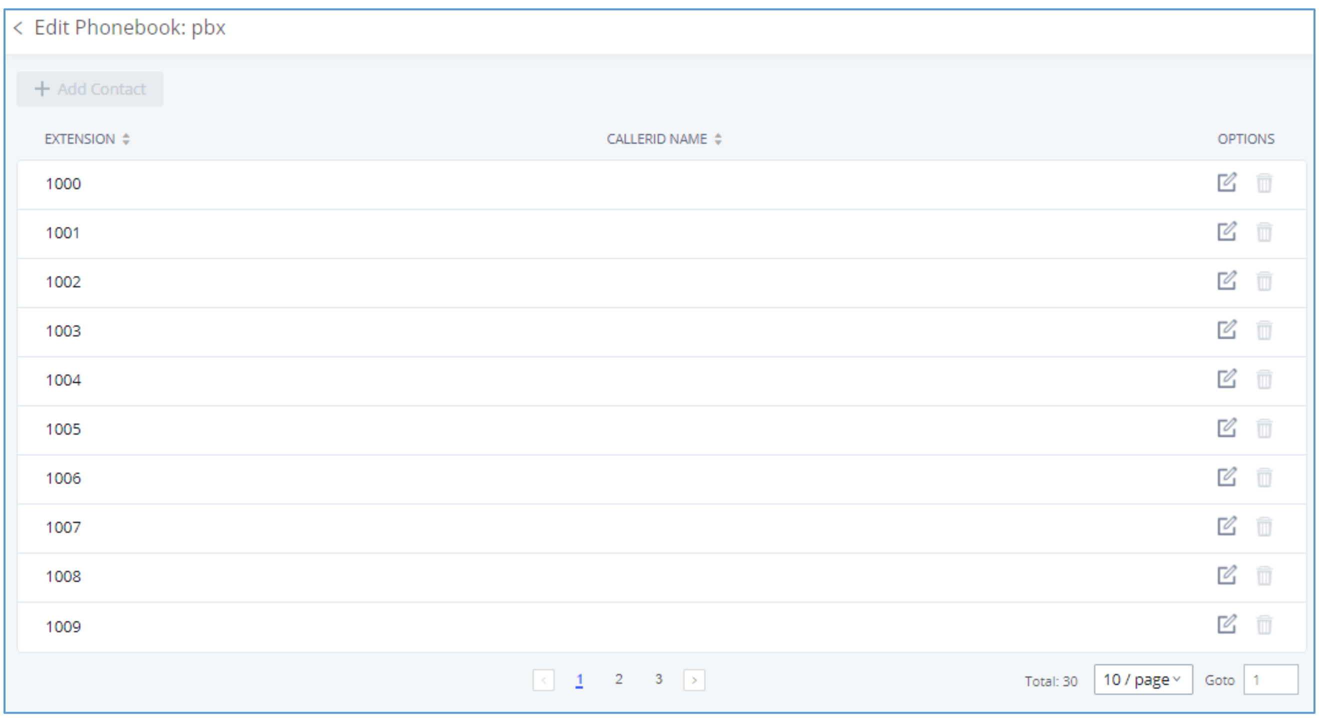


Figure 36: Default LDAP Phonebook Attributes

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. The first phonebook with default phonebook dn "ou=pbx,dc=pbx,dc=com" displayed on the LDAP server page is for extensions in this PBX. Users cannot add or delete contacts directly. The contacts information will need to be modified via Web GUI→**Extension/Trunk**→**Extensions** first. The default LDAP phonebook will then be updated automatically.

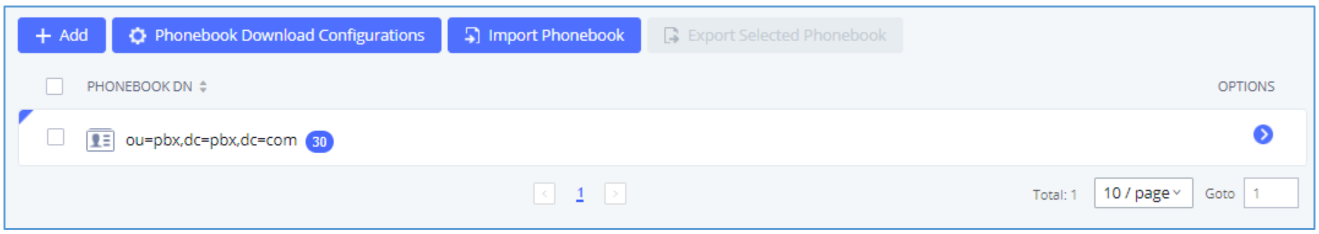


Figure 37: LDAP Server→LDAP Phonebook

- **Add new phonebook**

  A new sibling phonebook of the default PBX phonebook can be added by clicking on "Add" under "LDAP Phonebook" section.

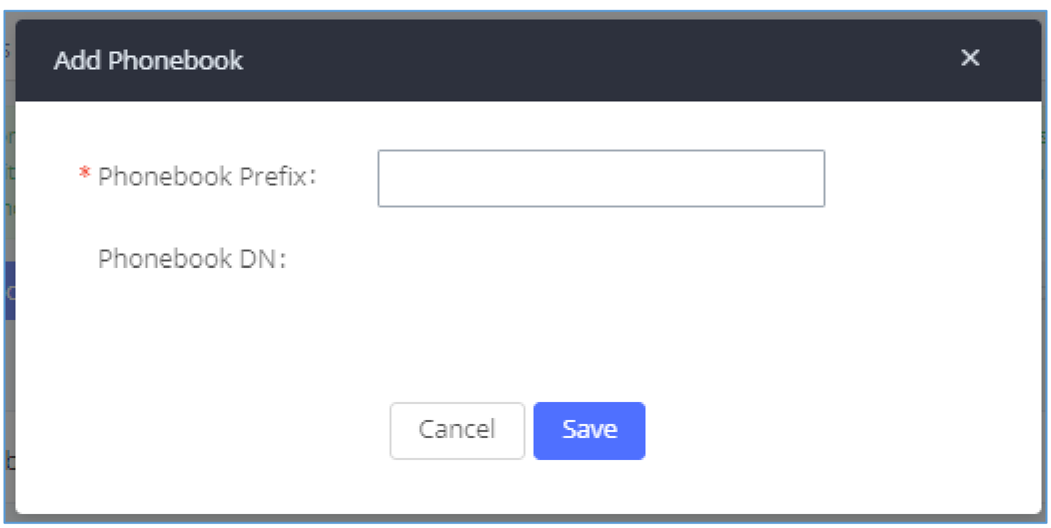


Figure 38: Add LDAP Phonebook

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.

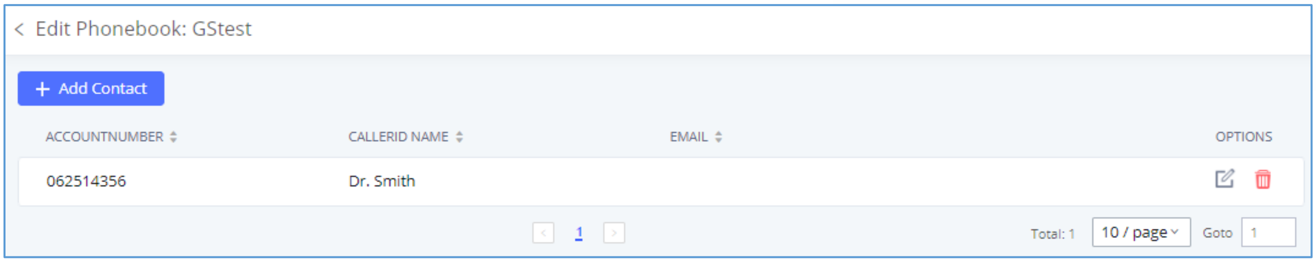


Figure 39: Edit LDAP Phonebook

- **Import phonebook from your computer to LDAP server**

Click on “Import Phonebook” and a dialog will prompt as shown in the figure below.

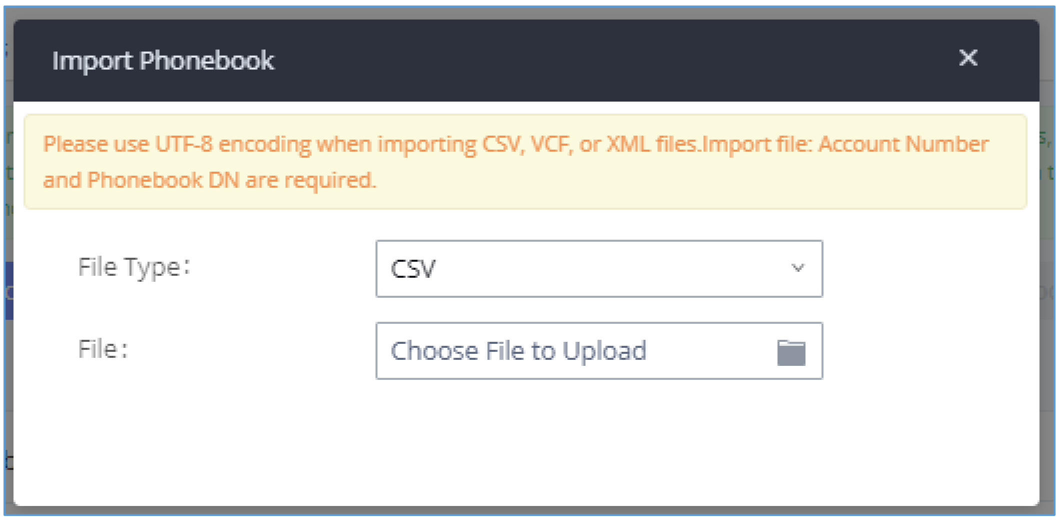


Figure 40: Import Phonebook

The file to be imported must be a CSV, VCF 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

Figure 41: 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.

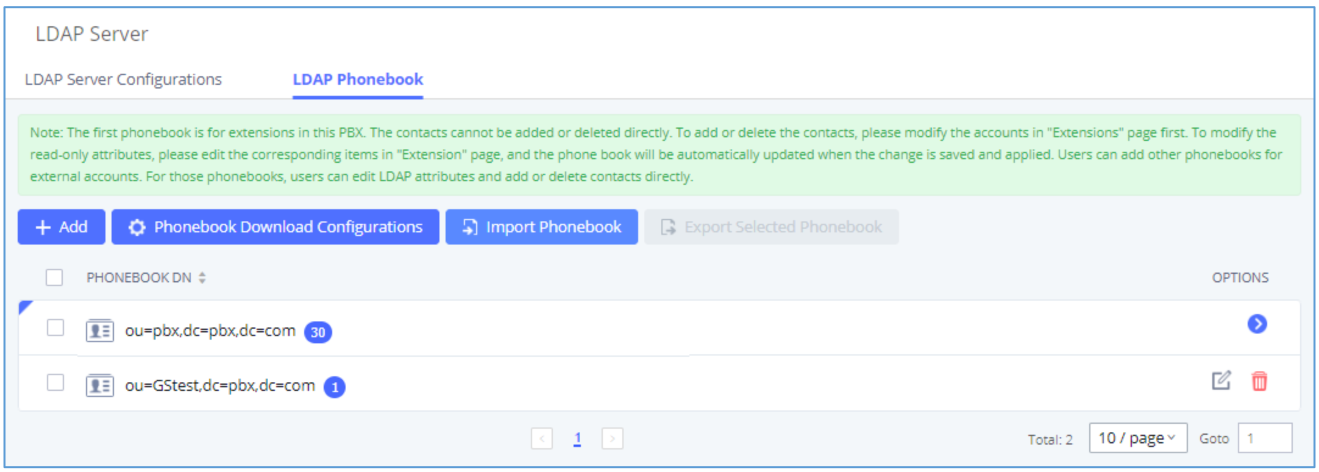


Figure 42: LDAP Phonebook After Import

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 CSV 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 or XML file for the users to add more contacts in it and import to the UCM630X again.

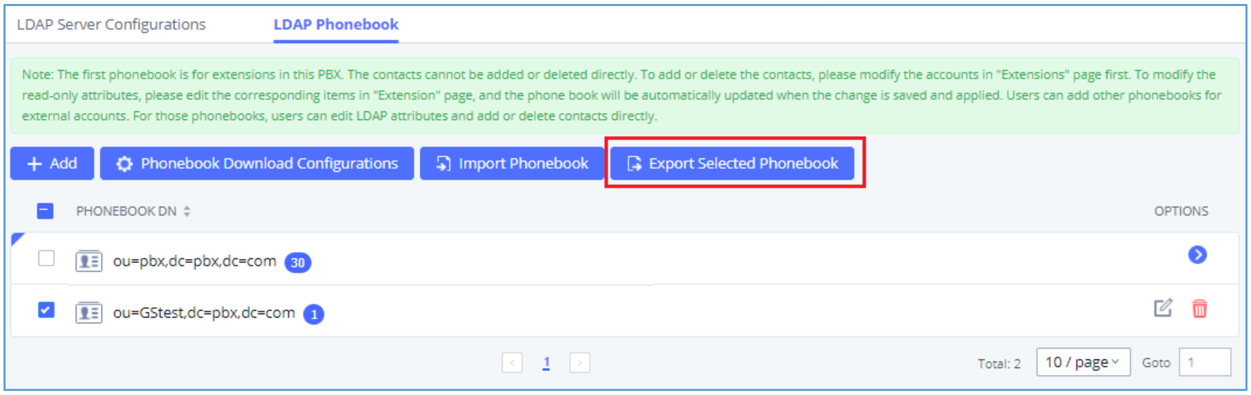


Figure 43: Export Selected LDAP Phonebook

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 Server :** Enter a name for the remote LDAP server
- **Server Address :** Enter the IP address or domain name for remote LDAP server.
- **Base DN:** dc=pbx,dc=com
- **Username:** Enter username if authentication is required
- **Password:** Enter password if authentication is required
- **Filter:** Enter the filter. Ex: (|(CallerIDName=%)(AccountNumber=%))
- **Port:** Enter the port number. Ex:389
- **LDAP Name Attributes:** Enter the name attributes for remote server
- **LDAP Number Attributes:** Enter the number attributes for remote server

The following figure gives a sample configuration for UCM acting as a LDAP client.

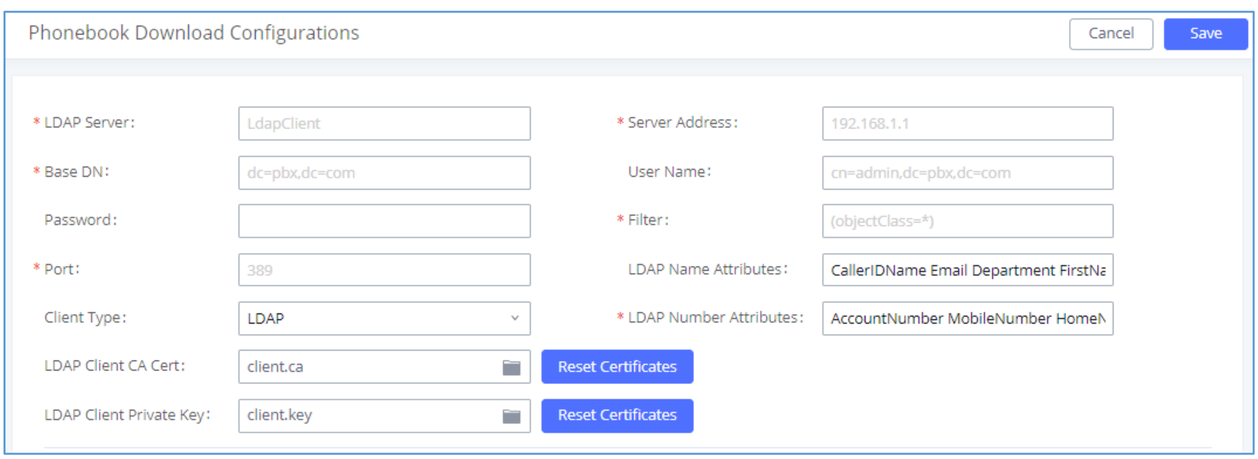


Figure 44: LDAP Client Configurations

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:** Please leave this field empty
- **Password:** Please leave this field empty
- **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 ***[Figure 34: LDAP Server Configurations]***.

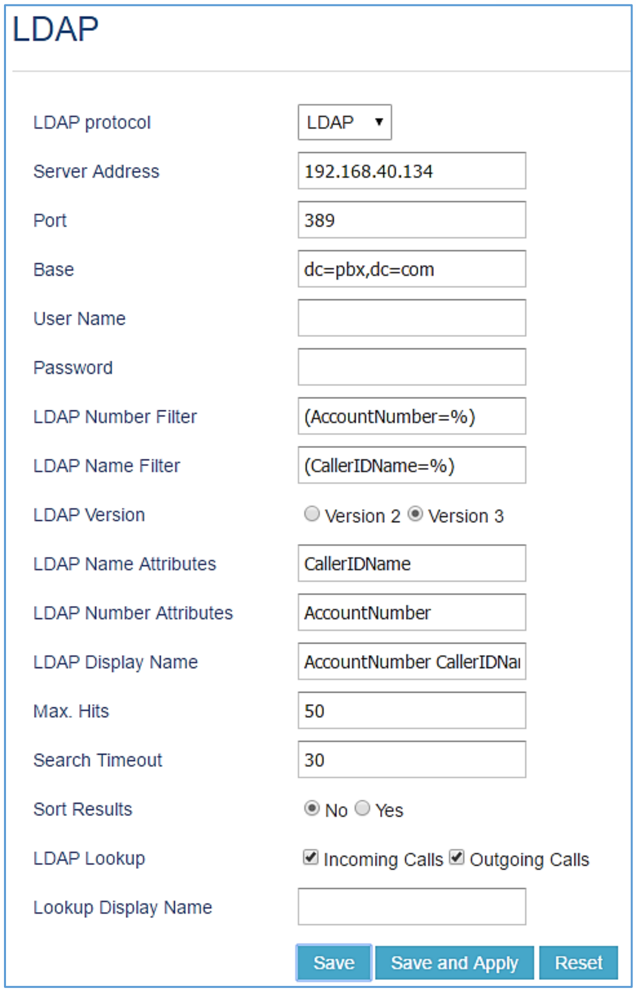


Figure 45: GXP2170 LDAP Phonebook Configuration

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**.

⚠ **Note:**

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.

Table 19: Time Auto Updating

Remote NTP Server	Specify the URL or IP address of the NTP server for the UCM630X to synchronize the date and time. The default NTP server is pool.ntp.org.
Enable DHCP Option 2	If set to "Yes", the UCM630X can get provisioned for Time Zone from DHCP Option 2 in the local server automatically. The default setting is "Yes".
Enable DHCP Option 42	If set to "Yes", the UCM630X can get provisioned for NTP Server from DHCP Option 42 in the local server automatically. This will override the manually configured NTP Server. The default setting is "Yes".
Time Zone	Select the proper time zone option so the UCM630X can display correct time accordingly.

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.

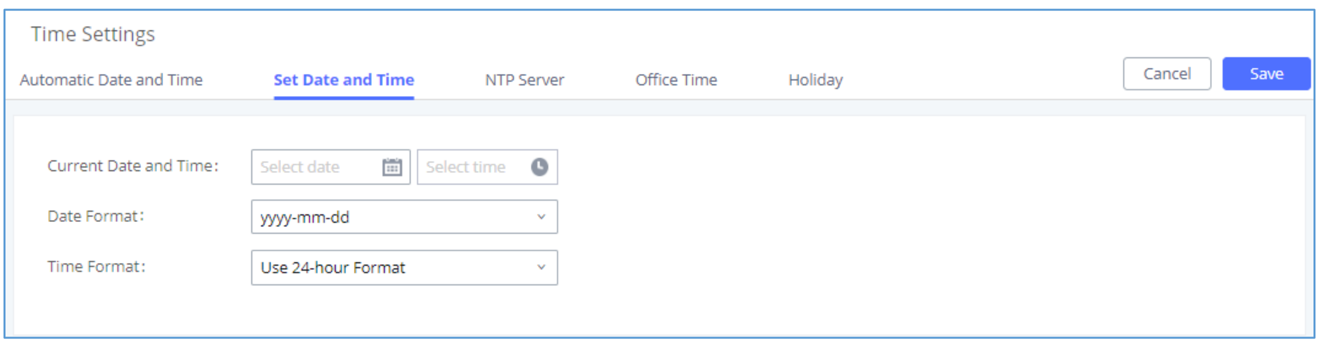


Figure 46: Set Time Manually

⚠ **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 schedule and inbound rule schedule. To configure office time, go to Web GUI→**System Settings→Time Settings→Office Time**. Click on "Add" to create an office time.

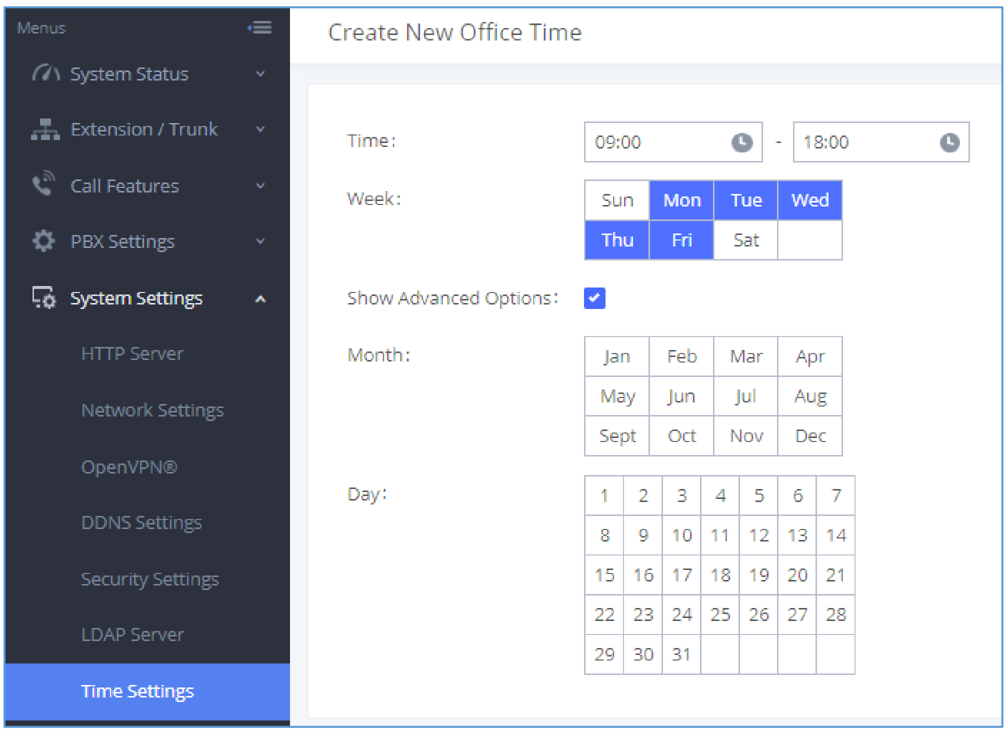


Figure 47: Create New Office Time

Table 20: 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.

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.

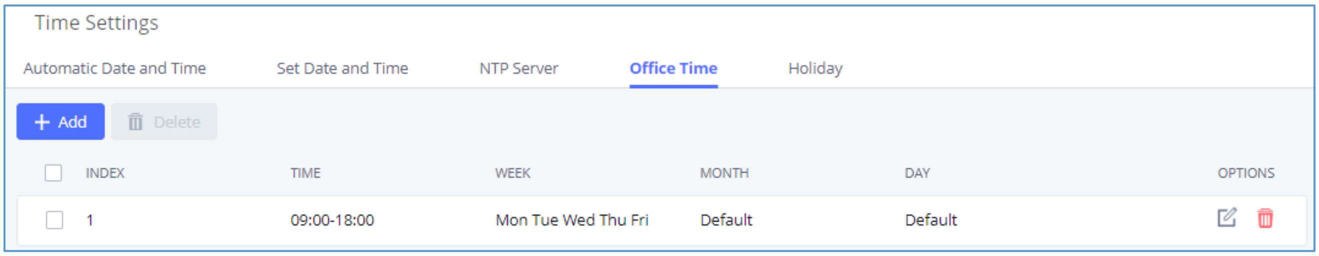


Figure 48: Settings→Time Settings→Office Time

- 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 UCM630X, the system administrator can define "holiday", which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure holiday, go to Web GUI→**System Settings→Time Settings→Holiday**. Click on **"Add"** to create holiday time.

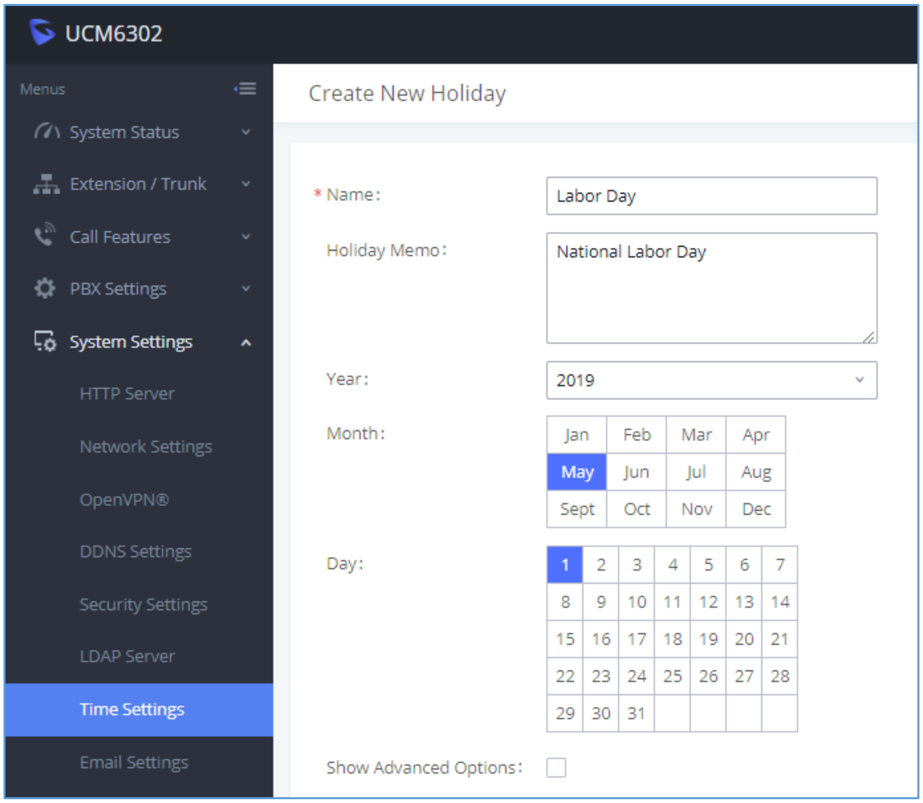


Figure 49: Create New Holiday

Table 21: Create New Holiday

Name	Specify the holiday name to identify this holiday.
Holiday Memo	Create a note for the holiday.
Month	Select the month for the holiday.
Day	Select the day for the holiday.
Show Advanced Options	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
Week	Select the days as holiday in one week.

Enter holiday "Name" and "Holiday Memo" for the new holiday. Then select "Month" and "Day". The system administrator can also define days in one week as advanced options. Once done, click on "Save" and then "Apply Change" for the holiday to take effect. The holiday will be listed in the web page as the figure shows below.

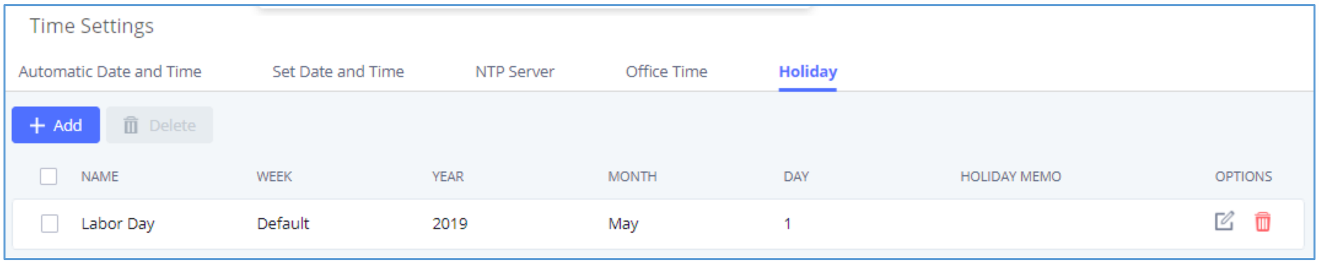


Figure 50: Settings→Time Settings→Holiday

- Click on to edit the holiday.
- Click on to delete the holiday.
- Click on **"Delete"** to delete multiple selected holidays at once.

⚠ **Note:**

For more details on how to use office time and holiday, please refer to the link below:
http://www.grandstream.com/sites/default/files/Resources/office_time_and_holiday_on_ucm6xxx.pdf

---

Email Settings

Email settings

The Email application on the UCM630X can be used to send out alert event Emails, Voicemail (Voicemail-To-Email) etc. The configuration parameters can be accessed via Web GUI→**System Settings→Email Settings→Email Settings**.

Table 22: Email Settings

TLS Enable	Enable or disable TLS during transferring/submitting your Email to another SMTP server. The default setting is "Yes".
Type	Select Email type. • **MTA:** Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it or no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. • **Client:** Submit Emails to the SMTP server. A SMTP server is required, and users need login with correct credentials.
Domain	Specify the domain name to be used in the Email when using type "MTA".

SMTP Server	Specify the SMTP server when using type "Client".
Enable SASL Authentication	Enable SASL Authentication. When disabled, UCM will not try to use the username and password for mail client login authentication. Most of the mail server requires login authentication while some others private mail servers allow anonymous login which requires disabling this option to send Email as normal. For Exchange Server, please disable this option.
Username	Username is required when using type "Client". Normally it is the Email address.
Password	Password to login for the above Username (Email address) is required when using type "Client".
POP/POP3 Server Address	Configure the POP/POP3 server address for the configured username Example: pop.gmail.com
POP/POP3 Server Port	Configure the POP/POP3 server port for the configured username Example: 995
Display Name	Specify the display name in the FROM header in the Email.
Sender	Specify the sender's Email address. For example: pbx@example.mycompany.com.

The following figure shows a sample Email setting on the UCM630X, assuming the Email is using *192.168.6.202* as the SMTP server.

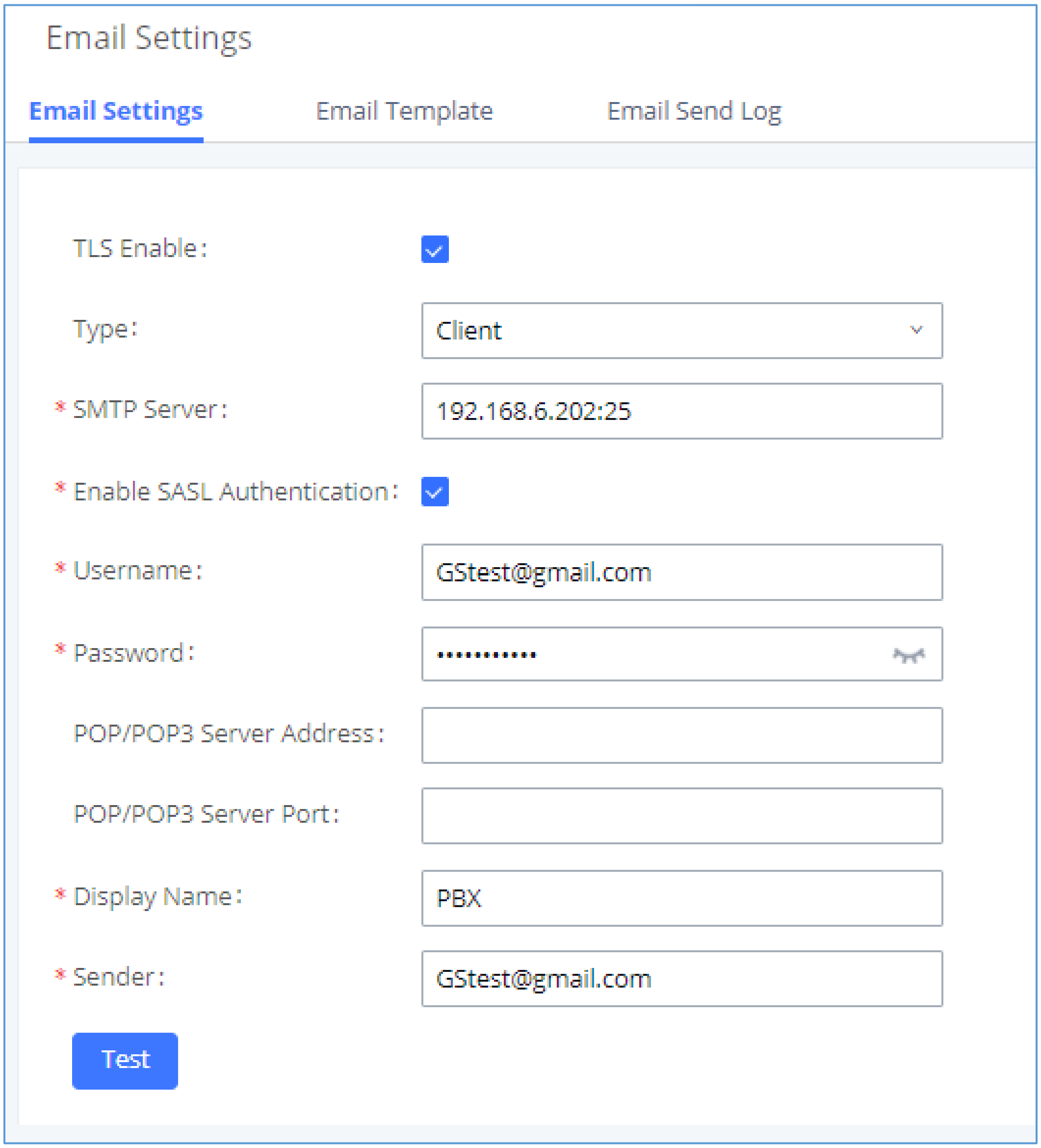
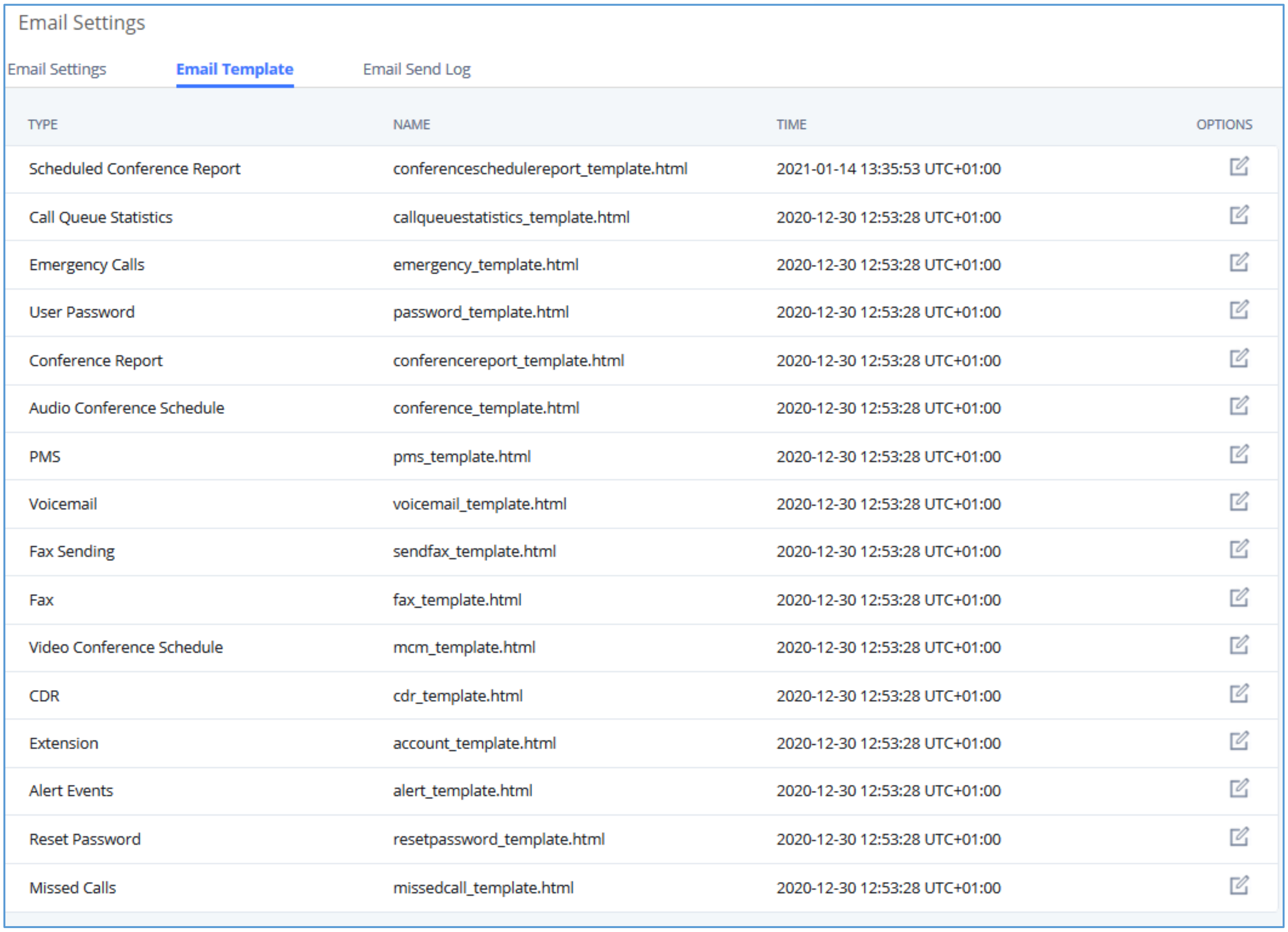


Figure 51: UCM630X Email Settings

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 Templates

The Email templates on the UCM630X can be used for email notification, the configuration parameters can be accessed via Web GUI→**Settings**→**Email Settings**→**Email Templates**.



Email Settings

Email Settings | **Email Template** | Email Send Log

TYPE	NAME	TIME	OPTIONS
Scheduled Conference Report	conferenceschedulereport_template.html	2021-01-14 13:35:53 UTC+01:00	
Call Queue Statistics	callqueuestatistics_template.html	2020-12-30 12:53:28 UTC+01:00	
Emergency Calls	emergency_template.html	2020-12-30 12:53:28 UTC+01:00	
User Password	password_template.html	2020-12-30 12:53:28 UTC+01:00	
Conference Report	conferencereport_template.html	2020-12-30 12:53:28 UTC+01:00	
Audio Conference Schedule	conference_template.html	2020-12-30 12:53:28 UTC+01:00	
PMS	pms_template.html	2020-12-30 12:53:28 UTC+01:00	
Voicemail	voicemail_template.html	2020-12-30 12:53:28 UTC+01:00	
Fax Sending	sendfax_template.html	2020-12-30 12:53:28 UTC+01:00	
Fax	fax_template.html	2020-12-30 12:53:28 UTC+01:00	
Video Conference Schedule	mcm_template.html	2020-12-30 12:53:28 UTC+01:00	
CDR	cdr_template.html	2020-12-30 12:53:28 UTC+01:00	
Extension	account_template.html	2020-12-30 12:53:28 UTC+01:00	
Alert Events	alert_template.html	2020-12-30 12:53:28 UTC+01:00	
Reset Password	resetpassword_template.html	2020-12-30 12:53:28 UTC+01:00	
Missed Calls	missedcall_template.html	2020-12-30 12:53:28 UTC+01:00	

Figure 52: Email Template

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.

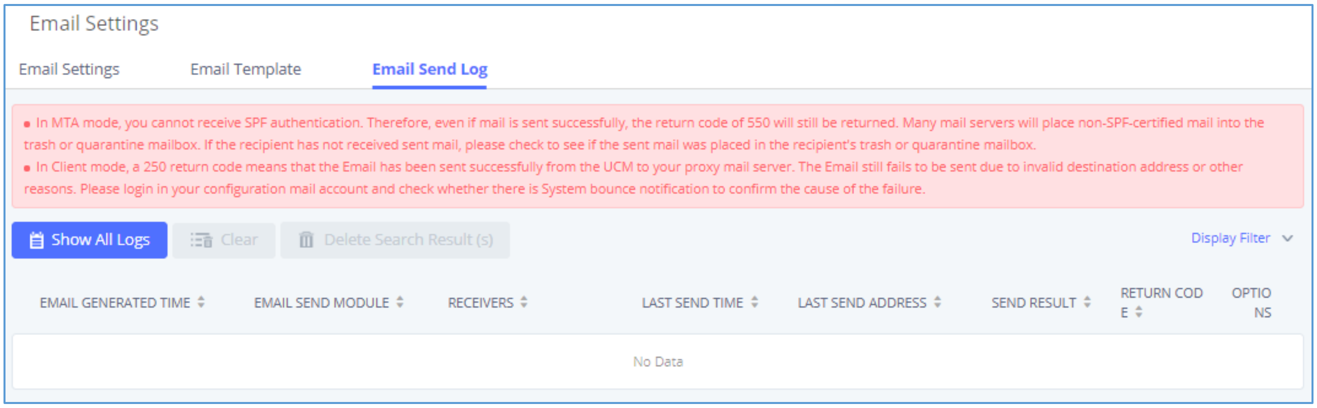
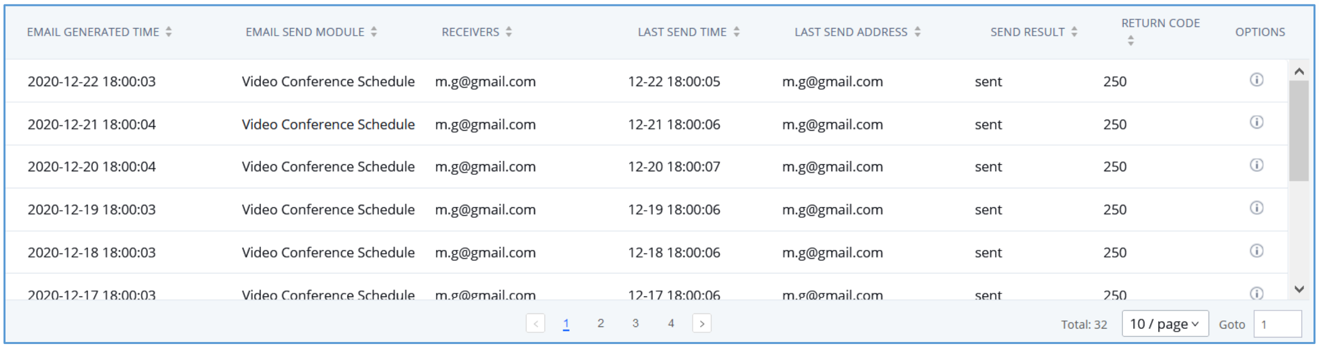


Figure 53: Email Send Log

Table 23: Email Log – Display Filter

Field	Description
Start Time	Enter the start time for filter
End Time	Enter the end time for filter
Receivers	Enter the email recipient, while searching for multiple recipients, please separate then with 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 logs will be shown on bottom of the “Email Send Log” page, as shown on the following figure.



EMAIL GENERATED TIME	EMAIL SEND MODULE	RECEIVERS	LAST SEND TIME	LAST SEND ADDRESS	SEND RESULT	RETURN CODE	OPTIONS
2020-12-22 18:00:03	Video Conference Schedule	m.g@gmail.com	12-22 18:00:05	m.g@gmail.com	sent	250	
2020-12-21 18:00:04	Video Conference Schedule	m.g@gmail.com	12-21 18:00:06	m.g@gmail.com	sent	250	
2020-12-20 18:00:04	Video Conference Schedule	m.g@gmail.com	12-20 18:00:07	m.g@gmail.com	sent	250	
2020-12-19 18:00:03	Video Conference Schedule	m.g@gmail.com	12-19 18:00:06	m.g@gmail.com	sent	250	
2020-12-18 18:00:03	Video Conference Schedule	m.g@gmail.com	12-18 18:00:06	m.g@gmail.com	sent	250	
2020-12-17 18:00:03	Video Conference Schedule	m.g@gmail.com	12-17 18:00:06	m.g@gmail.com	sent	250	

1 2 3 4 Total: 32 10 / page Goto 1

Figure 54: Email Logs

Below are the codes returned when sending emails and their description:

Table 24: 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 user name and password verification in the client mode is incorrect. Please check whether the user name and password are configured correctly.
550	Possible reasons: 1. The recipient's mailbox user name does not exist or is in a banned state, please check whether the email recipient is the correct email address. 2. 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. 3. 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	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".

TR-069

To configure TR-069 on Grandstream devices, set 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.
Periodic Inform Enable	Enables periodic inform. If set to 'Yes', device will send inform packets to the ACS.
Periodic Inform Interval	Periodic time when UCM630X will send inform packets to TR-069 ACS server. This option is specified in seconds.
ACS Connection Request Username	The username for the ACS to connect to UCM.
ACS Connection Request Password	The password for the ACS to connect to UCM.
Connection Request Port	Port for incoming connection requests. The default value is **7547**.
CPE Cert File	The Cert file for UCM to connect to the ACS via SSL.
CPE Cert Key	The Cert key for UCM to connect to the ACS via SSL.

PROVISIONING

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 Grandstream SIP devices in a zero-configuration manner by generating XML config file and having the phone to download it within LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

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 Web GUI→**Value-added Features**→**Zero Config**.

Configuration Architecture for End Point Device

Started from firmware version 1.0.7.10, the end point device configuration in zero config 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 Grandstream 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 individual device here.

Each layer also has its own structure in different levels. Please see figure below. The details for each layer are explained in sections ***[Global Configuration]***, ***[Model configuration]*** and ***[*Device Configuration*]***.

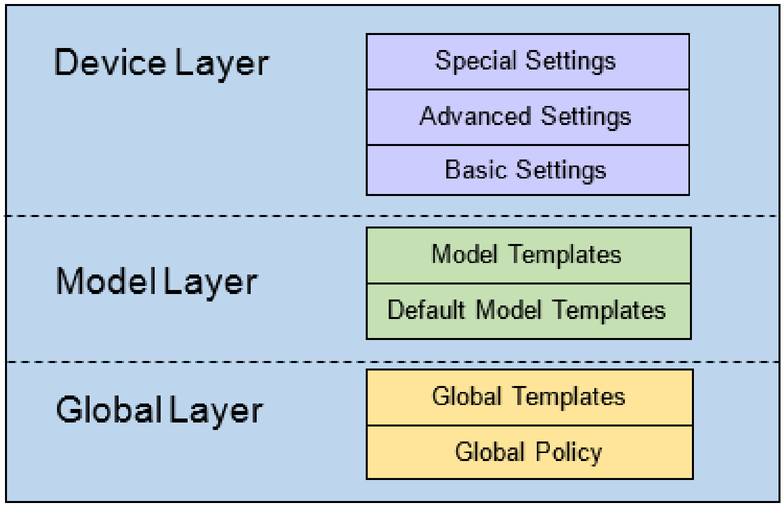


Figure 55: Zero Config Configuration Architecture for End Point Device

The configuration options in model layer and device layer have all the option in global layers already, i.e., the options in global layer is a subset of the options in model layer and device layer. If an option is set in all three layers with different values, the highest layer value will override the value in lower layer. For example, if the user selects English for Language setting in Global Policy and Spanish for Language setting in Default Model Template, the language setting on the device to be provisioned will use Spanish as model layer has higher priority than global layer. To sum up, **configurations in higher layer will always override the configurations for the same options/fields in the lower layer when presented at the same time.**

After understanding the zero-config configuration architecture, users could configure the available options for end point devices to be provisioned by the UCM630X by going through the three layers. This configuration architecture allows users to set up and manage the Grandstream end point devices in the same LAN area in a centralized way.

Auto Provisioning Settings

By default, the Zero Config feature is enabled on the UCM630X for auto provisioning. Three methods of auto provisioning are used.

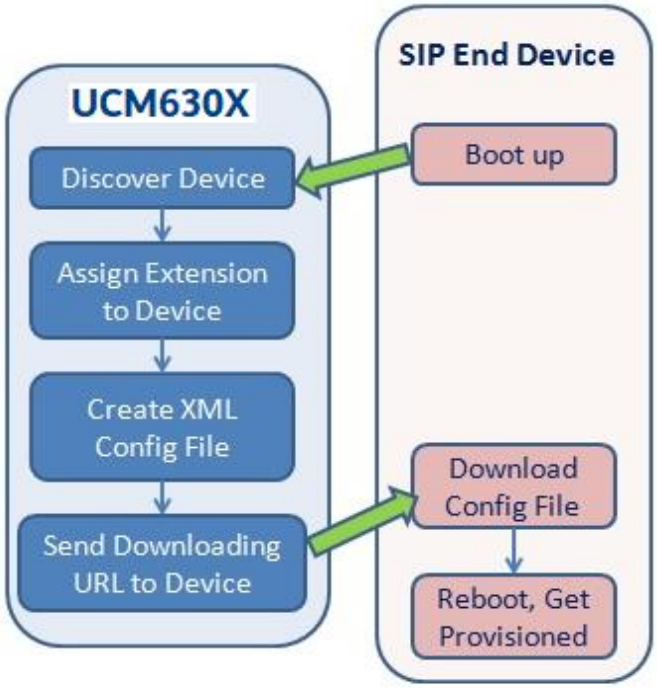


Figure 56: UCM630X Zero Config

- **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.

- **mDNS**
  When the phone boots up, it sends out mDNS query to get the TFTP server address. The UCM630X will respond with its own address. The phone will then send TFTP request to download the XML config file from the UCM630X.

To start the auto provisioning process, under Web GUI→**Value-added Features**→**Zero Config**→**Zero Config Settings**, fill in the auto provision information.

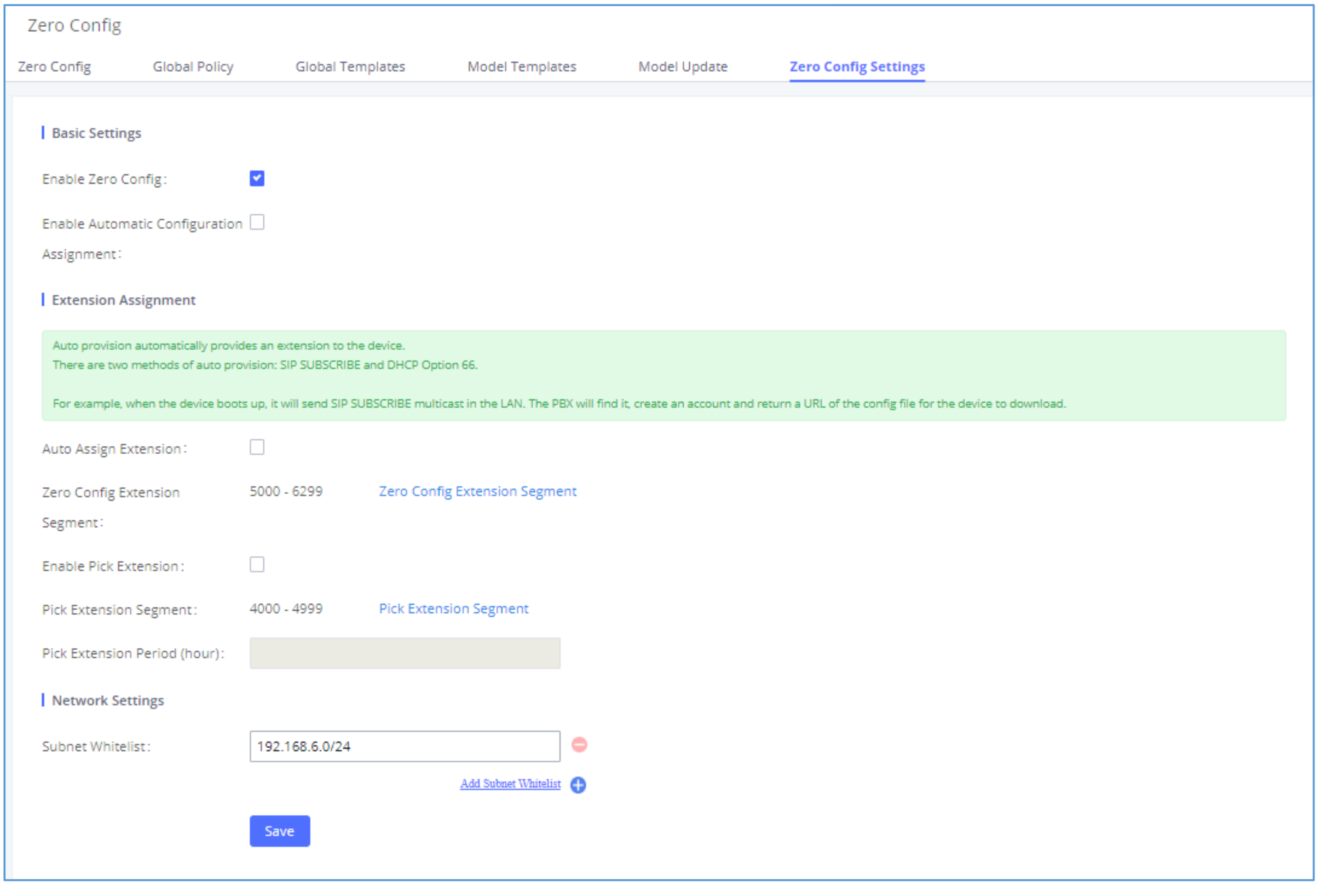


Figure 57: Auto Provision Settings

Table 25: Auto Provision Settings

Enable Zero Config	Enable or disable the zero-config feature on the PBX. The default setting is enabled.
Enable Automatic Configuration Assignment	By default, this is disabled. If disabled, when SIP device boots up, the UCM630X 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 UCM630X. **Note:** When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the UCM630X which will include the XML config file URL for the SIP device to download.
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 extension to be provisioned via 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.
Subnet Whitelist	This feature allows the UCM to provision devices in different subnets other than UCM network. Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is **<*IP*>/<CIDR>**. Examples: 10.0.0.1/8 192.168.6.0/24 **Note:** Only private IP ranges (10.0.0.0 | 172.16.0.0 | 192.168.0.0) are supported.

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

Grandstream endpoints are automatically discovered after bootup. Users could also manually discover device by specifying the IP address or scanning the entire LAN network. Three methods are supported to scan the devices.

- PING
- ARP

- SIP Message (NOTIFY)

Click on "Auto Discover" under Web GUI→**Value-added Features→Zero Config→Zero Config**, fill in the "Scan Method" and "Scan IP". The IP address segment will be automatically filled in based on the network mask detected on the UCM630X. If users need scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address. Then 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 UCM630X Web GUI→**Value-added Features→Zero Config→Auto Provisioning Settings**.

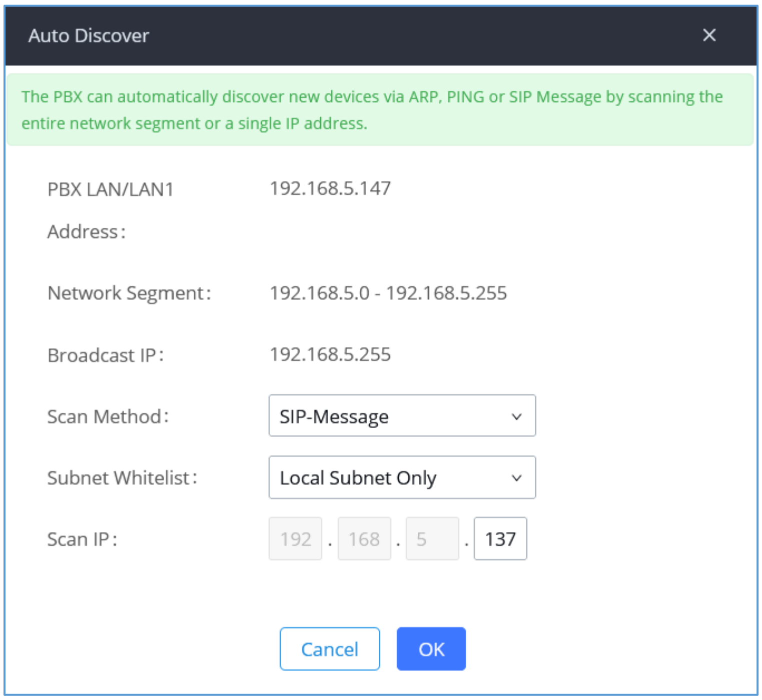
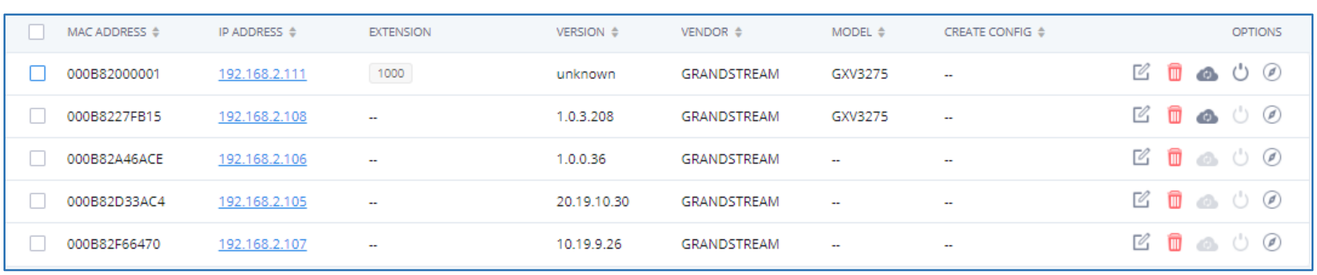


Figure 58: Auto Discover

The following figure shows a list of discovered phones. The MAC address, IP Address, Extension (if assigned), Version, Vendor, Model, Connection Status, Create Config, Options (Edit /Delete /Update /Reboot /Access Device WebGUI) are displayed in the list.



MAC ADDRESS	IP ADDRESS	EXTENSION	VERSION	VENDOR	MODEL	CREATE CONFIG	OPTIONS
000B82000001	192.168.2.111	1000	unknown	GRANDSTREAM	GXV3275	--	
000B8227FB15	192.168.2.108	--	1.0.3.208	GRANDSTREAM	GXV3275	--	
000B82A46ACE	192.168.2.106	--	1.0.0.36	GRANDSTREAM	--	--	
000B82D33AC4	192.168.2.105	--	20.19.10.30	GRANDSTREAM	--	--	
000B82F66470	192.168.2.107	--	10.19.9.26	GRANDSTREAM	--	--	

Figure 59: Discovered Devices

Uploading Devices List

Besides the built-in discovery method on the UCM, users could prepare a list of devices on .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://192.168.5.147:80		############	000B8249	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://192.168.5.147:80		############	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://192.168.5.147:80		############	000B826F	1.0.1.106	0	--	no	5080

Figure 60: Device List - CSV file Sample

Managing Discovered Devices

- **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 Filter: All to display corresponding results.
  - **All**: Display all discovered devices.
  - **Scan Results**: Display only manually discovered devices. [Discovery]
  - **IP Address**: Enter device IP and press **Search** button.
  - **MAC Address**: Enter device MAC and press **Search** button.
  - **Model:** Enter a model name and press Search button. Example: GXP2130.
  - **Extension:** Enter the extension number and press Search button.

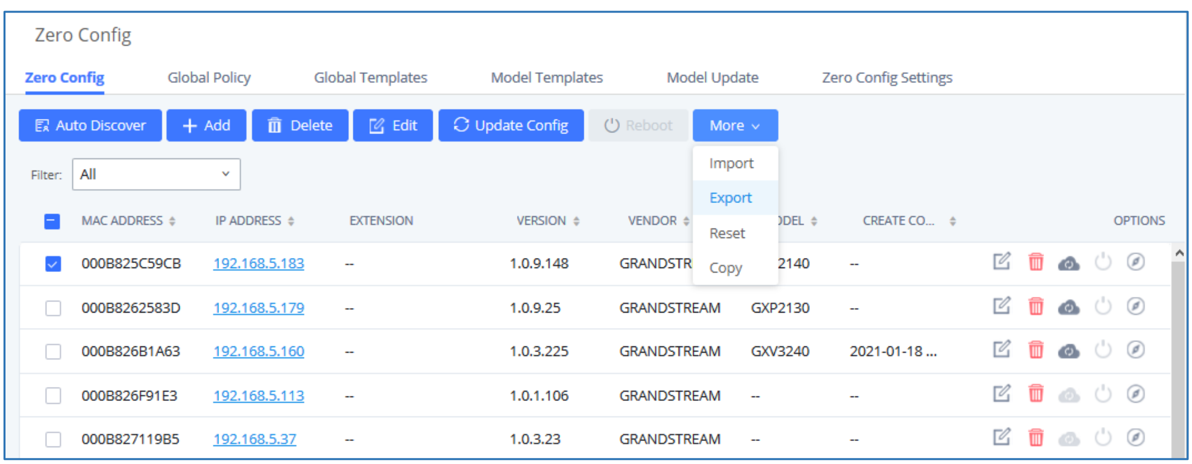


Figure 61: Managing Discovered Devices

From the main menu of zero config, users can perform the following operations:

- Click on **Auto Discover** in order to access to the discovery menu as shown on *[*Discovery*]* section.
- Click on **Add** to add a new device to zero config database using its MAC address.
- Click on **Delete** to delete selected devices from the zero-config database.
- Click on **Edit** to modify selected devices.
- Click on **Update Config** to batch update a list of devices, the UCM on this case will send SIP NOTIFY message to all selected devices in order to update them at once.
- Click on **Reboot** to reboot selected devices (the selected devices, should have been provisioned with extensions since the phone will authenticate the server which is trying to send it reboot command).
- Click on **Reset** to clear all devices configurations.
- Click on **Import** to upload CSV file containing list of devices.
- Click on **Export** to export CSV file containing list of devices. This file can be imported to another UCM to quickly set it up with the original UCM's devices.
- Click on **Copy** to copy configuration from one device to another. This can be useful for easily replace devices and note that this feature works only between devices of same model.

All these operations will be detailed on the next sections.

Global Configuration

Global Policy

Global configuration will apply to all the connected Grandstream SIP end point devices in the same LAN with the UCM630X no matter what the Grandstream device model it is. It is divided into two levels:

- **Global Policy**
- **Global Templates**

Note: Global Templates configuration has higher priority to **Global Policy** configuration.

Global Policy can be accessed in Web GUI→**Value-added Features**→**Zero Config**→**Global Policy** page. On the top of the configuration table, users can select category in the “Options” dropdown list to quickly navigate to the category. The categories are:

- **Localization**: configure display language, data, and time.
- **Phone Settings**: configure dial plan, call features, NAT, call progress tones and etc.
- **Contact List**: configure LDAP and XML phonebook download.
- **Maintenance**: configure upgrading, web access, Telnet/SSH access and syslog.
- **Network Settings**: configure 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.

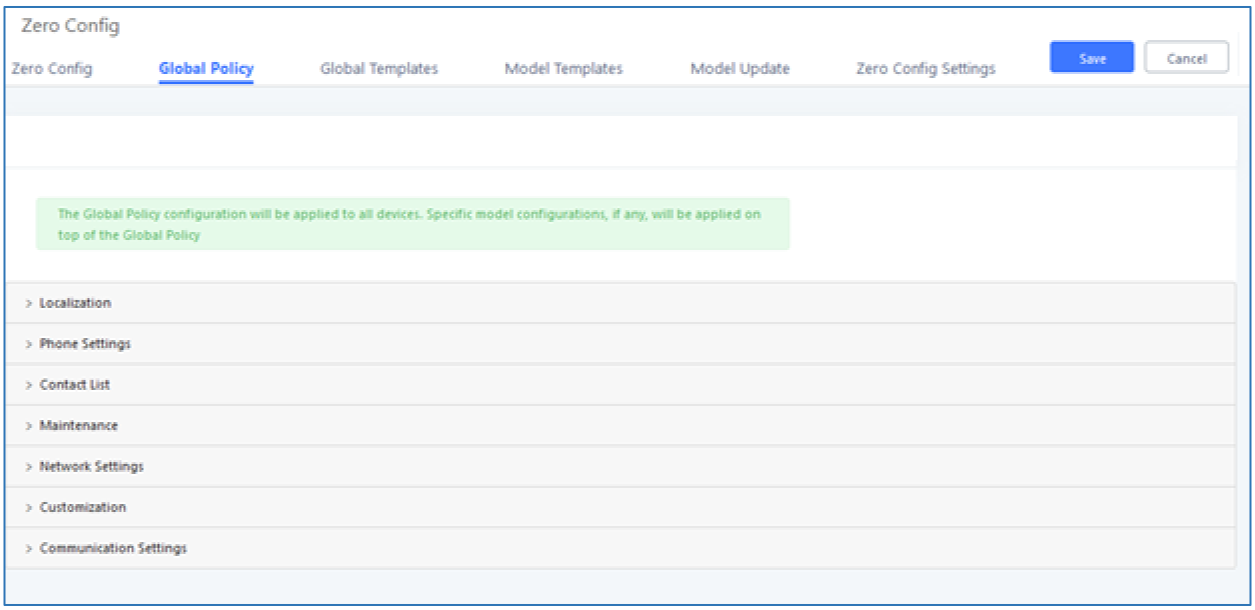


Figure 62: Global Policy Categories

The following tables list the Global Policy configuration parameters for the SIP end device.

Table 26: Global Policy Parameters – Localization

Language settings	
Language	Select the LCD display language on the SIP end 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 or 24-hour format on the SIP end device's LCD.
Enable NTP	To enable the NTP service.
NTP Server	Configure the URL or IP address of the NTP server. The SIP end 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 Saving Time	Select either to enable or disable the DST.

Table 27: Global Policy Parameters – Phone Settings

Default Call Settings	
Dial Plan	Configure the default dial plan rule. For syntax and examples, please refer to 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 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 user manual of the SIP devices to be provisioned for more details.

Table 28: Global Policy Parameters – Contact List

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 user manual for more details.
Name Filter	Configure the filter used for name lookups. Please refer to 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 which are returned in the LDAP search result. Example: gn cn sn description
Number Attribute	Specify the "number" attributes of each record which are returned in the LDAP search result. Example: telephoneNumber telephoneNumber Mobile
Display Name	Configure the entry information to be shown on 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. 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 client waits for server to return. Valid range is 0 to 180. Default value is 30.
Sort Results	Specify whether the searching result is sorted or not. 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 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 specify downloading protocol HTTP, HTTPS or TFTP and the server path to download the phonebook XML file. The server path could be 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 Minute). If set to 0, automatic download will be disabled. 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.

Table 29: Global Policy Parameters – Maintenance

Upgrade and Provision	
Firmware Source	Firmware source via ZeroConfig provisioning could a URL for external server address, local UCM directory or USB media if plugged in to the UCM630X. Select a source to get the firmware file:

	• **URL** If select 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 "Manage Storage" icon next to "Directory" option, upload firmware file and select 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 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 request 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.

Table 30: Global Policy Parameters – Network Settings

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 specify the Account ID, Password and Service Name for PPPoE.
Host Name	Specifies 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. Valid range is 0-63.
Layer 3 QoS For RTP	Assign the priority value of the Layer 3 QoS for RTP packets. Valid range is 0 -63.
Layer 3 QoS For SIP	Assign the priority value of the Layer 3 QoS for SIP packets. Valid range is 0 -63.
Layer 2 QoS Tag	Assign the VLAN Tag of the Layer 2 QoS packets. Valid range is 0 -4095.
Layer 2 QoS Priority Value	Assign the priority value of the Layer 2 QoS packets. 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 in order to keep the “ping hole” on the NAT router to open. 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.

Table 31: 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 source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as 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 source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as 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 source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as 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 source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as source, click to upload wallpaper file to the UCM630X.

Table 32: Global Policy Parameters – Communication Settings

Email Settings	
SMTP Settings	Check this option to configure the email settings that will be sent to the provisioned phones: • **Server** 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 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 Templates

Global Templates can be accessed in Web GUI→**Value-added Features**→**Zero Config**→**Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates. Later on, when the user configures the device in Edit Device dialog→Advanced Settings, the user 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 global template, users can select the categories and the parameters under each category to be used in the template. The global policy and the selected global template will both take effect when generating the config file. However, the selected global template has higher priority to the global policy when it comes to the same setting option/field. If the same option/field has different value configured in the global policy and the selected global template, the value for this option/field in the selected global template will override the value in global policy.

Click on "Add" to add a global template. Users will see the following configurations.

Table 33: Create New Template

Template Name	Create a name to identify this global template.
Description	Provide a description for the global template. This is optional.
Active	Check this option to enable the global template.

- Click on  to edit the global template.

The window for editing global template is shown in the following figure. In the “Options” field, after entering the option name key word, the options containing the key word will be listed. Users could then select the options to be modified under the global template.

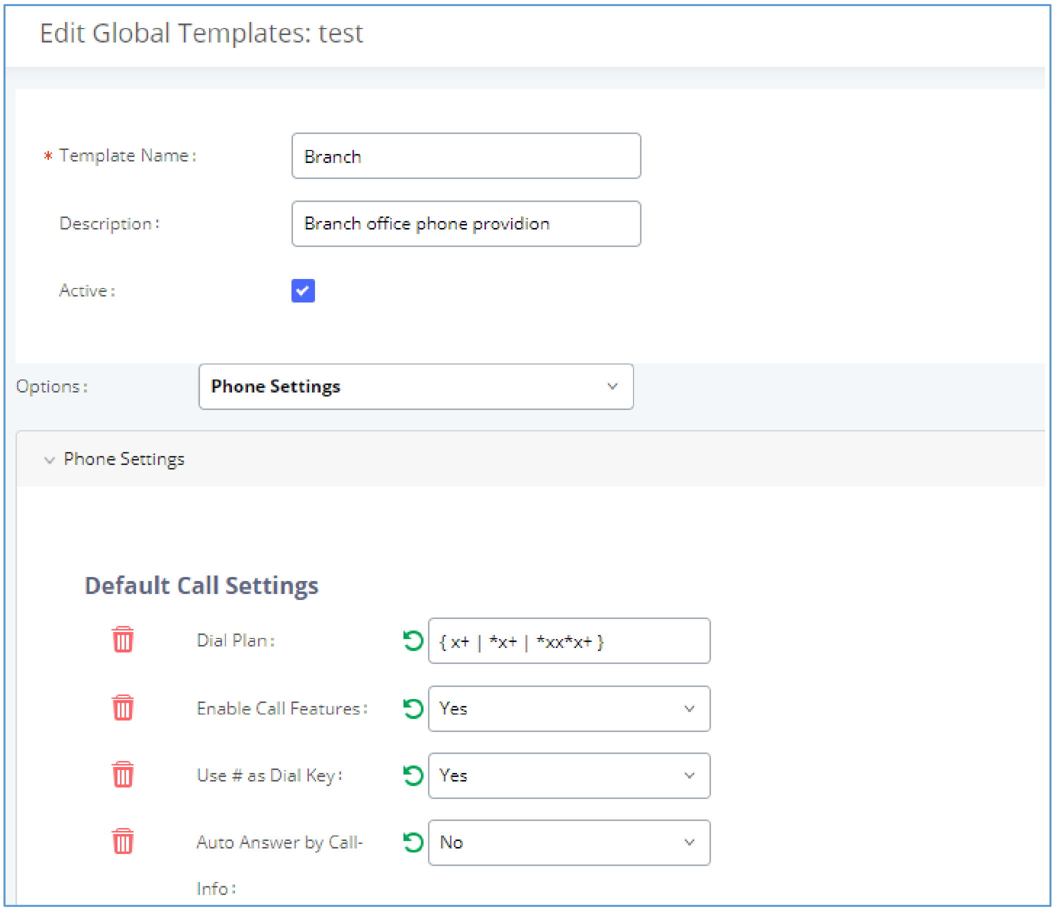


Figure 63: Edit Global Template

The added options will show in the list. Users can then enter or select value for each option to be used in the global template. On the left side of each added option, users can click on to delete this option from the template. On the right side of each option, users can click on to reset the option value to the default value.

Click on "Save" to save this global template.

- The created global templates will show in the Web GUI→Value-added Features→Zero Config→Global Templates page. Users can click on to delete the global template or delete multiple selected templates at once.
- Click on "Toggle Selected Template(s)" to toggle the status between enabled/disabled for the selected templates.

Model configuration

Model templates

Model layer configuration allows users to apply model-specific configurations to different devices. Users could create/edit/delete a model template by accessing Web GUI, page **Value-added Features→Zero Config→Model Templates**. If multiple model templates are created and enabled, when the user configures the device in Edit Device dialog→Advanced Settings, the user can select to use one of the model templates for the device. Please refer to section ***[Manage Devices]*** for more details on using the model template.

For each created model template, users can assign it as default model template. If assigned as default model template, the values in this model template will be applied to all the devices of this model. There is always only one default model template that can be assigned at one time on the UCM630X.

The selected model template and the default model template will both take effect when generating the config file for the device. However, the model template has higher priority to default model template when it comes to the same setting option/field. If the same option/field has different value configured in the default model template and the selected model template, the value for this option/field in the selected model template will override the value in default model template.

- Click on "Add" to add a model template.

Table 34: 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 default model template will be overridden if other selected model template has a different value for the same option.
Active	Check this option to enable the model template.

- Click on  to edit the model template.

  The editing window for model template is shown in the following figure. In the "Options" field, enter the option name key word, the option that contains the key word will be listed. User could then select the option to be modified under the model template.

Once added, the option will be shown in the list below. On the left side of each option, users can click on to remove this option from the model template. On the right side of each option, users can click on to reset the option to the default value.

User could also click on “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 configuration template here http://www.grandstream.com/support/tools.

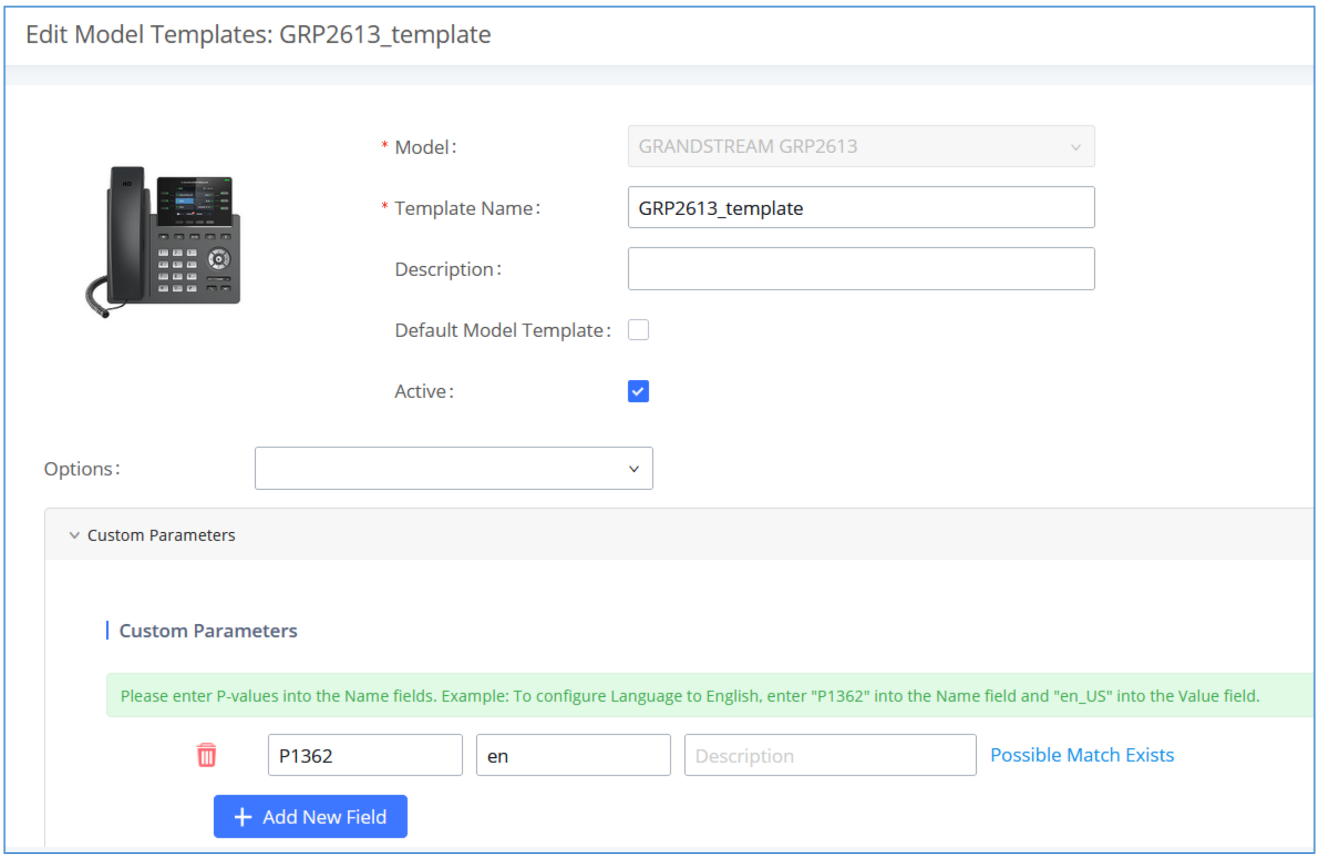


Figure 64: Edit Model Template

- Click on Save when done. The model template will be displayed on Web GUI→**Value-added Features→Zero Config→Model Templates** page.
- Click on to delete the model template or click on “Delete Selected Templates” to delete multiple selected templates at once.
- Click on “Toggle Selected Template(s)” to toggle the status between enabled/disabled for the selected model templates.

Model Update

UCM630X zero config feature supports provisioning all models of Grandstream SIP end devices including OEM device models.

OEM Models

Users can associate OEM device models with their original Grandstream-branded models, allowing these OEM devices to be provisioned appropriately.

- Click on Add OEM Models button.
- In the *Source Model* field, select the Grandstream device that the OEM model is based on from the dropdown list.
- For the *Destination Model* and *Destination Vendor* field, enter the custom OEM model name and vendor name.
- The newly added OEM model should now be selectable as an option in *Model* fields.

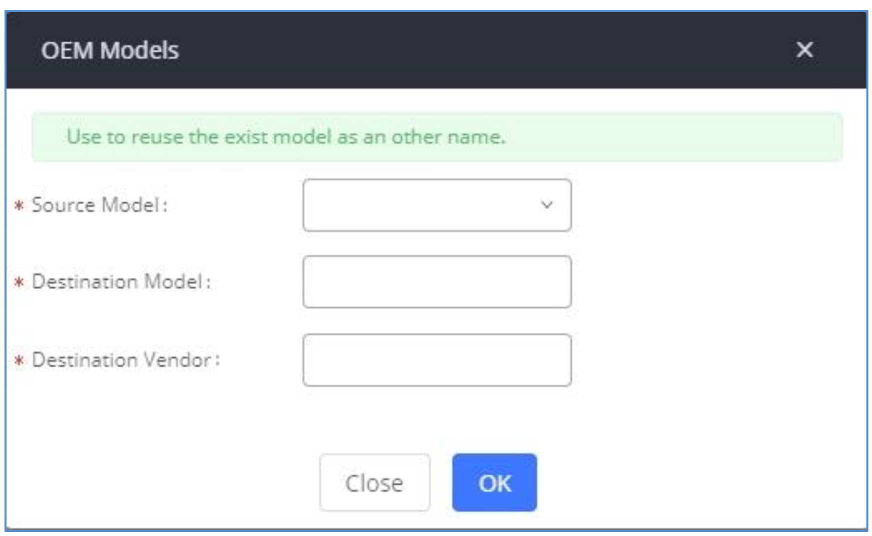


Figure 65: OEM Models

Model Template Package List

Templates for most of the Grandstream models are built in with the UCM630X already. Templates for GS Wave and Grandstream surveillance products require users to download and install under Web GUI→**Value-added Features**→**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.

- Click on to download the template.
- Click on to upgrade the model template. Users will see this icon available if the device model has template updated in the UCM630X.

Model Template Package List

VENDOR	MODEL	VERSION (REMOTE / LOCAL)	SIZE	OPTIONS
Grandstream	DP750	1.0/-	271K	
Grandstream	DP752	1.2/-	58K	
Grandstream	GAC2500	1.0/-	25K	
Grandstream	GDS3705	1.3/-	56K	
Grandstream	GDS3710	1.3/-	97K	
Grandstream	GRP2612	1.0/-	495K	
Grandstream	GRP2612P	1.0/-	495K	
Grandstream	GRP2612W	1.0/-	495K	
Grandstream	GRP2613	1.0/-	67K	
Grandstream	GRP2614	1.3/-	52K	

< 1 2 3 4 > Total: 37 10 / page

Figure 66: Template Management

Upload Model Template Package

In case the UCM630X is placed in the private network and Internet access is restricted, users will not be able to get packages by downloading and installing from the remote server. Model template package can be manually uploaded from local device through Web GUI. Please contact Grandstream customer support if the model package is needed for manual uploading.

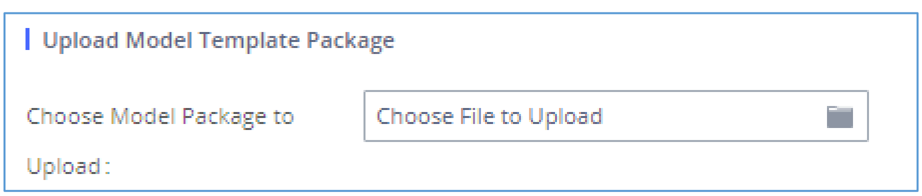


Figure 67: Upload Model Template Manually

Device Configuration

On Web GUI, page **Value-added Features→Zero Config→Zero Config**, users could create new device, delete existing device(s), make special configuration for a single device, or send NOTIFY to existing device(s).

Create New Device

Besides configuring the device after the device is discovered, users could also 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.

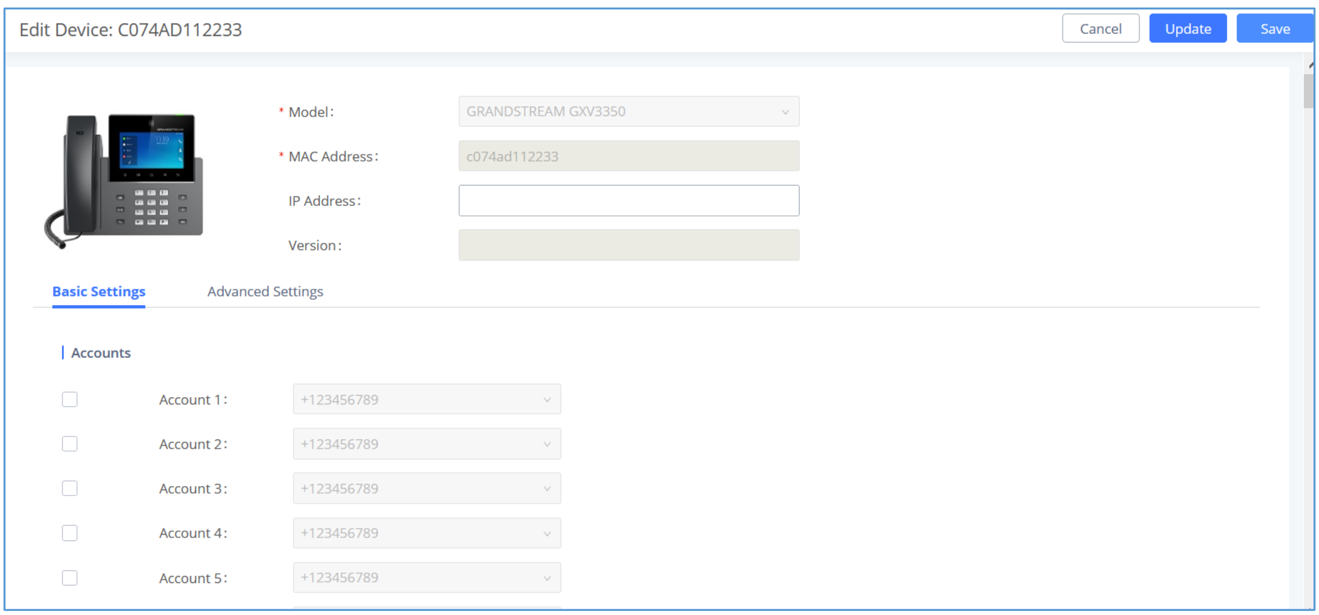
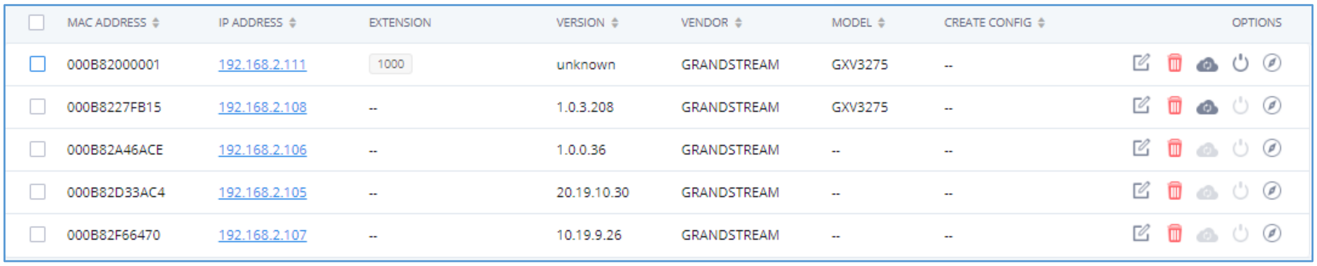


Figure 68: Create New Device

Manage Devices

The device manually created or discovered from Auto Discover will be listed in the Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page. Users can see the devices with their MAC address, IP address, vendor, model etc.



MAC ADDRESS	IP ADDRESS	EXTENSION	VERSION	VENDOR	MODEL	CREATE CONFIG	OPTIONS
000B82000001	192.168.2.111	1000	unknown	GRANDSTREAM	GXV3275	--	
000B8227FB15	192.168.2.108	--	1.0.3.208	GRANDSTREAM	GXV3275	--	
000B82A46ACE	192.168.2.106	--	1.0.0.36	GRANDSTREAM	--	--	
000B82D33AC4	192.168.2.105	--	20.19.10.30	GRANDSTREAM	--	--	
000B82F66470	192.168.2.107	--	10.19.9.26	GRANDSTREAM	--	--	

Figure 69: Manage Devices

- Click on to access the Web GUI of the phone.
- Click on 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.

Figure 70: Edit Device

A preview of the "Advanced" settings is shown in the above figure. There are five levels configurations as described in (1) (2) (3) (4) (5) below, with priority from the lowest to the highest. The configurations in all levels will take effect for the device. If there are same options existing in different level configurations with different value configured, the higher-level configuration will override the lower-level configuration.

(1) Global Policy

This is the lowest level configuration. The global policy configured in Web GUI→**Value-added Features→Zero Config→Global Policy** will be applied here. Clicking on "Modify Global Policy" to redirect to page **Value-added Features→Zero Config→Global Policy**.

(2) Global Templates

Select a global template to be used for the device and click on > to add. Multiple global templates can be selected, and users can arrange the priority by adjusting orders via ^ and v. All the selected global templates will take effect. If the same option exists on multiple selected global templates, the value in the template with higher priority will override the one in the template with lower priority. Click on < to remove the 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 model template under Web GUI→**Value-added Features→Zero Config→Model Templates** page. Please see default model template option in ***[Table 34: Create New Model Template].***

(4) Model Templates

Select a model template to be used for the device and click on > to add. Multiple model templates can be selected, and users can arrange the priority by adjusting orders via ^ and v. All the selected model templates will take effect. If the same option exists on multiple selected model templates, the value in the template with higher priority will override the one in the template with lower priority. Click on < to remove the 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 following dialog will show.

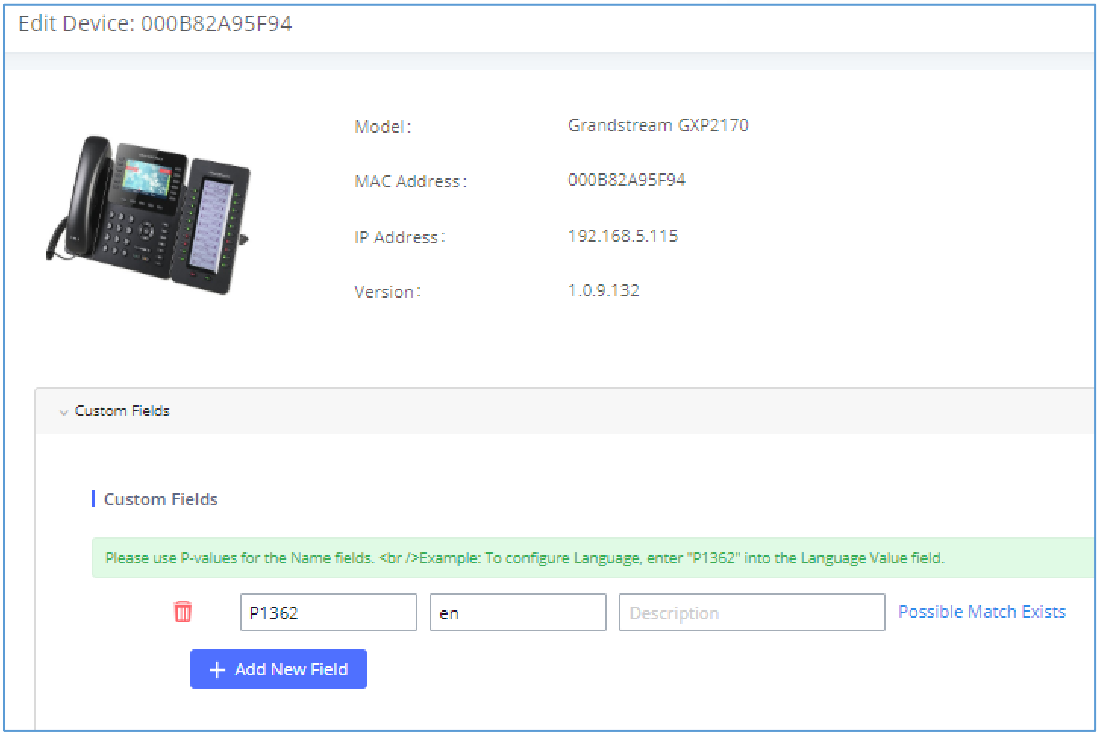


Figure 71: Edit Customize Device Settings

Scroll down in the dialog to view and edit the device-specific options. If the users would like to add more options which are not in the pre-defined list, click on "Add New Field" to add a P value number and the value to the configuration. The above figure shows setting P value "P1362" to "en", which means the display language on the LCD is set to English. The warning information on right tells that the option matching the P value number exists and clicking on it will lead to the matching option. For P value information of different models, please refer to configuration template here http://www.grandstream.com/sites/default/files/Resources/config-template.zip.

