

# UCM630x Audio Series – User Manual

Thank you for purchasing Grandstream UCM630xA series IP PBX appliance. The UCM6300A 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, voice meeting, video surveillance, web meetings, data, analytics, mobility, facility access, intercoms and more. The UCM6300A series supports up to 1500 users and includes a built-in web meetings and meeting solution that allows employees to connect from the desktop, mobile, GVC series devices and IP phones. It can be paired with the UCM6300A 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 UCM630xA 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 UCM6300A series also offers cloud setup and management through GDMS and an TableAPI 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 UCM6300A series provides a powerful platform for any organization.

## Alert

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.

## Caution

Please do not use a different power adaptor with the UCM630xA as it may cause damage to the product and void the manufacturer warranty.

## Note

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

## PRODUCT OVERVIEW

### Technical Specifications

The following table resumes all the technical specifications including the protocols / standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings for UCM630xA series.

Interfaces	
Analog Telephone FXS Ports	<ul style="list-style-type: none"><li>● <b>UCM6300A:</b> None</li><li>● <b>UCM6302A:</b> 2 RJ11 ports</li><li>● <b>UCM6304A:</b> 4 RJ11 ports</li><li>● <b>UCM6308A:</b> 8 RJ11 ports</li></ul> All ports have lifeline capability in case of power outage.
PSTN Line FXO Ports	<ul style="list-style-type: none"><li>● <b>UCM6300A:</b> None</li><li>● <b>UCM6302A:</b> 2 RJ11 ports</li><li>● <b>UCM6304A:</b> 4 RJ11 ports</li><li>● <b>UCM6308A:</b> 8 RJ11 ports</li></ul> 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	<ul style="list-style-type: none"><li>● <b>UCM6300A:</b> 1x USB 3.0, and 1x SD card interface</li><li>● <b>UCM6302A:</b> 1x USB 2.0, 1x USB 3.0, and 1x SD card interface</li></ul>

	<ul style="list-style-type: none"> <li>● <b>UCM6304A/6308A:</b> 2x USB 3.0 and 1x SD card interface</li> </ul>
<b>LED Indicators</b>	<ul style="list-style-type: none"> <li>● <b>UCM6300A/6302A/UCM6304A:</b> None</li> <li>● <b>UCM6308A:</b> Power 1/2, FXS, FXO, LAN, WAN, Heartbeat</li> </ul>
<b>LCD Display</b>	<ul style="list-style-type: none"> <li>● <b>UCM6300A/6302A/6304A:</b> 320*240 LCD with touch screen for Shortcut Keys and Scroll Bar.</li> <li>● <b>UCM6308A:</b> 128x32 dot matrix graphic LCD with DOWN and OK buttons</li> </ul>
<b>Reset Switch</b>	Yes, long press for factory reset and short press for reboot
<b>Voice Capabilities</b>	
<b>Voice-over-Packet Capabilities</b>	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
<b>Voice and Fax Codecs</b>	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
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
<b>Signalling and Control</b>	
<b>API</b>	Full API available for third-party platform and application integration.
<b>DTMF Methods</b>	Inband, RFC4733, and SIP INFO
<b>Provisioning Protocol and Plug-and-Play</b>	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
<b>Network Protocols</b>	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®
<b>Disconnect Methods</b>	Busy/Congestion/Howl Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect
<b>Security</b>	
<b>Media Encryption</b>	SRTP, TLS1.2, HTTPS, SSH, 802.1x
<b>Physical</b>	
<b>Universal Power Supply</b>	<ul style="list-style-type: none"> <li>● <b>UCM6300A/6302A:</b> Input: 100 ~ 240VAC, 50/60Hz; Output: DC 12V, 1.5A</li> <li>● <b>UCM6304A:</b> 1x DC 12V Power Jack Input: 100~240VAC, 50/60Hz;Output: DC 12V, 2A</li> <li>● <b>UCM6308A:</b> 2x DC 12V Power Jack Input: 100~240VAC,50/60Hz; Output: DC12V, 2A</li> </ul>
<b>Dimensions</b>	<ul style="list-style-type: none"> <li>● <b>UCM6300A/6302A/6304A:</b> 270mm(L) x 175mm(W) x 36mm(H)</li> <li>● <b>UCM6308A:</b> 485mm(L) x 187.2mm(W) x 46.2mm(H)</li> </ul>
<b>Weight</b>	<ul style="list-style-type: none"> <li>● <b>UCM6300A:</b> Unit weight 705g, Package weight 1131g</li> <li>● <b>UCM6302A:</b> Unit weight 725g, Package weight 1221g</li> <li>● <b>UCM6304A:</b> Unit weight 775g, Package weight 1621g</li> <li>● <b>UCM6308A:</b> Unit weight 2538g, Package weight 3463g</li> </ul>

<b>Temperature &amp; Humidity</b>	<ul style="list-style-type: none"> <li>• Operating: 32 - 113°F / 0 ~ 45°C, Humidity 10 - 90% (non-condensing)</li> <li>• Storage: 14 - 140°F / -10 ~ 60°C, Humidity 10 - 90% (non-condensing)</li> </ul>
<b>Mounting</b>	<ul style="list-style-type: none"> <li>• <b>UCM6300A/6302A/6304A:</b> Wall mount and desktop.</li> <li>• <b>UCM6308A:</b> Rack mount and desktop.</li> </ul>
<b>Additional Features</b>	
<b>Multi-language Support</b>	<ul style="list-style-type: none"> <li>• Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech, Turkish</li> <li>• Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Polish, Portuguese, Russian, Swedish, Turkish, Ukrainian, Hebrew, Arabic, Nederlands</li> <li>• Customizable language pack to support any other languages</li> </ul>
<b>Caller ID</b>	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 – BT, NTT
<b>Polarity Reversal/ Wink</b>	Yes, with enable/disable option upon call establishment and termination
<b>Call Center</b>	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/workload, in-queue announcement
<b>Customizable Auto Attendant</b>	Up to 5 layers of IVR (Interactive Voice Response) in multiple languages
<b>Telephony Operating System</b>	Based on Asterisk version 16
<b>Maximum Call Capacity</b>	<p><b>UCM6300A:</b></p> <ul style="list-style-type: none"> <li>• Users: <b>250</b></li> <li>• Concurrent calls (G.711): <b>50</b></li> <li>• Max concurrent SRTP calls: <b>50</b></li> </ul> <p><b>UCM6302A:</b></p> <ul style="list-style-type: none"> <li>• Users: <b>500</b></li> <li>• Concurrent calls (G.711): <b>75</b></li> <li>• Max concurrent SRTP calls: <b>75</b></li> </ul> <p><b>UCM6304A:</b></p> <ul style="list-style-type: none"> <li>• Users: <b>1000</b></li> <li>• Concurrent calls (G.711): <b>150</b></li> <li>• Max concurrent SRTP calls: <b>120</b></li> </ul> <p><b>UCM6308A:</b></p> <ul style="list-style-type: none"> <li>• Users: <b>1500</b></li> <li>• Concurrent calls (G.711): <b>200</b></li> <li>• Max concurrent SRTP calls: <b>150</b></li> </ul>
<b>Maximum Attendees of Meeting Bridges</b>	<ul style="list-style-type: none"> <li>• <b>UCM6300A:</b> 3 Meeting rooms and up to 50 parties</li> <li>• <b>UCM6302A:</b> 5 Meeting rooms and up to 75 parties</li> <li>• <b>UCM6304A:</b> 7 Meeting rooms and up to 120 parties</li> <li>• <b>UCM6308A:</b> 9 Meeting rooms and up to 150 parties</li> </ul>
<b>Wave App</b>	Free; Available for desktop (Windows 10+, Mac OS 10+), web (Firefox and Chrome Browsers) and mobile (Android & iOS), allows users to join UCM-hosted meetings, communicate with other users/solutions and make/receive calls using SIP accounts registered to a UCM6300 Audio series IP PBX

<b>Call Features</b>	Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, fax to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice conference, video conference, eventlist, feature codes, busy camp-on/ call completion, voice control, post-meeting reports, virtual fax sending/receiving, email to fax
<b>Firmware Upgrade</b>	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
<b>Internet Protocol Standards</b>	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028. RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550
<b>Compliance</b>	<ul style="list-style-type: none"> <li>● <b>FCC:</b> Part 15 (CFR 47) Class B, Part 68</li> <li>● <b>CE:</b> EN 55032, EN 55035, EN61000-3-2, EN61000-3-3, EN 62368.1, ES 203 021, ITU-T K.21</li> <li>● <b>IC:</b> ICES-003, CS-03 Part I Issue 9</li> <li>● <b>RCM:</b> AS/NZS CISPR 32, AS/NZS 62368.1, AS/CA S002, AS/CA S003.1/.2</li> <li>● <b>Power adapter:</b> UL 60950-1 or UL 62368-1</li> </ul>

### Technical Specifications

**i UCM630xA FXS ports lifeline functionality:** The UCM630xA 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

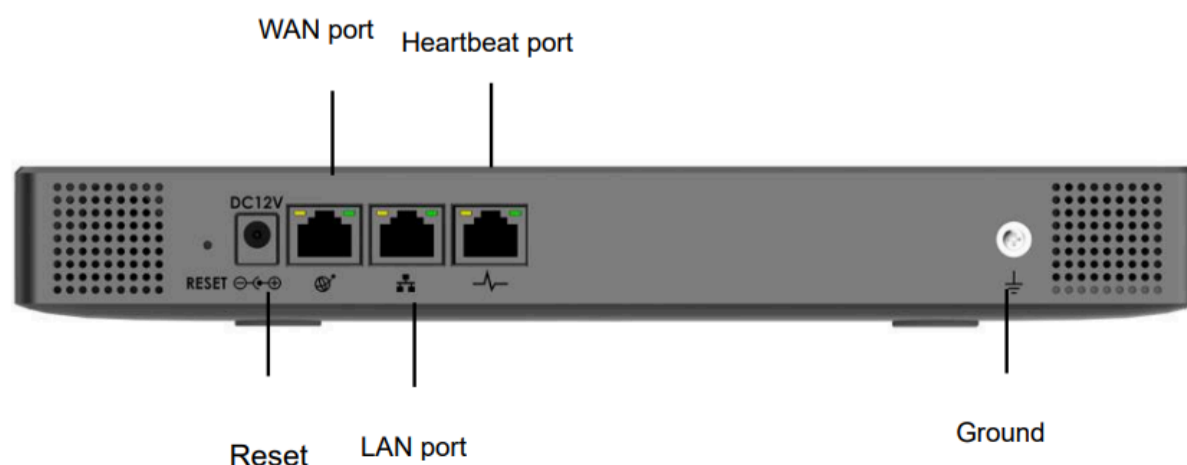
Before deploying and configuring the UCM630xA series, the device needs to be properly powered up and connected to a network. This section describes detailed information on installation, connection, and warranty policy of the UCM630xA series.

### Equipment Packaging

<b>Main Case</b>	1
<b>Power Adaptor</b>	1
<b>Ethernet Cable</b>	1
<b>Quick Installation Guide</b>	1