- 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.

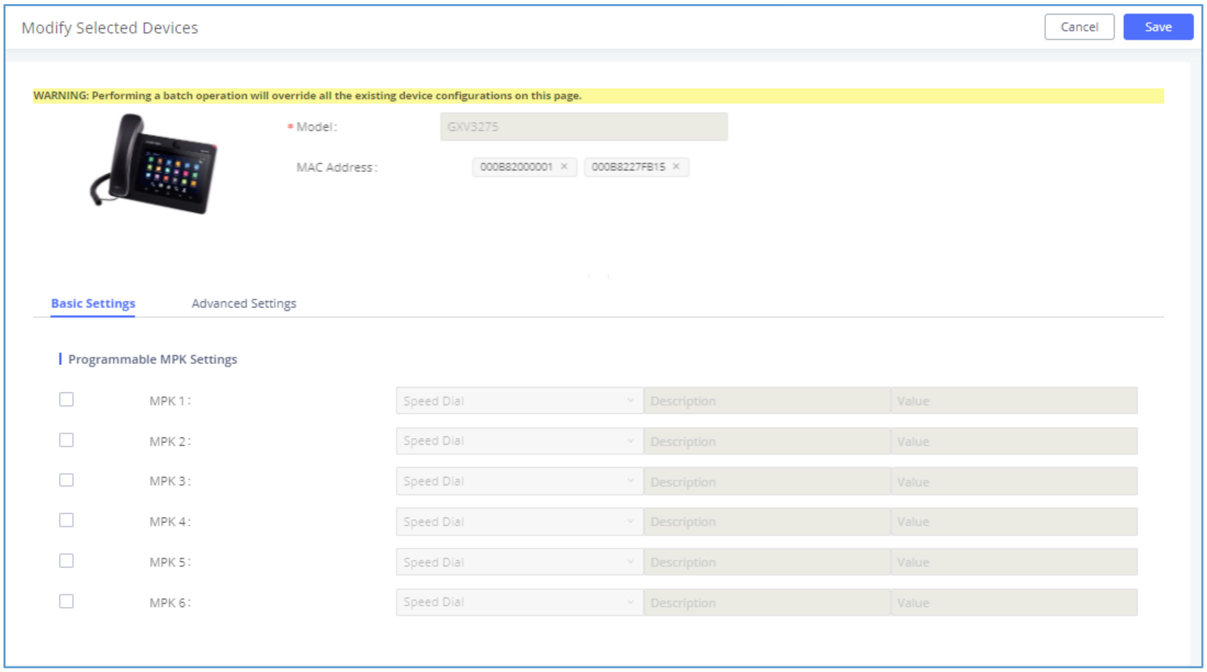


Figure 72: Modify Selected Devices - Same Model

If selected devices are of different models, the configuration dialog is like the following figure. Click on  to view more devices of other models. Users are only allowed to make modifications in Global Templates and Global Policy level.

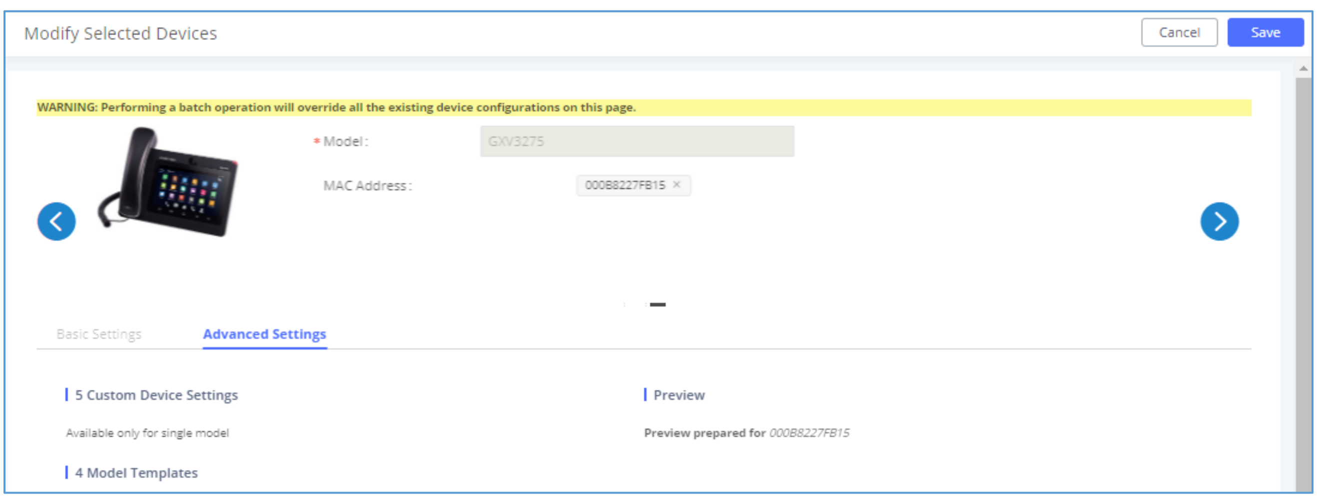


Figure 73: Modify Selected Devices - Different Models

⚠ **Note:**

Performing batch operation will override all the existing device configuration on the page.

After the above configurations, save the changes and go back to Web GUI→**Value-added Features→Zero Config→Zero Config** page. Users could then click on 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.

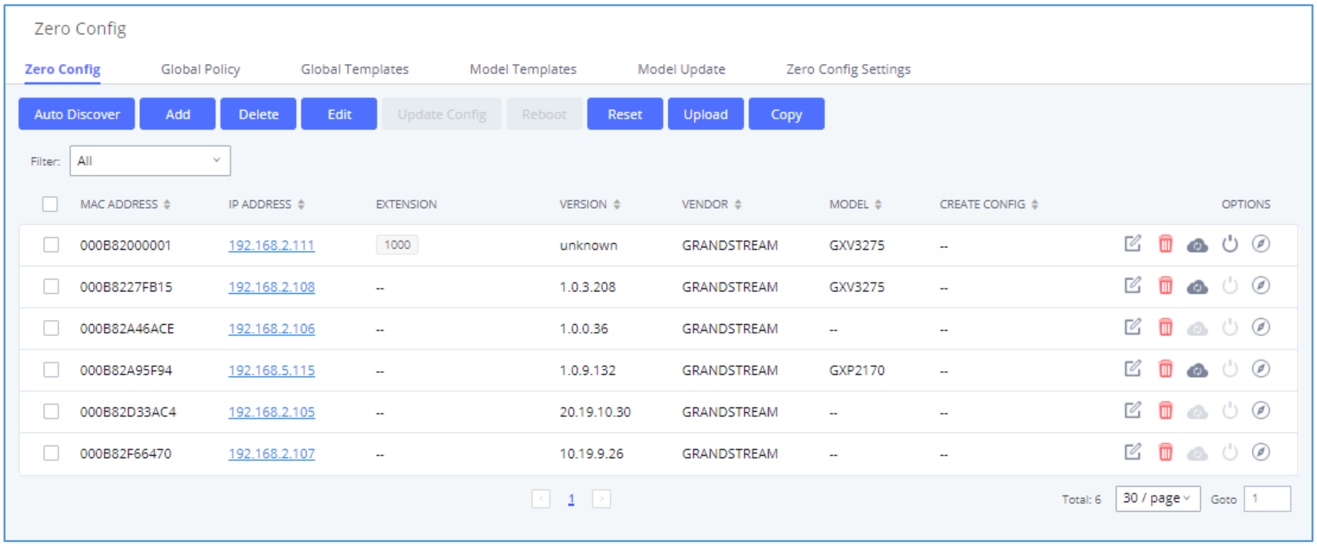


Figure 74: Device List in Zero Config

In 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 provisioning the office phones for the customer support team.

1. Go to Web GUI→**Value-added Features→Zero Config→Zero Config Settings**, select “Enable Zero Config”.

2. Go to Web GUI→**Value-added Features→Zero Config→Global Policy**, configure Date Format, Time Format and Firmware Source as follows.

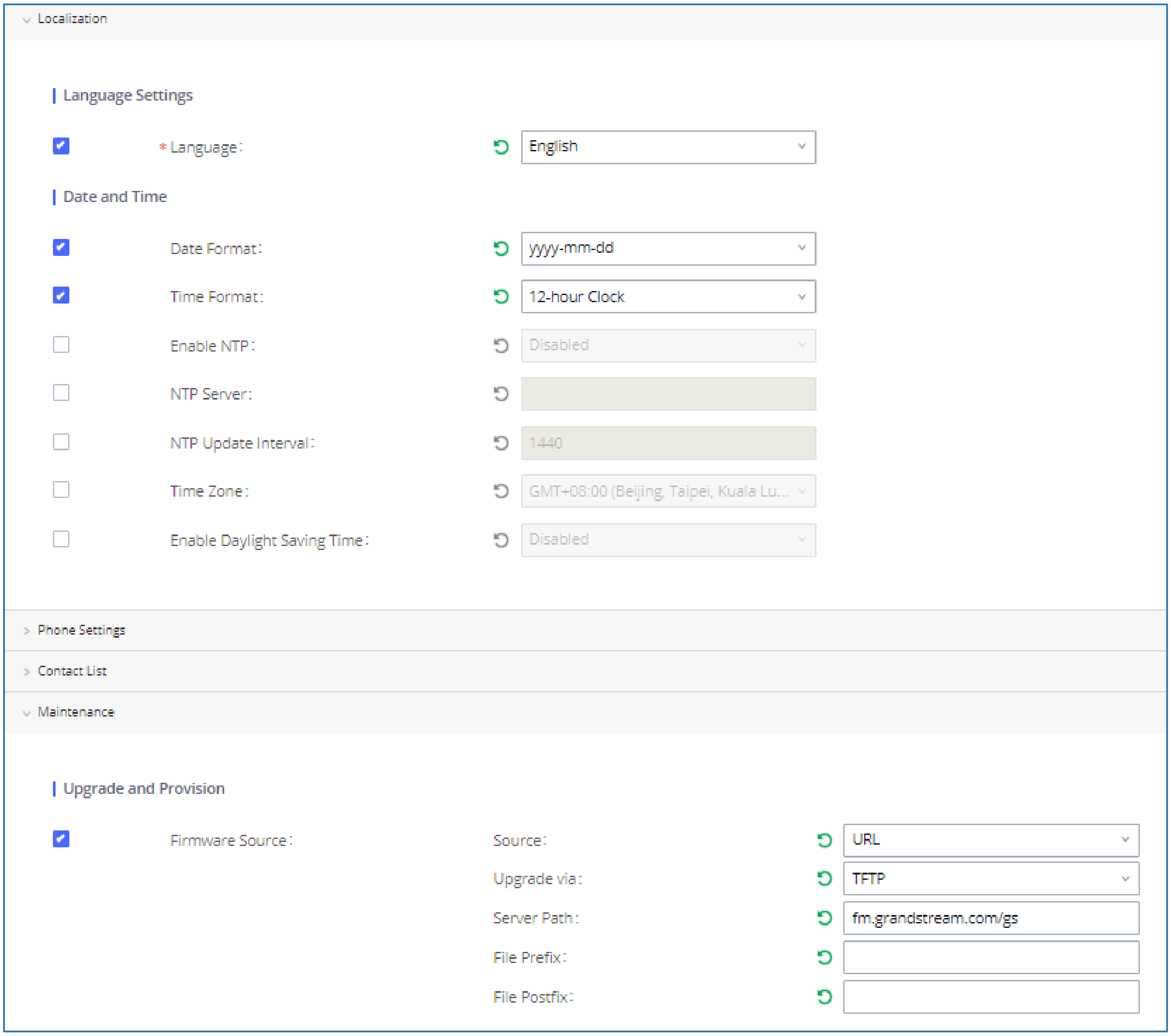


Figure 75: Zero Config Sample - Global Policy

3. Go to Web GUI→**Value-added Features→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 Web GUI→**Value-added Features→Zero Config→Model Templates**, create another model template "Spanish Support Template" for GXP2170. Add option "Language" and set it to "Español".

5. After 9 devices are powered up and connected to the LAN network, use "Auto Discover" function or "Create New Device" function to add the devices to the device list on Web GUI→**Value-added Features→Zero Config→Zero Config**.

6. On Web GUI→**Value-added Features→Zero Config→Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on 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 "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.

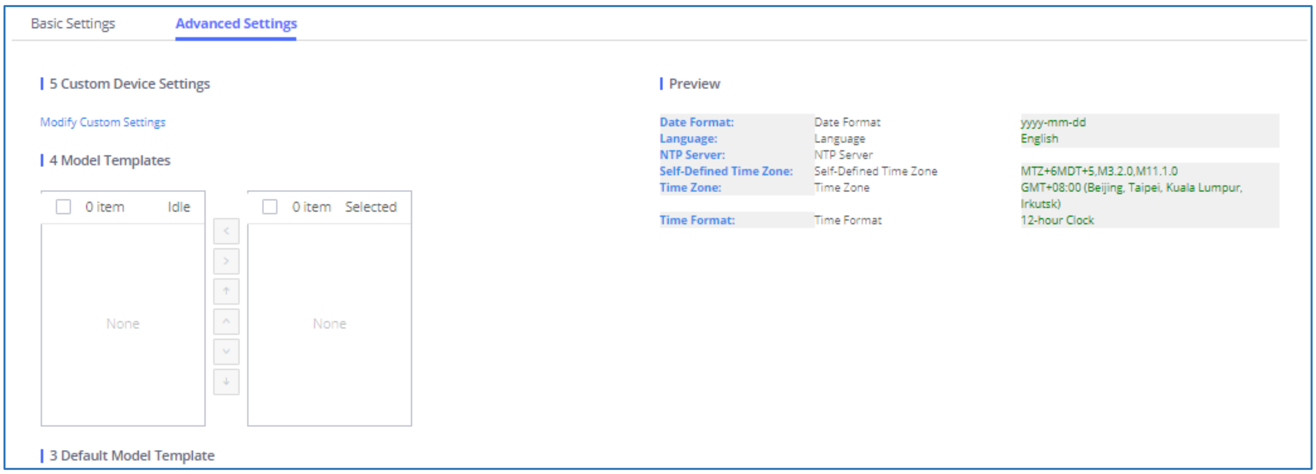


Figure 76: Zero Config Sample - Device Preview 1

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 "Advanced settings" tab to bring up the following dialog.

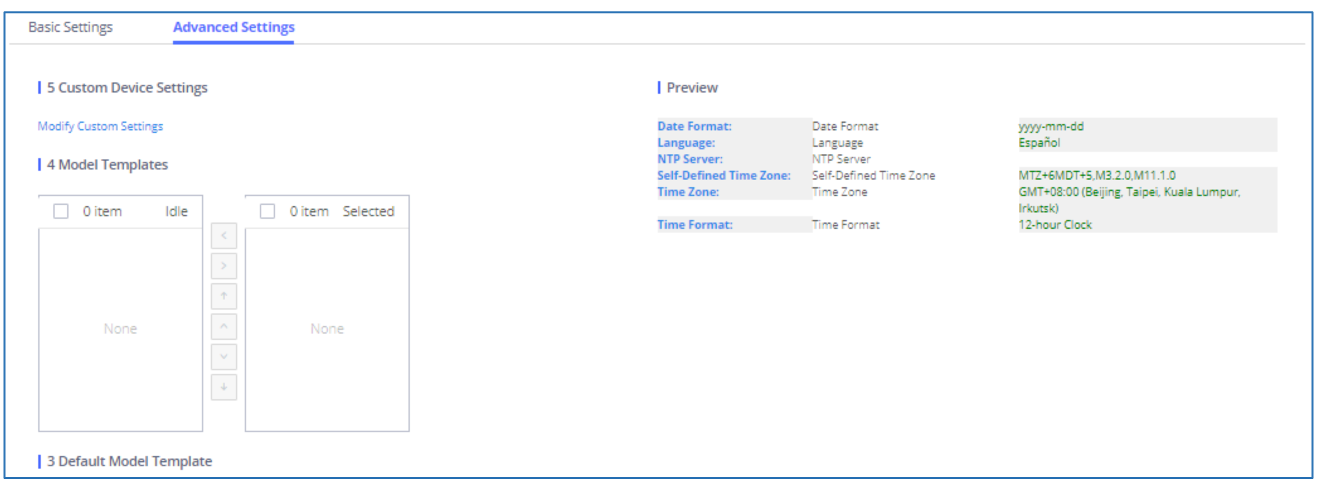


Figure 77: Zero Config Sample - Device Preview 2

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 “Español” since Model Template has the higher priority for the option “Language”, which overrides the value configured in default model template.

9. 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.

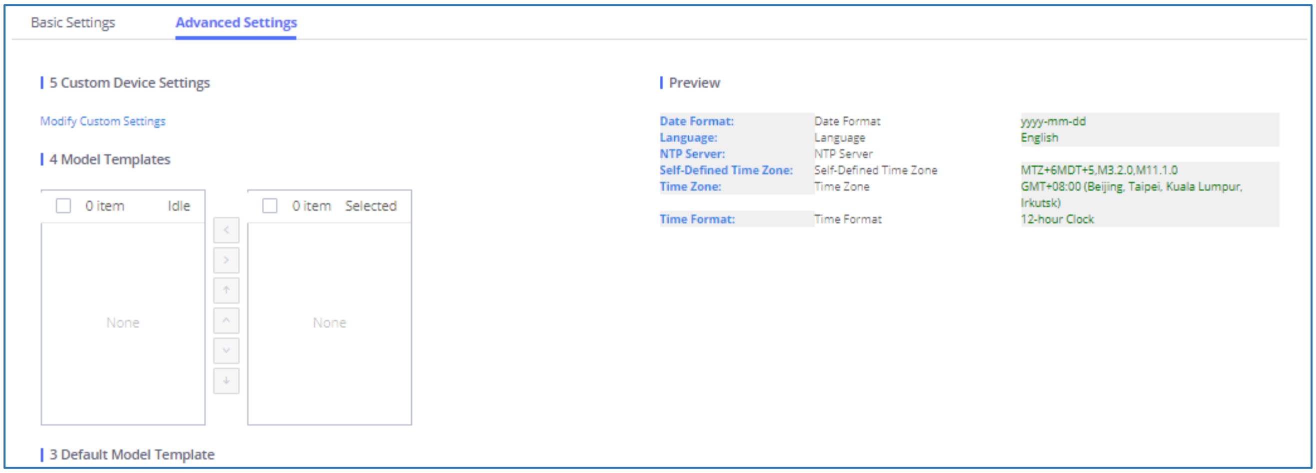


Figure 78: Zero Config Sample - Device Preview 3

10. Click on “Apply Changes” to apply saved changes.

11. On the Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page, click on to send NOTIFY to trigger the device to download 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 LCD display since it is not specified in the global policy.

EXTENSIONS

Create New User

Create New SIP Extension

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

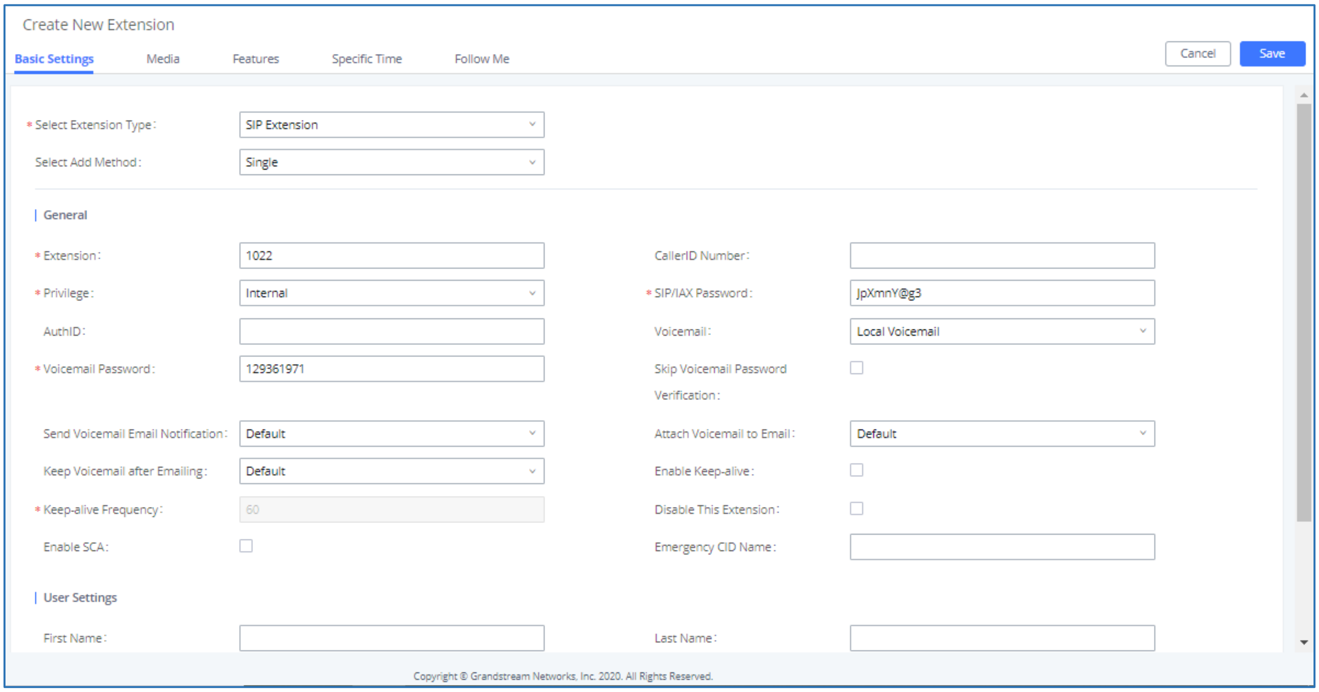


Figure 79: Create New Device

Extension options are divided into four categories:

- Basic Settings
- Media
- Features
- Specific Time
- Follow me

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

Table 35: SIP Extension Configuration Parameters→Basic Settings

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 purpose.
Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
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. • **Enable Remote Voicemail**: Forward the notify message from remote voicemail system for the user, and the local voicemail will be disabled. **Note:** Remote voicemail feature is used only for Infomatec (Brazil).
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 random generated password for security purpose.
Skip Voicemail Password Verification	When 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 or not to send emails to the extension's email address to notify of new voicemail.
Attach Voicemail to Email	Configures whether or not to attach voicemail audio file to the voicemail notification emails. **Note**: When set to "Default", the global settings in **Call Features → Voicemail → Voicemail Email Settings** will be used.

Keep Voicemail after Emailing	Whether to keep the local voicemail recording after sending them. If set to "Default", the global settings will be used. **Note**: When set to "Default", the global settings in **Call Features → Voicemail → Voicemail Email Settings** will be used.
Enable Keep-alive	If enabled, empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is "No".
Keep-alive Frequency	Configure the Keep-alive interval (in seconds) to check if the host is up. The default setting is 60 seconds.
Enable SCA	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 Call Features->SCA page.
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 numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
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 current available voice prompt languages on the UCM630X. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under Web GUI→**PBX Settings**→**Voice Prompt**→**Language Settings**.
Concurrent Registrations	The maximum endpoints which can be registered into this extension. For security concerns, the default value is 1.
Mobile Phone Number	Configure the phone number for the extension, user can type the related star code for phone number followed by the extension number to directly call this number. Example: user can type ***88**1000 to call the mobile number associated with extension 1000.

Table 36: SIP Extension Configuration Parameters→Media

SIP Settings	
NAT	Use NAT when the UCM630X is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it is related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.
Enable Direct Media	By default, the UCM630X will route the media steams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the UCM630X to negotiate endpoint-to-endpoint media routing. The default setting is "No".
DTMF Mode	Select DTMF mode for the user 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.
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. “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.
Alert-Info	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
SRTP	Enable SRTP for the call. The default setting is disabled.
Jitter Buffer	Select 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.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission. • **NACK** • **NACK+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.
FECC	Configure to enable Remote Camera Management.

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. Press "Add Local Network Address" to add more IP segments.
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.265, H.263, H.263p, RTX and VP8.

Table 37: SIP Extension Configuration Parameters→Features

Call Transfer	
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].
Call Forward Unconditional	Enable and configure the Call Forward Unconditional target number. Available options for target number are: • "**None**": Call forward deactivated. • "**Extension**": Select an extension from dropdown list as CFU target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFU target. • "**Queues**": Select a queue from dropdown list as CFU target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFU target. 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 "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 under Specific Time section. Scroll down the add Time Condition for 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 dropdown list as CFN target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFN target. • "**Queues**": Select a queue from dropdown list as CFN target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFN target. The default setting is "None".
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 under Specific Time section. Scroll down the add Time Condition for 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 dropdown list as CFB target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFB target. • "**Queues**": Select a queue from dropdown list as CFB target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFB target. The default setting is "None".

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 under Specific Time section. Scroll down the add Time Condition for 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.
DND 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 Specific Time section. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
DND Whitelist	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.
FWD Whitelist	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. By default, it is disabled.
CC Mode	Two modes for Call Completion are supported: • **Normal**: This extension is used as ordinary extension. • **For Trunk**: This extension is registered from a PBX. The default setting is "Normal".
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 can make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which 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.
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 caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which 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 on the basis of 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	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.

Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform 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 UCM630X. 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 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 password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Support Hot-Desking Mode	Check to enable Hot-Desking Mode on the extension. Hot-Desking allows to use the same endpoint device and login using extension/password combination. This feature is used in scenarios where different users need to use the same endpoint device during different time of a 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 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 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.
Enable WebRTC Support	Enable registration and call from WebRTC. For more details about WebRTC feature refer to [***Wave WebRTC Video Calling & Conferencing***]
Bind PMS Room	If enabled, the system will create a room whose room number, by default, will equal the extension number in PMS module. Note: If this room already exists, the configuration of the existing room will be overwritten.
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
The Maximum Number of Call Lines	The maximum number of simultaneous calls that the extension can have. 0 indicates no limit.
Enable Auto-Answer Support	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
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.
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.

Table 38: SIP Extension Configuration Parameters→Specific Time

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

Table 39: Table 34: SIP Extension Configuration Parameters→Follow Me

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.
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.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
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 IAX Extension

The UCM630X supports Inter-Asterisk eXchange (IAX) protocol. IAX is used for transporting VoIP telephony sessions between servers and terminal devices. IAX is like SIP but also has its own characteristic. For more information, please refer to RFC 5465.

To manually create 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.

Table 40: IAX Extension Configuration Parameters→Basic Settings

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 purpose.
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 random generated password for security purpose.
Skip Voicemail Password Verification	When 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 or not to send emails to the extension’s email address to notify of new voicemail.
Attach Voicemail to Email	Configures whether or not to attach 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 numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
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 current available voice prompt languages on the UCM630X. To add more languages in the list, please download 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.

Table 41: IAX Extension Configuration Parameters→Media

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.265, H.263, H.263p, RTX and VP8.

Table 42: IAX Extension Configuration Parameters→Features

Call Transfer	
Call Forward Unconditional	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 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 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 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.
DND Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Whitelist	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.
FWD Whitelist	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 caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of 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	
Allow call-barging	Members of the list can spy on this extension via feature codes.

Seamless transfer privilege control	
Allowed to seamless transfer	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 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 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 password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via 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 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	Send a log of missed calls to the extension's email address.

Calls	
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.

Table 43: IAX Extension Configuration Parameters→Specific Time

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

Table 44: IAX Extension Configuration Parameters→Follow Me

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.
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.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
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 user needs to connect analog phone lines or FAX machines to the UCM630X.

To manually create 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.

Table 45: FXS Extension Configuration Parameters→Basic Settings

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 random generated password for security purpose.
Skip Voicemail Password Verification	When 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 or not to send emails to the extension’s email address to notify of new voicemail.
Attach Voicemail to Email	Configures whether or not to attach voicemail audio file to the voicemail notification emails.
Keep Voicemail	Only applies if extension-level or global Send Voicemail to Email is enabled.

after Emailing	
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 numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
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 current available voice prompt languages on the UCM630X. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under Web GUI→**PBX Settings→Voice Prompt→Language Settings**.

Table 46: FXS Extension Configuration Parameters→Media

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 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 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 3-way calling feature on the user. The default setting is enabled.
Send CallerID After	Configure the number of rings before sending CID. Default setting is 1.
Fax Mode	For 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 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** .

Table 47: FXS Extension Configuration Parameters→Features

Call Transfer	
Call Forward Unconditional	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 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 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 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.
DND Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Whitelist	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..

FWD Whitelist	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 caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of 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, 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 call-barging	Members of the list can spy on this extension via feature codes.

Seamless transfer privilege control	
Allowed to seamless transfer	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 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 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 password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, this extension will be added to 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 ringback tone instead of the regular ringback tone.
Music On Hold	Select which Music On Hold class to suggest to 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.

Table 48: FXS Extension Configuration Parameters→Specific Time

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

Table 49: FXS Extension Configuration Parameters→Follow Me

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.
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.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
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 Add SIP Extensions

To add multiple SIP extensions, BATCH add can be used to create standardized SIP extension accounts. However, unique extension username cannot be set using BATCH add.
Under Web GUI→**Extension/Trunk**→**Extensions**, click on "Add" and select extension type as SIP extension, and "Select Add Method" as Batch.

Table 50: Batch Add SIP Extension Parameters

General	
Create Number	Specify the number of extensions to be added. The default setting is 5.
Extension Incrementation	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,...... **Note:** Up to 3 characters.
Extension	Configure the starting extension number of the batch of extensions to be added.
Permission	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 from 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. • **Enable Remote Voicemail**: Forward the notify message from remote voicemail system for the user, and the local voicemail will be disabled. **Note:** Remote voicemail feature is used only for Infomatec (Brazil).
SIP/IAX Password	Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions. • User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password. • Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. • User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password.

	Enter a password to be used on all the extensions in the batch.
Send Voicemail to Email	Send voicemail messages to the configured email address. If set to "Default", the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
CallerID Number	Configure CallerID Number when adding Batch Extensions. • Use Extension as Number Users can choose to use the extension number as CallerID • Use as Number Users can choose to set a specific number instead of using the extension number.
Skip Voicemail Password Verification	When 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.
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.
Disable This Extension	Check this box to disable this extension.
Enable SCA	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 Call Features->SCA page.
Emergency Calls CID	CallerID number that will be used when calling out and receiving direct callbacks.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.
Media	
NAT	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it is related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.
Enable Direct Media	By default, the PBX will route the media steams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing. The default setting is "No".

DTMF Mode	Select DTMF mode for the user 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.
Alert-info	When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS.
SRTP	Enable/disable SRTP for RTP stream encryption.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission. • **NACK** • **NACK+RTX(SSRC-GROUP)** • **OFF**
Video FEC	Check to enable Forward Error Correction (FEC) for Video.
FECC	Configure to enable FECC
Audio FEC	Check to enable Forward Error Correction (FEC) for Audio.
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. Press "Add Local Network Address" to add more IP segments.
Jitter Buffer	Select 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.
Codec Preference	Configure the codecs to be used.
Call Transfer	
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].

Call Forward Unconditional	Enable and configure the Call Forward Unconditional target number. Available options for target number are: • "**None**": Call forward deactivated. • "**Extension**": Select an extension from dropdown list as CFU target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFU target. • "**Queues**": Select a queue from dropdown list as CFU target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFU target. 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 "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 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 dropdown list as CFN target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFN target. • "**Queues**": Select a queue from dropdown list as CFN target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFN target. The default setting is "None".
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 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 dropdown list as CFB target. • "**Custom Number**": Enter a customer number as target. For example: *97. • "**Voicemail**": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • "**Ring Group**": Select a ring group from dropdown list as CFB target. • "**Queues**": Select a queue from dropdown list as CFB target. • "**Voicemail Group**": Select a voicemail group from dropdown list as CFB target. The default setting is "None".
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 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.
DND 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 on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
DND Whitelist	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.
FWD Whitelist	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. By default, it is disabled.
CC Mode	Two modes for Call Completion are supported: • **Normal**: This extension is used as ordinary extension. • **For Trunk**: This extension is registered from a PBX. The default setting is "Normal".
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 can make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which 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.
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 caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which 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 on the basis of 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	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform seamless transfer to the edited extension.
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 3 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 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	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can

Skip Trunk Auth	skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX list.
Enable WebRTC Support	Enable registration and call from WebRTC.
Bind PMS Room	If enabled, the system will create a room whose room number, by default, will equal the extension number in PMS module. Note: If this room already exists, the configuration of the existing room will be overwritten.
Music On Hold	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
Call Duration Limit	The maximum duration of call-blocking.
Maximum Call Duration	The maximum call duration (in seconds). The default value 0 means no limit.
Call Waiting	If disabled, UCM will not invite the extension when it is already in a call and will do the same work as the user is busy. **Note:** the option only works when the caller dials the extension directly.

Batch Add IAX Extensions

Under Web GUI→**Extension/Trunk**→**Extensions**, click on "Add", then select extension type as IAX Extension and the add method to be Batch.

T

able 51: Batch Add IAX Extension Parameters

General	
Create Number	Specify the number of extensions to be added. The default setting is 5.
Extension Incrementation	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,......
Extension	The extension number associated with this particular user/phone.
Permission	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 in order to make outbound calls from this rule.
CallerID Number	Configure the Caller ID number displayed when dialing calls from this user. Note: The Caller ID usage might be limited by your VoIP provider. In Batch Add Method,

	"e" means to use the extension as the number.
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.
SIP/IAX Password	Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions. • User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password. • Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. • User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password. • Enter a password to be used on all the extensions in the batch.
Send Voicemail to Email	Send voicemail messages to the configured email address. If set to "Default", the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
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 Voicemail Password Verification	When 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.
Disable This Extension	Check this box to disable this extension.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.
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/disable SRTP for RTP stream encryption.
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	Configure the codecs to be used.

Call Transfer	
Call Forward Unconditional	Enable and configure the Call Forward Unconditional target number.
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 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.
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 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.
CFB Time	Select time condition for Call Forward Busy. The available time conditions are “Office

Condition	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 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.
DND 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 on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
DND Whitelist	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.
FWD Whitelist	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 caller ID number.

External Number	Set the external number to be rang simultaneously. '-' is the connection character which 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 on the basis of 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	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform seamless transfer to the edited extension.
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 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 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 password when making outbound calls.

Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX list.
Music On Hold	Specify which Music On Hold class to suggest to the bridged channel when putting them 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

Batch Extension Resetting Functionality

Users can select multiple extensions and reset their settings to default by pressing the reset button and confirm the reset functionality. Once done, all settings in Basic Settings page will be restored to default values with the exception of 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 with the exception of 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. User can search an extension by specifying the extension number to find an extension quickly.

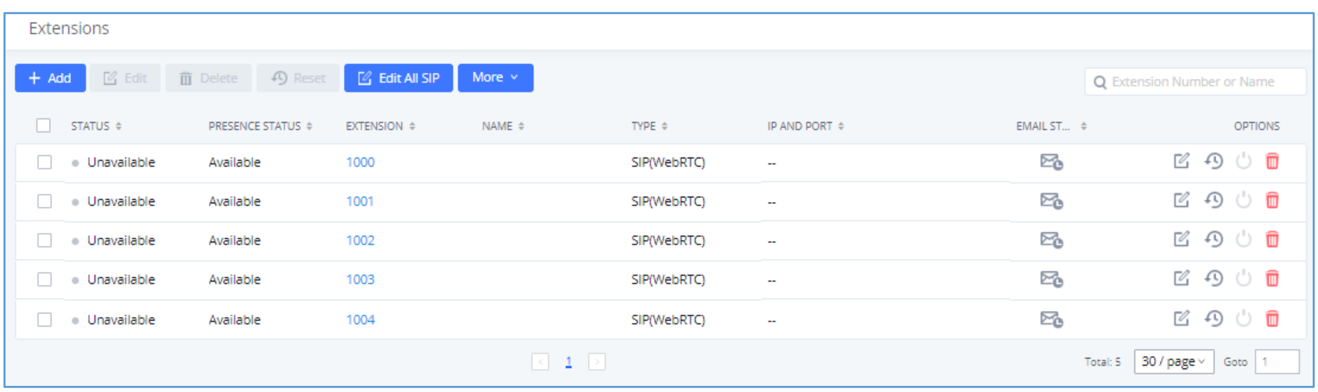


Figure 80: Manage Extensions

- **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 username and permissions and delete the user voicemail prompt and voice messages.

- **Reboot the user**

  Click on to send NOTIFY reboot event to the device which has an UCM630X extension already registered. To successfully reboot the user, "Zero Config" needs to be enabled on the UCM630X Web GUI→**Value-added Features→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".

- **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 csv format file with selected technology "SIP", "IAX" or "FXS". Click on "Export Extensions" button and select technology in the prompt below.

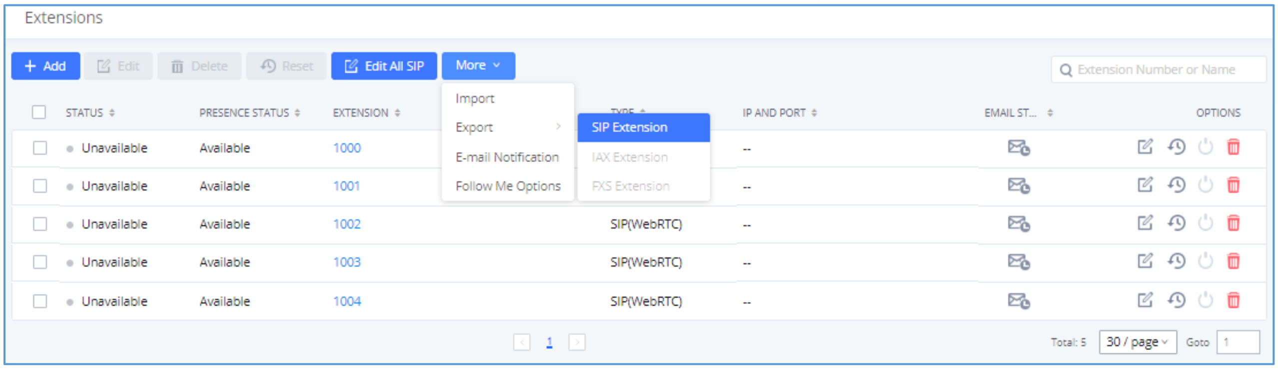


Figure 81: Export Extensions

The exported csv 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 flexibility to batch add extensions with similar or different configuration quickly into the PBX system.

1. Export extension csv file from the UCM630X by clicking on "Export Extensions" button.
2. Fill up the extension information you would like in the exported csv template.
3. Click on "Import Extensions" button. The following dialog will be prompted.

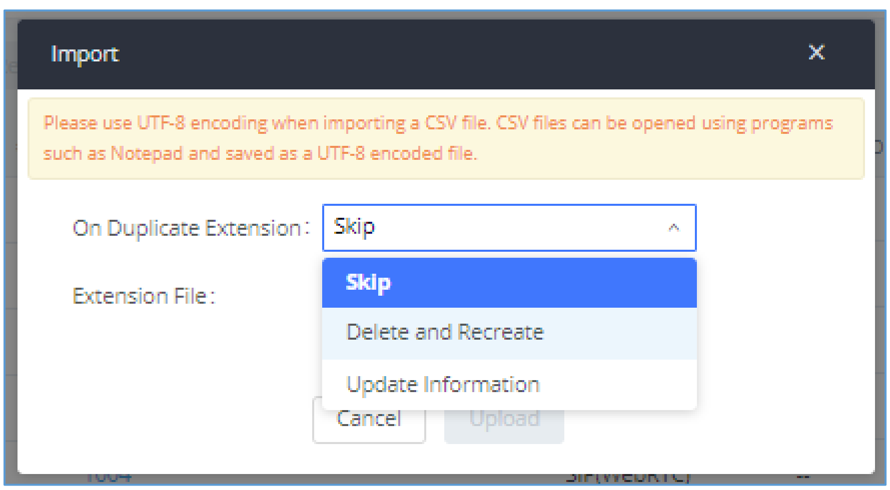


Figure 82: Import Extensions

4. Select the option in "On Duplicate Extension" to define how the duplicate extension(s) in the imported csv file should be treated by the PBX.
   - **Skip:** Duplicate extensions in the csv 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 csv 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 csv file has 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 csv file from local directory in the PC.
6. Click on "Apply Changes" to apply the imported file on the UCM630X.

Example of file to import:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Extension	Technology	Enable Voicemail	CallerID	SIP/IAX Password	Voicema	Skip Voicemail Password Verification	Ring Timeout	Auto Record	SRTP	Fax Mode	Strategy	Local Subnet 1	Local Sub
1000	SIP	yes	1000	admin123	61783	no		no	no	None	Allow All		
1001	SIP	yes	1001	admin123	955921	no		no	no	None	Allow All		
1002	SIP	yes	1002	admin123	269824	no		no	no	None	Allow All		
1003	SIP	yes	1003	admin123	363196	no		no	no	None	Allow All		
1004	SIP	yes	1004	admin123	12860	no		no	no	None	Allow All		

Figure 83: Import File

Table 52: SIP extensions Imported File Example

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, H.265,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 WebRTC	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

Table 53: IAX 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, H.265,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

Table 54: FXS 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 **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 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

The CSV 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.

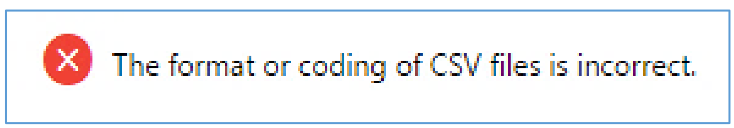


Figure 84: Import Error

Extension Details

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

- **Extension**: Shows the Extension number.
- **Status**: Shows the status of the extension.
- **Presence status**: Indicates the Presence Status of this extension.
- **Terminal Type**: 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.

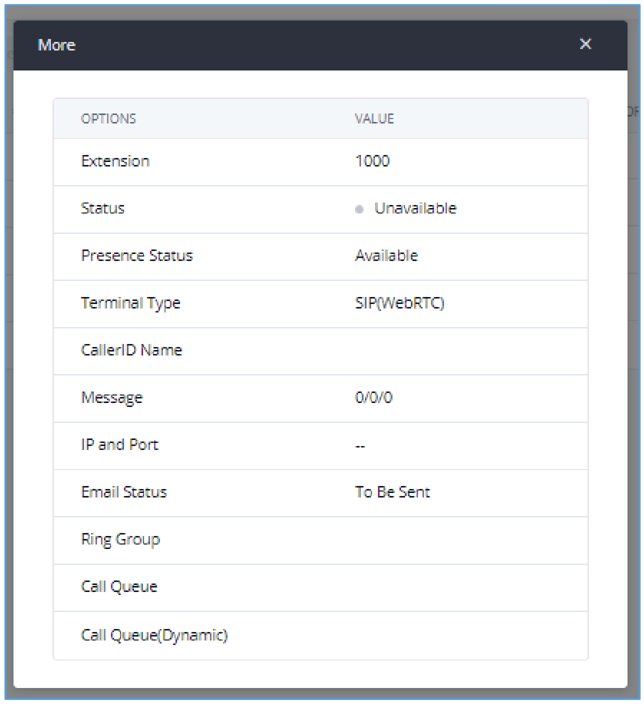


Figure 85: Extension Details

E-mail Notification

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

When click on ”More” > “E-mail Notification” button, the following message will be prompted in the web page. Click on OK to confirm sending the account information to all users’ Email addresses.

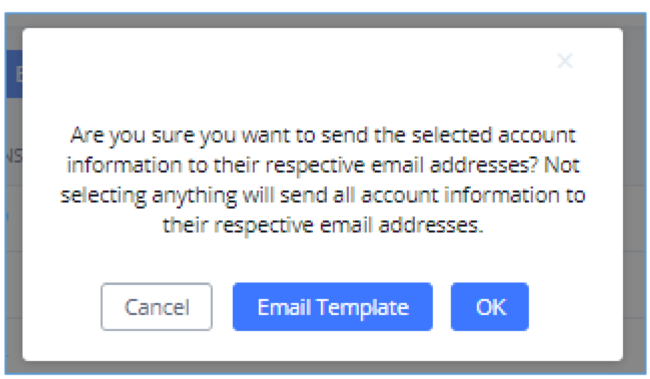


Figure 86: E-mail Notification - Prompt Information

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

General Settings

Server Address	192.168.5.147:5060
Account Name	Mia
SIP User ID	1000
Authenticate ID	1000
Authenticate Password	pas1

Figure 87: Account Registration Information

GSWave Settings

Login URL	https://192.168.5.147:8090/#/
Login URL for Public	https://c074ad0a8c94-10671.b.gdms.cloud/#/
Login Name	1000
Login Password	pas1

Use Web App to scan qr code and log in

Figure 88: GSWave Settings and QR Code

Multiple Registrations per Extension

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

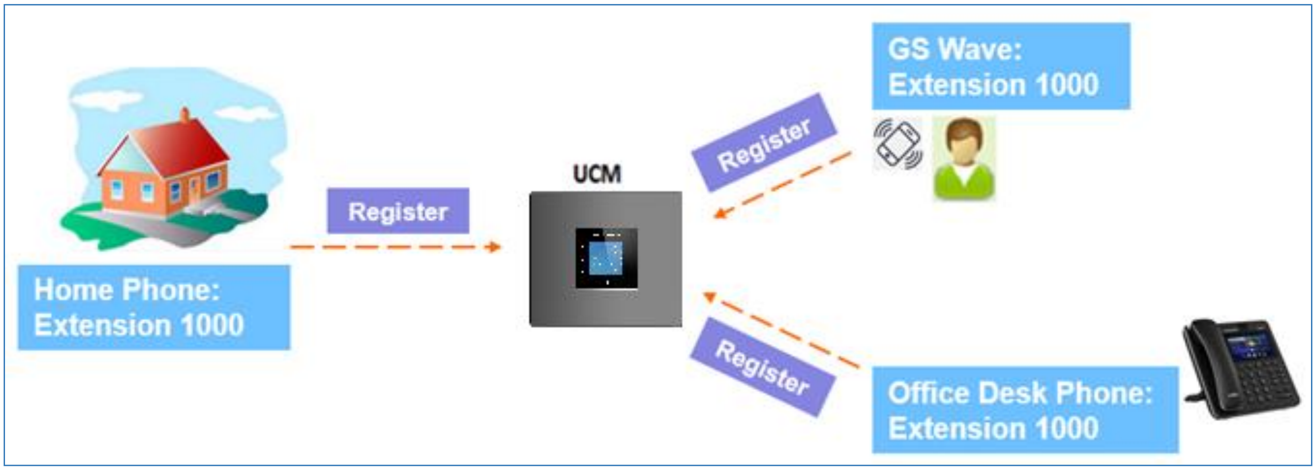


Figure 89: Multiple Registrations per Extension

This feature can be enabled by configuring option “Concurrent Registrations” under Web GUI→**Extension/Trunk→Edit Extension**. The default value is set to 1 for security purpose. Maximum is 10.

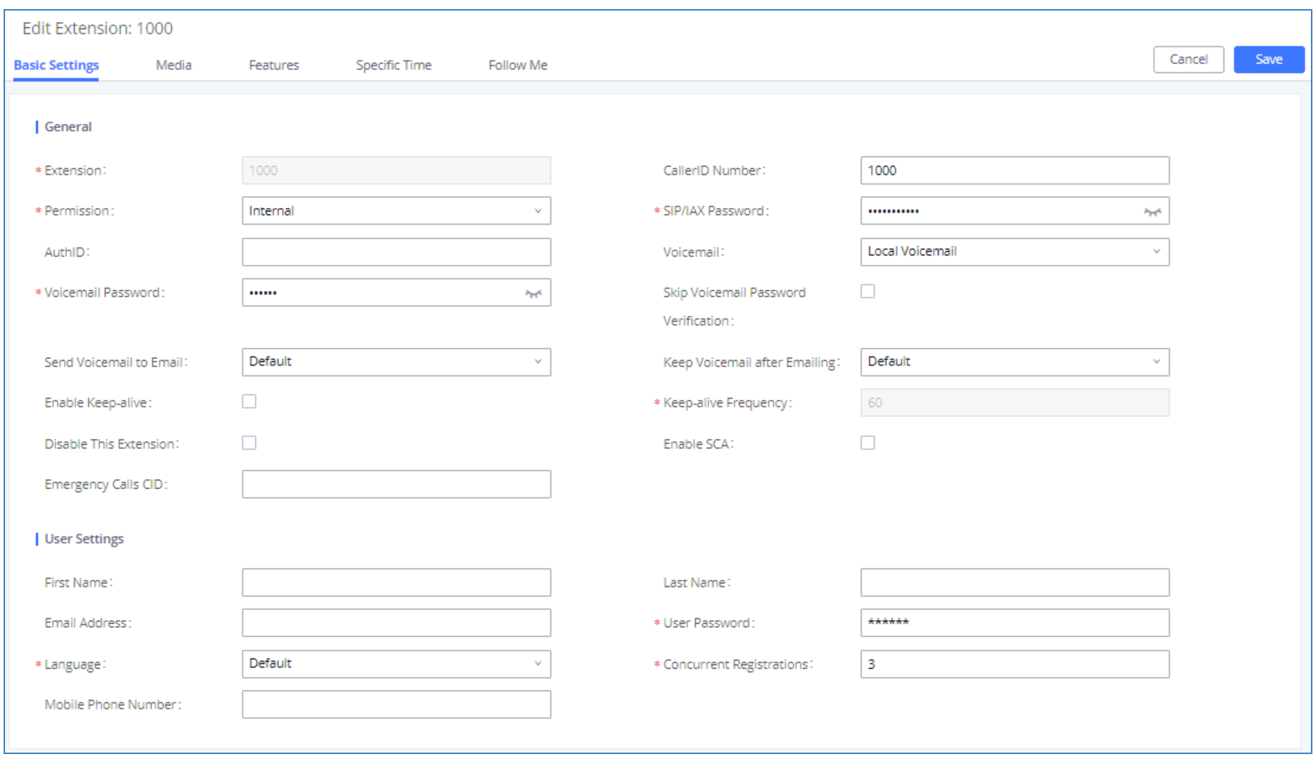


Figure 90: Extension - Concurrent Registration

SMS Message Support

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

Figure 91: SMS Message Support

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 business environment.

Configure Extension Groups

Extension group can be configured via Web GUI→**Extension/Trunk**→**Extension Groups**.

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

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

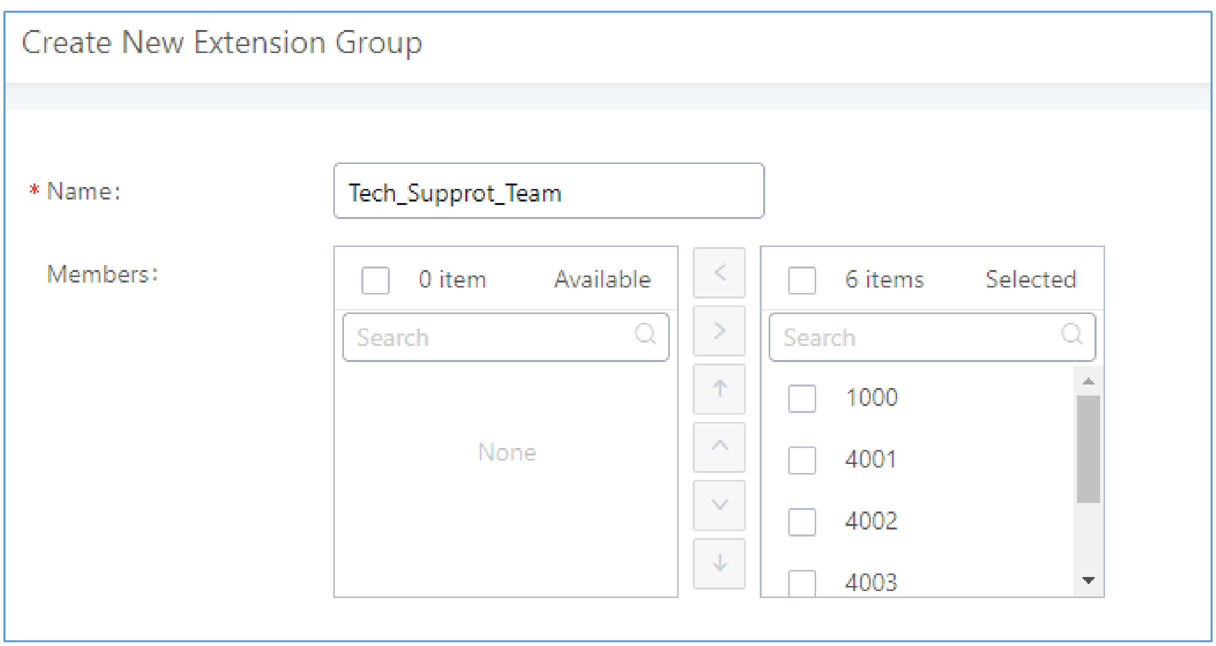


Figure 92: Edit Extension Group

Click on in order 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.

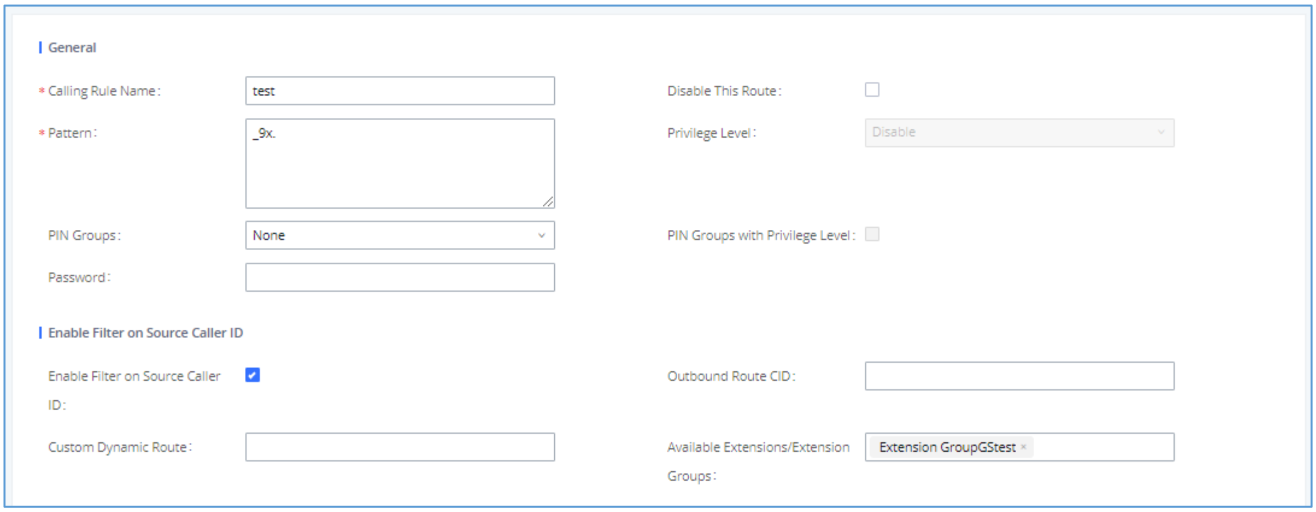


Figure 93: Select Extension Group in Outbound Route

ANALOG TRUNKS

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

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

Analog Trunk Configuration

The analog trunk options are listed in the table below.

Table 55: Analog Trunk Configuration Parameters

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 and etc.
Advanced Options	
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.
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	When 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 Onhook 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	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 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 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**.
Disable This Trunk	If selected, the trunk will be disabled and incoming/Outgoing calls via this trunk will not be possible.
DAHDI Out Line Selection	This is to implement 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→2→1→2→1→2→..., 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.
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.

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.
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 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 detecting, please make sure there are more than one channel configured and working properly. If the detection has busy tone, the "Tone Country" option will be set as "Custom".

PSTN Detection

The UCM630X provides 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 "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.

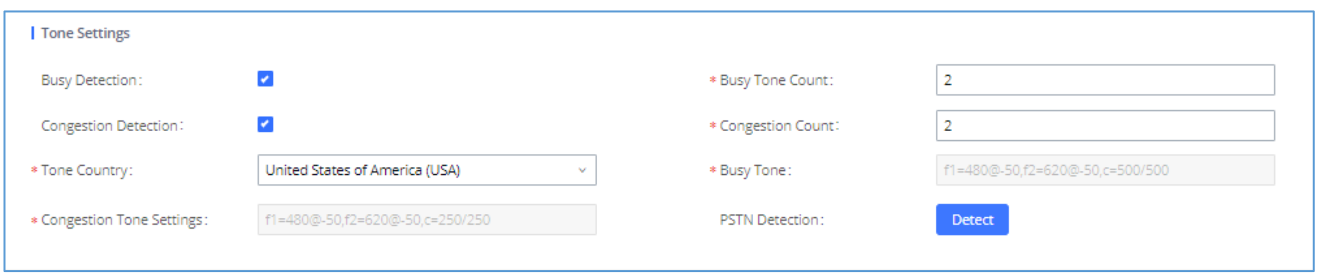


Figure 94: UCM630X FXO Tone Settings

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

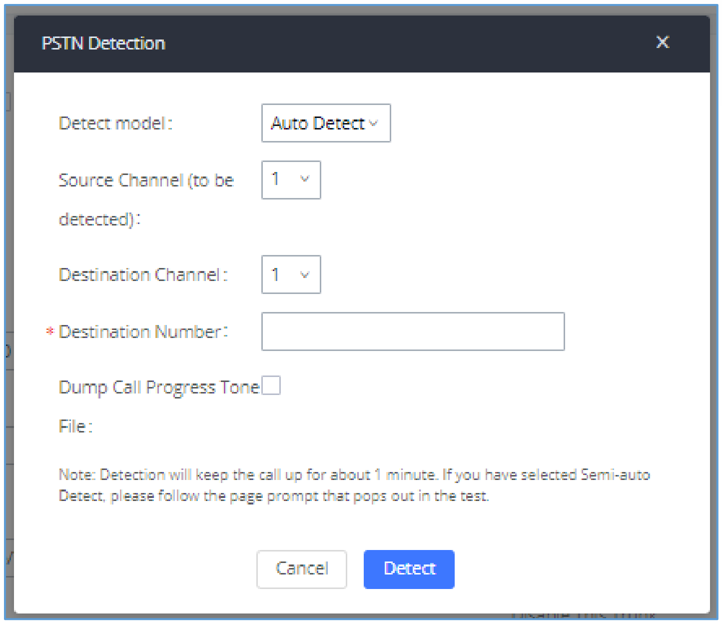


Figure 95: UCM630X PSTN Detection

- 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 detecting. 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.

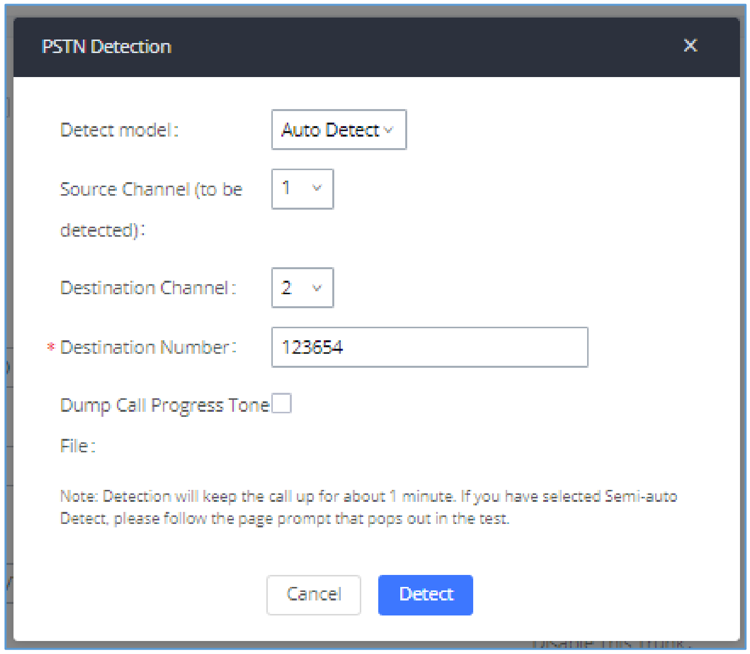


Figure 96: UCM630X PSTN Detection: Auto Detect

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

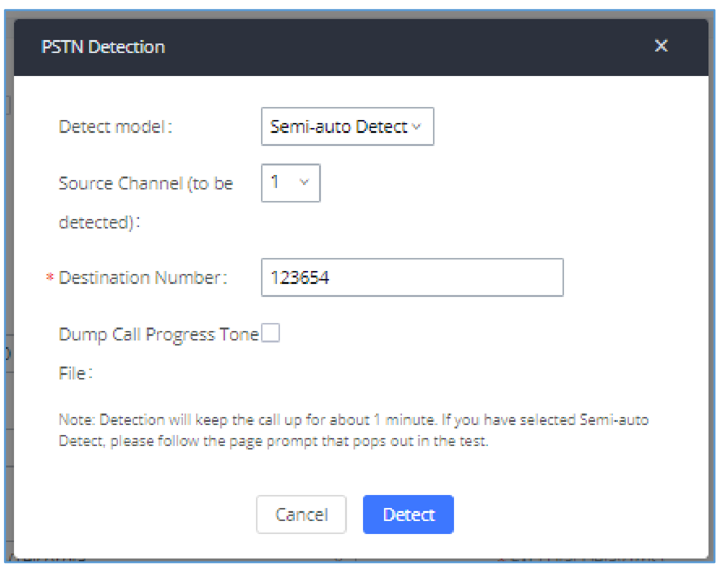


Figure 97: UCM630X PSTN Detection: Semi-Auto Detect

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 other 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 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.

Table 56: PSTN Detection for Analog Trunk

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 caller (Source Channel) and another channel will be used as 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, source channel will be used as caller and send the call to the configured Destination Number. Users will then need follow the prompts in Web GUI to help finish the detection. The default setting is "Auto Detect".
Source Channel	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.

⚠ **Note:**

- 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 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

VoIP Trunk Configuration

VoIP trunks can be configured in UCM630X under Web GUI→**Extension/Trunk**→**VoIP Trunks**. Once created, the VoIP trunks will be listed with Provider Name, Type, Hostname/IP, Username and Options to edit/detect the trunk.

- Click on "Add SIP Trunk" or "Add IAX Trunk" to add a new VoIP trunk.
- Click on to configure detailed parameters for the VoIP trunk.
- Click on to configure Direct Outward Dialing (DOD) for the SIP Trunk.
- Click on to start LDAP Sync.
- Click on to delete the VoIP trunk.

For VoIP trunk example, please refer to the document in the following link:
http://www.grandstream.com/sites/default/files/Resources/ucm6xxx_sip_trunk_guide.pdf

The VoIP trunk options are listed in the table below.

Table 57: Create New SIP Trunk

Type	Select the VoIP trunk type. • Peer SIP Trunk • Register SIP Trunk
Provider Name	Configure a unique label (up to 64 character) 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 Original CID	Keep the CID from the inbound call when dialing out. This setting will override "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".

NAT	Turn on this setting when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall.
Disable This Trunk	If checked, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
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.
Caller ID Number	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 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 new name of the caller when the extension has no CallerID Name configured.
Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.
Allow outgoing calls if registration fails	Uncheck to block outgoing calls if registration fails. If "Need Registration" option is unchecked, this setting will be ignored.
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 from the provider when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for "Register SIP Trunk" type.
Auto Record	Enable automatic recording for the 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**.

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, the RemoteConnect related parameters will be set synchronously. Please make sure the trunk host is allocated by GDMS or it supports TLS.

Table 58: SIP Register Trunk Configuration Parameters

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.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". • UDP • TCP • TLS
SIP URI Scheme When Using TLS	When TLS is selected as Transport for register trunk, users can select between SIP and SIPS URI scheme
Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
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.

Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.
Allow outgoing calls if registration failure	If enabled outgoing calls even if the registration to this trunk fail will still be able to go through. Note that if we uncheck “Need Registration” option, this option will 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. This can be used to override the “From” Header. For example, "trunk.UCM630X.provider.com" is the From Domain in From Header: sip:1234567@trunk.UCM630X.provider.com.
From User	Configure the actual username of the extension. This can be used to override the “From” Header. There are cases where there is a single ID for registration (single trunk) with multiple DIDs. For example, "1234567" is the From User in From Header: 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 "Register SIP Trunk" type.
Auth Trunk	If enabled, the UCM will send 401 response to the incoming call to authenticate the trunk.
Auto Record	Enable automatic recording for the 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**.
RemoteConnect Mode	If enabled, the RemoteConnect related parameters will be set synchronously. Please make the trunk host is allocated by GDMS or it supports TLS.
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.

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.265, H.263, H.263p and VP8.
Send PPI Header	If enabled, the SIP INVITE message sent to the trunk will contain 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 SIP INVITE message.
PPI Mode	**Default** – Include the trunk’s preferred CID (configured in *Basic Settings*) in the PPI Header. **Original CID** – Include the original CID in the PPI Header. **DOD Number** – Include the trunk’s DOD number in the PPI Header. If no DOD number has been set, the trunk’s preferred CID will be used.
Send PAI Header	If enabled, the SIP INVITE message sent to the trunk will contain 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. **Note:** “Send PAI Header” needs to be enabled to use this feature
Send Anonymous	If checked, the "From" header in outgoing INVITE message will be set to anonymous.
DOD As From Name	If enabled and "From User" is configured, the INVITE's From header will contain the DOD number.
Passthrough PAI Header	If checked and option "Send PAI Header" 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 P-Access-Network-Info header.
Access Network Info	The access network information in the P-Access-Network-Info header.

Send Anonymous	If checked, the "From" header in outgoing INVITE message will be set to anonymous.
Outbound Proxy Support	Select to enable outbound proxy in this trunk. The default setting is "No".
Outbound Proxy	When outbound proxy support is enabled, enter the IP address or URL of the outbound proxy.
Remove OBP from Route	It is used to set if the phone system will remove outbound proxy URI from the route header. If is set to “Yes”, it will remove the route header from SIP requests. The default setting is “No”.
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".
GIN Registration	If enabled, the UCM will send a GIN REGISTER (generate implicit numbers).
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 64-bit codec, i.e., PCMU and PCMA. • **Auto:** Send DTMF using RFC4733 if offered. Otherwise, inband will be 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	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. The default setting is 60 seconds.
The Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission.
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure to enable Forward Error Correction (FEC) for video.
ICE support	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.

FECC	Configure to enable Far-end Camera Control
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
STIR/SHAKEN	Block disturbance calls, this function needs to be supported by the opposite end.
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 which 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.

Table 59: SIP Peer Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Auto Record	Enable automatic recording for the 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 "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
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.
Caller ID Number	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.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". • UDP • TCP • TLS
RemoteConnect Mode	If enabled, the RemoteConnect related parameters will be set synchronously. Please make the trunk host is allocated by GDMS or it supports TLS.
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.
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.265, H.263, H.263p and VP8.
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.
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.
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:** 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 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	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. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission.
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure to enable Forward Error Correction (FEC) for video.
ICE support	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.
FECC	Configure to enable Far-end Camera Control
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
IPVT Mode	Configures the UCM to be used exclusively for IPVT. **Warning:** This will lock out certain UCM features.
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 for LDAP sync feature. The UCM630X will automatically modify the remote contacts by adding prefix parsed from this rule.
LDAP Dialed Prefix	Specify the prefix for LDAP sync feature. The UCM630X will automatically modify the remote contacts by adding this prefix.
LDAP Last Sync Date	The last successful sync date.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
STIR/SHAKEN	Block disturbance calls, this function needs to be supported by the opposite end.
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 can make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which 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.

Table 60: Create New IAX Trunk

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 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 "Register IAX Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register IAX Trunk" type is selected.
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID Number	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 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.

Table 61: IAX Register Trunk Configuration Parameters

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 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 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.265, 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 "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 settings 0, which means no limited.

Table 62: IAX Peer Trunk Configuration Parameters

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 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.265, 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 "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 settings 0, which means no limited.

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.

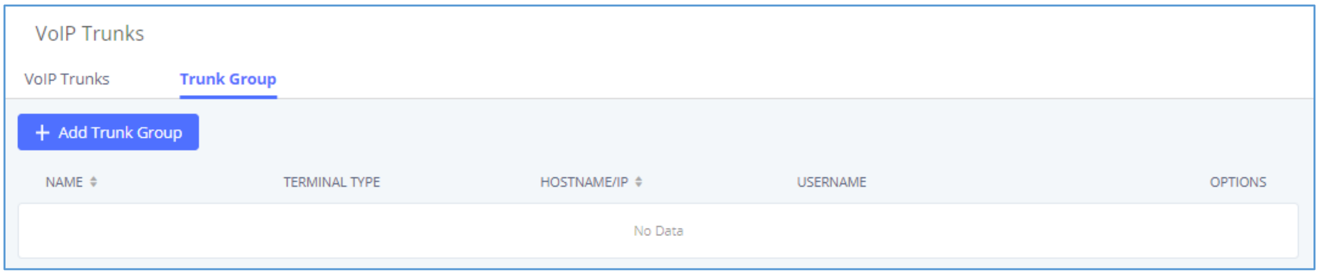


Figure 98: Trunk Group

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

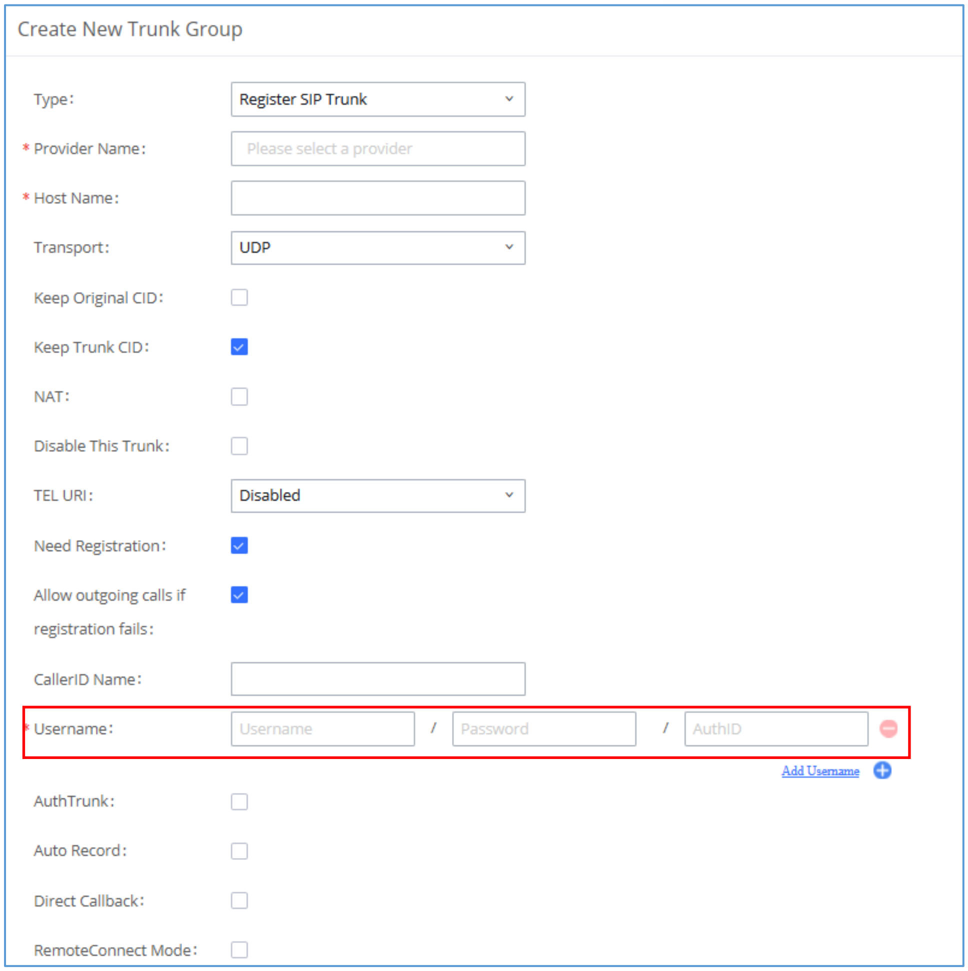


Figure 99: Trunk Group Configuration

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 to 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 to access the DOD options for the selected SIP Trunk.

3. Click "Add DOD" to begin your DOD setup

4. For "DOD Number" enter one of the numbers (DIDs) from your SIP trunk provider. In the example above Company ABC received 4 DIDs from their provider. ABC will enter in the number for the CEO's direct line.

5. Set the DOD name and If extension number need to be appended to the DID number click on “Add Extension”.

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.

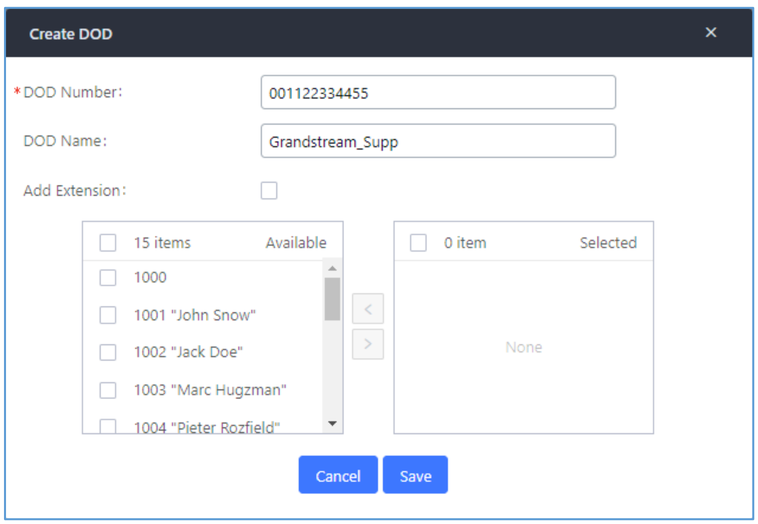


Figure 100: DOD extension selection

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 to a particular DOD.

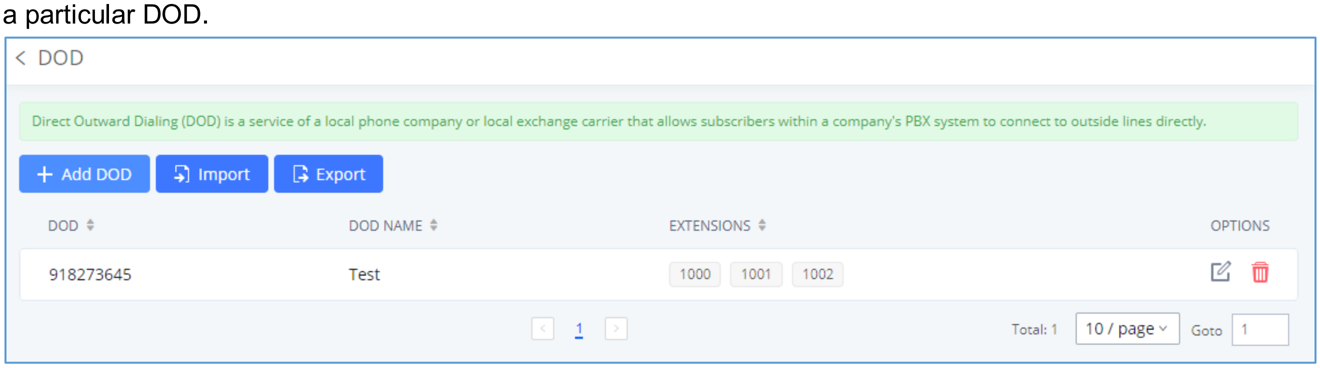


Figure 101: Edit DOD

Note: Users can import and export DOD files.

SLA STATION

The UCM630X supports SLA 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 line 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 SLA Station

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

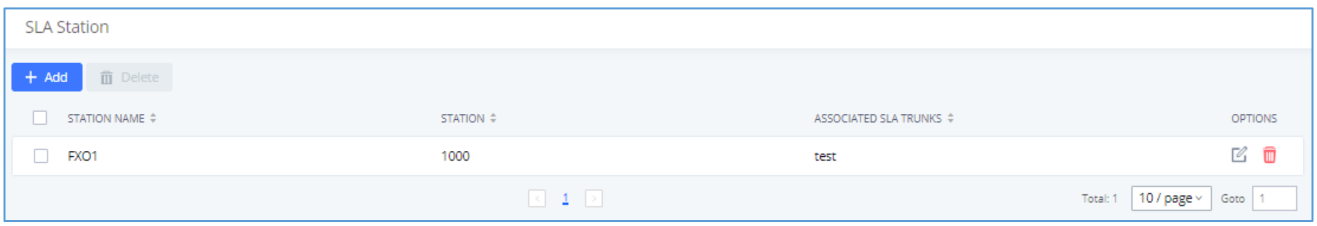


Figure 102: SLA Station

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

Table 63: SLA Station Configuration Parameters

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 delay before ringing the station when a call first coming 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".

Sample Configuration

1. On the UCM630X, go to Web GUI→**Extension/Trunk→Analog Trunks** page. Create 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.

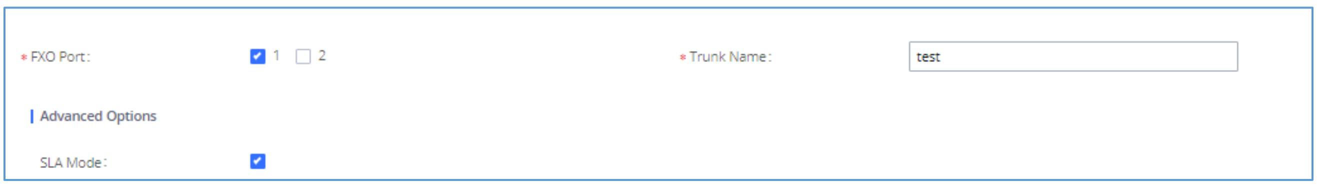


Figure 103: Enable SLA Mode for Analog Trunk

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

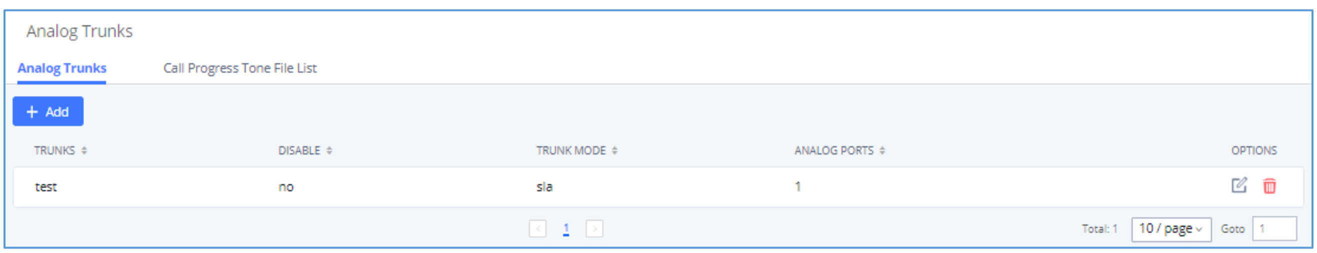


Figure 104: Analog Trunk with SLA Mode Enabled

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 two stations, 1002 and 1005, are configured to be associated with SLA trunk "fxo1".

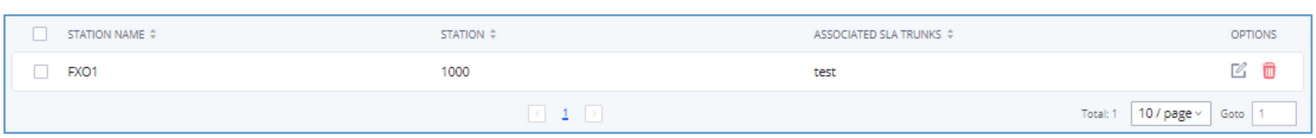


Figure 105: SLA Example - SLA Station

4. On the SIP phone 1, configure to register UCM630X extension 1002. Configure the MPK as BLF mode and the value must be set to “extension_trunkname”, which is 1002_fxo1 in this case.

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

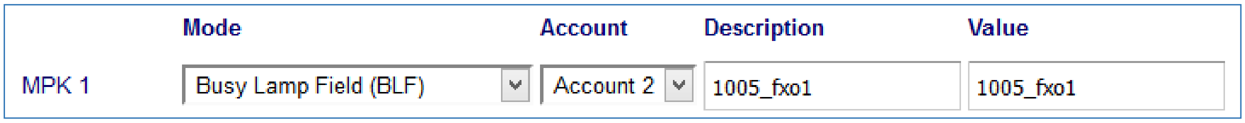


Figure 106: SLA Example - MPK Configuration

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 idle state, pressing 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 external number for the outbound call.

- **Making an outbound call from the station/extension, using BLF key**
  When the extension is in idle state, pressing the MPK and users could dial external numbers directly.

- **Answering call using LINE key**
  When the station is ringing, pressing 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.

CALL ROUTES

Outbound Routes

In the following sections, we will discuss the steps and parameters used to configure and manage outbound rules in UCM630X, these rules are the regulating points for all external outgoing calls initiated by the UCM through all types of trunks: SIP, Analog and Digital.

Configuring Outbound Routes

In the UCM630X, an outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g., "Local" 7-digit dials through an FXO while "Long distance" 10-digit dials through a low-cost SIP trunk). Users can also set up a failover trunk to be used when the primary trunk fails.

Go to Web GUI→**Extension/Trunk**→**Outbound Routes** to add and edit outbound rules.

- Click on + Add to add a new outbound route.
- Click on to edit the outbound route.
- Click on to delete the outbound route.

On the UCM630X, the outbound route priority is based on “Best matching pattern”. For example, the UCM630X has outbound route A with pattern 1xxx and outbound route B with pattern 10xx configured. When dialing 1000 for outbound call, outbound route B will always be used first. This is because pattern 10xx is a better match than pattern 1xxx. Only when there are multiple outbound routes with the same pattern configured.

Table 64: Outbound Route Configuration Parameters

Outbound Rule Name	Configure the name of the calling rule (e.g., local, long_distance, and etc.). Letters, digits, _ and - are allowed.
Pattern	All patterns are prefixed by "_" 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. In this example, 1,2,3,4,5,6,7,8,9 is 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 is to connect characters and it will be ignored.

	• [] Contain special characters ([x], [n], [z]) represent letters x, n, z.
Disable This Route	After creating the outbound 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 UCM. Users can enable it again when it is needed.
Password	Configure the password for users to use this rule when making outbound calls.
Local Country Code	If your local country code is affected by the outbound blacklist, please enter it here to bypass the blacklist.
Call Duration Limit	Enable to configure the maximum duration for the call using this outbound route.
Maximum Call Duration	Configure the maximum duration of the call (in seconds). The default setting is 0, which means no limit.
Warning Time	Configure the warning time for the call using this outbound route. If set to x seconds, the warning tone will be played to the caller when x seconds are left to end the call.
Auto Record	If enabled, calls using this route will automatically be recorded.
Warning Repeat Interval	Configure the warning repeat interval for the call using this outbound route. If set to X seconds, the warning tone will be played every x seconds after the first warning.
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 privilege level for the outbound rule. • **Internal:** The lowest level required. All users can use this rule. • **Local:** Users with Local, National, or International level can use this rule. • **National:** Users with National or International level can use this rule. • **International:** The highest level required. Only users with international level can use this rule. • **Disable:** The default setting is "Disable". If selected, only the matched source caller ID will be allowed to use this outbound route. Please be aware of the potential security risks when using "Internal" level, which means all users can use this outbound rule to dial out from the trunk.
Enable Filter on Source Caller ID	When enabled, users could specify extensions allowed to use this outbound route. "Privilege Level" is automatically disabled if using "Enable Filter on Source Caller ID". The following two methods can be used at the same time to define the extensions as the source caller ID.

	1. Select available extensions/extension groups from the list. This allows users to specify arbitrary single extensions available in the PBX. 2. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one. • 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. Note: Multiple patterns can be used. Patterns should be separated by comma "**,**". Example: _X. , _NNXXNXXXXX , _818X.
Outbound Route CID	Attempt to use the configured outbound route CID. This CID will not be used if DOD is configured.
Send This Call Through Trunk	
Trunk	Select the trunk for this outbound rule.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.
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.
Use Failover Trunk	
Failover Trunk	Failover trunks can be used to make sure that a call goes through an alternate route when the primary trunk is busy or down. If "Use Failover Trunk" is enabled and "Failover trunk" is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through. UCM630X support up to 10 failover trunks. Example: The user's primary trunk is a VoIP trunk and the user would like to use the PSTN when the VoIP trunk is not available. The PSTN trunk can be configured as the failover trunk of the VoIP trunk.

Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.
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.
Time Condition	
Time Condition Mode	Use Main Trunk or Failover Trunk: Use the Main Trunk and its settings during the configured time conditions. If the main trunk is unavailable, the Failover Trunk and its settings will be used instead. Use Specific Trunks: Use specific trunks during the configured time conditions. The Strip and Prepend settings of the Main Trunk will be used. If a trunk is unavailable during its time condition, no failover trunks will be used.

Outbound Blacklist

The UCM630X allows users to configure 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 in the blacklist. Please note that the blacklist settings apply to all outbound routes.

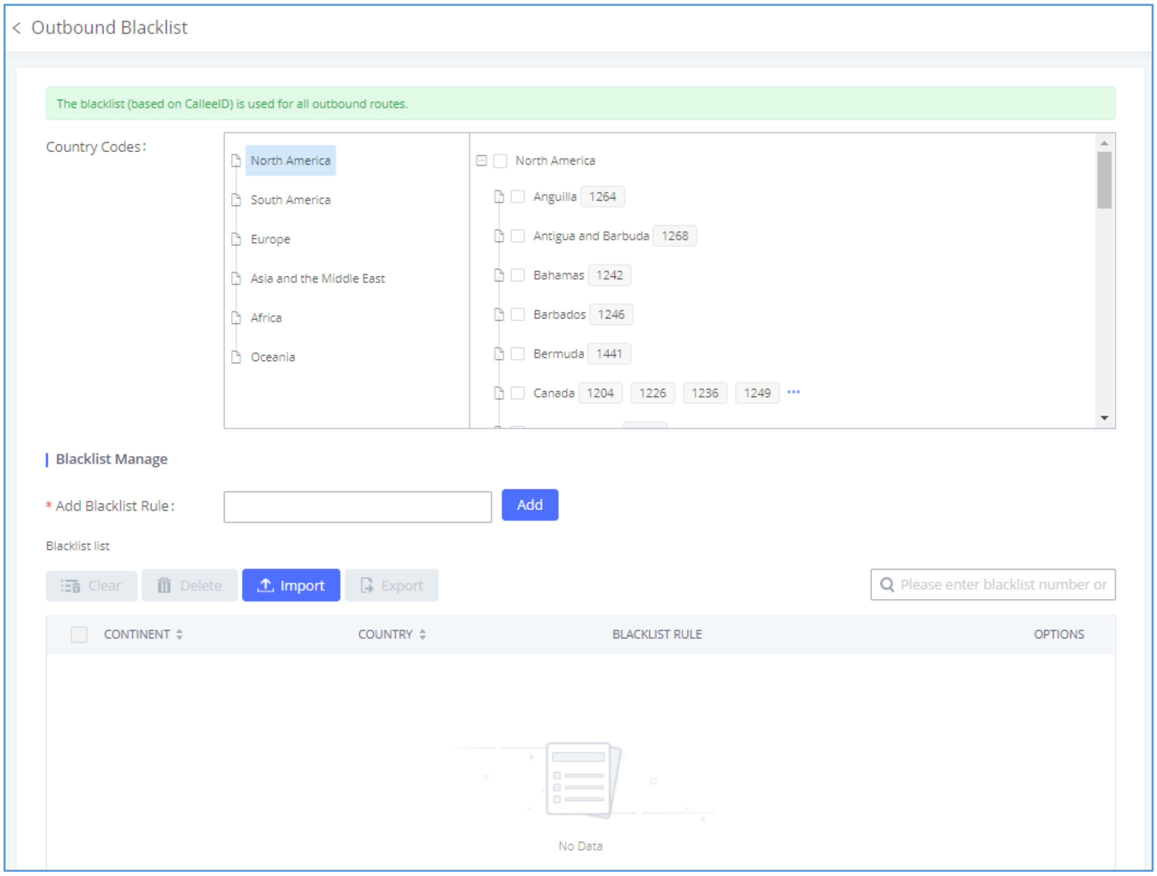


Figure 107: Country Codes

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

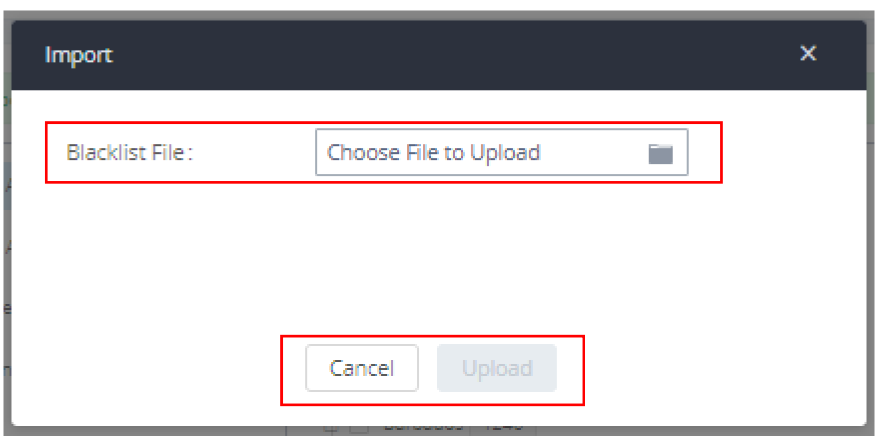


Figure 108: Blacklist Import/Export

Scheduled Sync

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

Table 65: 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). Valid range is 0-23.
Sync Frequency	Create new sync every x day(s). The valid range is 1 to 30.

PIN Groups

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

Table 66: Outbound Routes/PIN Group

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 asked once dialing via a trunk
PIN Name	Specify the name of the PIN

Once user click on PIN Groups the following figure shows to configure the new PIN.