UCM630xA Equipment Packaging

### UCM6300A front and back view

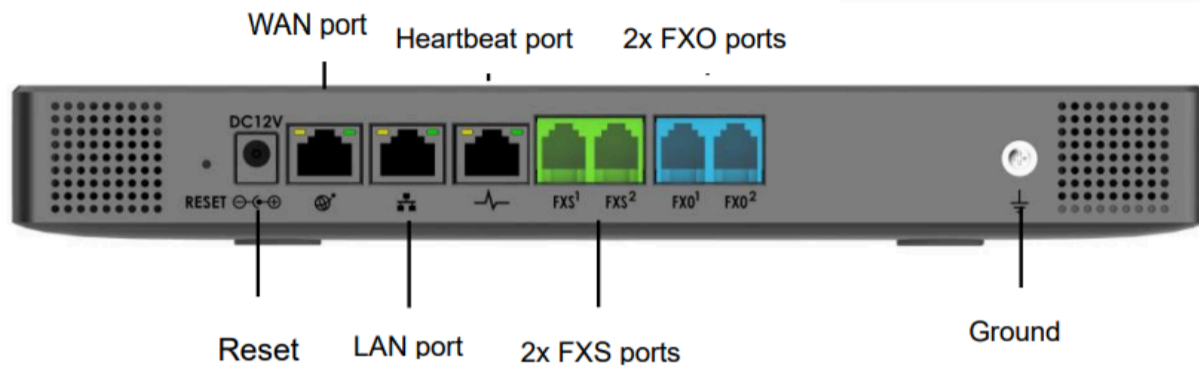


UCM6300A Back View



UCM6300A Front View

**UCM6302A front and back view**

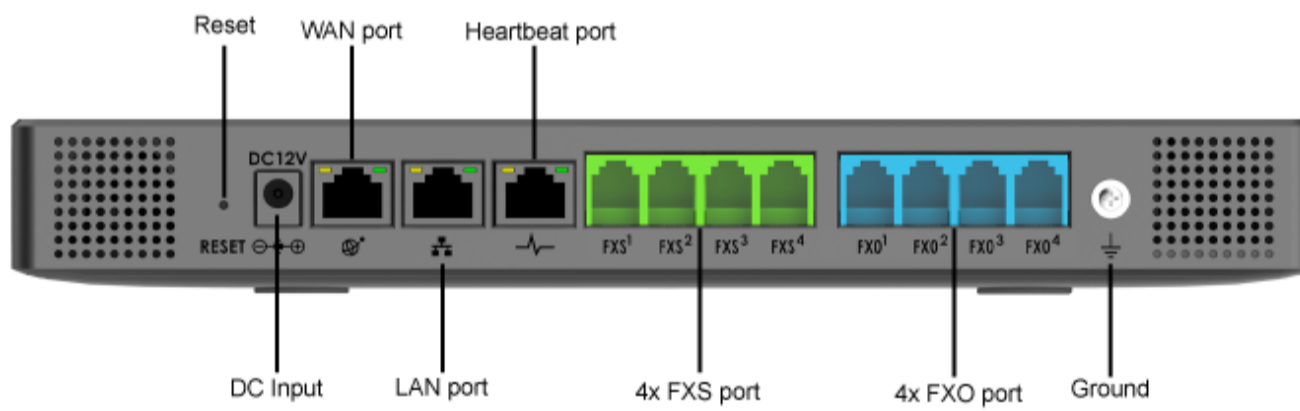


UCM6302A Back View



UCM6302A Front View

**UCM6304A front and back view**

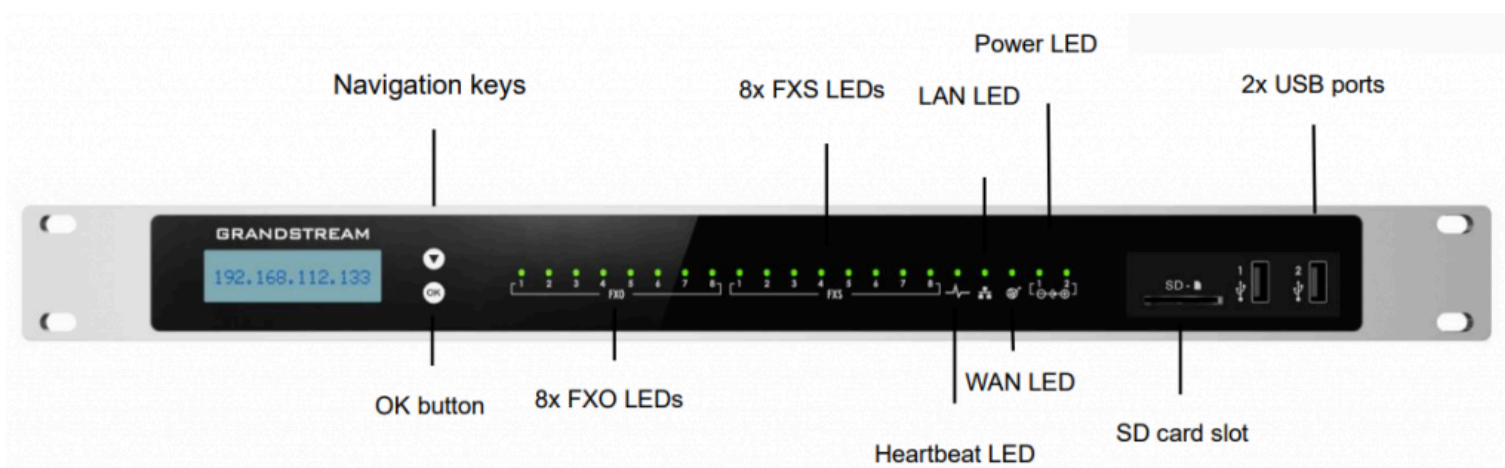


UCM6304A Front View

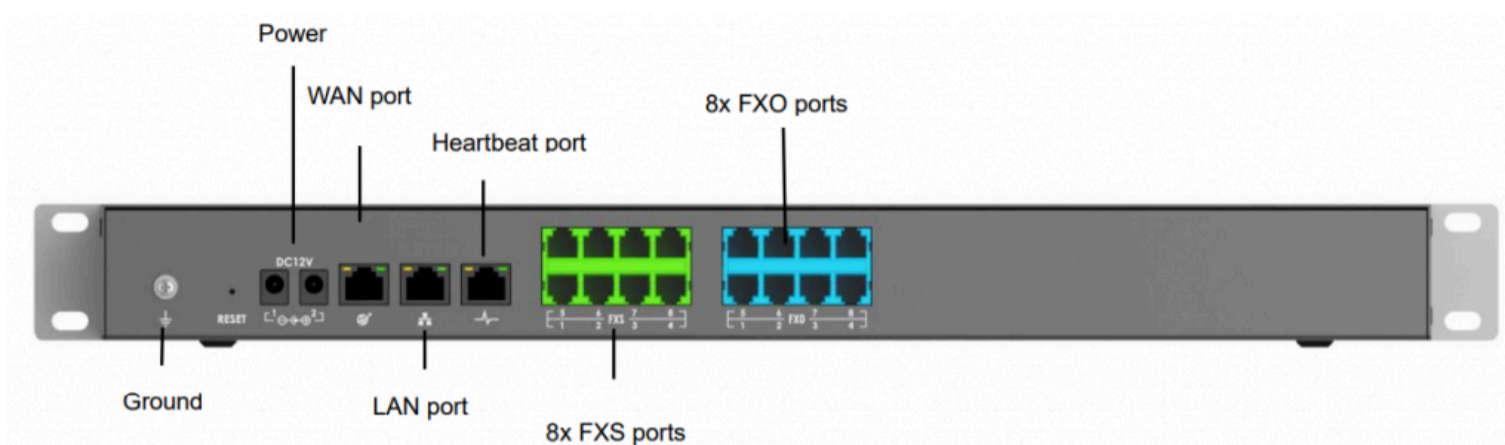


UCM6304A Back View

**UCM6308A front and back view**



UCM6308A Front View



UCM6308A Back View

### ✓ Safety Compliances

The UCM630xA series IP PBX complies with FCC/CE and various safety standards. The UCM630xA power adapter is compliant with the UL standard. Use the universal power adapter provided with the UCM630xA package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

### i Warranty

If the UCM630xA 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.

### i Warning

Use the power adapter provided with the UCM630xA 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 UCM630xA 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 the table [LCD Menu Options].

- **Menu Navigation**

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

- **Exit**

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

- **LCD Backlight**

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

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

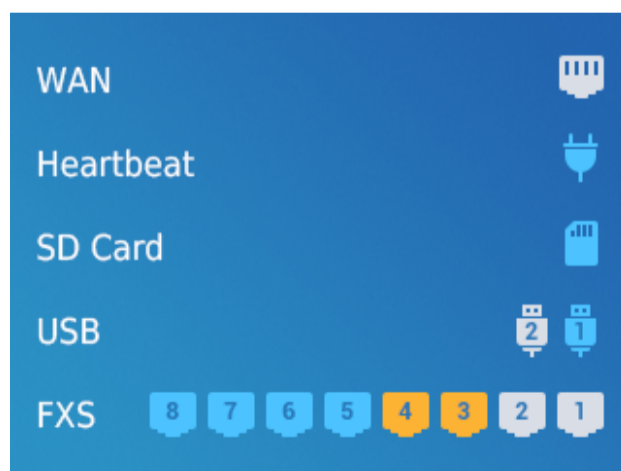
<b>View Events</b>	<ul style="list-style-type: none"> <li>○ <b>Critical Events</b></li> <li>○ <b>Other Events</b></li> </ul>
<b>Device Info</b>	<ul style="list-style-type: none"> <li>○ <b>Hardware:</b> Hardware version number</li> <li>○ <b>Software:</b> Software version number</li> <li>○ <b>P/N:</b> Part number</li> <li>○ <b>WAN MAC:</b> WAN side MAC address</li> <li>○ <b>LAN MAC:</b> LAN side MAC address</li> <li>○ <b>Uptime:</b> System uptime</li> </ul>
<b>Network Info</b>	<ul style="list-style-type: none"> <li>○ <b>WAN Mode:</b> DHCP, Static IP, or PPPoE</li> <li>○ <b>WAN IP:</b> IP address</li> <li>○ <b>WAN Subnet Mask</b></li> <li>○ <b>LAN IP:</b> IP address</li> <li>○ <b>LAN Subnet Mask</b></li> </ul>
<b>Network Menu</b>	<ul style="list-style-type: none"> <li>○ <b>WAN Mode:</b> Select WAN mode as DHCP, Static IP or PPPoE</li> <li>○ <b>Static Route Reset:</b> Select this to reset static route settings.</li> </ul>

<b>Factory Menu</b>	<ul style="list-style-type: none"> <li>○ <b>Reboot</b></li> <li>○ <b>Factory Reset</b></li> <li>○ <b>LCD Test Patterns</b></li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>○ <b>Fan Mode</b></li> </ul> <p>Select Auto or On.</p> <ul style="list-style-type: none"> <li>○ <b>LED Test Patterns</b></li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>○ <b>RTC Test Patterns</b></li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>○ <b>Hardware Testing</b></li> </ul> <p>Select Test SVIP to verify hardware connections within the device. The result will display on the LCD when the test is complete.</p>
<b>Web Info</b>	<ul style="list-style-type: none"> <li>○ <b>Protocol:</b> Web access protocol (HTTP/ HTTPS). HTTPS is used by default.</li> <li>○ <b>Port:</b> Web access port number, which is 8089 by default.</li> </ul>
<b>SSH Switch</b>	<ul style="list-style-type: none"> <li>○ <b>Enable SSH</b></li> <li>○ <b>Disable SSH</b></li> </ul> <p>SSH access is disabled by default</p>

*LCD Menu Options*

## Use the LED Indicators

The UCM6300A/6302A has LED indicators on the network port to display connection status and the following picture shows the other ports status.



*Ports Status*

The UCM6304A/6308A has LED indicators in the front to display connection status. The following table shows the status definitions.

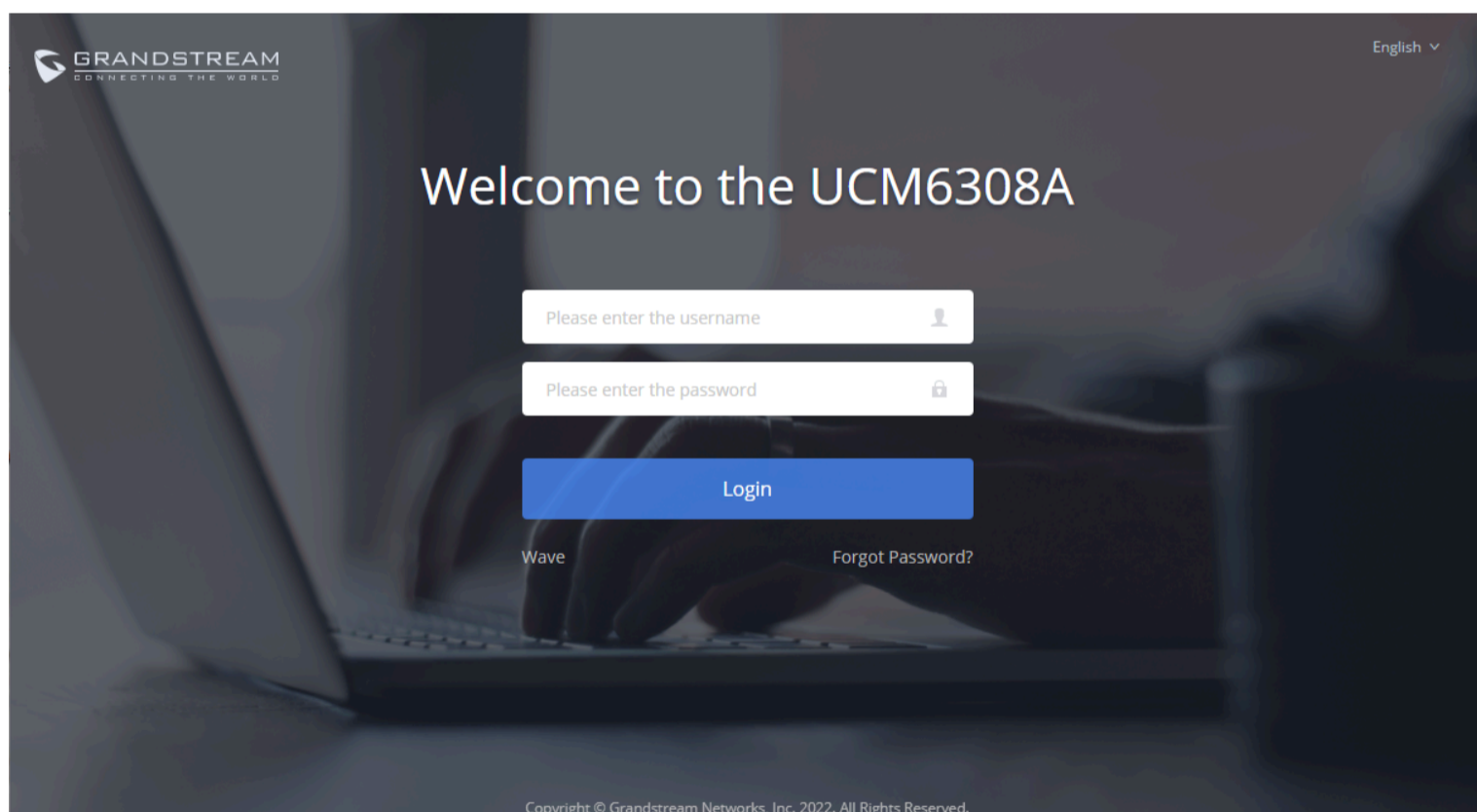
LED Indicator	LED Status
Power 1/Power 2	
PoE	
LAN	<ul style="list-style-type: none"> <li>○ <b>Solid:</b> Connected</li> </ul>
WAN	<ul style="list-style-type: none"> <li>○ <b>Fast Blinking:</b> Data Transferring</li> </ul>
USB	<ul style="list-style-type: none"> <li>○ <b>Slow Blinking:</b> Trying to connect</li> </ul>
SD	<ul style="list-style-type: none"> <li>○ <b>OFF:</b> Not Connected</li> </ul>
FXS ports	
FXO ports	

UCM6304A/6308A LED Indicators

## Using the Web UI

### Accessing the Web UI

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



UCM630xA Web GUI Login Page

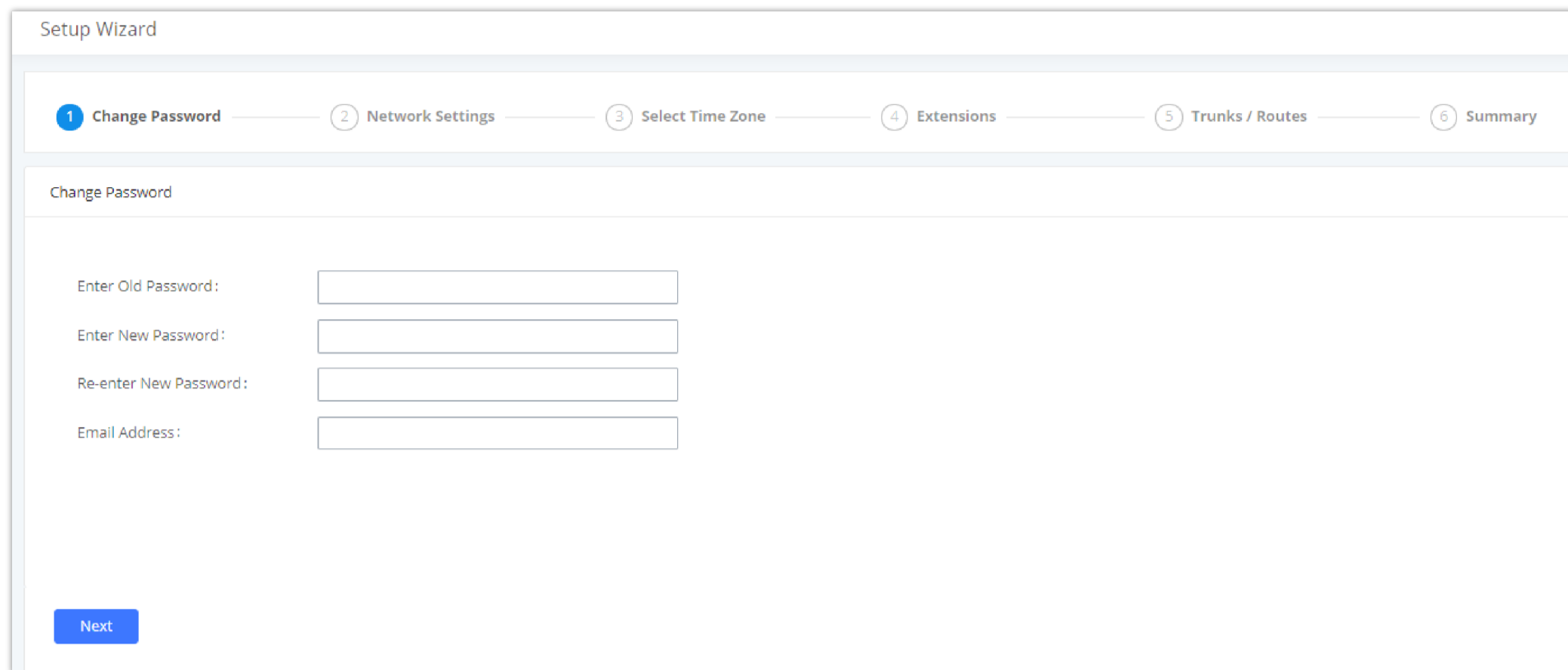
1. Make sure your computer is on the same network as the UCM.
2. Make sure that the UCM's IP address is displayed on its LCD.
3. Enter the UCM's IP address into a web browsers' address bar. The login page should appear (please see the above image).
4. Enter default administrator username "admin" and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

**i** By default, the UCM630xA has **Redirect From Port 80** enabled. As such, if users type in the UCM630xA 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 UCM630xA 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.



The screenshot shows the 'Setup Wizard' interface with a progress bar at the top containing six steps: 1. Change Password (active), 2. Network Settings, 3. Select Time Zone, 4. Extensions, 5. Trunks / Routes, and 6. Summary. Below the progress bar, the 'Change Password' section contains four input fields: 'Enter Old Password:', 'Enter New Password:', 'Re-enter New Password:', and 'Email Address:'. A blue 'Next' button is located at the bottom left of the form.

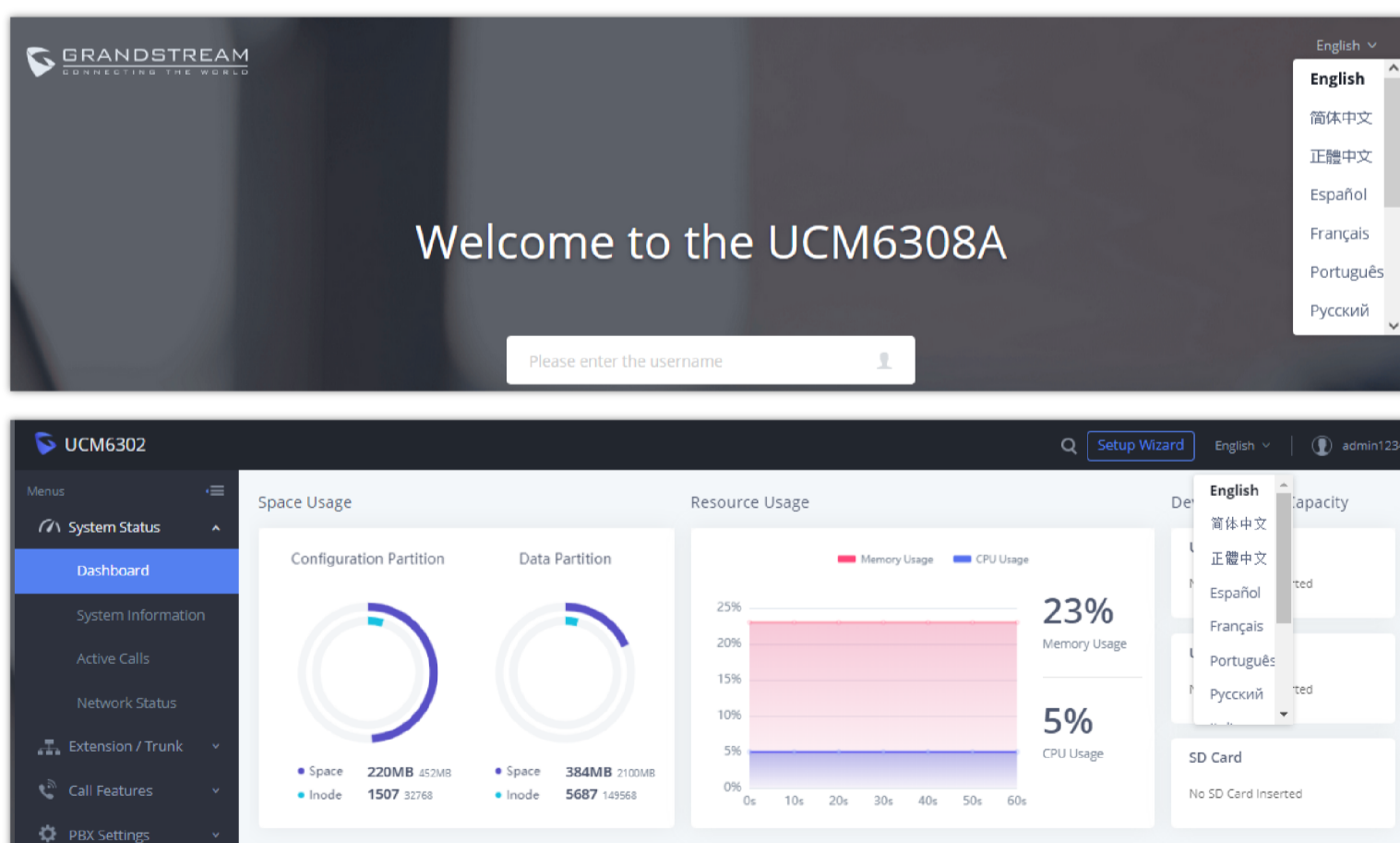
UCM630xA Setup Wizard

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.

## Web GUI Languages

Currently the UCM630xA series Web GUI supports **English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, Russian, Italian, Polish, German etc.**

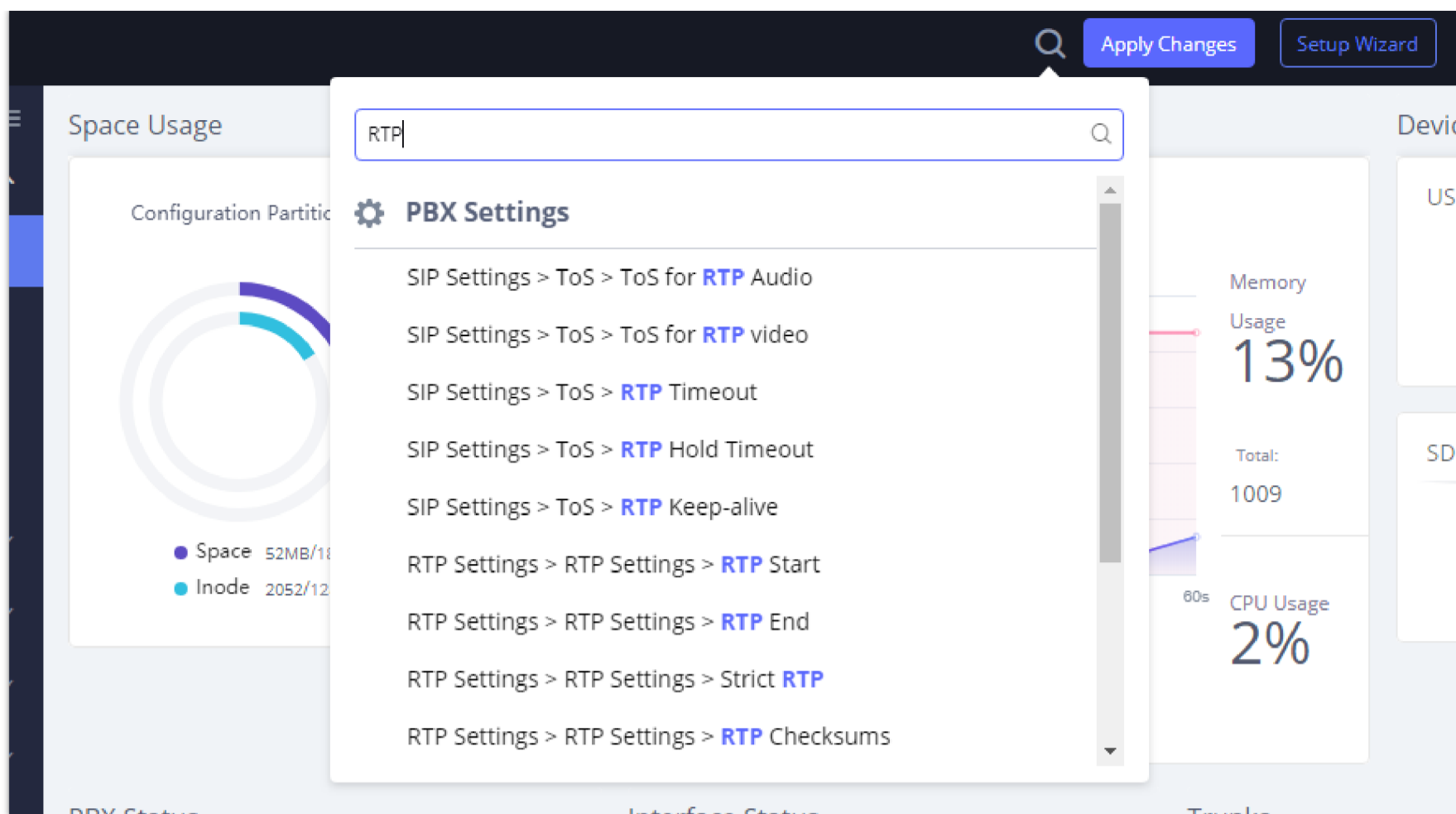
Users can select the UCM's web UI display language in the top-right corner of the page.



UCM630xA Web GUI Language

## Web GUI Search Bar

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



Web GUI Search Bar

## Saving and Applying Changes

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

## Setting Up an Extension

Power on the UCM630xA 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 UCM630xA 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.