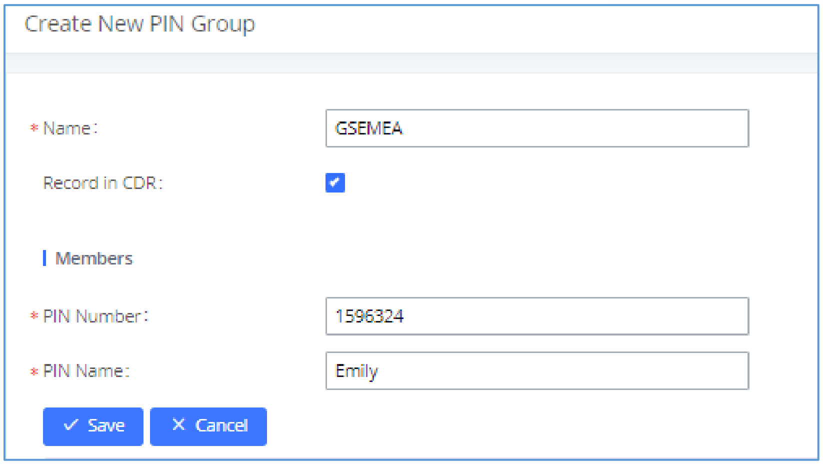


Figure 109: Create New PIN Group

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

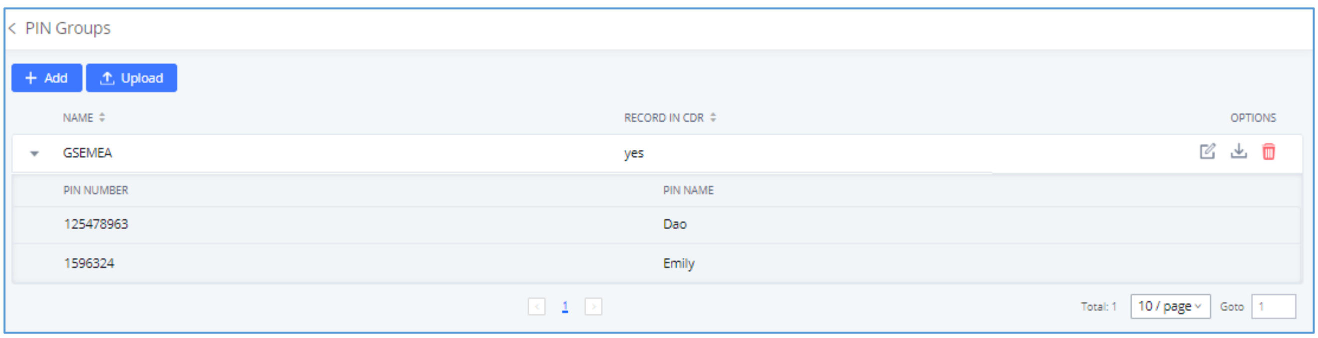


Figure 110: PIN Members

Note:

If PIN group is enabled on outbound route level, password, privilege level and enable 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.

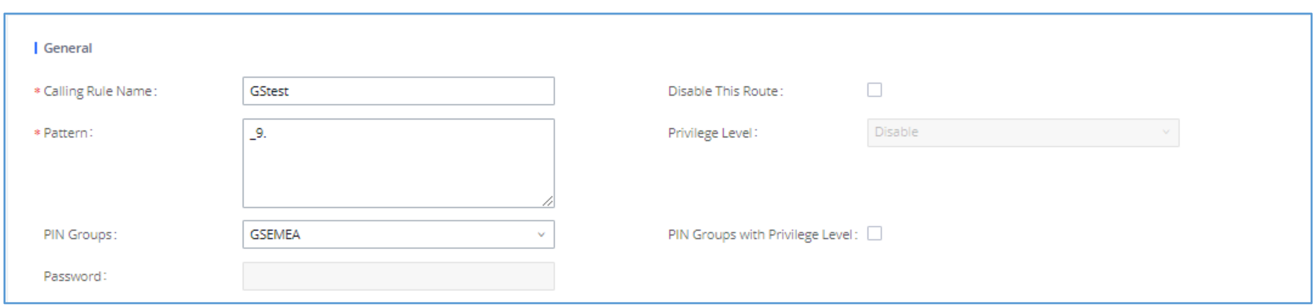


Figure 111: Outbound PIN

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

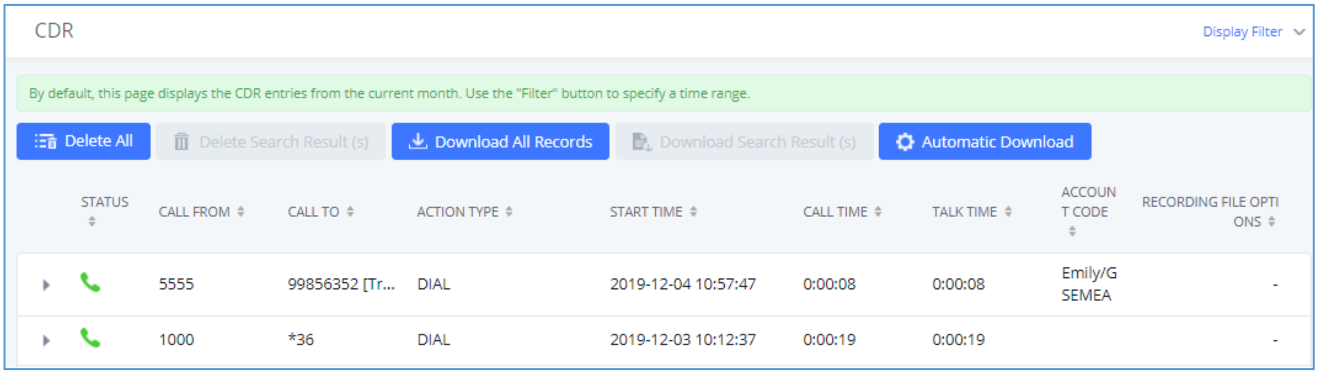


Figure 112: CDR Record

- **Importing PIN Groups from CSV files:**

User can also import PIN Groups by uploading CSV files for each group. To do this:

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

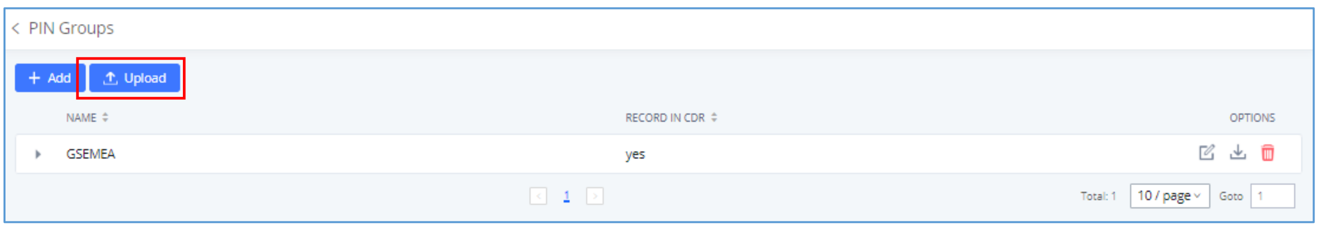


Figure 113: Importing PIN Groups from CSV files

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

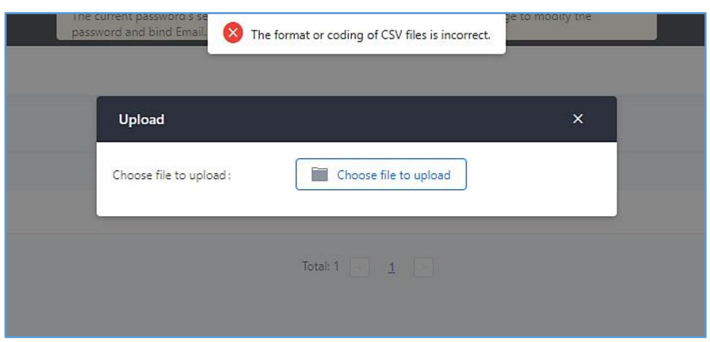
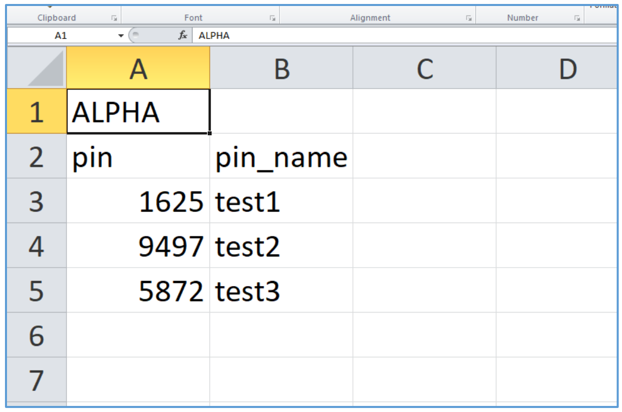


Figure 114: Incorrect CSV File

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				

Figure 115: 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.

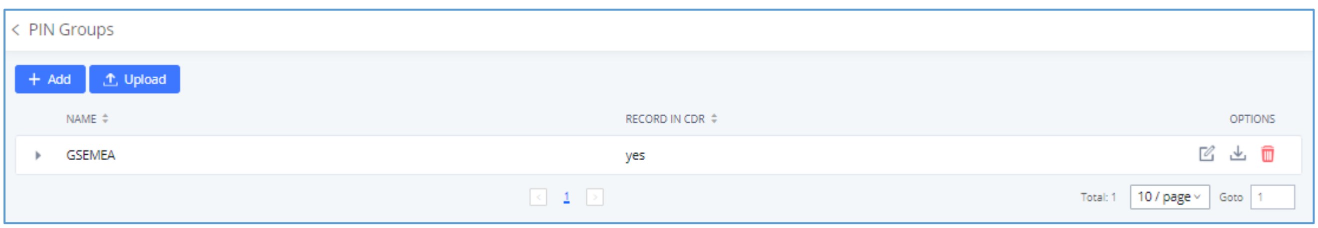


Figure 116: CSV File Successful Upload

Inbound Routes

Inbound routes can be configured via Web GUI→**Extension/Trunk**→**Inbound Routes**.

- Click on + Add to add a new inbound route.
- Click on "Blacklist" to configure blacklist for all inbound routes.
- Click on to edit the inbound route.
- Click on to delete the inbound route.

Inbound Rule Configurations

Table 67: Inbound Rule Configuration Parameters

<table>
<tr><td>Trunks</td><td>Select the trunk to configure the inbound rule.</td></tr>
<tr><td>Inbound Route Name</td><td>Configure the name of the Inbound Route. For example, "Local", "LongDistance" and etc.</td></tr>
<tr><td rowspan="2">Pattern</td><td>

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.
The pattern can be composed of two parts, Pattern and CallerID Pattern. The first part is used to specify the dialed number while the second part is used to specify the caller ID and it is optional, if set it means only the extension with the specific caller ID can call in or call out. For example, pattern '_2XXX/1234' means the only extension with the caller ID '1234' can use this rule.

</td></tr>
<tr><td>
Note:

Multiple patterns can be used. Each pattern should be entered in new line.
Users can add comments to the end of patterns to better organize and keep track of complex rules by typing “/*” and “*/” before and after each comment respectively

Example:
<table>
<tr><th>Pattern</th><th>CallerID Pattern</th></tr>
<tr><td>_X.</td><td>1000</td></tr>
<tr><td>_ NNXXNXXXXX /* 10-digit long distance */</td><td>1001</td></tr>
</table>
</td></tr>
<tr><td>Disable This Route</td><td>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 UCM. Users can enable it again when it is needed.</td></tr>
<tr><td>Seamless Transfer Whitelist</td><td>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.</td></tr>
<tr><td>Ringback tone</td><td>Choose the custom ring back tone to play when caller reaches the route.</td></tr>
</table>

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 UCM 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***.
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 field will show allowing to manipulate the CalleID Number and the Caller ID Name.
CalleID 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${CALLERID(num)}:** Prepends n to a CID number, where n is a number.
CallerID Name	Default string is **${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 fix name to incoming caller.
Enable Route-Level Inbound Mode	Gives uses the ability to configure inbound mode per individual route. When enabled two field 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 user 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, user can use feature code to switch between different modes/destinations.
Dial Trunk	This option shows up only when "By DID" is selected. If enabled, the external users dialing in to the trunk via this inbound route can dial outbound call using the UCM'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, check this level might be risky for security purpose. • **Local:** User 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 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 are: • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Groups • IVR • Voicemail Groups • Dial By Name • All
Default Destination	Select the default destination for the inbound call. • Extension • Voicemail • Conference Room • Call Queue • Ring Group • Paging/Intercom • Voicemail Group • DISA • IVR • External Number • By DID When "By DID" is used, the UCM 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
Strip	Specify the number of digits to strip from the beginning of the DID. This is used when "By DID" is selected in "Default Destination".

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.
Time Condition	
Start Time	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 UCM 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 "Strip" option. • Dial By Name • External Number • Callback

Inbound Route: Prepend Example

UCM630X now allows user to prepend digits to an inbound DID pattern, with strip taking precedence over prepend. With the ability to prepend digits in inbound route DID pattern, 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 become 2163.
4. UCM630X will now forward the incoming call to extension 2163.

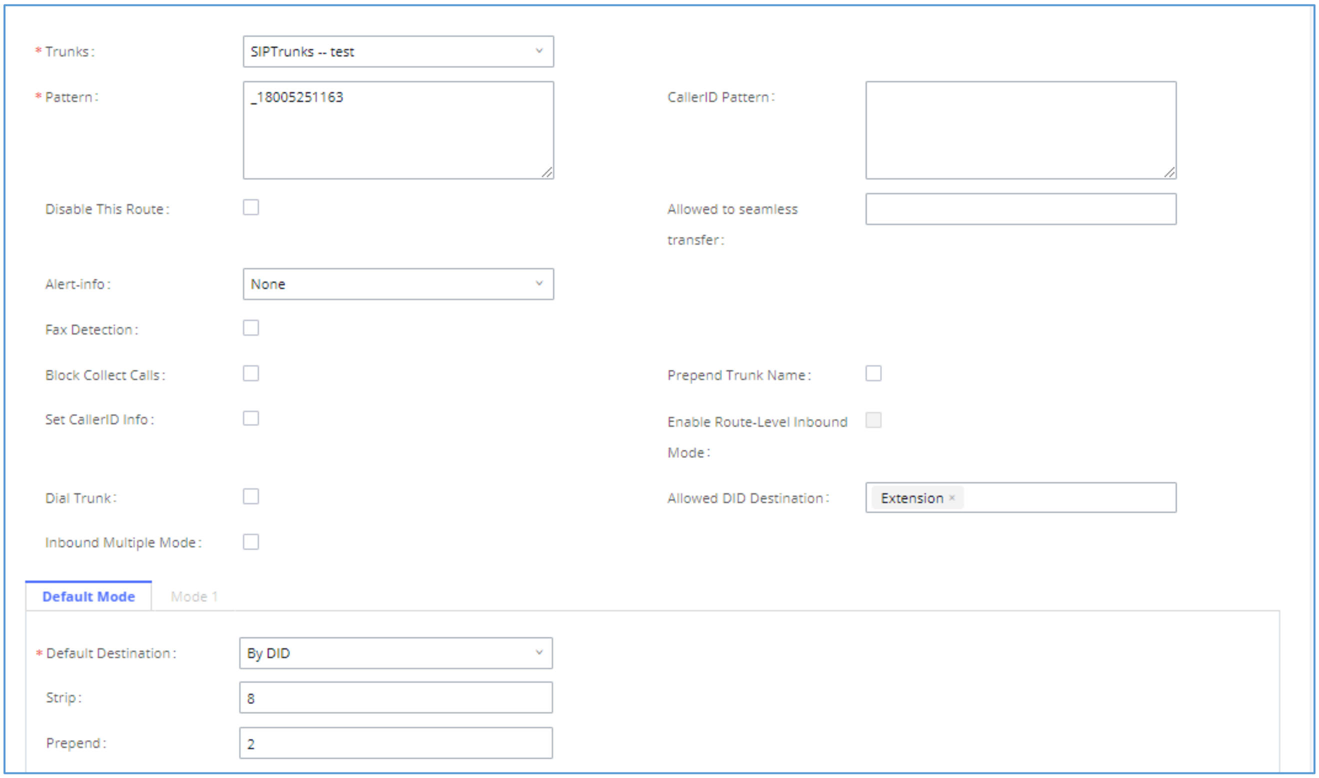


Figure 117: Inbound Route feature: Prepend

Inbound Route: Multiple Mode

In the UCM630X, the user can configure inbound route to enable multiple mode to switch between different destinations. The inbound multiple mode can be enabled under Inbound Route settings.

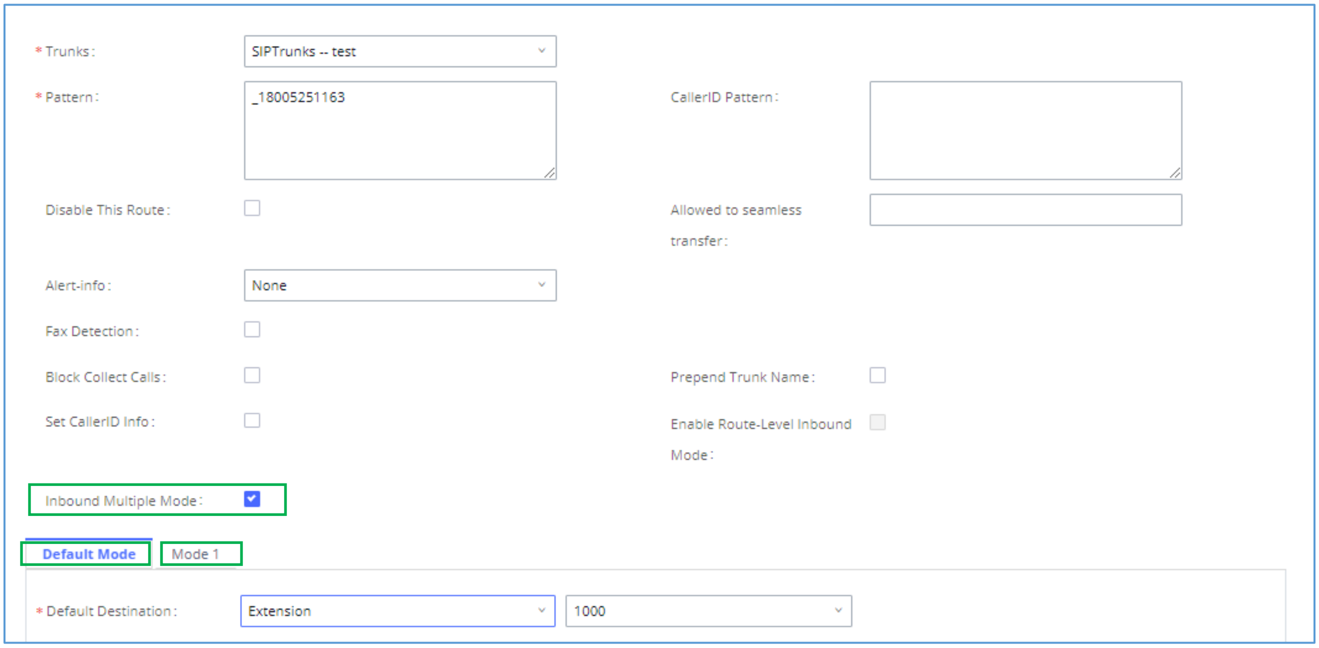
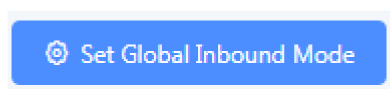


Figure 118: Inbound Route - Multiple Mode

When Multiple Mode is enabled for the inbound route, the user can configure a “Default Destination” and a “Mode 1” destination for all routes. By default, the call coming into the inbound routes will be routed to the default destination.

SIP end devices that have registered on the UCM630X can dial feature code *62 to switch to inbound route “Mode 1” and dial feature code *61 to switch back to “Default Destination”. Switching between different mode can be easily done without Web GUI login.

For example, the customer service hotline destination has to be set to a different IVR after 7PM. The user can dial *62 to switch to “Mode 1” with that IVR set as the destination before off work.

To customize feature codes for “Default Mode” and “Mode 1”, click on 

under “Inbound Routes” page, check “Enable Inbound Multiple Mode” option and change “Inbound Default Mode” and “Inbound Mode 1” values (By default, *61 and *62 respectively).

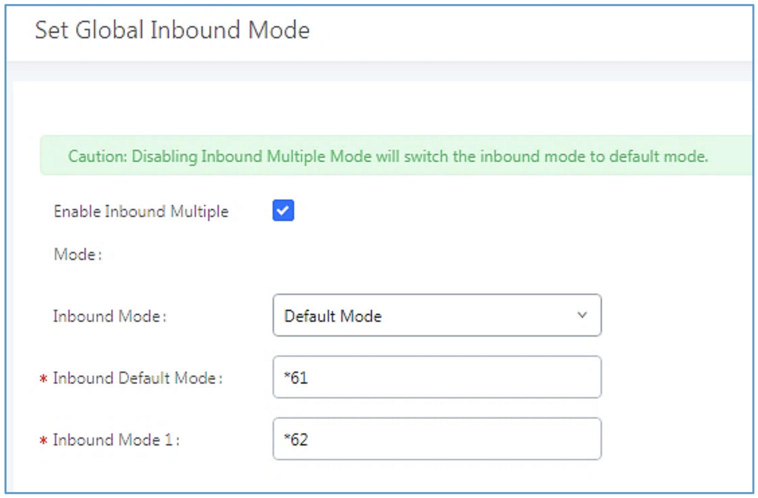


Figure 119: Inbound Route - Multiple Mode Feature Codes

Inbound Route: Route-Level Mode

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

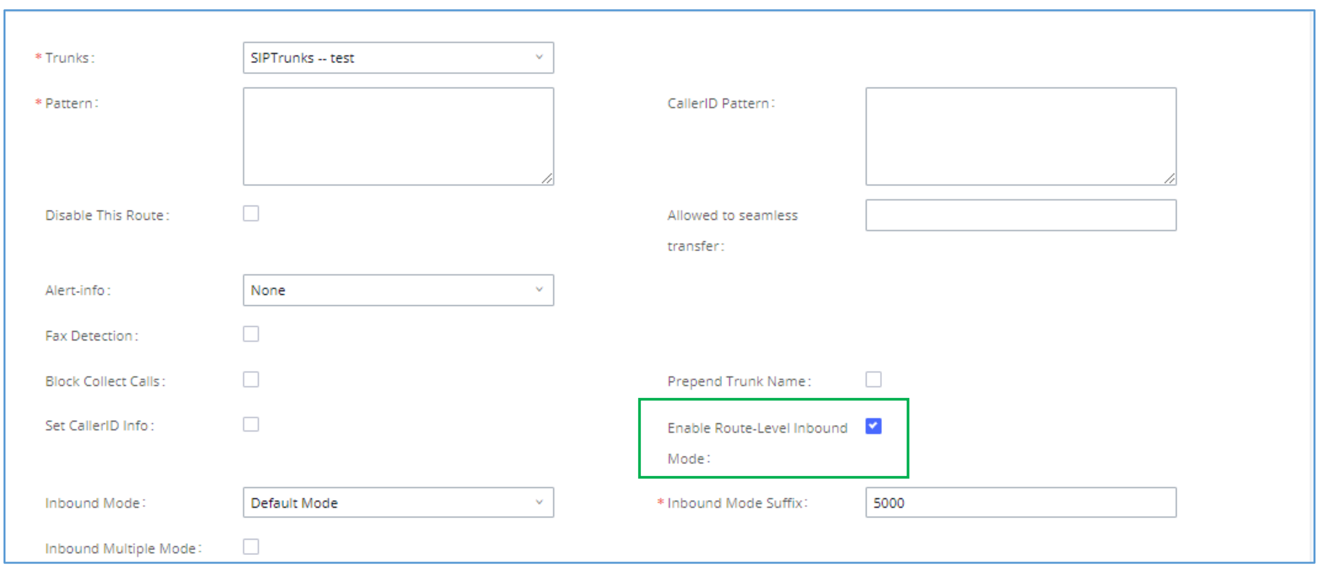


Figure 120: Inbound Route - Route-Level Mode

Global inbound mode must be enabled before configuring Route-Level Inbound Mode. Additionally, the Mode 1 must be configured as well.

When Route-Level Inbound Mode is enabled, the user can configure a “Default Destination” and a “Mode 1” destination for each specific route. By default, the call coming into this specific inbound route will be routed to the default destination.

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

For example, Inbound Default Mode feature code is set to **61* and the Inbound Mode suffix 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 *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 Route: 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 Set Global Inbound Mode button and enable Inbound Multiple Mode.
3. Edit the subscribe number field to the desired BLF value.

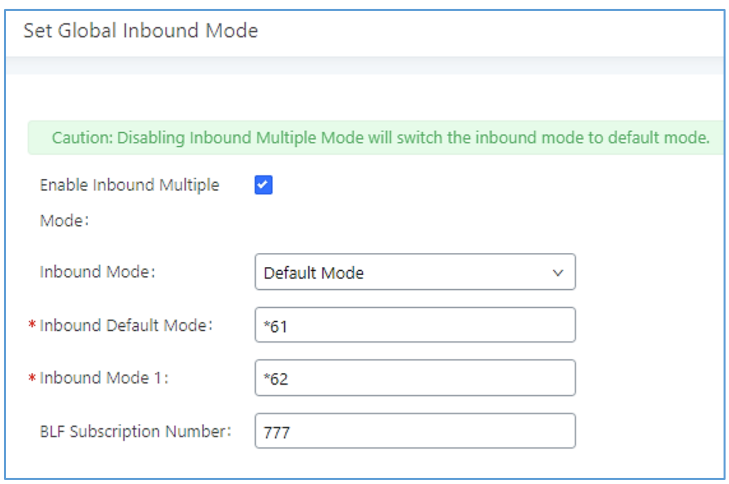


Figure 121: Global Inbound Mode

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".

Figure 122: 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.

Figure 123: Inbound Mode - Mode 1

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.

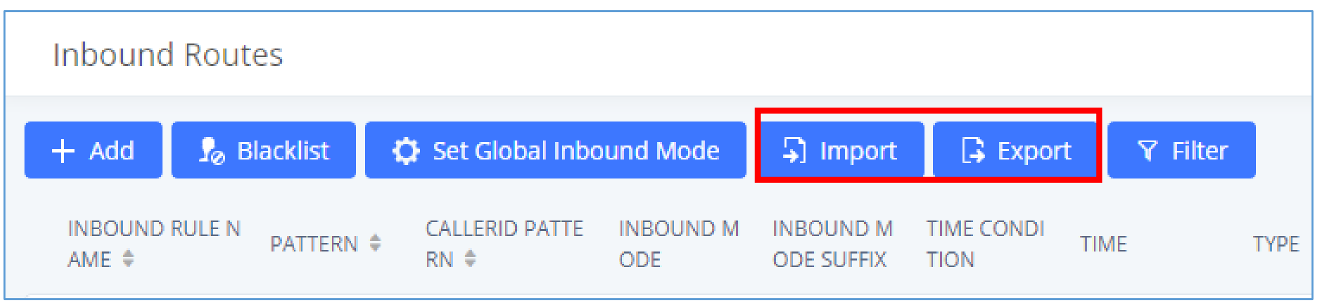


Figure 124: Import/Export Inbound Route

The imported file should be on CSV 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… User 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… User 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.

FAX with Two Media

The UCM630X supports Fax re-INVITE with multiple codec negotiation. If a Fax re-INVITE contains both T.38 and PCMA/PCMU codec, UCM630X will choose T.38 codec over PCMA/PCMU.

Blacklist Configurations

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

- Select the checkbox for "Blacklist Enable" to turn on Blacklist feature for all inbound routes. Blacklist is disabled by default.
- Enter a number in "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 "Blacklist list" and click on or click on "Clear" button to remove all the numbers on the blacklist.
- User can also export the inbound route blacklist by pressing on Export button.

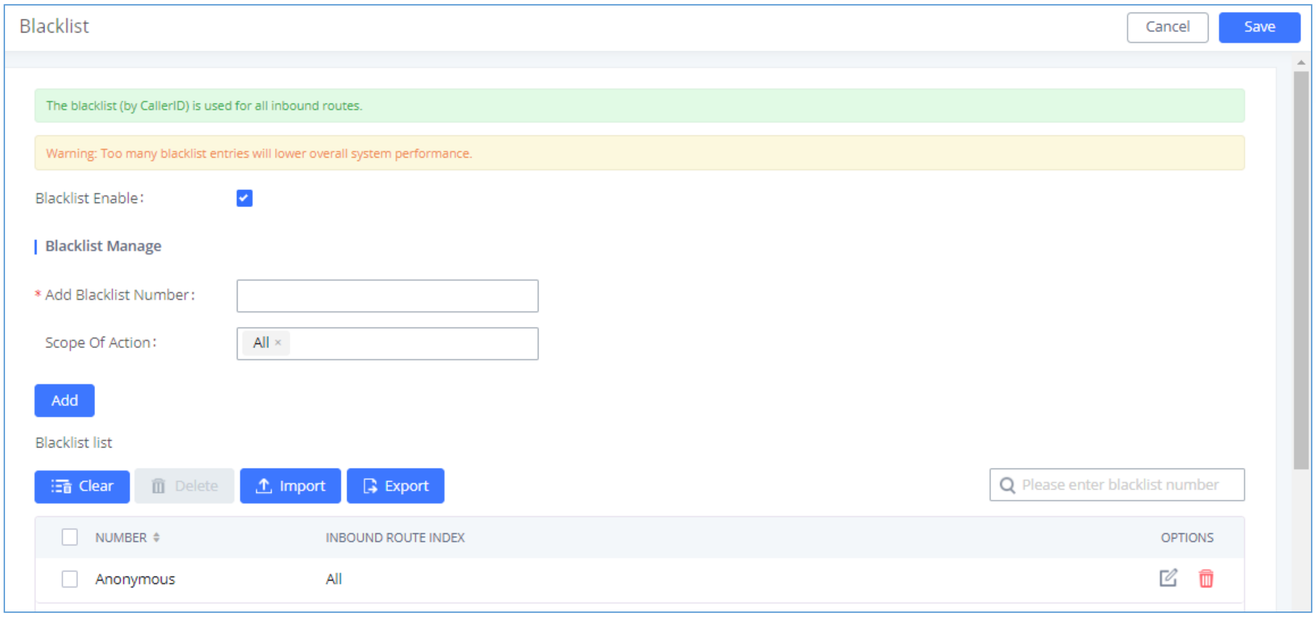


Figure 125: Blacklist Configuration Parameters

- To add blacklist number in batch, click on “Import” to upload blacklist file in csv format. The supported csv format is as below.

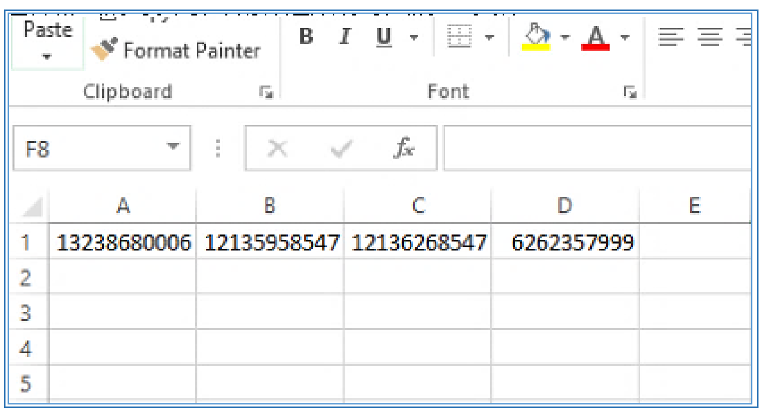


Figure 126: Blacklist csv File

⚠ **Note:**

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→**Call Features**→**Feature Codes**.

FAX SERVER

The UCM6300 series supports T.30/T.38 Fax 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→**Call Features→FAX/T.38**. The list of received Fax files will be displayed in 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.

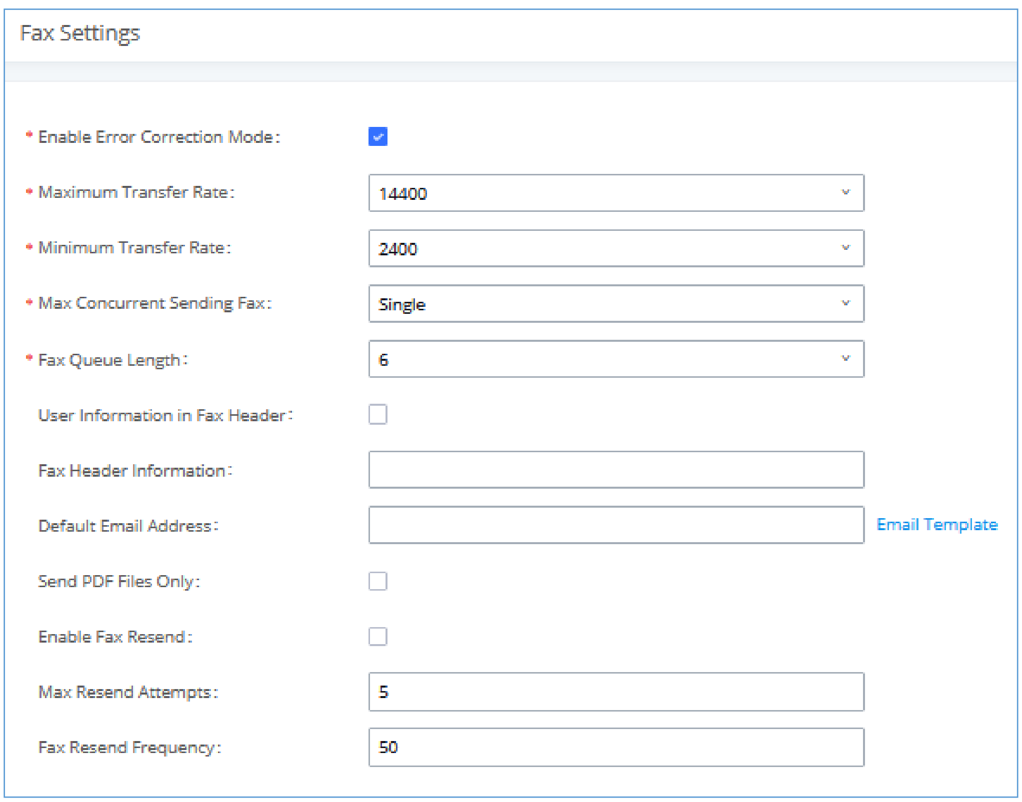


Figure 127: Fax Settings

Table 68: FAX/T.38 Settings

Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is "Yes".
Maximum Transfer Rate	Configure the maximum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14400. The default setting is 14400.
Minimum Transfer Rate	Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14000. The default setting is 2400.
Max Concurrent Sending Fax	Configure the concurrent fax that can be sent by UCM6300. Two modes “Only” and “More” are supported. • **Only** Under this mode, the UCM6300 allows only single user to send fax at a time. • **More** Under this mode, the UCM6300 supports multiple concurrent fax sending by the users. By default, this option is set to “only”.
Fax Queue Length	Configure the maximum length of Fax Queue from 6 to 10. The default setting is 6.
User Information in Fax Header	If enabled this this will give users the option to send a special header in SIP fax messages.
Fax Header Information	Adds fax header into the fax file.
Default Email Address	Configure the Email address to send the received Fax to if user's Email address cannot be found. **Note:** The extension's Email address or the Fax's default Email address needs to be configured in order to receive Fax from Email. If neither of them is configured, Fax will not be received from Email.
Template Variables	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users. The template variables are:

	• ${CALLERIDNUM} : Caller ID Number • ${CALLERIDNAME} : Caller ID Name • ${RECEIVEEXTEN} : The extension to receive the Fax • ${FAXPAGES} : Number of pages in the Fax • ${VM_DATE} : The date and time when the Fax is received
Send PDF Files Only	If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.
Enable Fax Resend	Enables the fax resend option which allow the UCM to keep attempting to send faxes up to a specified amount of times. Additionally, if a fax still fails to send, a *Resend* button will appear in the File Send Progress list in *Value-Added Features→Fax Sending* to allow manual resending.
Max Resend Attempts	Configures the maximum attempts number to resend the fax. Default value is set to 5.
Fax Resend Frequency	Configures the Fax Resend Frequency. Default value is set to 50.

Receiving Fax

Example Configuration to Receive Fax from PSTN Line

The following instructions describe how to use the UCM6300 to receive fax from 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 "Fax Detection" option is set to "NO".

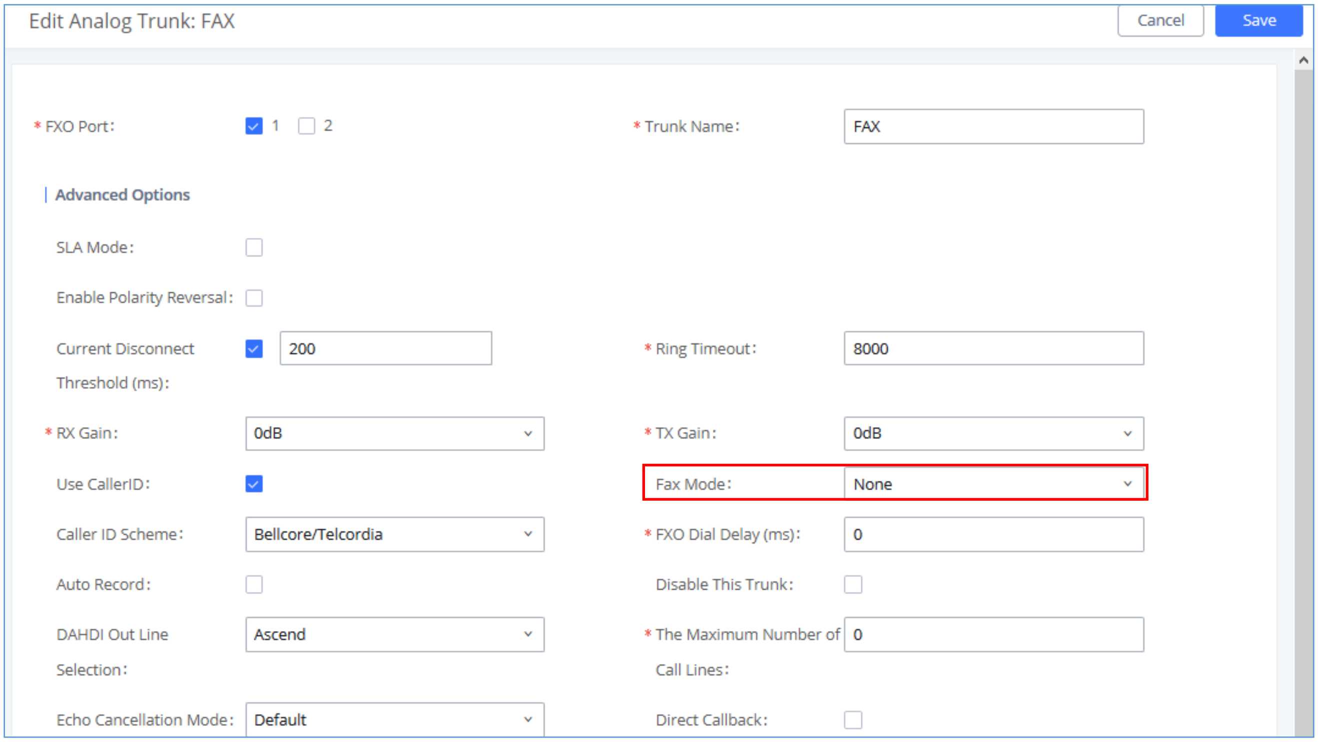


Figure 128: Configure Analog Trunk

5. Go to UCM6300 Web GUI→**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.

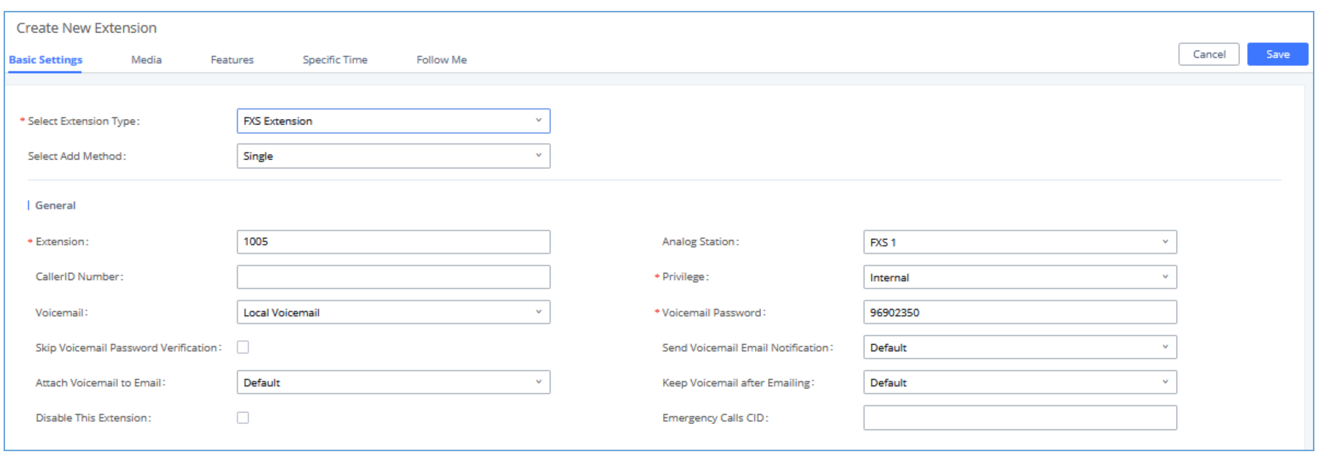


Figure 129: Configure Extension for Fax Machine: FXS Extension

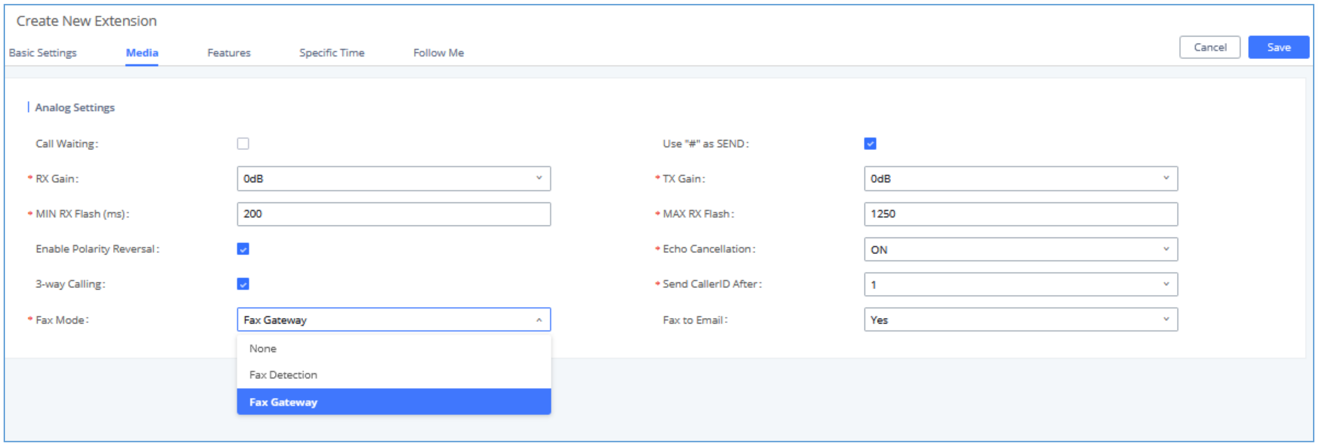


Figure 130: Configure Extension for Fax Machine: Analog Settings

7. Go to Web GUI→**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.

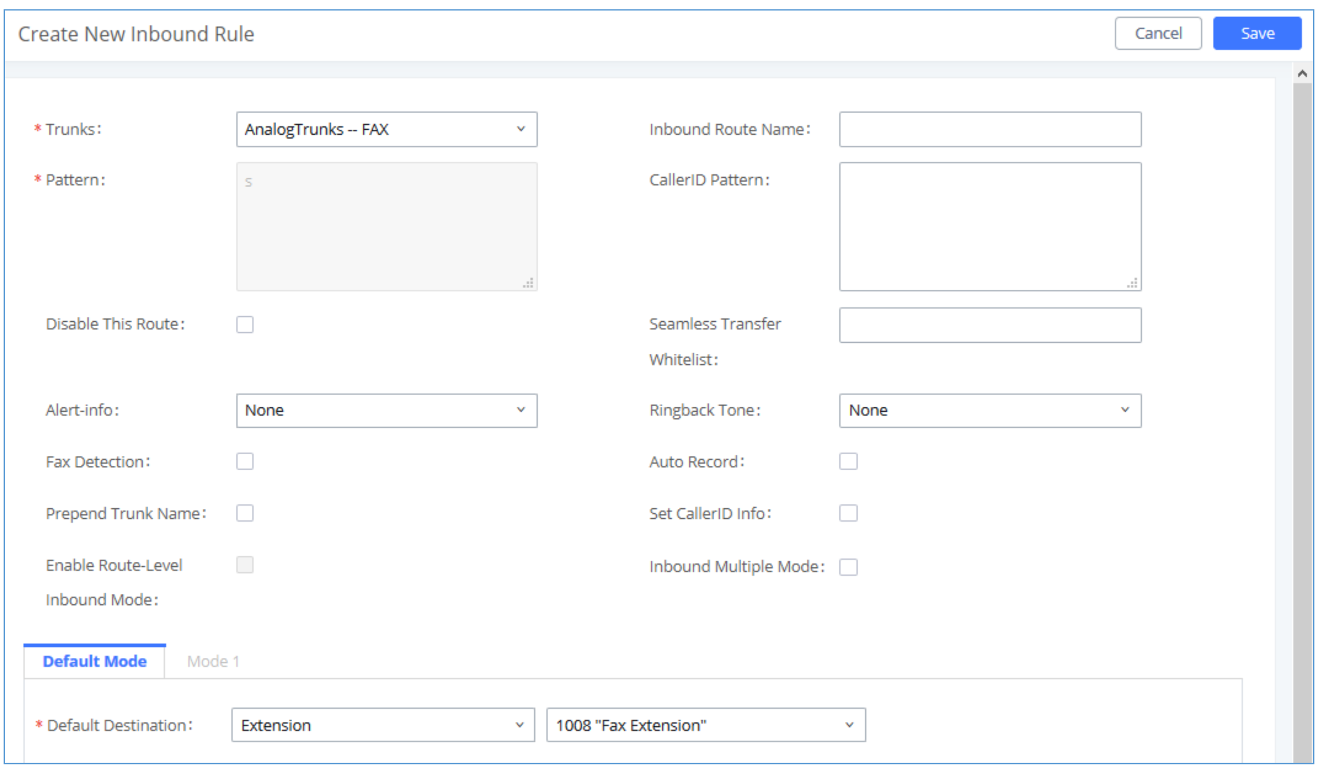


Figure 131: Configure Inbound Rule for Fax

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→**Call Features**→**Fax/T.38** page. Create a new Fax extension.

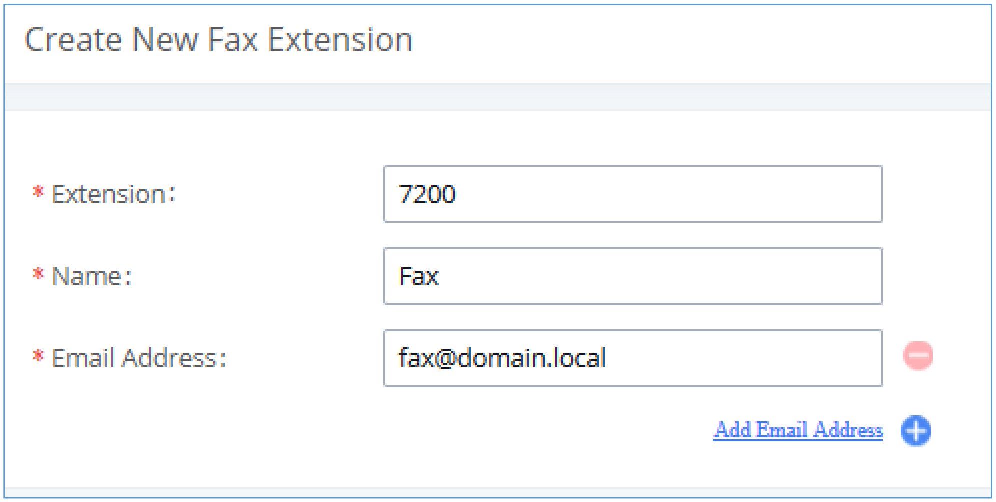


Figure 132: Create Fax Extension

3. Go to UCM6300 Web GUI→**Extension/Trunk**→**Analog Trunks** page. Create a new analog trunk. Please make sure "Fax Detection" is set to "No".

4. Go to UCM6300 Web GUI→**Extension/Trunk**→**Inbound Routes** page. Create a new inbound route and set the default destination to the Fax extension.

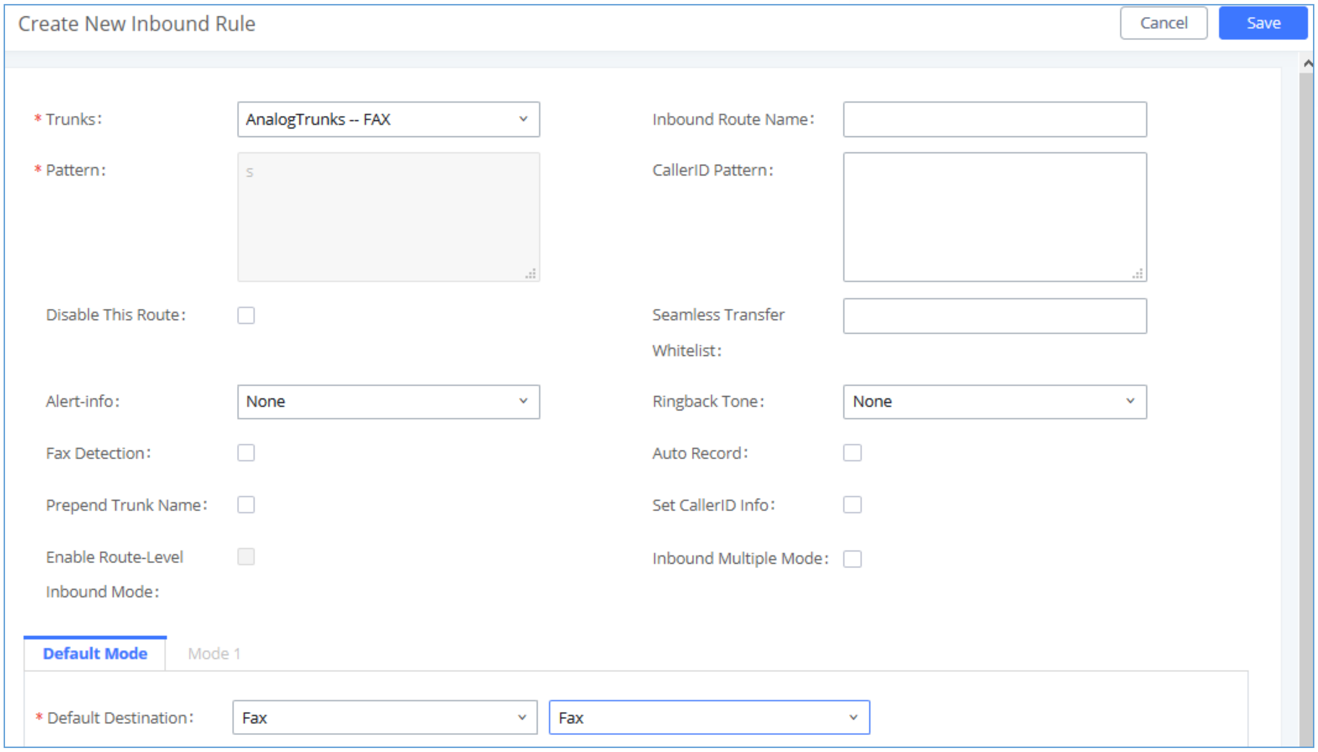


Figure 133: Inbound Route to Fax Extension

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.

Note: 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.

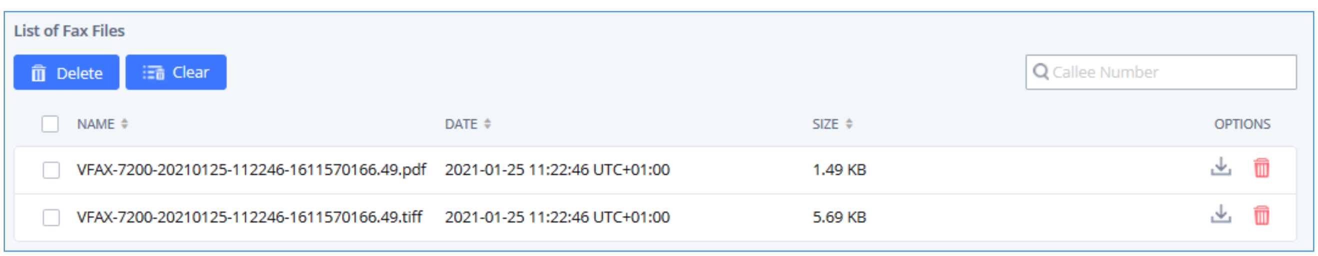


Figure 134: List of Fax Files

FAX Sending

Besides the support of Fax machines, The UCM6300 supports also sending Fax via Web GUI access. This feature can be found on Web GUI→**Value-added Features**→**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.

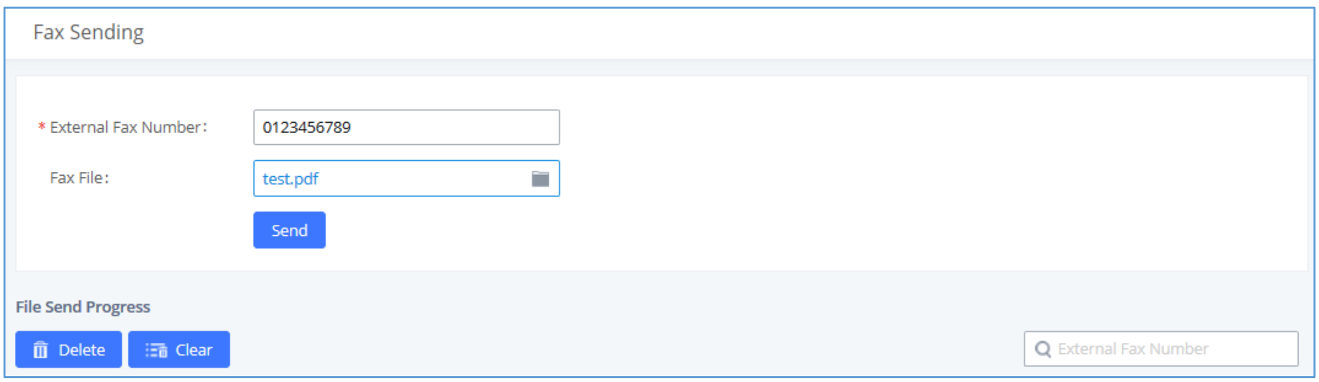


Figure 135: Fax Sending in Web GUI

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

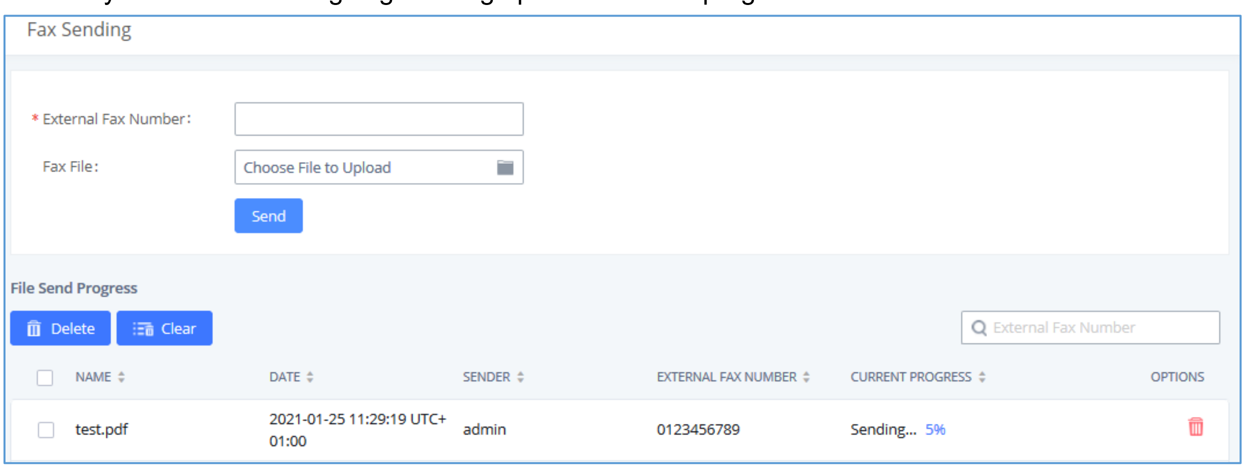


Figure 136: Fax Send Progress

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

AUDIO CONFERENCE

The UCM630X supports conference room allowing multiple rooms used at the same time.
The conference room configurations can be accessed under Web GUI→**Call Features**→**Audio Conference**. In this page, users could create, edit, view, invite, manage the participants, and delete conference rooms. The conference room status and conference call recordings (if recording is enabled) will be displayed in this web page as well.

The UCM admin can create multiple audio conference rooms for users to dial in.

UCM630x series	Number of audio conference room	Participant limit
UCM6301	3	75
UCM6302	8	150
UCM6304	15	200
UCM6308	25	300

Conference Room Configurations

- Click on "Add" to add a new conference room.
- Click on to edit the conference room.
- Click on to delete the conference room.

Table 69: Conference Room Configuration Parameters

Extension	Configure the conference number for the users to dial into the conference. **Note:** Up to 64 characters.
Privilege	Please select the permission level for outgoing calls.
Password	When configured, the users who would like to join the conference call must enter this password before accessing the conference room. **Note:** The password must be at least 4 characters.
Host Password	Configure the password to join the conference room as Moderator. Conference Moderator can manage the conference call via IVR (if "Enable Caller Menu" is enabled) as well as invite other parties to join the conference by dialing "0" (permission required from the invited party) or "1" (permission not required from the invited party) during the conference call.

	Note: If the Moderator Password field is left blank, moderator functionality will not be available for the meeting.
Enable Caller Menu	If enabled, conference participant could press the * key to access the conference room menu. The default setting is "No".
Record Conference	If enabled, the calls in this conference room will be recorded automatically in a .wav format file. All the recording files will be displayed and can be downloaded in the conference web page. The default setting is "No".
Kicking Warning Interval	If there is only one participant in a conference room, a kick warning prompt will play at the configured interval. If no input from the participant is received after the prompt, he will be automatically kicked out of the conference. The valid range is 1-60 minutes.
Wait For Moderator	If enabled, the participants will not hear each other until the host joins the conference. The default setting is "No". **Note:** If "Quiet Mode" is enabled, the voice prompt for "Wait For Admin" will not be announced.
Allow User Invite	If enabled, users could press 0 to invite other users (with the users' permission) or press 1 to invite other users (without the user's permission) to join the conference. The default setting is "No". **Note:** Conference administrator can always invite other users without enabling this option.
Announce Callers	If enabled, the caller will be announced to all conference participants when there the caller joins the conference. The default setting is "No". **Note:** "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.
Quiet Mode	If enabled, if there are users joining or leaving the conference, voice prompt or notification tone will not be played. The default setting is "No". **Note:** "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.
Play Hold Music	If enabled, the UCM630X will play Hold music when there is only one user in the conference. The default setting is "No".
Custom Music On Hold	Select the music on hold class to be played in conference call. Music On Hold class can be set up under Web GUI→**PBX Settings**→**Music On Hold**.

Skip Authentication	If enabled, the invitation from Web GUI for a conference room with password will skip the authentication for the invited users. The default setting is "No".

Conference Settings contains the following options:

Table 70: Conference Settings

Enable Talk detection	If enabled, the AMI will send the corresponding event when a user starts or ends talking.
DSP Talking Threshold	The time in milliseconds of sound above what the dsp has established as base line silence for a user before a user is considered to be talking. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 200.
DSP Silence Threshold	The time in milliseconds of sound falling within the what the dsp has established as base line silence before a user is considered to be silent. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 2500.

Users can check the talking Caller IDs in conference control page (UCM WebUI→Call Features→Conference). The image will move up and down when the user is talking.

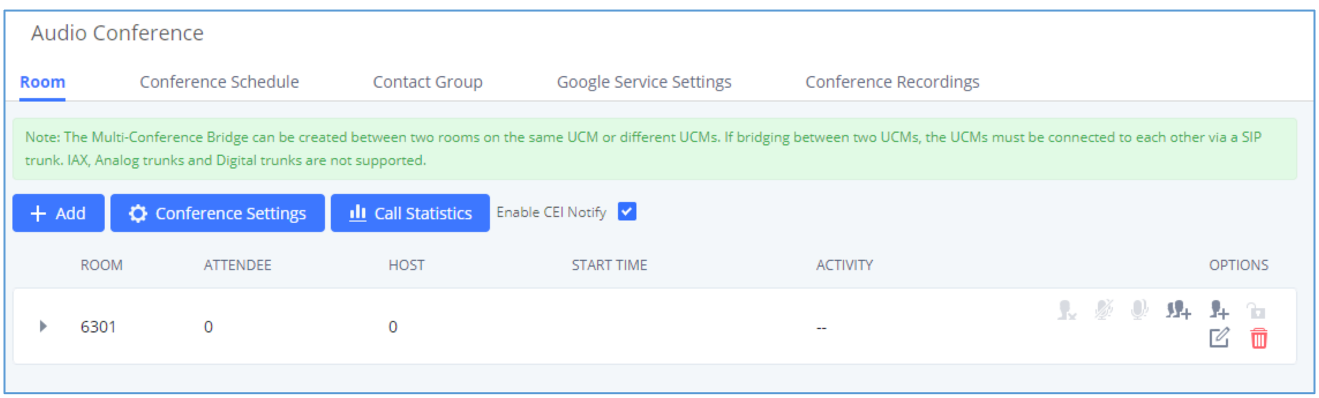


Figure 137: Conference

Conference Call Operations

Join a Conference Call

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

Invite Other Parties to Join Conference

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

- **Invite from Web GUI.**

For each conference room in UCM630X Web GUI→**Call Features**→**Conference**, 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.

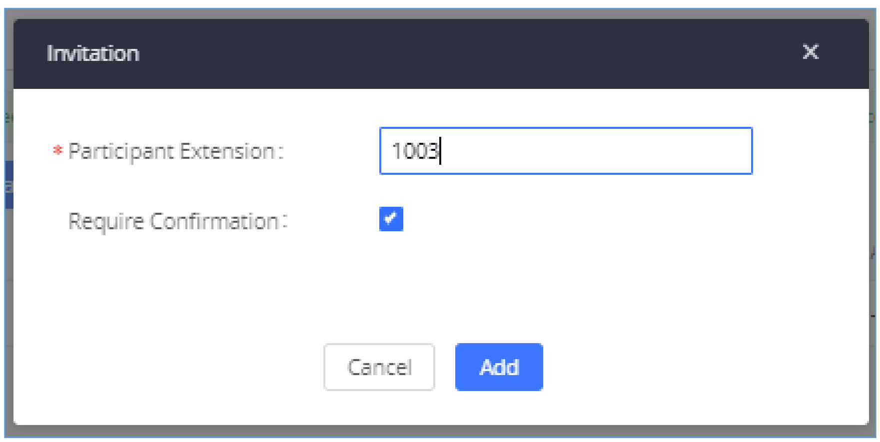


Figure 138: Conference Invitation from Web GUI

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

A conference participant can invite other parties to the conference by dialing from the phone during the conference call. Please make sure option "Enable User Invite" is turned on for the conference room first. Enter 0 or 1 during the conference 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 conference.

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.

⚠ **Note:**

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 Conference

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

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

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

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

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

If "Enable Caller Menu" is enabled, conference participant can input * to enter the IVR menu for the conference. Please see options listed in the table below.

Table 71: Conference Caller IVR Menu

Conference 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.
Conference 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.

⚠ **Note:**

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

Google Service Settings Support

UCM630X now supports Google OAuth 2.0 authentication. This feature is used for supporting UCM630X conference scheduling system. Once OAuth 2.0 is enabled, UCM630X conference system can access Google calendar to schedule or update conference.

Google Service Settings can be found under Web GUI→**Call Features→Conference→Google Service Settings→Google Service Settings**.

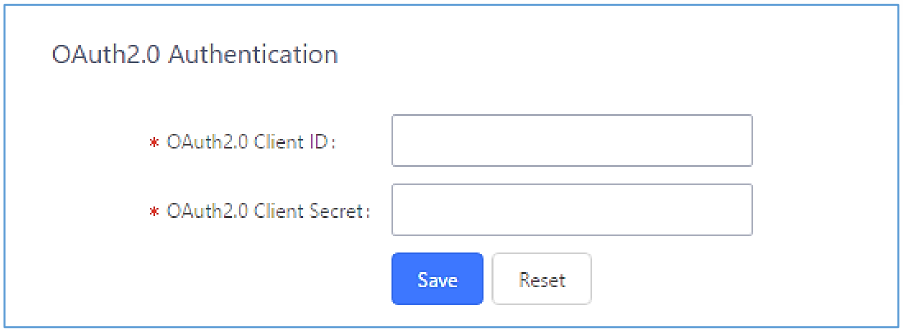


Figure 139: Google Service Settings→OAuth2.0 Authentication

If you already have OAuth2.0 project set up on **Google Developers** web page, please use your existing login credential for "OAuth2.0 Client ID" and "OAuth2.0 Client Secret" in the above figure for the UCM630X to access Google Service.

If you do not have OAuth2.0 project set up yet, please following the steps below to create new project and obtain credentials:

1. Go to Google Developers page https://console.developers.google.com/start Create a New Project in Google Developers page.

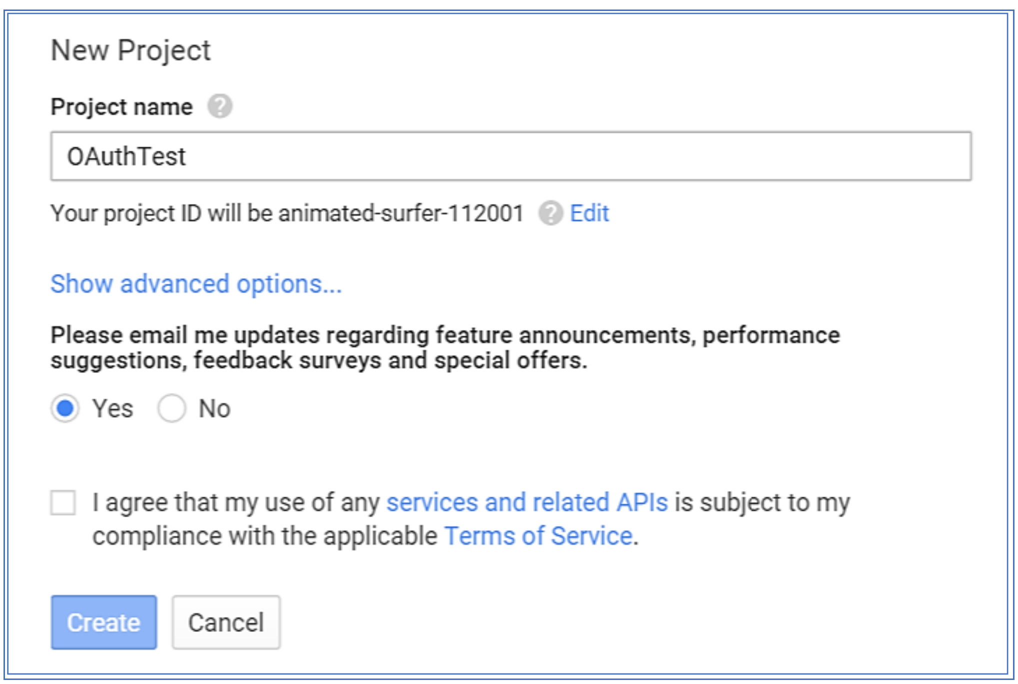


Figure 140: Google Service→New Project

2. Enable Calendar API from API Library.

3. Click “Credentials” on the left drop down menu to create new OAuth2.0 login credentials.

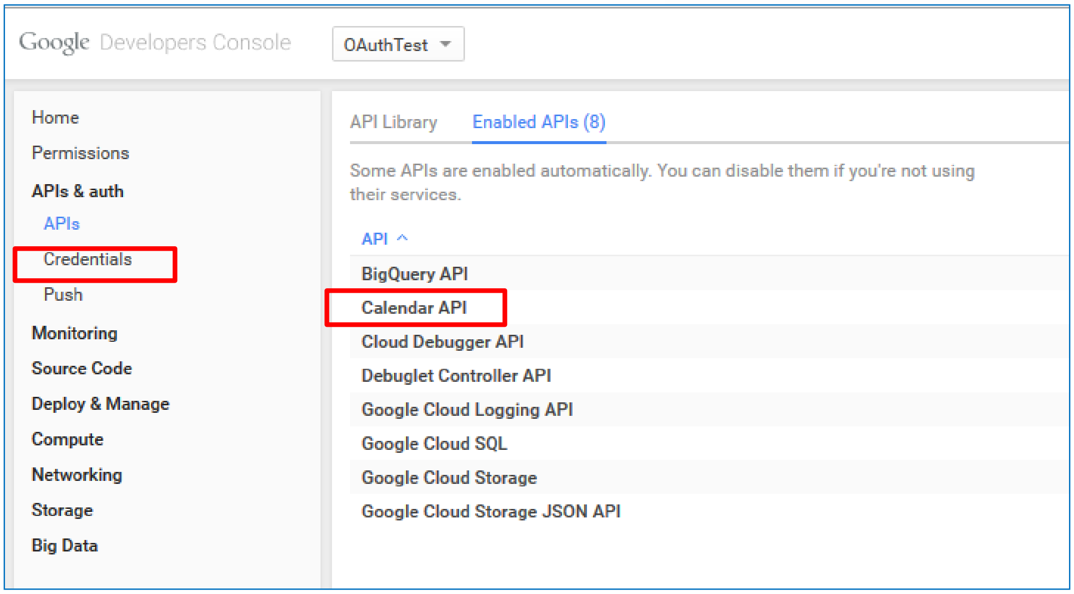


Figure 141: Google Service→Create New Credential

4. Use the newly created login credential to fill in “OAuth2.0 Client ID” and “OAuth2.0 Client Secret”.
5. Click “Get Authentication Code” to obtain authentication code from Google Service.

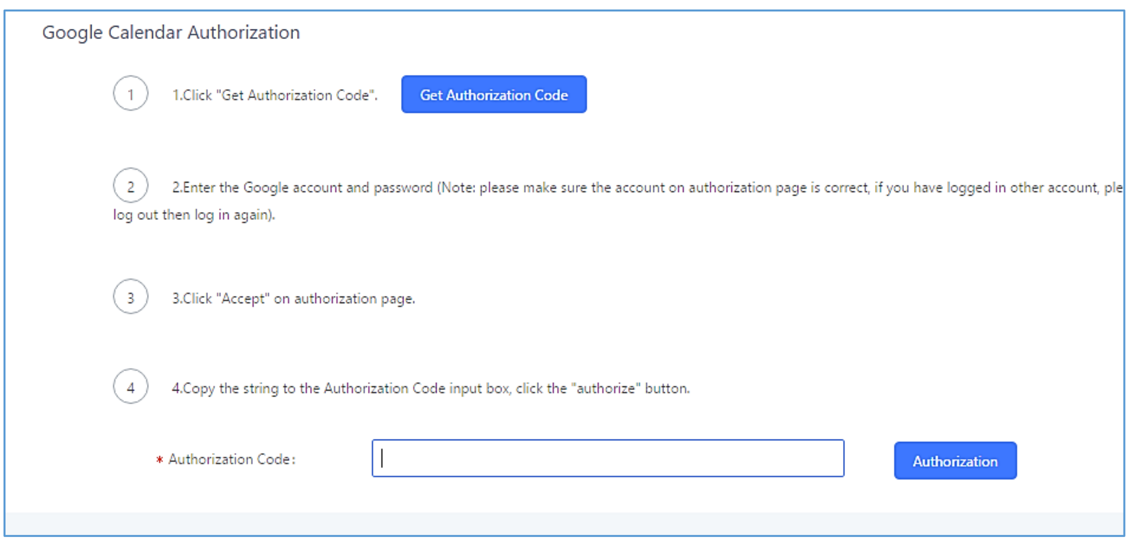


Figure 142: Google Service→OAuth2.0 Login

6. Now UCM630X is connected with Google Service.

You can also configure the Status update, which automatically refresh your Google Calendar with the configured time (m). **Note:** Zero means disable.

Conference Schedule

Conference Schedule can be found under UCM630X Web GUI → **Call Features** → **Audio Conference**→ **Conference Schedule.** Users can create, edit, view, and delete a Conference Schedule.

- Click on "Schedule Meeting" to add a new Conference Schedule.
- Click on the scheduled conference to edit or delete the event.

After the user configures UCM630X with Google Service Settings ***[Google Service Settings Support]*** and enables Google Calendar for Conference Schedule, the conference schedule on the UCM630X can be synchronized with Google Calendar for authorized Google account.

Table 72: Conference Schedule Parameters

Schedule Options	
Conference Subject	Configure the name of the scheduled conference. Letters, digits, Other special characters are also supported. such as #%&@*=
Conference Room	Select a conference room for this scheduled conference.
Password	Configure the conference login password.
Time Zone	Select the conference tome zone.
Host Password	Configure Host Password.
Wait For Moderator	If enabled, conference participants will not hear each other until the host joins the conference. **Note:** If Quiet Mode is enabled, the voice prompt for this option will not be played.
Host	Configure Host.
Schedule Time	Set the beginning date and duration of this scheduled conference. Please be aware to avoid time conflicts in the same conference room.
Meeting Duration	The maximum allowed meeting duration that can be set is 8 hour(s).
Description	The description of scheduled conference.
Repeat	Choose when to repeat a scheduled conference.
Invitees	Local extensions, remote extensions, and special extensions are supported.
Enable Google Calendar	Select this option to sync scheduled conference with Google Calendar. **Note:** Google Service Setting OAuth2.0 must be configured on the UCM630X. Please refer to section ***[Google Service Settings Support]***.
Remote Conference	Invite a remote conference.

Conference Room Options	
Enable Caller Menu	If this option is enabled, conference participants will be able to access conference room menu by pressing the * key.
Record Conference	If this option is enabled, conference call will be recorded in .wav format. The recorded file can be found from **Conference** page.
Quiet Mode	If this option is enabled, the notification tone or voice prompt for joining or leaving the conference will not be played. **Note:** Option "Quiet Mode" and option "Announce Caller" cannot be enabled at the same time.
Allow User Invite	If this option is enabled, the user can: • Press '0' to invite others to join the conference with invited party's permission • Press '1' to invite without invited party's permission • Press '2' to create a multi-conference room to another conference room • Press '3' to drop all current multi-conference rooms. **Note:** Conference Administrator is always allowed to access this menu.
Announce Callers	If this option is enabled, when a participant joins the conference room, participant's name will be announced to all members in the conference room. **Note:** Option "Quiet Mode" and option "Announce Caller" cannot be enabled at the same time.
Play Hold Music	If this option is enabled, UCM630X will play Hold Music while there is only one participant in the conference room, or the conference is not yet started.
Custom Music On Hold	Custom Music On Hold.
Skip Authentication	If this option is enabled, the invitation from Web GUI via a trunk with password will not require authentication. **Note:** Please be aware of the potential security risks when turning on this option.

Once the Conference Schedule is configured, scheduled conference will be displayed as below figure.

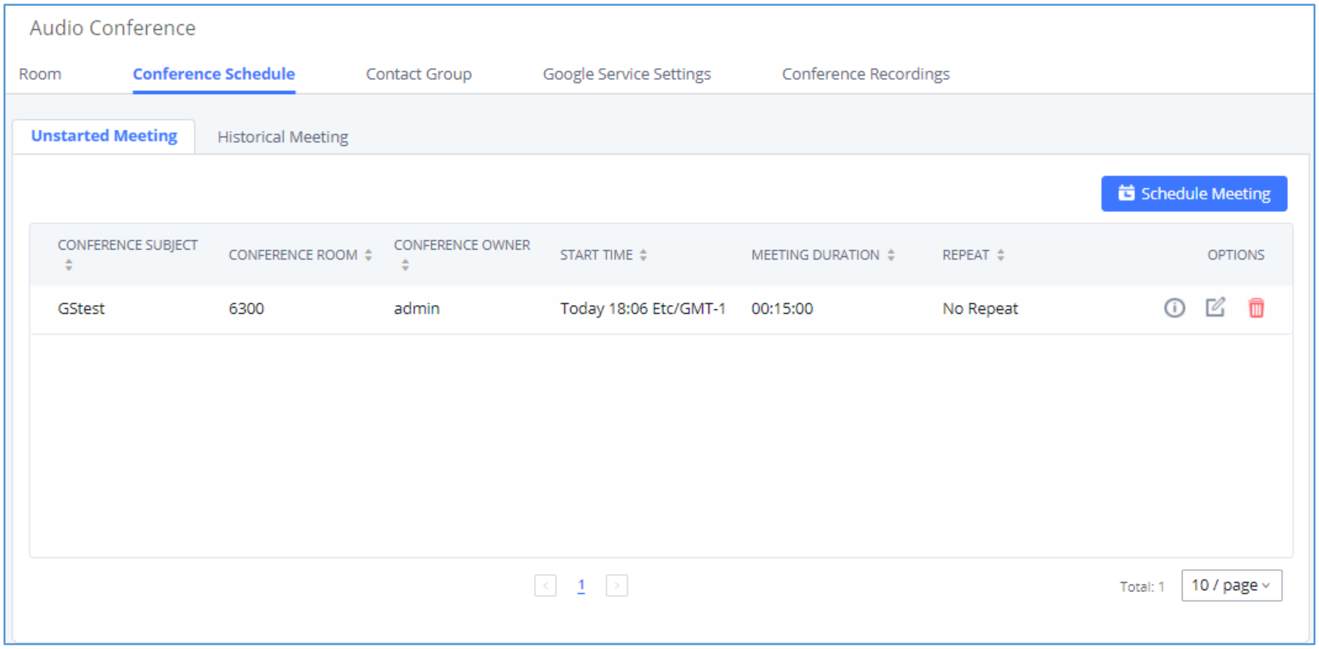


Figure 143: Conference Schedule

Once the conference room is scheduled, at the scheduled conference time, UCM630X will send INVITE to the extensions that have been selected for conference.

Once the conference starts, it will be displayed under **Unstarted Meeting** with an "Ongoing" status, as displayed below.

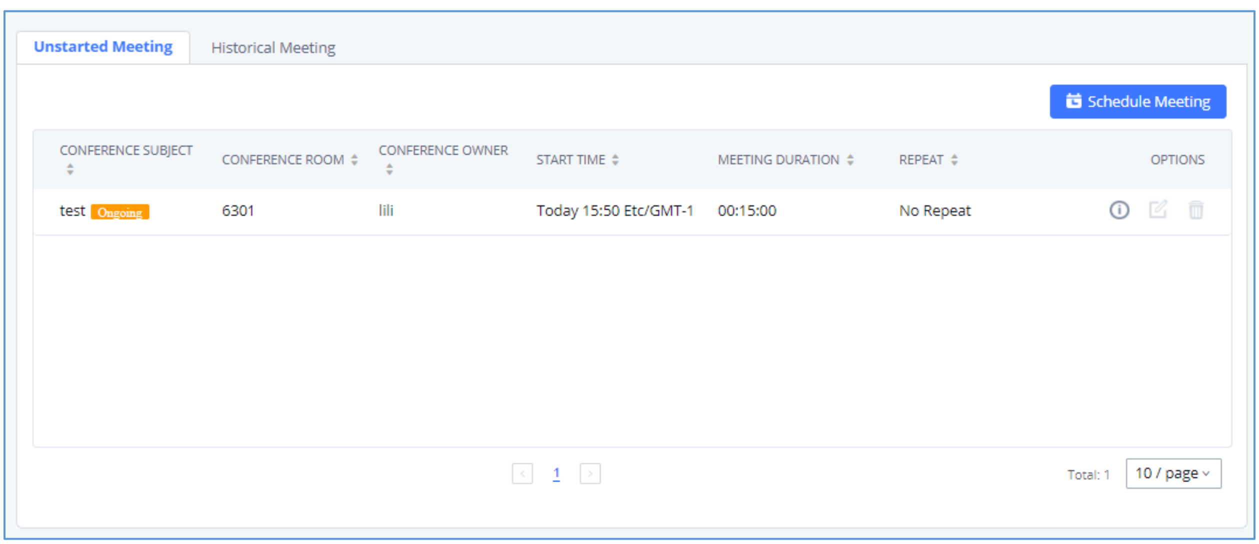


Figure 144: Conference Scheduled-Ongoing

Once the conference is finished, the conference will be displayed under Historical meeting as below:

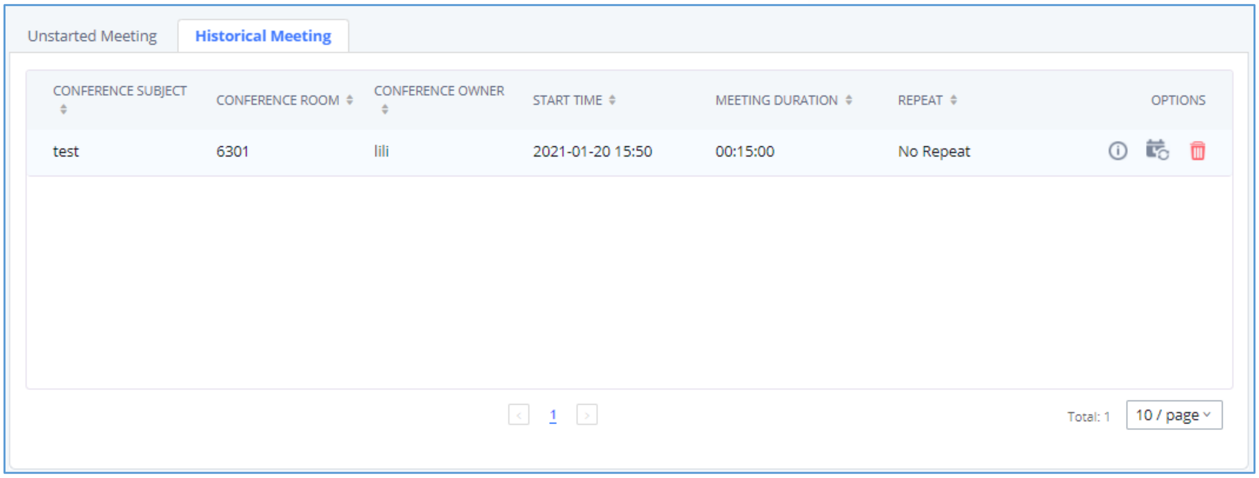


Figure 145: Conference Schedule-Completed

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.

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

Contact Group

The UCM630X allows users to define a group of contacts and attribute it to a conference room. When a designed extension calls the conference room, the UCM will make a call to all the other numbers on the contact groups to join the conference.

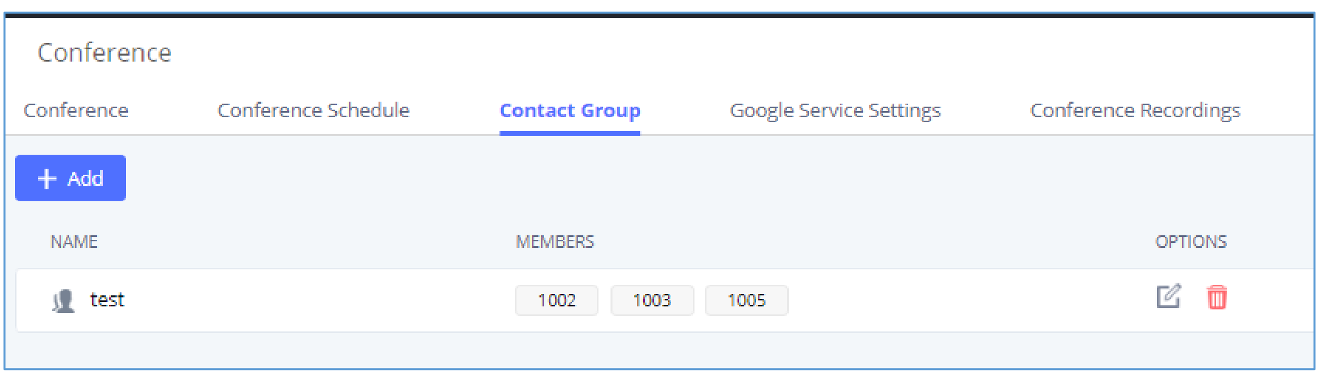


Figure 146: Contact Group

Conference Recordings

The UCM630X allows users to record the conference call and retrieve the recording from Web GUI→**Call Features→ Audio Conference→Conference Recordings**.

To record the conference call, when the conference room is in idle, enable "Record Conference" from the conference room configuration dialog. Save the setting and apply the change. When the conference 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 "Delate All Recording Files" or delete multiple recording files at once by clicking on "Delete" after selecting the recording files.

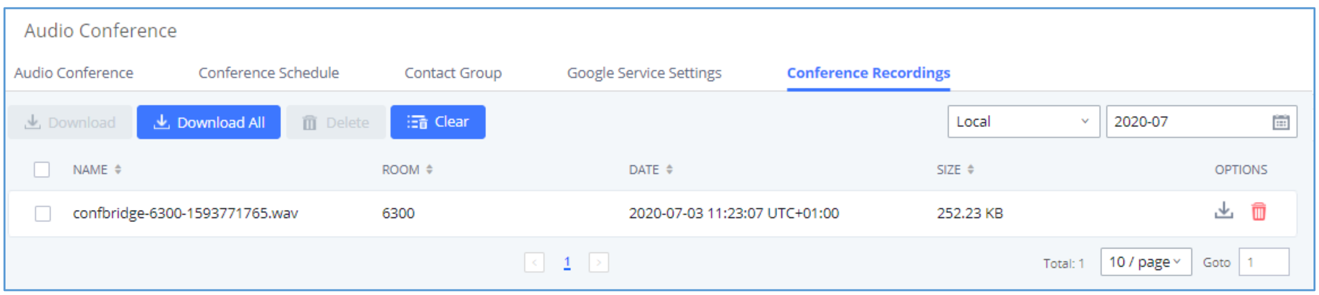


Figure 147: Conference Recordings

Conference Call Statistics

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

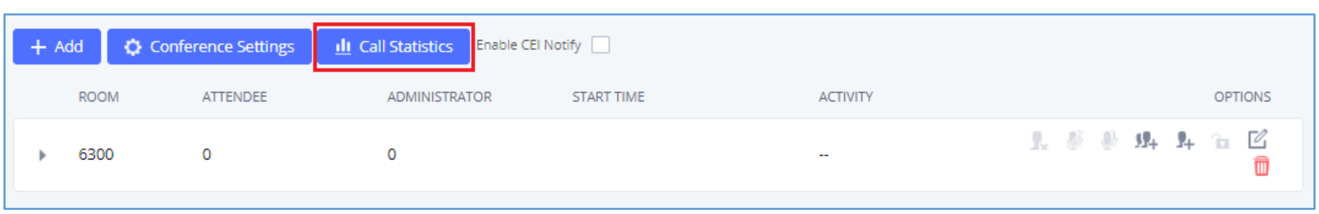


Figure 148: Conference Call Statistics

Figure 149: Conference 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			

Figure 150: Conference Report on CSV

VIDEO CONFERENCE

With the UCM you can easily create, schedule, manage, and join video conference calls, from your desktop or laptop computer. UCM Video conferencing uses WebRTC technology, so all the participants don't have to download and install any additional software or plugins. UCM Video Conferencing must be enabled by the administrator for the concerned extensions. The video conference configurations can be accessed under Web GUI→**Call Features**→**Video Conference**. In this page, users could enable, set the Basic setting, create, edit, view, manage, delete conference rooms, and edit the Conference Schedule.

Below are the UCM video conference specifications supported for each model:

UCM630x series	Number of video conference room	Participant limit
UCM6301	4	20
UCM6302	6	30
UCM6304	8	60
UCM6308	10	80

Video Conference

- Click on "Add" to add a new conference room.
- Click on to edit the conference room.
- Click on to delete the conference room.

Table 73: Video Conference room Configuration Parameters

Extension	Configure the conference number for the users to dial into the conference. **Note:** Up to 64 characters.
Password	When configured, the users who would like to join the conference call must enter this password before accessing the conference room. **Note:** • Only digits are allowed. • The password has to be at least 4 characters. All repetitive and sequential digits (e.g., 0000, 1111, 1234 and 2345) or common digits (e.g., 111222 and 321321) are not allowed.

Host Password	Configure the Host password.
Privilege	Please select the permission level for outgoing calls.
Allow User Invite	If enabled, participants can invite other users to the video conference.

Conference Settings contains the following options:

Table 74: Conference Settings

Enable Talk detection	If enabled, the AMI will send the corresponding event when a user starts or ends talking.
DSP Talking Threshold	The time in milliseconds of sound above what the dsp has established as base line silence for a user before a user is considered to be talking. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 200.
DSP Silence Threshold	The time in milliseconds of sound falling within the dsp has established as base line silence before a user is considered to be silent. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 2500.
Max Number of Video Feeds	Set the maximum number of video feeds supported per conference room.
Audio Codec Preference	Configures the preferred codecs for temporary accounts such as conference participants who joined via link.
Packet Loss Retransmission	Packet Loss Retransmission configuration for temporary accounts (conference participants without registered extensions who entered the conference via link)
Jitter Buffer	Select jitter buffer method for temporary accounts such as conference participants who joined via link. **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 that will not exceed the value of "Max Jitter Buffer"). **NetEQ:** Dynamic jitter buffer via NetEQ.

Conference Schedule

Conference Schedule can be found under UCM **Web GUI → Call Features→Video Conference → Conference Schedule.** Users can create, edit, view, and delete a Conference Schedule.

- Click on "Add" to add a new Conference Schedule.
- Click on the scheduled conference to edit or delete the event.