### General Settings

Device Name:

Enable CPU Flow Control:

CPU Flow Control Threshold:

Data Partition Write Threshold:

*General Settings Interface*

<b>General Settings</b>	
<b>Device Name</b>	Configure the name of the UCM.
<b>Enable CPU Flow Control</b>	Enables the CPU flow control.
<b>CPU Flow Control Threshold</b>	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 <b>90%</b> .
<b>Data Partition Write Threshold</b>	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 <b>90%</b> .

*General Settings Parameters*

## IM Settings

### IM Settings

In IM Settings tab, the user can choose to enable or disable read receipts when exchanging messaging using Wave.

### IM Settings

IM Settings
Cloud IM Service
IM Server

Read Receipts

New Message Email Notification  [Email Template](#)

\* Maximum chat file size(M)

*IM Settings*

<b>Read Receipts</b>	<ol style="list-style-type: none"> <li>1. Configures whether Wave users can see the read status of sent messages when using local IM.</li> <li>2. If using Cloud IM, read receipts must be configured on the IM server (GDMS or custom IM server) being used. To configure this on GDMS, navigate to the top right corner of the GDMS page <b>Plan &amp; Services-&gt;My Plans-&gt;Edit Cloud IM</b> page.</li> </ol>
----------------------	---

<b>New Message Email Notification</b>	Regardless of whether you are currently using local IM or Cloud IM, when Wave is offline under this domain for more than 7 days after enabling it, an email notification of new messages will be sent when a new message is received.
<b>Maximum Chat File Size (MB)</b>	<ol style="list-style-type: none"> <li>1. Configures whether Wave users can see the maximum chat file size when using local IM.</li> <li>2. If using Cloud IM, maximum chat file size must be configured on the IM server (GDMS or custom IM server) being used.</li> </ol> <p>To configure this on GDMS, navigate to the top right corner of the GDMS page <b>Plan &amp; Services-&gt;My Plans-&gt;Edit Cloud IM page</b></p>

## Cloud IM Service

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

The screenshot shows the 'IM Settings' dialog box with the 'Cloud IM Service' tab selected. The 'IM Server' sub-tab is also active. The configuration fields are as follows:

- Enable Cloud IM:**
- Local Proxy:**
- Cloud IM Server Address:**  (Note: To view the external CloudIM server address, please go to [RemoteConnect](#))
- \* Service ID:**
- \* Key:**
- \* Department Name:**
- Trusted User:**
- Prepend:**
- Sync Local Chat Data:**

At the bottom, there is a link: [Get more information about Cloud IM Settings at <Cloud IM Server Admin Guide>](#)

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

### Cloud IM

Cloud IM Service	
<b>Enable Cloud IM</b>	If you have purchased the Cloud IM package or purchased the Grandstream IM server, you can configure it. If you have not purchased it, the configuration will not take effect, but PBX local IM service is allowed. Please note that after enabling this feature, local chat data will not be visible.
<b>Local Proxy</b>	If enabled, the local proxy will be used to forward files and text messages if the IM server cannot be connected to upon Wave login due to certificate issues.
<b>Cloud IM Server Address</b>	The address of the server that provides IM service, you can fill in the address of the Cloud IM server provided by the RemoteConnect package or the IM server address of the GDMS.
<b>Service ID</b>	The service ID of the Cloud IM server.
<b>Key</b>	The Key to the Cloud IM server.
<b>Site Name</b>	Enter the name of the site.
<b>Trusted User</b>	The trusted user of the cloud IM. Only letters, numbers, and special characters are allowed.

<b>Prefix</b>	As the extension prefix, it is added before the extension number.
<b>Sync Local Chat Data</b>	<p>Syncing existing local chat data to Cloud IM server. The Wave chat feature will not be available during the syncing process. It is recommended to avoid syncing during active working hours.</p> <p><b>- Time Range</b></p> <ul style="list-style-type: none"> <li>• All</li> <li>• Last 12 Months</li> <li>• Last 6 Months</li> <li>• Last 3 Months</li> <li>• Last Month</li> </ul> <p><b>- Data Type</b></p> <ul style="list-style-type: none"> <li>• IM Data</li> <li>• Images</li> <li>• Files</li> </ul>

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

## IM Server

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

**IM Server**

Company Name:	GStest	Trusted User:	C074AD0A8C94
Server Address:	c074ad0a8c94-10671.b.gdms.cloud	Service ID:	100001
Key:	2322458e635c4b98871b37b5079087c6		

[Close IM Server Mode](#)

---

**Bound Device Information**

DEPARTMENT	MAC ADDRESS	DIAL PREFIX
No Data		

*IM server configuration interface*

<b>Company name</b>	The entered company name
<b>Server Address</b>	The domain name or IP address of the Cloud IM server.
<b>Service ID</b>	The service ID of the Cloud IM server.
<b>Key</b>	The Key of the Cloud IM server.
<b>Trusted User</b>	The trusted user of the cloud IM. Only letter, number, and special characters are allowed.
<b>Bound device information</b>	
<b>Department</b>	The department represented by the bound UCM.
<b>MAC Address</b>	MAC address of the bound UCM device.
<b>Dial prefix</b>	Extension prefix

*IM Server parameters*

## 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**.

<b>Redirect From Port 80</b>	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".
<b>External Host</b>	Configure a URL and port (optional) used to access the UCM web portal if the UCM is behind NAT.
<b>Port</b>	Specifies the port number used to access the UCM HTTP server. Default is "8089".
<b>Enable IP Address Allowlist</b>	IP Allowlist restricts all IP addresses except for those in the allowlist from accessing the device via HTTP(S) (i.e., web portal, ZeroConfig, CTI apps).
<b>Permitted IP(s)</b>	List of addresses that can access the UCM web portal. Ex: 192.168.6.233 / 255.255.255.255
<b>Wave Settings</b>	
<b>Cross-origin Address Allowlist</b>	The UCM will accept cross-server requests from addresses in the whitelist, which should be formatted as https://domain, https://ip:port or *. Entering * will allow cross-server requests from all addresses. <b>Note:</b> This option allow third parties to embed a Wave portal into their websites. This allows the users to log into wave using their extension numbers and use limited Wave features. For more details, please refer to the following link: <a href="https://doc.grandstream.dev/WAVE-SDK/EN/#api-Quick%20Start-Overview">https://doc.grandstream.dev/WAVE-SDK/EN/#api-Quick%20Start-Overview</a>
<b>External Host</b>	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. <b>Note:</b> When a RemoteConnect plan is activated for the UCM, this field will be automatically populated. This link will be pushed to Wave when the UCM is deployed in a Remote Disaster Recovery setup to automatically switch to the backup server once the failover occurs.
<b>Port</b>	The port to access Wave Web and Wave Mobile. If behind NAT, please make sure to map the external port to this port.
<b>Certificate Settings</b>	
<b>Default Certificate Auto Renewal</b>	If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected.
<b>Options</b>	Selects the method of acquiring SSL certificates for the UCM web server. Two methods are currently available: <ul style="list-style-type: none"> <li>• <b>Upload Certificate:</b> Upload the appropriate files from one's own PC.</li> <li>• <b>Request Certificate:</b> Enter the domain for which to request a certificate for from "Let's Encrypt".</li> </ul>
<b>TLS Private Key</b>	Uploads the private key for the HTTP server. <b>Note:</b> Key file must be under 2MB in file size and *.pem format. The file name will automatically be changed to "private.pem".
<b>TLS Cert</b>	Uploads the certificate for the HTTP server. <b>Note:</b> Certificate must be under 2MB in file size and *.pem format. This will be used for TLS connections and contains a private key for the client and a signed certificate for the server.

<b>Domain</b>	Enter the domain to request the certificate for and click on "Request Certificate" button. <div style="text-align: center; border: 1px solid blue; padding: 5px; display: inline-block;">Request Certificate</div>
---------------	--

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 UCM630xA 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.

- o UCM630xA 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 UCM6300A, UCM6302A, UCM6304A and UCM6308A, respectively.

<b>Method</b>	Select "Route", "Switch" or "Dual" mode on the network interface of UCM630X. The default setting is "Switch". <ul style="list-style-type: none"> <li>● <b>Route:</b> WAN port will be used for the uplink connection. LAN port will function similarly to a regular router port.</li> <li>● <b>Switch:</b> WAN port will be used for the uplink connection. LAN port will be used as a bridge for connections.</li> <li>● <b>Dual:</b> 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.</li> </ul>
<b>MTU</b>	Specifies the maximum transmission unit value. Default is 1492.
<b>IPv4 Address</b>	
<b>Preferred DNS Server</b>	If configured, this will be used as the Primary DNS server.
<b>WAN (when "Method" is set to "Route")</b>	
<b>IP Method</b>	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
<b>IP Address</b>	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
<b>Subnet Mask</b>	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
<b>Gateway IP</b>	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
<b>DNS Server 1</b>	Enter the DNS server 1 address for static IP settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static IP settings.
<b>Username</b>	Enter the username to connect via PPPoE.
<b>Password</b>	Enter the password to connect via PPPoE.

<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assign the VLAN tag of the layer 2 QoS packets for the WAN port.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assign the priority value of the layer 2 QoS packets for the WAN port.
<b>Enable VoIP VLAN</b>	If enabled, the following VLAN settings will be added to achieve VoIP data diversion.
<b>IP Method</b>	The UCM's address type. Static IP: Manual configuration of address information.
<b>IP Address</b>	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
<b>Subnet Mask</b>	Enter the subnet mask. For example, "255.255.255.0".
<b>Gateway IP</b>	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	This assigns VLAN tag for Layer 2 QoS packets.If you are unsure of the second layer of Qos, please do not change the second layer VLAN tag and priority, this wrong configuration may cause the device to fail to obtain IP address. If set to 0, VLAN is disabled.
<b>Layer 2 QoS 802.1p Priority Value</b>	This assigns priority value for Layer 2 QoS packets.
<b>LAN (when Method is set to "Route")</b>	
<b>IP Address</b>	Enter the IP address assigned to the LAN port. The default setting is 192.168.2.1.
<b>Subnet Mask</b>	Enter the subnet mask. The default setting is 255.255.255.0.
<b>DHCP Server Enable</b>	Enable or disable DHCP server capability. The default setting is "Yes".
<b>DNS Server 1</b>	Enter DNS server address 1. The default setting is 8.8.8.8.
<b>DNS Server 2</b>	Enter DNS server address 2. The default setting is 208.67.222.222.
<b>Allow IP Address From</b>	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
<b>Allow IP Address To</b>	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
<b>Default IP Lease Time</b>	Enter the IP lease time (in seconds). The default setting is 43200.
<b>LAN (when Method is set to "Switch")</b>	
<b>IP Method</b>	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
<b>IP Address</b>	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
<b>Subnet Mask</b>	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
<b>Gateway IP</b>	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
<b>DNS Server 1</b>	Enter the DNS server 1 address for static IP settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static IP settings.
<b>Username</b>	Enter the username to connect via PPPoE.

<b>Password</b>	Enter the password to connect via PPPoE.
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assign the VLAN tag of the layer 2 QoS packets for the LAN port. The accepted range is 2-4094.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assign the priority value of the layer 2 QoS packets for the LAN port. The default value is 0.
<b>Enable VoIP VLAN</b>	If enabled, the following VLAN settings will be added to achieve VoIP data diversion.
<b>IP Method</b>	The UCM's address type. Static IP: Manual configuration of address information.
<b>IP Address</b>	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
<b>Subnet Mask</b>	Enter the subnet mask. For example, "255.255.255.0".
<b>Gateway IP</b>	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	This assigns VLAN tag for Layer 2 QoS packets.If you are unsure of the second layer of Qos, please do not change the second layer VLAN tag and priority, this wrong configuration may cause the device to fail to obtain IP address. The accepted range is 2-4094.
<b>Layer 2 QoS 802.1p Priority Value</b>	This assigns priority value for Layer 2 QoS packets.
<b>LAN 1 / LAN 2 (when Method is set to "Dual")</b>	
<b>Default Interface</b>	If "Dual" is selected as "Method", users will need to 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.
<b>IP Method</b>	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
<b>IP Address</b>	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
<b>Subnet Mask</b>	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
<b>Gateway IP</b>	Enter the gateway IP address for static IP settings when the port is assigned as the default interface. The default setting is 0.0.0.0.
<b>DNS Server 1</b>	Enter the DNS server 1 address for static IP settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static IP settings.
<b>Username</b>	Enter the username to connect via PPPoE.
<b>Password</b>	Enter the password to connect via PPPoE.
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assign the VLAN tag of the layer 2 QoS packets for the LAN port. The accepted range is 2-4094.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assign the priority value of the layer 2 QoS packets for the LAN port. The default value is 0.
<b>IP Method</b>	The UCM's address type. Static IP: Manual configuration of address information.