Table 75: Video Conference Schedule Parameters

Schedule Options	
Conference Subject	Configure the name of the scheduled conference. Letters, digits, _ and - are allowed.
Conference Room	Select a conference room for this scheduled conference.
Password	Configure Conference login password.
Time	Set the beginning date and duration of this scheduled conference. Please be aware to avoid time conflicts in the same conference room.
Time Zone	Configure the time zone
Host	Configure the conference's host
Host password	Configure the conference's host password
Repeat	Choose when to repeat a scheduled conference.
Email Reminder (m)	Email reminders will be sent out x minutes prior to the start of the conference. Valid range is 5-1440. 60 is the default value. 0 indicates not to send out email reminders for the conference.
Allow User Invite	If enabled, participants can invite other users to the video conference.
Call Participants	If enabled, invited participants will be called when the meeting starts.
Invitees	Select the participants to invite to the conference. Enter either extension numbers or email addresses.
Description	Set a description of scheduled conference.

Once created, at the scheduled conference time, UCM630X will send INVITE to the extensions that have been selected for conference.

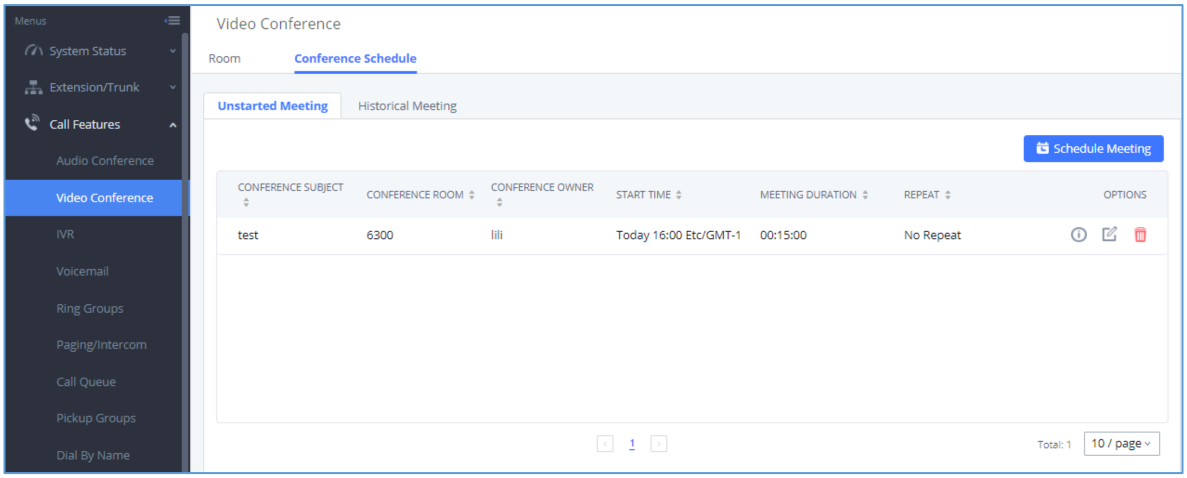


Figure 151: Video Conference Schedule

Once the conference starts, it will be displayed under **Unstarted Meeting** with an "Ongoing" status, as displayed below.

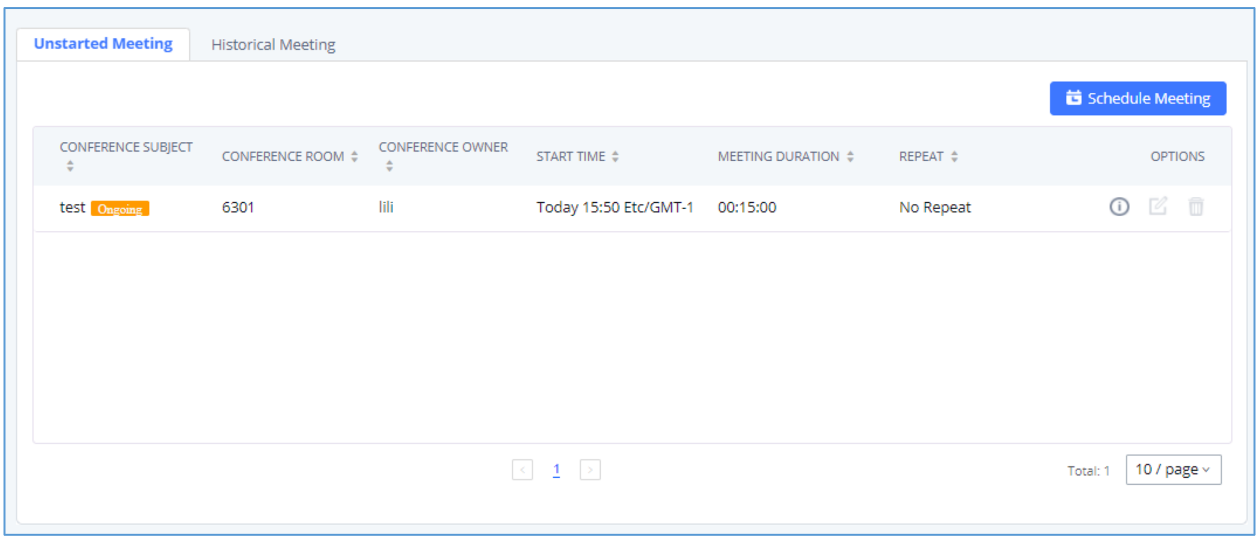


Figure 152: Video Conference Scheduled-Ongoing

Once the conference is finished, the conference will be displayed under Historical meeting as below:

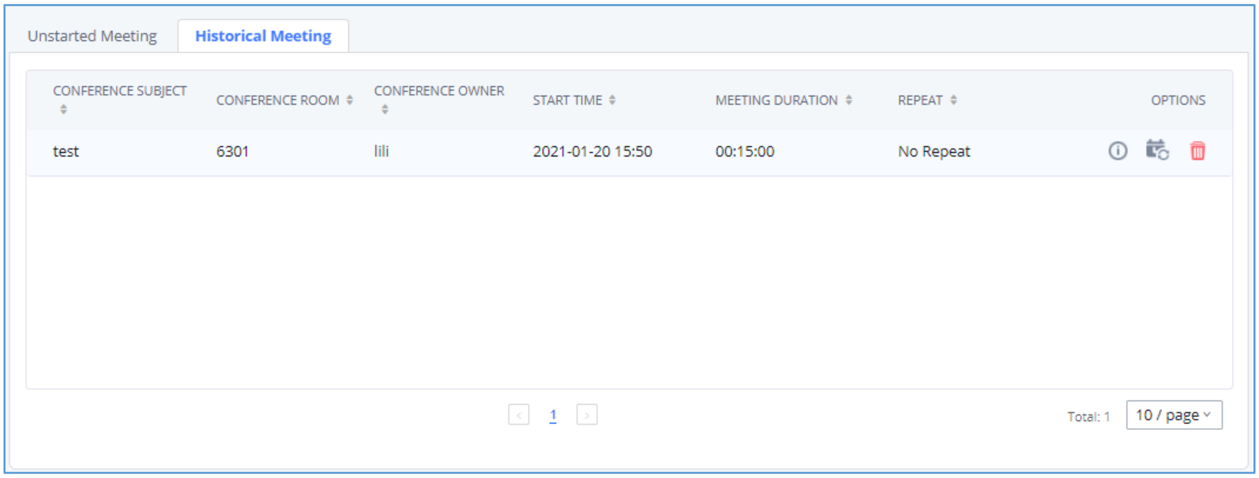


Figure 153: Video Conference Scheduled-Completed

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

Notes:

- Video conferencing can be resource-intensive and may cause performance issues with the UCM when used.
- To ensure the best experience, please use Google Chrome (v67 or higher) or Mozilla Firefox (v60).

Wave WebRTC Video Calling & Conferencing

Web audio and video calls and conferencing can now be achieved through the UCM's new WebRTC page. To get started with this new feature, please make sure to:

1. Navigate to **Value-Added Features → WebRTC** and enable WebRTC support.

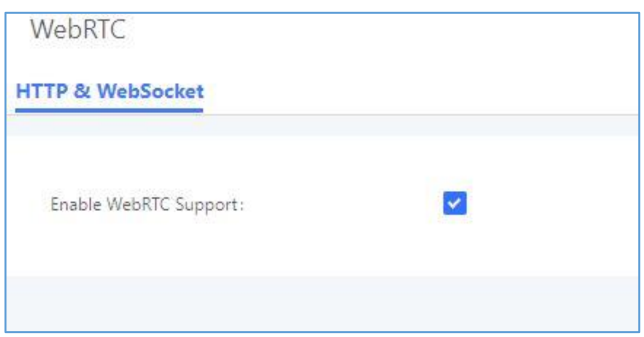


Figure 154: Enabling WebRTC Feature

2. Enable the WebRTC on the extensions that would use this feature under **Extension / Trunk → Extensions** by editing the concerned extensions.

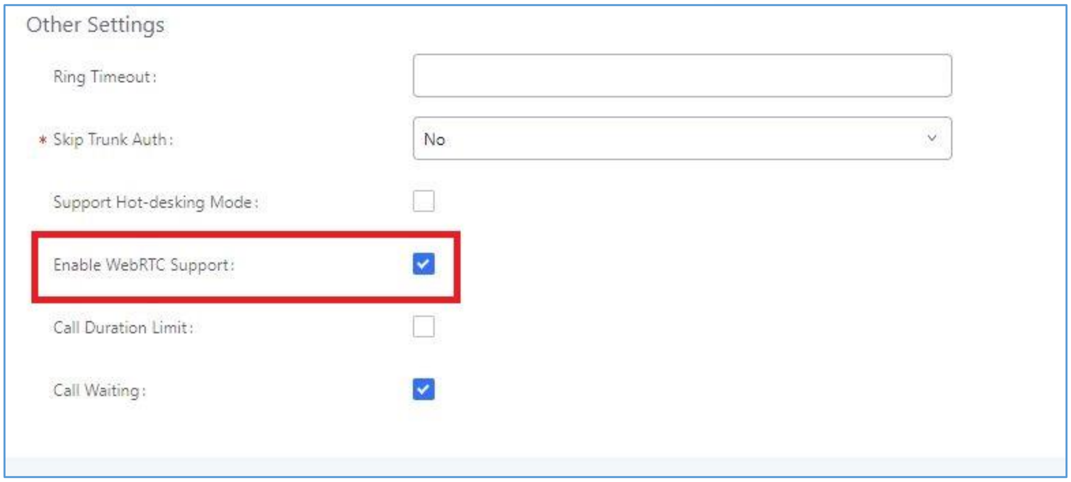


Figure 155: Enabling WebRTC on Extensions

The UCM offers the possibility to login to an extension via Grandstream Wave Portal using user portal password in addition to SIP registration password, where it offers a sleek interface to host conferences, receive email reminders for scheduled conferences, manage contacts, initiate calls, call transfer, chat functionality and more. Access the page by entering the UCM's server address and port which is 8090.
(e.g. https://my.ucm.com:8090).

Figure 156: Grandstream Wave Interface

For more details about the Wave Web, please refer to the following guides:
http://www.grandstream.com/sites/default/files/Resources/GS_Wave_Web_administration_guide.pdf
http://www.grandstream.com/sites/default/files/Resources/GS_Wave_Web_user_guide.pdf

Grandstream Wave is also available in Androind/IOS version where it can be downloaded from Google Play or AppStorre. For more details, please refer to the following guide:
http://www.grandstream.com/sites/default/files/Resources/GSWave_mobile_app_User_Guide.pdf

Desktop version is also supported in Windows and MacOS and can be downloaded from:
https://fw.gdms.cloud/wave/download/

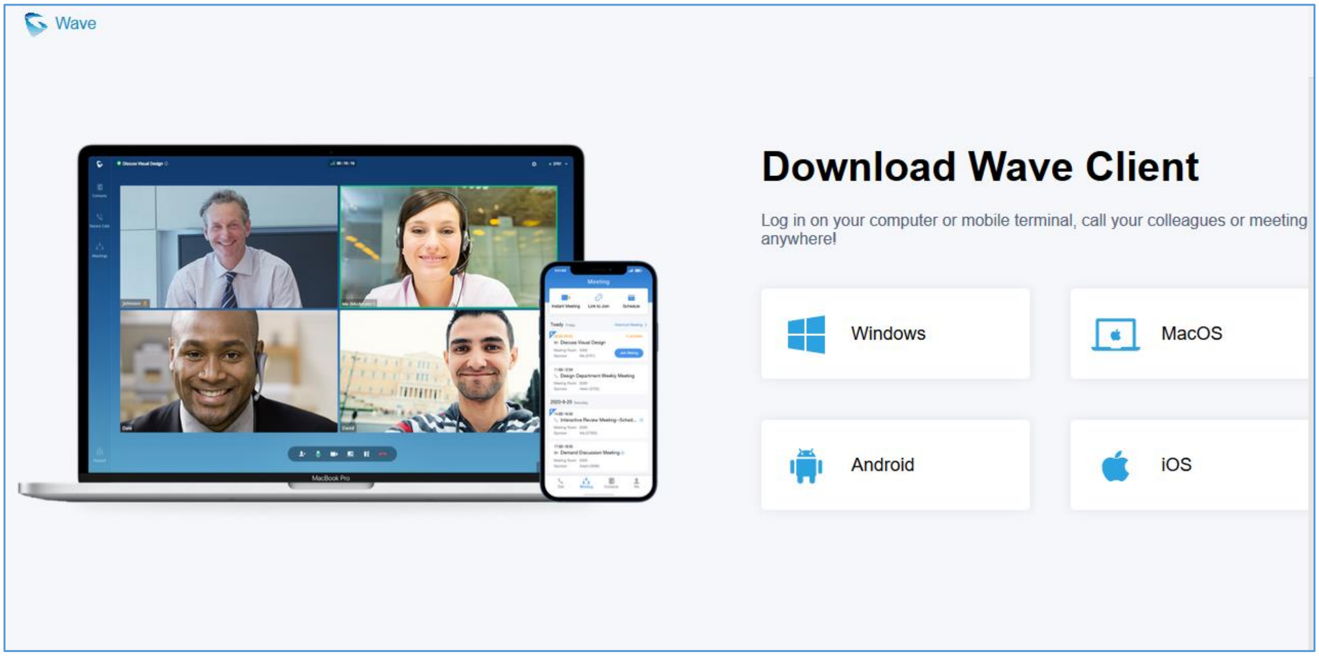


Figure 157: Download Wave Client

IVR

Configure IVR

IVR configurations can be accessed under the UCM630X Web GUI→**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.

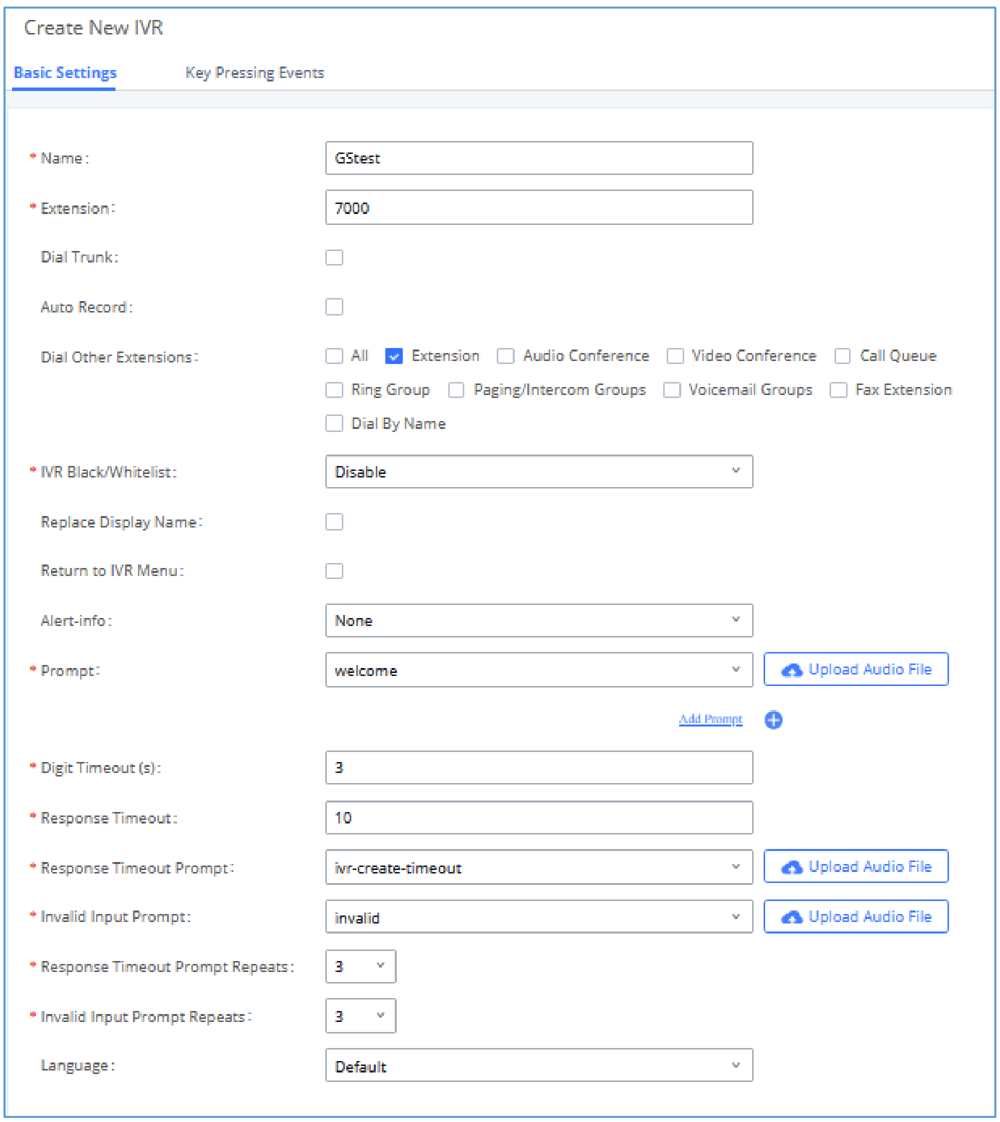


Figure 158: Create New IVR

Table 76: IVR Configuration Parameters

Basic Settings	
Name	Configure the name of the IVR. Letters, digits, _ and - are allowed.
Extension	Enter the extension number for users to access the IVR.
Dial Trunk	If enabled, all callers to the IVR can use trunk. The permission must be configured for the users to use the trunk first. The default setting is "No".
Auto Record	If enabled, calls to this IVR will automatically be recorded.
Permission	Assign permission level for outbound calls if "Dial Trunk" is enabled. 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 IVR, the UCM630X will compared the IVR's permission level with the outbound route's privilege level. If the IVR's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Dial Other Extensions	This controls the destination that can be reached by the external caller via the inbound route. The available destinations are: • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Groups • Voicemail Groups • Dial by Name • All
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.

Prompt	Select an audio file to play as the welcome prompt for the IVR. Click on "Prompt" to add additional audio file under Web GUI→**PBX Settings**→**Voice Prompt**→**Custom Prompt**.
Digit Timeout	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	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.
Invalid Input Prompt	Select the prompt message to be played when an invalid extension is pressed.
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 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.
Language	Select the voice prompt language to be used for this IVR. 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 current available voice prompt languages on the UCM630X. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under Web GUI→**PBX Settings**→**Voice Prompt**→**Language Settings**.
Key Pressing Events	
Key Press Event: **Press 0** **Press 1** **Press 2** **Press 3** **Press 4** **Press 5** **Press 6** **Press 7** **Press 8** **Press 9**	Select the event for each key pressing for 0-9, *, Timeout and Invalid. The event options are: • Extension • Voicemail • Conference Rooms • Voicemail Group • IVR • Ring Group • Queues • Page Group • Custom Prompt

Press *	• Hangup • DISA • Dial by Name • External Number • Callback
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.

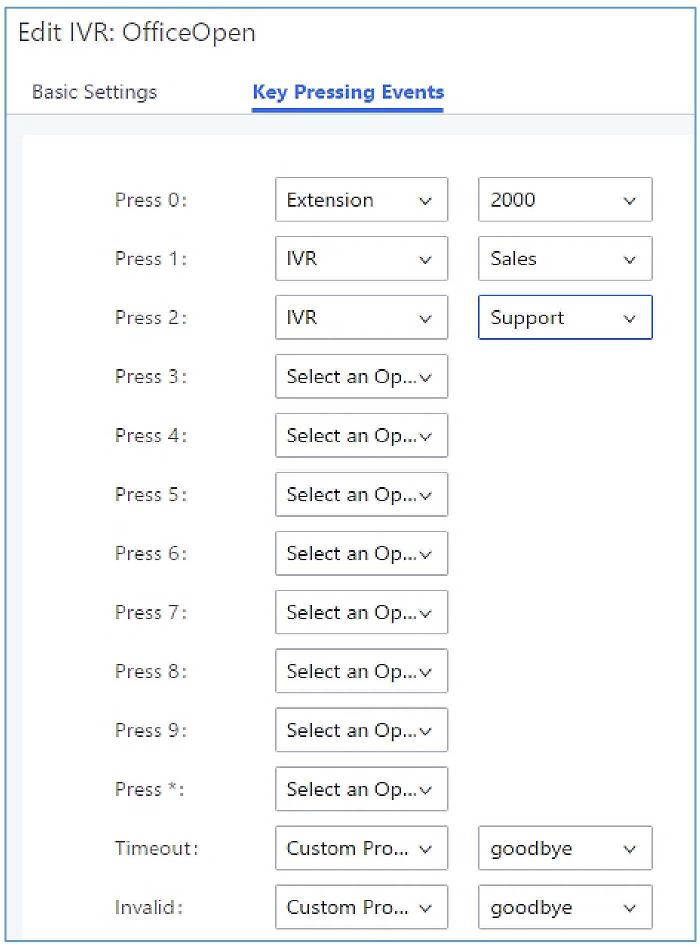


Figure 159: Key Pressing Events

Black/White List 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.

Note: up to 500 extensions are allowed on the back/whitelist.

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

- If the user selects “Blacklist 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 “Whitelist Enable” and adds extension in the list, only the extensions in the list can be allowed to be reached via IVR.

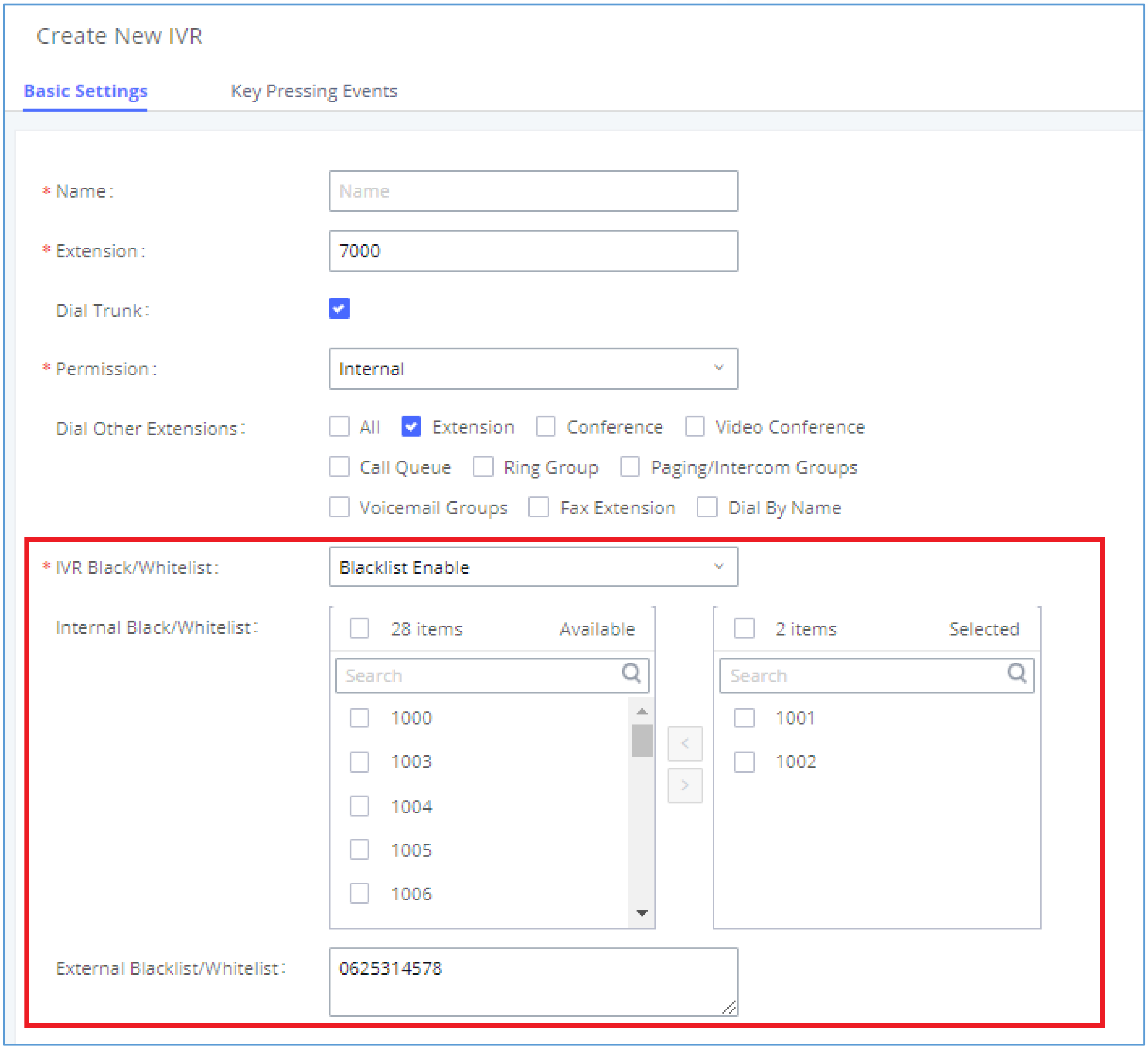


Figure 160: Black/Whitelist

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.

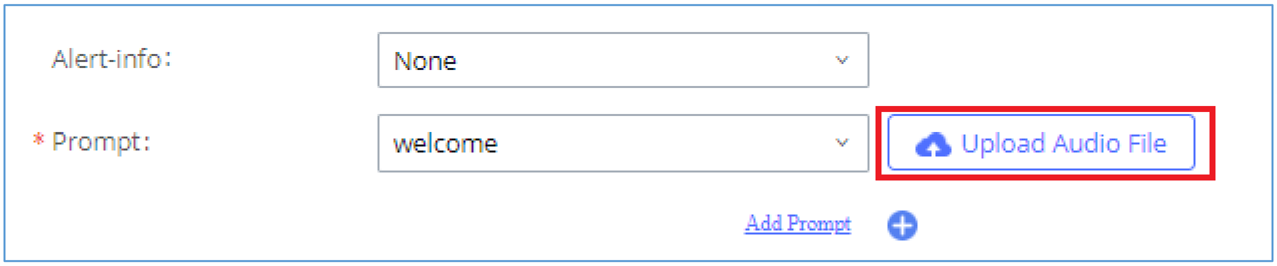


Figure 161: Click on Prompt to Create IVR Prompt

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.

LANGUAGE SETTINGS FOR 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: ***English (United States), Arabic, Chinese, Dutch, English (United Kingdom), French, German, Greek, Hebrew, Italian, Polish, Portuguese, Russian, Spanish, Catalan, Swedish and Turkish.***

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 Web GUI→**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.

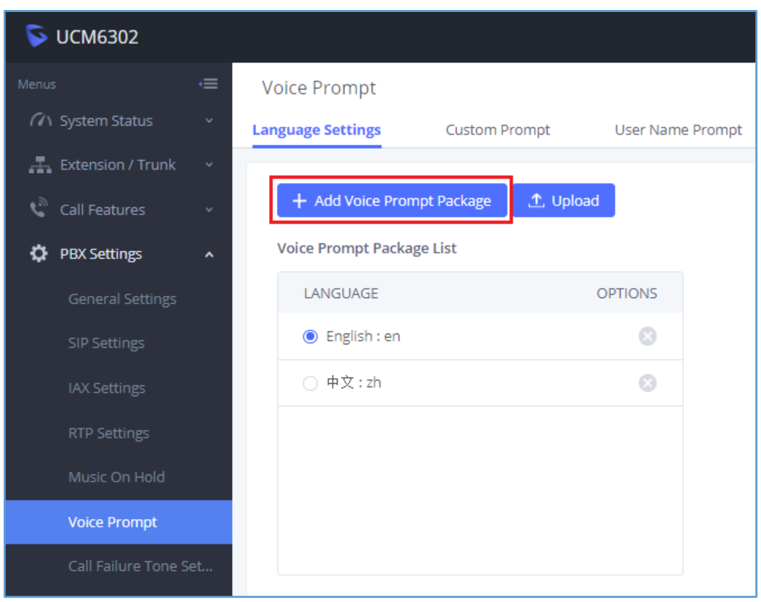


Figure 162: Language Settings for Voice Prompt

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.

Figure 163: Voice Prompt Package List

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

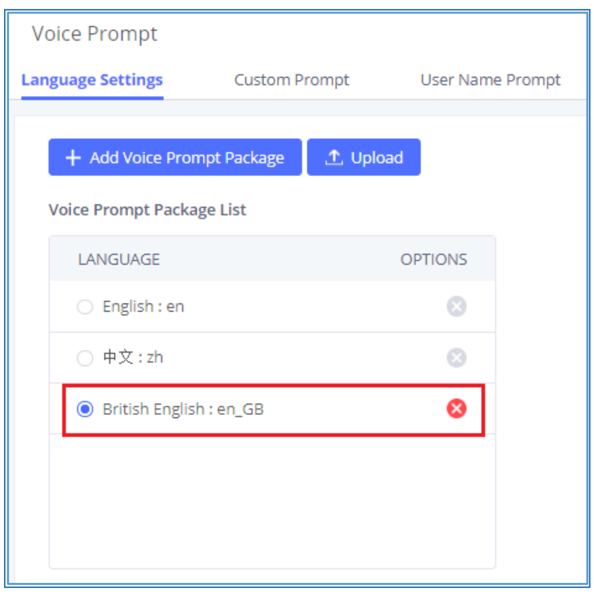


Figure 164: New Voice Prompt Language Added

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.

Customize Specific Prompt

On the UCM630X, if the user needs to replace some specific customized prompt, the user can upload a single specific customized prompt from Web GUI→**PBX Settings**→**Voice Prompt**→**Language Settings** and click on **"Upload"** instead of the entire language pack.

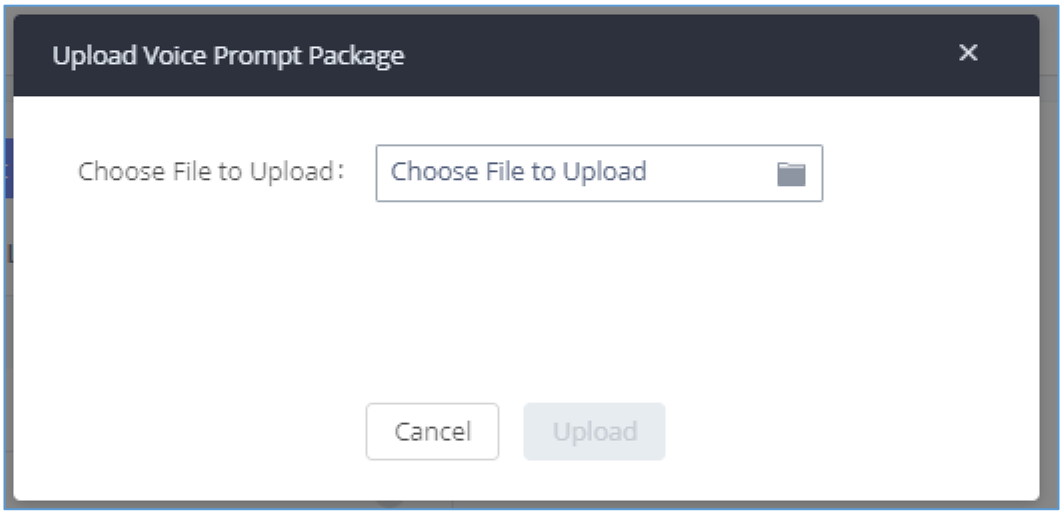


Figure 165: Upload Single Voice Prompt for Entire Language Pack

Username Prompt Customization

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.

VOICEMAIL

Configure Voicemail

If the voicemail is enabled for UCM630X extensions, the configurations of the voicemail can be globally set up and managed under Web GUI→**Call Features**→**Voicemail**.

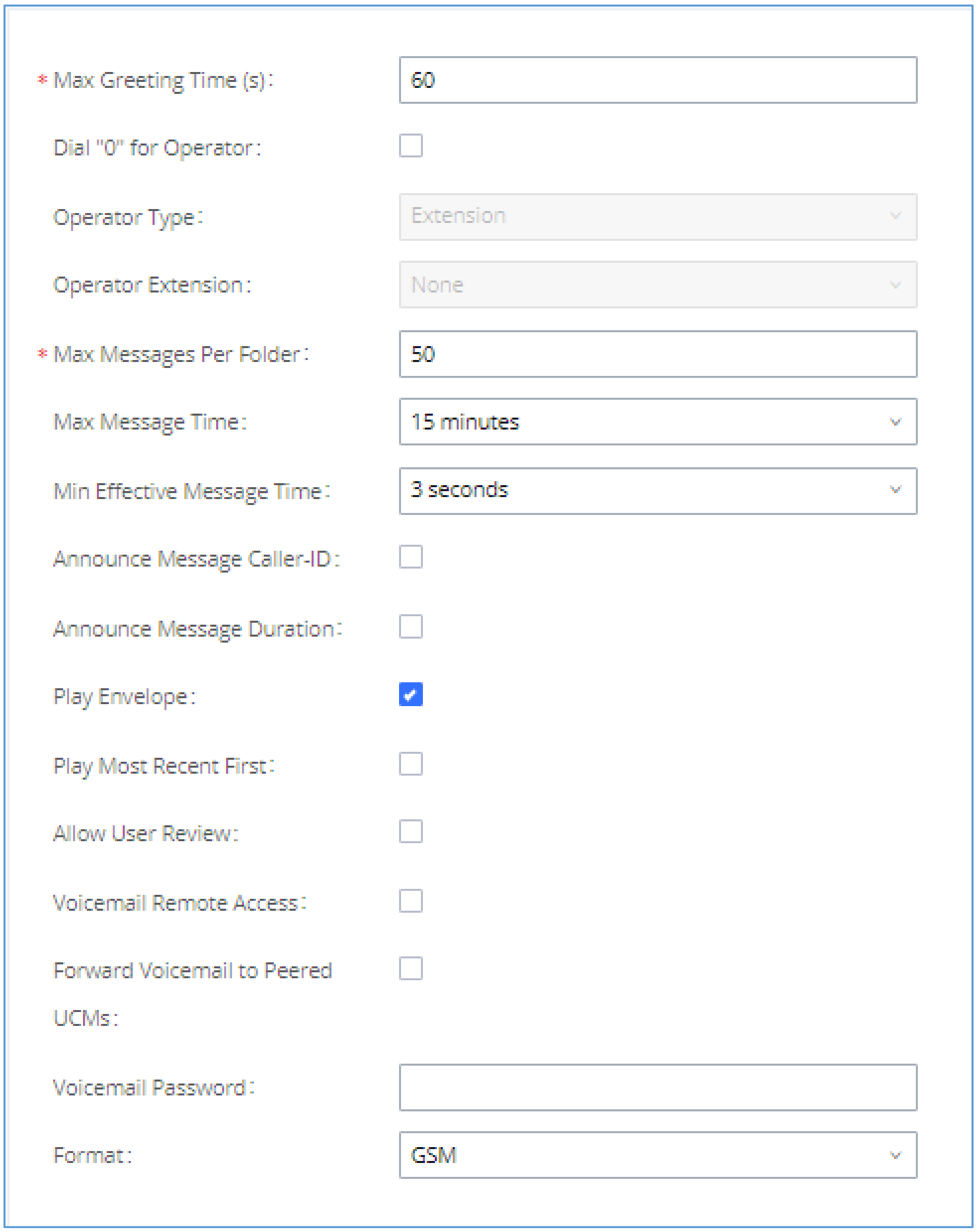


Figure 166: Voicemail Settings

Table 77: Voicemail Settings

Max Greeting Time (s)	Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds.
Dial '0' For Operator	If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator's extension.
Operator Type	Configure the operator type; either an extension or a ring group.
Operator Extension	Select the operator extension, which will be dialed when users press 0 to exit voicemail application. The operator extension can also be used in IVR.
Max Messages Per Folder	Configure the maximum number of messages per folder in users' voicemail. The valid range 10 to 1000. The default setting is 50.
Max Message Time	Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the max message time. The default setting is 15 minutes. The available options are: • 1 minute • 2 minutes • 5 minutes • 15 minutes • 30 minutes • Unlimited
Min Effective Message Time	Configure the minimum duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Message Time. The default setting is 3 seconds. The available options are: • No minimum • 1 second • 2 seconds • 3 seconds • 4 seconds • 5 seconds **Note:** Silence and noise duration are not counted in message time.
Announce Message Caller-ID	If enabled, the caller ID of the user who has left the message will be announced at the beginning of the voicemail message. The default setting is "No".
Announce Message Duration	If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is "No".
Play Envelope	If enabled, a brief introduction (received time, received from, and etc.) of each message will be played when accessed from the voicemail application. The default setting is "Yes".
Play Most Recent First	If enabled, it will play the most recent message first.

Allow User Review	If enabled, users can review the message following the IVR before sending.
Voicemail Remote Access	If enabled, external callers routed by DID and reaching VM will be prompted by the UCM with 2 options: • ***Press 1 to leave a message.*** To leave a message for the extension reached by DID. • **Press 2 to access voicemail management system.** This will allow caller to access any extension VM after entering extension number and its VM password. **Note:** This option applies to inbound call routed by DID only. The default setting is "Disabled".
Forward Voicemail to Peered UCMs	Enables the forwarding of voicemail to remote extensions on peered SIP trunks. The default setting is "Disabled".
Voicemail Password	Configures the default voicemail password that will be used when an extension is reset.
Format	Warning: WAV files take up significantly more storage space than GSM files.

Note: Resetting an extension will reset Voicemail Password, Send Voicemail to Email, and Keep Voicemail after Emailing values to default. Previous custom voicemail prompts and messages will be deleted.

Access Voicemail

If the voicemail is enabled for UCM630X extensions, the users can dial the voicemail access number (by default *97) to access their extension's voicemail. The users will be prompted to enter the voicemail password and then can enter digits from the phone keypad to navigate in the IVR menu for different options.

Otherwise the user can dial the voicemail access code (by default *98) followed by the extension number and password in order to access to that specific extension's voicemail.

Table 78: Voicemail IVR Menu

Main Menu	Sub Menu 1	Sub Menu 2
1 – New messages	3 - Advanced options	1 - Send a reply
		2 - Call the person who sent this message
		3 - Hear the message envelop
		4 - Leave a message
		* - Return to the main menu
	5 - Repeat the current message	

	7 - Delete this message	
	8 - Forward the message to another user	
	9 – Save	
	* - Help	
	# - Exit	
2 – Change folders	0 - New messages	
	1 - Old messages	
	2 - Work messages	
	3 - Family messages	
	4 - Friend messages	
	# - Cancel	
3 – Advanced options	1 - Send a reply	
	2 - Call the person who sent this message	
	3 - Hear the message envelop	
	4 - Leave a message	
	* - Return to the main menu	
0 – Mailbox options	1 - Record your unavailable message	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	2 - Record your busy message	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	3 - Record your name	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	4 - Record temporary greeting	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	5 - Change your password	
	* - Return to the main 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.

Table 79: Voicemail Email Settings

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

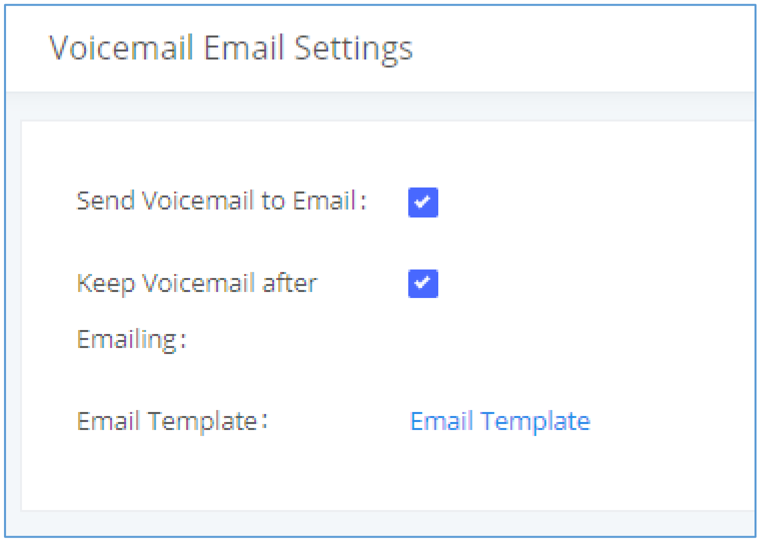


Figure 167: Voicemail Email Settings

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 Web GUI → **Call Features** → **Voicemail** → **Voicemail Group**. Click on "Add" to configure the group.

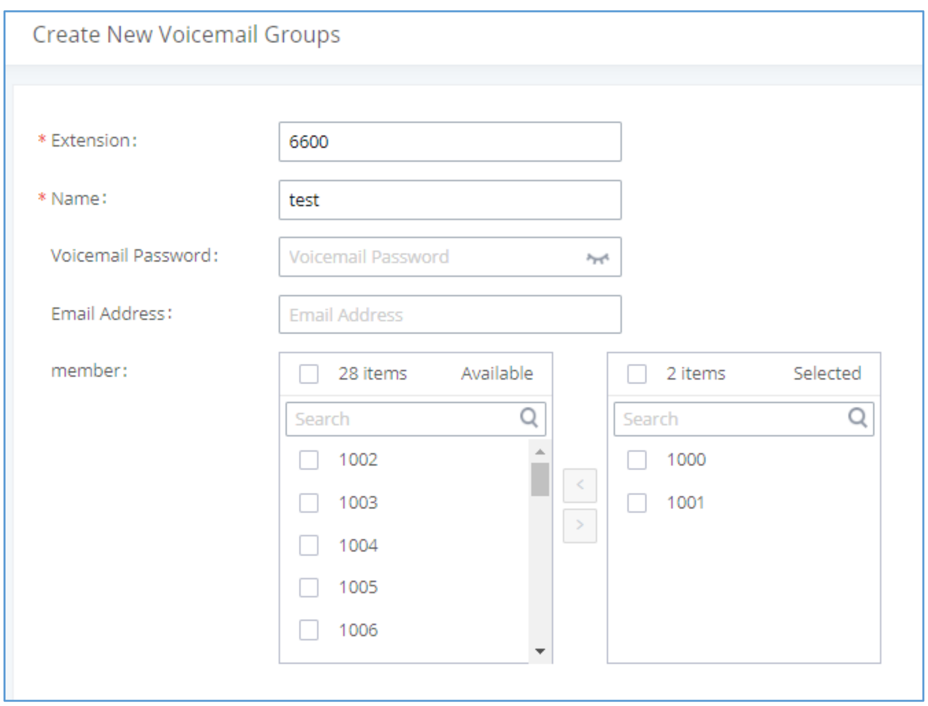


Figure 168: Voicemail Group

Table 80: Voicemail Group Settings

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.
Voicemail Password	Configure the voicemail password for the users to check voicemail messages.
Email Address	Configure the Email address for the voicemail group extension.
Member	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.

RING GROUP

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 Web GUI→**Call Features**→**Ring Group**.

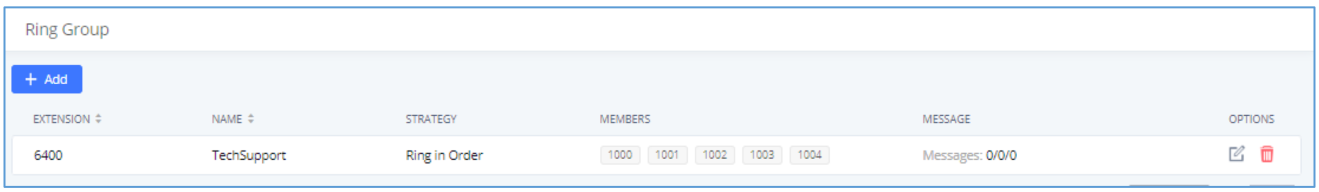


Figure 169: Ring Group

- Click on + Add 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.

Table 81: Ring Group Parameters

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 Web GUI→**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.

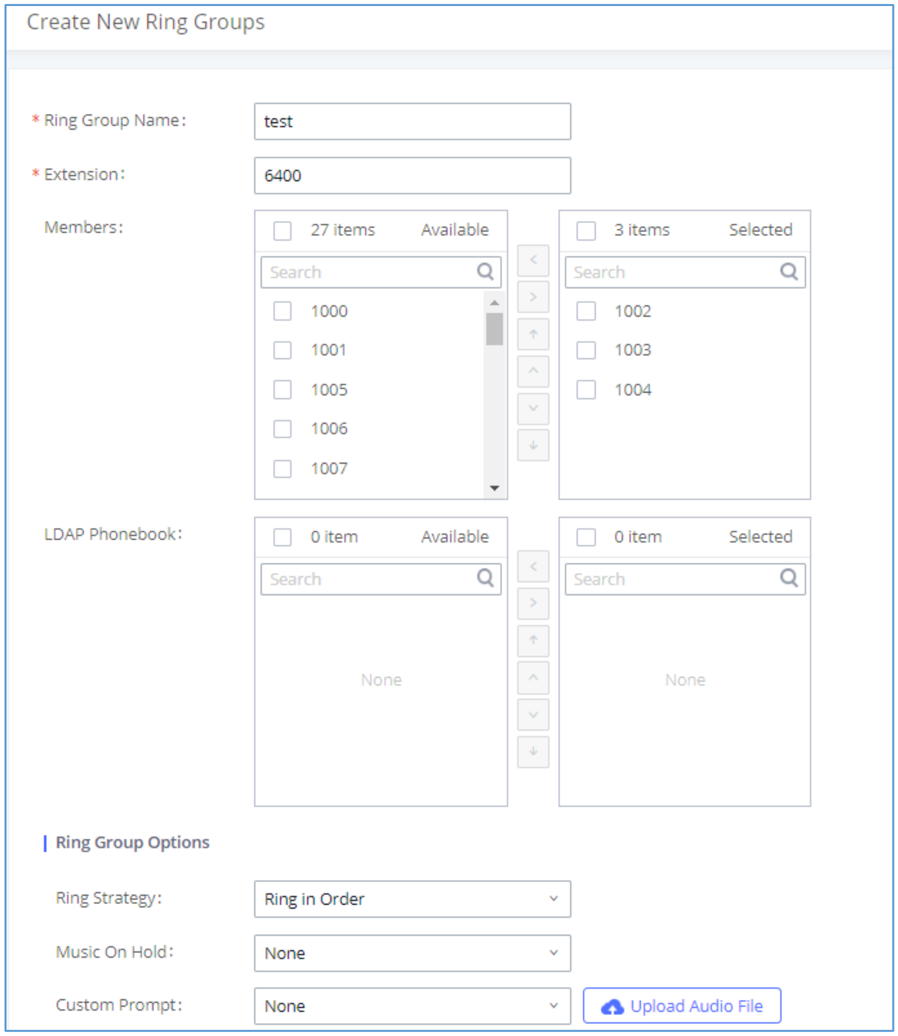


Figure 170: Ring Group Configuration

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**.**

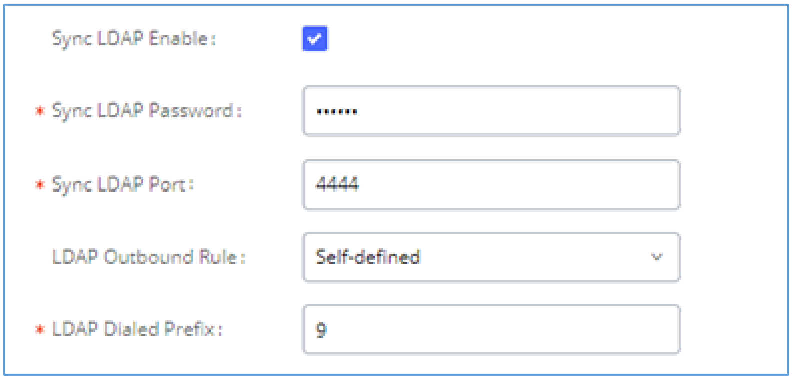


Figure 171: Sync LDAP Server option

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.

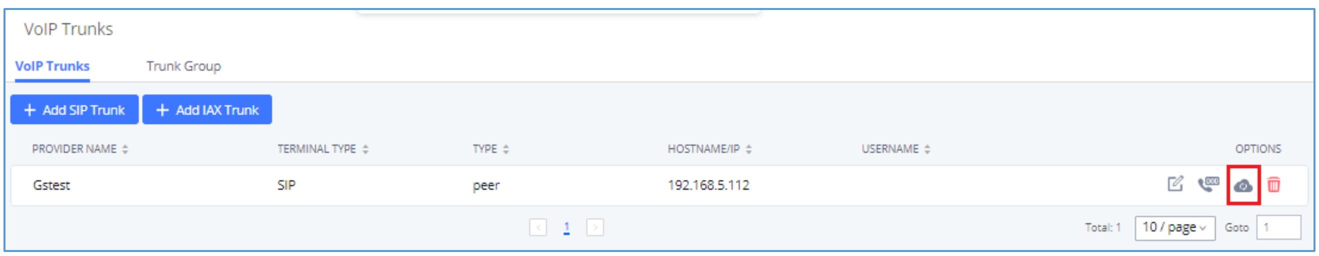


Figure 172: Manually Sync LDAP Server

4. Under **Ring Groups** setting page, click "Add". **Ring Groups** can be found under Web GUI→**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.

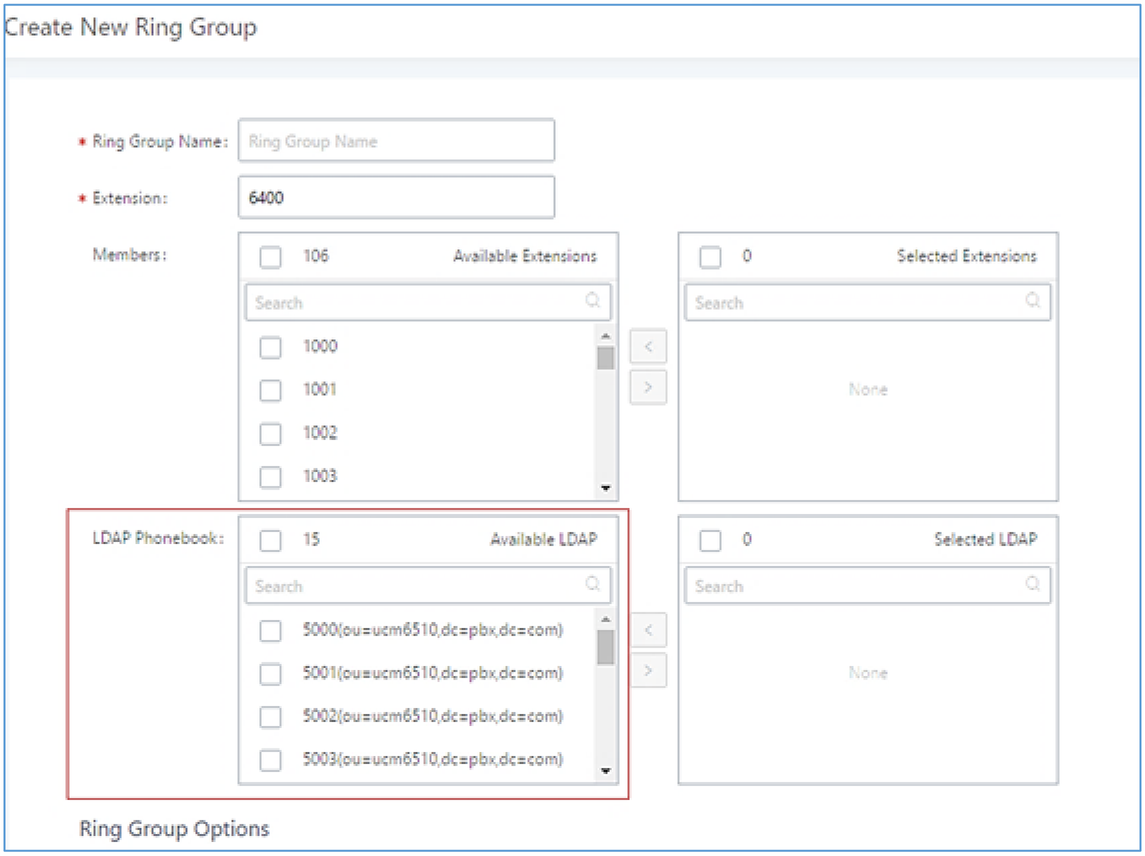


Figure 173: Ring Group Remote Extension

PAGING AND INTERCOM GROUP

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→**Call Features**→**Paging/Intercom**.

Configure Paging/Intercom Group

- Click on "Add" to add paging/intercom group.
- Click on to edit the paging/intercom group.
- Click on to delete the paging/intercom group.
- Click on "Paging/Intercom Group Settings" to edit Alert-Info Header. This header will be included in the SIP INVITE message sent to the callee in paging/intercom call.

Configure Multicast Paging

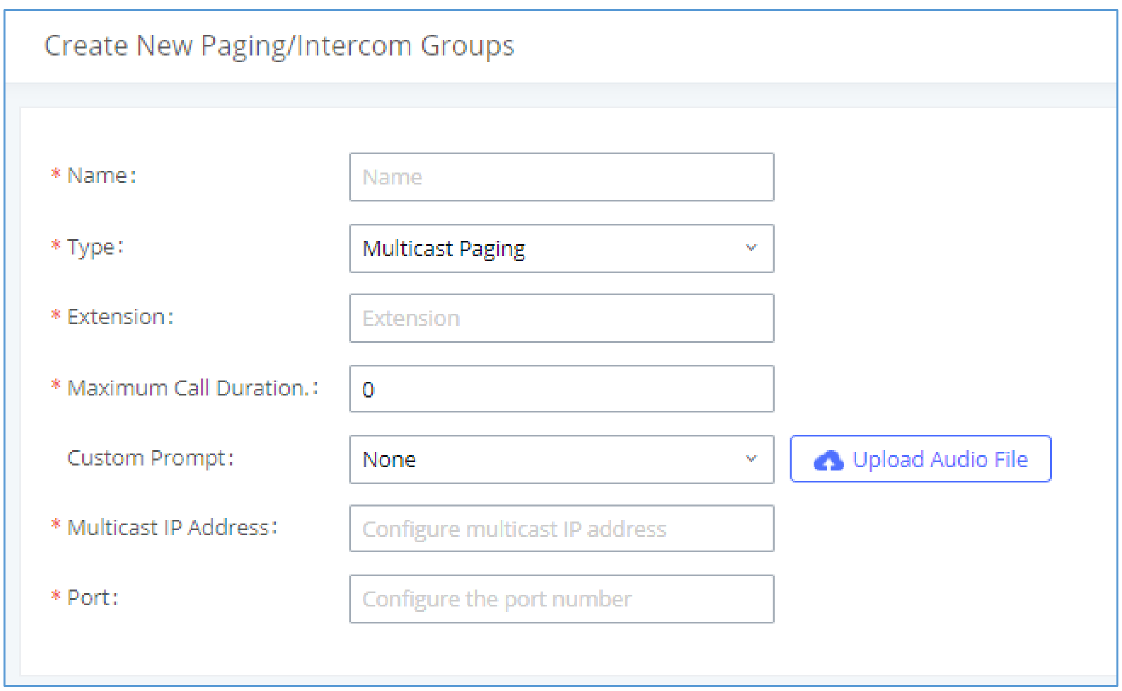


Figure 174: Multicast Paging

Table 82: Multicast Paging Configuration Parameters

Name	Configure paging/intercom group name.
Type	Select "Multicast Paging".
Extension	Configure the paging/intercom group extension.
Multicast IP Address	The allowed multicast IP address range is 224.0.1.0 - 238.255.255.255. **Note:** This field appears only when "Type" is set to "Multicast Paging".
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
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.
Multicast IP Address	Select which extensions are allowed to use the paging/intercom feature for this paging group.
Port	Specify port for multicast paging. **Note:** This field appears only when "Type" is set to "Multicast Paging".

Configure 2-way Intercom

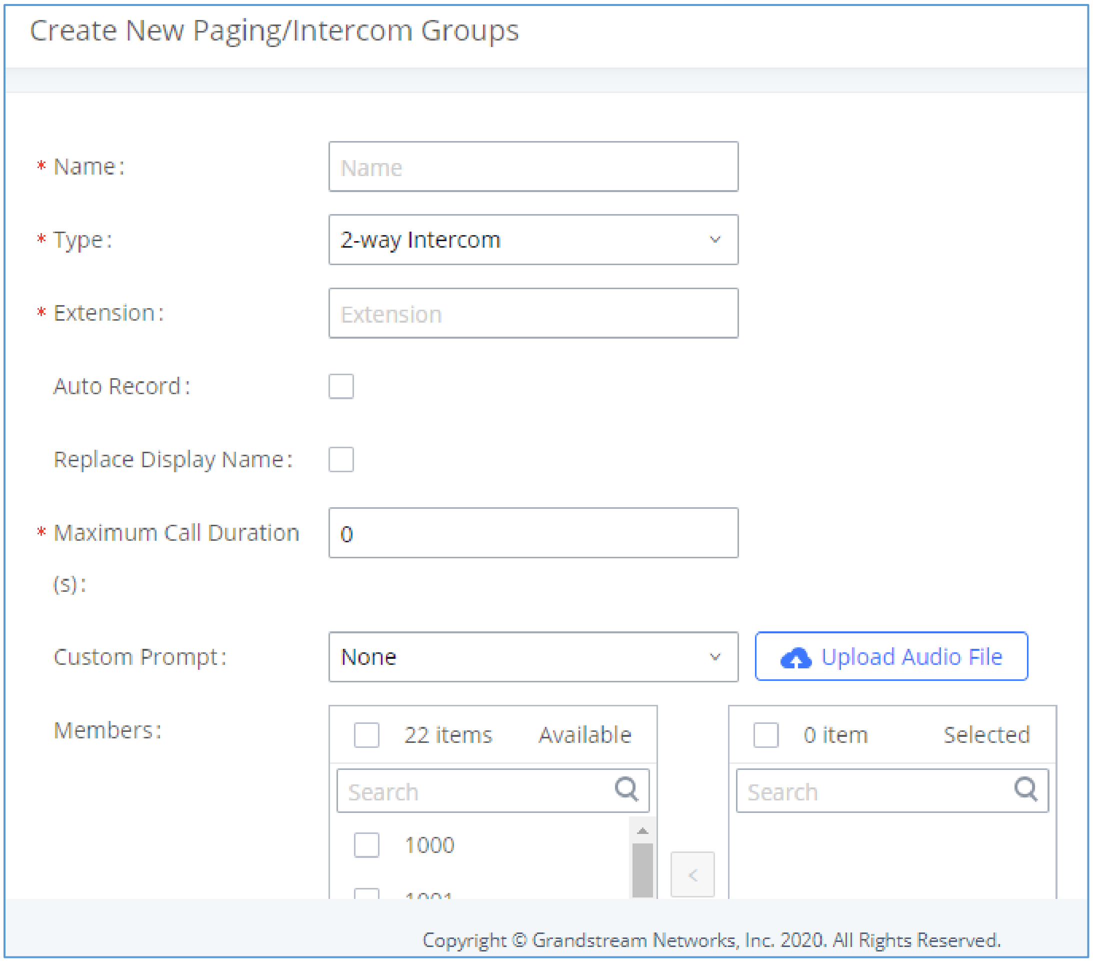


Figure 175: 2-way Intercom

Table 83: 2-way Intercom Configuration Parameters

Name	Configure paging/intercom group name.
Type	Select "2-way Intercom".
Extension	Configure the paging/intercom group extension.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the UCM will replace the caller display name with Paging/Intercom name.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.

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.
Members	Select available users from the left side to the paging/intercom group member list on the right.
Paging/Intercom Whitelist	Select which extensions are allowed to use the paging/intercom feature for this paging group.

Configure 1-way Paging

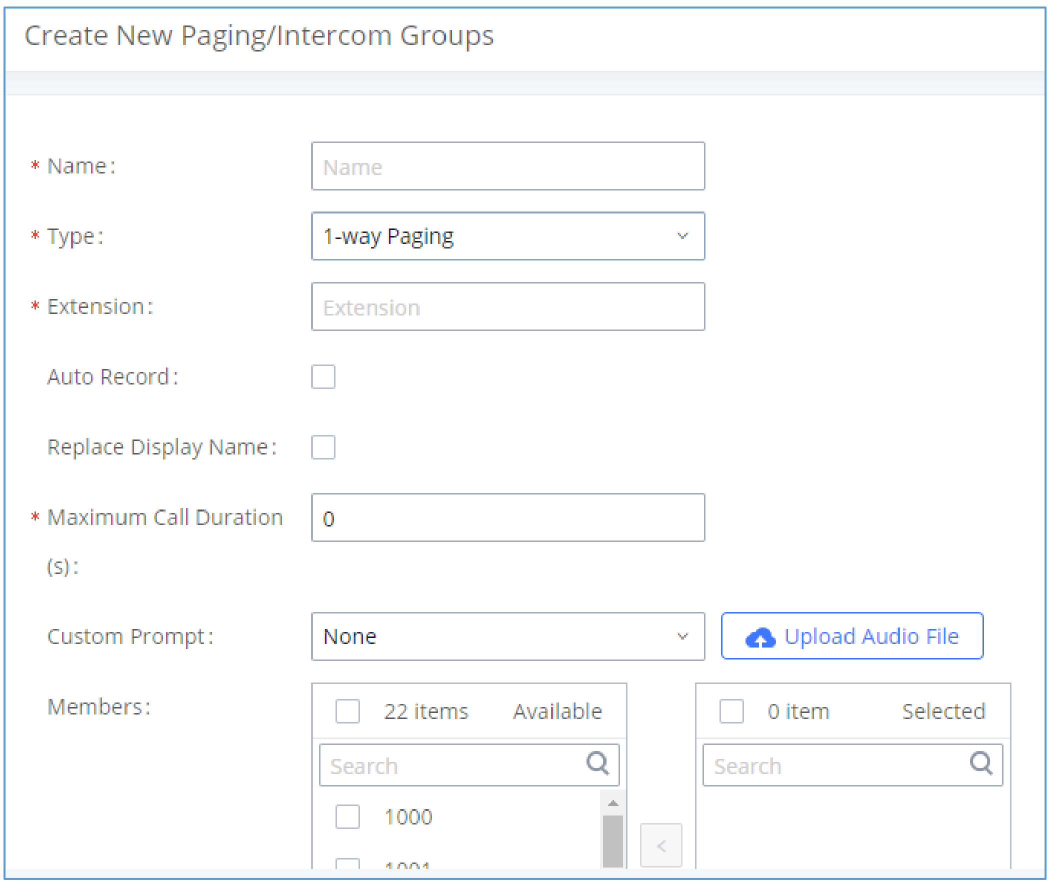


Figure 176: 1-way Paging

Table 84: 1-way Paging Configuration Parameters

Name	Configure paging/intercom group name.
Type	Select "1-way Paging".
Extension	Configure the paging/intercom group extension.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the UCM will replace the caller display name with Paging/Intercom name.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
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.
Members	Select available users from the left side to the paging/intercom group member list on the right.
Paging/Intercom Whitelist	Select which extensions are allowed to use the paging/intercom feature for this paging group.

Configure Announcement Paging

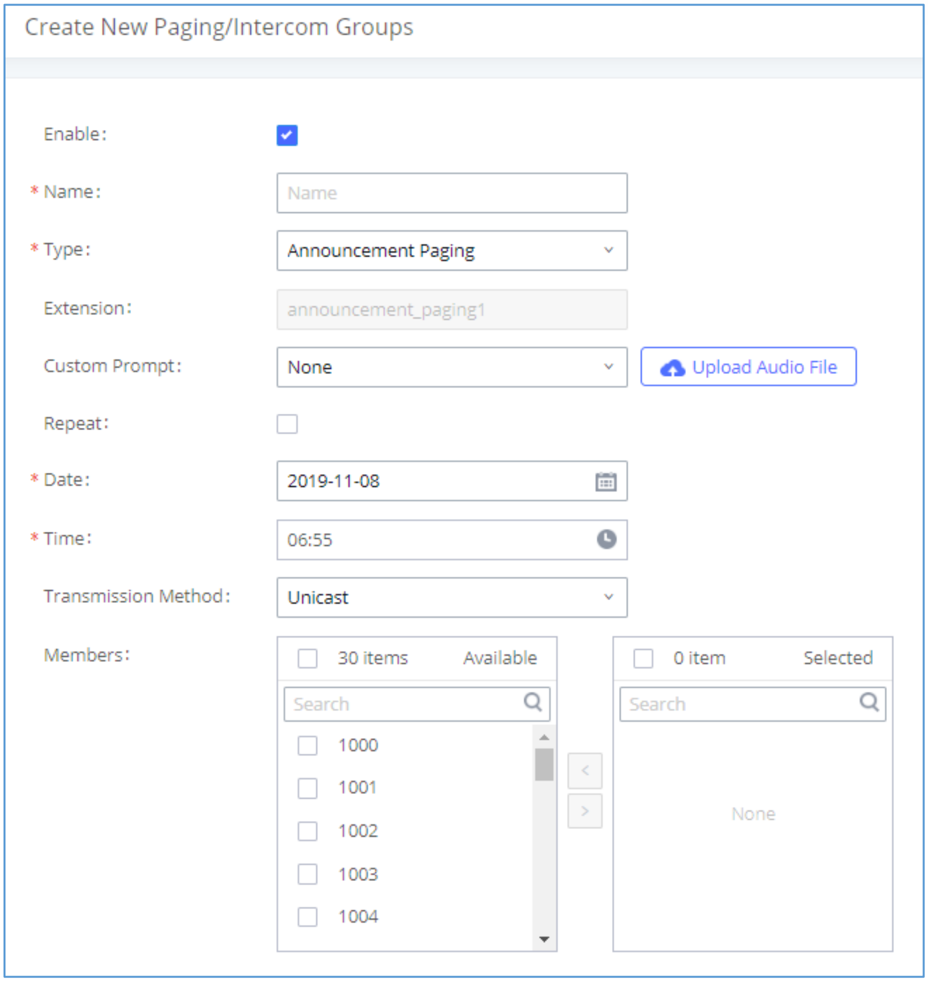


Figure 177: Announcement Paging

Table 85: Announcement Paging Configuration Parameters

Enable	Enable/Disable Announcement Paging.
Name	Configure paging/intercom group name.
Type	Select "Announcement 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.
Repeat	If enabled, the announcement page will be repeated for the selected weekdays.
Date	Configure Announcement Paging Date.

Time	Configure Announcement Paging Time.
Transmission Method	Configure Announcement Paging transmission method. **Unicast**: Depending on members selection **Multicast:** Depending on Multicast IP address and Port
Members	Select available users from the left side to the paging/intercom group member list on the right.

Paging/Intercom Group Settings

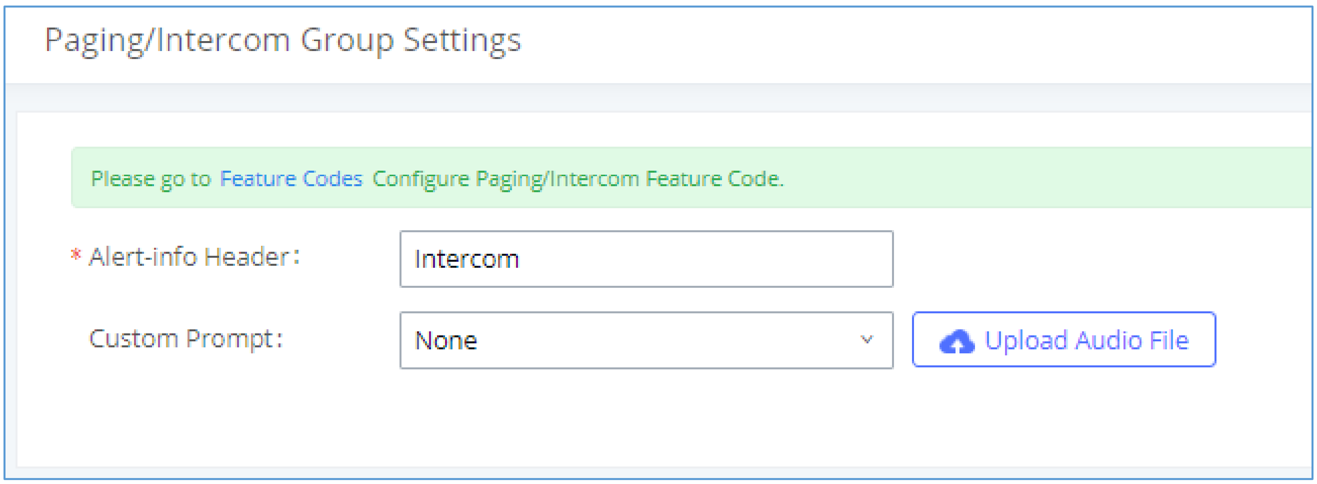


Figure 178: Page/Intercom Group Settings

The UCM630X has pre-configured paging/intercom feature code. By default, the Paging Prefix is *81 and the Intercom Prefix is *80. To edit page/intercom feature code, click on "Feature Codes" in the "Paging/Intercom Group Settings" dialog. Or users could go to Web GUI→**Call Features**→**Feature Codes** directly.

Configure a Scheduled Paging/Intercom

Users can schedule paging/intercom calls by using the Schedule Paging/Intercom page. To schedule, click the Add button on the new page and configure the caller, the group to use, and the time to call out.

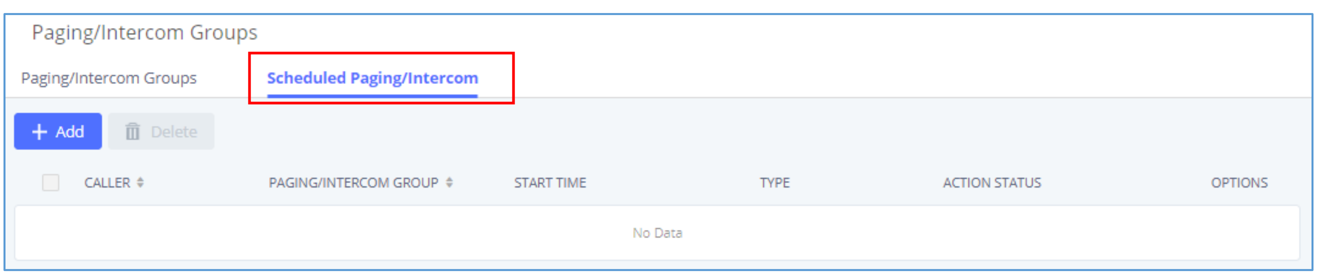


Figure 179: Schedule Paging/Intercom page

Table 86: Schedule Paging / Intercom Settings

Caller	Configure the caller ID for the paging / intercom group.
Paging/Intercom Group	Select the paging / intercom group from the list of the available groups.
Start Time	Configure the start time of the scheduled paging / intercom call.
Type	Select the type for the scheduled paging / intercom call. The available types are: **Single** time or **Daily** basis. Default is "Single".
Action Status	Display the action status of the scheduled paging / intercom call.

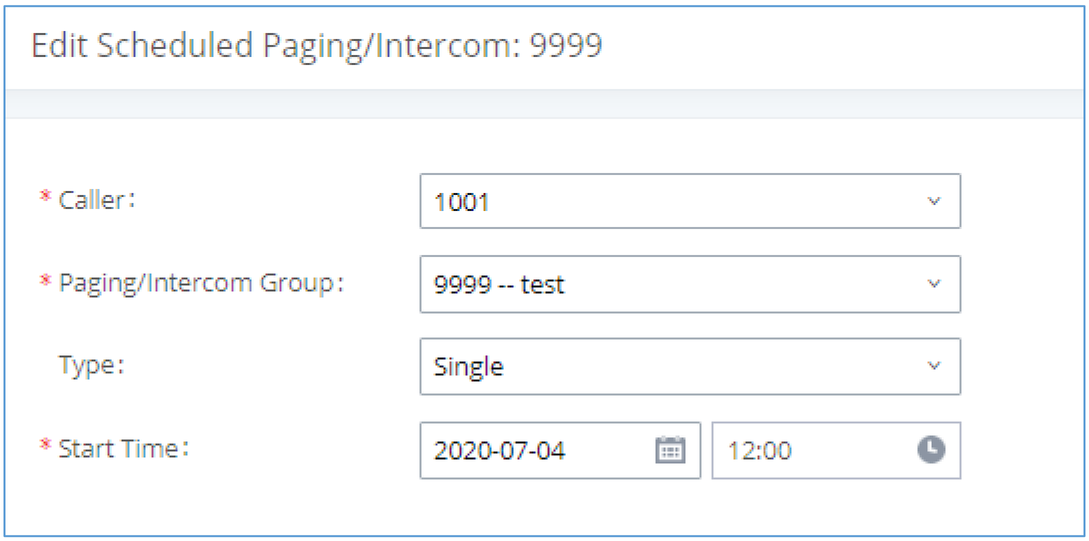


Figure 180: Creating a scheduled paging/intercom call

CALL QUEUE

The UCM630X supports call queue by using static agents or dynamic agents. Call Queue system can accept more calls than the available agents. Incoming calls will be held until next representative is available in the system. This section describes the configuration of call queue under Web GUI→**Call Features**→**Call Queue**.

Configure Call Queue

Call queue settings can be accessed via Web GUI→**Call Features**→**Call Queue**.

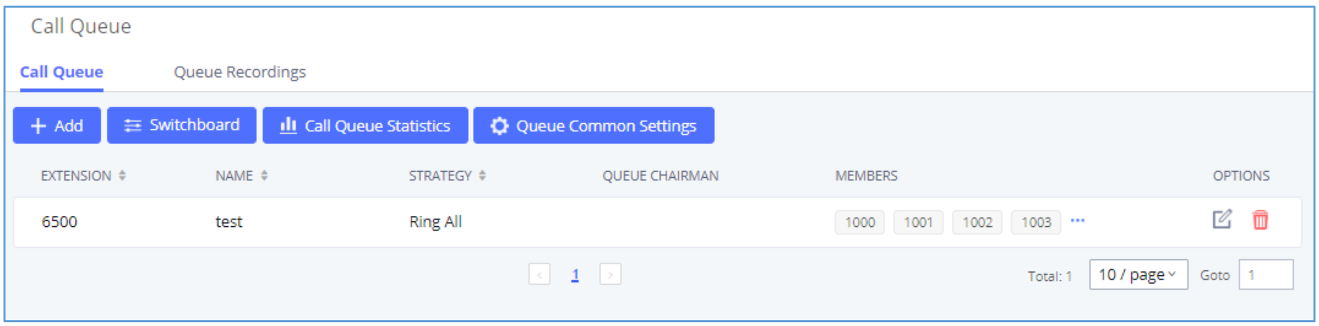


Figure 181: Call Queue

UCM630X supports custom prompt feature in call queue. This custom prompt will active after the caller waits for a period of time in the Queue. Then caller could choose to leave a message/ transfer to default extension or keep waiting in the queue.

To configure this feature, please go to UCM Web GUI→**Call Features**→**Call Queue**→Create New Queue/Edit Queue→Queue Options→set Enable Destination to Enter Destination with Voice Prompt. Users could configure the wait time with Voice Prompt Cycle.

- Click on "Add" to add call queue.
- Click on to edit the call queue. The call queue configuration parameters are listed in the table below.
- Click on to delete the call queue.

Table 87: Call Queue Configuration Parameters

Basic Settings	
Extension	Configure the call queue extension number.
Name	Configure the call queue name to identify the call queue.
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".
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 that have been connected with agents. It only includes calls not connected yet. The default setting is 0, which means unlimited. When the maximum value is reached, the caller will be treated with busy tone followed by the next calling rule after attempting to enter the queue.
Wrapup Time	Configure the number of seconds before a new call can ring the queue after the last call on the agent is completed. If set to 0, there will be no delay between calls to the queue. The default setting is 10 seconds.
Retry Time	Configure the number of seconds to wait before ringing the next agent.
Ring Time	Configure the number of seconds an agent will ring before the call goes to the next agent. The default setting is 30 seconds.
Auto Record	If enabled, the calls on the call queue will be automatically recorded. The recording files can be accessed in Queue Recordings under Web GUI→**Call Features→Call Queue**.
Max Wait Time	Configure the timeout after which users will be disconnected from the call queue. The default setting is "60". 0 means unlimited. **Note:** It is recommended to configure "Wait Time" longer than the "Wrapup Time".
Welcome Prompt	If enabled, users can upload an audio file that will be played as an Initial tone when dialing the queue number.
Destination	Once Max Wait Time has been configured, select to which destination send the calls that have timed out. The default is to “Hang up” the call.

Destination Prompt Cycle	Configure the voice prompt cycle (in seconds) of the call queue. Once all agents are busy and the voice prompt will be played, and you can press the appropriate key to transfer to failover destination.
Custom Prompt	When playing a custom prompt, press 1 to transfer to failover destination.
Destination	Select failover destination to send callers after pressing 1 upon hearing the custom prompt.
Advanced Settings	
- **Virtual Queue** - **Caller Announcement** - **Queue Chairman**	Refer to ***Call Center Settings and Enhancements*** section for detailed information about these features.
Enable Position Announcement	If enabled, the system will inform callers waiting in the queue of their positions in line.
Enable Wait Time Announcement	If enabled, the estimated wait time for the call to get answered will periodically be announced to the caller. Note: Wait time will not be announced if less than one minute.
Announcement Interval	The interval at which caller positions and estimated wait times will be announced.
Enable Agent Login	Enables agent login/logout feature for static agents (supported only on GXP21XX phones with firmware higher than 1.0.9.18).
Leave When Empty	Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict". • **Yes** Callers will be disconnected from the queue if all agents are paused or invalid. • **No** Never disconnect the callers from the queue when the queue is empty. • **Strict** Callers will be disconnected from the queue if all agents are paused, invalid or unavailable.
Dial in Empty Queue	Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No". • **Yes** Callers can always dial into a call queue. • **No** Callers cannot dial into a queue if all agents are paused or invalid.

	• **Strict** Callers cannot dial into a queue if the agents are paused, invalid or unavailable.
Failover Destination	Choose the destination where the call will be directed when the queue is empty or when all the agents are not logged in, here are the destinations that can be configured: • Play Sound. • Extension. • Voicemail. • Queues. • Ring Group. • Voicemail Group. • IVR. • External Number.
Enable Agent Login	Enabling agent login will cause the dynamic agents to be unavailable.
Queue Chairman	The queue chairman can log into his web portal to operate the queue.
Report Hold Time	If enabled, the UCM630X will report (to the agent) the duration of time of the call before the caller is connected to the agent. The default setting is "No".
Replace Display Name	If enabled, the UCM will replace the caller display name with the Call Queue name so that the caller knows the call is incoming from a Call Queue.
Enable Feature Codes	Enable feature codes option for call queue. For example, *83 is used for “Agent Pause”
Autofill	Configure to enable autofill.
Dynamic Login Password	If enabled, the configured PIN number is required for dynamic agent to log in. The default setting is disabled.
Alert-Info	When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS.
Agents	
Static Agents	Go to “Agents” Tab and Select the available users to be the static agents in the call queue. Choose from the available users on the left to the static agents list on the right. Click on to choose. And use UP and Down arrow to select the order of the agent within the call queue.

Static Agents limitation:

To guarantee a high level of audio quality with the call queue feature, UCMs will limit the number of static agents allowed to be assigned depending on the UCM model used. If the user attempts to configure the number of static agents to be more than the maximum allowed number, a warning message will appear.

The following table lists the maximum number of static agents for each UCM model:

Table 88: Static Agent Limitation

UCM Model	Max Static Agents in Call Queue
UCM6301	10
UCM6302	60
UCM6304	100
UCM6308	120

Click on "Global Queue Settings" to configure Agent Login Extension Postfix and Agent Logout Extension Postfix. Once configured, users could log in the call queue as dynamic agent.

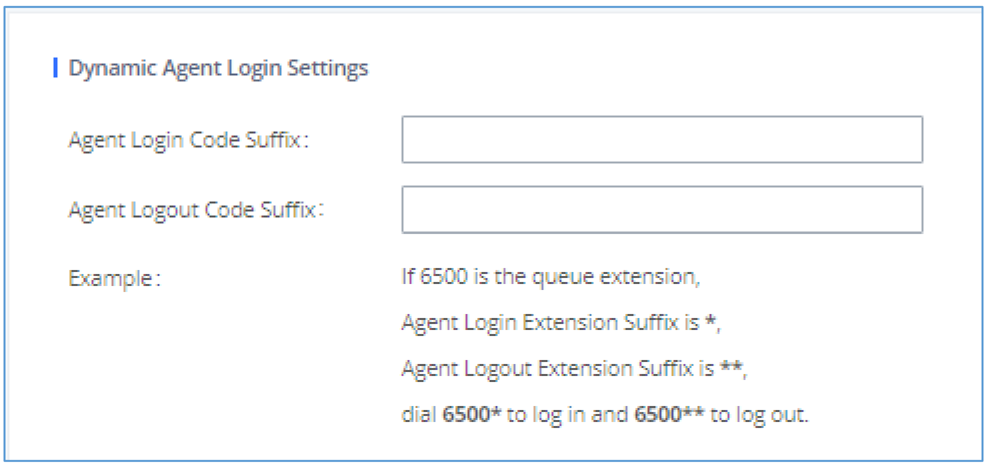


Figure 182: Agent Login Settings

For example, if the call queue extension is 6500, Agent Login Extension Postfix is * and Agent Logout Extension Postfix is **, users could dial 6500* to login to the call queue as dynamic agent and dial 6500** to logout from the call queue. Dynamic agent does not need to be listed as static agent and can log in/log out at any time.

- Call queue feature code "Agent Pause" and "Agent Unpause" can be configured under Web GUI→**Call Features→Feature Codes**. The default feature code is *83 for "Agent Pause" and *84 for "Agent Unpause".

  Note: When dialing the “Agent Pause” feature code, users can specify the reason for it. The following reasons are available: (1) Lunch, (2) Hourly Break, (3) Backoffice, (4) Email, and (5) Wrap.

- Queue recordings are shown on the Call Queue page under “Queue Recordings” Tab. Click on to download the recording file in .wav format; click on to delete the recording file. To delete multiple recording files by one click, select several recording files to be deleted and click on “Delete Selected Recording Files” or click on “Delete All Recording Files” to delete all recording files.

Call Center Settings and Enhancements

UCM supports light weight call center features including virtual queue and position announcement, allowing the callers to know their position on the call queue and giving them the option to either stay on the line waiting for their turn or activate a callback which will be initiated by the UCM one an agent is free.

To configure call center features, press on an existing call queue and go under the advanced settings tab. Following parameters are available:

Table 89: Call Center Parameters

Enable Virtual Queue	Enable virtual queue to activate call center features.
Virtual Queue Period	Configure the time in (s) after which the virtual queue will take effect and the menu will be presented to the caller to choose an option. Default is 20s.
Virtual Queue Mode	**Offered to caller after timeout:** After the virtual queue period passes, the caller will enter the virtual call queue and be presented with a menu to choose an option, the choices are summarized below: • Press * to set current number as callback number. • Press 0 to set a callback number different than current caller number. • Press # to keep waiting on the call queue. **Triggered on user request:** In this mode, the callers can activate the virtual queue by pressing 2, then they will be presented with the menu to choose an option as below: • Press * to set current number as callback number. • Press 0 to set a callback number different than current caller number. • Press # to keep waiting on the call queue.
Virtual Queue Outbound Prefix	System will add this prefix to dialed numbers when calling back users.
Enable Virtual Queue Timeout	When this option is enabled and after a caller registers a call back request on the virtual queue. While all the agents are busy, the UCM will call an agent once he/she is idle again, this timeout is used for how long the UCM continues calling the agent and if the agent doesn’t answer the call then the callback request will timeout and expire.
Write Timeout	Configure the virtual queue callback timeout period in seconds.
Enable Virtual Queue Position Announcement	Enable the announcement of the caller’s position periodically. **Note:** Queue position will now be announced to the caller upon entering the queue.

Position Announcement Interval	Configure the period of time in (s) during which the UCM will announce the caller's position in the call queue.
Enable Virtual Queue Wait Time Announcement	When enabled the UCM will announce the estimated queue wait time to callers if the estimated wait time is longer than 1 minute.
Queue Chairman	Select the extension to act as chairman of the queue (monitoring).
Virtual Queue Welcome Prompt	Click on "Upload Audio File" to upload the VQ welcome prompt.
Enable Agent Login	When enabled, statics agents can conveniently log in and out of a queue by configuring a programmable key on their phones as a shortcut. **Notes**: ✓ This feature is currently available only for GXP21xx phones on firmware 1.0.9.18 or greater. ✓ After enabling the feature, users need to set the option on GXP21XX phone under "**Account→SIP Settings→Advanced Features→Special Feature**" to "**UCM Call Center**". A softkey labeled "UCM-CC" will appear on the bottom of the phone's screen. ✓ When this option is enabled, dynamic agent login will be no longer supported. ✓ In case of concurrent registrations, changing agent status on one phone (login/logout) will be reflected on all phones.

Queue Auto fill enhancement:

The waiting callers are connecting with available members in a parallel fashion until there are no more available members or no more waiting callers.

For example, in a call queue with linear method, if there are two available agents, when two callers call in the queue at the same time, UCM will assign the two callers to each of the two available agents at the same time, rather than assigning the second caller to second available agent after the first agent answers the call from the first caller.

Queue Statistics

Along with call center features, users can also gather detailed call queue statistics allowing them to make better changes/decision to manage better the call distribution and handling based on time, agent, and queue.
To access call queue statistics, go to Web GUI→**Call Features**→**Call Queue** and click on "Call Queue Statistics", the following page will be displayed:

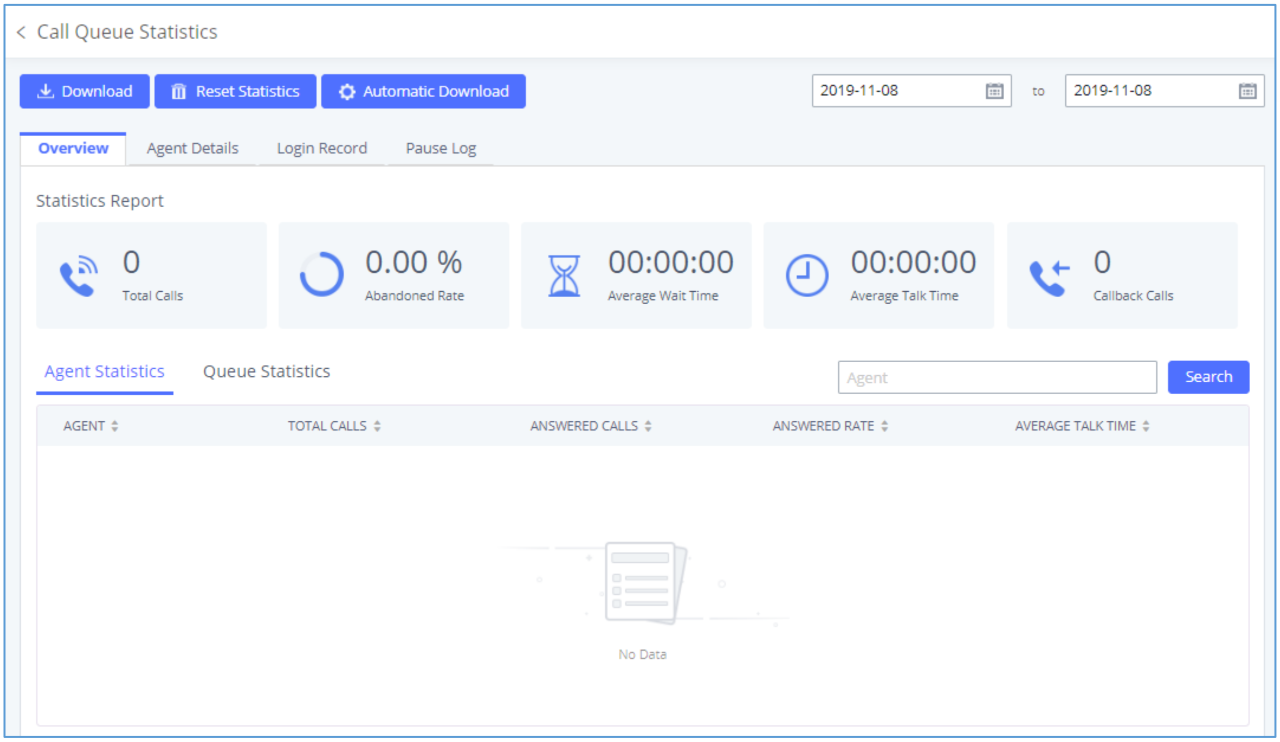


Figure 183: Call Queue Statistics

By selecting a time interval, administrators can get detailed statistics for agent(s) such as total calls, answered calls etc, as well as for the queue(s) such as ABANDONED CALLS also a detailed information for the queue's call log by clicking on **Options→Information** button and the below window will pop up:

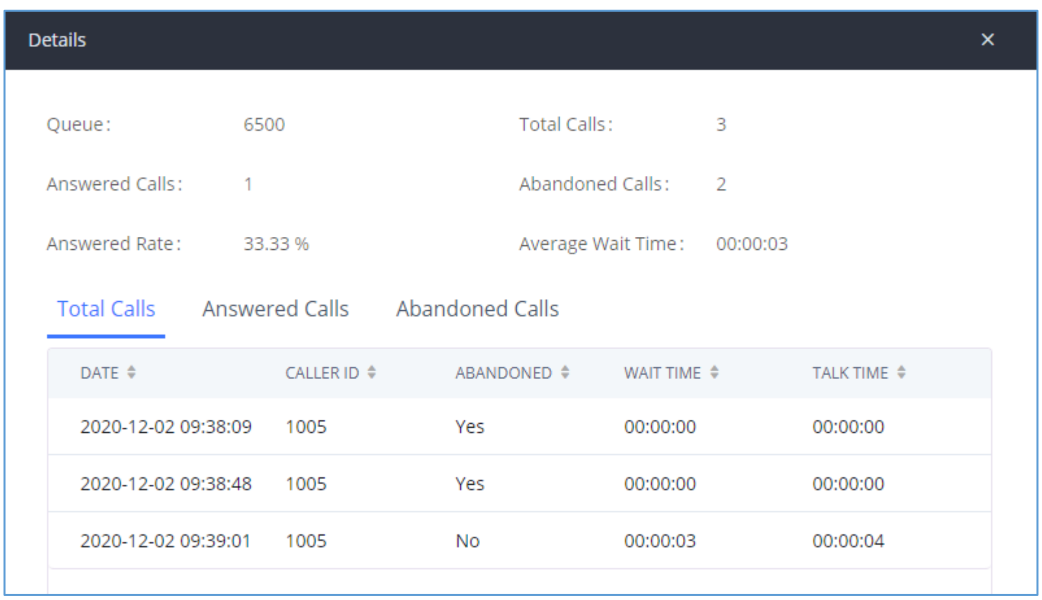


Figure 184: Queue's call log details

User can download statistics on CSV format by clicking on the "**Download**", also the statistics can be cleared using "**Reset Statistics**" button.