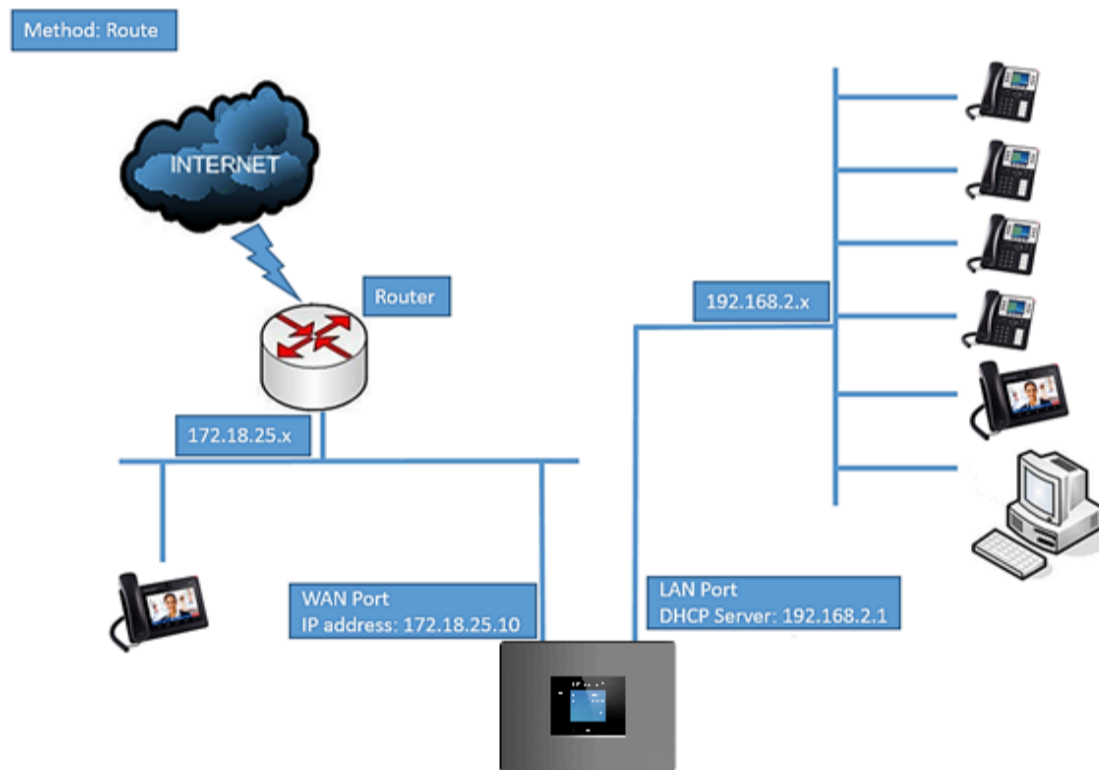
<b>IP Address</b>	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
<b>Subnet Mask</b>	Enter the subnet mask. For example, "255.255.255.0".
<b>Gateway IP</b>	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	This assigns VLAN tag for Layer 2 QoS packets.If you are unsure of the second layer of Qos, please do not change the second layer VLAN tag and priority, this wrong configuration may cause the device to fail to obtain IP address. The accepted range is 2-4094.
<b>Layer 2 QoS 802.1p Priority Value</b>	This assigns priority value for Layer 2 QoS packets.
<b>IPv6 Address</b>	
<b>WAN (when "Method" is set to "Route")</b>	
<b>IP Method</b>	Select Auto or Static. The default setting is Auto
<b>IP Address</b>	Enter the IP address for static IP settings.
<b>IP Prefixlen</b>	Enter the Prefix length for static settings. Default is 64
<b>DNS Server 1</b>	Enter the DNS server 1 address for static settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static settings.
<b>LAN (when Method is set to "Route")</b>	
<b>DHCP Server</b>	Select Disable, Auto, or DHCPv6.  <ul style="list-style-type: none"> <li>● <b>Disable:</b> the DHCPv6 server is disabled.</li> <li>● <b>Auto:</b> Stateless address auto configuration using NDP protocol.</li> <li>● <b>DHCPv6:</b> Stateful address auto configuration using DHCPv6 protocol.</li> </ul> The default setting is Disabled.
<b>DHCP Prefix</b>	Enter DHCP prefix. (Default is 2001:db8:2:2::)
<b>DHCP prefixlen</b>	Enter the Prefix length for static settings. Default is 64
<b>DNS Server 1</b>	Enter the DNS server 1 address for static settings. Default is (2001:4860:4860::8888 )
<b>DNS Server 2</b>	Enter the DNS server 2 address for static settings. Default is (2001:4860:4860::8844 )
<b>Allow IP Address From</b>	Configure starting IP address assigned by the DHCP prefix and DHCP prefixlen.
<b>Allow IP Address To</b>	Configure the ending IP address assigned by the DHCP Prefix and DHCP prefixlen.
<b>Default IP Lease Time</b>	Configure the lease time (in second) of the IP address.
<b>LAN (when Method is set to "Switch")</b>	
<b>IP Method</b>	Select Auto or Static. The default setting is Auto
<b>IP Address</b>	Enter the IP address for static IP settings.

<b>IP Prefixlen</b>	Enter the Prefix length for static settings. Default is 64
<b>DNS Server 1</b>	Enter the DNS server 1 address for static settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static settings.
<b>LAN 1 / LAN 2 (when Method is set to "Dual")</b>	
<b>Default Interface</b>	Users will need to 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.
<b>IP Method</b>	Select Auto or Static. The default setting is Auto
<b>IP Address</b>	Enter the IP address for static IP settings.
<b>IP Prefixlen</b>	Enter the Prefix length for static settings. Default is 64
<b>DNS Server 1</b>	Enter the DNS server 1 address for static settings.
<b>DNS Server 2</b>	Enter the DNS server 2 address for static settings.
<b>Network Port Traffic Control</b>	
<b>LAN (when Method is set to "Switch")</b>	
<b>Enable Network Port Traffic Storm Alert</b>	The UCM will send a an alert notification/email when there is an excessive number of packets in the LAN that impacts the overall performance of the network. <b>Note:</b> To enable this feature email or HTTP notification should be set up correctly In <b>Maintenance → System Events</b> .
<b>Ignore Safe Operational Flow</b>	When enabled, it will ignore traffic storm alarms triggered by users' own operations after logging in, including security operations such as firmware upgrades, uploading backup files, beeping, zero-configuration templates/firmware, recording files, and downloading files from network disks.
<b>Network Port Receiving Traffic Control</b>	You can monitor the traffic in the RX direction on each network port and generate an alarm when the corresponding alarm event is turned on and the set threshold value is exceeded. The threshold range is 1 - 1024000 in kbps and 1 - 1000 in mbps.
<b>LAN 1 &amp; LAN 2 (when Method is set to "Dual")</b>	
<b>Enable Network Port Traffic Storm Alert</b>	The UCM will send a an alert notification/email when there is an excessive number of packets in the LAN that impacts the overall performance of the network. <b>Note:</b> To enable this feature email or HTTP notification should be set up correctly In <b>Maintenance → System Events</b> .
<b>Ignore Safe Operational Flow</b>	When enabled, it will ignore traffic storm alarms triggered by users' own operations after logging in, including security operations such as firmware upgrades, uploading backup files, beeping, zero-configuration templates/firmware, recording files, and downloading files from network disks.
<b>LAN1 &amp; LAN2 - Network Port Receiving Traffic Control</b>	You can monitor the traffic in the RX direction on each network port and generate an alarm when the corresponding alarm event is turned on and the set threshold value is exceeded. The threshold range is 1 - 1024000 in kbps and 1 - 1000 in mbps.
<b>LAN &amp; WAN (When Method is set to Route Mode)</b>	

<p><b>Enable Network Port Traffic Storm Alert</b></p>	<p>The UCM will send a an alert notification/email when there is an excessive number of packets in the LAN that impacts the overall performance of the network.</p> <p><b>Note:</b> To enable this feature email or HTTP notification should be set up correctly In <b>Maintenance</b> → <b>System Events</b>.</p>
<p><b>Ignore Safe Operation Flow</b></p>	<p>When enabled, it will ignore traffic storm alarms triggered by users' own operations after logging in, including security operations such as firmware upgrades, uploading backup files, beeping, zero-configuration templates/firmware, recording files, and downloading files from network disks.</p>
<p><b>WAN: Network Port Receiving Traffic Control</b></p>	<p>You can monitor the traffic in the RX direction on each network port and generate an alarm when the corresponding alarm event is turned on and the set threshold value is exceeded.</p> <p>The threshold range is 1 - 1024000 in kbps and 1 - 1000 in mbps.</p>
<p><b>LAN: Network Port Receiving Traffic Control</b></p>	<p>You can monitor the traffic in the RX direction on each network port and generate an alarm when the corresponding alarm event is turned on and the set threshold value is exceeded.</p> <p>The threshold range is 1 - 1024000 in kbps and 1 - 1000 in mbps.</p>

o **Method: Route**

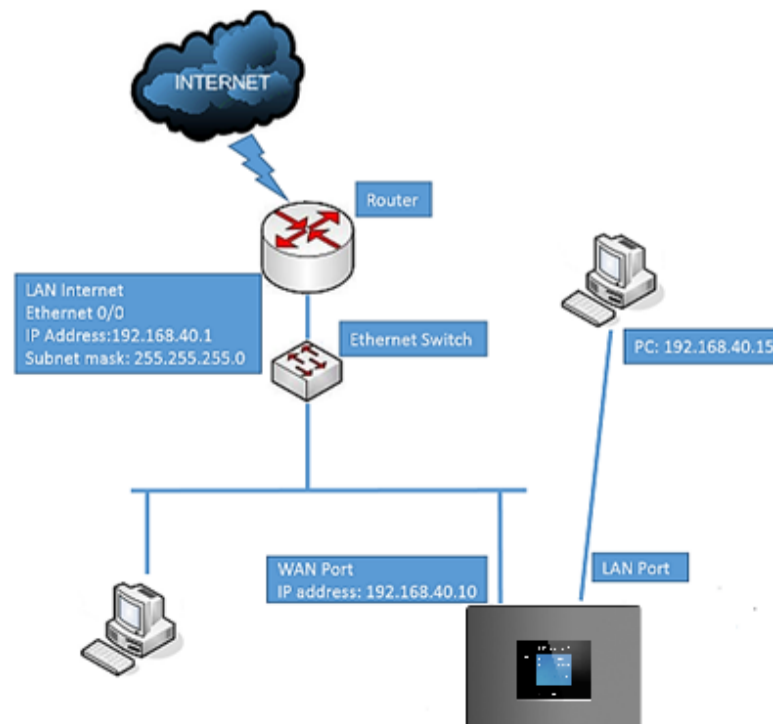
When the UCM630xA has, method set to Route in network settings, WAN port interface is used for uplink connection and LAN port interface is used as a router. Please see a sample diagram below.



UCM6302A Network Interface Method: Route

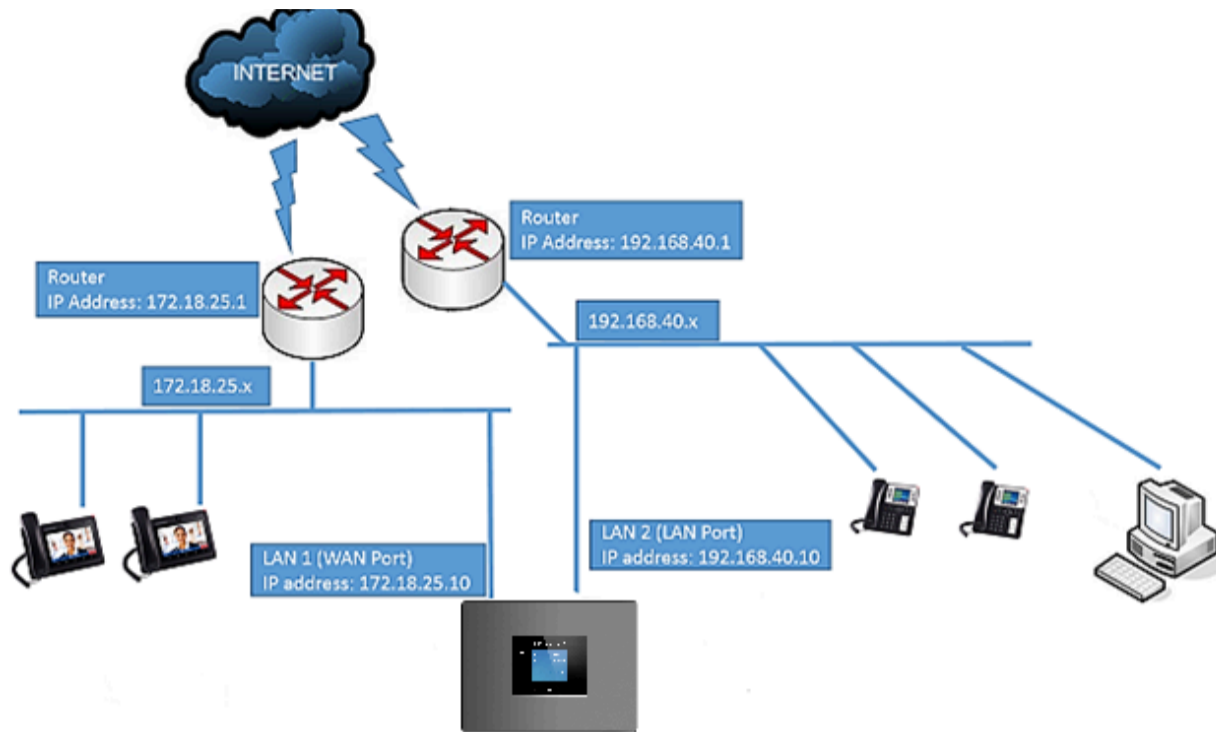
o **Method: Switch**

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



o **Method: Dual**

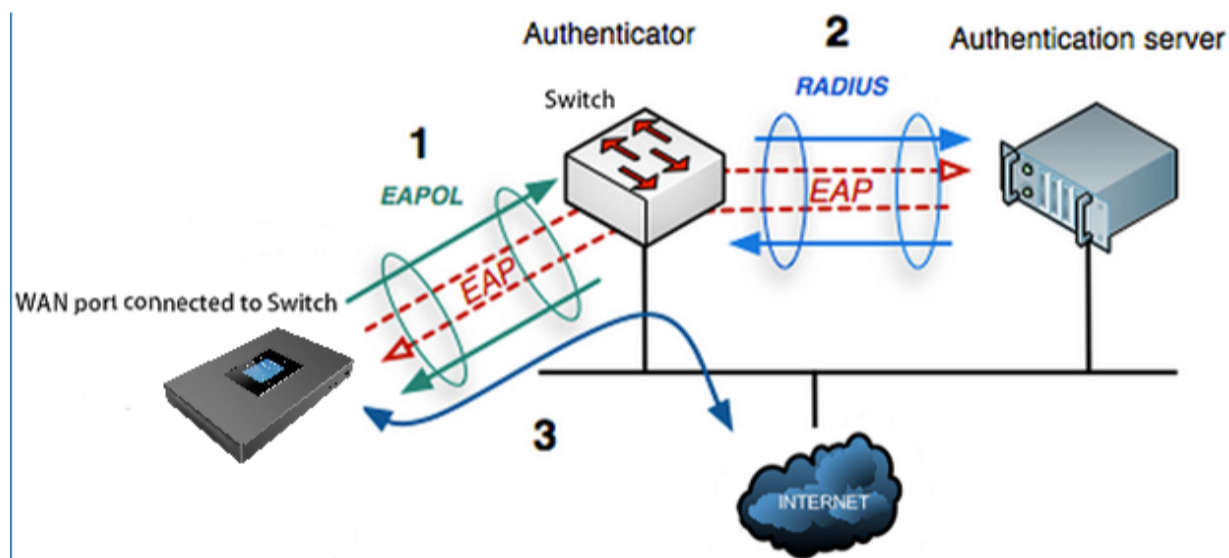
Both WAN port and LAN port are used for uplink connection. Users will need assign LAN 1 or LAN 2 as the default interface in option "Default Interface" and configure "Gateway IP" if static IP is used for this interface.



UCM6302A 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 UCM630xA supports 802.1X as a supplicant/client to be authenticated. The following diagram and figure show UCM630xA use 802.1X mode "EAP-MD5" on WAN port as client in the network to access Internet.



UCM630xA Using 802.1X as Client

Network Settings	
Basic Settings	<u>802.1X Settings</u>
802.1X Mode:	EAP-MD5
* Identity:	8021xxUCM6302
* MD5 Password:	.....

UCM630xA Using 802.1X EAP-MD5



The following table shows the configuration parameters for 802.1X on UCM630xA. 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.

<b>802.1X Mode</b>	Select 802.1X mode. The default setting is "Disable". The supported 802.1X mode are: <ul style="list-style-type: none"> <li>○ EAP-MD5</li> <li>○ EAP-TLS</li> <li>○ EAP-PEAPv0/MSCHAPv2</li> </ul>
<b>Identity</b>	Enter 802.1X mode Identity information.
<b>MD5 Password</b>	Enter 802.1X mode MD5 password information.
<b>802.1X CA Certificate</b>	Select 802.1X certificate from local PC and then upload.
<b>802.1X Client Certificate</b>	Select 802.1X client certificate from local PC and then upload.

*UCM630xA Network Settings → 802.1X*

## Static Routes

The UCM630xA 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 UCM630xA 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 UCM630xA 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.

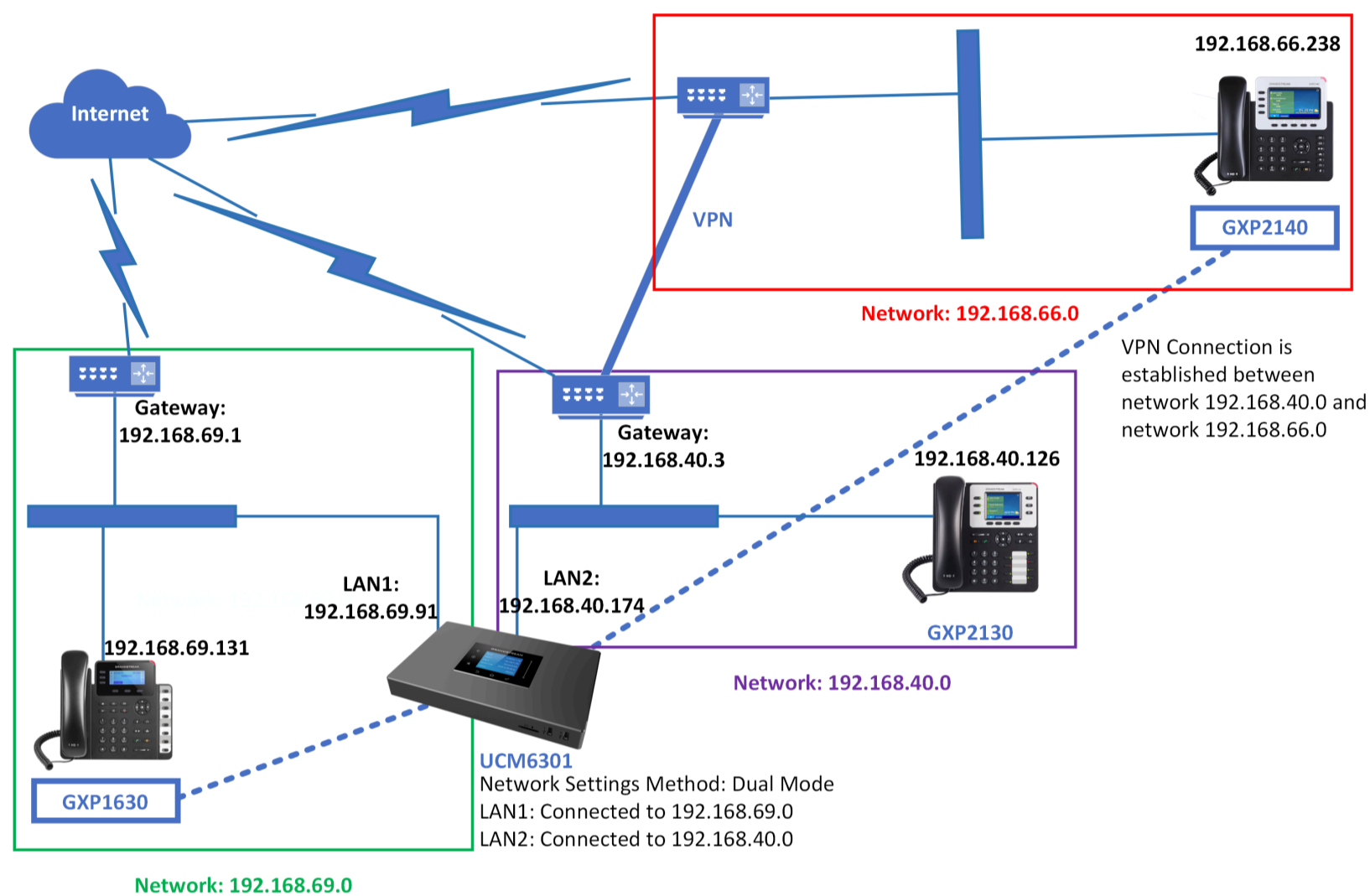
<b>Destination</b>	Configure the destination IPv4 address or the destination IPv6 subnet for the UCM630xA to reach using the static route.  Example: IPv4 address – <b>192.168.66.4</b>  IPv6 subnet – <b>2001:740:D::1/64</b>
<b>Subnet Mask</b>	Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255.  Example: <b>255.255.255.0</b>
<b>Gateway</b>	Configure the IPv4 or IPv6 gateway address so that the UCM630xA can reach the destination via this gateway. Gateway address is optional.  Example: <b>192.168.40.5 or 2001:740:D::1</b>

<b>Interface</b>	Specify the network interface on the UCM630xA to reach the destination using the static route.  LAN interface is eth0; WAN interface is eth1.
------------------	---

UCM630xA Network Settings → Static Routes

Static routes configuration can be reset from LCD menu → Network Menu.

The following diagram shows a sample application of static route usage on UCM6304A.



--- GXP1630 and GXP2140 call each other

UCM6304A Static Route Sample

The network topology of the above diagram is as below:

- Network 192.168.69.0 has IP phones registered to UCM6304A LAN 1 address
- Network 192.168.40.0 has IP phones registered to UCM6304A LAN 2 address
- Network 192.168.66.0 has IP phones registered to UCM6304A 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 UCM6304A. Therefore, we need configure a static route on the UCM6304A so that the phones in isolated networks can make calls between each other.

Create New IPV4 Static Route

* Destination :	192.168.66.0
Subnet Mask :	255.255.255.0
Gateway :	192.168.40.3
* Protocol Type :	WAN

UCM6304A 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.

<b>WAN Port</b>	Specify the WAN port number or a range of WAN ports. Unlimited number of ports can be configured.  <b>Note:</b> 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.
<b>LAN IP</b>	Specify the LAN IP address.
<b>LAN Port</b>	Specify the LAN port number or a range of LAN ports.  <b>Note:</b> 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.
<b>Protocol Type</b>	Select protocol type "UDP Only", "TCP Only" or "TCP/UDP" for the forwarding in the selected port. The default setting is "UDP Only".

UCM630xA Network Settings →Port Forwarding

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

- UCM630xA network mode is set to "Route".
- UCM630xA WAN port is connected to uplink switch, with a public IP address configured, e.g. 1.1.1.1.
- UCM630xA 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 UCM630xA. It obtains IP address 192.168.2.100 from UCM630xA DHCP pool.
- On the UCM630xA Web GUI→**System Settings**→**Network Settings**→**Port Forwarding**, configure a port forwarding entry as the figure shows below.