The statistics can be automatically sent to a specific email address on a preconfigured Period, this can be done by clicking on "**Automatic Download**", and user will be directed to below page where he can configure the download period (Day/Week/Month) and the Email where the statistics will be sent (Email settings should be configured correctly):

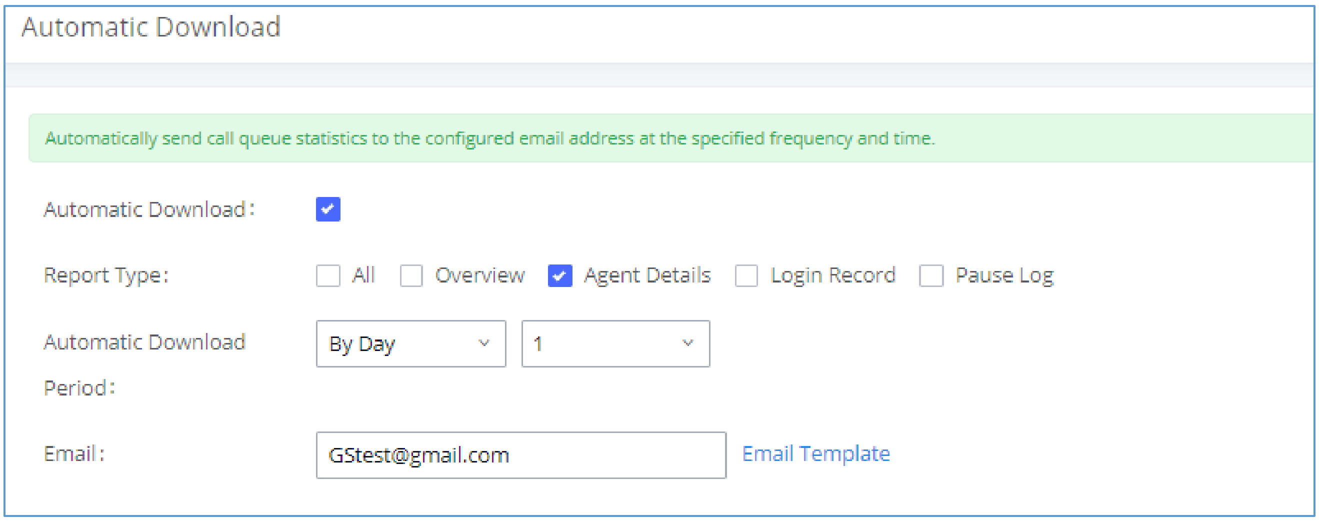


Figure 185: Automatic Download Settings - Queue Statistics

Significantly more information is now available UCM's queue statistics page. In addition to the information presented in previous firmware, users can now view a call log that displays calls to all agents and queues, a dynamic agent login/logout record, and a pause log. Statistics reports for these new pages can be obtained by pressing the Download button in the top left corner of the Call Queue Statistics page. The reports are in .CSV format and will be packaged into a single tar.gz file upon download.

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

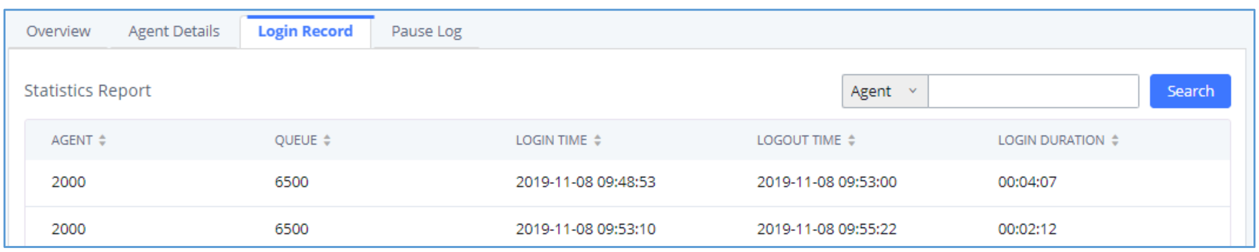
- Time – the date and time the call was received.
- Agent – the agent that was rung for the call.
- Queue – the queue that the call went to.
- Caller ID Number – the CID of the caller
- Abandoned – indicates whether the call was picked up or not by that specific agent. If the call rang several agents 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.

TIME	AGENT	QUEUE	CALLER ID NUMBER	ABANDONED	WAIT TIME	TALK TIME
2019-11-08 10:56:36	2000	6500	1000	No	00:00:05	00:00:29
2019-11-08 11:09:07	2000	6500	1000	No	00:00:07	00:01:51
2019-11-08 11:18:17	2000	6500	1000	Yes	00:00:04	00:00:00

Figure 186: Agent details

Login Record is a report that shows the timestamps of dynamic agent logins and logouts and calculates the amount of time the dynamic agents were logged in. Dynamic agents are extensions that log in and out either via agent login/logout codes (configured in Global Queue Settings page) or by using the GXP21xx call queue softkey. A new record will be created only when an agent logs out. 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.



AGENT	QUEUE	LOGIN TIME	LOGOUT TIME	LOGIN DURATION
2000	6500	2019-11-08 09:48:53	2019-11-08 09:53:00	00:04:07
2000	6500	2019-11-08 09:53:10	2019-11-08 09:55:22	00:02:12

Figure 187: Login Record

Pause Log is a report that shows the times of agent pauses and unpauses and calculates the amount of time that agents are paused. If an agent is part of several queues, an entry will be created for each queue. An entry will only be created after an agent unpauses. The following information is available:

- Agent **–** the extension that paused and unpaused.
- Queue – the queue that the agent is in.
- Pause Time – the time that the agent paused.
- Resume Time – the time that the agent unpaused.
- Pause Duration – the total length of time the agent was paused for.

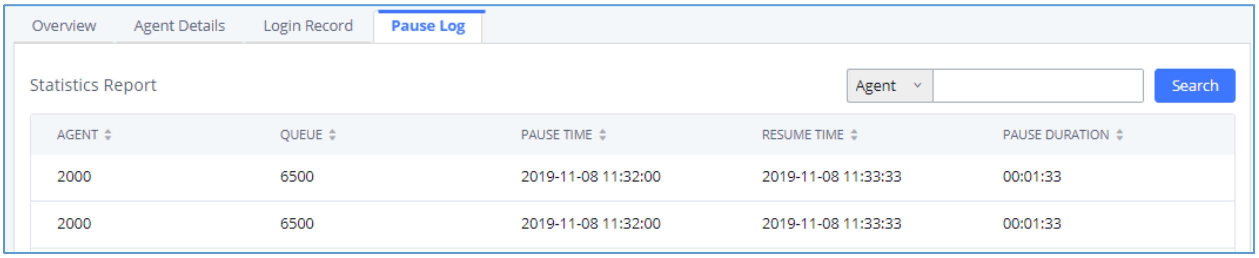


Figure 188: Pause Log

Switchboard

Switchboard is a Web GUI tool for call queue monitoring and management, admin can access to it from the menu **Call Features→Call Queue** then press "Switchboard".

Following page will be displayed:

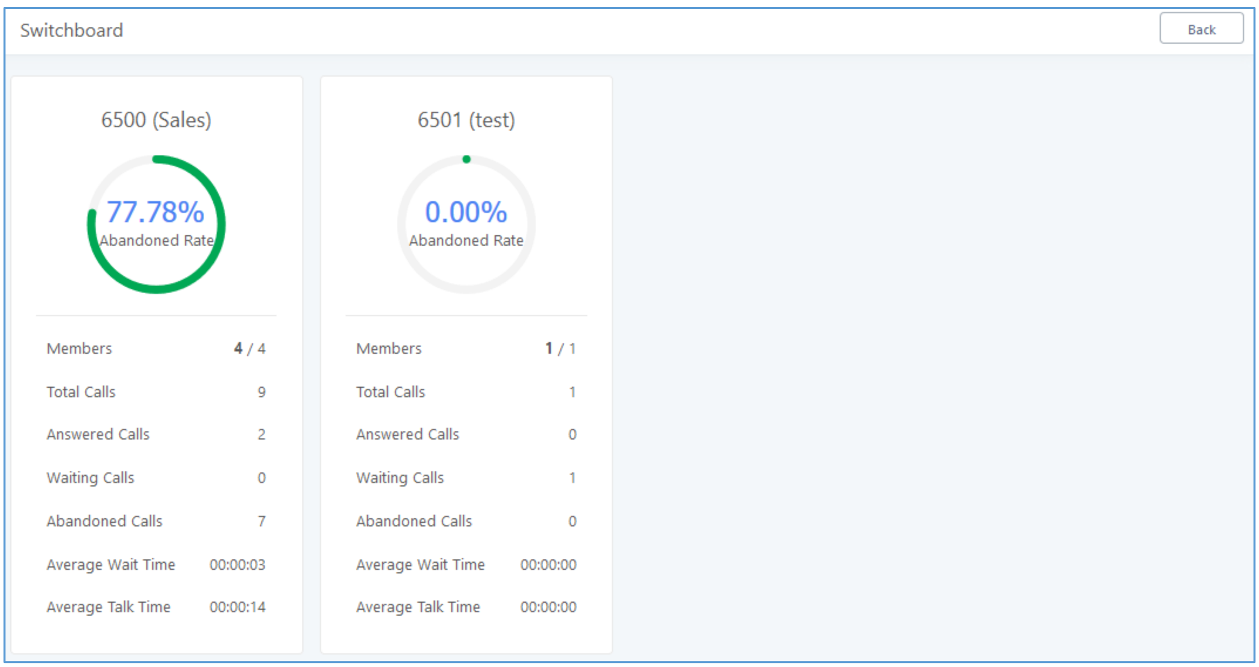


Figure 189: Switchboard Summary

Page above summarizes the available queues statistics and if one of the queues is clicked the user will be directed to page below:

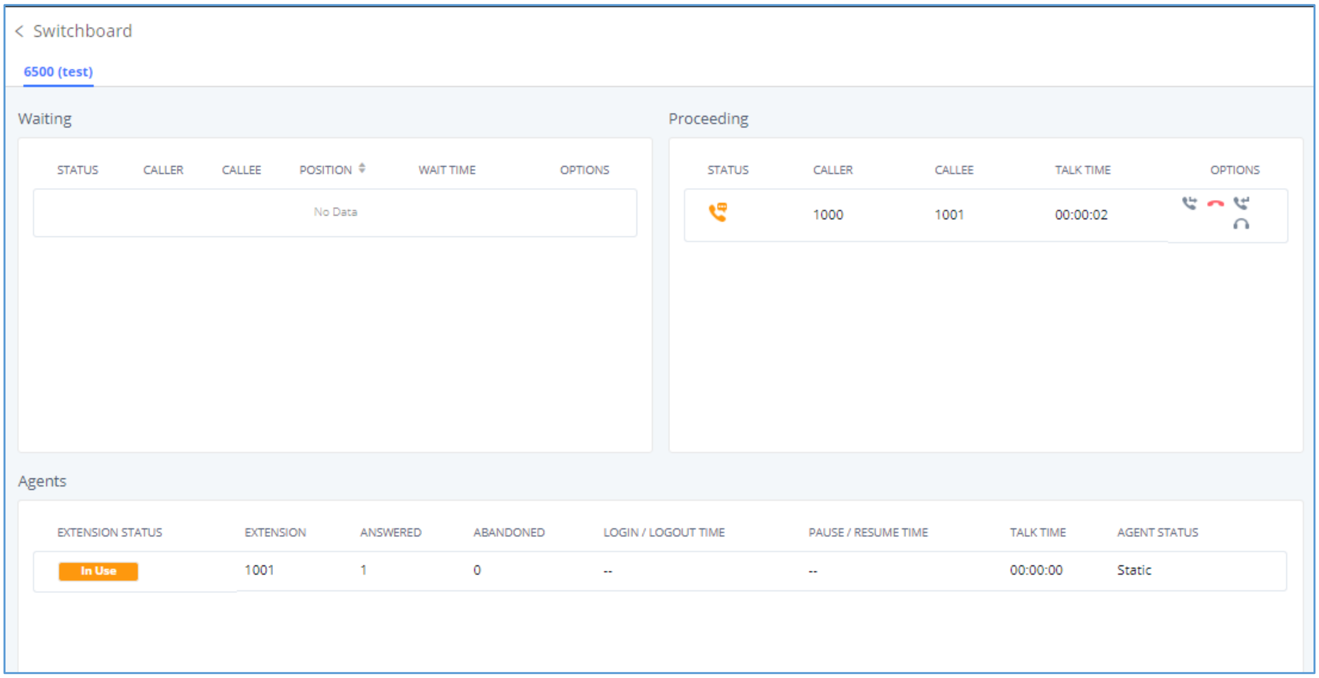


Figure 190: Call Queue Switchboard

The table below gives a brief description for the main menus:

Table 90: Switchboard Parameters

Waiting	This menu shows the current waiting calls along with the caller id and the option to hang-up call by pressing on the button.
Proceeding	Shows the current established calls along with the caller id and the callee (agent) as well as the option to hang-up, transfer, add conference or barge-in the call.
Agents	Displays the list of agents in the queue and the extension status (idle, ringing, in use or unavailable) along with some basic call statistics and agent's mode (static or dynamic). **Note:** the dashboard will show the number of calls (answered and abandoned) of each agent. For dynamic agents, it will count the number of calls starting from the last login time.

There are three different privilege levels for Call Queue management from the switchboard: Super Admin, Queue Chairman, and Queue Agent.

- **Super Admin** - Default admin of the UCM. Call queue privileges include being able to view and edit all queue agents, monitor, and execute actions for incoming and ongoing calls for each extension in Switchboard, and generate Call Queue reports to track performance.

- **Queue Chairman** - User appointed by Super Admin to monitor and manage an assigned queue extension via Switchboard. The Queue Chairman can log into the UCM user portal with his extension number and assigned user password. To access the Switchboard, click on "*Value-added Features"* in the side menu and click on "*Call Queue".* In the image below, User 1001 is the Queue Chairman appointed to manage Queue Extension 6500 and can see all the agents of the queue in the Switchboard.

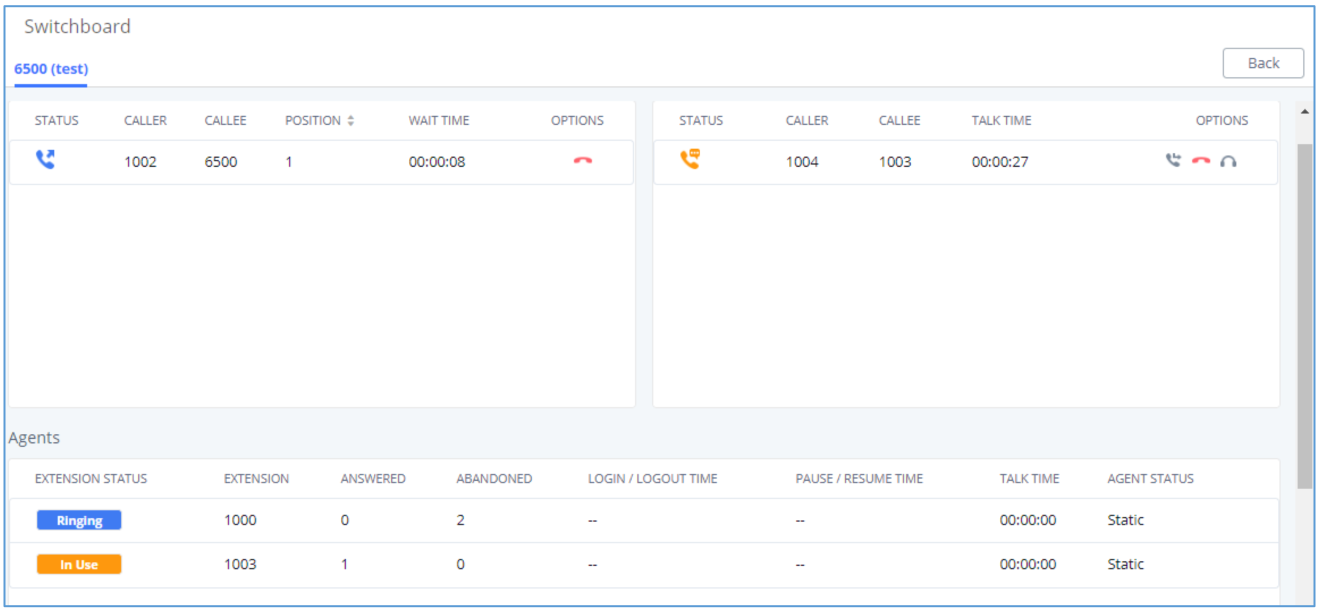


Figure 191: Queue Chairman

- **Queue Agent** - User appointed by Super Admin to be a member of a queue extension. A queue agent can log into the UCM user portal with his extension number and assigned user password. To access the Switchboard, click on "*Value-added Features"* in the side menu and click on "*Call Queue*". However, a queue agent can view and manage only his own calls and statistics, but not other agents' in the queue extension. In the image below, User 1000 is a queue agent and can see only his own information in the Switchboard.

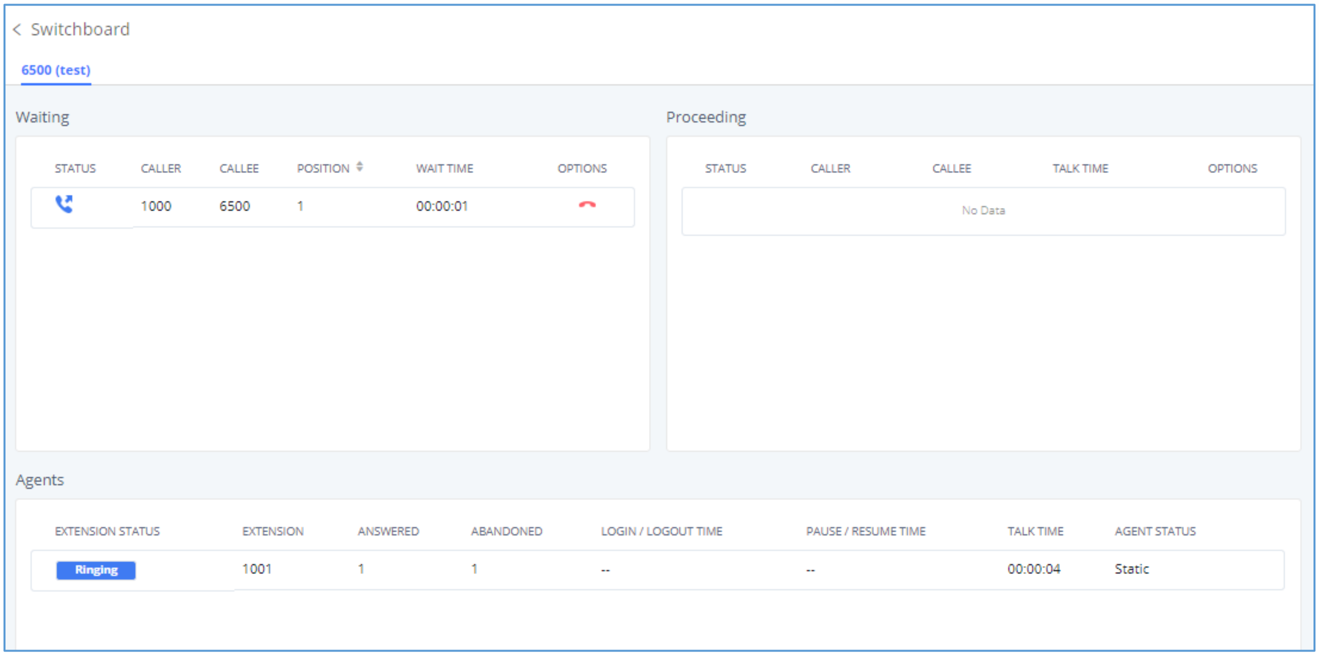


Figure 192: Queue Agent

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.

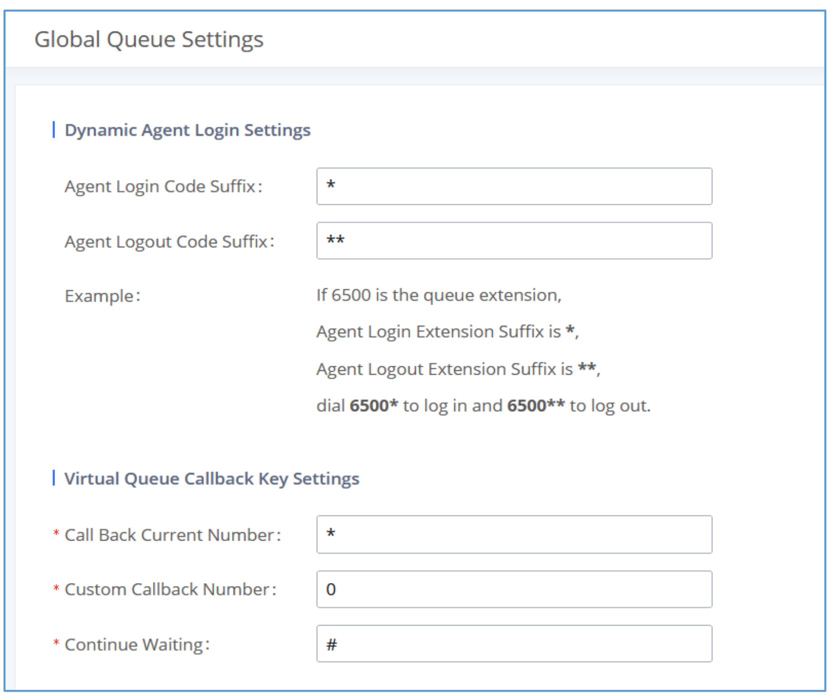


Figure 193: Global Queue Settings

Table 91: Global Queue Settings

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.
Virtual Queue Callback Key Settings	
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.

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

- Click on + Add to create a new pickup group.
- 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.

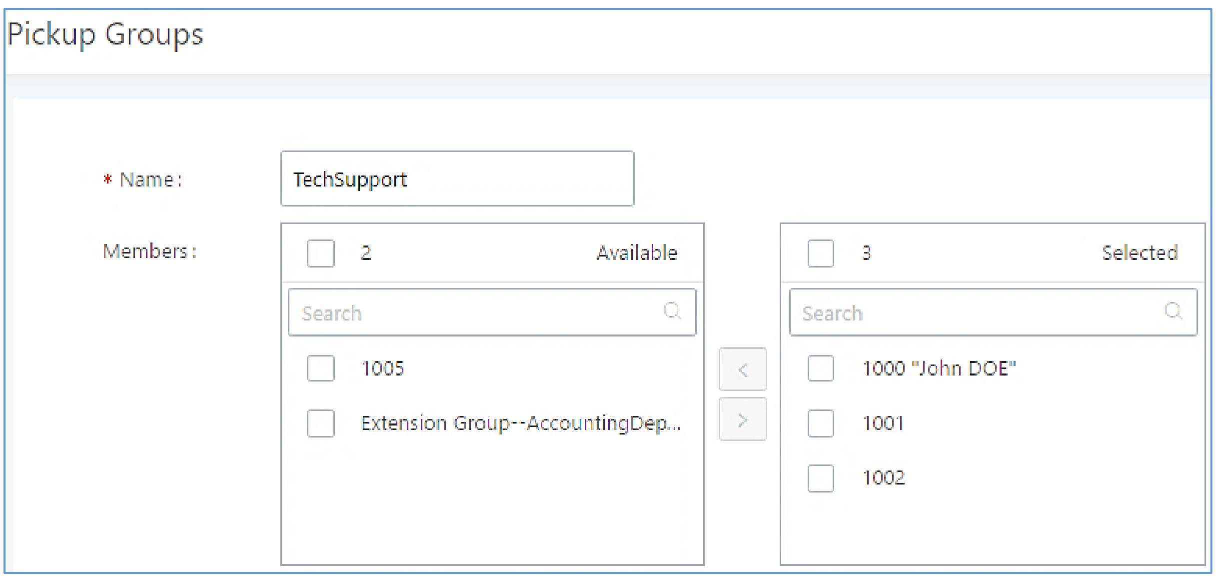


Figure 194: Edit Pickup Group

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→**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

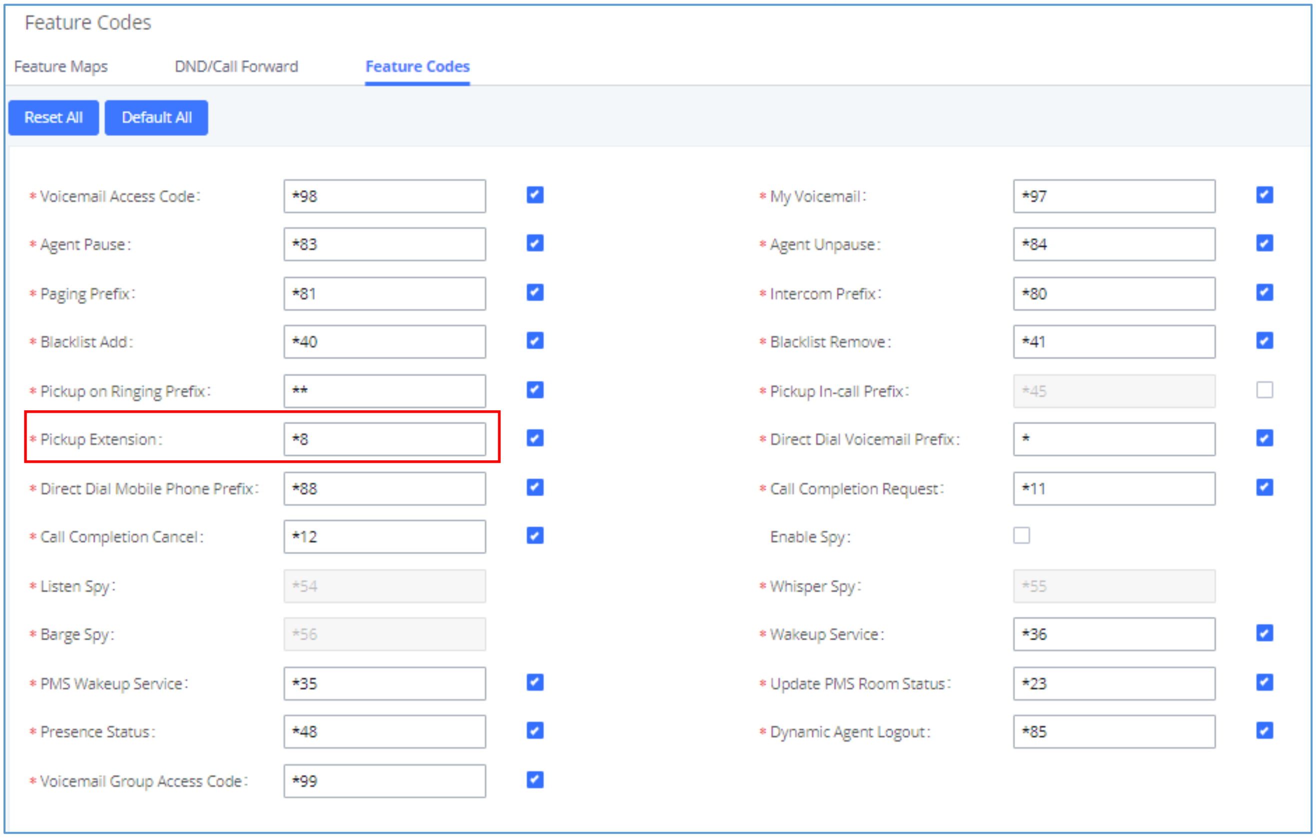


Figure 195: Edit Pickup Feature Code

MUSIC ON HOLD

Music On Hold settings can be accessed via Web GUI→**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.

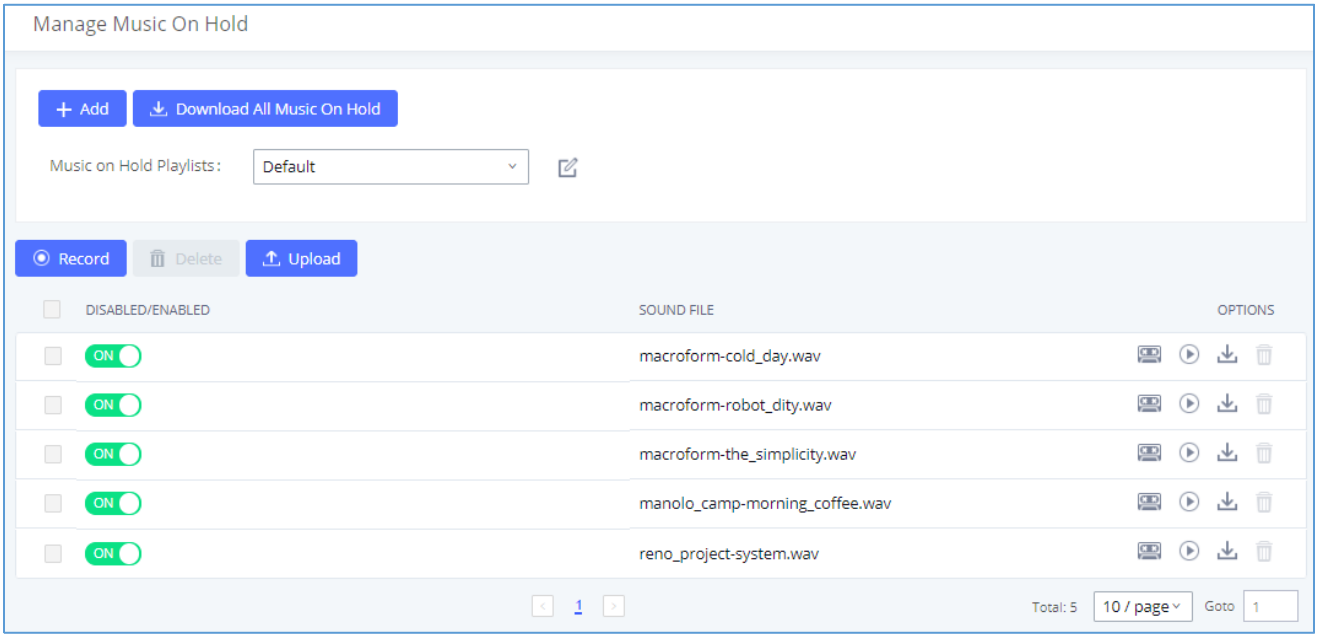


Figure 196: Music On Hold Default Class

- 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 on 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 Delete 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.

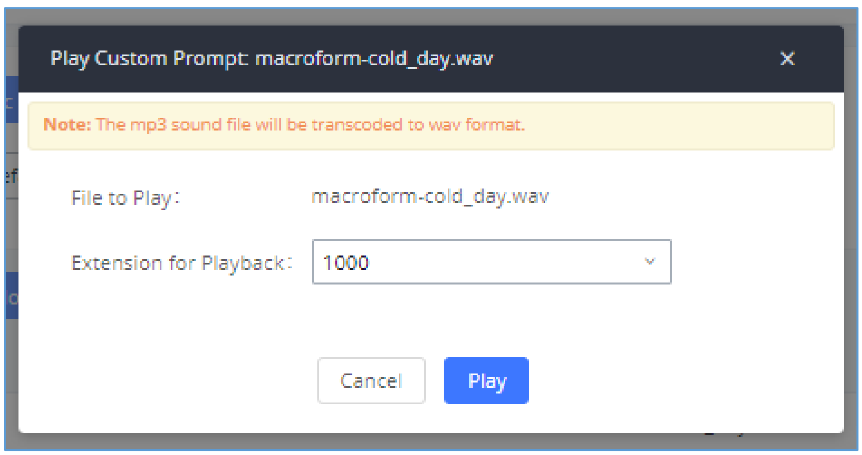


Figure 197: Play Custom Prompt

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.

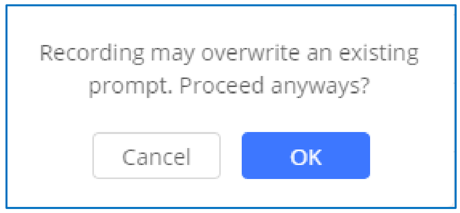


Figure 198: Information Prompt

3. Click OK.

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

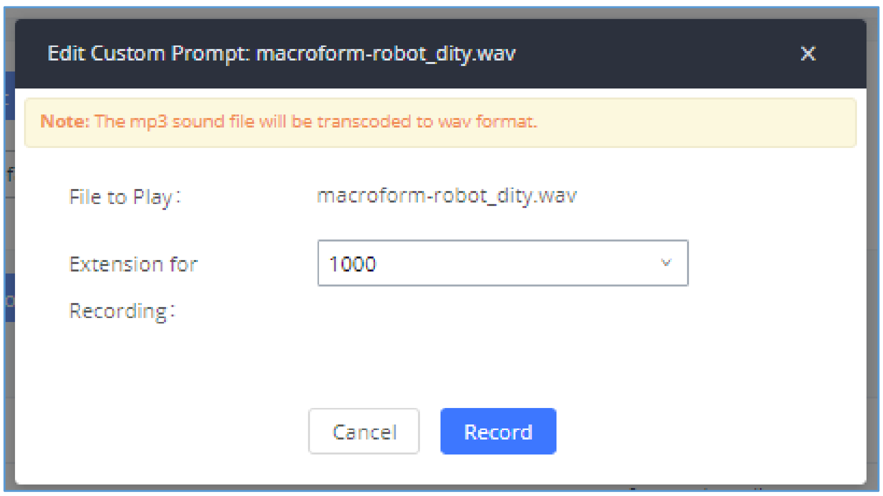


Figure 199: Record Custom Prompt

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.

⚠ **Notes:**

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.

BUSY CAMP-ON

The UCM630X supports busy camp-on/call completion feature that allows the PBX to camp on a called party and inform the caller as soon as the called party becomes available given the previous attempted call has failed.

The configuration and instructions on how to use busy camp-on/call completion feature can be found in the following guide:

http://www.grandstream.com/sites/default/files/Resources/ucm6xxx_busy_camp_on_guide.pdf

PRESENCE

UCM does support SIP presence feature which allows users to advertise their current availability status and willingness to receive calls, this way other users can use their phones in order to monitor the presence status of each user and decide whether to call them or not based on their advertised availability.

This feature is different than BLF which is used to monitor the dialog status for each extension (Ringing, Idle or Busy). Instead the SIP presence module gives more options for users to choose which state they want to put themselves in.

In order to configure the presence status of an extension from the web GUI, users can access the menu of configuration using one of the two following methods:

- From admin account, go under the menu **Extension/Trunk→Extensions** and choose the desired extension to edit then navigate to the “Features” tab.

  OR

- From the User Portal, go under the menu Basic **Information→Extensions** and navigate to the Features tab to have the following options.

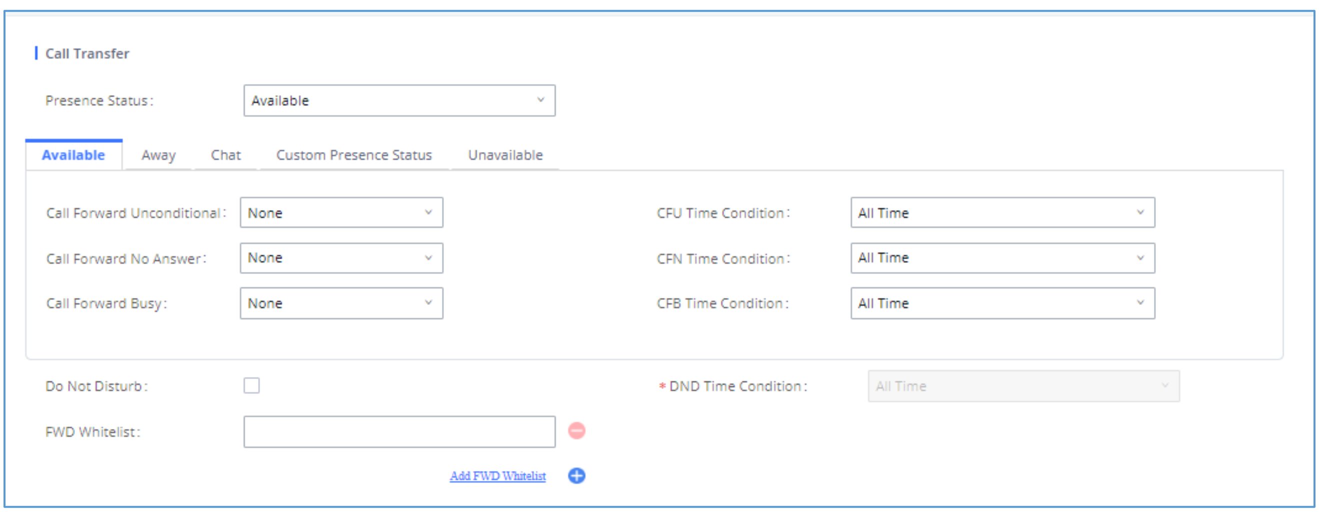


Figure 200: SIP Presence Configuration

Select which status to set from the presence status selection drop list, six options are available and below is a brief description of these states:

Table 92: SIP Presence Status

Available	The contact is online and can participate in conversations/phone calls.
Away	The contact is currently away (ex: for lunch break).
Chat	The contact has limited conversation flexibility and can only be reached via chat.
Do Not Disturb	The Contact is on DND (Do Not Disturb) mode.
Custom Presence Status	Please enter the presence status for this mode on the Web GUI. Up to 64 characters.
Unavailable	The contact is unreachable for the moment, please try to contact later.

Another option to set the presence status and which is more practical is using the feature code from the user's phone, one the user dials the feature code (default is *48), a prompt will be played to select which status they want to put themselves in, by pressing the corresponding key.

The feature code can be enabled and customized from the Web GUI→**Call Features**→**Feature Codes**.

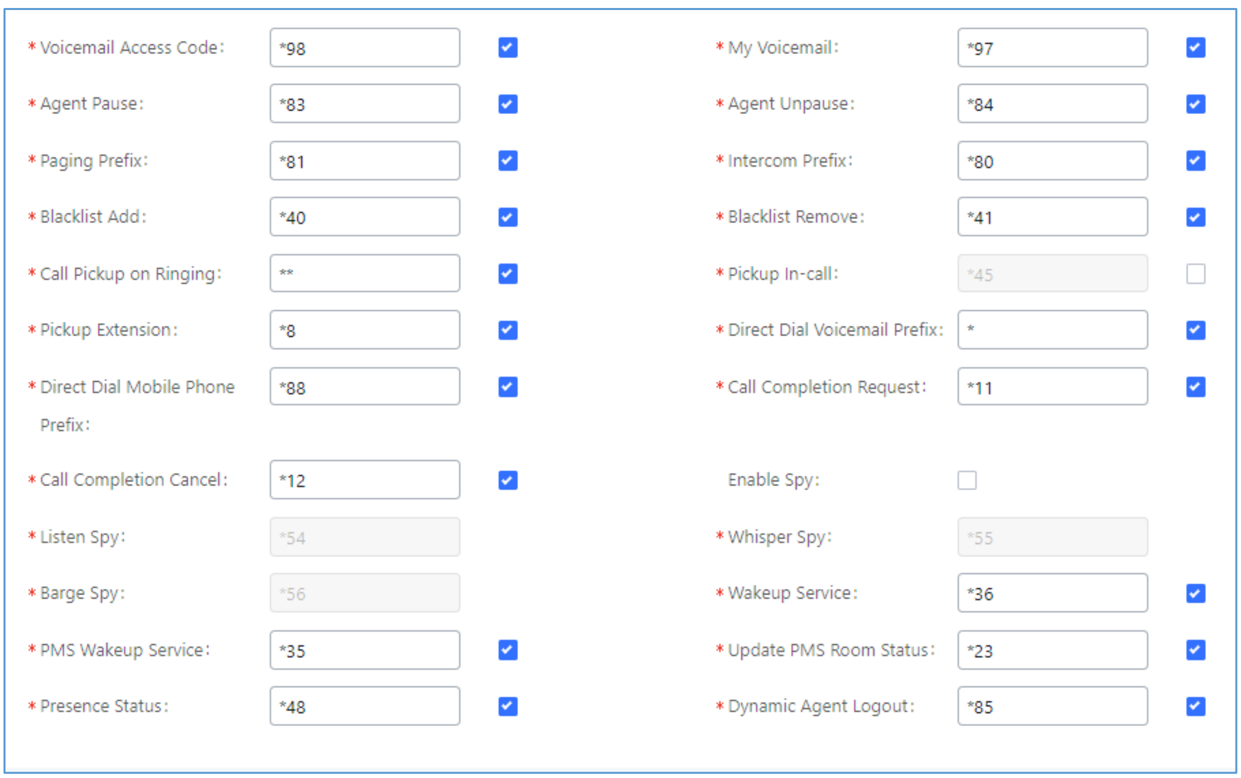


Figure 201: SIP Presence Feature Code

When a user does change his/her SIP presence status by making a call using presence feature code, the UCM will create a corresponding CDR entry showing the call as **Action type** = **PRSENCE_STATUS.**

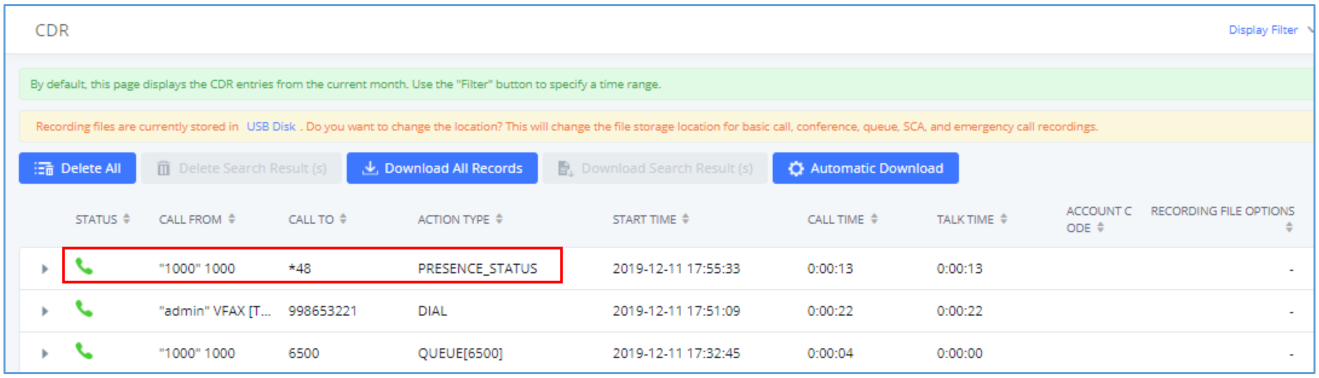


Figure 202: Presence Status CDR

FOLLOW ME

Follow Me is a feature on the UCM630X that allows users to direct calls to other phone numbers and have them ring all at once or one after the other. Calls can be directed to users' home phone, office phone, mobile and etc. The calls will get to the user no matter where they are. Follow Me option can be found under extension settings page Web GUI→**Extension/Trunk→Extensions.**

To configure follow me:

1. Choose the extension and click on .
2. Go to the Follow me tab to add destination numbers and enable the feature.

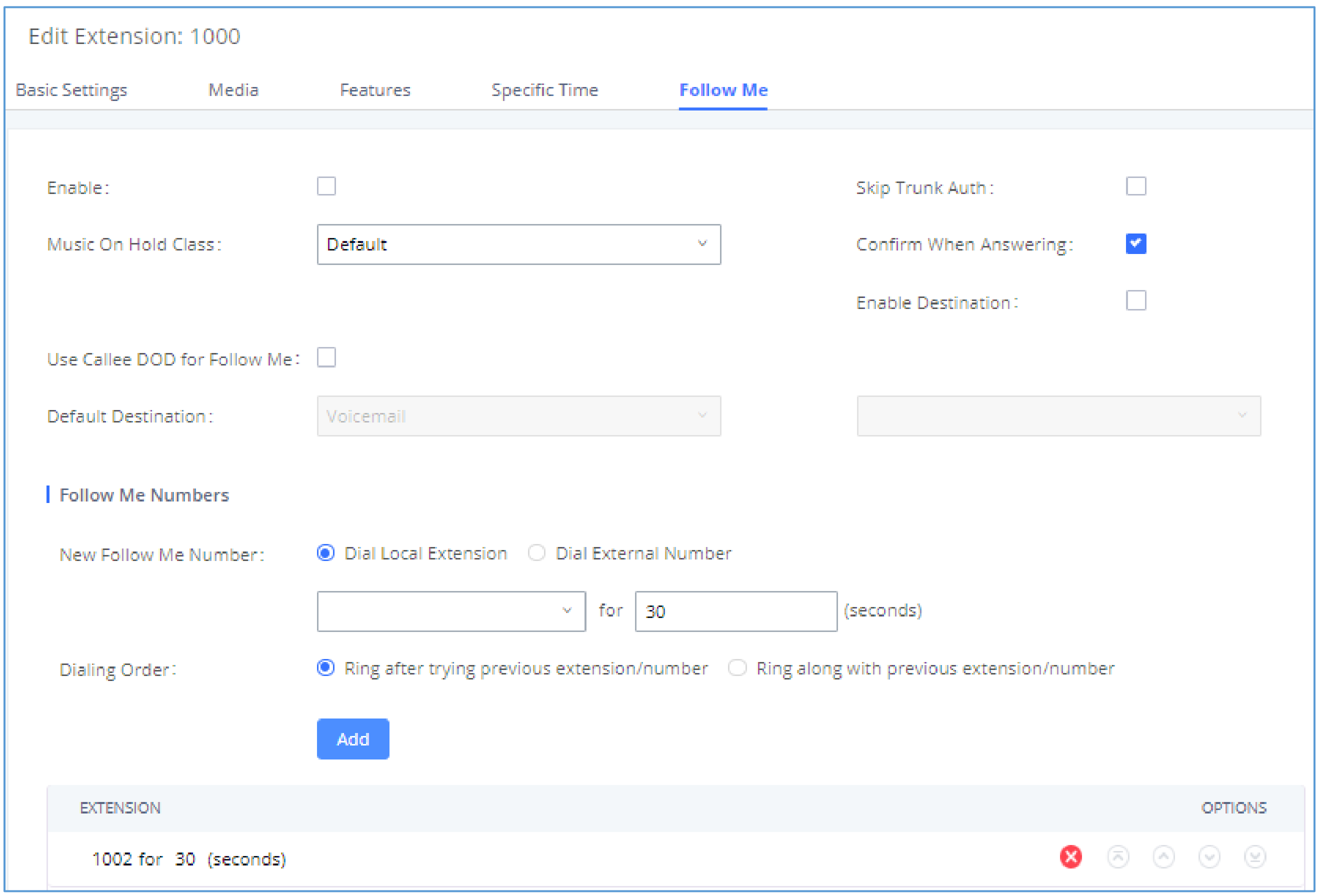


Figure 203: Edit Follow Me

3. Click on + Add to add local extensions or external numbers to be called after ringing the extension selected in the first step.
4. Once created, it will be displayed on the follow me list. And you can click on to delete the Follow Me.

The following table shows the Follow Me configuration parameters:

Table 93: Follow Me Settings

Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If external number is added in the Follow Me, please make sure this option is enabled or the "Skip Trunk Auth" option of the extension is enabled, otherwise the external Follow Me number cannot be reached.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking users
Confirm When Answering	By default, it is enabled, and user will be asked to press 1 to accept the call or to press 2 to reject the call after answering a Follow Me call. If it is disabled, the Follow Me call will be established once after the user answers.
Enable Destination	When enabled, the call will be routed to the default destination if no one in the Follow Me extensions answers the call.
Default Destination	Configure the destination if no one in the Follow Me extensions answers the call. The available options are: • Extension • Voicemail • Queues • Ring Group • Voicemail Group • IVR • External Number
Follow Me Numbers	The added numbers are listed here. Click on to arrange the order. Click on to delete the number. Click on + Add to add new numbers.
New Follow Me Number	Add a new Follow Me number which could be a 'Local Extension' or 'External Number'. The selected dial plan should have permissions to dial the defined external number.
Dialing Order	Select the order in which the Follow Me destinations will be dialed to reach the user: ring all at once or ring one after the other.

Click on "Follow Me Options" under Web GUI→**Extension/Trunk**→**Extension** page to enable or disable the options listed in the following table.

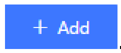
Table 94: Follow Me Options

Playback Incoming Status Message	If enabled, the PBX will playback the incoming status message before starting the Follow Me steps.
Record the Caller's Name	If enabled, the PBX will record the caller's name from the phone so it can be announced to the callee in each step.
Playback Unreachable Status Message	If enabled, the PBX will playback the unreachable status message to the caller if the callee cannot be reached.

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→**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.

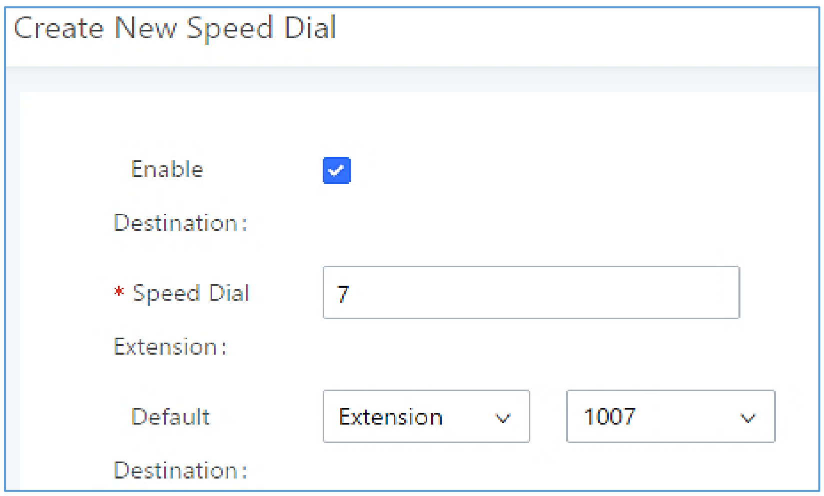
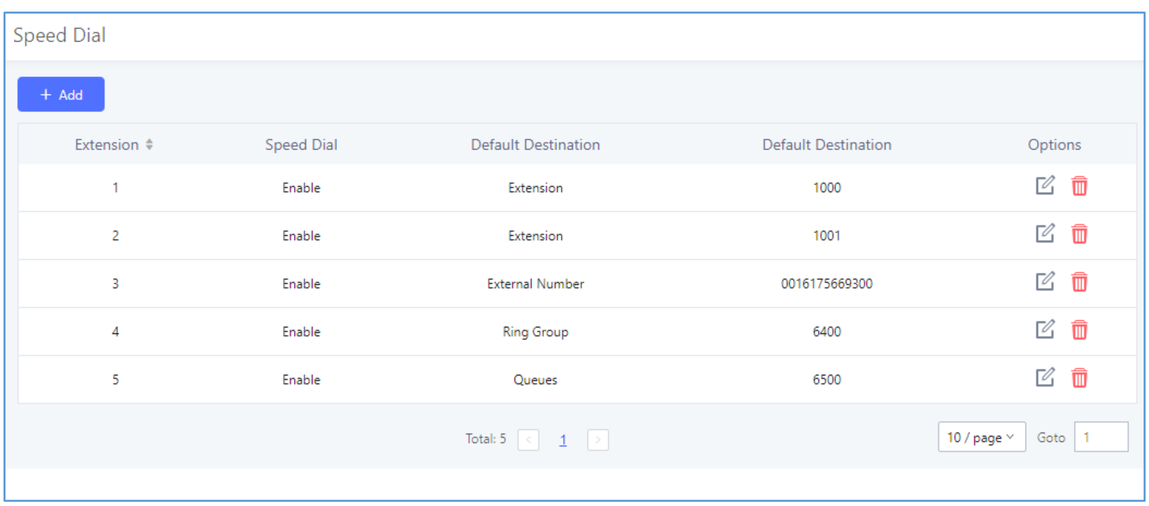


Figure 204: Speed Dial Destinations



Extension	Speed Dial	Default Destination	Default Destination	Options
1	Enable	Extension	1000	
2	Enable	Extension	1001	
3	Enable	External Number	0016175669300	
4	Enable	Ring Group	6400	
5	Enable	Queues	6500	

Figure 205: List of Speed Dial

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→**Call Features**→**DISA**.

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

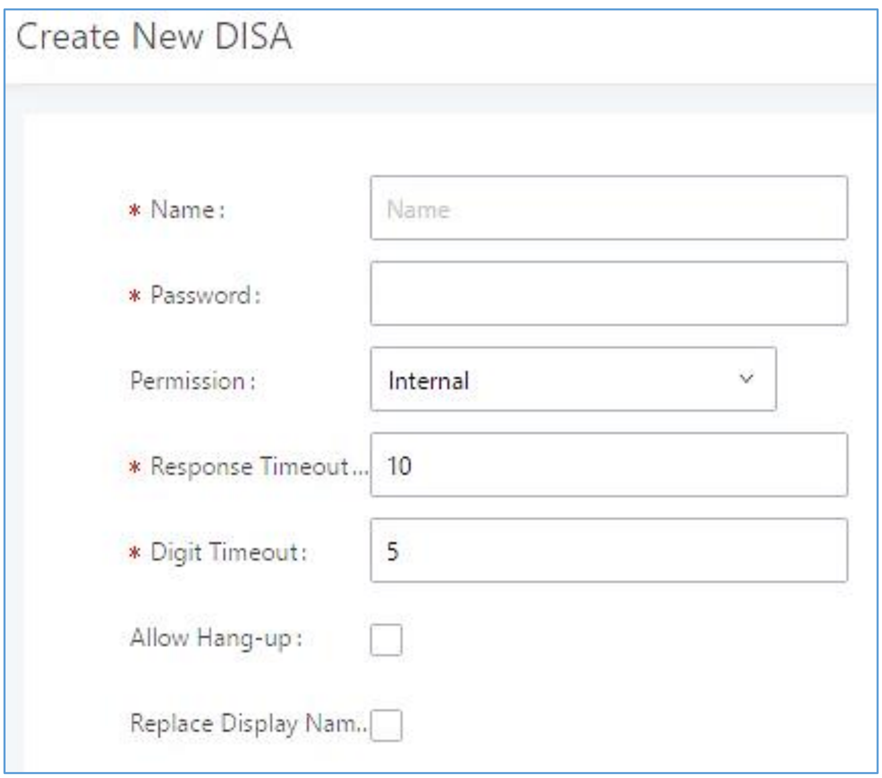


Figure 206: Create New DISA

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

Table 95: DISA Settings

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 UCM630X 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 UCM630X 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 UCM630X 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 UCM 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.

EMERGENCY

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.

UCM6xxx series are also now in full compliance with Kari's Law and Ray Baum's Act, for more information, please refer to the following links:

https://www.fcc.gov/mlts-911-requirements

http://www.grandstream.com/sites/default/files/Resources/UCM_Emergency_Calls_Guide.pdf

In addition, Emergency calls can be automatically recorded by toggling on the new Auto Record and recordings can be viewed in the new Emergency Recordings tab on the same page. Additionally, users can have these recordings be sent to the configured email address(es).

Email alerts are also supported after enabling the notification for the event under "**Maintenance → System Events**"

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

1. Navigate on the web GUI under "**Call Features → Emergency Calls**"
2. Click on + Add 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.

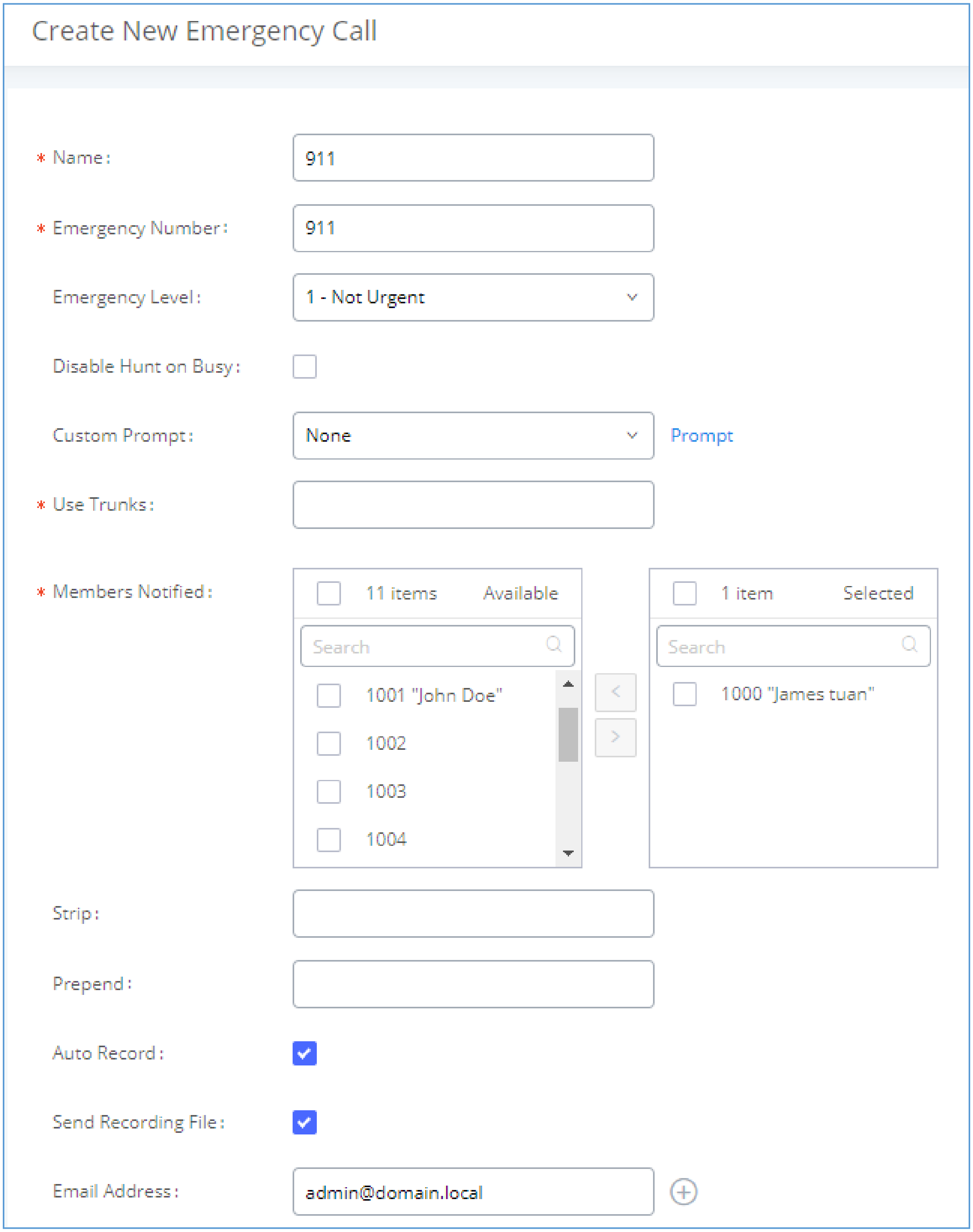


Figure 207: Emergency Number Configuration

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

Table 96: Emergency Numbers Parameters

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.
Members Notified	Select the members who will be notified when an emergency call occurs.
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.

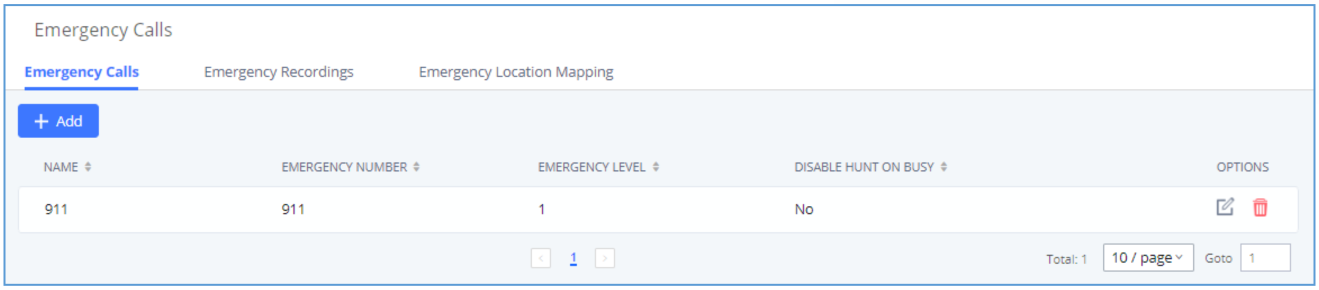


Figure 208: 911 Emergency Sample

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→**Call Features**→**Callback** page and click on + Create New Callback. Configuration parameters are listed in the following table.

Table 97: Callback Configuration Parameters

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.

BLF AND EVENT LIST

BLF

The UCM630X supports BLF monitoring for extensions, ring group, call queue, conference room and parking lot. For example, on the user's phone, configure the parking lot number 701 as the BLF monitored number. When there is a parked call on 701, the LED for this BLF key will light up in red, meaning a call is parked against this parking lot. Pressing this BLF key can pick up the call from this parking lot.

⚠ **Note:**

On the Grandstream GXP series phones, the MPK supports "Call Park" mode, which can be used to park the call by configuring the MPK number as call park feature code (e.g., 700). MPK "Call Park" mode can also be used to monitor and pickup parked call if the MPK number is configured as parking lot (e.g., 701).

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→**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.

Table 98: Event List Settings

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 UCM630X. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions/Extension Groups listed on the local UCM630X to be monitored in the event list.
Remote Extensions	If LDAP sync is enabled between the UCM630X and the peer UCM630X, 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

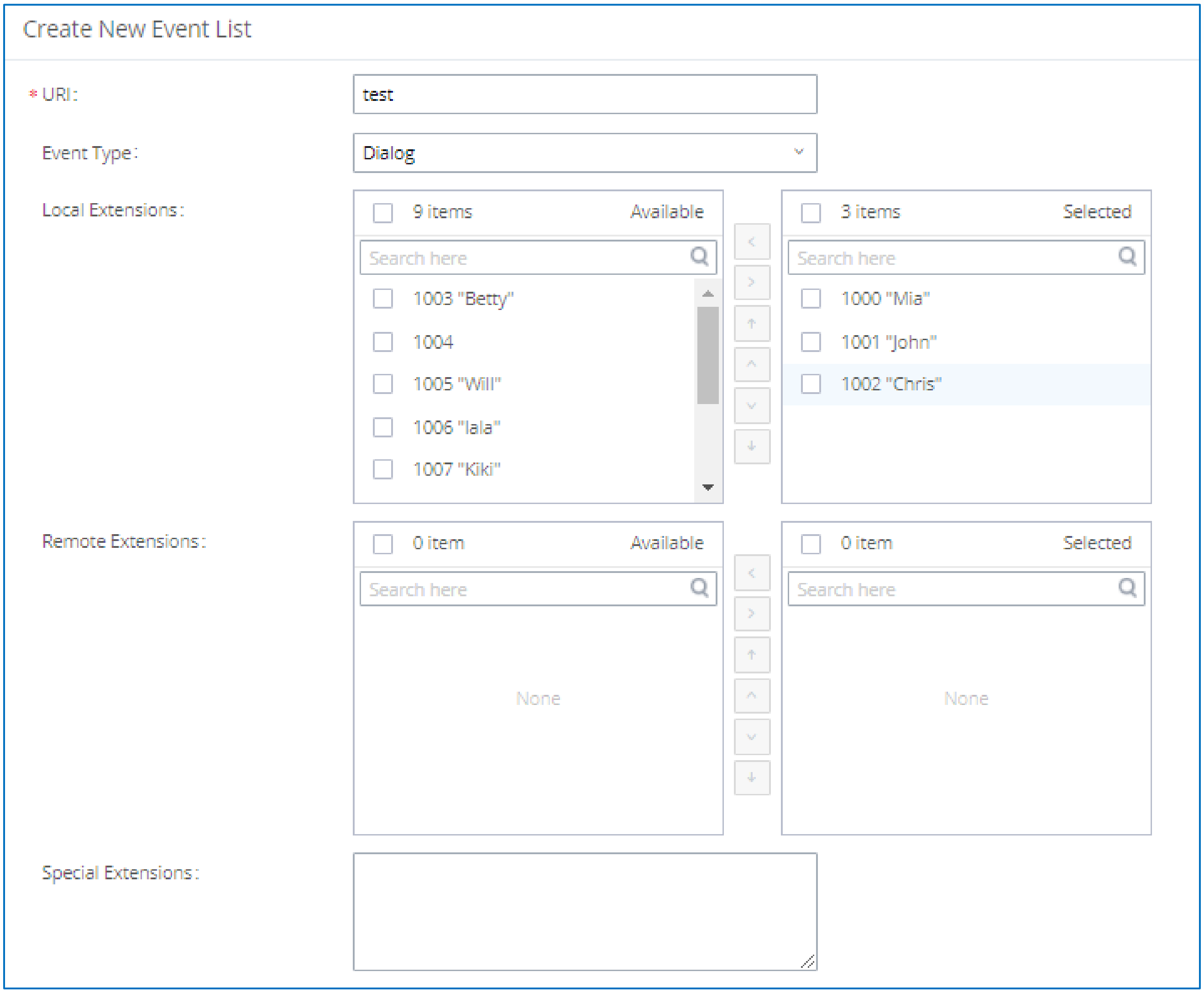


Figure 209: Create New Event List

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.

⚠ **Notes:**

- 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.

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→**Call Features**→**Dial By Name**.

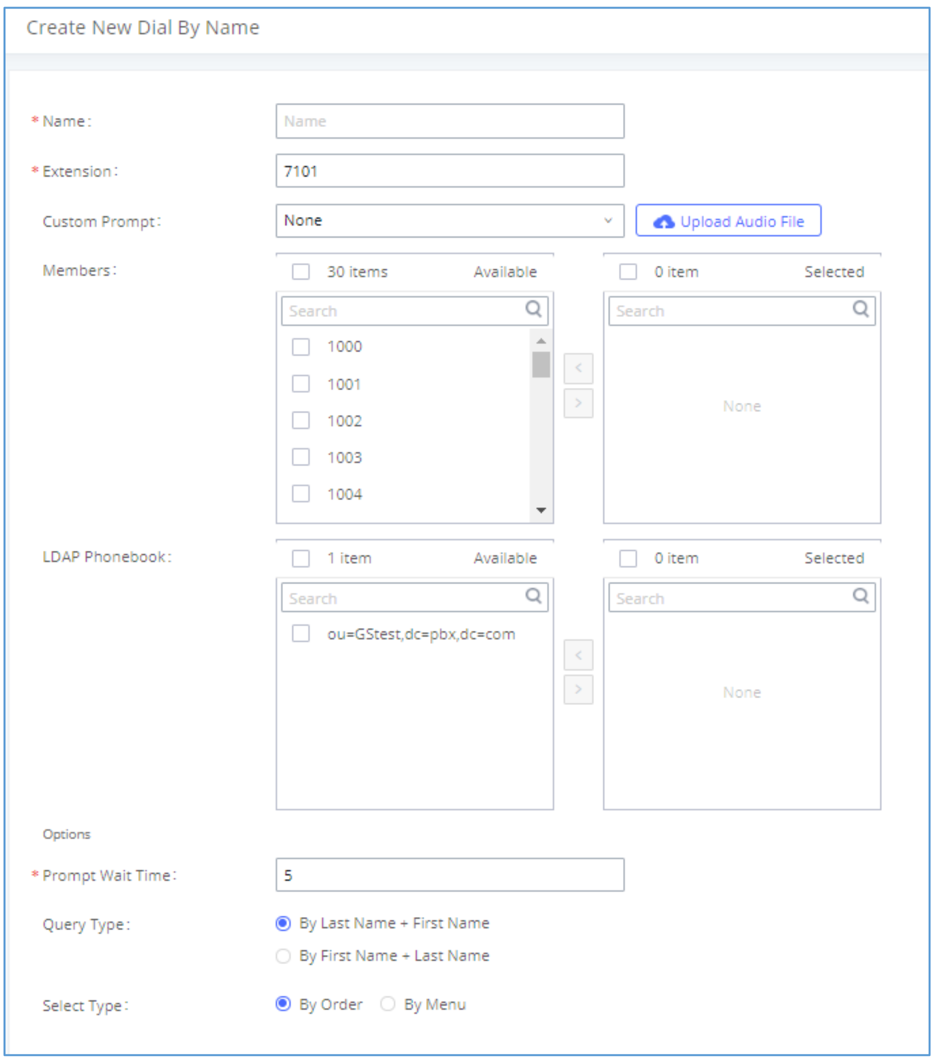


Figure 210: Create Dial by Name Group

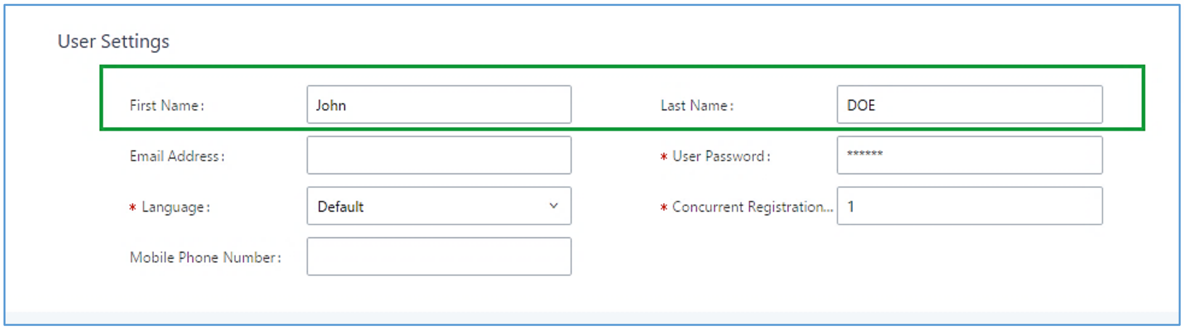


Figure 211: Configure Extension First Name and Last Name

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.
   <u>By First Name</u>: enter the first 3 digits of the first name to search the directory.
   <u>By Last Name</u>: 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.

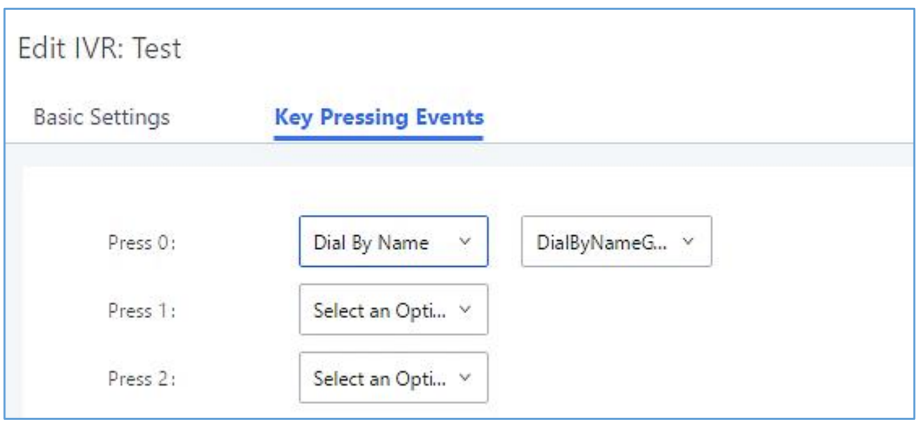


Figure 212: Dial By Name Group In IVR Key Pressing Events

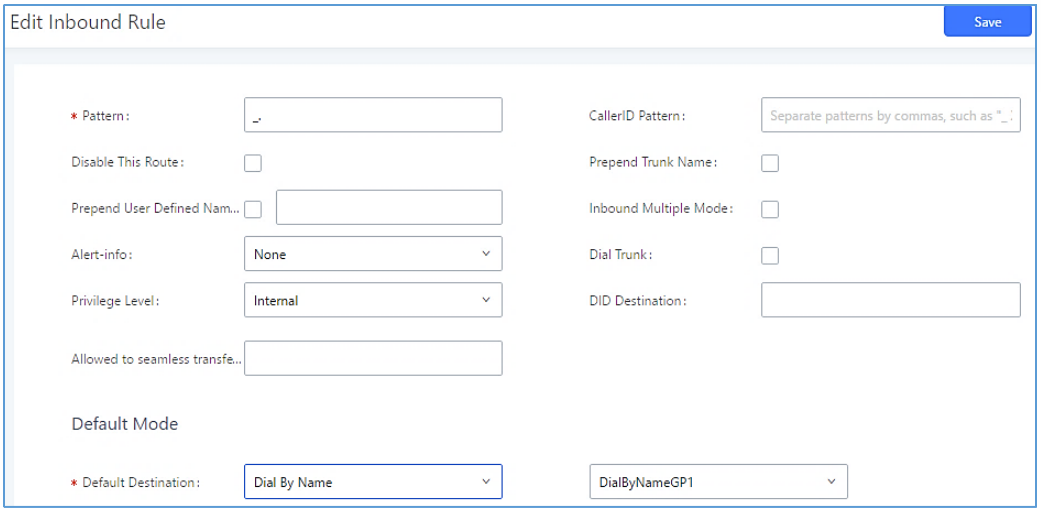


Figure 213: Dial By Name Group In Inbound Rule

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

ACTIVE CALLS AND MONITOR

The active calls on the UCM630X are displayed in Web GUI→**System Status**→**Active Calls** page. Users can monitor the status, hang up the call as well as barge in the active calls in real time manner.

Active Calls Status

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

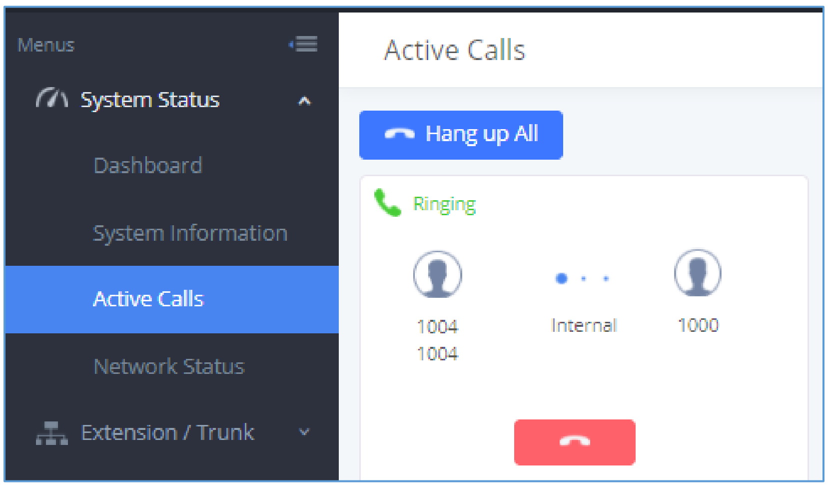


Figure 214: Status→PBX Status→Active Calls - Ringing

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

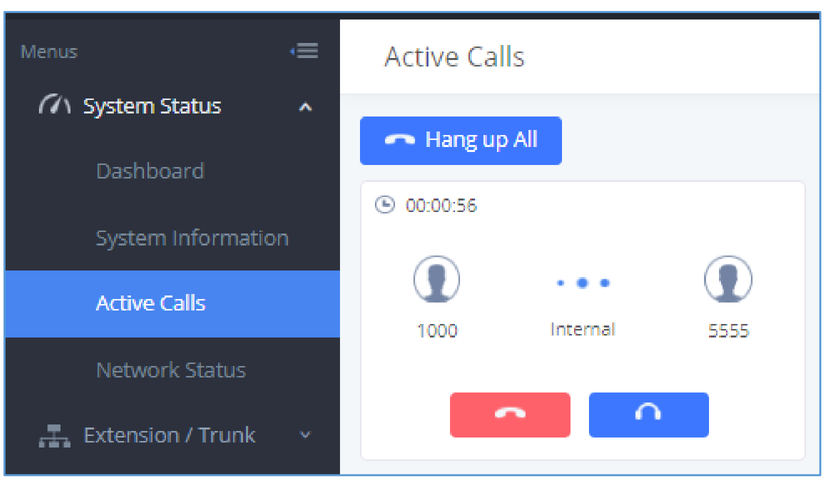


Figure 215: Status→PBX Status→Active Calls – Call Established

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.

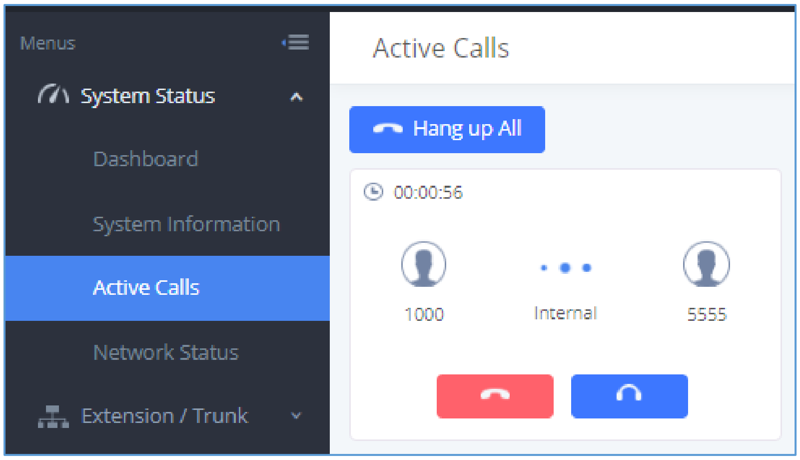


Figure 216: Call Connection less than half hour

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.

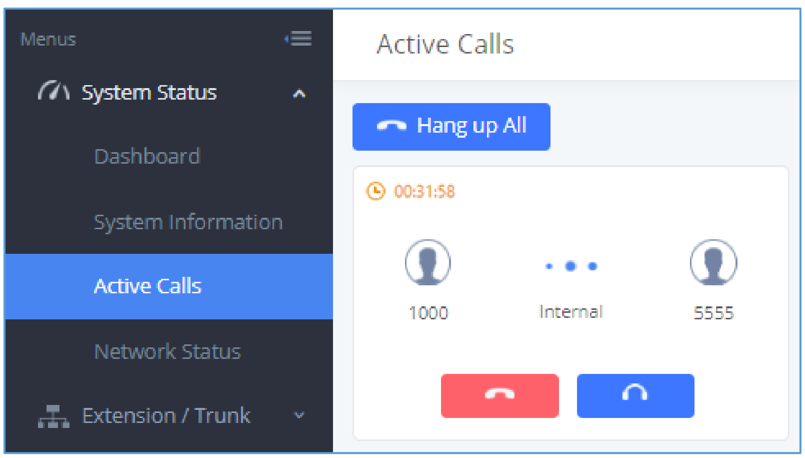


Figure 217: Call Connection between half an hour and one hour

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.

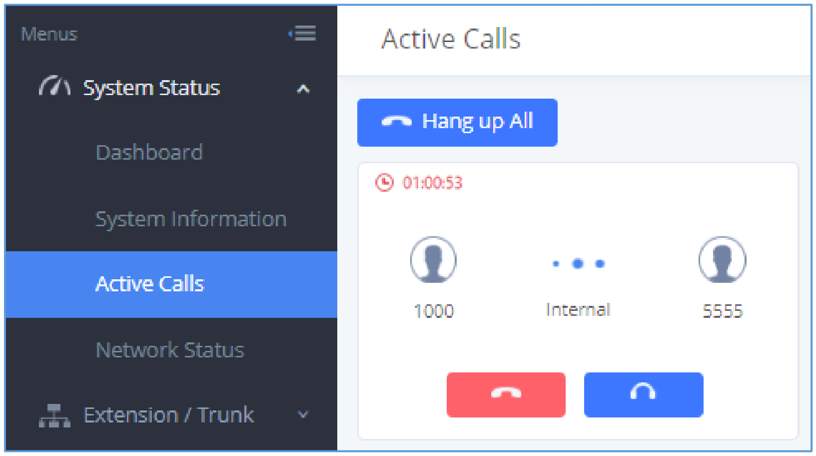


Figure 218: Call Connection more than one hour

Hang Up Active Calls

To hang up an active call, click on icon in the active call dialog. Users can also click on Hang up all to hang up all active calls.

Call Monitor

During an active call, click on icon and the monitor dialog will pop up.

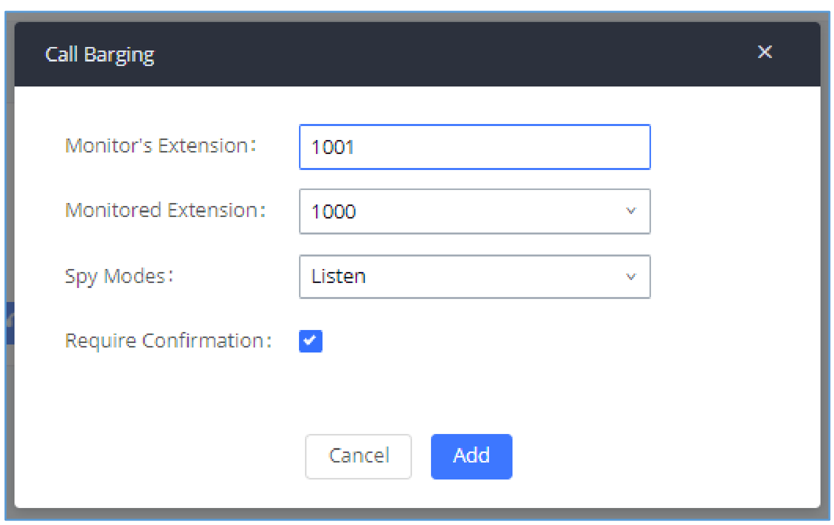


Figure 219: Configure to Monitor an Active Call

In the "Monitor" dialog, configure the following to monitor an active call:

1. Enter an available extension for "Monitor's Extension" which will be used to monitor the active call.

2. “Monitored Extension” must be one of the parties in the active call to be monitored.
3. Select spy mode. There are three options in “Spy Mode”.
   - **Listen**
     In “Listen” mode, the extension monitoring the call can hear both parties in the active call but the audio of the user on this extension will not be heard by either party in the monitored active call.
   - **Whisper**
     In “Whisper” mode, the extension monitoring the call can hear both parties in the active call. The user on this extension can only talk to the selected monitored extension and he/she will not be heard by the other party in the active call. This can be usually used to supervise calls.
   - **Barge**
     In “Barge” mode, the extension monitoring the call can talk to both parties in the active call. The call will be established similar to three-way conference.
4. Enable or disable “Require Confirmation” option. If enabled, the confirmation of the invited monitor’s extension is required before the active call can be monitored. This option can be used to avoid adding participant who has auto-answer configured, or call forwarded to voicemail.
5. Click on “Add”. An INVITE will be sent to the monitor’s extension. The monitor can answer the call and start monitoring. If “Require Confirmation” is enabled, the user will be asked to confirm to monitor the call.

Another way to monitor active calls is to dial the corresponding feature codes from an extension. Please refer to ***[Table 99: UCM630X Feature Codes]*** and [***Call Recording]*** section for instructions.

CALL FEATURES

The UCM630X supports call recording, transfer, call forward, call park and other call features via feature code. This section lists all the feature codes in the UCM630X and describes how to use the call features.

Feature Codes

Table 99: UCM630X Feature Codes

Feature Maps	
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.
Seamless Transfer	• Default code: ***44** (Disabled by default). • Seamless Transfer allows user to perform blind transfer using UCM 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.

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.
Start/Stop Call Recording	• Default code: ***3** • Enter the code followed by # or SEND to start recording the audio call and the UCM630X 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 Whitelist	Enable the Recording Whitelist feature
Recording Operation Whitelist	Select extension in the whitelist that can use the *3 recording function.
Feature Code Digits Timeout	Set the maximum interval (ms) between digits for feature code activation
DND/Call Forward	
Do Not Disturb (DND) Activate	• Default code: ***77**
Do Not Disturb (DND) Deactivate	• Default code: ***78**
Call Forward Busy Activate	• Default Code: ***90** • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.

Call Forward Busy Deactivate	• Default Code: ***91**
Call Forward No Answer Activate	• Default Code: ***92** • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward No Answer Deactivate	• Default Code: ***93**
Call Forward Unconditional Activate	• Default Code: ***72** • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward Unconditional Deactivate	• Default Code: ***73**
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.
Feature Codes	
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.
My Voicemai	• Default Code: ***97** • Press *97 to access the voicemail box.
Agent Pause	• Default Code: ***83** • Pause the agent in all call queues.
Agent Unpause	• Default Code: ***84** • Unpause the agent in all call queues.
Paging Prefix	• Default Code: ***81** • To page an extension, enter the code followed by the extension number.
Intercom Prefix	• Default Code: ***80** • To intercom an extension, enter the code followed by the extension number.
Blacklist Add	• Default Code: ***40** • To add a number to blacklist for inbound route, dial *40 and follow the voice prompt to enter the number.

Blacklist Remove	• Default Code: ***41** • To remove a number from current blacklist for inbound route, dial *41 and follow the voice prompt to remove the number.
Call Pickup on Ringing	• Default Code: ** • To pick up a call for any extension xxxx, enter the code followed by the extension number xxxx.
Pickup In-call	• Default Code: ***45** (Disabled by default). • If “Pickup In-call” feature is enabled, only the extensions added in “Allowed to seamless transfer” in the extension’s Seamless Transfer Privilege Control List” can pick up the call.
Pickup Extension	• Default Code: ***8** • This code is for the pickup group, which can be assigned for each extension on the extension configuration page. • If there is an incoming call to an extension, the other extensions within the same pickup group can dial *8 directly to pick up the call.
Direct Dial Voicemail Prefix	• Default Code: * • This code is for the user to directly dial or transfer to an extension's voicemail. • For example, directly dial *5000 will have to call go into the extension 5000's voicemail. If the user would like to transfer the call to the extension 5000's voicemail, enter *5000 as the transfer target number.
Direct Dial Mobile Phone Prefix	• Default Code: ***88** • If you have the permission to call mobile phone number, use this prefix plus the extension number can dial the mobile phone number of this extension directly.
Call Completion Request	• Default Code: ***11** • This code is for the user who wants to use Call Completion to complete a call.
Call Completion Cancel	• Default Code: ***12** • This code is for the user who wants to cancel Call Completion request.
Enable Spy	Check this box to enable spy feature codes. Disabled by default.

Listen Spy	• Default Code: ***54** ("Enable Spy" needs to be checked) • This is the feature code to listen in on a call to monitor performance. Monitor's line will be muted, and neither party will hear from the monitor's extension.
Whisper Spy	• Default Code: ***55** ("Enable Spy" needs to be checked) • This is the feature code to speak to one side of the call (for example, whisper to employees to help them handle a call). Only one side will be able to hear from the monitor's extension.
Barge Spy	• Default Code: ***56** ("Enable Spy" needs to be checked) • This is the feature code to join in on the call to assist both parties.
Wakeup Service	• Default Code: ***36** • Dial this code to access UCM wakeup service, you can add, update, activate or deactivate wakeup service.
PMS Wakeup Service	• Default Code: ***35** • Dial this code to access UCM PMS wakeup service, you can add, update, activate or deactivate PMS wakeup service.
PMS Remote Wakeup Service	• Default Code: ***37** • Allows the user to add, update, activate, and deactivate PMS wakeup service for other extensions.
Update PMS Room Status	• Default Code: ***23** • Use this code with maid code to update PMS room status. Choose the status to set after hearing the prompt, for example: for maid 001 dial *23001 and then 1 after hearing the prompt.
Presence Status	• Dial this code to set the presence status of the extension. • Possible options are: **1**:"unavailable" **2**:"available" **3**:"away" **4**:"chat" **5**:"dnd" **6**:"userdef"
Dynamic Agent Logout	• Default Code: *85 • Use this code to logout the dynamic agent from all queues.

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

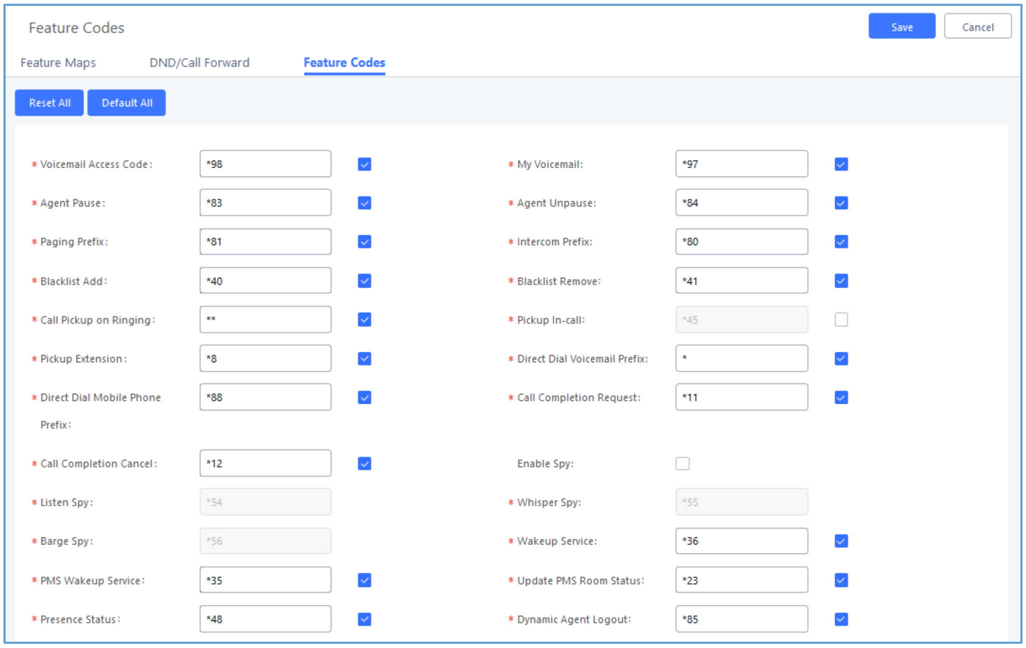


Figure 220: Enable/Disable Feature codes

Parking Lot

User can create parking lots and their related slots under Web GUI→ **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.