+ Create New Port Forwarding

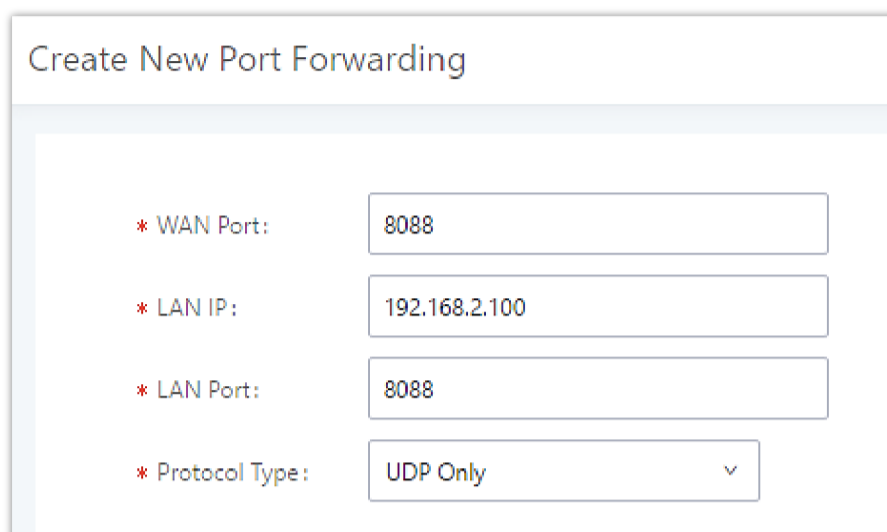
Click on

**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 UCM630xA.

**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.



Create New Port Forwarding

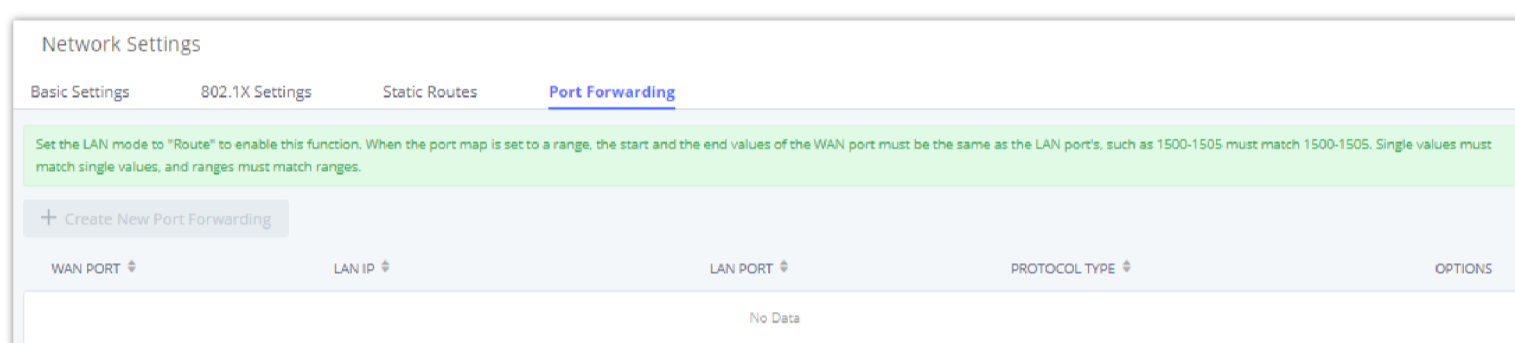
\* WAN Port: 8088

\* LAN IP: 192.168.2.100

\* LAN Port: 8088

\* Protocol Type: UDP Only

*Create New Port Forwarding*



Network Settings

Basic Settings 802.1X Settings Static Routes **Port Forwarding**

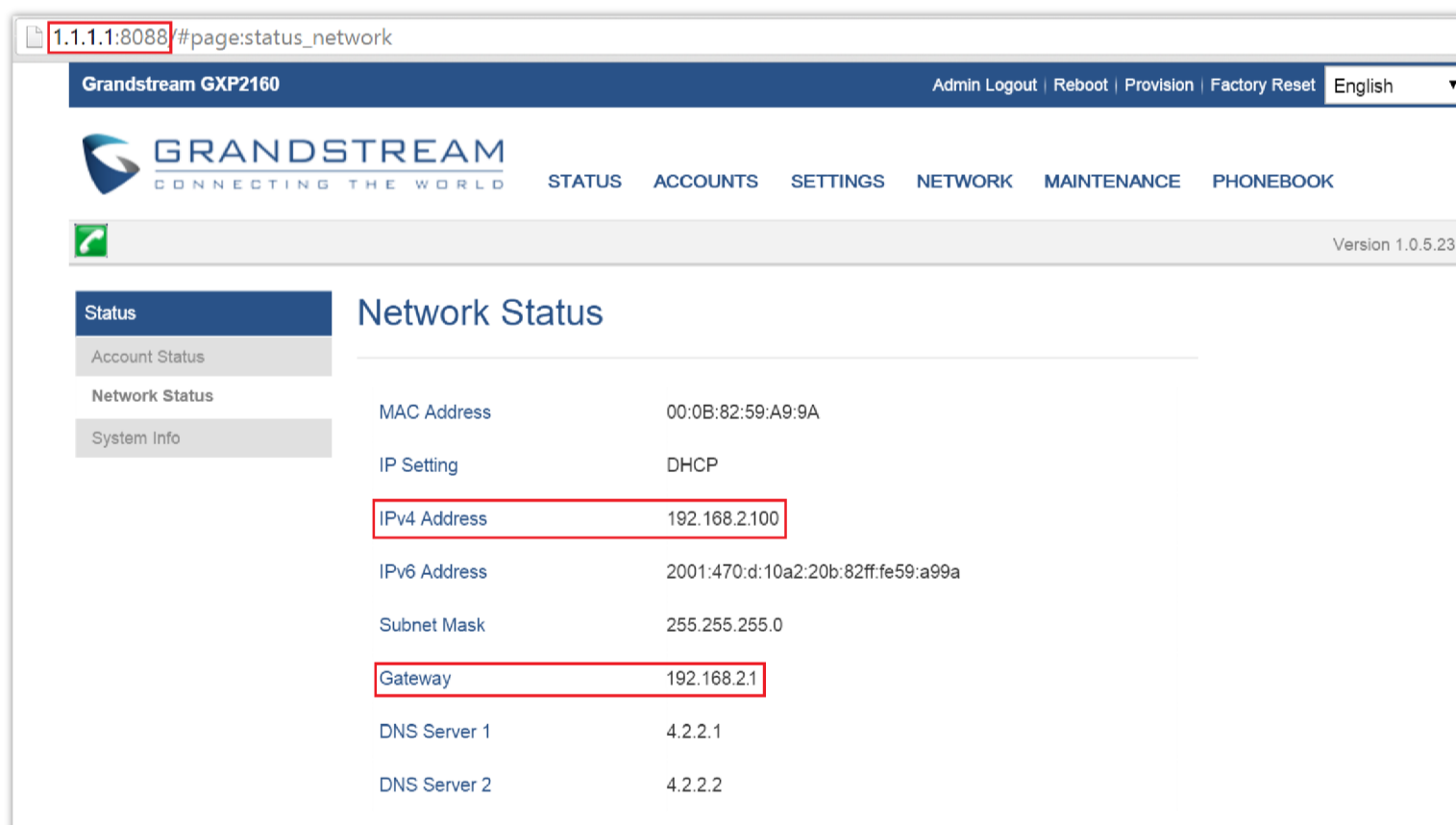
Set the LAN mode to "Route" to enable this function. When the port map is set to a range, the start and the end values of the WAN port must be the same as the LAN port's, such as 1500-1505 must match 1500-1505. Single values must match single values, and ranges must match ranges.

+ Create New Port Forwarding

WAN PORT	LAN IP	LAN PORT	PROTOCOL TYPE	OPTIONS
No Data				

*UCM630xA 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).



1.1.1.1:8088/#page:status\_network

Grandstream GXP2160 Admin Logout | Reboot | Provision | Factory Reset English

GRANDSTREAM CONNECTING THE WORLD STATUS ACCOUNTS SETTINGS NETWORK MAINTENANCE PHONEBOOK

Version 1.0.5.23

Status Network Status

Account Status

Network Status

System Info

MAC Address	00:0B:82:59:A9:9A
IP Setting	DHCP
IPv4 Address	192.168.2.100
IPv6 Address	2001:470:d:10a2:20b:82ff:fe59:a99a
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
DNS Server 1	4.2.2.1
DNS Server 2	4.2.2.2

*GXP2160 Web Access using UCM6302A Port Forwarding*

## ARP Settings

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

<b>ARP GC Threshold 1</b>	Minimum number of entries to keep. Garbage collector will not purge entries if there are fewer than this number. The default value is 128.
---------------------------	--

<b>ARP GC Threshold 2</b>	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.
<b>ARP GC Threshold 3</b>	Maximum number of non-PERMANENT neighbor entries allowed. Increase this when using large numbers of interfaces and when communicating with large numbers of directly connected peers. The default value is 1024.

ARP Settings

## OpenVPN®

OpenVPN® settings allow the users to configure UCM630xA to use VPN features, the following table gives details about the various options in order to configure the UCM as OpenVPN Client.

• OpenVPN uses TLS version 1.2. Please make sure that the OpenVPN server has the same TLS version, otherwise the connection will fail.

OpenVPN® Enable:

Configuration Method:

OpenVPN® Server Address:

OpenVPN® Server Protocol:

OpenVPN® Device Mode:

OpenVPN® Use Compression:

Allow Weak SSL Ciphers:

OpenVPN® Encryption Algorithm:

OpenVPN® CA Cert:

OpenVPN® Client Cert:

OpenVPN® Client Key:

User Authentication:

Username:

Password:

© 2002-2014 OpenVPN Technologies, Inc.  
OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

OpenVPN® Feature on the UCM630xA

<b>OpenVPN® Enable</b>	Enable / Disable the OpenVPN® feature.
<b>Configuration Method</b>	Select the OpenVPN® configuration method. <b>Manual Configuration:</b> Allows to configure OpenVPN® settings manually. <b>Upload Configuration File:</b> Allows to upload .ovpn and .conf files to the UCM and to automatically configure OpenVPN® settings.
<b>OpenVPN® Server Address</b>	Configures the hostname/IP and port of the server. For example 192.168.1.2:22
<b>OpenVPN® Server Protocol</b>	Specify the protocol user, user should use the same settings as used on the server
<b>OpenVPN® Device mode</b>	Use the same setting as used on the server. <ul style="list-style-type: none"> <li>• <b>Dev TUN:</b> Create a routed IP tunnel.</li> <li>• <b>Dev TAP:</b> Create an Ethernet tunnel.</li> </ul>

<b>OpenVPN® Use Compression</b>	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.
<b>Enable Weak SSL Ciphers</b>	Either to enable the Weak SSL ciphers or not.
<b>OpenVPN® Encryption Algorithm</b>	Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server.
<b>OpenVPN® CA Cert</b>	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
<b>OpenVPN® Client Cert</b>	Upload a client certificate. This file will be renamed as 'client.crt' automatically.
<b>OpenVPN® Client Key</b>	Upload a client private key. This file will be renamed as 'client.key' automatically.
<b>Username</b>	Username used to authenticate into the server.
<b>Password</b>	Password used to authenticate into the server.

## DDNS Settings

DDNS setting allows user to access UCM630xA via domain name instead of IP address.

The UCM supports DDNS service from the following DDNS provider:

- o dydns.org
- o noip.com
- o freedns.afraid.org
- o zoneedit.com
- o oray.net

Here is an example of using noip.com for DDNS.

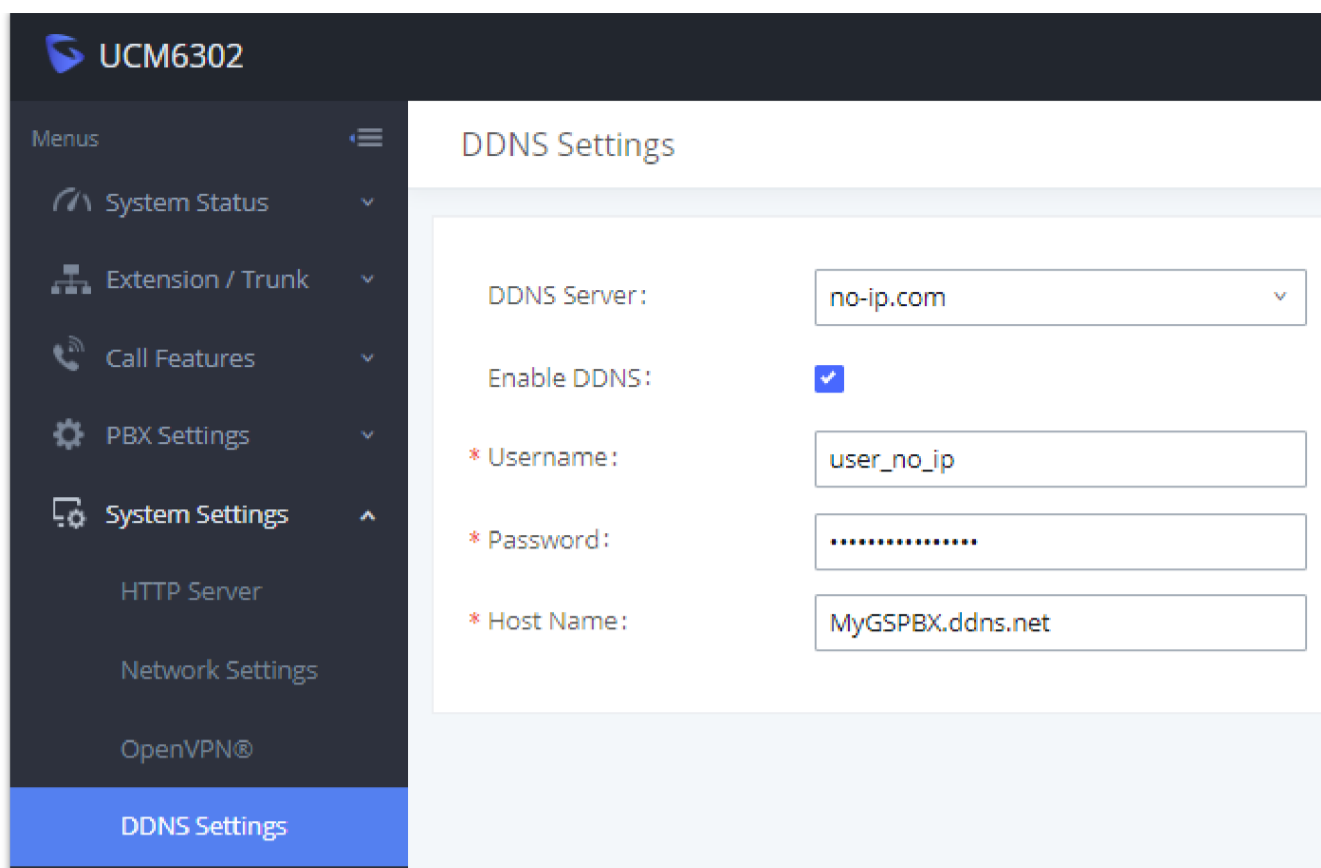
1. Register domain in DDNS service provider. Please note the UCM630xA needs to have public IP access.