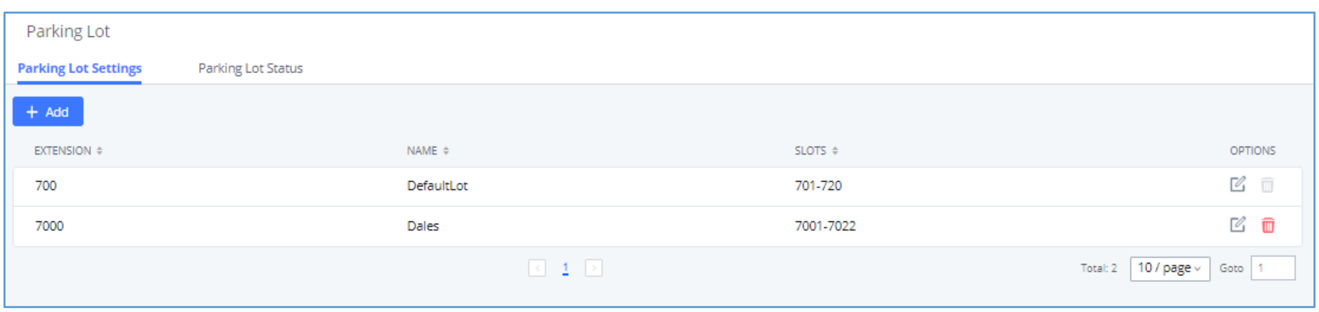


Figure 221: Parking Lot

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

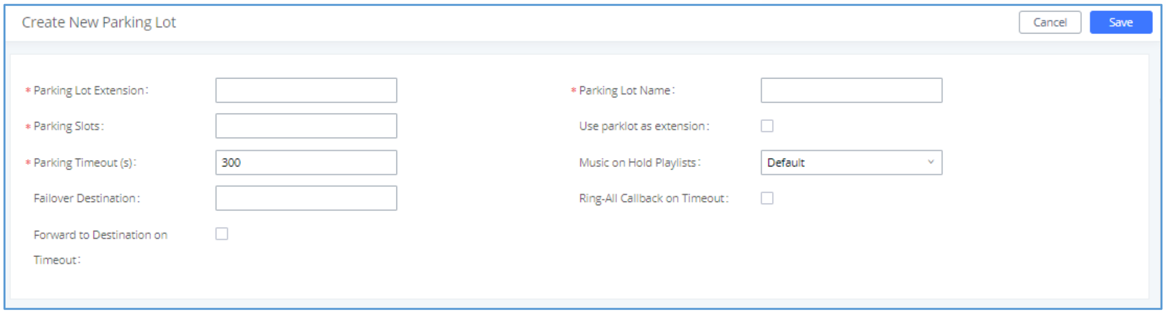


Figure 222: New Parking Lot

Table 100 : Parking Lot

Parking Lot Extension	• Default Extension: **700** • During an active call, initiate blind transfer and then enter this code to park the call.
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 Parklot 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.

.

Figure 223: Monitored Call Park CID name

Call Recording

The UCM630X allows users to record audio during the call. If "Auto Record" is turned on for an extension, ring group, call queue or trunk, the call will be automatically recorded when there is established call with it. Otherwise, please follow the instructions below to manually record the call.

1. Make sure the feature code for "Start/Stop Call Recording" is configured and enabled.
2. After establishing the call, enter the "Start/Stop Call Recording" feature code (by default it is *3) followed by # or SEND to start recording.
3. To stop the recording, enter the "Start/Stop Call Recording" feature code (by default it is *3) followed by # or SEND again. Or the recording will be stopped once the call hangs up.
4. The recording file can be retrieved under Web GUI→**CDR**. Click on to show and play the recording or click on to download the recording file.

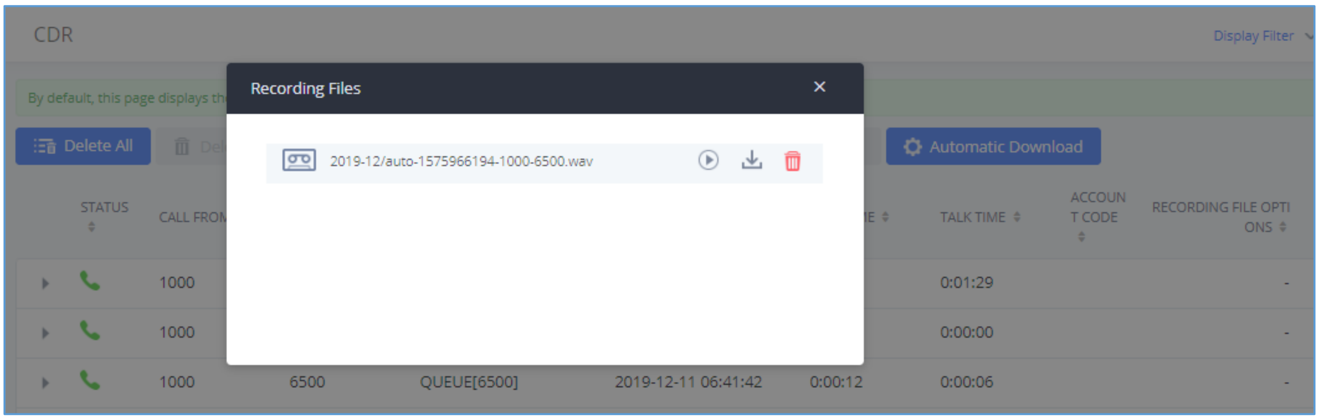


Figure 224: Download Recording File from CDR Page

The above recorded call's recording files are also listed under the UCM630X Web GUI→**CDR**→**Recording Files**.

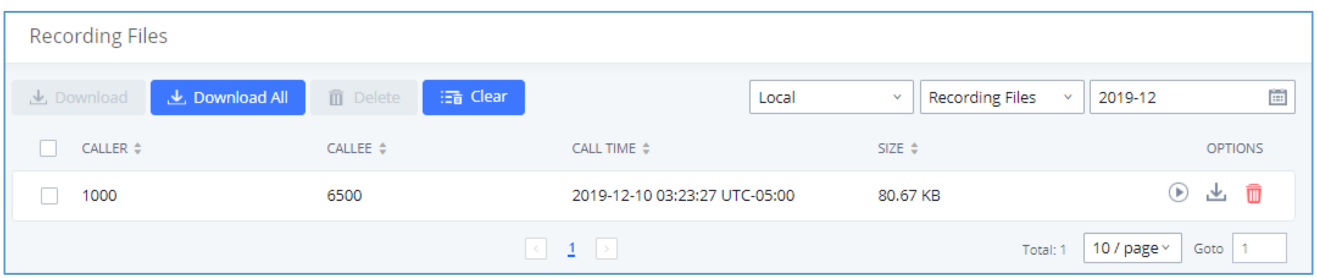


Figure 225: Download Recording File from Recording Files Page

Enable Spy

If “Enable Spy” option is enabled, feature codes for Listen Spy, Whisper Spy and Barge Spy are available for users to dial from any extension to perform the corresponding actions.

Assume a call is on-going between extension A and extension B, user could dial the feature code from extension C to listen on their call (*54 by default), whisper to one side (*55 by default), or barge into the call (*56 by default). Then the user will be asked to enter the number to call, which should be either side of the active call, extension A or B in this example.

⚠ **Caution:**

"Enable Spy" allows any user to listen to any call by feature codes. This may result in the leakage of user privacy.

Shared Call Appearance (SCA)

Shared Call Appearance (SCA) 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.

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

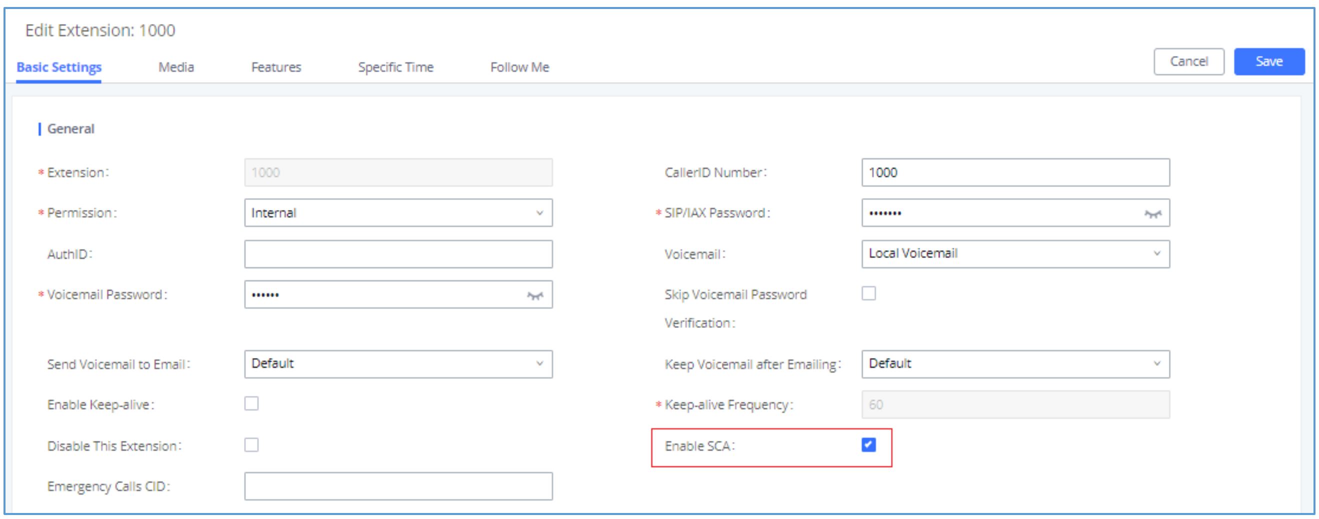


Figure 226: Enabling SCA option under Extension's Settings

2. After enabling the option, navigate to *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.

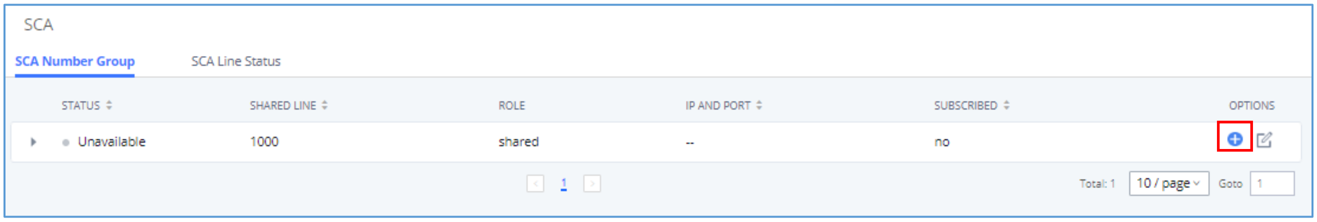


Figure 227: SCA Number Configuration

3. Configure the private number as desired.

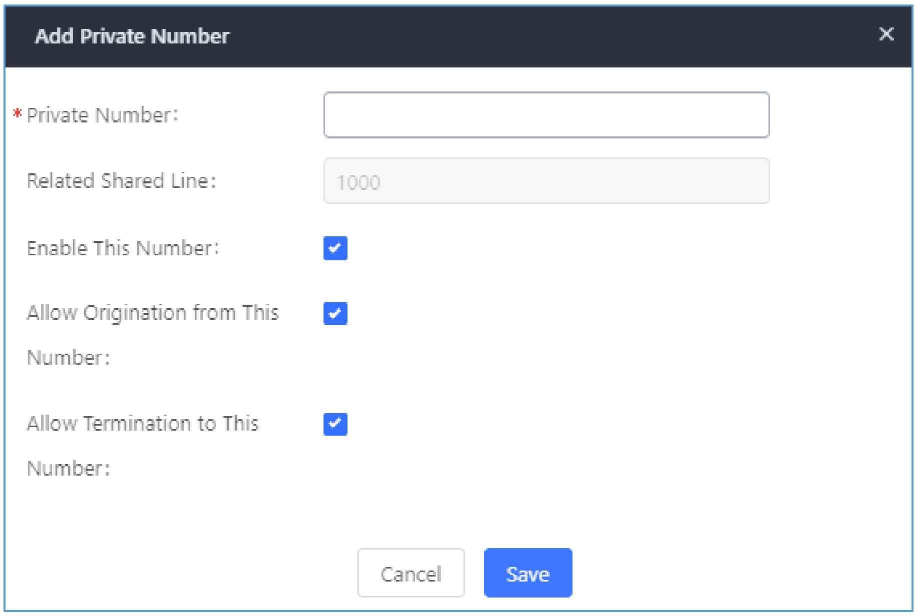


Figure 228: SCA Private Number Configuration

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.

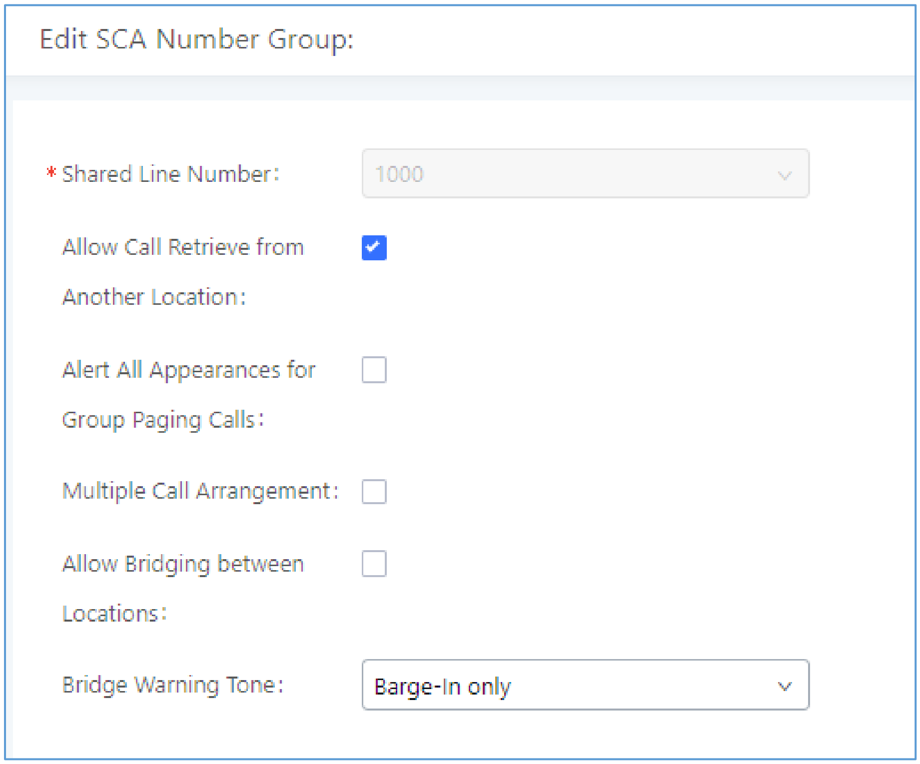


Figure 229: SCA Options

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:

Table 101: Add SCA Private Number

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 feature.
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.

The following table describes the options available when editing the SCA number:

Table 102: Editing the SCA Number

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. By default, it is set to “Barge-In Only”.

ANNOUNCEMENT

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

To configure Announcement, users need to follow below steps:

1. Navigate on the web GUI under “Call Features → Announcement”
2. Click on + Add to add a new Announcement.
3. Configure the required fields Name, Prompt, Default Destination to be used for the announcement.

Save and apply the configuration.

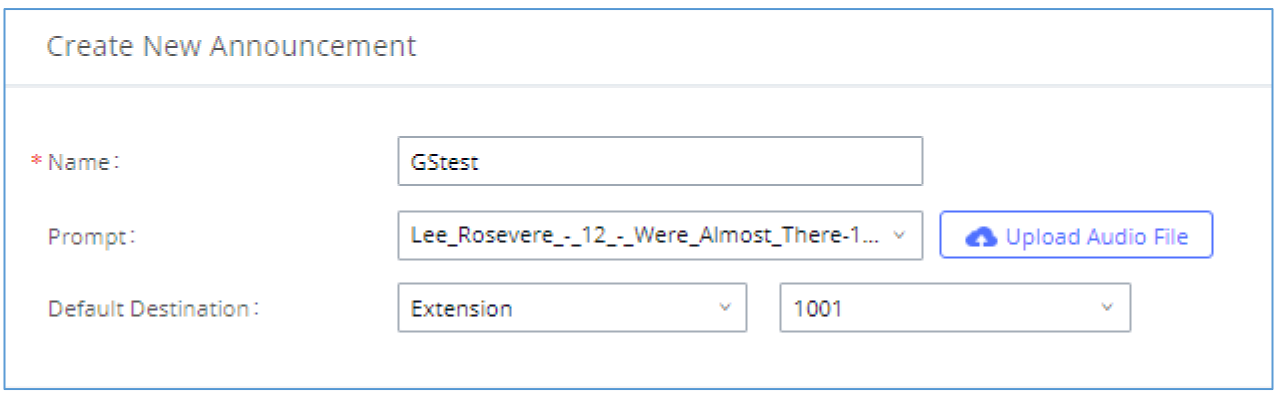


Figure 230: Announcement settings

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

Table 103: Announcement Parameters

Name	Configure the name of the Announcement.
Prompt	Audio file that needs to be uploaded in order to be played for a specific destination.
Default Destination	Select the destination where to play the audio file.

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 Web GUI→**PBX Settings→General Settings.**

PBX Settings/General Settings

Table 104: Internal Options/General

General Preferences	
Global Outbound CID	Configure the global CallerID used for all outbound calls when no other CallerID is defined with higher priority. If no CallerID is defined for extension or trunk, the global outbound CID will be used as CallerID.
Global Outbound CID Name	Configure the global CallerID Name used for all outbound calls. If configured, all outbound calls will have the CallerID Name set to this name. If not, the extension's CallerID Name will be used.
Ring Timeout	Configure the number of seconds to ring an extension before the call goes to the user's voicemail box. The default setting is 60. **Note:** This is the global value used for each extension if "Ring Timeout" field is left empty on the extension configuration page.
Call Duration Limit	Configure the maximum duration of call-blocking.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit.
Warning Time (s)	The amount of seconds before the maximum call duration is reached to play the warning tone to the caller.
Warning Repeat Interval (s)	The amount of seconds that must pass after the first warning tone before another warning tone is played.
Enable 486 to Failover Trunk	Reroutes failed outbound calls that receive a 486 response through the failover trunk to retry the call. If disabled, calls that receive a 486 response will be terminated.
Record Prompt	If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the UCM630X will play voice prompt "The call will be recorded". The default setting is "No".
Device Name	The name of the UCM you are using.

International Call Prefix	When this configuration is empty, International Call Prefix can be empty or +.
Conference Max Concurrent Audio	Maximum number of participants that can be heard simultaneously in audio/video conferences. If the number of participants talking at any given point exceeds this value, the audio of the excess participants will not be heard.
Conference Voice Indicator Sensitivity	Configures the sensitivity of the talking indicator in conferences. Setting this higher will make the talking indicator appear more easily for lower volumes of audio. Note: This does not adjust audio input sensitivity itself. Lower volumes of sounds may still be heard even if the talking indicator does not show the source.
Conference Voice Quality	Voice quality of audio and video conferences
Extension Preferences	
Enforce Strong Passwords	If enabled, strong password will be enforced for the password created on the UCM630X. The default setting is "No". Strong Password Rules: 1. Password for voicemail, voicemail group, outbound route, DISA, call queue and conference require non-repetitive and non-sequential digits, with a minimum length of 4 digits. Repetitive digits pattern (such as 0000, 1111, 1234, 2345, and etc.), or common digits pattern (such as 111222, 321321 and etc.) are not allowed to be configured as password. 2. Password for extension registration, Web GUI admin login, LDAP and LDAP sync requires alphanumeric characters containing at least two categories of the following, with a minimum length of 4 characters. • Numeric digits • Lowercase alphabet characters • Uppercase alphabet characters • Special characters
Enable Random Password	If enabled, random password will be generated when the extension is created. The default setting is "Yes". It is recommended to enable it for security purpose.
Enable Auto E-mail To User	If enabled, UCM630X will send Email notification to user automatically after editing extension settings or adding a new extension.

Disable Extension Range	If set to "Yes", users could disable the extension range pre-configured/configured on the UCM630X. The default setting is "No". **Note:** It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.
Extension Ranges	The default extension range assignment is: • User Extensions: 1000-6299 User Extensions is referring to the extensions created under Web GUI→**Extension/Trunk**→**Extensions** page. • Pick Extensions: 4000-4999 This refers to the extensions that can be manually picked from end device when being provisioned by the UCM630X. There are two related options in zero config page→Zero Config Settings, "Pick Extension Segment" and "Enable Pick Extension". If "Enable Pick Extension" under zero config settings is selected, the extension list defined in "Pick Extension Segment" will be sent out to the device after receiving the device's request. This "Pick Extension Segment" should be a subset of the "Pick Extensions" range here. This feature is for the GXP series phones that support selecting extension to be provisioned via phone's LCD. • Auto Provision Extensions: 5000-6299 This sets the range for "Zero Config Extension Segment" which is the extensions can be assigned on the UCM630X to provision the end device. • Conference Extensions: 6300-6399 • Ring Group Extensions: 6400-6499 • Queue Extensions: 6500-6599 • Voicemail Group Extensions: 6600-6699 • IVR Extensions: 7000-7100 • Dial By Name Extensions: 7101-7199

PBX Settings/RTP Settings

RTP Settings

Table 105: Internal Options/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".
ICE Support	Configure whether to support ICE. The default setting is enabled. ICE is the integrated use of STUN and TURN structure to provide reliable VoIP or video calls and media transmission, via a SIP request/ response model or multiple candidate endpoints exchanging IP addresses and ports, such as private addresses and TURN server address.
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.
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.
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.

Payload

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

Table 106: Internal Options/Payload

AAL2-G.726	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112.
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.
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
H.264	Configure the payload type for H.264. The default setting is 99.
H.265	Configure the payload type for H.264. 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.
Main Video FEC	Configure the Main Video FEC
RTP FECC	Configure the RTP FECC
RTX	Configure the RTX
G.722.1	G.722.1：Low-complexity coder, 24kbps.
G.722.1C	G.722.1C：Low-complexity coder, 48kbps.

PBX Settings/Voice Prompt Customization

Record New Custom Prompt

In the UCM630X Web GUI→**PBX Settings**→**Voice Prompt**→**Custom Prompt** page, click on “Record” and follow the steps below to record new IVR prompt.

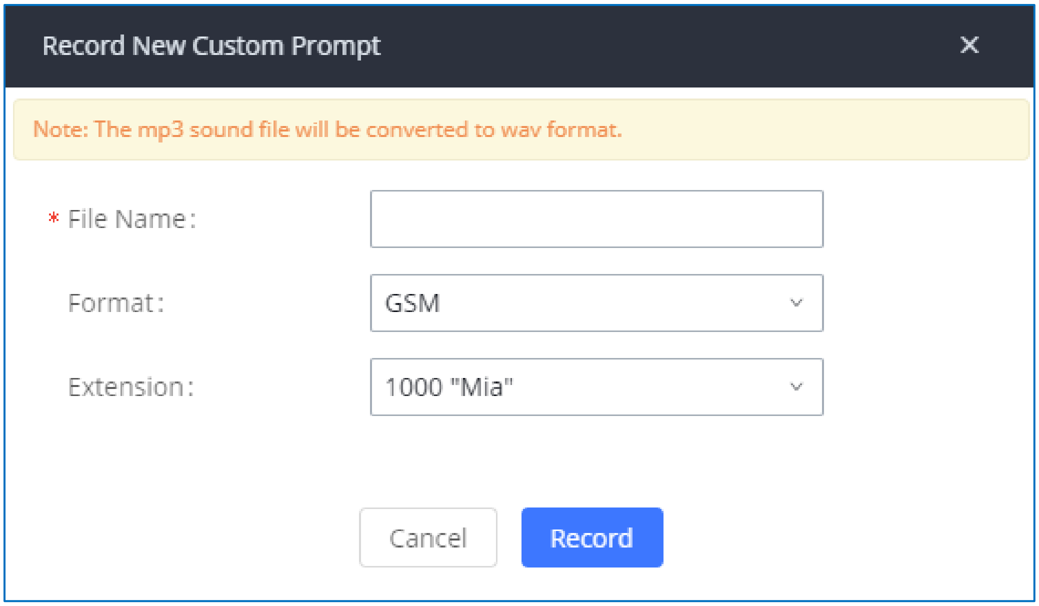


Figure 231: Record New Custom Prompt

1. Specify the IVR file name.
2. Select the format (GSM or WAV) for the IVR prompt file to be recorded.
3. Select the extension to receive the call from the UCM630X to record the IVR prompt.
4. Click the "Record" button. A request will be sent to the UCM630X. The UCM630X will then call the extension for recording the IVR prompt from the phone.
5. Pick up the call from the extension and start the recording following the voice prompt.
6. The recorded file will be listed in the IVR Prompt web page. Users could select to re-record, play, or delete the recording.

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 5M.

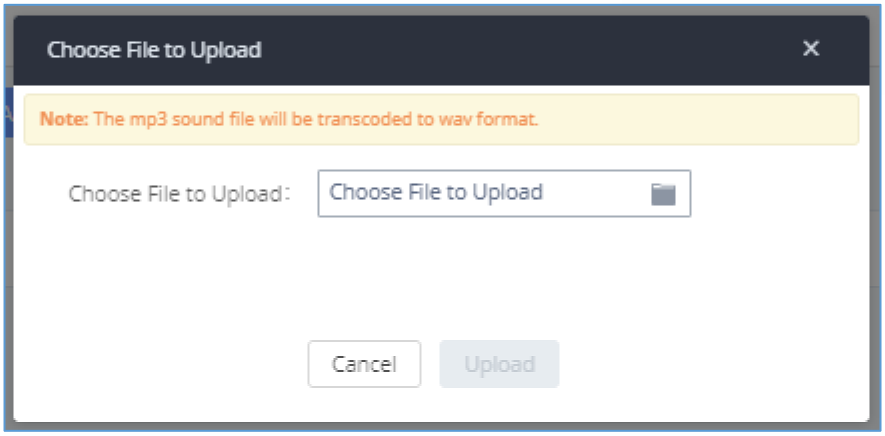


Figure 232: Upload Custom Prompt

Click on "choose file to upload" to start uploading. Once uploaded, the file will appear in the Custom Prompt web page.

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.

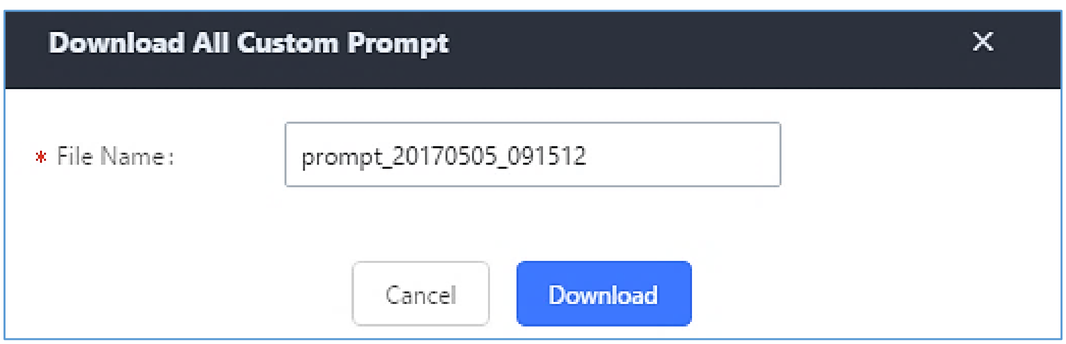


Figure 233: Download All Custom Prompt

Note: The downloaded file will have a .tar extension.

PBX Settings/ Call Failure Tone Settings

SIP Trunk Prompt Tone

Prompt Tone Settings tab has been added to the UCM to help users choose which prompt will be played by the UCM during call failure, the following voice message responses have been added and can be set to be played for 4XX, 5XX, and 6XX call failures:

- Default for 404 and 604 status codes: **"***Your call can't be completed as dialed. Please check the number and dial again.***"**
- Default for 5xx status codes: **"***Server error. Please check your device*.**"**
- Default for 403 and 603 status codes: **"***The call was rejected by the server. Please try again later.***"**
- Default for all other status codes: **"***All circuits are busy now. Please try again later*.**"**

Additionally, custom voice messages recorded and uploaded in **PBX Settings→Voice Prompt→Custom Prompt** can be used for these failure responses instead of the default messages.

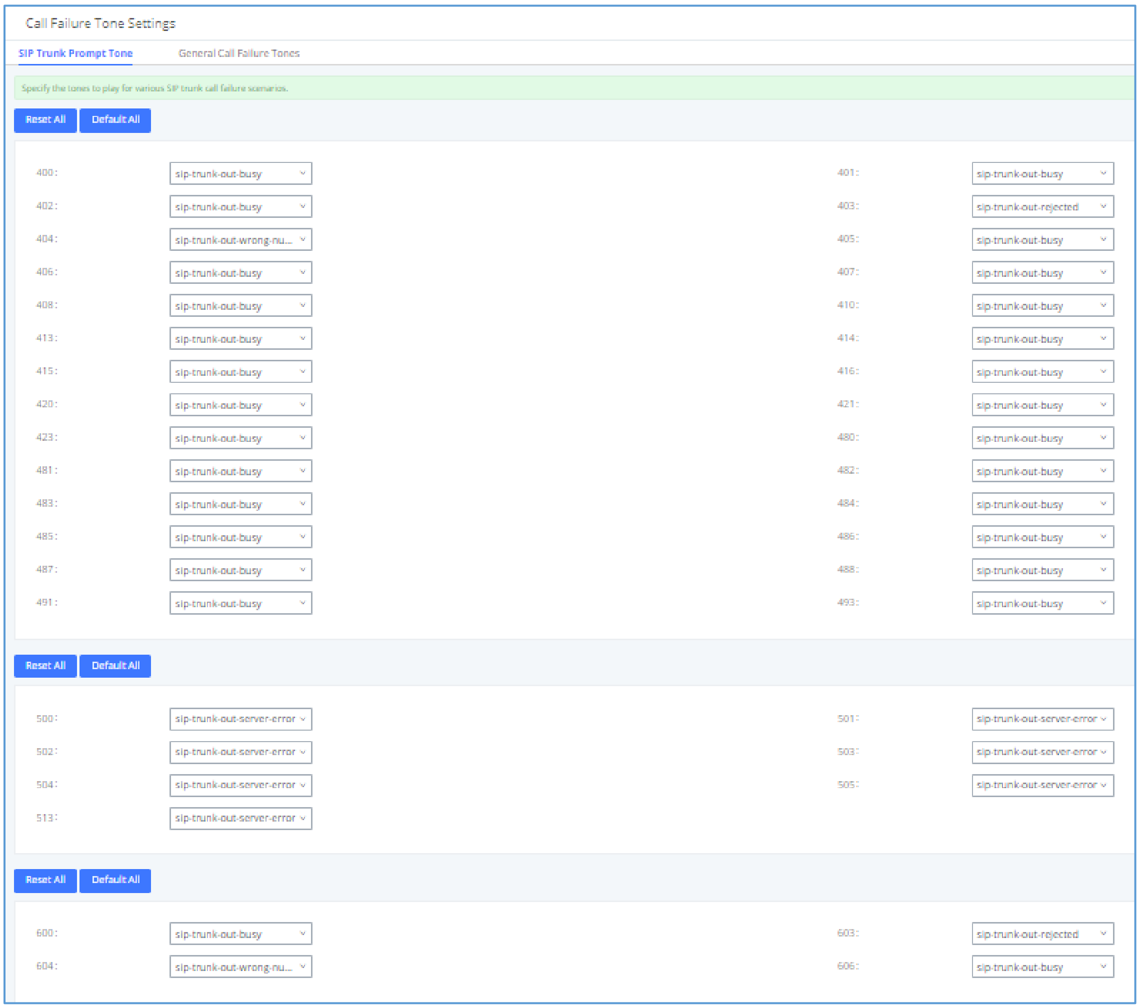


Figure 234: SIP Trunk Prompt Tone

General Call Prompt Tone

Moreover, users also have the possibility to customize the prompt for typical call failure reasons like (no permission to allow outbound calls, busy lines, incorrect number dialed …Etc.).

To customize these prompts user could record and upload their own files under "'**PBX Settings → Voice Prompt → Custom Prompts**" then select each one for specific call failure case under "**PBX Settings** -> **Call Failure Tone Settings → General Call Prompt Tone**" page as shown on the following figure:

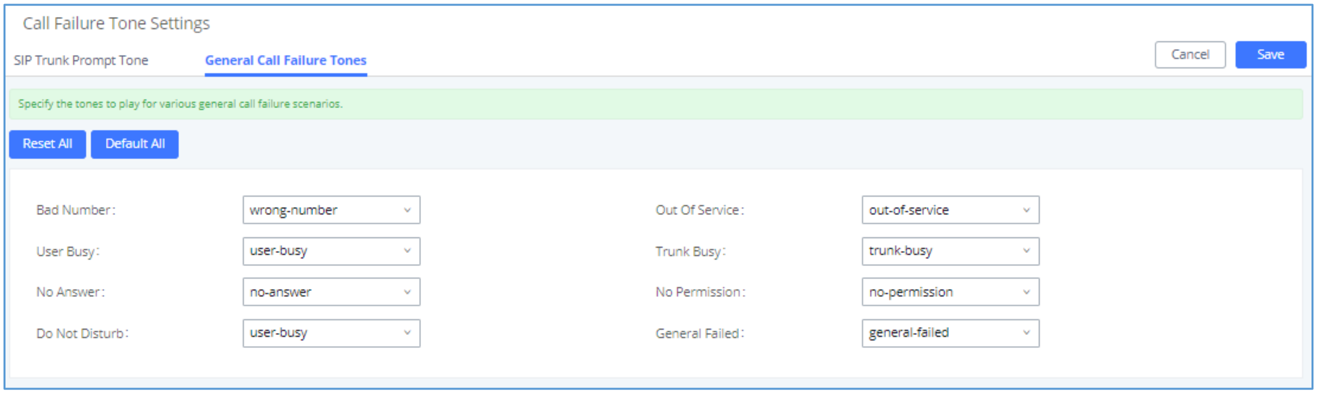


Figure 235: General call Failure Prompts

PBX Settings/Recordings Storage

The UCM630X supports call recordings automatically or manually and the recording files can be saved in external storage plugged in the UCM630X or on the UCM630X locally. To manage the recording storage, users can go to UCM630X Web GUI→**PBX Settings→Recordings Storage** page and select whether to store the recording files in USB Disk, SD card, GDMS or locally on the UCM630X.

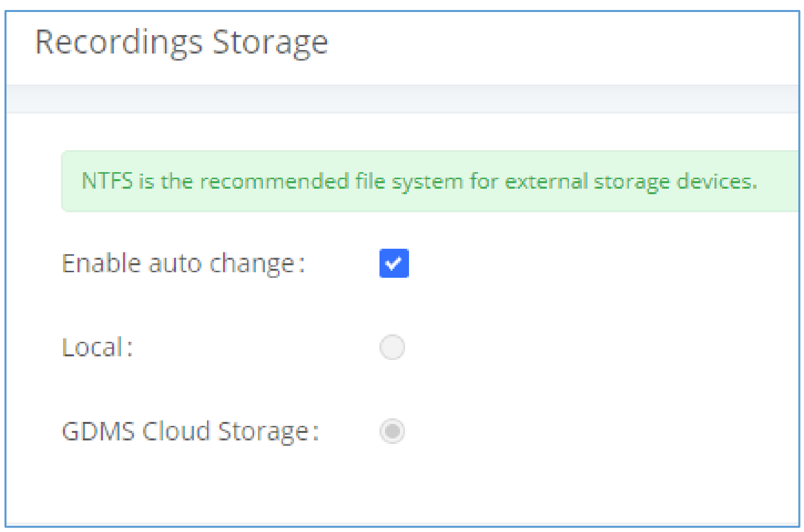


Figure 236: Settings→Recordings Storage

- If "**Enable Auto Change**" is selected, the recording files will be automatically saved in the available USB Disk or SD card plugged into the UCM630X. If both USB Disk and SD card are plugged in, the recording files will be always saved in the USB Disk.

- If "**Local**" is selected, the recordings will be stored in UCM630X internal storage.

- If "**GDMS Cloud Storage**" is selected, recording data will no longer be stored locally and if you need to listen to the recording, download the recording file to the computer side and play it offline.

- If "**USB Disk**" or "**SD Card**" is selected, the recordings will be stored in the corresponding plugged in external storage device. Please note the options "USB Disk" and "SD Card" will be displayed only if they are plugged into the UCM630X.
  Once "USB Disk" or "SD Card" is selected, click on "OK". The user will be prompted to confirm to copy the local files to the external storage device.

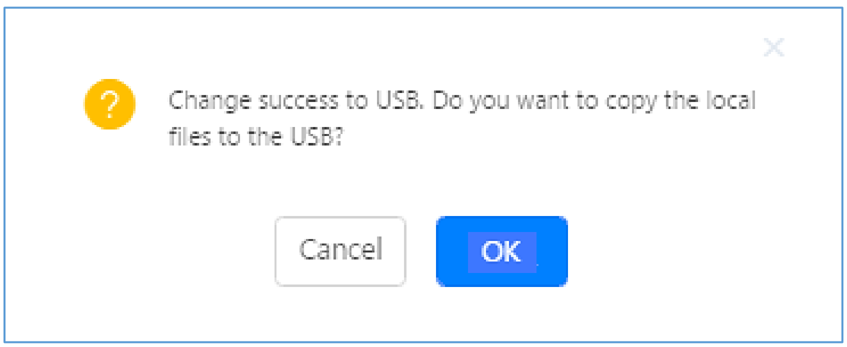


Figure 237: Recordings Storage Prompt Information

Click on "OK" to continue. The users will be prompted a new dialog to select the categories for the files to be copied over.

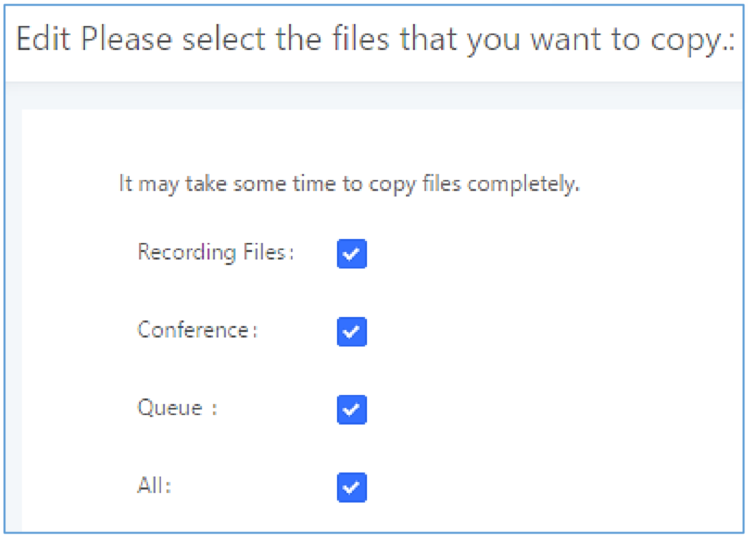


Figure 238: Recording Storage Category

On the UCM630X, recording files are generated and exist in 3 categories: normal call recording files, conference recording files, and call queue recording files. Therefore, users have the following options when select the categories to copy the files to the external device:

- **Recording Files**: Copy the normal recording files to the external device.
- **Conference**: Copy the conference recording files to the external device.
- **Queue**: Copy the call queue recording files to the external device.
- **All**: Copy all recording files to the external device.

PBX Settings/NAS

The UCM supports adding and backing up recordings to a network-attached storage (NAS) server. Following table describes NAS settings:

Table 107: NAS Settings

Enable	Enabled / Disable the NAS recording functionality.
Host	Configure the Domain or IP address of the NAS server. **Note**: Currently, only IP addresses are supported in the Host/IP field.
Share Name	Specify the name of the shared folder.
Username	Specify the account username to access the NAS server.
Password	Configure the account password to access the NAS server.
Status	If configured correctly, the Status field will show “Mounted”, and the newly

	added NAS server will be shown on the Mounted Netdisk List. Additionally, the NAS will appear as a selectable storage option in the PBX Settings→Recording Storage page and CDR→Recording Files page.

SIP SETTINGS

The UCM630X SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

SIP Settings/General

Table 108: SIP Settings/General

Realm For Digest Authentication	Configure the host name or domain name for the UCM630X. Realms MUST be globally unique according to RFC3261. The default setting is Grandstream.
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. The default setting is 0.0.0.0, which means binding to all addresses.
Bind IPv6 Address	Configure the IPv6 address to bind to. The default is : "[::]" and it means to bind to all IP addresses.
Allow Guest Calls	If enabled, the UCM630X allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is "No". **Warning:** Please be aware of the potential security risk when enabling "Allow Guest Calls" as this will allow any user with the UCM630X address to dial into the UCM630X.
Allow Transfer	If set to "No", all transfers initiated by the endpoint in the UCM630X will be disabled (unless enabled in peers or users). The default setting is "Yes".
MWI From	When sending MWI NOTIFY requests, this value will be used in the "From:" header as the "name" field. If no "From User" is configured, the "user" field of the URI in the "From:" header will be filled with this value.
Enable Diversion Header	If disabled, the UCM will not forward the diversion header.
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".

SIP Settings/MISC

Table 109: SIP Settings/Misc

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.
Video	
Max Bit Rate (kb/s)	Configure the maximum bit rate (in kb/s) for video calls. The default setting is 384.
Support SIP Video	Select to enable video support in SIP calls. The default setting is "Yes".
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. The default setting is "No".
SDP Attribute Passthrough	
Enable Attribute Passthrough	If enable, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passthrough.
Early Media	
Enable Use Final SDP	If enabled, call negotiation will use final response SDP.
Blind Transfer	
Allow callback 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.
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.

SIP Settings/Session Timer

Table 110: SIP Settings/Session Timer

Force Timer	If checked, always request, and run session timer.
Timer	If checked, run session timer only when requested by other UA.
Session Expire	Configure the maximum session refresh interval (in seconds). Default is 1800.
Min SE	Configure the minimum session refresh interval (in seconds). The default setting is 90.

SIP Settings/TCP and TLS

Table 111: SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the UCM630X. The default setting is "No".
TCP Bind IPv4 Address	Configure the IP address for 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 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.
TLS Enable	Configure to allow incoming TLS connections with the UCM630X. 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.
TLS Do Not Verify	If enabled, the TLS server's certificate will not be verified when acting as a client. The default setting is "Yes".
TLS Self-Signed CA	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. **Note:** The size of the uploaded ca file must be under 2MB.
TLS Cert	This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as "TLS.pem" automatically. **Note:** The size of the uploaded certificate file must be under 2MB.
TLS CA Cert	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. **Note:** The size of the uploaded CA certificate file must be under 2MB.
TLS CA List	Display a list of files under the CA Cert directory.

SIP Settings/NAT

Table 112: SIP Settings/NAT

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.
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	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

SIP Settings/TOS

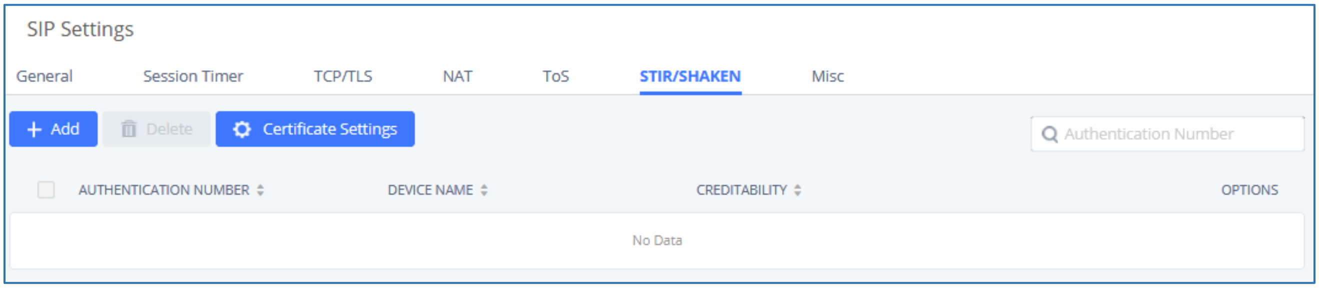
Table 113: SIP Settings/ToS

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.

Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".
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	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	Passthrough PAI Header

SIP Settings/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:

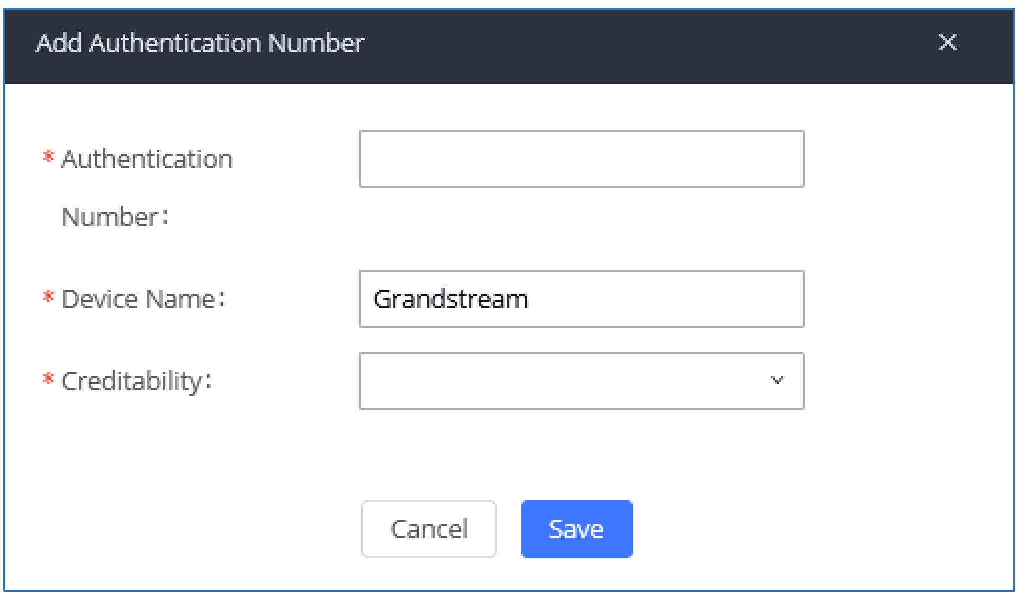


Figure 239:SIP Settings/STIR/SHAKEN - Add Authentication Number

Table 114: SIP Settings/STIR/SHAKEN - Add Authentication Number Settings

Authentication Number	Configure the Authentication Number.
Device Name	Configure the device name.
Creditability	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:

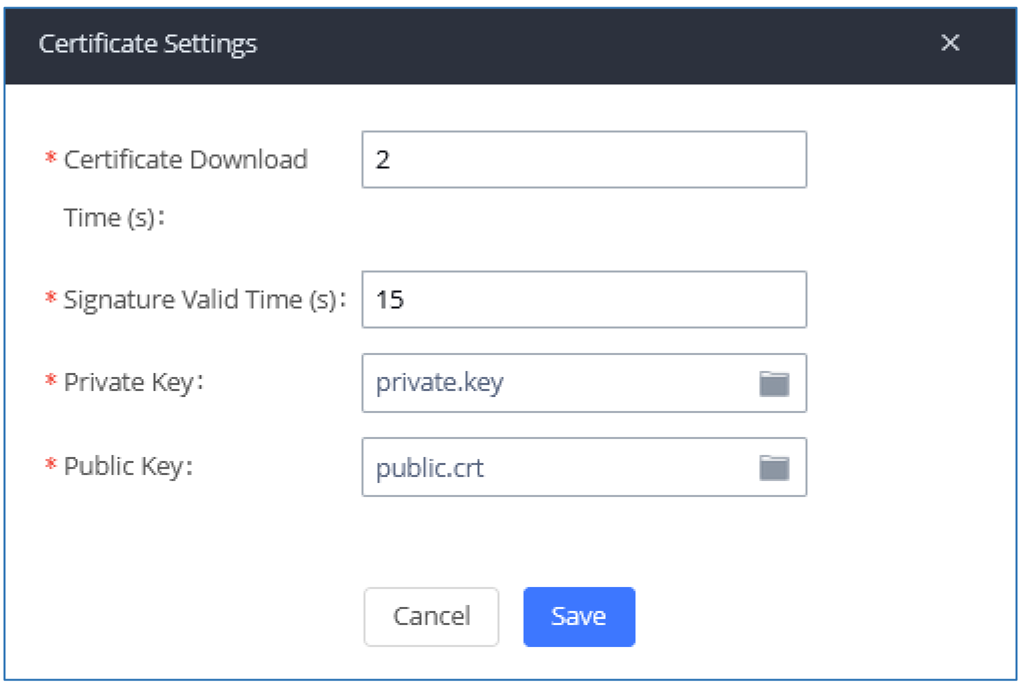


Figure 240: SIP Settings/STIR/SHAKEN – Certificate Settings

Table 115: SIP Settings/STIR/SHAKEN – Certificate Settings

Certificate Download Time (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.

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".
Public Key	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".

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.

Figure 241: Transparent Call-Info

IAX SETTINGS

The UCM630X IAX global settings can be accessed via Web GUI→**PBX Settings**→**IAX Settings**.

IAX Settings/General

Table 116: IAX Settings/General

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".
ADSI	Select to enable ADSI phone compatibility. The default setting is "No".
Music On Hold Interpret	Specify which Music On Hold class this channel would like to listen to when being put on hold. This music class is only effective if this channel has no music class configured and the bridged channel putting the call on hold has no "Music On Hold Suggest" setting.
Music On Hold Suggest	Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold.
Bandwidth	Configure the bandwidth for IAX settings. The default setting is "Low".

IAX Settings/Registration

Table 117: IAX Settings/Registration

IAX Registration Options	
Min Reg Expire	Configure the minimum period (in seconds) of registration. The default setting is 60.
Max Reg Expire	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.
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 Trunk Options	
Trunk Frequency	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 Settings/Security

Table 118: IAX Settings/Static Defense

Call Token Optional	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.
Max Unvalidated Call Numbers	Configure the maximum number of Unvalidated calls for all IP addresses.
Max Call Numbers	Configure to limit the number of calls for a give IP address of IP range.
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.

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.

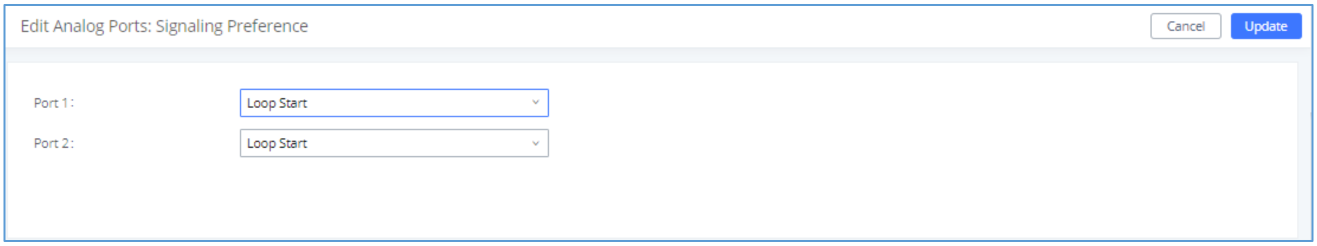


Figure 242: FXS Ports Signaling Preference

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.

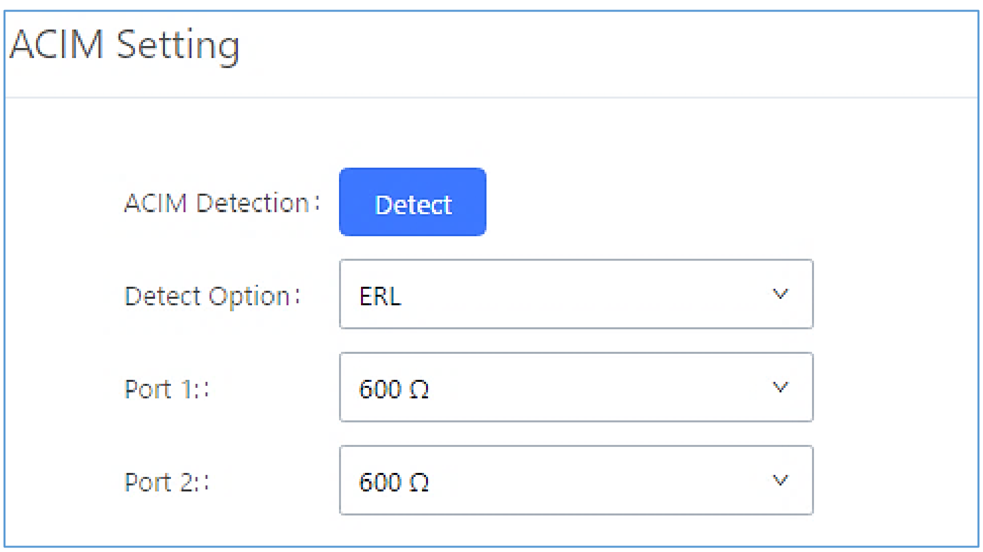


Figure 243: FXO Ports ACIM Settings

Table 119: PBX Interface 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 600Ω.
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.

DAHDI Settings

When users encounter issues such as audio delay in outbound calls using the analog trunk, they can adjust DAHDI settings on the UCM to attempt to lessen or resolve the issues.

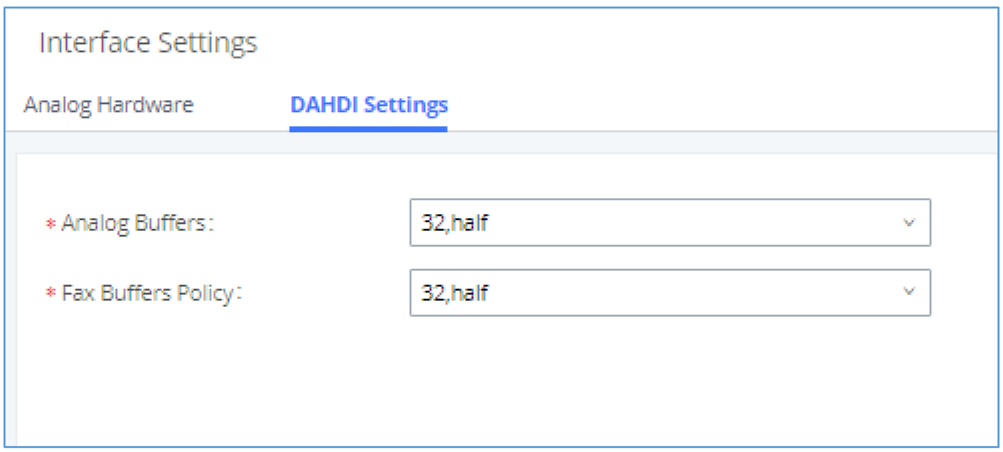


Figure 244: DAHDI Settings

For the value of the option such as “32, half”:
The number in the option indicates the number of read/write buffers for TDM (DAHDI).
The “Half”, “Immediate” or “Full” option indicates the strategy when reading/writing data from buffer.

- “**Half**”: Data will be read/written from buffer when half of the buffer is occupied with data.
- “**Immediate**”: Read/write from buffer whenever there is data occupying the buffer.
- “**Full**”: Data will be read/written from buffer when buffer is fully occupied with data.

Normally, DAHDI settings should be kept default and should be adjusted only when users encounter analog trunk/Fax-related issues.

UCM RemoteConnect

An integrated & important part of Grandstream's GDMS cloud-based device management service which runs on Amazon AWS with 99.999% reliability, the UCM RemoteConnect cloud service supports hassle-free Work-From-Home audio/video communications & collaborations using WebRTC-based license-free "Grandstream Wave" soft phones for desktop/Web/mobile devices (plus GUV series of USB headsets/Webcams), zero-touch out-of-box automated NAT firewall traversal for remote users & devices, IT-friendly remote management of UCM and attached endpoint devices, and more.

The RemoteConnect can be configured under **Value-added Features→RemoteConnect** After purchasing the RemoteConnect package.

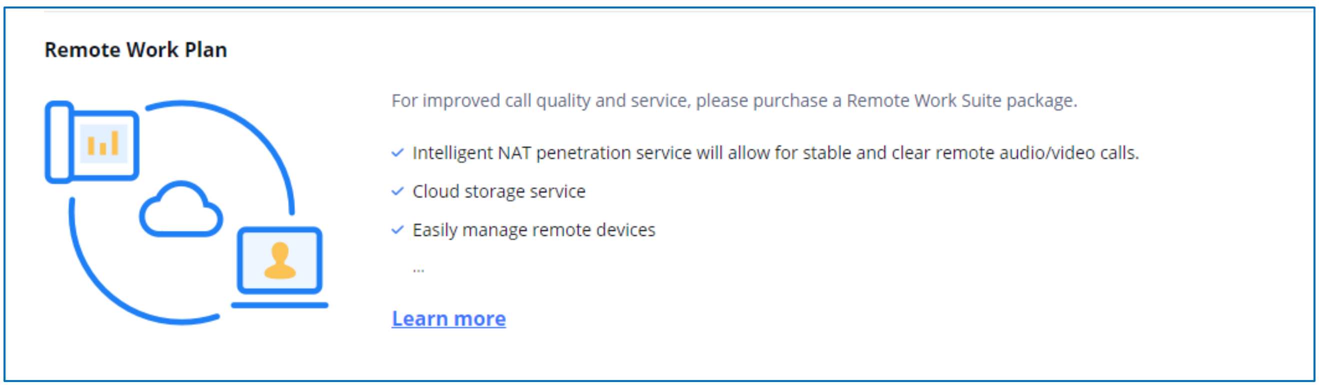


Figure 245: RemoteConnect

On GDMS platform, sign in and go to Device→PBX Device page, click on "Add Device" to add your UCM6300 device to GDMS system, once done an open beta plan will be assigned to the UCM.

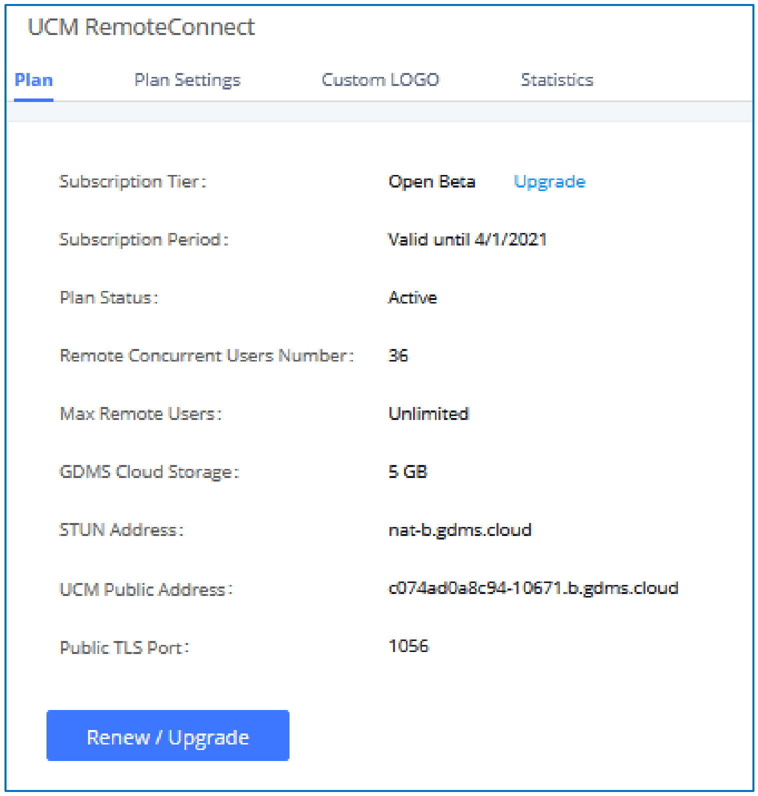


Figure 246: UCM RemoteConnect - Effective Plan

Note

- After the UCM is added on GDMS, automated NAT traversal, SIP extension sync-up and basic statistics features are available without manual configuration required.

Plan Settings

After UCM is added into GDMS, all SIP extensions on the UCM will be synced up to GDMS automatically for users to allocate and manage SIP extension for their end devices. Also, the media NAT Traversal service, alert event sync configuration items are checked by default, the CDR data cloud storage in GDMS should be manually checked according to user needs.

The settings are under UCM **webGUI→Value-added Services→UCM RemoteConnect→Plan Settings**.

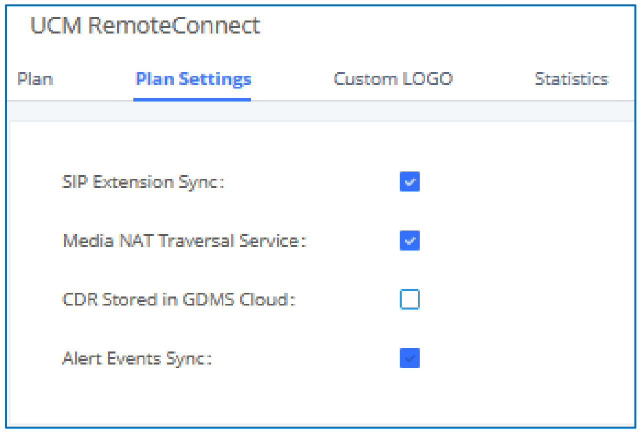


Figure 247: UCM RemoteConnect Plan Settings

Custom logo

Custom logo feature allows users to select a local image file as the new logo. The pictures are in different formats and sizes according to the location of the logo. They are 64*64px (only ico format is supported), 256*256px, 80*80px, which applies for "UCM Login", "Reset Password", "Email Template", "Wave/Login", "Browser Tab interface preview".

- LOGO 1: Replaces Browser tab icon
- LOGO 2: Replaces the Grandstream banner on the top left corner of the management login page and emails.
- LOGO 3: Replaces the Grandstream logo on the top left corner of the Wave Web interface and UCM management interface.

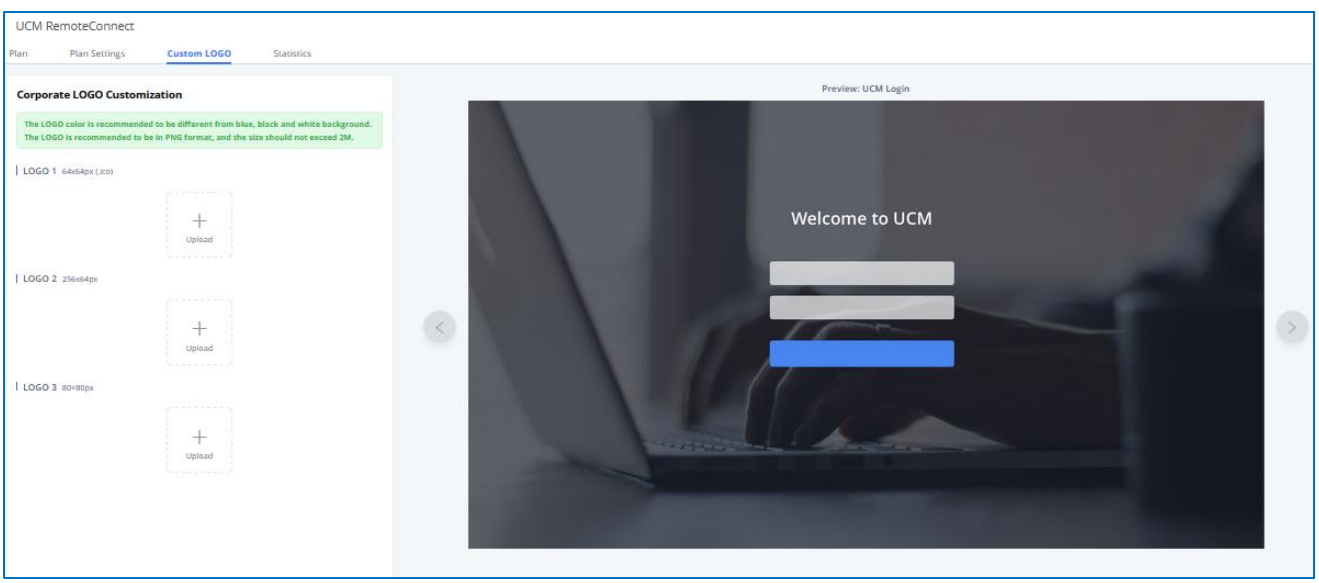


Figure 248: Custom Logo

Statistics

After using UCM RemoteConnect, all remote calls will be logged and concurrent remote calls will be displayed on the UCM. The concurrent remote calls can be viewed under UCM web GUI→Value-Added Features→UCM RemoteConnect→Statistics page.

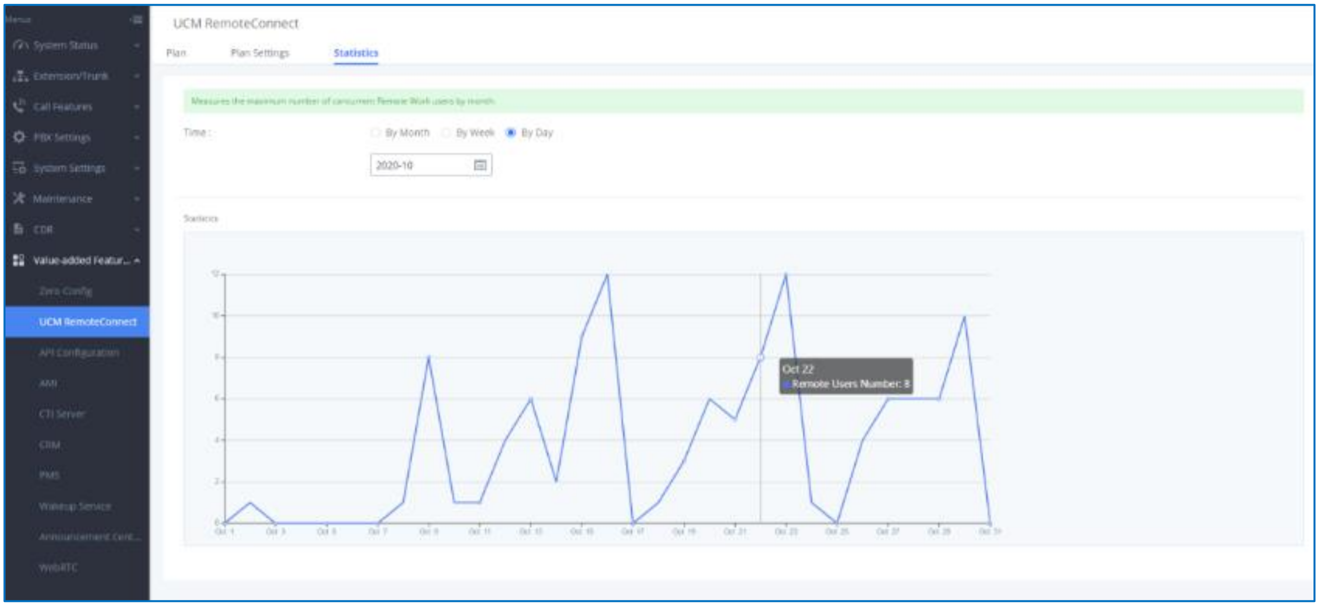


Figure 249: Concurrent Remote Calls

For more information, please visit http://ucmrc.gdms.cloud/intro.html and read our [UCM63XX RemoteConnect guides](#)

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 **Value-added Features→API Configuration**. The API configuration parameters are listed in the table below.

Table 120: Configuration Parameters (New)

HTTPS API Settings (New)	
Enable	Enable/Disable API. The default setting is enable.
Username	Configure the username for API Authentication.
Password	Configure the password for API Authentication.
Call Control	If enabled, 3rd party applications will be able to manage inbound calls via API actions. **acceptCall** will accept incoming calls while **refuseCall** will reject them. If no actions are done within 10 seconds, calls will automatically be accepted.

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.

Table 121: New API Supported Queries

Queries Supported
getSystemStatus
getSystemGeneralStatus
listAccount
getSIPAccount
updateSIPAccount

listVoIPTrunk
addSIPTrunk
getSIPTrunk
updateSIPTrunk
deleteSIPTrunk
listOutboundRoute
addOutboundRoute
getOutboundRoute
updateOutboundRoute
deleteOutboundRoute
listInboundRoute
addInboundRoute
getInboundRoute
updateInboundRoute
deleteInboundRoute
playPromptByOrg
listBridgedChannels
listUnBridgedChannels
Hangup
callbarge
listQueue
getQueue
updateQueue
addQueue
deleteQueue
loginLogoffQueueAgent
pauseUnpauseQueueAgent
listPaginggroup
addPaginggroup
getPaginggroup
updatePaginggroup

deletePaginggroup
MulticastPaging
MulticastPagingHangup
listIVR
addIVR
getIVR
updateIVR
deleteIVR
cdrapi
recapi
pmsapi
queueapi
getPinSets
addPinSets
updatePinSets
deletePinSets

Table 122: API Configuration Parameters

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 **value-added Features → API Configuration → Upload Prompts User Configuration.** By default, the username and password for voice prompt user are “Username: uploader; Password: uploader123”.

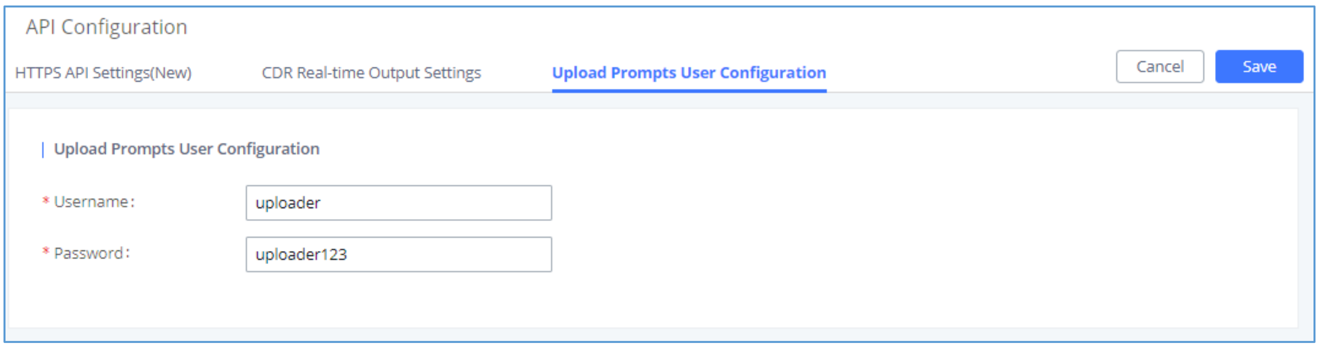


Figure 250: Upload Prompt User Configuration

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=9191a6394c21b3aabd779213c7179462&filename=test.mp3

   If UCM's HTTP server is set to HTTP, the example of the request sent to the UCM is：

   http://192.168.124.89:8089/cgi?action=uploadprompt&username=uploader&password=9191a6394c21b3aabd779213c7179462&filename=test.mp3

Note: 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:
http://www.grandstream.com/sites/default/files/Resources/ucm6xxx_cdr_rec_api_guide.pdf

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, Web GUI→**Value-added Features**→**CTI Server** as shown on below screenshot:

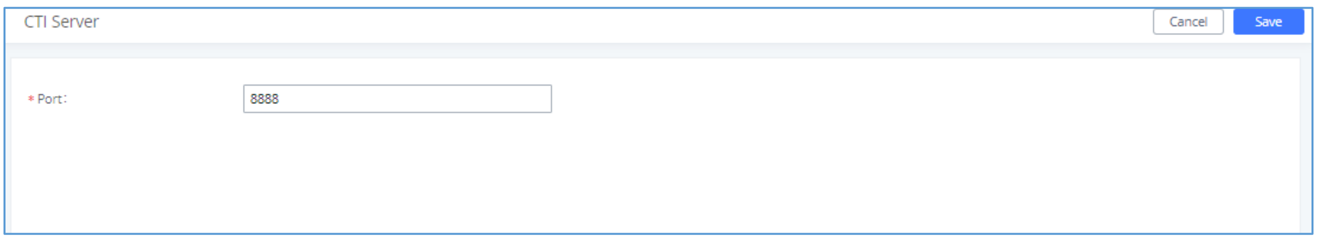


Figure 251: CTI Server Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link: http://www.grandstream.com/sites/default/files/Resources/GS_Affinity_Guide.pdf

ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)

The UCM630X supports Asterisk Manager Interface (AMI) 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 UCM630X Web GUI→**Value-added Features**→**AMI**. For details on how to use AMI on UCM630X, please refer to the following AMI guide:

http://www.grandstream.com/sites/default/files/Resources/UCM_series_AMI_guide.pdf

---

⚠ **Warning:**

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.

CRM INTEGRATION

Customer relationship management (**CRM**) is a term that 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 support the following CRMs: SugarCRM, vTigerCRM, ZohoCRM, Salesforce CRM and ACT! CRM, which allows users to look for contact information in the Contacts, Leads and / or Accounts tables, shows the contact record in CRM page, and saves the call information in the contact’s history.

SugarCRM

Configuration page of the SugarCRM can be accessed via admin login, on the UCM WebGUI→**Value-added Features**→**CRM**.

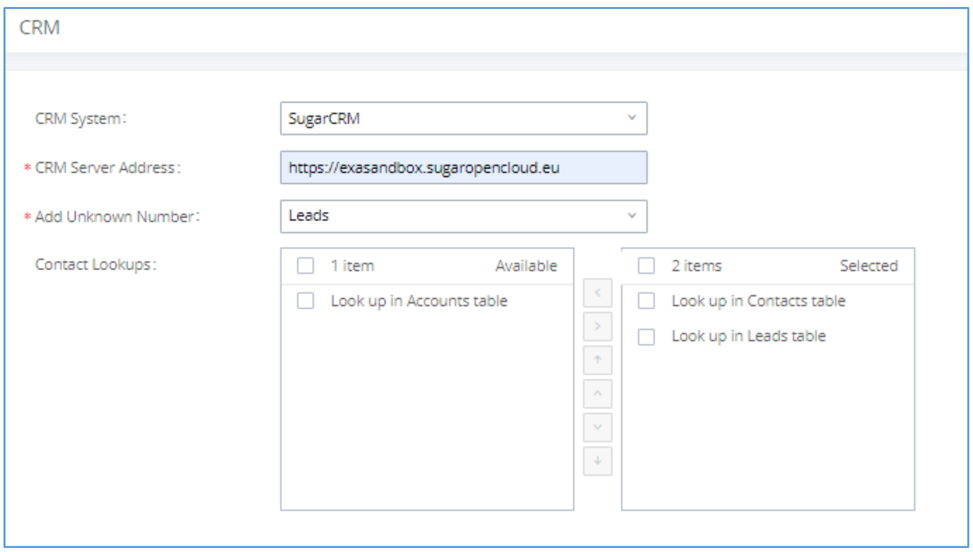


Figure 252: SugarCRM Basic Settings

1. Select “SugarCRM” from the CRM System Dropdown in order to use SugarCRM.

Table 123: SugarCRM Settings

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
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.

Once settings on admin access are configured:

2. Click on Save and Apply Changes.
3. Logout from admin access.
4. Login to the UCM as user and navigate under "User Portal→Value-added Feature→CRM User Settings".

Click on "**Enable CRM**" and enter the username/password associated with the CRM account then click on Save and Apply Changes. The status will change from "Logged Out" to "Logged In". User can start then using SugarCRM features.

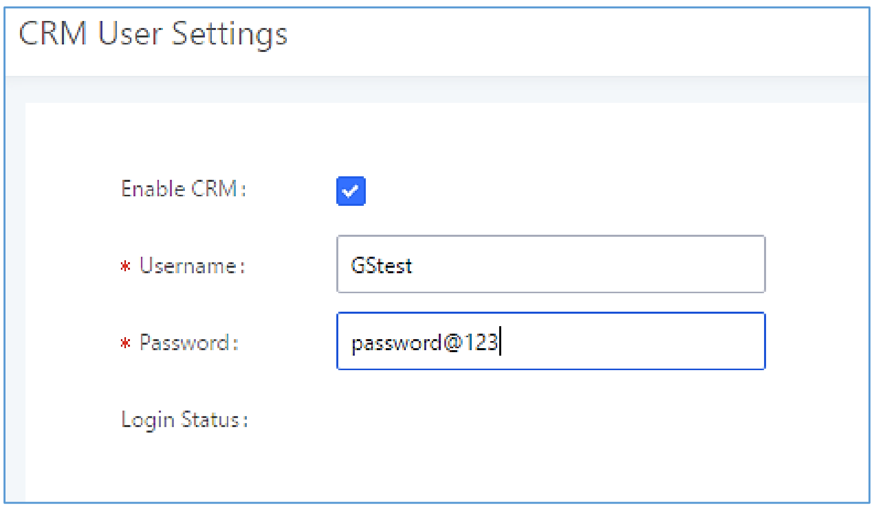


Figure 253: CRM User Settings

VTigerCRM

Configuration page of the vTigerCRM can be accessed via admin login, on the UCM WebGUI→**Value-added Features→CRM**.

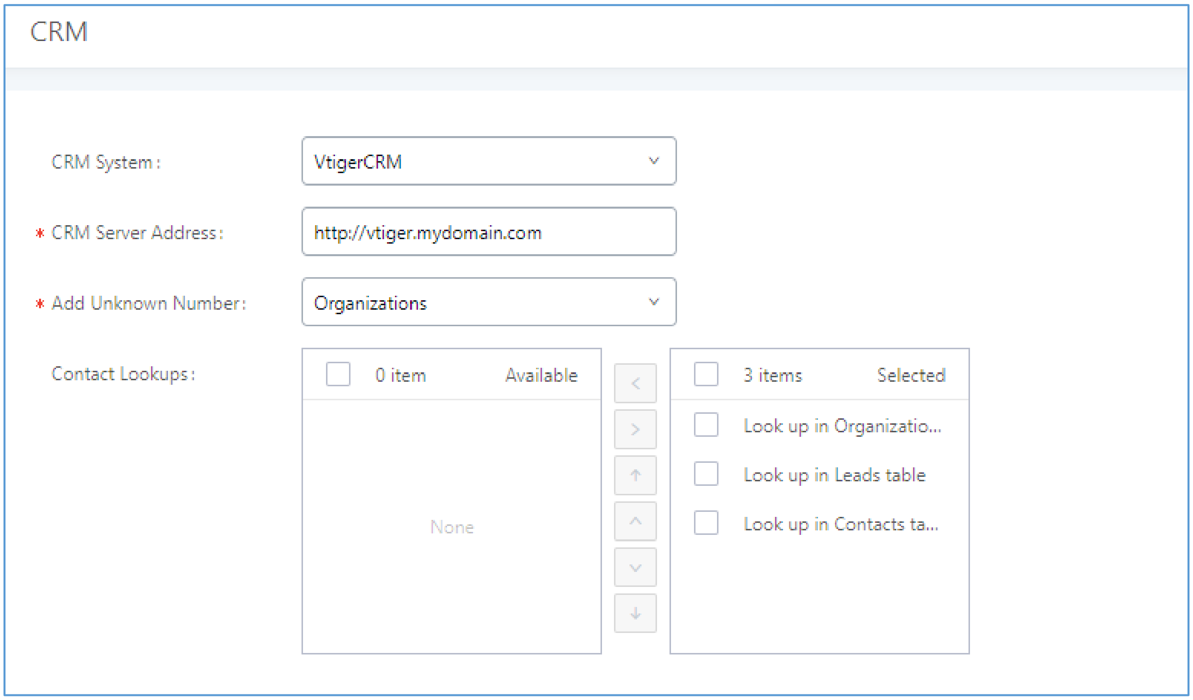


Figure 254: vTigerCRM Basic Settings

1. Select "vTigerCRM" from the CRM System Dropdown in order to use vTigerCRM.

Table 124: vTigerCRM Settings

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
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.

Once settings on admin access are configured:

2. Click on Save and Apply Changes.
3. Logout from admin access.
4. Login to the UCM as user and navigate under "User Portal→Value-added Feature→CRM User Settings".

Click on "**Enable CRM**" and enter the username/password associated with the CRM account then click on

Save and Apply Changes. The status will change from “Logged Out” to “Logged In”. User can start then using SugarCRM features.

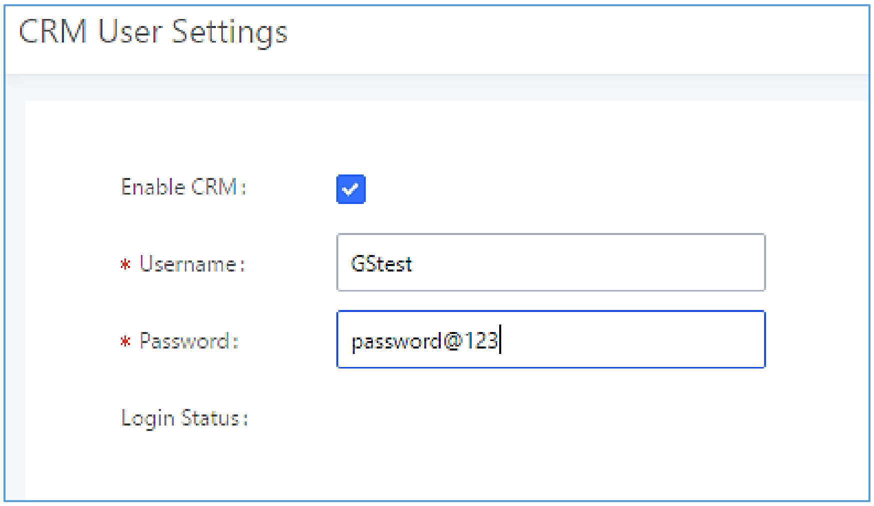


Figure 255: CRM User Settings

ZohoCRM

Configuration page of the ZohoCRM can be accessed via admin login, on the UCM WebGUI→**Value-added Features**→**CRM**.

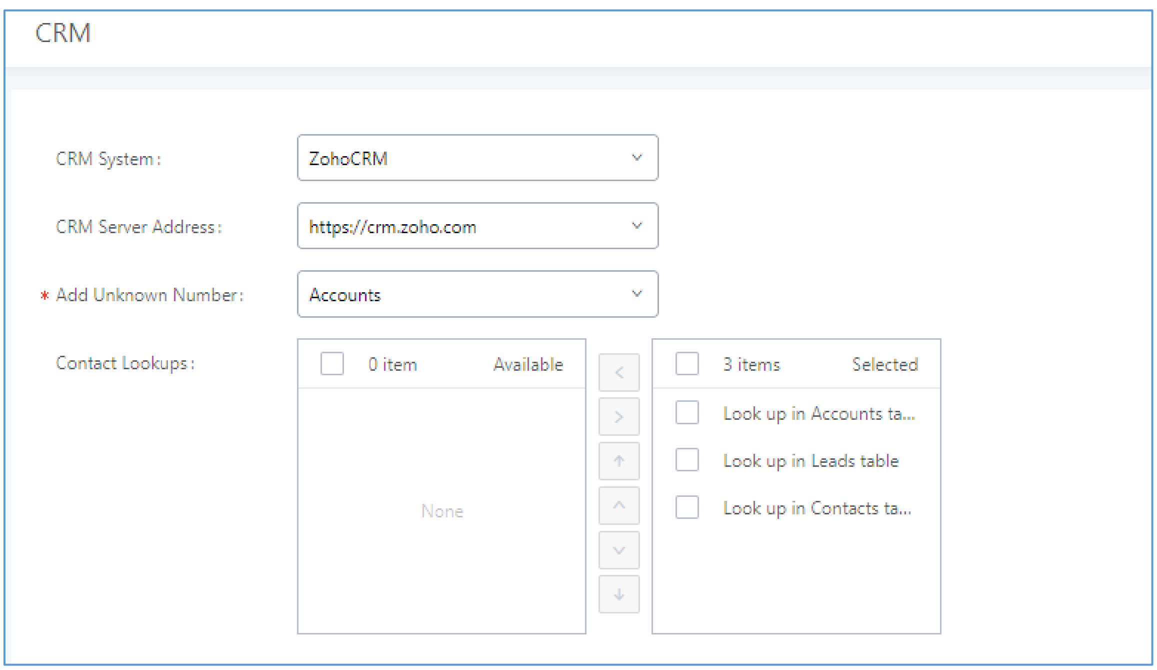


Figure 256: ZohoCRM Basic Settings

1. Select “ZohoCRM” from the CRM System Dropdown in order to use ZohoCRM.

Table 125: ZohoCRM Settings

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
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.

Once settings on admin access are configured:

2. Click on Save and Apply Changes.
3. Logout from admin access.
4. Login to the UCM as user and navigate under “User Portal→Value-added Feature→CRM User Settings”.

Click on “**Enable CRM**” and enter the username/password associated with the CRM account then click on Save and Apply Changes. The status will change from “Logged Out” to “Logged In”. User can start then using ZohoCRM features.

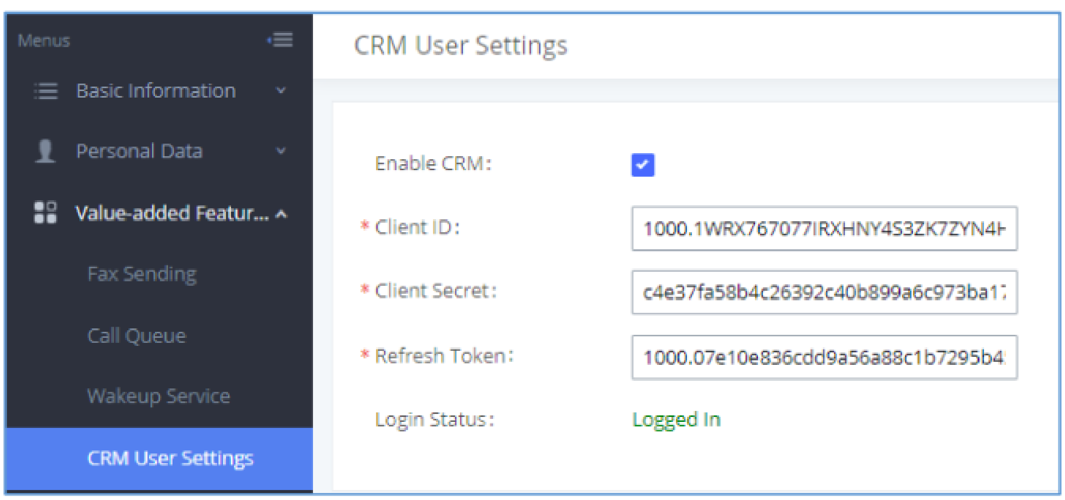


Figure 257: CRM User Settings

Note: ZohoV2CRM is supported as well while the CRM Server Address **https://www.zohozpis.com**

Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI→**Value-added Features**→**CRM**".

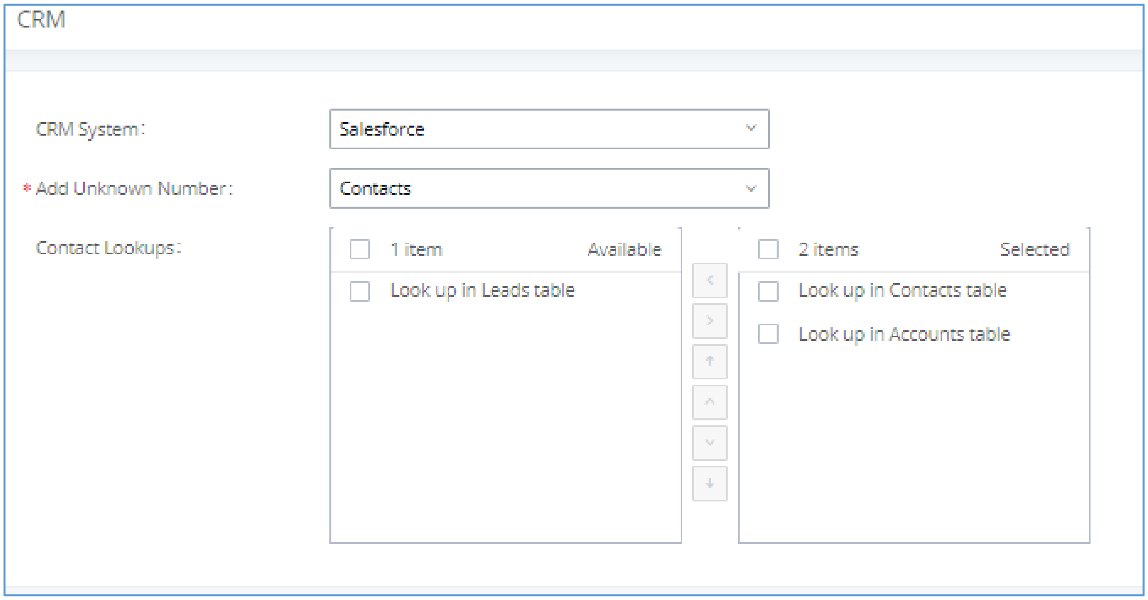


Figure 258: Salesforce Basic Settings

1. Select "Salesforce" from the CRM System Dropdown in order to use Salesforce CRM.

Table 126: Salesforce Settings

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
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.

Once settings on admin access are configured:

2. Click on Save and Apply Changes.
3. Logout from admin access.
4. Login to the UCM as user and navigate under "User Portal→Value-added Feature→CRM User Settings".

Click on "**Enable CRM**" and enter the **username**, **password** and **Security Token** associated with the CRM account then click on Save and Apply Changes. The status will change from "Logged Out" to "Logged In". User can start then using Salesforce CRM features.

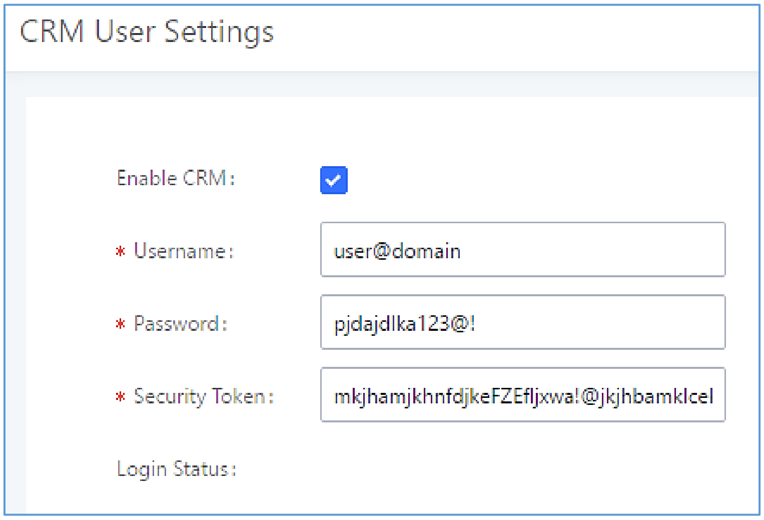


Figure 259: Salesforce User Settings

ACT! CRM

Configuration page of the ACT! CRM can be accessed via admin login, on the UCM Web GUI→**Value-added Features**→**CRM**".

The configuration steps of the ACT! CRM are as follows:

1. Navigate to **Value-Added Features**→**CRM** and select the "ACT! CRM" option.

Figure 260: Enabling ACT! CRM

2. Log into the UCM as a regular user and navigate to **Value-Added Features**→**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://mycloud.act.com/act/Help

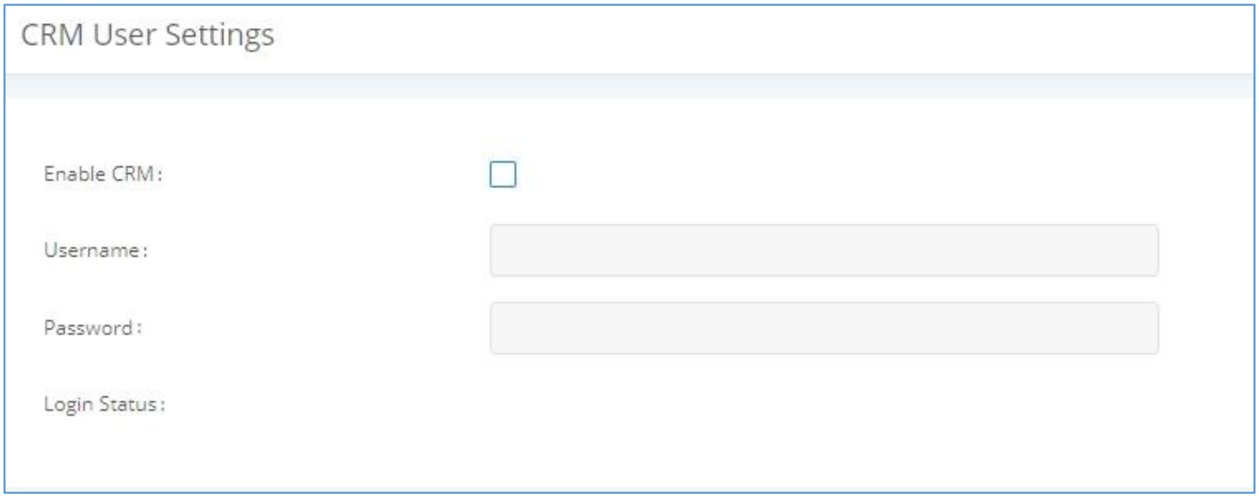


Figure 261: Enabling CRM on the User Portal

Note: For more information on the ACT! CRM integration, please refer to the ACT! CRM documentation on our website.

PMS INTEGRATION

UCM630X supports Hotel 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→**Value-added Features→PMS.**

Note: The PMS integration on UCM is currently supported only with one of the three following solutions.

The PMS module built-in the UCM supports the following features based on each solution:

Table 127: PMS Supported Features

Feature	Mitel	HMobile	HSC	IDS
Check-In	✓	✓	✗	✓
Check-out	✓	✓	✗	✓
Wake-up Call	✓	✓	✗	✓
Name Change	✓	✗	✓	✗
Update	✗	✓	✗	✓
Set Credit	✓	✗	✗	✗
Set Station Restriction	✓	✗	✓	✗
Room Status	✗	✓	✗	✓
Room Move	✗	✓	✗	✓
Do Not Disturb	✗	✓	✓	✗
Mini Bar	✗	✓	✗	✓
MSG	✗	✓	✗	✗
MWI	✗	✗	✓	✗
Unconditional Call Forward	✗	✗	✓	✗

HMobile PMS Connector

In this mode, the system can be divided into three parts:

- PMS (Property Management System)
- PMSI (Property Management System Interface)
- PBX

Grandstream UCM6XXX series have integrated HMobile Connect PMSI which supports a large variety of PMS software providing following hospitality features: 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 (HMobile Connect) acting as interface between both parties.

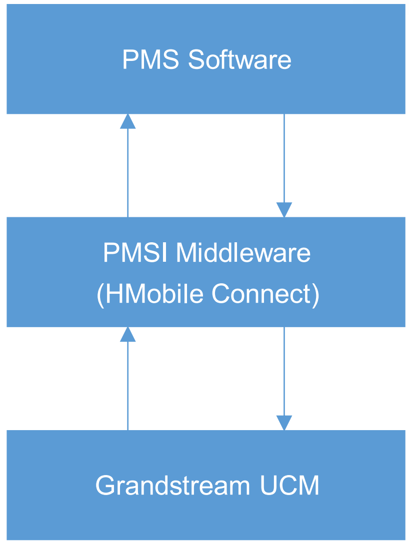


Figure 262: UCM & PMS interaction

HSC PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series have integrated HSC PMS providing following features:

- Changing Display Name
- Set Station Restriction
- Call forwarding
- DND
- Name Change
- MWI

Note:

3. 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.
4. 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.

5. Added HTTPS support

The following figure illustrates the communication flow between the PBX (Grandstream UCM6xxx Series) and PMS software (HSC). The communication between both parties is direct with no middleware.

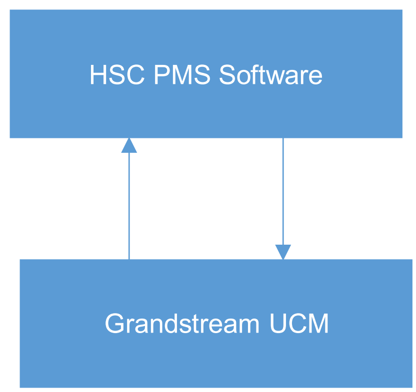


Figure 263: UCM & HSC PMS interaction

Mitel PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series have integrated Mitel PMS providing 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 UCM6xxx Series) and PMS software (Mitel). The communication between both parties is direct with no middleware.

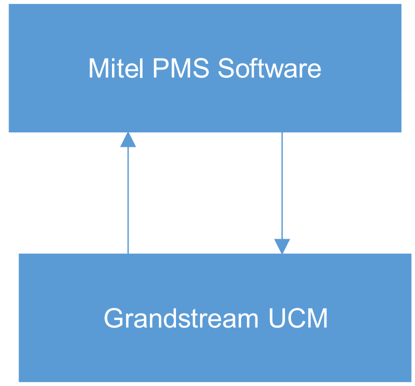


Figure 264: UCM & Mitel PMS interaction

IDS PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

The Grandstream UCM series integrates IDS PMS to set room status, Mini Bar, wake up calls, activate/deactivate dialing permissions, and more.

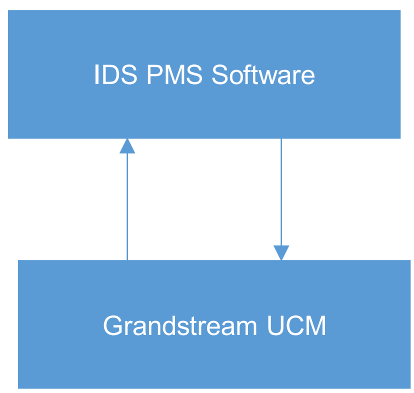


Figure 265: UCM & IDS PMS interaction

PMS API

The PMS API allows users to use their own 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 online HTTPS API, Pmsapi section.

Connecting to PMS

On the UCM WebGUI→**Value-added Features**→**PMS**→**Basic Settings**" set the connection information for the PMS platform.

Table 128: PMS Basic Settings

Field	Description
PMS Module	Users can select the desired PMS module from the drop-down list. • Hmobile. • Mitel. • HSC. • IDS. • PMS API.
Wakeup Prompt	Prompt used when answering the wakeup calls it can be customized from "**PBX Settings**→**Voice Prompt**→**Custom Prompt.**
PMS URL	Enter the PMS system URL
UCM Port	Enter the Port used by the PMS system
Username	Enter the Username to connect to the PMS system
Password	Enter the password to connect to the PMS system
Site	Enter PMS site
Back Up Voicemail Recordings	If enabled, this option allows backing up voicemail recordings to external storage after check-out. **Note:** This option is available only when the PMS Module is set to PMS API.
Email address	Email address to send voicemail recordings to upon backup.

In order to use some PMS features please activate the feature code associated under "**Call Features**→**Feature Codes**"

- Update PMS Room Status
- PMS Wake Up Service

PMS Features

Room Status

User can create Rooms by clicking on ”Add Room”, the following Figure will be displayed then.

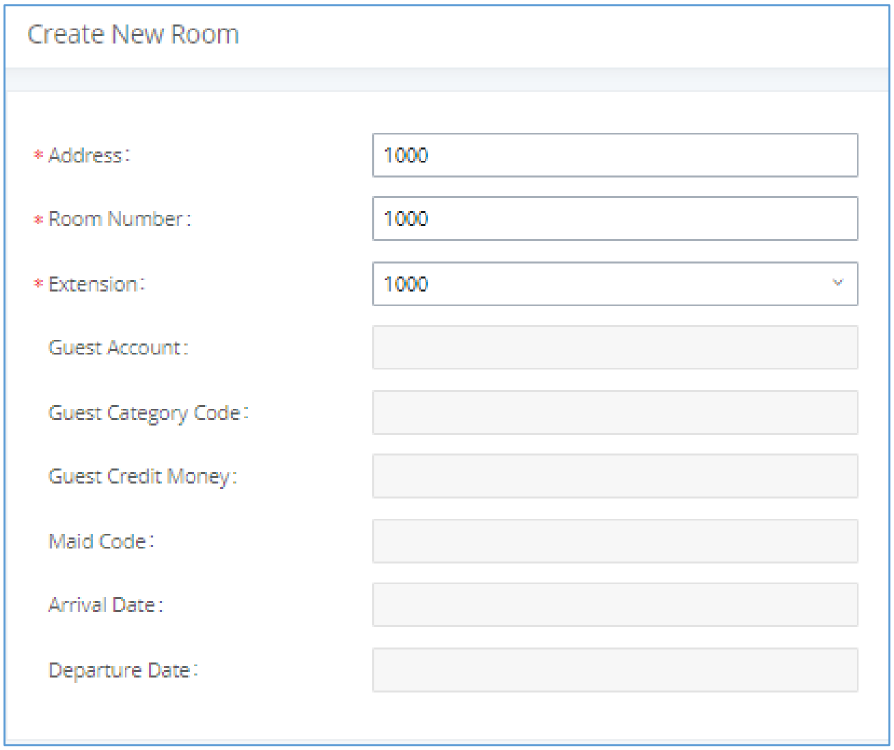


Figure 266: Create New Room

Click “Save” to create the new room, the fields above can be configured from the PMS platform, once set the following screen will be shown:

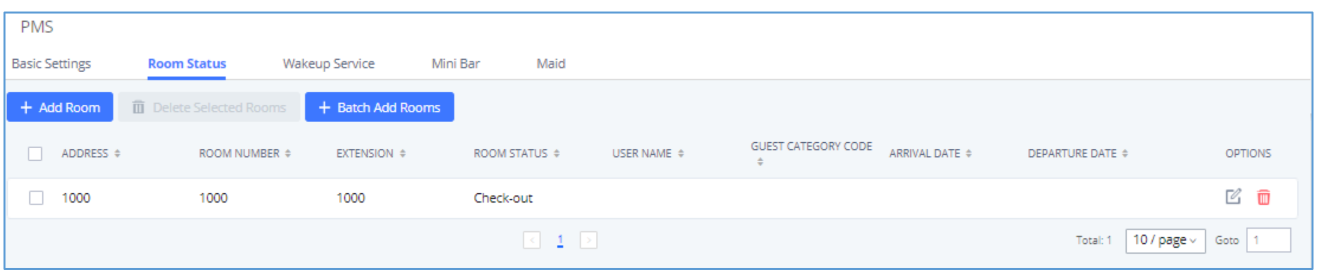


Figure 267: Room Status

User can create a batch of rooms as well by clicking on + Batch Add Rooms, the following window will pop up:

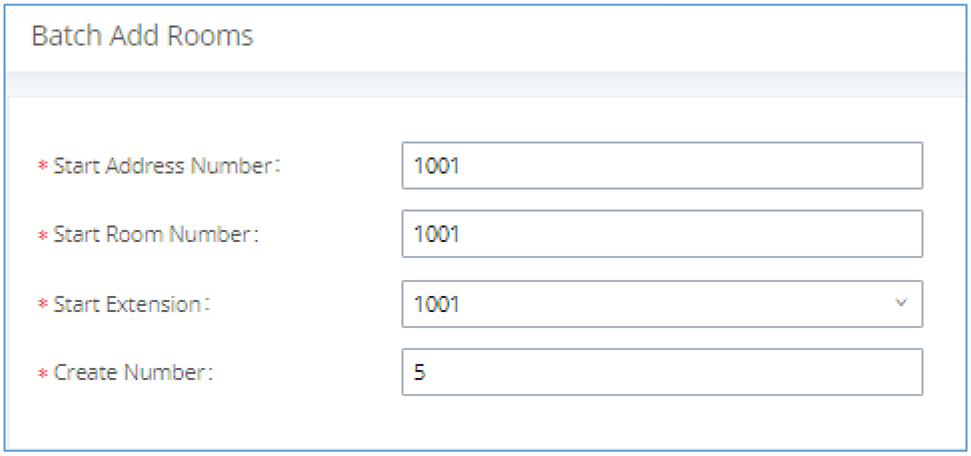


Figure 268: Add batch rooms

Wake Up Service

In order to create a New Wake up service, user can click on "Add", the following window will pop up:

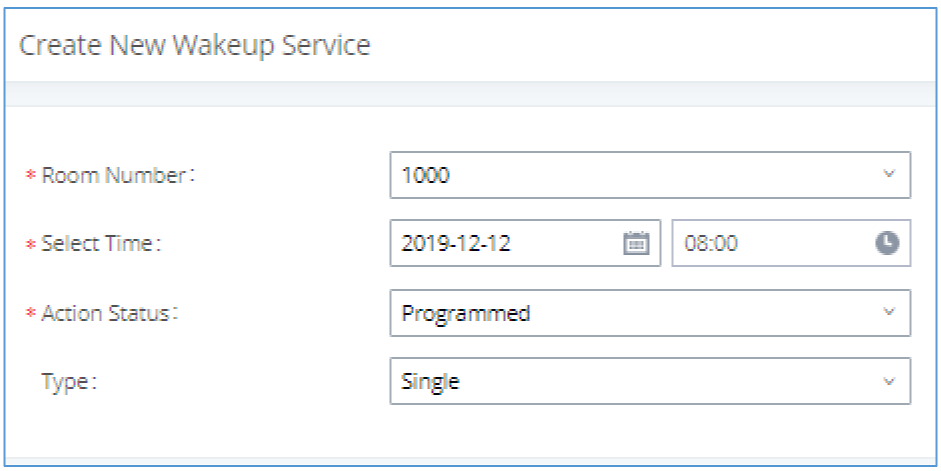


Figure 269: Create New Wake Up Service

Table 129: PMS Wake up Service

Field	Description
Room Number	Select the room number where to call with a limitation of 63 characters.
Select Time	Set the time of the wakeup call
Action Status	Show the status of the call: • Programmed: the call is scheduled for the time set • Cancelled: the call is canceled • Executed: the wakeup call is made **Note**: Editing an already executed wakeup service will automatically change the service's status to "Programmed".

Type	• Single: The call will be made once on the specific time. • Daily: The call will be repeated every day on the specific time

Once the call is made on the time specified, the following figure show the status of the wakeup call.

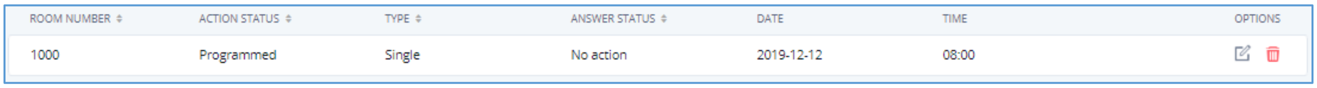


Figure 270: Wakeup Call executed

This call has been executed but has been rejected, that why we can see the **"Busy"** status.

Mini Bar

In order to create a new mini bar, click on "Add Mini Bar" under UCM WebGUI→**Value-added Features→PMS→Mini Bar,** the following window will pop up:

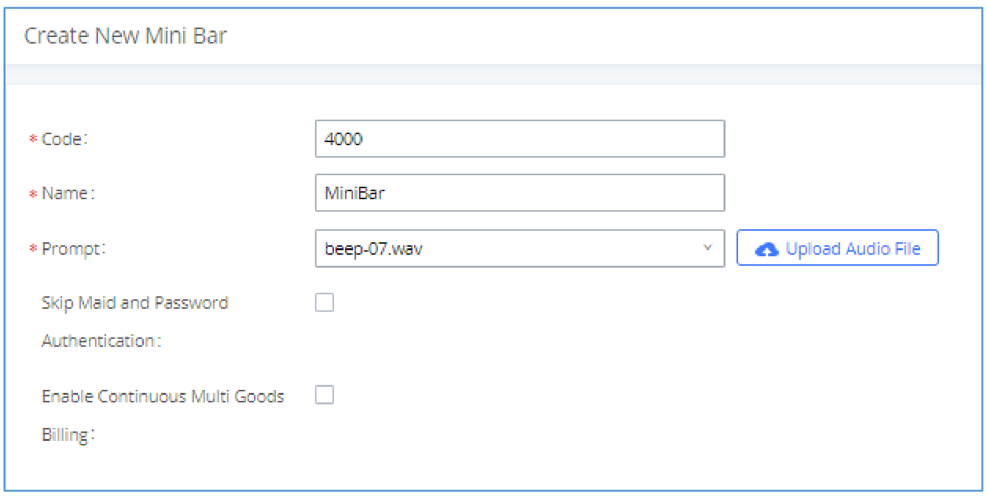


Figure 271: Create New Mini Bar

Table 130: Create New Mini Bar

Code	Enter a non-existing extension number to be dialed when using the mini bar feature.
Name	Enter a name for the mini bar.
Prompt	Select the Prompt to play once connected to the mini bar.
Skip Maid and Password Authentication	If enabled, the default maid code will be 0000, no authentication is required. (Enter 0000 followed by # to access the consumer goods)
Enable Continuous Multi Goods Billing	If enabled, please separate the goods' codes by*.

In order to create a new maid, click on **+ Create New Maid** under UCM WebGUI→**Value-added Features→PMS→Maid**.

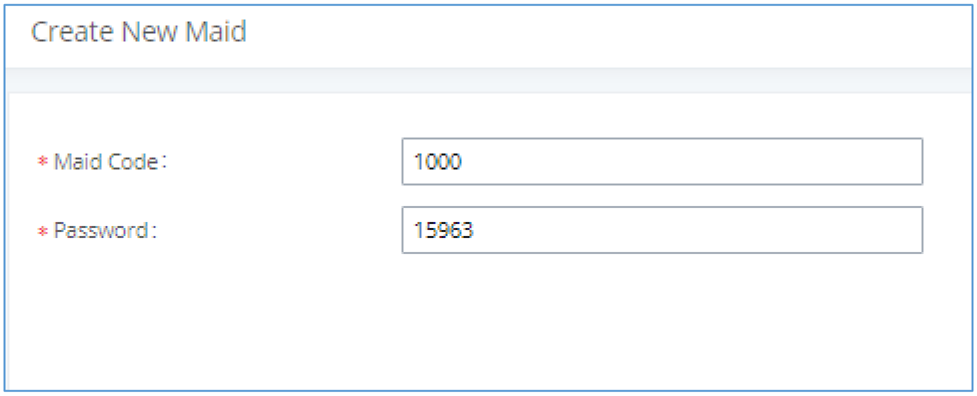


Figure 272: Create New Maid

Table 131: Create New Maid

Maid Code	Enter the Code to use when the maid wants to use the Mini Bar.
Password	Enter the password associated with the maid.

In order to create a new consumer goods, click on **+ Create New Consumer Goods** under UCM WebGUI→**Value-added Features→PMS→Mini Bar,** the following window will popup.

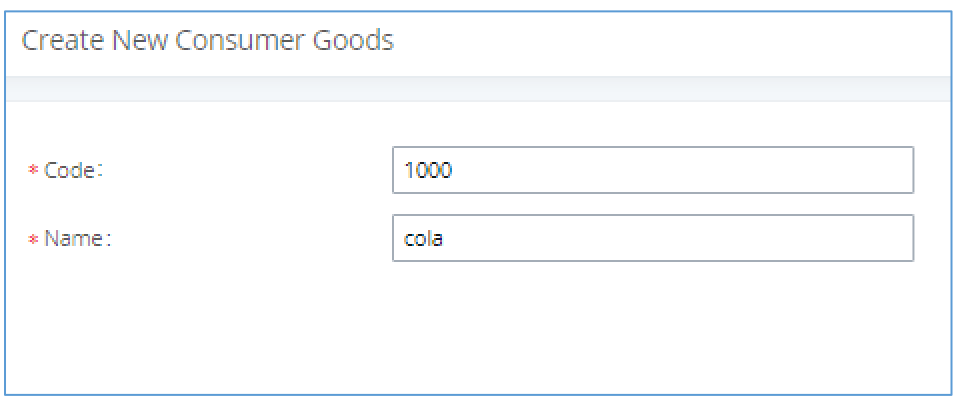


Figure 273: Create New Consumer Goods

Code	Enter the Goods Code.
Name	Enter the Name of the Goods

The Minibar page displays as:

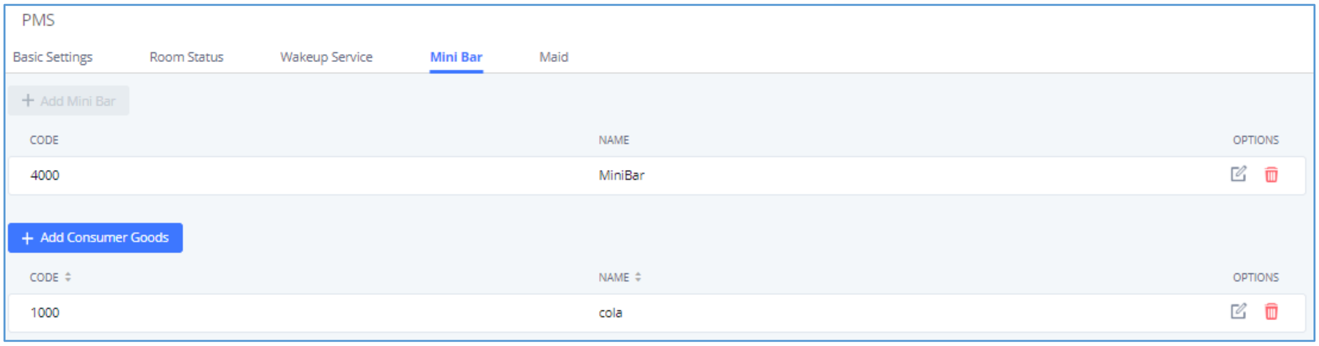


Figure 274: Mini Bar

WAKEUP SERVICE

The Wake Up service can be used to schedule a reminder or wake up calls to any valid destination. This service is available on the UCM630X as a separated module.

There are three ways to set up Wakeup Service:

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

Wake Up Service using Admin Login

1. Login to the UCM as admin.
2. Wake Up service can be found under Web GUI→**Value-added Features→Wakeup Service**, click on "Add" to create a new wakeup service. The following window will pop up.

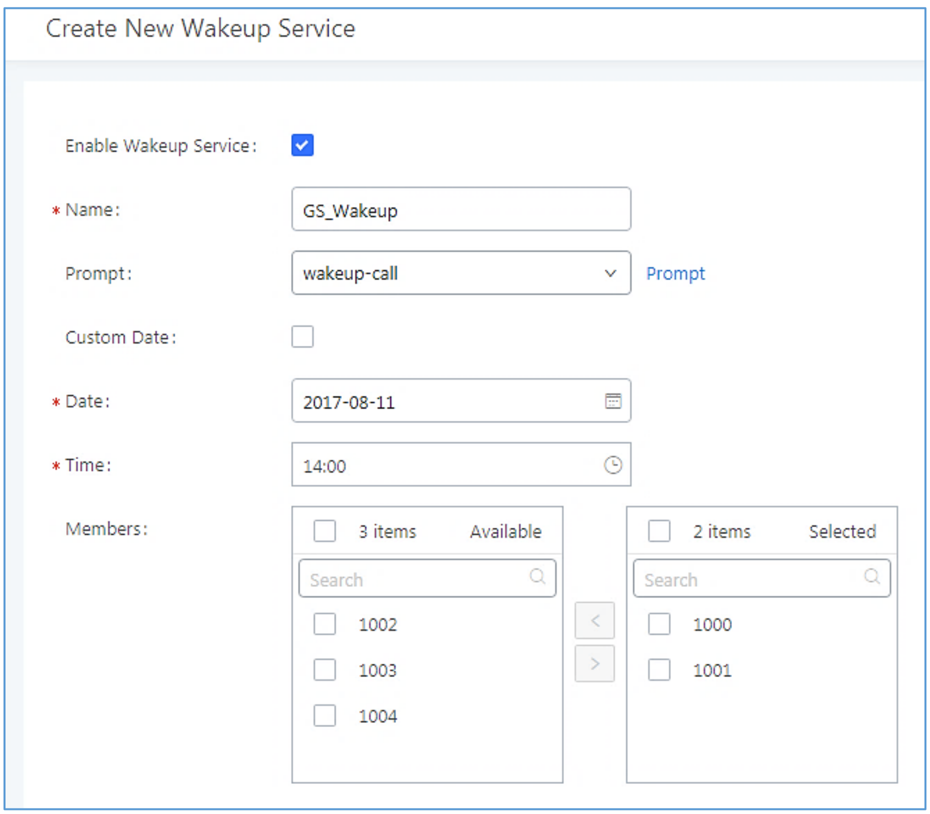


Figure 275: Create New Wakeup Service

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

Table 132: Wakeup Service

Enable Wakeup Service	Enable Wakeup service.
Name	Enter a name (up to 64 characters) to identify the wakeup service.
Prompt	Select the prompt to play for that extension.
Custom Date	If disabled, users can select a specific date and time. If enabled users can select multiple days of the week to perform the wakeup.
Date	Select the date or dates when to performs the wakeup call.
Time	Select the time when to play the wakeup call.
Members	Select the members involved within the wakeup service group.

4. Click Save and Apply Changes to apply the changes.

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

Note: the wakeup service has the following limitation on how many members can be added depending on UCM model.

Table 133: Max Wakeup Members

UCM Model	Max members in a Wakeup Service
UCM6301	50
UCM6302	100
UCM6304	150
UCM6308	200

Wake Up Service from User Portal

1. Login to the user portal on the UCM630X.
2. Wake Up service can be found under "Value-added Features→Wakeup Service", click on "Add" to create a new wakeup service.
3. Configures the Name, Prompt, Date and Time for the user to make the wakeup to.

4. Click Save and Apply Changes to apply the changes.

Wake Up Service using Feature Code

1. Login to the UCM as admin.
2. Enable “Wakeup Service” from the WebGUI under “**Call Features→Feature Codes**”.

3. Click Save and Apply Changes to apply the changes.

4. Dial “*36” which is the feature code by default to access to the UCM wakeup service to add, update, activate or deactivate UCM wakeup service.

ANNOUNCEMENTS CENTER

The UCM630X supports Announcements 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.

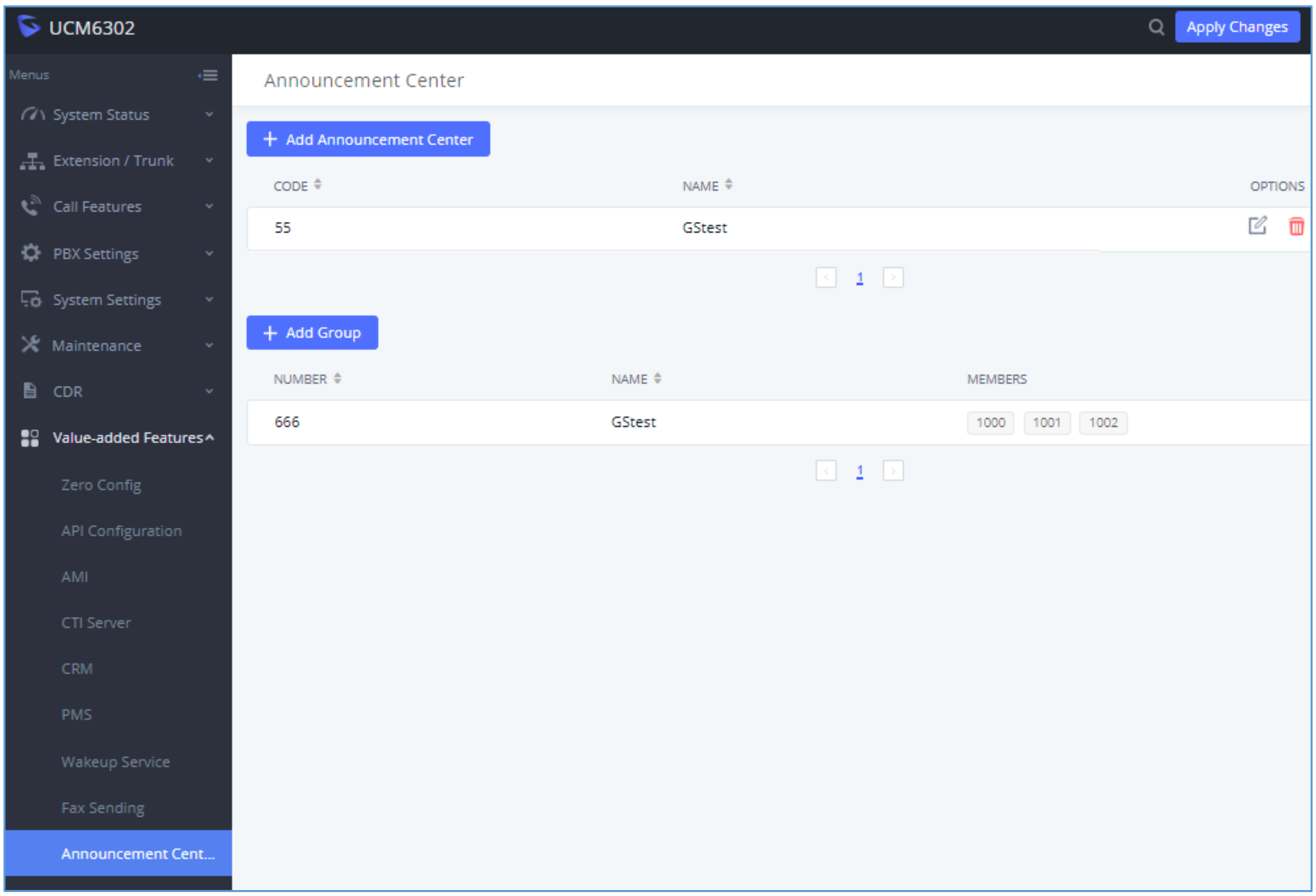


Figure 276: Announcements Center

Announcements Center Settings

Table 134: Announcements Center Settings

Name	Configure a name for the newly created Announcements 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.
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.

Group Settings

Table 135: 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.
Members	Select the group members from the available list.

Announcements Center feature can be found under Web GUI→**Value-added Features**→**Announcements 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.

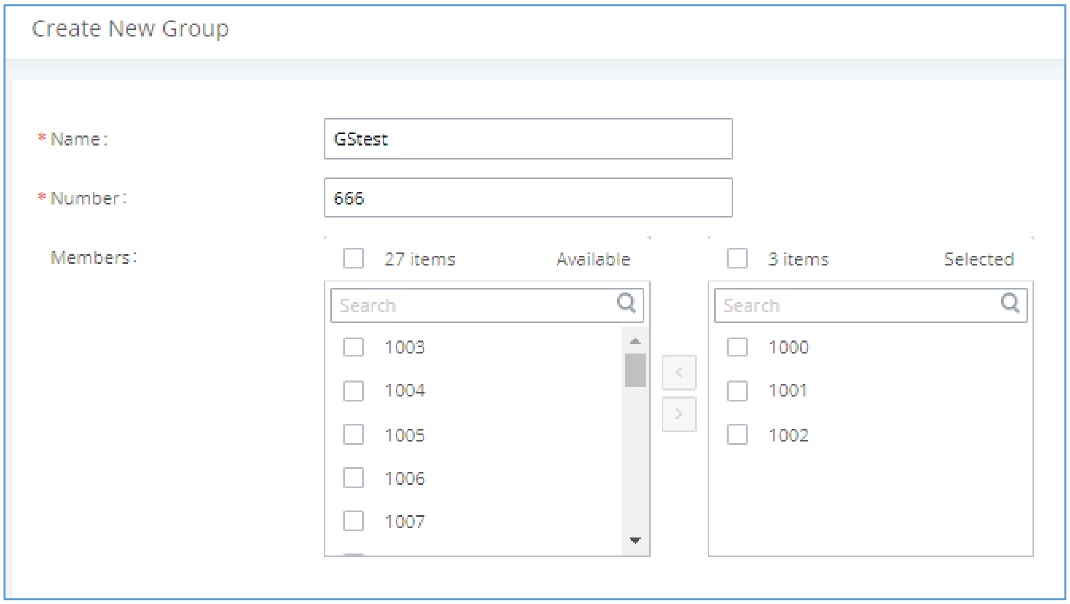


Figure 277: Announcements Center Group Configuration

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

1. Click 

to create a new Announcement Center.
2. Give a name to the newly created Announcement Center.
3. Specify the code which will be used with group number to send the voice message to.
4. 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.

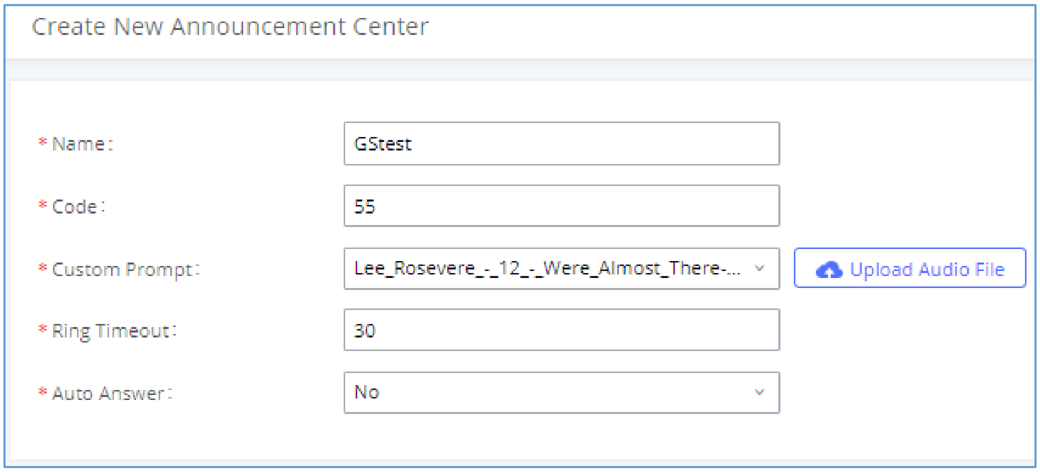


Figure 278: Announcements Center Code Configuration

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.

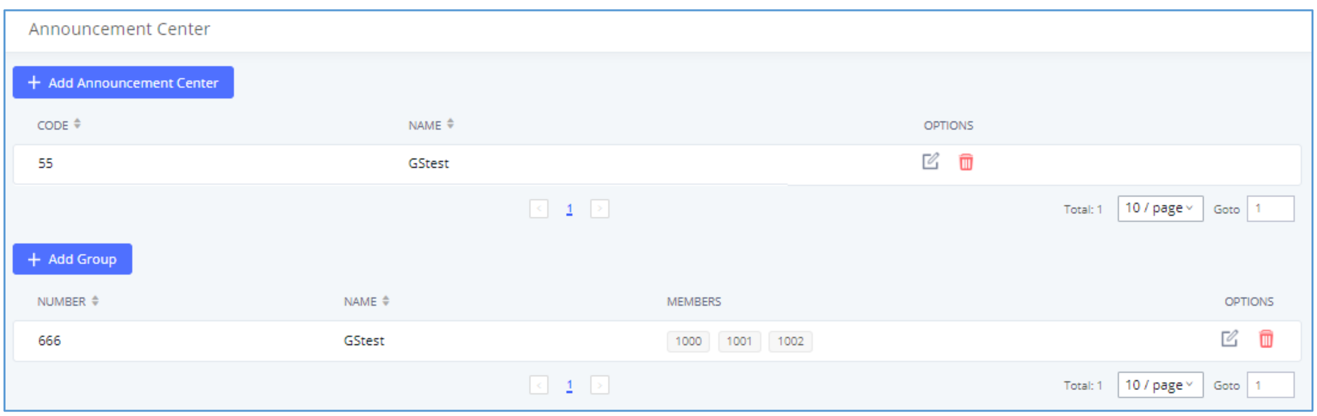


Figure 279: Announcements Center Example

STATUS AND REPORTING

PBX Status

The UCM630X monitors the status for Trunks, Extensions, Queues, Conference Rooms, Interfaces and Parking lot. It presents administrators the real-time status in different sections under Web GUI→**System Status→Dashboard**.

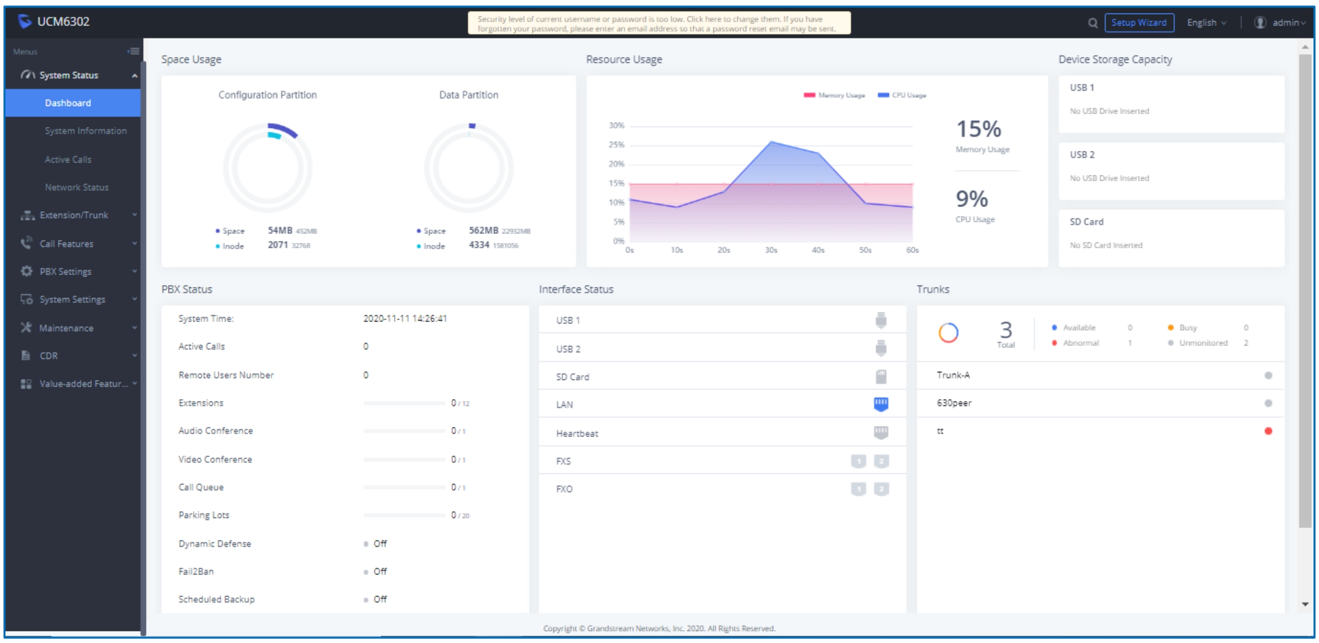


Figure 280: Status→PBX Status

Trunks

Users could see all the configured trunk status in this section.

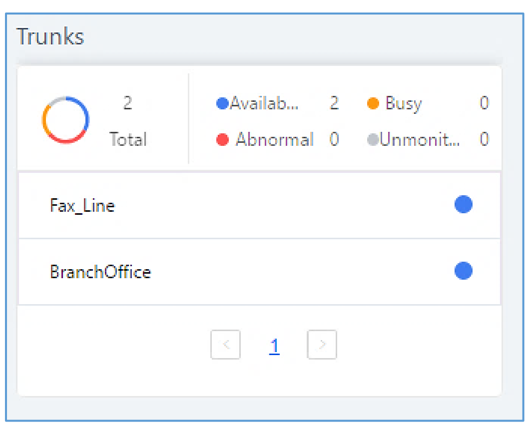


Figure 281: Trunk Status

Table 136: Trunk Status

Status	Display trunk status. • <u>Analog trunk status</u>: **Available** **Busy** **Unavailable** **Unknown Error** • <u>SIP Peer trunk status</u>: **Unreachable**: The hostname cannot be reached. **Unmonitored**: Heartbeat feature is not turned on to be monitored. **Reachable**: The hostname can be reached. • <u>SIP Register trunk status</u>: **Registered** **Unrecognized Trunk**
Trunks	Display trunk name
Type	Display trunk Type: • Analog • SIP • IAX
Username	Display username for this trunk.
Port/Hostname/IP	Display Port for analog trunk, or Hostname/IP for VoIP (SIP/IAX) trunk.

Extensions

Extensions Status can be seen from the same configuration page, users can go under Web GUI→**Extension/Trunk**→**Extensions** and following page will be displayed listing the extensions and their status information.

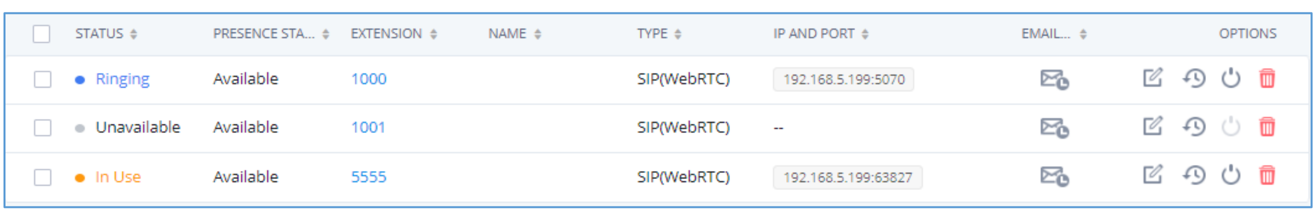


Figure 282: Extension Status

Table 137: Extension Status

Status	Display extension number (including feature code). The color indicator has the following definitions. • Green: Free • Blue: Ringing • Yellow: In Use • Grey: Unavailable
Presence Status	Display the presence status of the extension.
Extension	Display the extension number.
Name	First name and last name of the extension.
IP and Port	Display the IP and port number of the registered device.
Email	Display Email Notification status for the extension. When notification is waiting for be sent, shows and once sent it will display
Terminal Type	Displays extension type. • SIP User • IAX User • Analog User • Ring Groups • Voicemail Groups

Interfaces Status

This section displays interface/port connection status on the UCM630X. The following example shows the interface status for UCM6304 with USB, WAN port, FXS1, FXS2 and FXO1 connected.

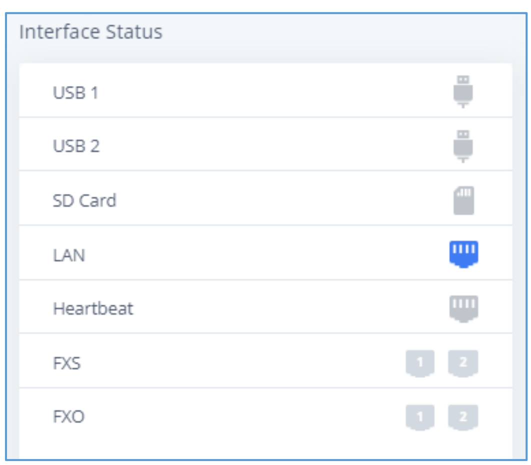
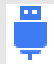
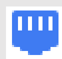
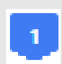
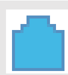
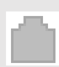


Figure 283: UCM6304 Interfaces Status

Table 138: Interface Status Indicators

	USB connected.
	USB disconnected.
	SD Card connected.
	SD Card disconnected.
	LAN/WAN connected.
	LAN/WAN not configured.
	LAN/WAN disconnected.
	FXS/FXO connected.
	FXS/FXO waiting.
	FXS/FXO busy.
	FXS/FXO not configured.
	FXS/FXO disconnected.

System Status

The UCM630X system status can be accessed via Web GUI→**Status**→**System Status**, which displays the following system information.

General

Under Web GUI→**System Status**→**System Information**→**General**, users could check the hardware and software information for the UCM630X. Please see details in the following table.

Table 139: System Status→General

System Status →System Information→General	
Model	Product model.
Part Number	Product part number.
System Time	Current system time. The current system time is also available on the upper right of each web page.
Up Time	System up time since the last reboot.
Boot	Boot version.
Core	Core version.
Base	Base version.
Program	Program version. This is the main software release version.
Recovery	Recovery version.
Lang	Lang version
GSWave	GSWave version

Network

Under Web GUI→**System Status→System Information→Network**, users could check the network information for the UCM630X. Please see details in the following table.

Table 140: System Status→Network

System Status→System Status→Network	
MAC Address	Global unique ID of device, in HEX format. The MAC address can be found on the label coming with original box and on the label located on the bottom of the device.
IPv4 Address	IPv4 address.
IPv6 Address Link	IPv6 address
Gateway	Default gateway address.
Subnet Mask	Subnet mask address.
DNS Server	DNS Server address.
Duplex Mode	Duplex Mode
Speed	Speed

Storage Usage

Users could access the storage usage information from Web GUI→**System Status**→**Dashboard**→**Storage Usage**. It shows the available and used space for Space Usage and Inode Usage.

Space Usage includes:

- **Configuration partition**
  This partition contains PBX system configuration files and service configuration files.
- **Data partition**
  Voicemail, recording files, IVR file, Music on Hold files etc.
- **USB disk**
  USB disk will display if connected.
- **SD Card**
  SD Card will display if connected.

Inode Usage includes:

- **Configuration partition**
- **Data partition**

Note:

Inode is the pointer used for file reference in the system. The system usually has limited resources of pointers

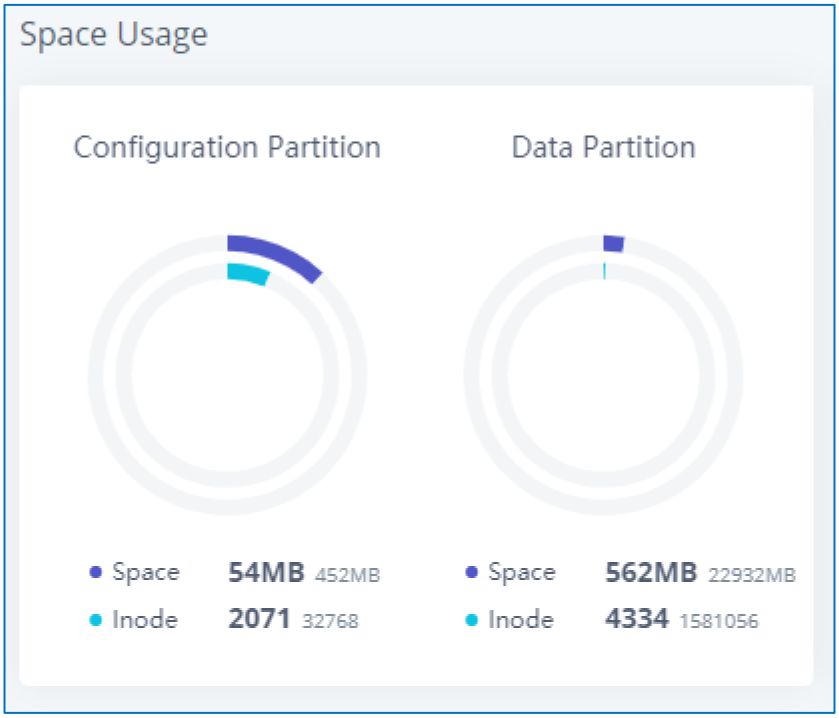


Figure 284: System Status→Storage Usage

Resource Usage

When configuring and managing the UCM630X, users could access resource usage information to estimate the current usage and allocate the resources accordingly. Under Web GUI → **System Status** → **Dashboard** → **Resource Usage**, the current CPU usage and Memory usage are shown in the pie chart.

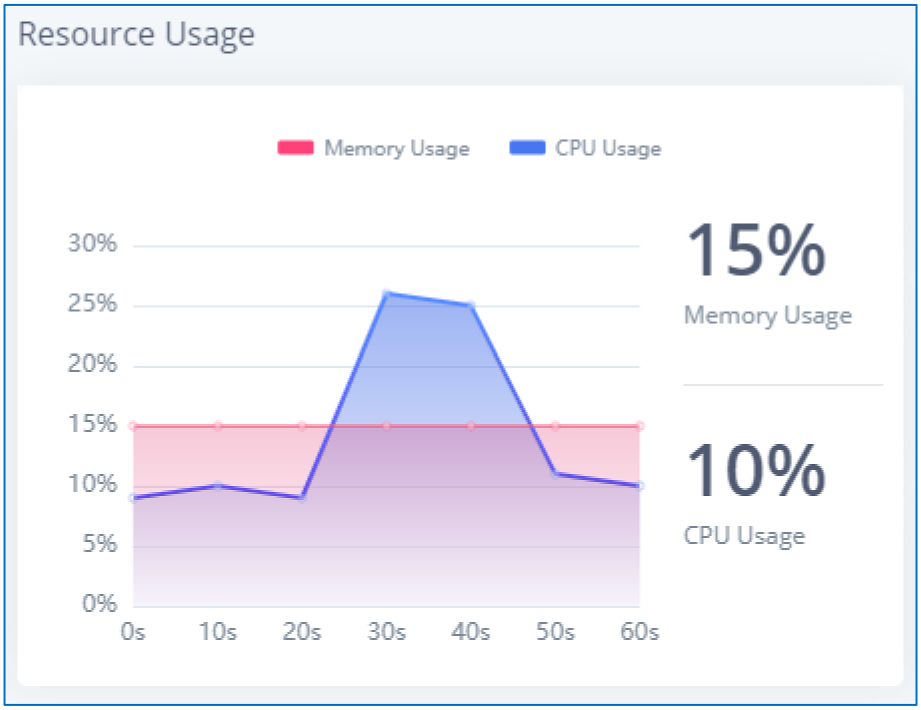


Figure 285: System Status→Resource Usage

System Events

The UCM630X can monitor important system events, log the alerts, and send Email notifications to the system administrator.

Alert Events List

The system alert events list can be found under Web GUI → **Maintenance** → **System Events**. The following event and their actions are currently supported on the UCM630X which will have alert and/or Email generated if occurred:

Table 141: Alert Events

Action index	Alert Events
1	Disk Usage
2	Modify Super Admin Password
3	Memory Usage
4	System Reboot
5	System Update
6	System Crash

7	Register SIP failed
8	Register SIP trunk failed
9	Restore Config
10	User login success
11	User login failed
12	SIP Internal Call Failure
13	SIP Outgoing Call through Trunk Failure
14	Fail2ban Blocking
15	SIP Lost Registration
16	SIP Peer Trunk Status
17	User Login Banned
18	HA failure warning
19	Emergency Calls
20	The CDR database is corrupted
21	NAS
22	Data Sync Backup
23	Remote Concurrent Calls
24	External Disk Status
25	CPU Usage Call Control

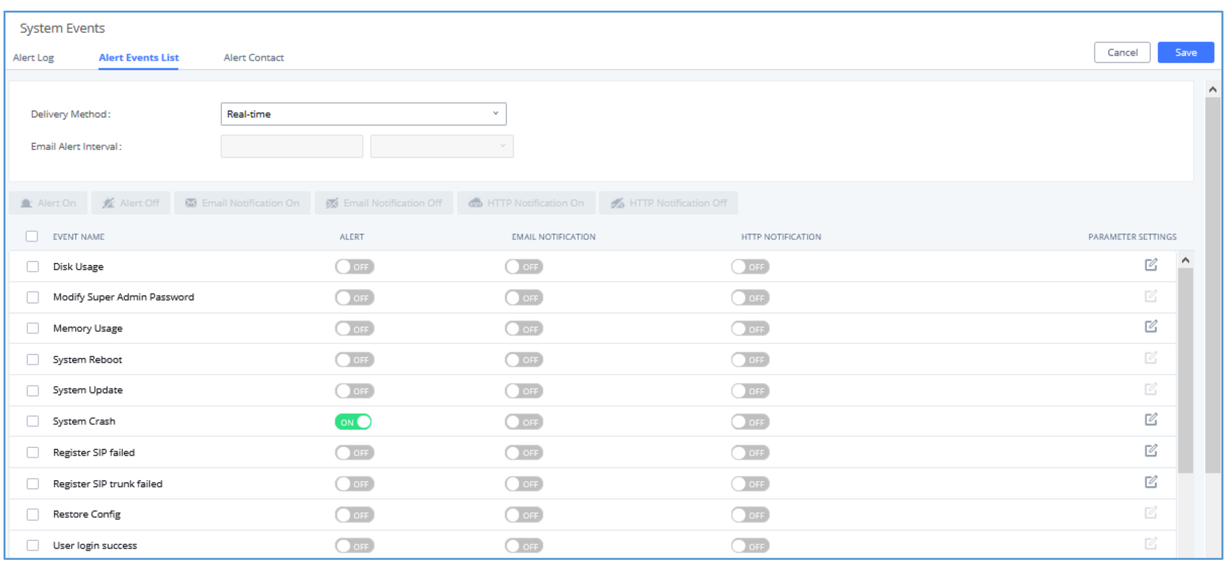


Figure 286: Alert Event List

Note: For users who have purchased a GDMS package, once the option **Alert Events Sync** is enabled under **RemoteConnect,** the triggered events will be pushed to their GDMS platform.
For more information, please refer to:
http://www.grandstream.com/sites/default/files/Resources/UCM63xx_RemoteConnect_User_Guide.pdf

Click on to configure the parameters for each event. See examples below.

1. Disk Usage

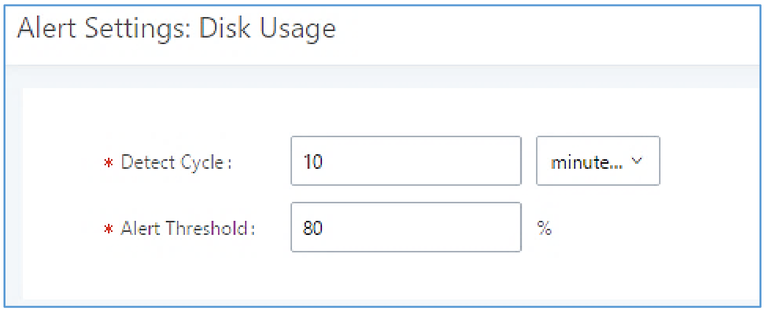


Figure 287: System Events→Alert Events Lists: Disk Usage

- **Detect Cycle**: The UCM630X will perform the internal disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold**: If the detected value exceeds the threshold (in percentage), the UCM630X system will send the alert.

Note: If the threshold is exceeded, any behavior of operating the disk will be rejected, including stopping file upload, IM writing, recording and CDR recording.

2. External Disk Usage

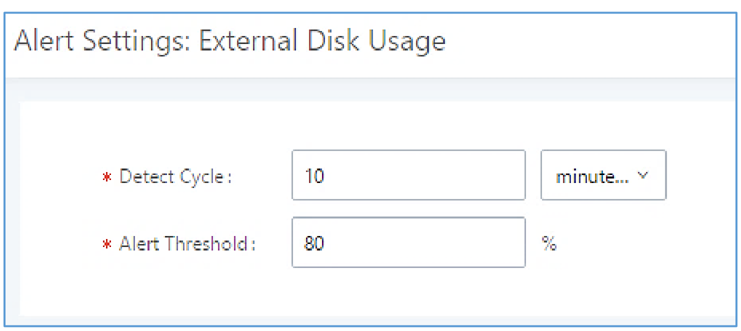


Figure 288: System Events→Alert Events Lists: External Disk Usage

- **Detect Cycle**: The UCM630X will perform the External disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold**: If the detected value exceeds the threshold (in percentage), the UCM630X system will send the alert.

3. Memory Usage

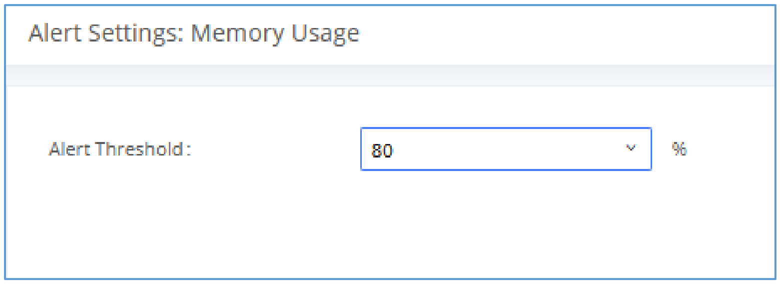


Figure 289: System Events→Alert Events Lists: Memory Usage

- **Alert Threshold**: If the detected value exceeds the threshold (in percentage), the UCM630X system will send the alert.

4. System Crash

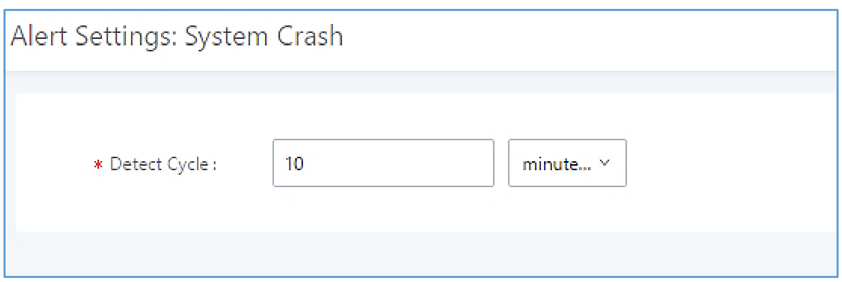


Figure 290: System Events→Alert Events Lists: System Crash

- **Detect Cycle**: The UCM will detect the event at each cycle based on the specified time. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

Click on the switch OFF ON to turn on/off the alert and Email notification for the event. Users could also select the checkbox for each event and then click on button "Alert On", "Alert Off", "Email Notification On", "Email Notification Off" to control the alert and Email notification configuration.

5. Modify Super Admin Password

Once the super administrator password is modified, the system will record the password modification event in the alarm log.

6. System Reboot

UCM will detect the system restart and will send an alert for it.

7. System Reboot

Once the system is upgraded, the system upgrade event will be recorded in the alarm log.

8. SIP registration failed

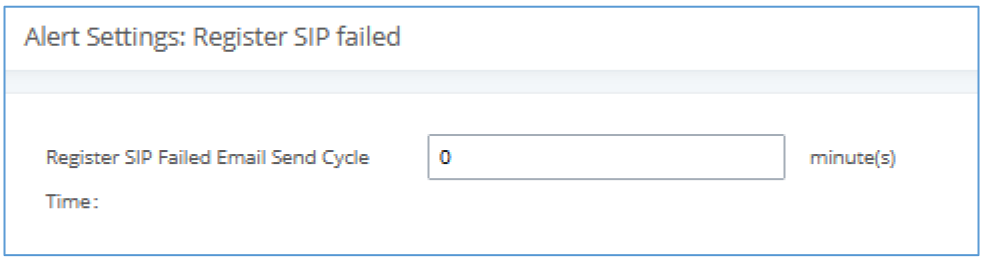


Figure 291:System Events→Alert Events Lists: Register SIP Failed

Configure the sending period of the SIP registration failure alert. The first registration failure alert of the same IP to the same SIP account will be sent immediately, and then no alerts will be sent for similar failure warnings in the cycle time. After the cycle time expires, an alert will be sent again to count the number of occurrences of similar SIP registration failure alerts during the cycle. When set to 0, alerts are always sent immediately.

9. Register SIP trunk failed

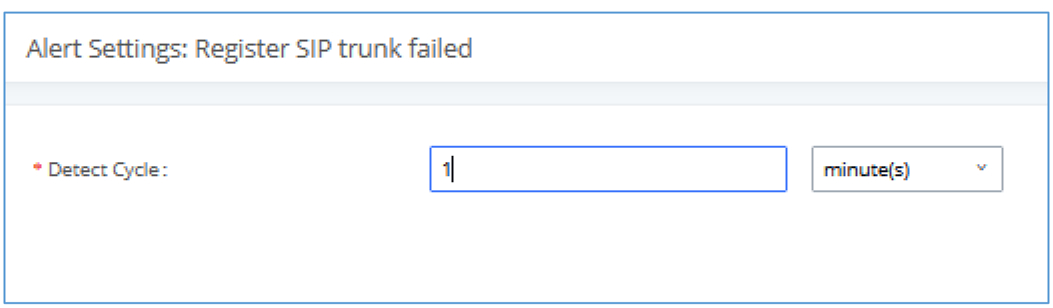


Figure 292: System Events→Alert Events Lists: Register SIP Trunk Failed

- **Detect Cycle:** The UCM will detect the failure of SIP trunk registration at a set interval. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

10. Restore Config

Once the system configuration is restored, the configuration restoration event will be recorded in the alert log.

11. User login success

Successful user login events will be recorded in the alert log.

12. User login failed

User login failure events will be recorded in the alert log.

13. SIP Internal Call Failure

If the system SIP extension call fails within the office, the event will be recorded in the alert log.

14. SIP Outgoing Call through Trunk Failure

If the system SIP trunk outgoing call fails, the event will be recorded in the alert log.

15. Fail2ban blocking

If the system Fail2ban is blocking, the event will be recorded in the alert log.

16. SIP lost registration

If System SIP extension registration is lost, the event will be recorded in the alert log.

17. SIP peer trunk status

If the SIP peer trunks status is abnormal, the event will be recorded in the alert log.

18. User login banned

If user login is blocked, the event will be recorded in the alert log.

19. Emergency Calls

If the system generates an emergency call, the event will be recorded in the alert log.

20. NAS

If the system network disk is abnormal, the event will be recorded in the alarm log.

21. Data Sync Backup

If the system performs data synchronization and backup abnormalities, the event will be recorded in the alert log.

22. Remote concurrent calls

If the remote concurrent call fails, the event will be recorded in the alert log.

23. External disk status

If the external disk of the system is Connected/Disconnected, the event will be recorded in the alarm log.

24. CPU Flow control

The CPU flow control threshold is defined under **System Settings -> General Settings**, and the default value is 90%. When the traffic exceeds the predetermined value, the event will be recorded in the alert log and new calls will be prohibited.

Alert Log

Under Web GUI→**Maintenance**→**System Events**→**Alert Log**, system messages from triggered system events are listed as alert logs. The following screenshot shows system crash alert logs.

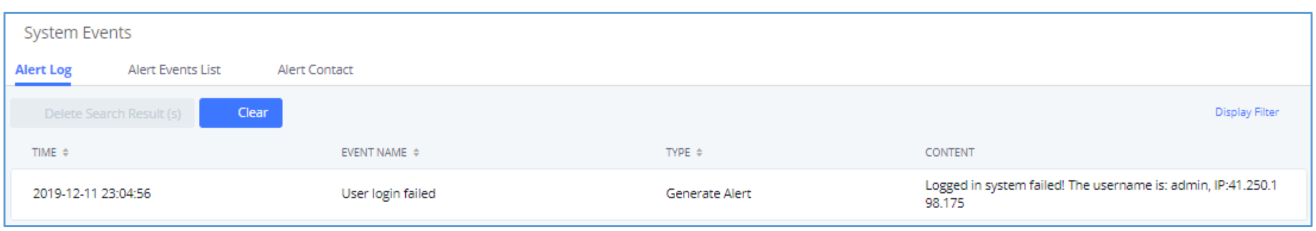


Figure 293: System Events→Alert Log

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 Filter. 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”.

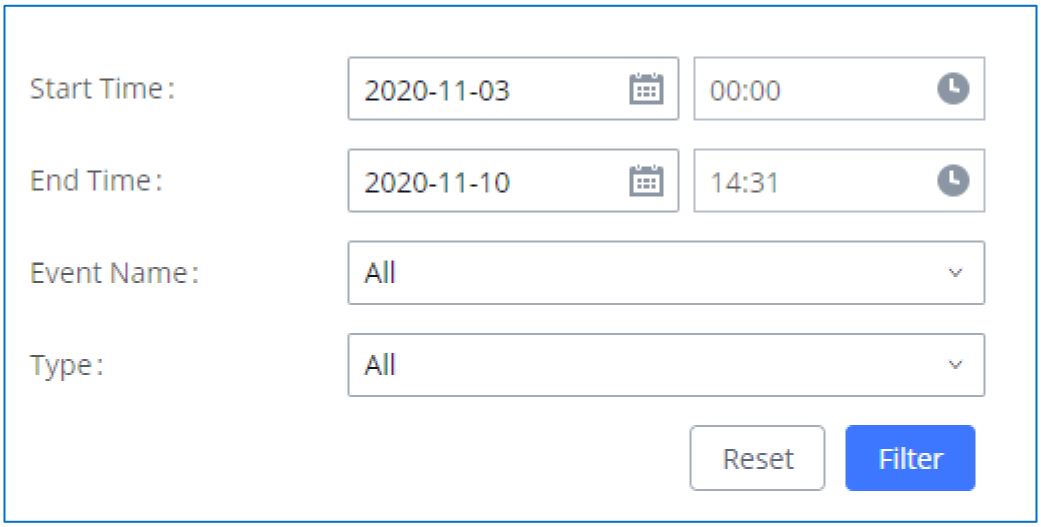


Figure 294: Filter for Alert Log

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 Web GUI→**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.

Table 142: Alert Contact

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**

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":"${WARNING_MSG}"}*
Notification Template	Customize the notification template to receive relevant alert information. By default: *{"action":"${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 *${TIME}* : Current System Time *${CPU_USED}* : CPU Usage *${MEM_USED}* : Memory Usage *${ACTION}* : Message Type. Refer to [Table 141: Alert Events] *${DISK_USED}* : Disk Usage *${EXTERNAL_DISK_USED}* : Disk Usage

CDR

CDR (Call Detail Record) is a data record generated by the PBX that contains attributes specific to a single instance of phone call handled by the PBX. It has several data fields to provide detailed description for the call, such as phone number of the calling party, phone number of the receiving party, start time, call duration, etc.

On the UCM630X, the CDR can be accessed under Web GUI→**CDR**→**CDR**. Users could filter the call report by specifying the date range and criteria, depending on how the users would like to include the logs to the report. Click on "Filter" button to display the generated report.

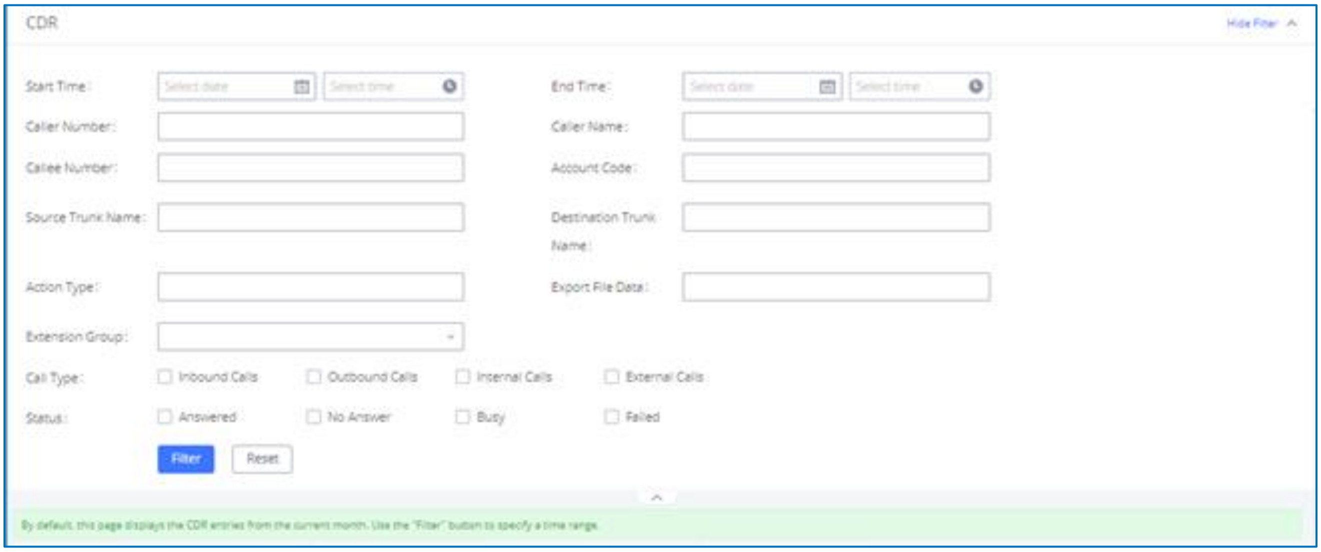


Figure 295: CDR Filter

Table 143: CDR Filter Criteria

Call Type	Groups the following: • **Inbound calls**: Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension. • **Outbound calls**: Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension. • **Internal calls**: Internal calls are calls from one internal extension to another extension, which are not sent over a trunk. • **External calls**: External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension.
Status	Filter with the call status, the available statuses are the following: • Answered • No Answer • Busy • Failed
Source Trunk Name	Select source trunk(s) and the CDR of calls going through inbound the trunk(s) will be filtered out.
Destination Trunk Name	Select destination trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.
Action Type	Filter calls using the Action Type, the following actions are available:

	• Announce • Announcement page • Dial • Announcements • Callback • Call Forward • Conference • DISA • Follow Me • IVR • Page • Parked Call • Queue • Ring Group • Transfer • VM • VMG • Video Conference • VQ_Callback • Wakeup • Emergency Call • Emergency Notify • SCA
Extension Group	Specify the Extension Group name to filter with.
Export File Data	Select the fields that will be exported, the following fields are available: • Account Code • Session • Premier caller • Action type • Source trunk name • Destination trunk name • Caller number • Caller ID • Caller name • Callee number • Answer by • Context • Start time

	• Answer time • End time • Call time • Talk time • Source channel • Dest channel • Call status • Dest channel extension • Last app • Last data • AMAFLAGS • UIQUEID • Call type • NAT
Account Code	Select the account Code to filter with. If pin group CDR is enabled, the call with pin group information will be displayed as part of the CDR under Account Code Field.
Start Time	Specify the start time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
End Time	Specify the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
Caller Number	Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out. User could specify a particular caller number or enter a pattern. '.' matches zero or more characters, only appears in the end. 'X' matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end. For example: **3XXX**: It will filter out CDR that having caller number with leading digit 3 and of 4 digits' length. **3.**: It will filter out CDR that having caller number with leading digit 3 and of any length.
Caller Name	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
Callee Number	Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out. **Note:** The "Callee Number" filter field supports specifying Pattern (example: 3XXX) or using Leading digits (example: 3.) as filtering options.

The call report will display as the following figure shows.

STATUS	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
	5555	1000	DIAL	2019-12-11 09:53:03	0:00:11	0:00:06		-

STATUS	PREMIER CALLER	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
	5555	5555	1000	DIAL	2019-12-11 09:53:03	0:00:11	0:00:06		-

Figure 296: Call Report

The CDR report has the following data fields:

- **Start Time**
  Format: 2019-12-11 09:53:03

- **Action Type**
  Example:
  IVR
  DIAL
  WAKEUP

- **Call From**
  Example format: 5555

- **Call To**
  Example format: 1000

- **Call Time**
  Format: 0:00:11

- **Talk Time**
  Format: 0:00:06

- **Account Code**
  Example format:
  Grandstream/Test

- **Status**
  Answered, Busy, No answer or Failed.

Users could perform the following operations on the call report.

- **Sort by "Start Time"**
  Click on the header of the column to sort the report by "Start Time". Clicking on "Start Time" again will

reverse the order.

- **Download Searched Results**
  Click on “Download Search Result(s)” to export the records filtered out to a .csv file.

- **Download All Records**
  Click on “Download All Records” to export all the records to a .csv file.

- **Delete All**

  Click on Delete All button to remove all the call report information.

- **Delete Search Result**

  On the bottom of the page, click on Delete Search Result (s) button to remove CDR records that appear on search results.

  Note: When deleting CDR, a prompt will now appear asking whether to delete all recording files or not.

- **Play/Download/Delete Recording File (per entry)**
  If the entry has audio recording file for the call, the three icons on the rightest column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

Click on to play the recording file; click on to download the recording file in .wav format; click on to delete the recording file (the call record entry will not be deleted).

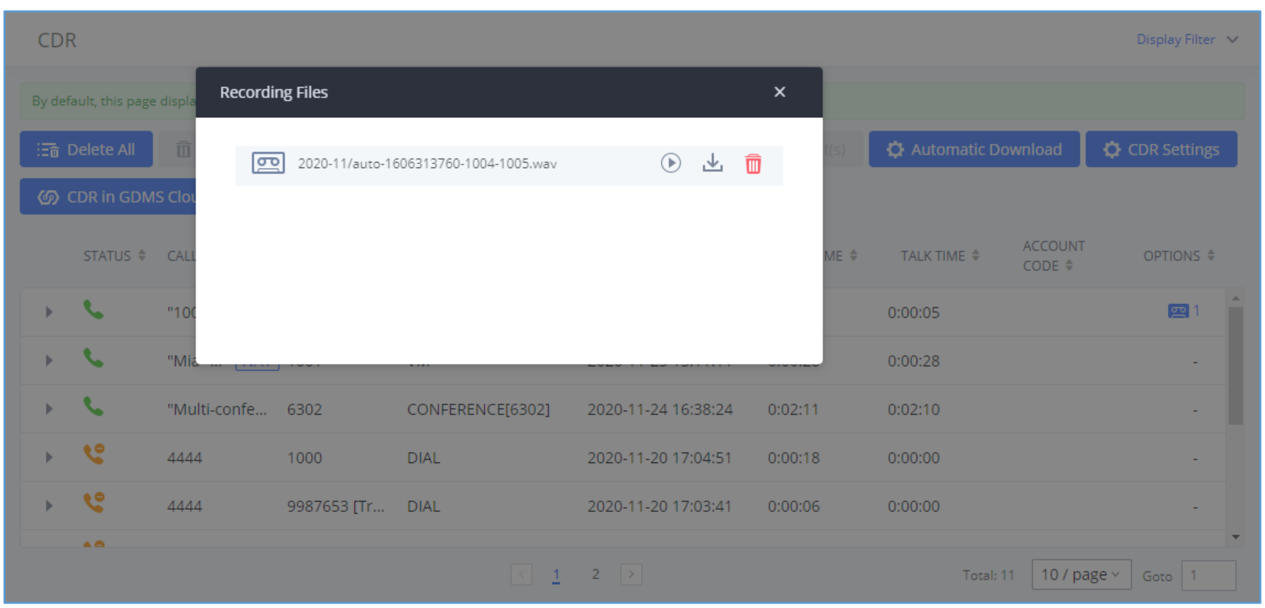


Figure 297: Call Report Entry with Audio Recording File

- **Automatic Download CDR Records**

  User could configure the UCM630X to automatically download the CDR records and send the records to multiple Email recipients in a specific hour. Click on "Automatic Download Settings" and configure the parameters in the dialog below.

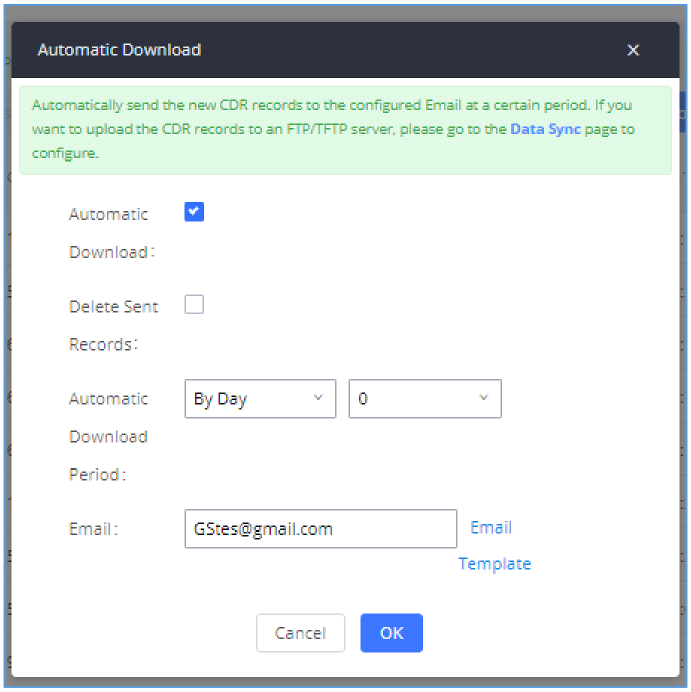
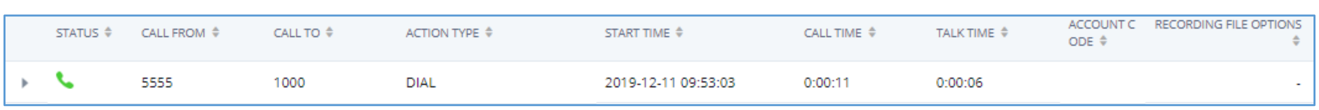


Figure 298: Automatic Download Settings

To receive CDR record automatically from Email, check "Enable" and select a time period "By Day" "By Week" or "By Month", select Hour of the day as well for the automatic download period. Make sure you have entered an Email or multiple email addresses where to receive the CDR records.

Note: users have the option to delete the sent records **"Delete Sent Records"**

Starting from UCM630X firmware 1.0.10.x, transferred call will no longer be displayed as a separate call entry in CDR. It will display within call record in the same entry. CDR new features can be found under Web GUI→**CDR**→**CDR**. The user can click on the option icon for a specific call log entry to view details about this entry, such as premier caller and transferred call information.



	STATUS	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
		5555	1000	DIAL	2019-12-11 09:53:03	0:00:11	0:00:06		-

Figure 299: CDR Report

"ablili lolo" 1000... 9985632 DIAL 2019-12-10 03:23:14 0:00:13 0:00:07 1

STATUS	PREMIER CALLER	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
	1000	"ablili lolo" 1000...	9985632	DIAL	2019-12-10 03:23:14	0:00:00	0:00:00		-
	1000	"ablili lolo" 1000...	6500	QUEUE[6500]	2019-12-10 03:23:14	0:00:00	0:00:00		1
	1000	"ablili lolo" 1000...	5555	QUEUE[6500]	2019-12-10 03:23:14	0:00:13	0:00:07		-

Figure 300: Detailed CDR Information

Downloaded CDR File

The downloaded CDR (.csv file) has different format from the Web GUI CDR. Here are some descriptions.

- **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

Figure 301: 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

Figure 302: 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

Figure 303: 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.

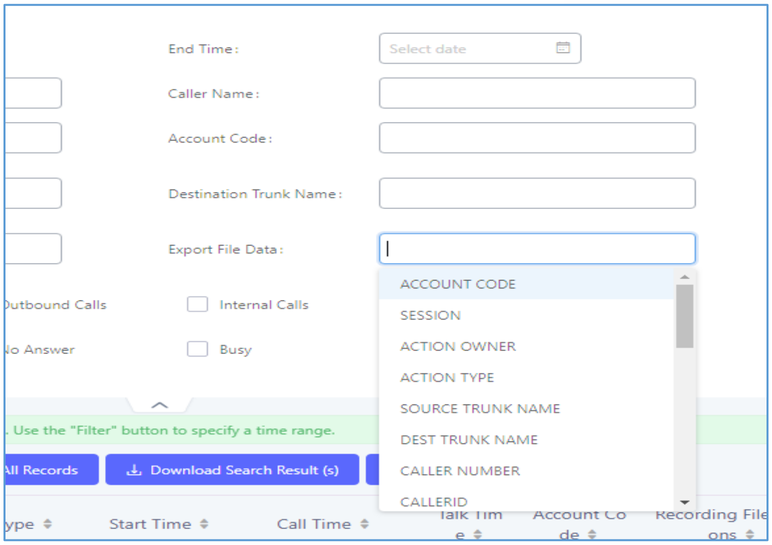


Figure 304: CDR Export File data

CDR in GDMS Cloud

Cloud Storage for CDR Record which can be displayed under **CDR → CDR in GDMS Cloud**.

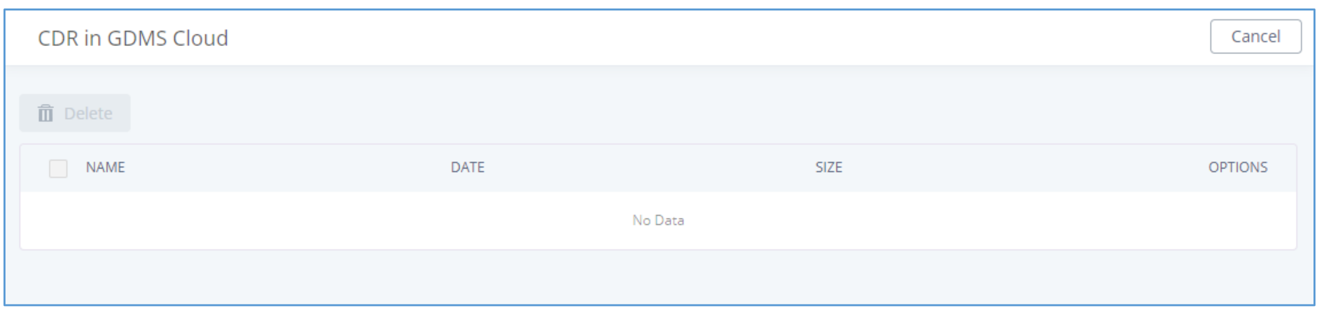


Figure 305: CDR in GDMS Cloud

Statistics

CDR Statistics is an additional feature on the UCM630X which provides users a visual overview of the call report across the time frame. Users can filter with different criteria to generate the statistics chart.

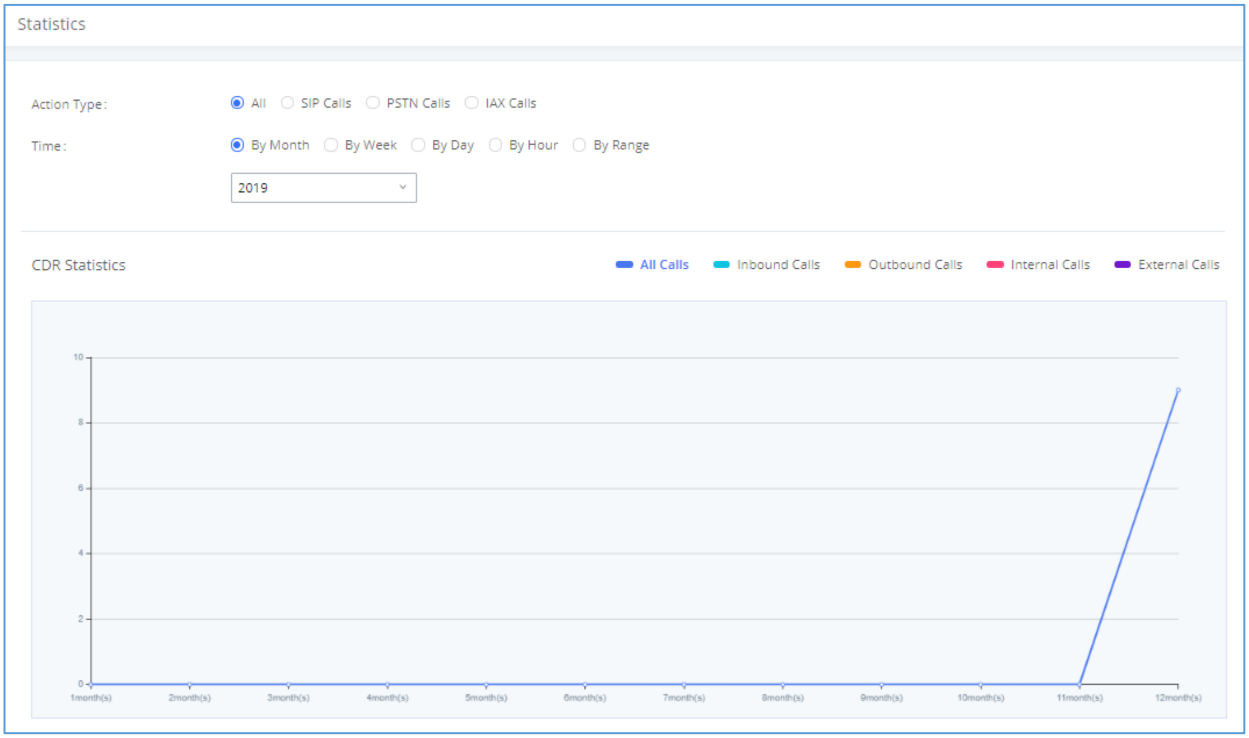


Figure 306: CDR Statistics

Table 144: CDR Statistics Filter Criteria

Trunk Type	Select one of the following trunk type. • All • SIP Calls • PSTN Calls
Call Type	Select one or more in the following checkboxes. • Inbound calls • Outbound calls • Internal calls • External calls • All calls
Time Range	• 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. For example, 2016-01 To 2016-03.

Recording Files

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.

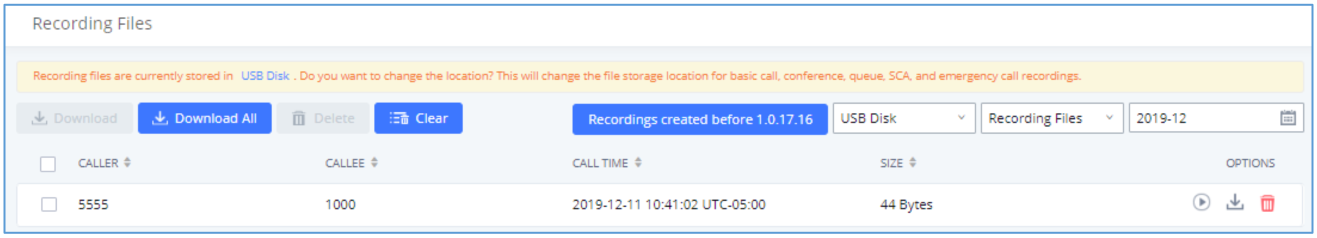


Figure 307: CDR→Recording Files

- Click on "**Delete Selected Recording Files**" to delete the recording files.
- Click on "**Delete All Recording Files**" to delete all recording files.
- Click on "**Batch Download Recording Files**" in order to download the selected recording files.
- Click on "**Download All Recording Files**" to download all recordings files.
- 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.

USER PORTAL

Users could log into their web GUI portal using the extension number and user password. When an extension is created in the UCM630X, the corresponding user account for the extension is automatically created. The user portal allows access to a variety of features which include user information, extension configuration and CDR as well as settings and managing value-added features like Call Queue, Wakeup Service and CRM.

Users also can access their personal data files (call recordings, Voicemail Prompts …).

The login credentials are configured by Super Admin. The following figure shows the dialog of editing the account information by Super Admin. The Username must be the extension number and it is not configurable, and the password is set on “User Password” field and it should not be confused with the SIP extension password.

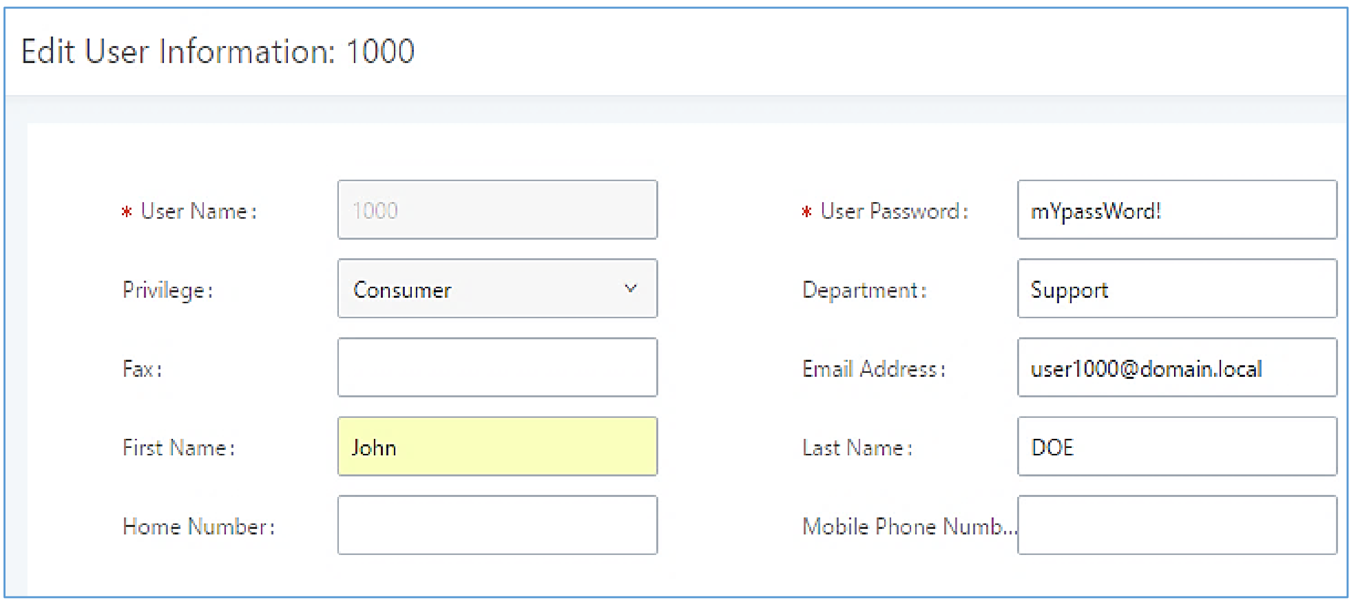


Figure 308: Edit User Information by Super Admin

The following screenshot shows an example of login page using extension number 1000 as the username.

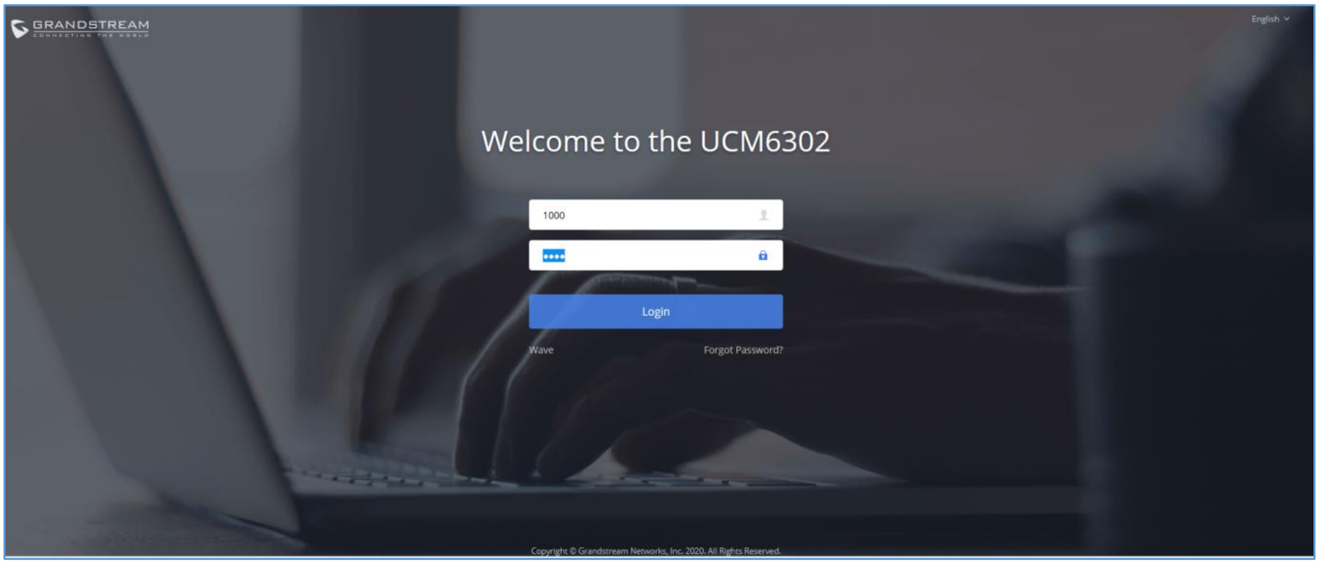


Figure 309: User Portal Login

After login, the Web GUI display is shown as below.

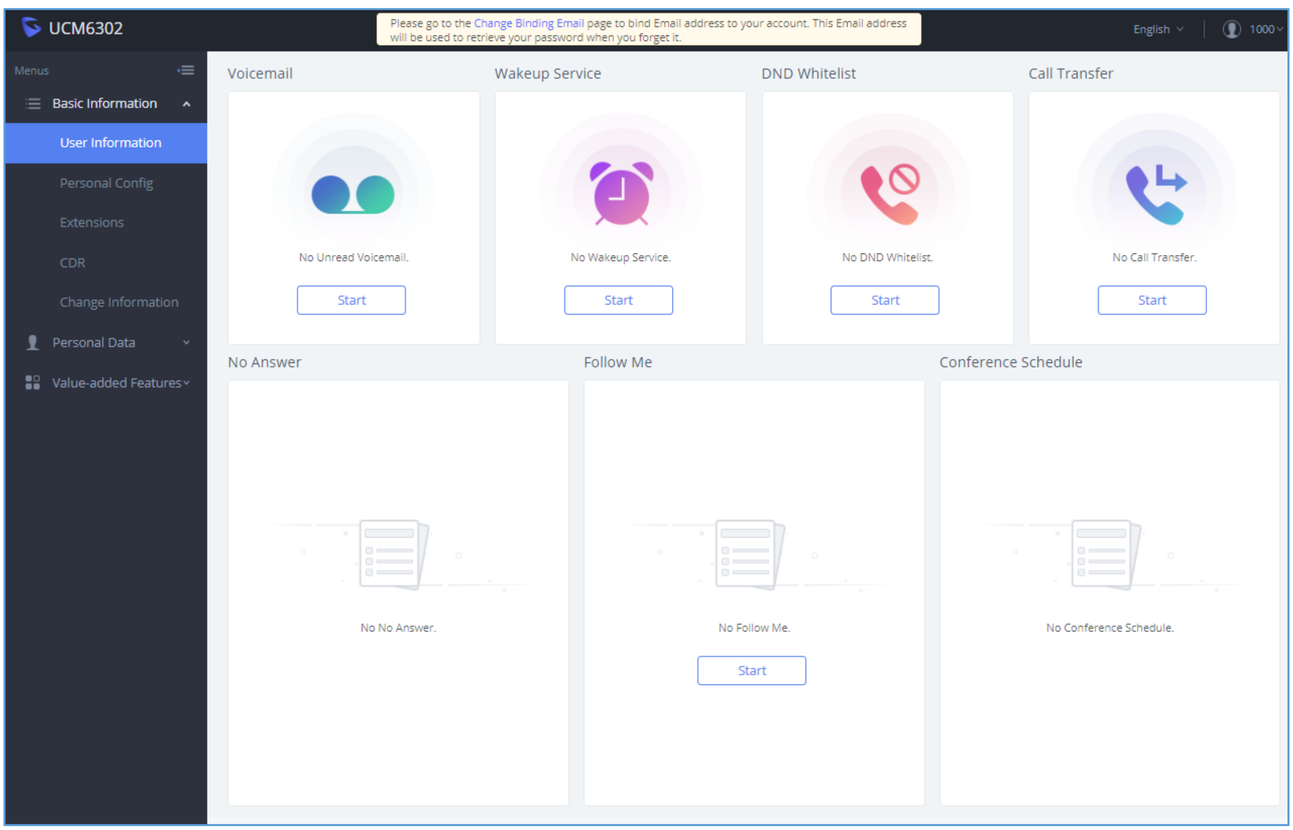


Figure 310: User Portal Layout

After successful login, the user has the following three configuration tabs:

Basic Information

Under this menu, the user can configure and change his/her personal information including (first name, last name, password, email address, department…). And they can also set and activate their extension features (presence status, call forward, DND ….) to be reflected on the UCM.
Also, the user can see from this menu the Call Details Records and search for specific ones along with the possibility to download the records on CSV format for later usage.

Personal Data

Under this section, the user can access and manage their personal data files which includes (voicemail files, call recordings …) along with the possibility to set Follow me feature to without requesting the Super admin to set the feature from admin account.

Value-added Features

On this section, the user has access to manage and use all rich value-added features which includes.

+ If user is a member of call queue, they can check the queue's activity from the "Call Queue" section.
+ Create and enable Wake Up service.
+ Enable and configure CRM connection to either SugarCRM or Salesforce.

For the configuration parameter information in each page, please refer to ***[Table 145: User Management→Create New User]*** for options in **User Portal→Basic Information→User Information** page; please refer to ***[EXTENSIONS]*** for options in **User Portal→Basic Information→Extension** page; please refer to ***[CDR]*** for **User Portal→Basic Information→CDR** page.

MAINTENANCE

User Management

User management is on Web GUI→**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.

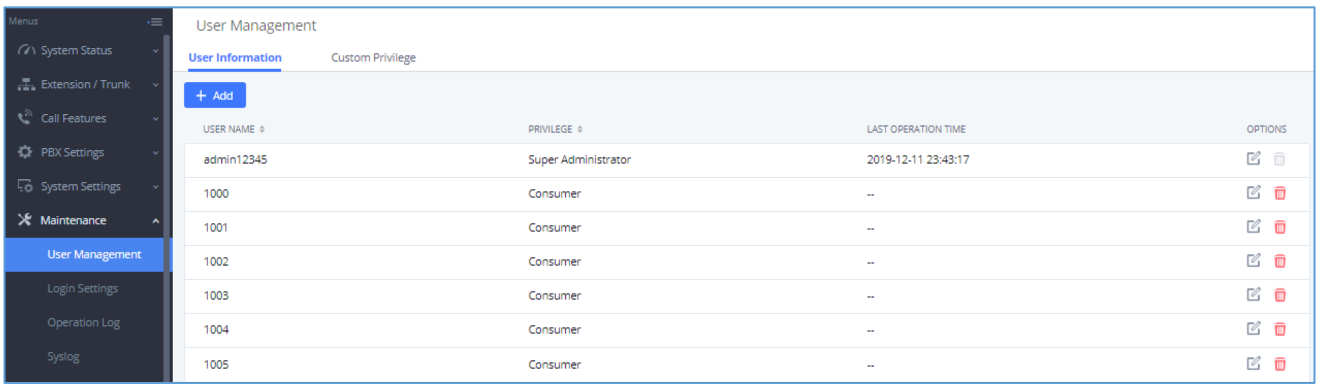


Figure 311: User Management Page Display

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.

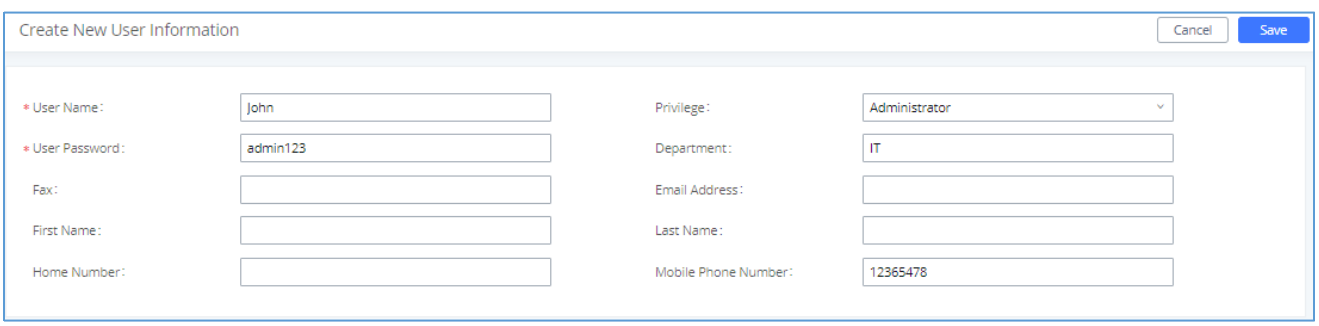


Figure 312: Create New User

Table 145: User Management→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 ".
Privilege	This is the role of the Web GUI user. Currently only "Admin" is supported when Super Admin creates a new user.
Department	Enter the necessary information to keep a record for this user.
Email Address	
First Name	
Last Name	
Home Number	
Phone Number	

Once created, the Super Admin can edit the users by clicking on or delete the user by clicking on .

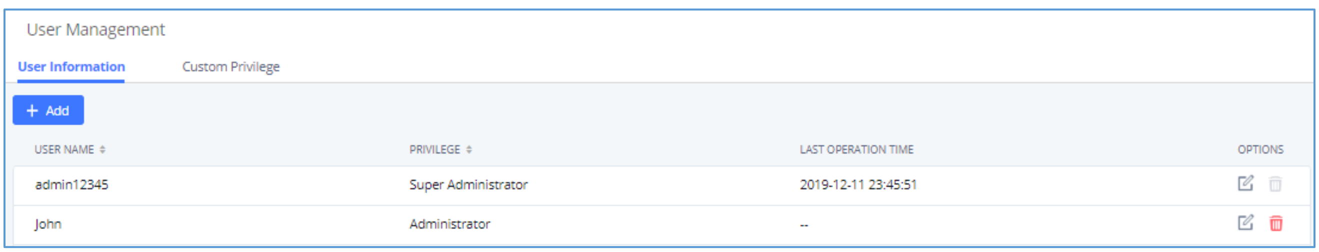


Figure 313: User Management – New Users

Custom Privilege

Four privilege levels are supported:

- **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 "Admin" privilege
  - Super Admin can edit and delete one or more users with "Consumer" privilege
  - Super Admin can view operation logs generated by all users.
  - By default, the user account "admin" is configured with "Super Admin" privilege and it is the only user with "Super Admin" privilege. The Username and Privilege level cannot be changed or deleted.
  - Super Admin could change its own login password on Web GUI→**Maintenance→Login Settings** page.

- Super Admin could view operations done by all the users in Web GUI→**Maintenance→User Management→Operation Log**

- **Administrator**
  - Users with "Admin" privilege can only be created by "Super Admin" user.
  - "Admin" privilege users are not allowed to access the following pages:

    Maintenance→Upgrade

    Maintenance→Cleaner

    Maintenance→Reset/Reboot

    Settings→User Management→Operation Log
  - "Admin" privilege users cannot create new users for login.

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 to edit the "Admin" account and include backup operation permission for these types of users.

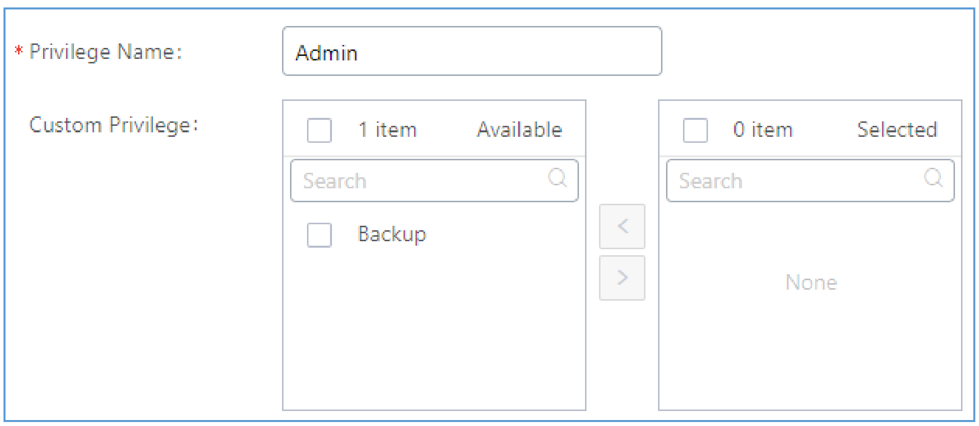


Figure 314: Assign Backup permission to "Admin" users

- **Consumer**
  - A user account for Web GUI login is created automatically by the system when a new extension is created.
  - The user could log in the Web GUI with the extension number and password to access user information, extension configuration, CDR of that extension, personal data, and value-added features. For more details; please refer to [User Portal Guide](#).
  - The SuperAdmin user can click on on the "General_User" in order to enable/disable the custom privilege from deleting their own recording files, changing SIP credentials, and disabling voicemail service in their user portal account.

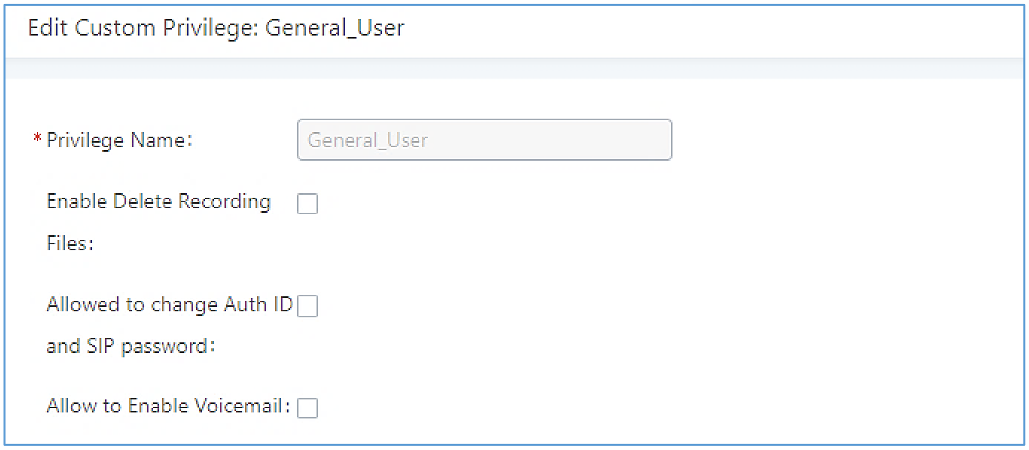


Figure 315: General User

- **Custom Privilege**

The Super Admin user can create users with different privileges. 33 items are available for privilege customization.

- API Configuration
- API Configuration
- Backup
- Callback
- Call Queue
- CDR Recording Files
- CDR Records
- CDR Statistics
- Audio Conference
- Dial By Name
- DISA
- Emergency Calls
- Event List
- Extensions
- Outbound Routes
- Inbound Routes
- Feature Codes
- IVR
- Paging/Intercom
- Parking Lot
- Pickup Groups

- PMS - Wakeup Service
- Ring Groups
- SCA
- Speed Dial
- System Status
- System Events
- Time Settings
- Video Conference
- Voicemail
- Voice Prompt
- Wakeup Service
- Zero Config
- LDAP Server
- UCM RemoteConnect
- Announcement.

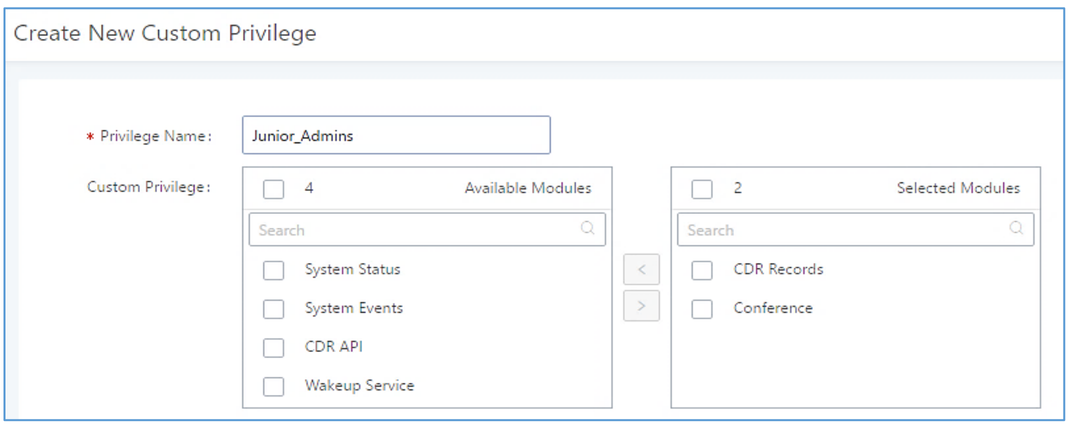


Figure 316: Create New Custom Privilege

Log in UCM630X as super admin and go to **Maintenance→User Management→Custom Privilege**, create privilege with customized available modules.

To assign custom privilege to a sub-admin, navigate to UCM Web GUI→**Maintenance→User Management→User Information**→Create New User/Edit Users, select the custom privilege from "Privilege" option.

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.

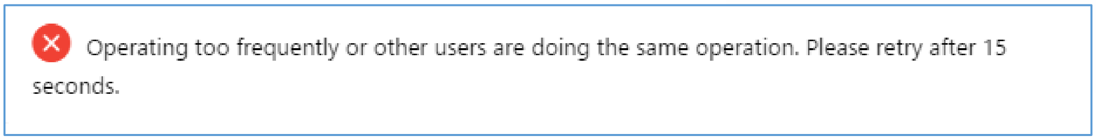


Figure 317: Multiple User Operation Error Prompt

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 Web GUI→**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.

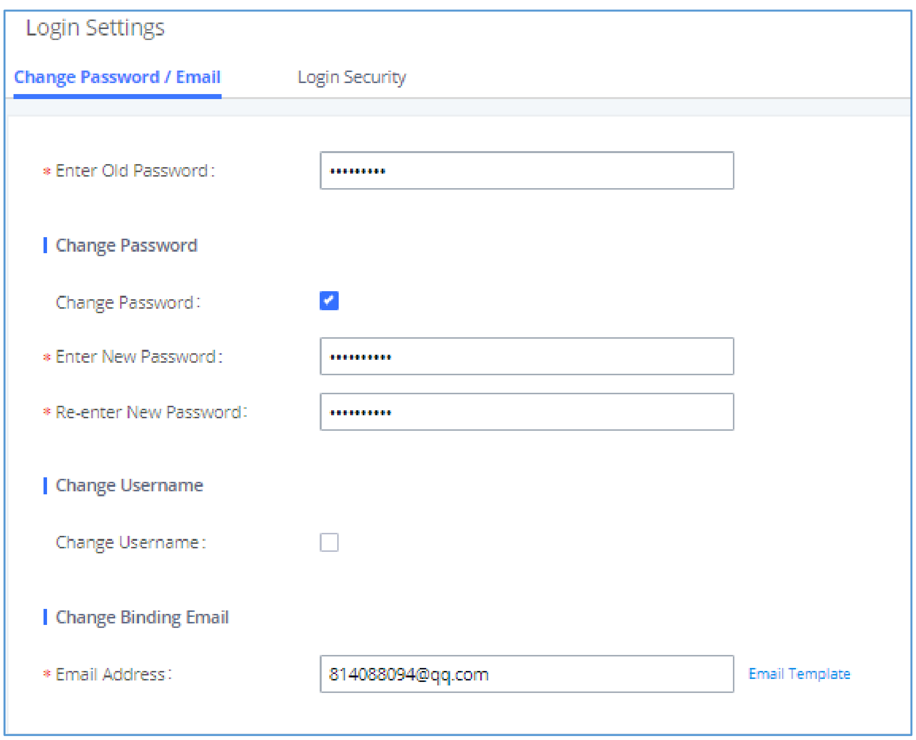


Figure 318: Change Password

Enter Old Password	Enter the Old Password for UCM630X
Change Password	Enable Change Password
Enter New Password	Enter the New Password for UCM630X
Re-enter New Password	Retype the New Password for UCM630X
Change Username	Enable Change Username
Please enter the username	Enter the Username
Email Address	The Email address is the User Email Address. It is used for receiving password information if the user forgets his password.

Change Username

UCM630X allows users now to change Super Administrator username.

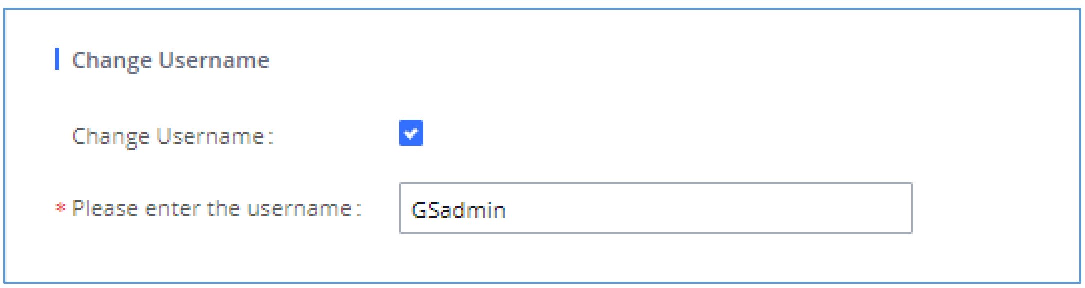


Figure 319: Change Username

Change binding Email

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 Web GUI→ **Maintenance→Login Settings→Change Password / Email**

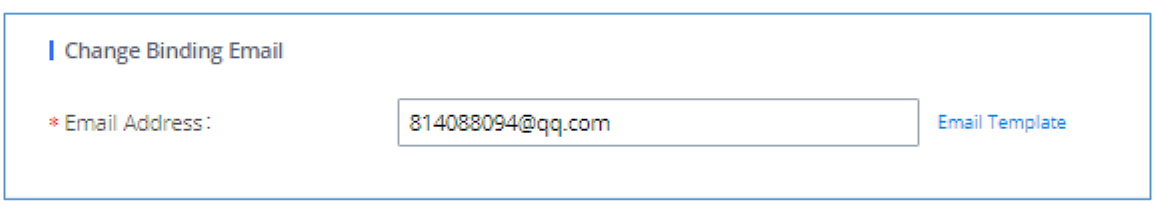


Figure 320: Change Binding Email

Table 146: Change Binding Email option

Email Address	Email Address is used to retrieve password when password is lost

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 web GUI→**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.
If set to 0, there is no timeout for the Web GUI login session and the user will not be automatically logged out.

"**Maximum number of login attempts**" can prevent the UCM630X from brutal force decryption, if this number is exceeded user IP address will be banned from accessing the UCM for a period of time based on user configuration, the default value is 5.

"**User ban period**" specify the period of time in minutes an IP will be banned from accessing the UCM if the User max number of try login is exceeded, the default value is 5.

"**Login Banned User List**" show the list of IPs' banned from the UCM.

"**Login Whitelist**" User can add a list of IPs' to avoid the above restriction, thus, they can exceed the User max number of try login.

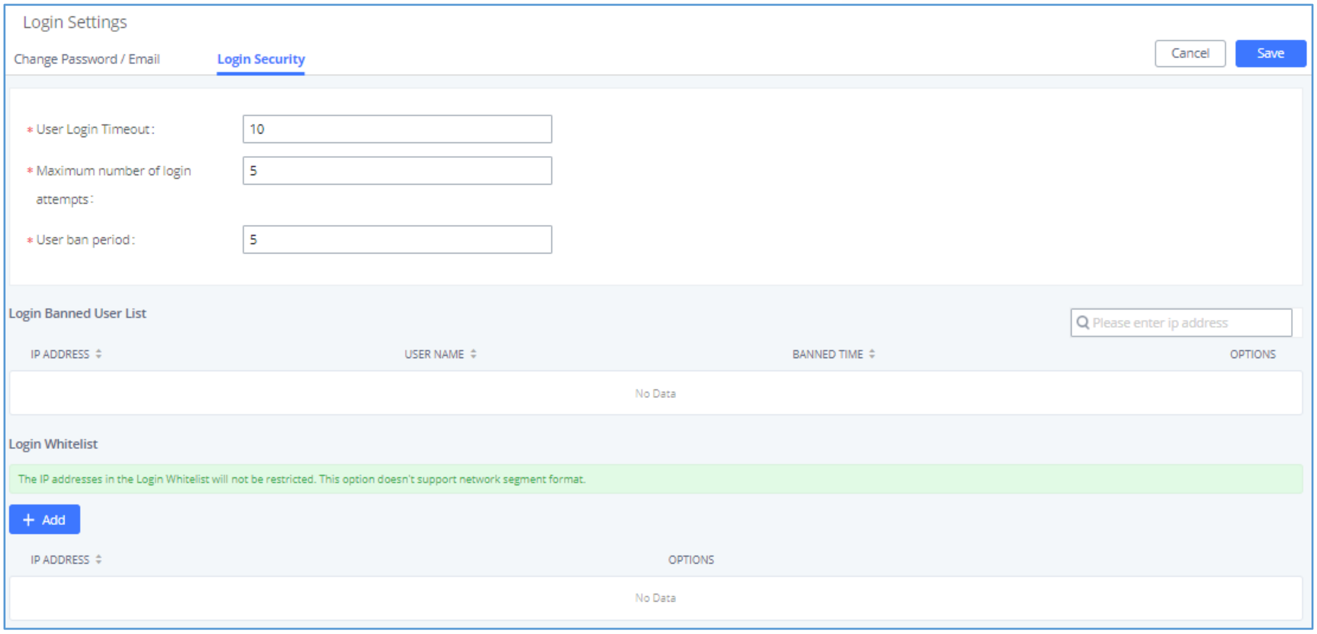


Figure 321: Login Timeout Settings

Operation Log

Super Admin has the authority to view operation logs on UCM630X Web GUI→**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 and etc. There are 7 columns to record the operation details “Date”, “Username”, “IP Address”, “Results”, “Page Operation”, “Specific Operation” and “Remark”.

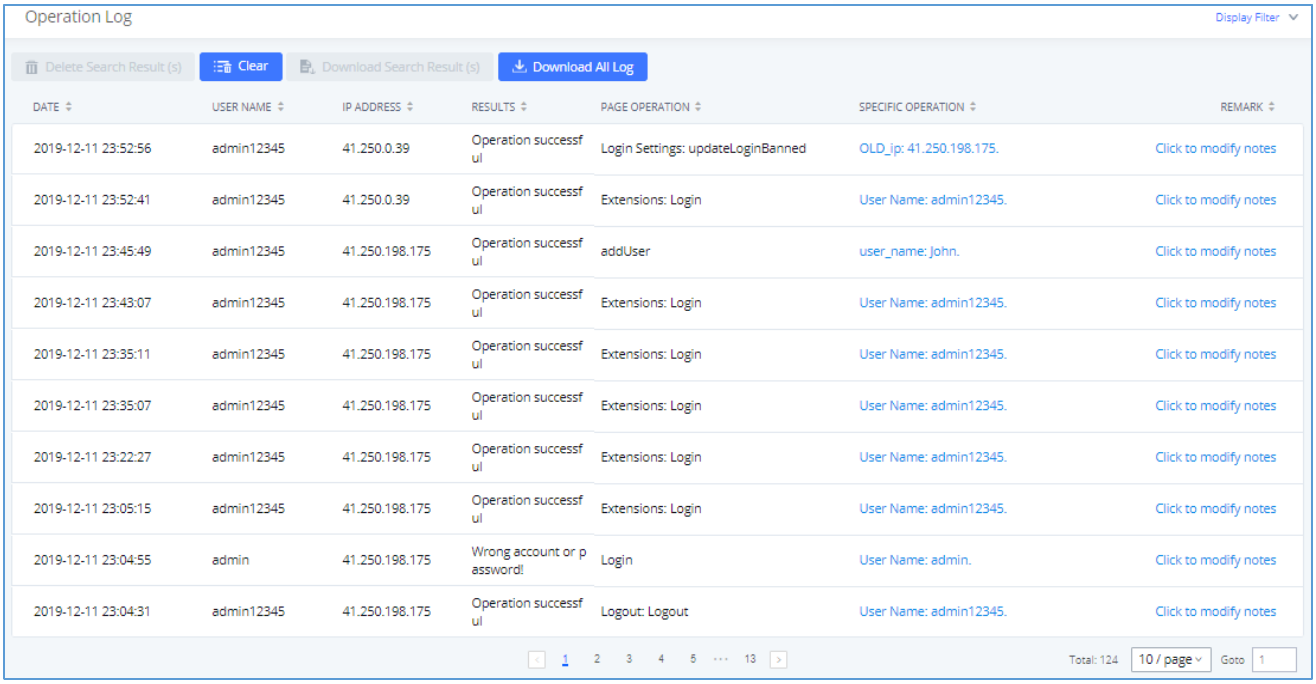


Figure 322: Operation Logs

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.

Table 147: Operation Log Column Header

Date	The date and time when the operation is executed.
Username	The username of the user who performed the operation.
IP Address	The IP address from which the operation is 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 to view the options and values configured by this operation.
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”.

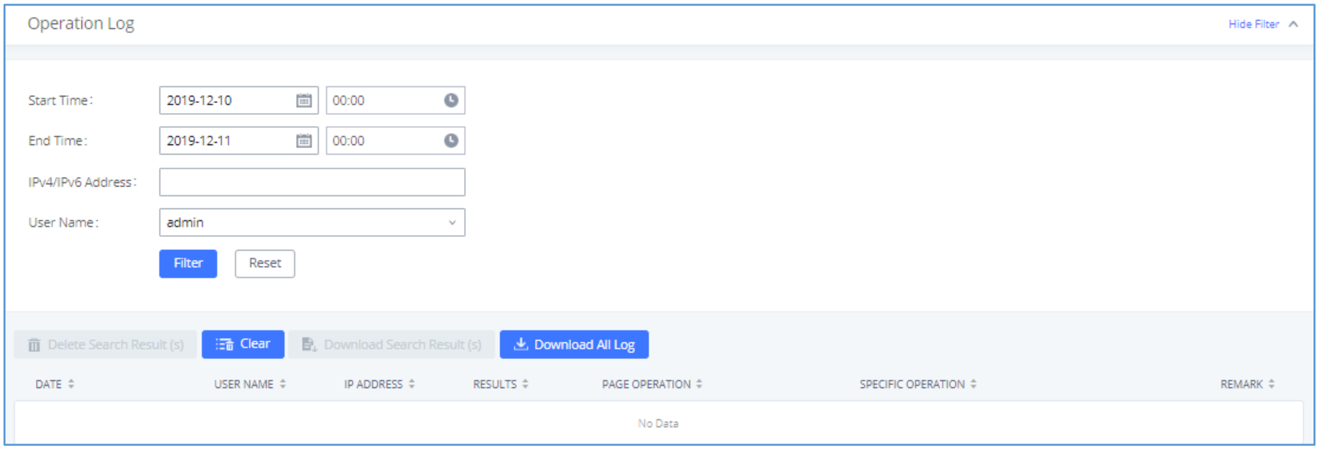
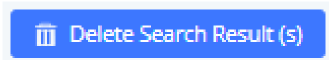


Figure 323: Operation Logs Filter

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.

Upgrading

The UCM630X can be upgraded to a new firmware version locally. And in order to do that, please follow the below steps:

1. Download the latest UCM630X firmware file from the following link and save it in your PC.

   http://www.grandstream.com/support/firmware

2. Log in the Web GUI as administrator in the PC.
3. Go to Web GUI→**Maintenance**→**Upgrade**, upload the firmware file by clicking on "choose file to upload" and select the firmware file from your PC. The default firmware file name is UCM630Xfw.bin

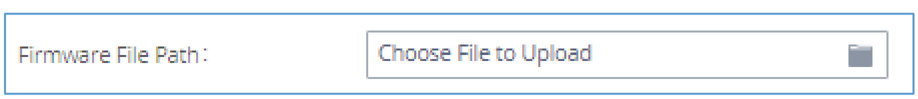


Figure 324: Local Upgrade

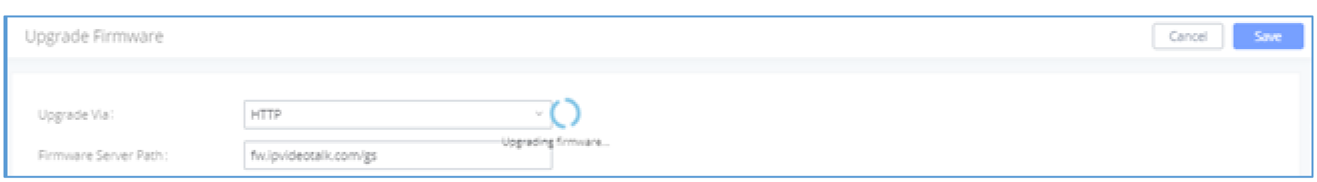


Figure 325: Upgrading Firmware Files

4. Wait until the upgrading process is successful and a window will be popped up in the Web GUI.

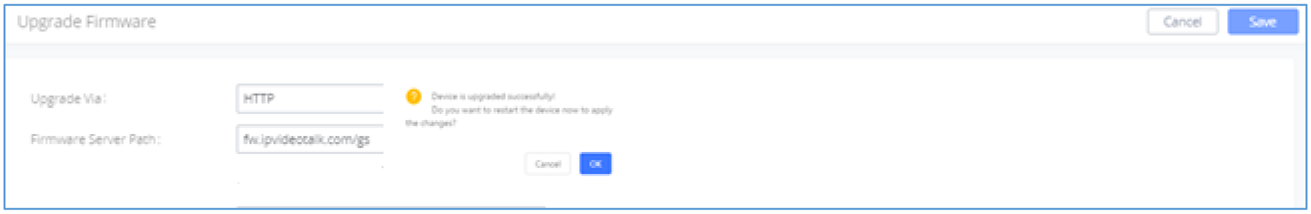


Figure 326: Reboot UCM630X

5. Click on "OK" to reboot the UCM630X and check the firmware version after it boots up.

⚠ **Notes:**

- Please do not interrupt or power cycle the UCM630X during upgrading process.
- The firmware file name allows the use of the special characters besides the following restricted characters: # $ ^ & * + ( ) [ ] / ; ' | , < > ?

No Local Firmware Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have TFTP/HTTP/HTTPS server, some free windows version TFTP servers are available for download from
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
http://tftpd32.jounin.net

Please check our website at http://www.grandstream.com/support/firmware for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the UCM630X to the same LAN segment;
3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the UCM630X web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the UCM630X.

End users can also choose to download a free HTTP server from http://httpd.apache.org/ or use Microsoft IIS web server.

Backup

The UCM630X configuration can be backed up locally or via network. The backup file will be used to restore the configuration on UCM630X when necessary.

Backup/Restore

Users could backup the UCM630X configurations for restore purpose under Web GUI→**Maintenance→Backup→Backup/Restore**.
Click on "Backup" to create a new backup file. Then the following dialog will show.

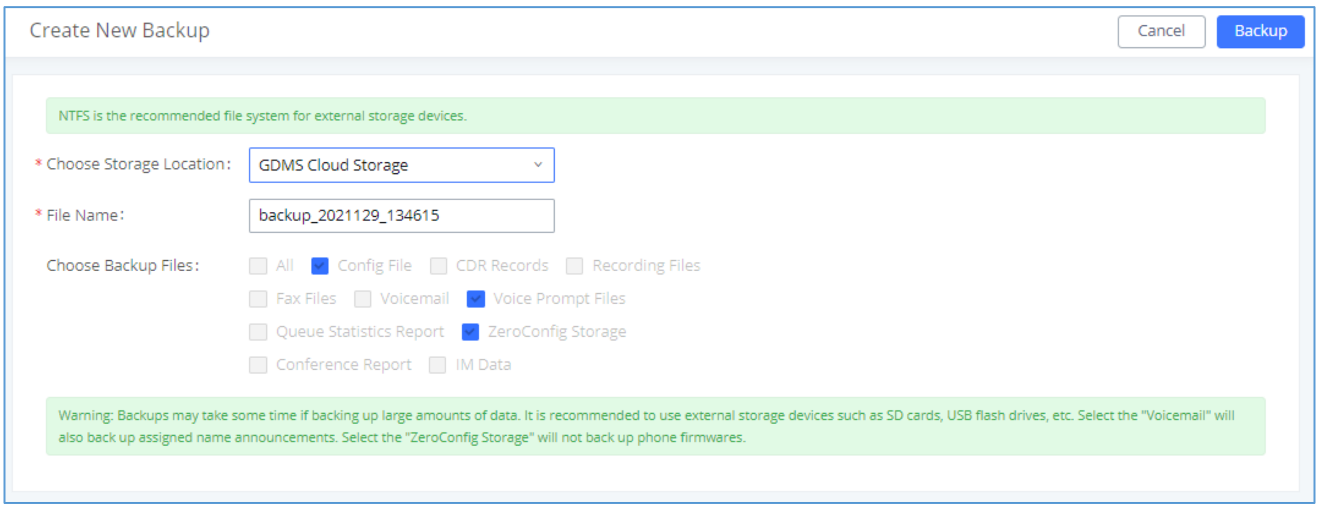


Figure 327: Create New Backup

1. Choose the type(s) of files to be included in the backup.
2. Choose where to store the backup file: USB Disk, SD Card, Local, NAS or GDMS.
3. Name the backup file.
4. Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download , restore , or delete it from the UCM630X internal storage or the external device.

Click on Upload to upload backup file from the local device to UCM630X. The uploaded backup file will also be displayed in the web page and can be used to restore the UCM630X.
Note: users can restore backups of models with more FXO ports to models with less FXO ports as long as the configurations related to the extra FXO ports are removed.

Please make sure the FXO port settings, total number of extensions and total number of conference rooms are compactable before restoring to another UCM model. Otherwise it will prompt a warning and stop the restore process as shown below:

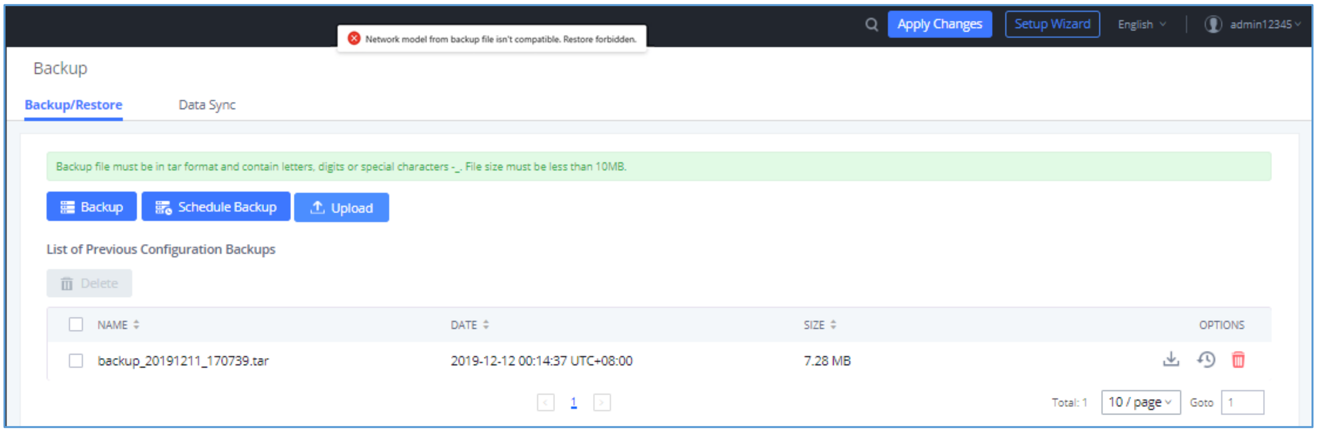


Figure 328: Restore Warning

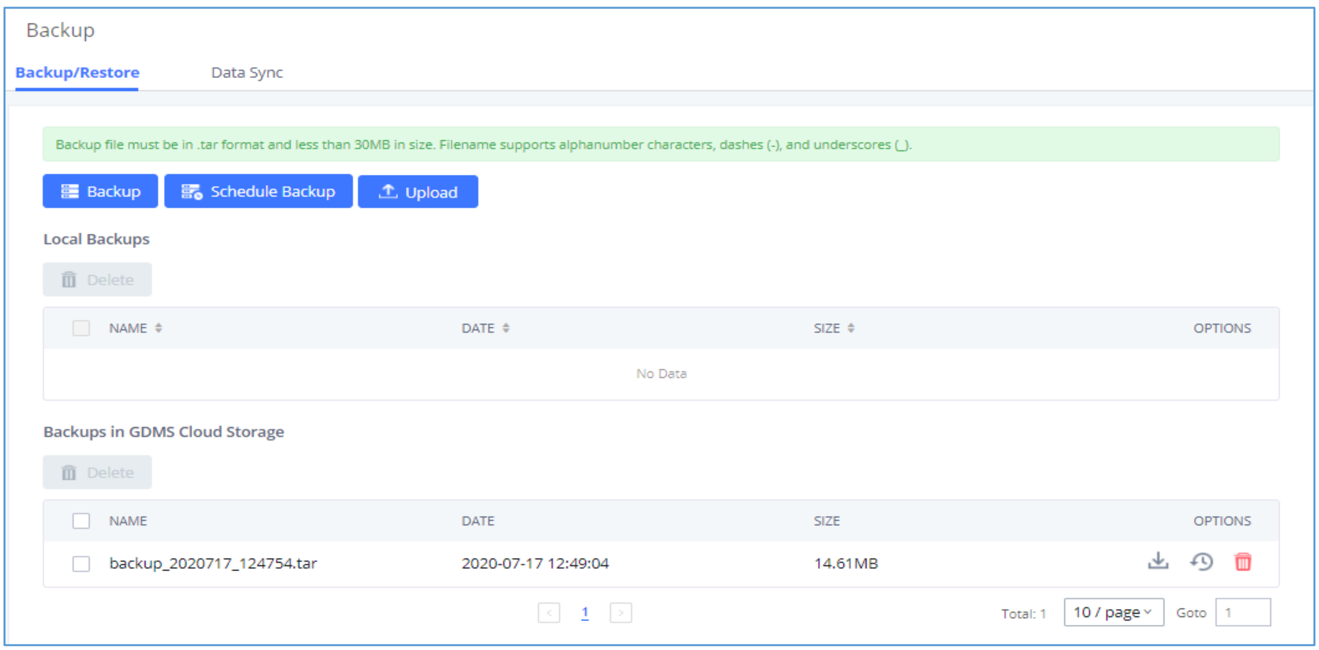
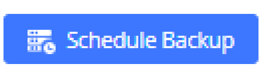


Figure 329: Backup / Restore

The 

option allows UCM to perform automatically backup on the user specified time. Regular backup file can only be stored in USB / SD card / SFTP server. User is allowed to set backup time from 0-23 and how frequent the backup will be performed.

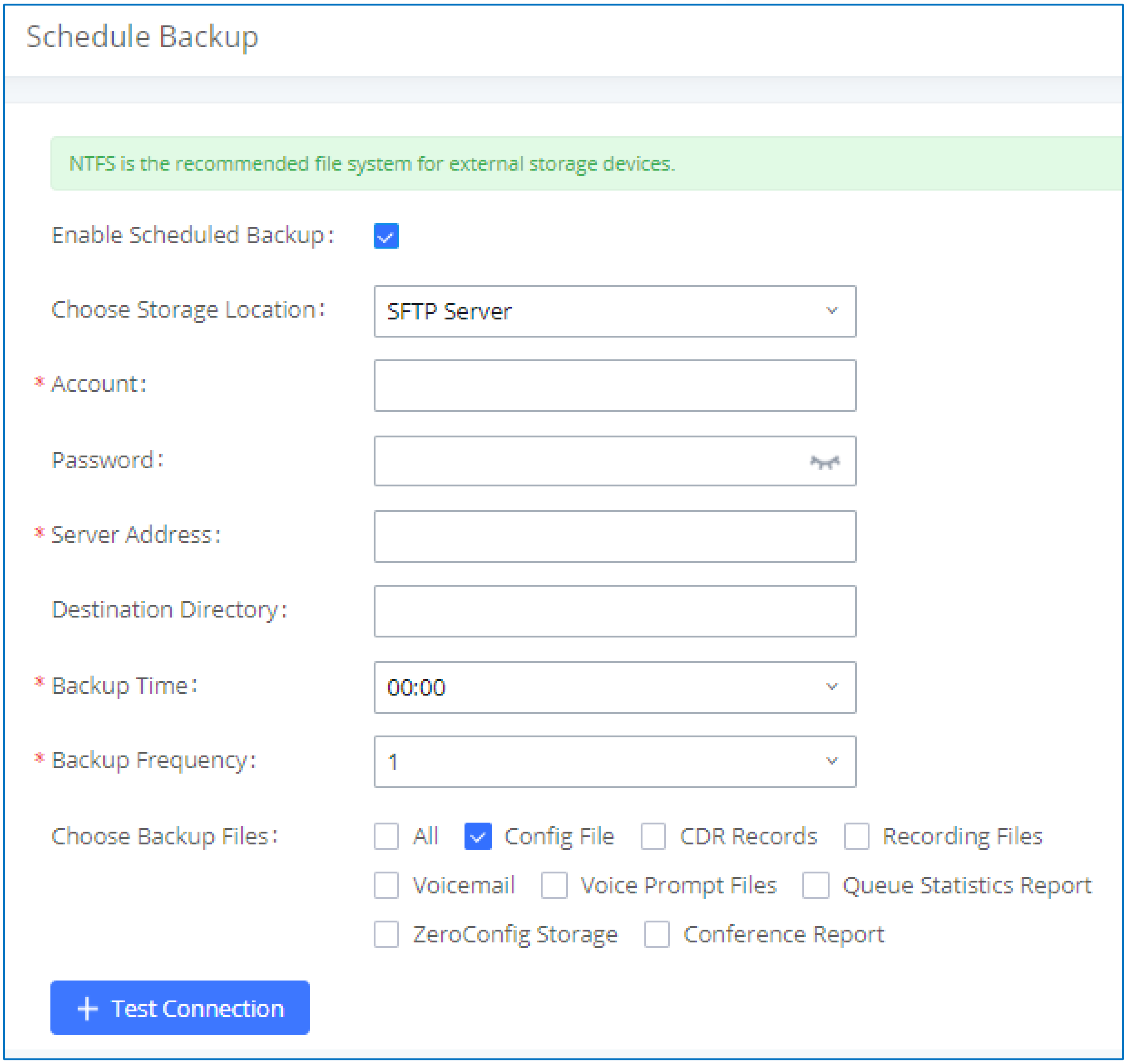


Figure 330: Local Backup

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 Web GUI→**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

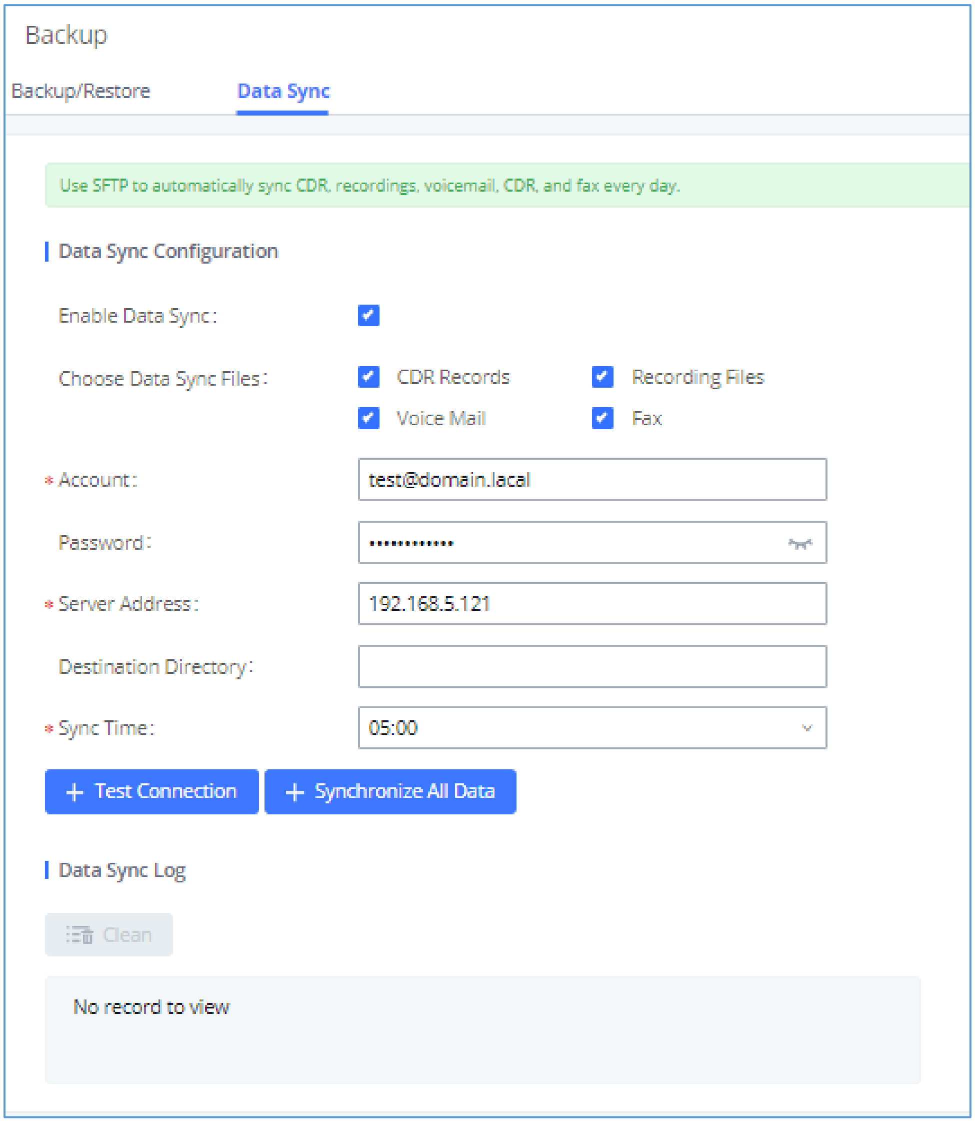


Figure 331: Data Sync

Table 148: Data Sync Configuration

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 + Test Connection. 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 + Synchronize All Data instead of waiting for the backup time interval to come.

Restore Configuration from Backup File

To restore the configuration on the UCM630X from a backup file, users could go to Web GUI → **Maintenance** → **Backup** → **Backup/Restore**.

- A list of previous configuration backups is displayed on the web page. Users could click on of the desired backup file and it will be restored to the UCM630X.
- If the backup was stored on GDMS, it will be displayed under Backups GDMS Cloud Storage, that can be restored by clicking on
- If users have other backup files on PC to restore on the UCM630X, click on "Upload Backup File" first and select it from local PC to upload on the UCM630X. Once the uploading is done, this backup file will be displayed in the list of previous configuration backups for restore purpose. Click on to restore from the backup file.

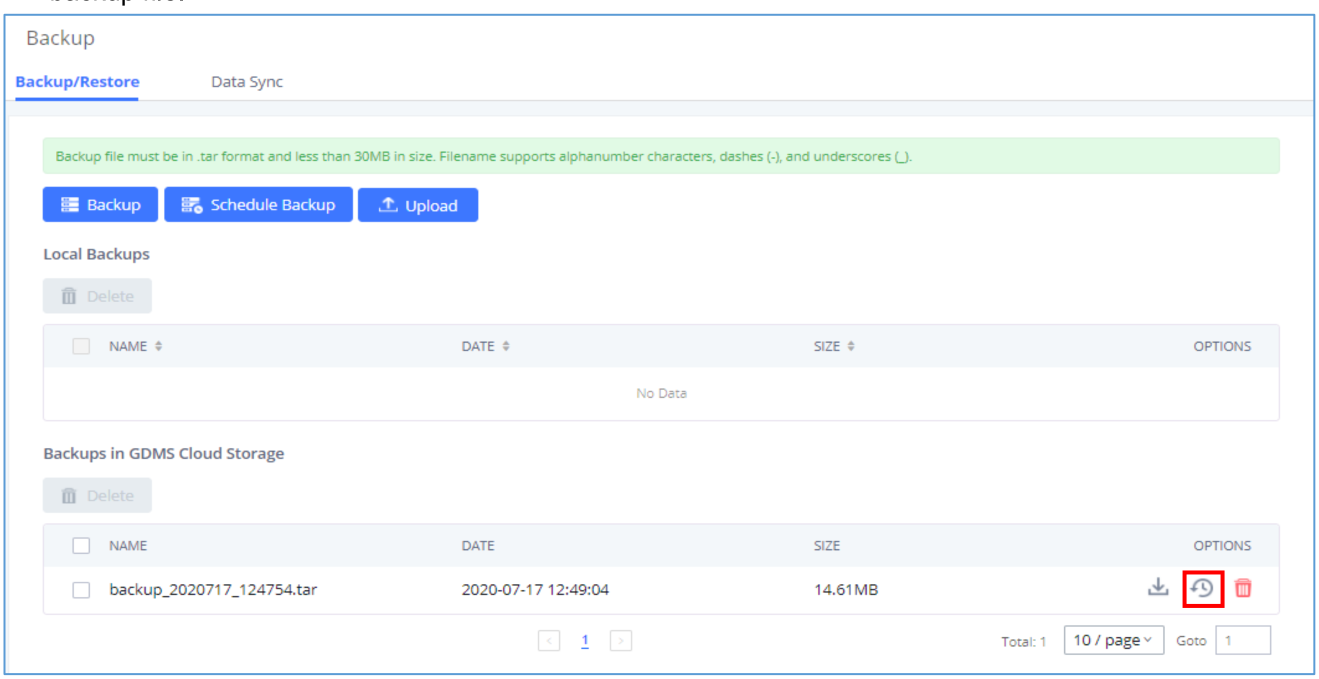


Figure 332: Restore UCM630X from Backup File

⚠ **Note:**

- The uploaded backup file must be a tar file with no special characters like *,!,#,@,&,$,%,^,(,),/,\,space in the file name.
- The uploaded back file size must be under 10MB.

System Cleanup/Reset

Reset and Reboot

Users could perform reset and reboot under Web GUI→**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.

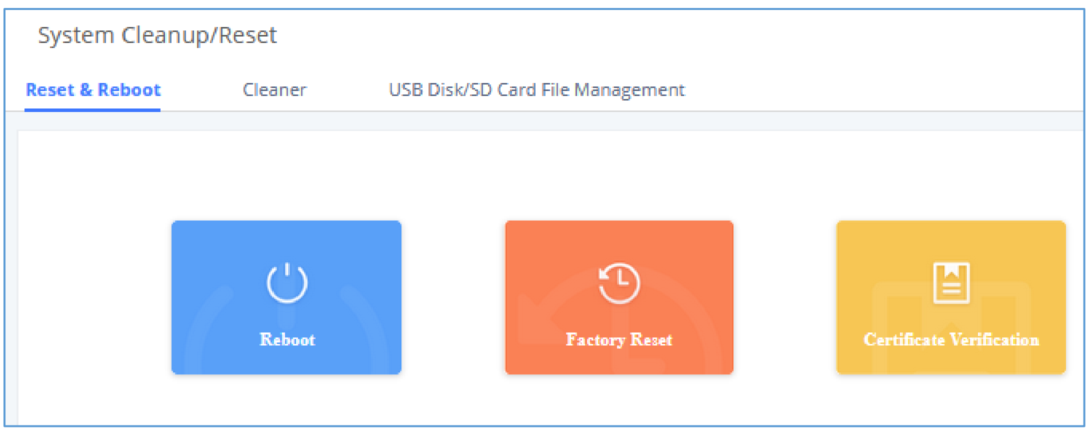


Figure 333: Reset and Reboot

- User can also verify UCM certificate under the same path.

Cleaner

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails etc… manually and automatically under Web GUI→**Maintenance**→**System Cleanup/Reset**→**Cleaner**.
The following screenshot show the settings and parameters to configure the manual cleaner feature on UCM630X.

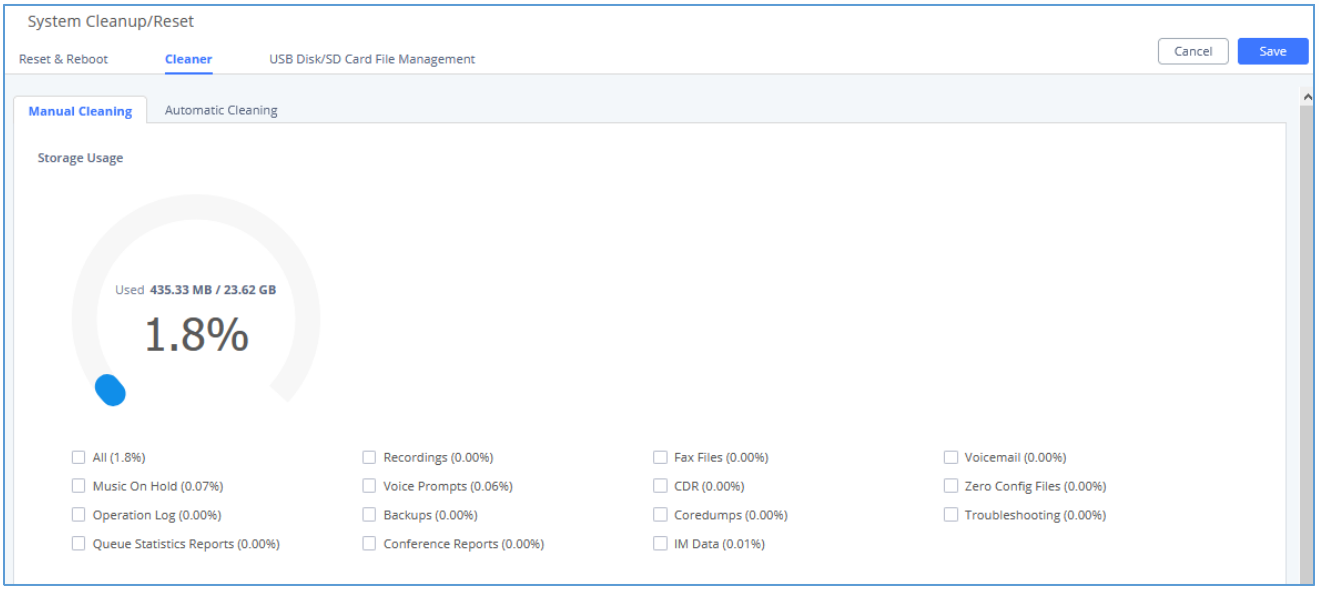


Figure 334: Manual Cleaning

Users can either clean all the data on the UCM or specify the modules to clean such as: Recordings, Fax Files, Voicemail, Music on Hold, Voice Prompts, CDR, ZeroConfig Files, Operation Log, Backups, Coredumps, Troubleshooting, Queue Statistics Reports, Conference Reports, IM Data.

User can also set an automatic cleaning under **Cleaner→Automatic Cleaning**. The following screenshot show the settings and parameters to configure the cleaner feature on UCM630X.

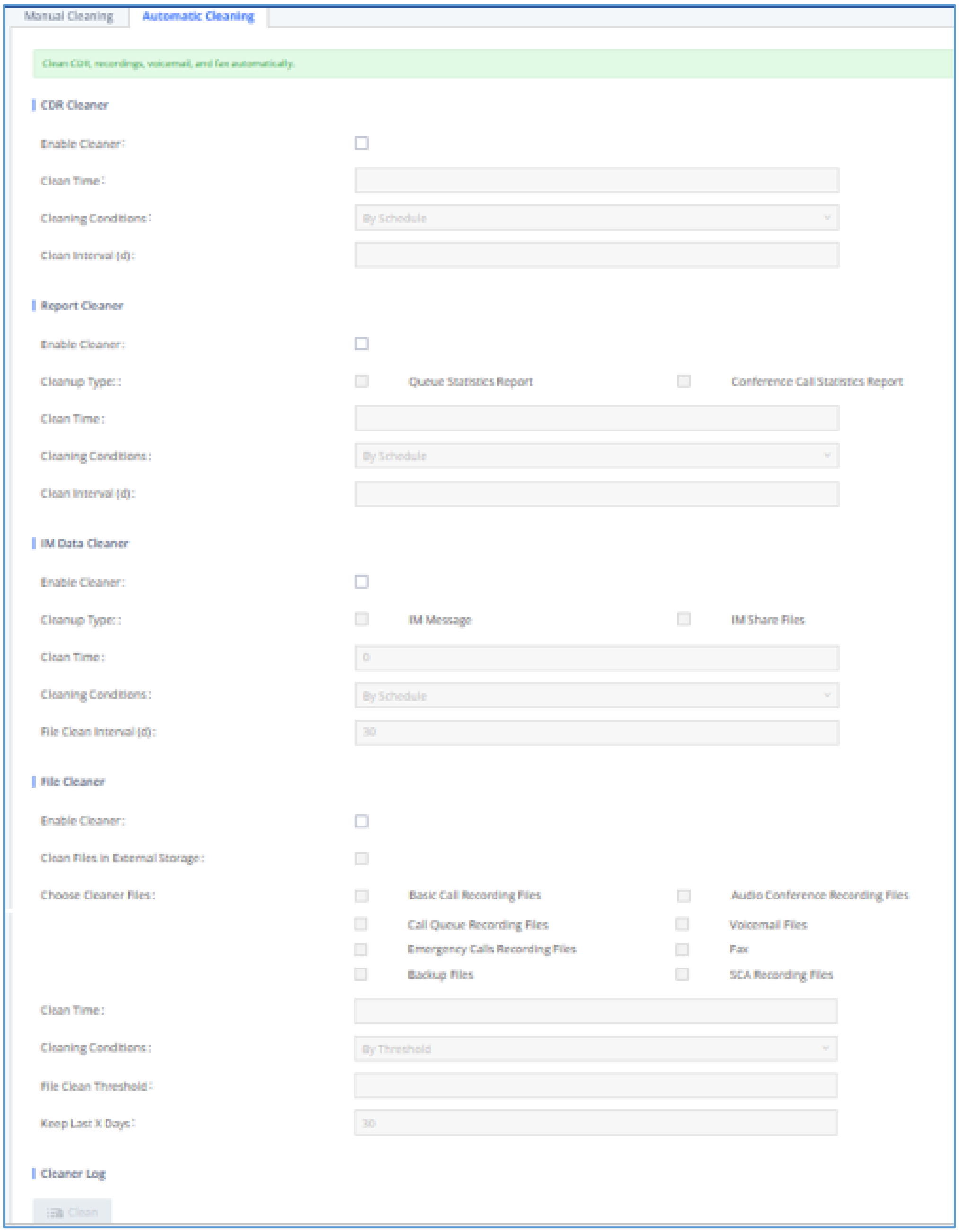


Figure 335: Automatic Cleaning

Table 149: Automatic Cleaning Configuration

Enable CDR Cleaner	Enable the CDR Cleaner function.
CDR 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 3 days ago.

	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	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**.
Keep Last X Day	Enter the number of days of call log entries to keep when **Keep Last X days** is selected as **Cleaning Conditions**.
Enable Queue Statistics Report Cleaner	Enable scheduled queue log cleaning. By default, is disabled.
Queue Statistics Report Cleaner 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 has been reached, Queue Statistics 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 entries to keep when **Keep Last X Records** is selected as **Cleaning Conditions**.
Keep Last X Day	Enter the number of days of call log entries to keep when **Keep Last X days** is selected as **Cleaning Conditions**.
Enable Conference Statistics Report Cleaner	Enable scheduled Conference log cleaning. By default, is disabled.

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 Statistics Report has been reached, Conference 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 Conference Statistics Report entries to keep when **Keep Last X Records** is selected as **Cleaning Conditions**.
Keep Last X Day	Enter the number of days of call log entries to keep when **Keep Last X days** is selected as **Cleaning Conditions**.
Enable File Cleaner	Enter the Voice Records Cleaner function.
Clean Files in External Device	If enabled the files in external device (USB/SD card) will be atomically cleaned up as configured.
Choose Cleaner File	Select the files for system automatic clean. • Basic Call Recording Files. • Conference Recording Files. • Call Queue Recording Files. • Voicemail Files. • Backup 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
Cleaner Log	Press Clean "button" to clean cleaner log.

All the cleaner logs will be listed on the bottom of the page.

USB/SD Card Files Cleanup

Users could configure to clean or download the Call Detail Report/Voice Records/Voice Mails automatically under Web GUI→**Maintenance**→**System Cleanup/Reset**→**USB / SD Card Files Cleanup**.

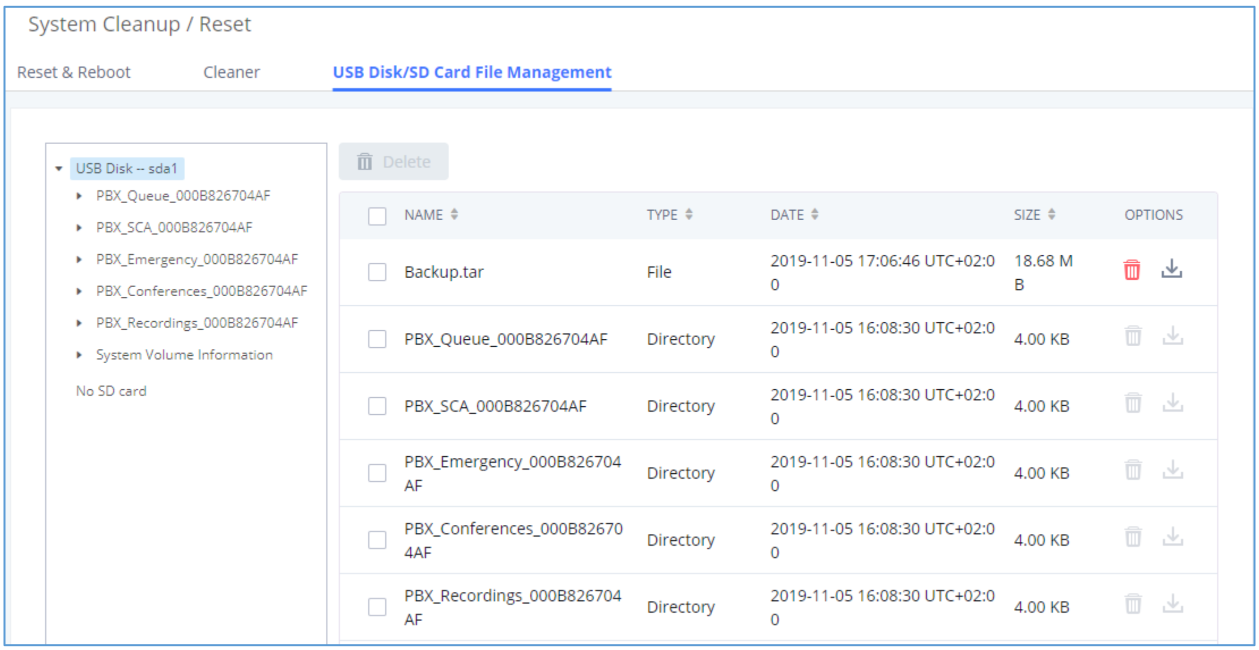


Figure 336: USB/SD Card Files Cleanup

Table 150: USB/SD Card Files Cleanup

Current Path	Displays the current path.
Directory	Select the directory user want to clean.
Delete Selected File	Select multiple entries to delete from USB or SD card.

System Recovery

In some cases (for example after wrong upgrading procedure where the user doesn't follow the correct steps to perform an upgrade) the system may go into some hardware/software issues where the web UI access is lost as well as SSH, in this case the only solution would be to perform a full system recovery in order to reset or update the software version of the device in order to use it again.

1. To access recovery mode on UCM, please follow below steps:
2. Remove the power from the unit and keep the network cable connected.
3. Press using a PIN the reset button and keep holding.
4. Plug back the power supply while maintaining the reset button pressed.
5. Wait for couple of seconds until you hear a click sound.
6. Release the reset button, and the system should display on the LCD a message “Recovery Mode” along with an IP address.

Once at this stage, the administrator can access the recovery mode web portal by typing in either the IP0 address (typically WAN) or IP1 address (typically LAN) into a browser address bar. The following page should appear:

Figure 337: UCM6302 Recovery Web Page

Make sure to enter the correct admin password, and press login to access the recovery mode page :

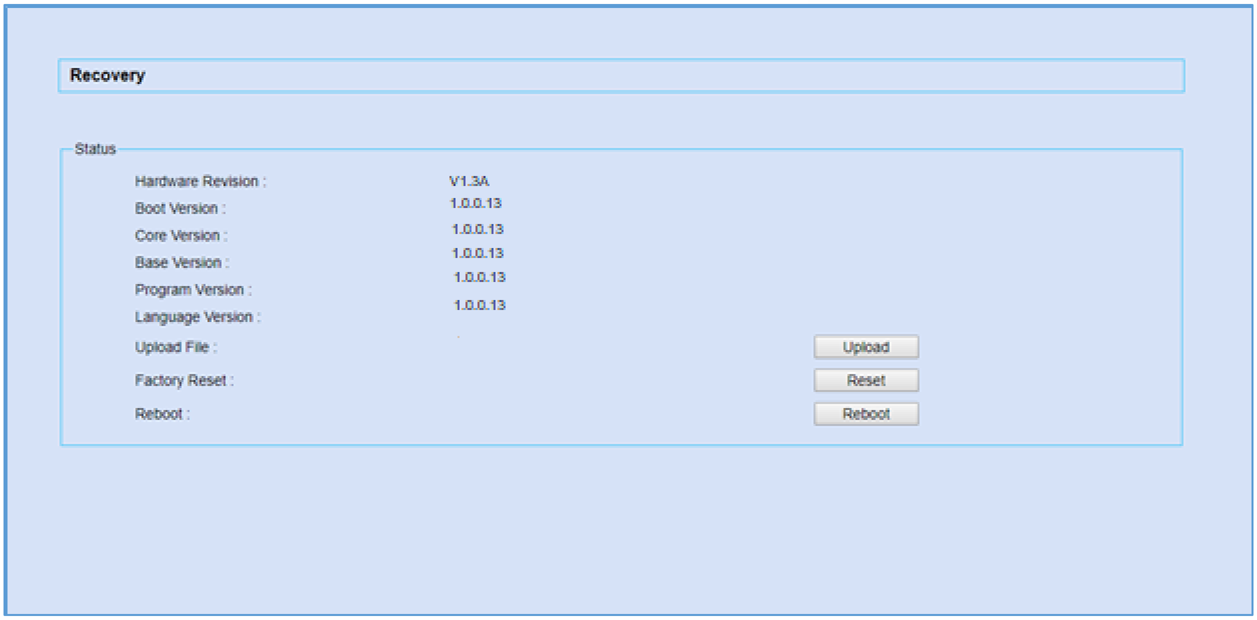


Figure 338: Recovery Mode

From here, the user can either upload a firmware file, factory reset or just reboot the device.

Syslog

On the UCM630X, users could dump the syslog information to a remote server under Web GUI→**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).

⚠ **Note:**

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.

Network Troubleshooting

On the UCM630X, users could capture traces, ping remote host and traceroute remote host for troubleshooting purpose under Web GUI→**Maintenance**→**Network Troubleshooting**.

The following sections shows the steps to capture different types of traffic traces for analysis purposes.

Ethernet Capture

The captured trace can be downloaded for analysis. The instructions or result will be displayed in the Web GUI output result.

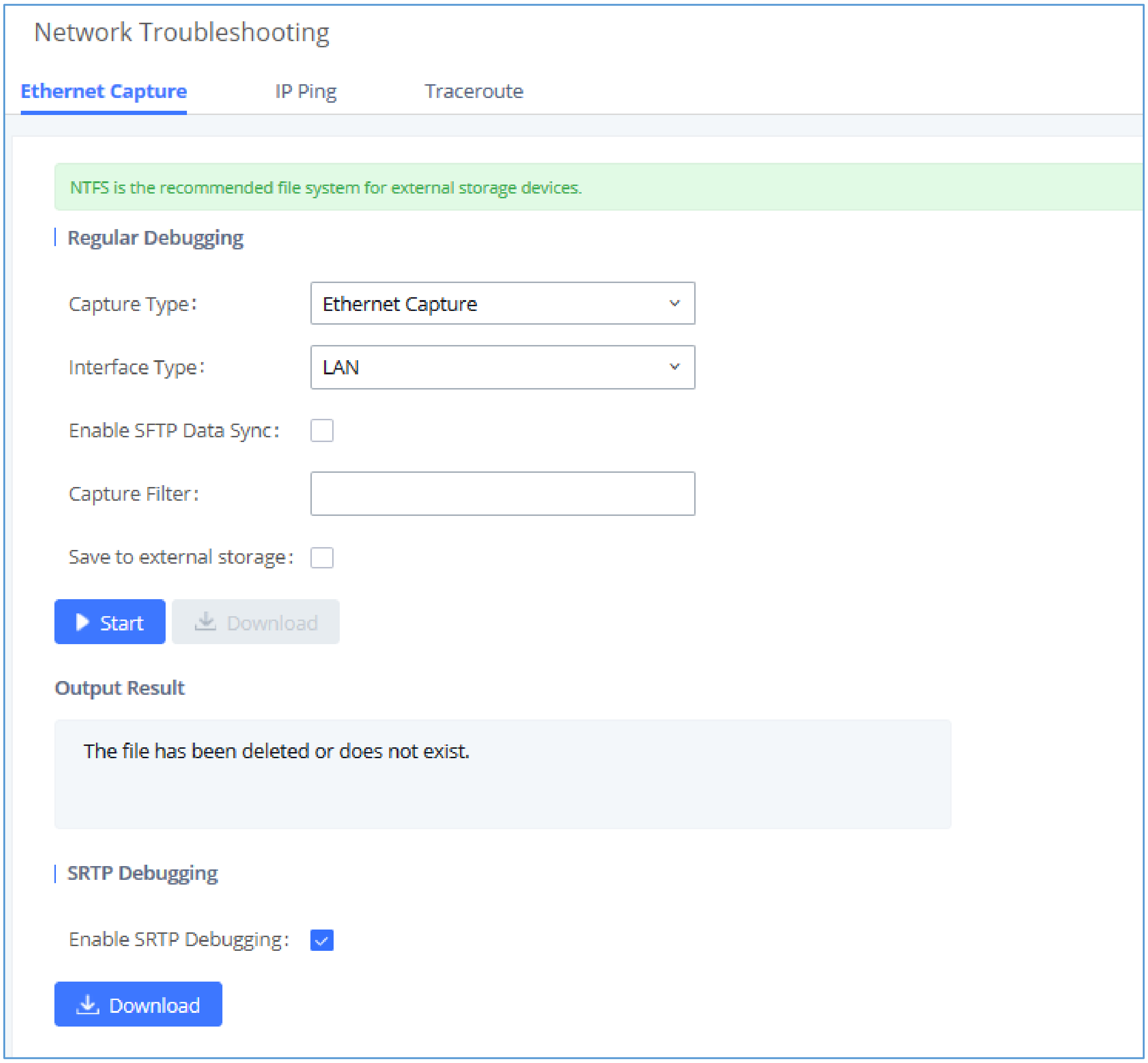


Figure 339: Ethernet Capture

Table 151: Ethernet Capture

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 GS Wave Web calling and conferencing issues.
Interface Type	Select the network interface to monitor.
Enable SFTP Data Sync	Check this box to save the capture files in the SFTP server. Please make sure the configuration of data synchronization works before.

Storage to External Device	Check this box to activate storage of the capture either on the USB or SD Card.
Capture Filter	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto…).
Save to external storage	Save to external storage
Start	Click to start the trace.
Stop	Click to stop the trace.
Download	Click to download the trace if trace is 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.
Note: 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.

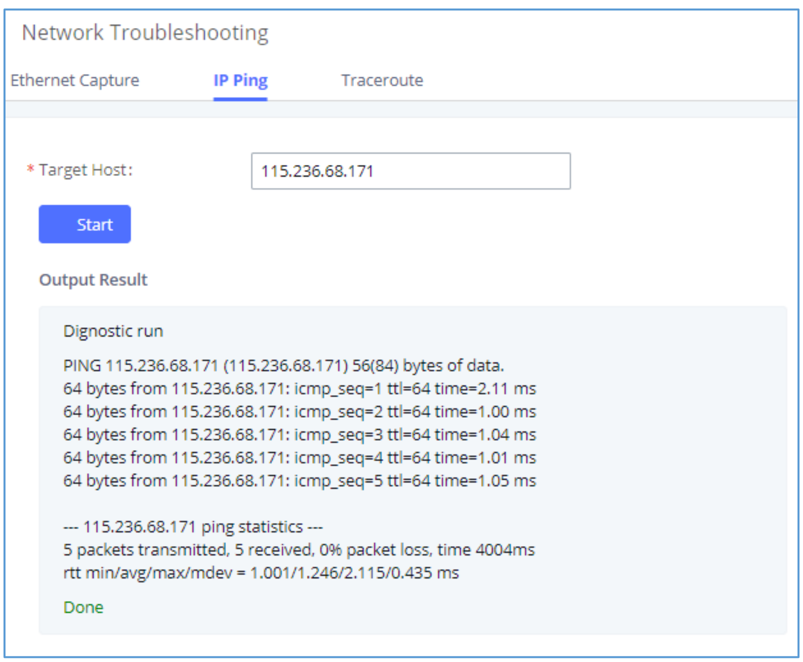


Figure 340: Ping

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.

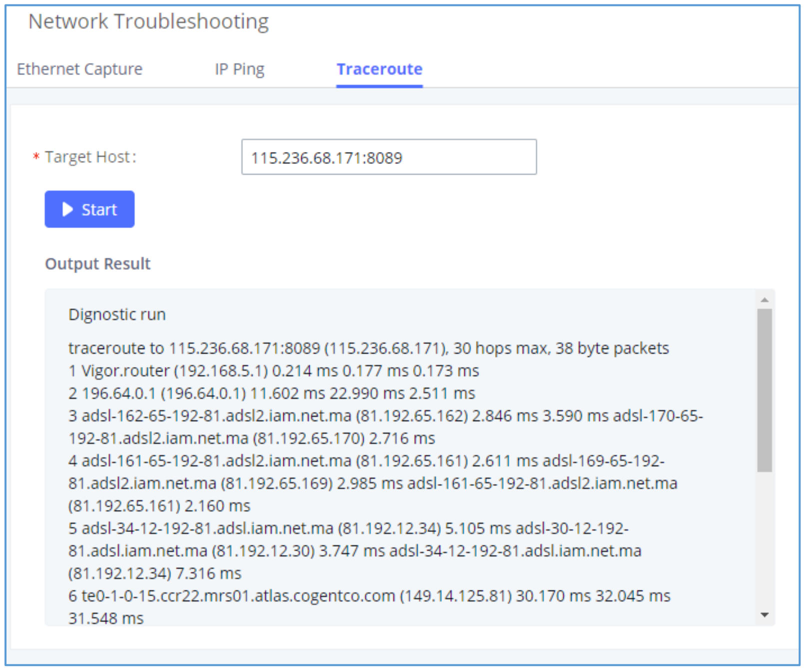


Figure 341: Traceroute

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.

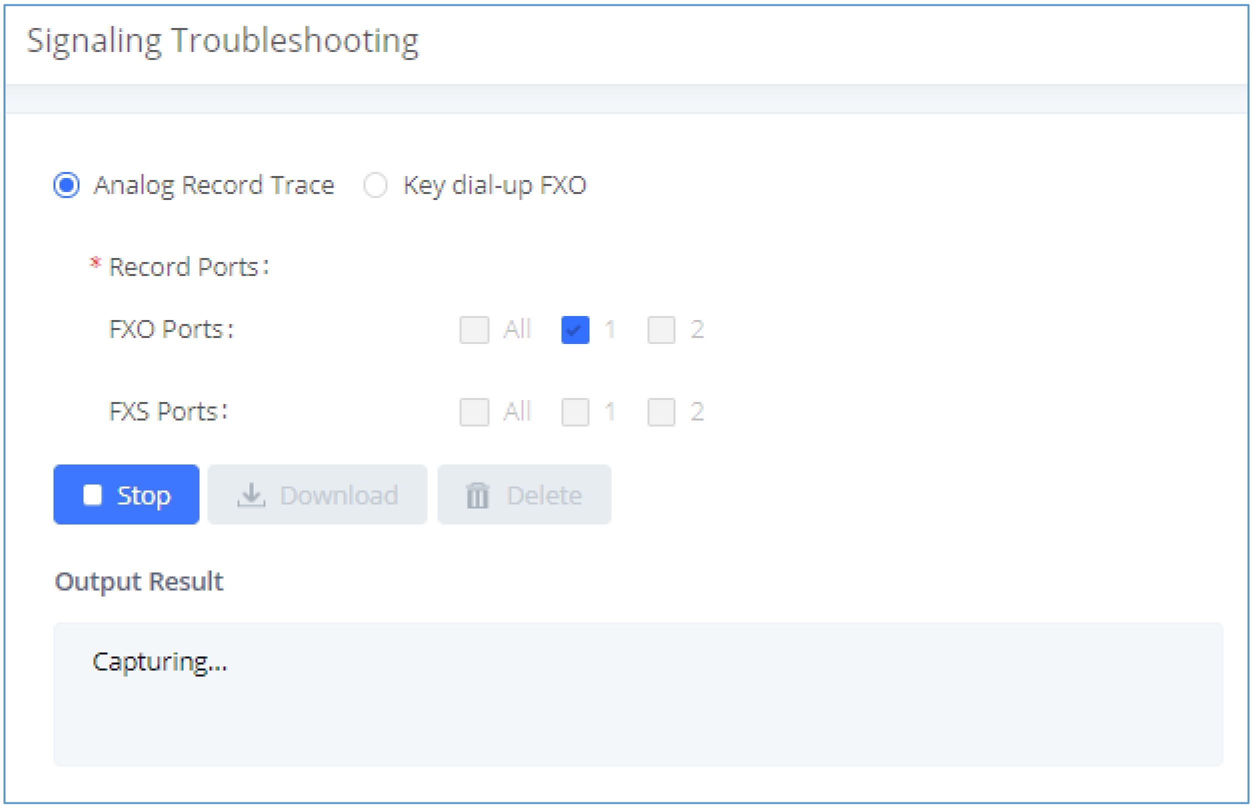


Figure 342: Troubleshooting Analog Trunks

- **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".

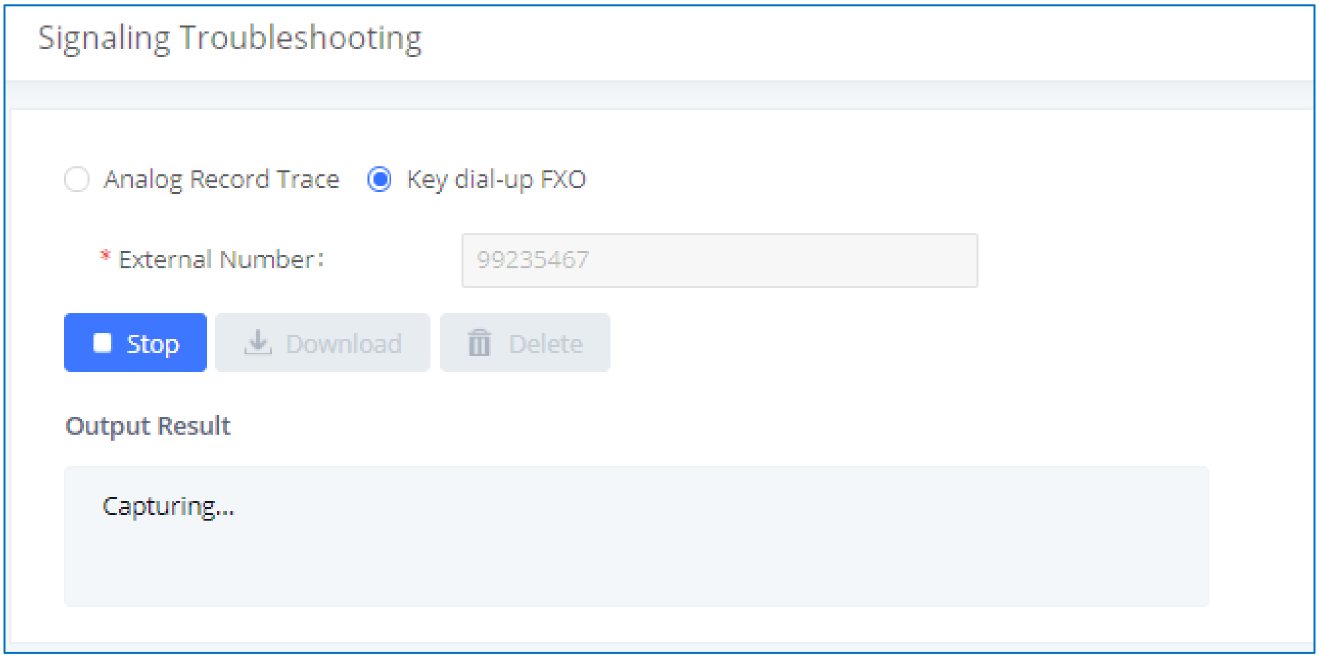


Figure 343: A Key Dial-up FXO

Note: 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.
http://www.grandstream.com/index.php/support

Service Check

Enable Service Check to periodically check UCM630X. Check Cycle is configurable in seconds and the default setting is 60 sec. Check Times is the maximum number of failed checks before restart the UCM630X. The default setting is 3. If there is no response from UCM630X after 3 attempts (default) to check, current status will be stored and the internal service in UCM630X will be restarted.

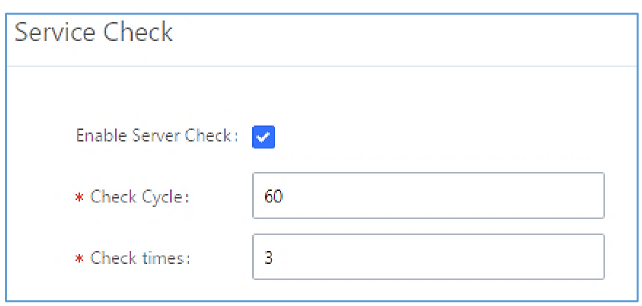
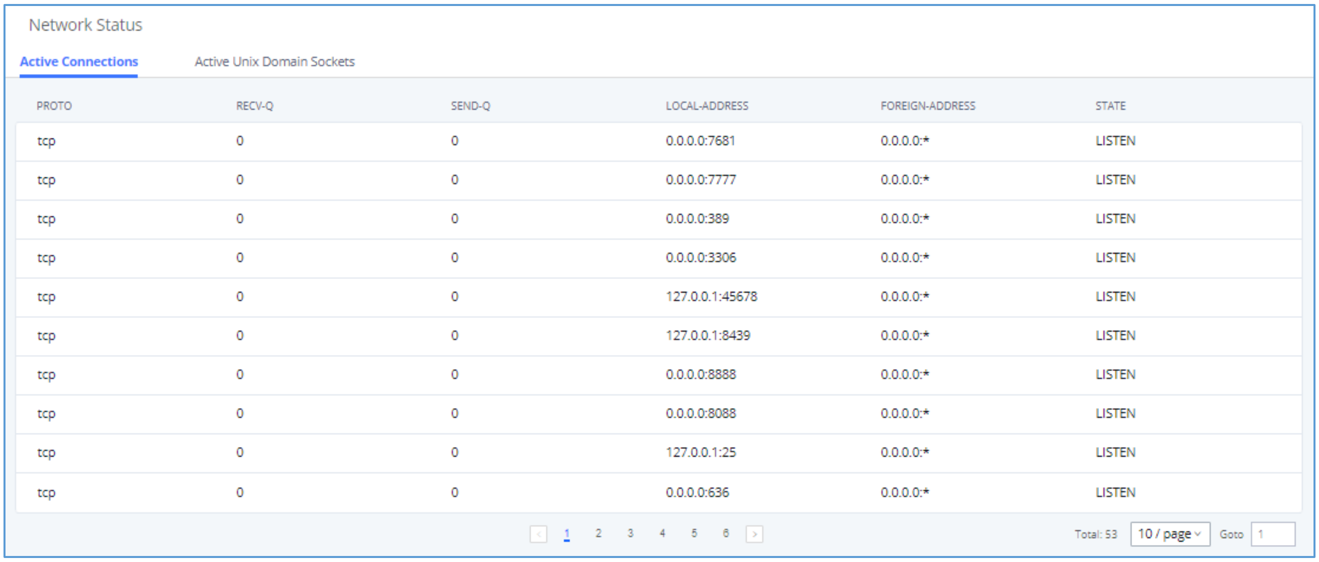


Figure 344: Service Check

Network Status

In UCM630X Web GUI→**System Status**→**Network Status**, the users can view active Internet connections. This information can be used to troubleshoot connection issue between UCM630X and other services.


Network Status

Active Connections | Active Unix Domain Sockets

PROTO	RECV-Q	SEND-Q	LOCAL-ADDRESS	FOREIGN-ADDRESS	STATE
tcp	0	0	0.0.0.0:7681	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:7777	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:389	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:45678	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8439	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8888	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8088	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:636	0.0.0.0:*	LISTEN

1 2 3 4 5 6 Total: 53 10 / page Goto 1

Figure 345: Network Status

EXPERIENCING THE UCM630X SERIES IP PBX

Please visit our website: http://www.grandstream.com to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all of your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for purchasing Grandstream UCM630X series IP PBX appliance, it will be sure to bring convenience and color to both your business and personal life.