**Hostname Information**

<b>Hostname:</b>	haograndstream.ddns.net <span style="float: right;">?</span>
<b>Host Type:</b>	<input checked="" type="radio"/> DNS Host (A) <input type="radio"/> DNS Host (Round Robin) <input type="radio"/> DNS Alias (CNAME) <span style="float: right;">?</span> <input type="radio"/> Port 80 Redirect <input type="radio"/> Web Redirect
<b>IP Address:</b>	<input style="width: 100px;" type="text" value="1.2.3.4"/> Last Update: 2015-01-07 17:29:20 PST <span style="float: right;">?</span>
<b>Assign to Group:</b>	<input style="width: 150px;" type="text" value="- No Group -"/> <input type="button" value="▼"/> <input type="button" value="Configure Groups"/> <span style="float: right;">?</span>
<b>Enable Wildcard:</b>	Wildcards are a Plus / Enhanced feature. <a href="#">Upgrade Now!</a> <span style="float: right;">?</span>
<b>Advanced Records:</b>	TXT, SPF, and SRV records and the use of some special clients are Plus / Enhanced features. <a href="#">Upgrade now</a> to use them. <span style="float: right;">?</span>

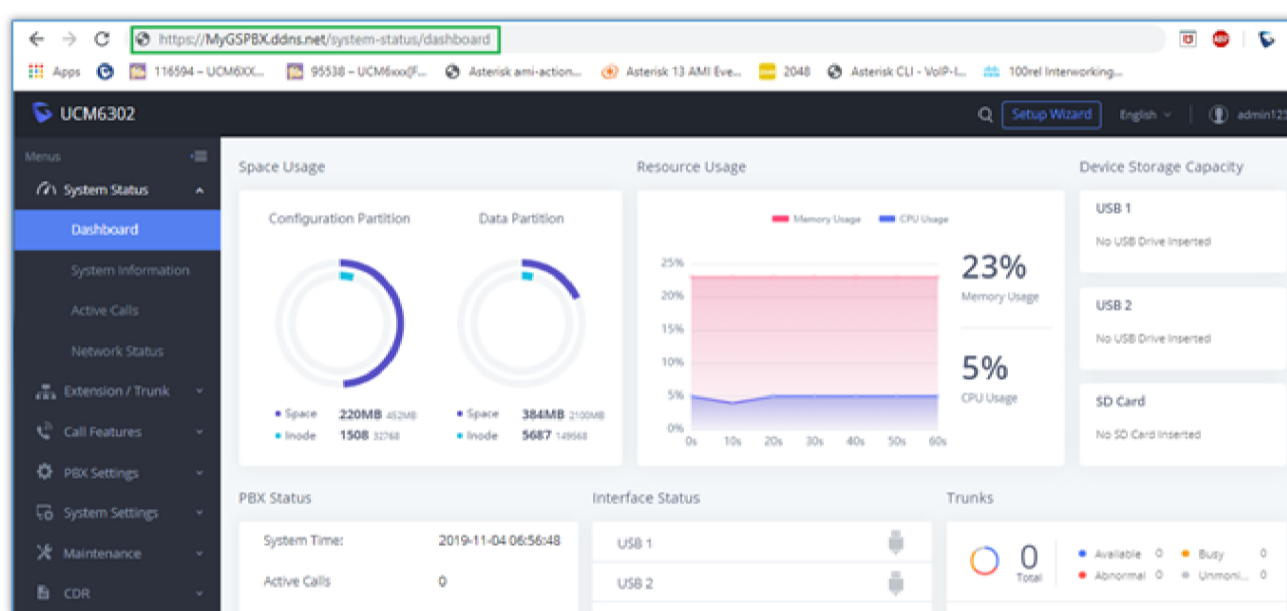
*Register Domain Name on noip.com*

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



UCM630xA DDNS Setting

3. Now you can use domain name instead of IP address to connect to the UCM630xA Web GUI.



Using Domain Name to Connect to UCM630xA

## Security Settings

The UCM630xA provides users firewall security configurations to prevent certain malicious attack to the UCM630xA system. Users could configure to allow, restrict, or reject specific traffic through the device for security and bandwidth purpose. The UCM630xA also provides Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. To configure firewall settings in the UCM630xA, 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 UCM630xA.

Port	Process	Type	Protocol or Service
7777	Asterisk	TCP/IPv4	SIP
389	Slapd	TCP/IPv4	LDAP
6060	zero_config	UDP/IPv4	UCM630xA zero_config service

Port	Process	Type	Protocol or Service
5060	Asterisk	UDP/IPv4	SIP
4569	Asterisk	UDP/IPv4	IAX
38563	Asterisk	udp/ipv4	SIP
10000	gs_avs	udp/ipv4	gs_avs
10001	gs_avs	udp/ipv4	gs_avs
10002	gs_avs	udp/ipv4	gs_avs
10003	gs_avs	udp/ipv4	gs_avs
10004	gs_avs	udp/ipv4	gs_avs
10005	gs_avs	udp/ipv4	gs_avs
10006	gs_avs	udp/ipv4	gs_avs
10007	gs_avs	udp/ipv4	gs_avs
10010	gs_avs	udp/ipv4	gs_avs
10012	gs_avs	udp/ipv4	gs_avs
10013	gs_avs	udp/ipv4	gs_avs
10014	gs_avs	udp/ipv4	gs_avs
10015	gs_avs	udp/ipv4	gs_avs
10018	gs_avs	udp/ipv4	gs_avs
10019	gs_avs	udp/ipv4	gs_avs
10020	gs_avs	udp/ipv4	gs_avs
6066	Python	udp/ipv4	python
3306	Mysqld	tcp/ipv4	mysqld
45678	Python	udp/ipv4	python
8439	Lighttpd	tcp/ipv4	HTTP
8088	asterisk	tcp/ipv4	SIP
8888	Pbxmid	tcp/ipv4	pbxmid
25	Master	tcp/ipv4	master
636	Slapd	tcp/ipv4	SLDAP
4569	asterisk	udp/ipv6	IAX
42050	asterisk	udp/ipv6	SIP
7681	Pbxmid	tcp/ipv4	pbxmid

*UCM630xA Firewall → Static Defense → Current Service*

For typical firewall settings, users could configure the following options on the UCM630xA.

<b>Ping Defense Enable</b>	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 (UCM630xA) interface.
<b>SYN-Flood Defense Enable</b>	<p>Allows the UCM630xA 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.</p> <ul style="list-style-type: none"> <li>○ eth(0)LAN defends against attacks directed to the LAN IP address of the UCM630xA.</li> <li>○ eth(1)WAN defends against attacks directed to the WAN IP address of the UCM630xA.</li> </ul> <p>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.</p>

<b>Ping-of-Death Defense Enable</b>	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 (UCM630xA) interface.
-------------------------------------	---

*Typical Firewall Settings*

Under "Custom Firewall Settings", users could create new rules to accept, reject or drop certain traffic going through the UCM630xA. 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

**Create New Firewall Rule**

---

\* Rule Name:

\* Action:

\* Type:

\* Interface:

\* Service:



*Create New Firewall Rule*

<b>Rule Name</b>	Specify the Firewall rule name to identify the firewall rule.
<b>Action</b>	<p>Select the action for the Firewall to perform.</p> <ul style="list-style-type: none"> <li>○ ACCEPT</li> <li>○ REJECT</li> <li>○ DROP</li> </ul>
<b>Type</b>	<p>Select the traffic type.</p> <ul style="list-style-type: none"> <li>○ <b>IN</b></li> </ul> <p>If selected, users will need specify the network interface "LAN" or "WAN" (for UCM630xA) for the incoming traffic.</p> <ul style="list-style-type: none"> <li>○ <b>OUT</b></li> </ul>
<b>Interface</b>	Select the interface to use the Firewall rule.

<b>Service</b>	<p>Select the service type.</p> <ul style="list-style-type: none"> <li>○ <b>FTP</b></li> <li>○ <b>SSH</b></li> <li>○ <b>Telnet</b></li> <li>○ <b>HTTP</b></li> <li>○ <b>LDAP</b></li> <li>○ <b>Custom</b></li> </ul> <p>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".</p>
<b>Source IP Address and Port</b>	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).
<b>Destination IP Address and Port</b>	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).
<b>Protocol</b>	Select the protocol for the rule to be used.

#### *Firewall Rule Settings*

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 UCM630xA 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 UCM630xA 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 UCM630xA firewall, which will then be displayed in the web page. Please refer to the following table for dynamic defense options on the UCM630xA.

<b>Dynamic Defense Enable</b>	Enable dynamic defense. The default setting is disabled.
<b>Blacklist Update Interval</b>	Configure the blacklist update time interval (in seconds). The default setting is 120.
<b>Connection Threshold</b>	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.
<b>Dynamic Defense Whitelist</b>	<p>Allowed IPs and ports range, multiple IP addresses and port range.</p> <p>For example:</p> <p><b>192.168.2.100-192.168.2.105, 1000:9999</b></p>

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 UCM630xA it will be added into UCM630xA blacklist.
- This host 192.168.5.7 will be blocked by the UCM630xA 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 UCM630xA it will not be added into UCM630xA blacklist. It can still establish TCP connection with the UCM630xA.

The screenshot shows the 'Dynamic Defense' configuration page. At the top, there are four tabs: 'Static Defense', 'Dynamic Defense' (which is selected and underlined), 'Fail2Ban', and 'SSH Access'. Below the tabs, the page title is 'Dynamic Defense'. The configuration includes: 'Dynamic Defense Enable' with a checked checkbox; '\* Blacklist Update Interval (s):' with a text input field containing '500'; '\* Connection Threshold:' with a text input field containing '20'; and 'Dynamic Defense Whitelist:' with a text area containing '192.168.5.100-192.168.5.200 1500:2000'.

Configure Dynamic Defense

## Fail2ban

Fail2Ban feature on the UCM630xA provides intrusion detection and prevention for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. Once the entry is detected within "Max Retry Duration", the UCM630xA 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.

The screenshot shows the 'Fail2Ban' configuration page under 'Security Settings'. At the top, there are four tabs: 'Static Defense', 'Dynamic Defense', 'Fail2Ban' (which is selected and underlined), and 'SSH Access'. Below the tabs, the page title is 'Global Settings'. The configuration includes: 'Enable Fail2Ban:' with an unchecked checkbox; 'Banned Duration (s):' with a text input field containing '600'; 'Max Retry Duration (s):' with a text input field containing '600'; and 'Fail2ban Whitelist:' with a table structure. The table has two columns: 'Fail2ban Whitelist' and 'Description / Comment'. There is a red minus button to the right of the 'Description / Comment' column and a blue plus button labeled 'Add Fail2ban Whitelist' below it. Below the 'Global Settings' section is the 'Local Settings' section, which includes: 'Asterisk Service:' with an unchecked checkbox; 'Login Attack Defense:' with an unchecked checkbox; 'Customer Service System Call' with an unchecked checkbox; and 'Defense:' with an unchecked checkbox.

Fail2ban Settings

### Global Settings

<b>Enable Fail2Ban</b>	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.
<b>Banned Duration</b>	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.
<b>Max Retry Duration</b>	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.
<b>MaxRetry</b>	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5.
<b>Fail2Ban Whitelist</b>	Configure IP address, CIDR mask, or DNS host in the whitelist. Fail2Ban will not ban the host with a matching address in this list. Up to 50 addresses can be added to the list descriptions/comments can be added for each whitelist entry for admin to log what's the whitelist IP address is for.
<b>Local Settings</b>	
<b>Asterisk Service</b>	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.
<b>Listening Port Number</b>	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.
<b>MaxRetry</b>	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".
<b>Login Attack Defense</b>	Enables defense against excessive login attacks to the UCM's web GUI. The default setting is disabled.
<b>Listening Port Number</b>	This is the Web GUI listening port number which is configured under System Settings→ HTTP Server→ Port. The default is 8089.
<b>MaxRetry</b>	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.
<b>Customer Service System Call Defense</b>	Enable call defense in the customer service system. Off by default.
<b>Listening Port Number</b>	The current service listening port. Default UDP port: 5060, TCP port: 5060, 5061, WebSocket communication port: 8088.
<b>MaxRetry</b>	Set the maximum number of calls allowed in the "time span". The local matching threshold has a higher priority than the global matching threshold. The default setting is 5.
<b>Blacklist</b>	
<b>Blacklist</b>	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 UCM630xA 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.

Tick "Enable remote SSH" option, the system will allow remote SSH access via the GDMS platform. This option is turned off by default, and it is strongly recommended to turn off this option when remote troubleshooting is not required.

**Security Settings**

Static Defense      Dynamic Defense      Fail2Ban      SSH Access

---

Enable SSH Access     

Enable Remote SSH     

\* Access Token

SSH Access

<b>Enable SSH Access</b>	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.
<b>Enable Remote SSH</b>	If this option is enabled, remote SSH access will be allowed through the Feedback platform. It is strongly recommended to keep this disabled unless remote troubleshooting is necessary.
<b>Access Token</b>	Please enter the token to request SSH data.

## Data/File Encryption

The UCM6300 Series offers encryption for your data stored on the internal storage space of the UCM or on the attached storage units (e.g., SD Card, USB HDD/SSD, USB Flash Drive). This feature will harden the security and confidentiality of your data, which renders it impossible to read data in case they end up acquired by unauthorized parties.

## Security Settings

Static Defense   Dynamic Defense   Fail2Ban   SSH Access   Data/File Encryption

Encrypted storage of sensitive information/files on the device prevents leakage of sensitive information and unauthorized access to information.

Type    All    Config File    IM Files    IM Message    Recording Files  
 Video Recording Files    Voicemail

**i** Encryption of audio and video files on external storage will prevent direct opening/viewing of them outside the UCM webUI. [Decryption Tool](#) will be required to decrypt and open them. See [Instructions](#) for usage details.

Secret Key

[Export](#)   [Update](#)   **i**

### Data/File Encryption Status

[Encrypt](#)

<input type="checkbox"/> Type	Security	Options
<input type="checkbox"/> Config File	<div style="width: 100%; height: 10px; background-color: green;"></div> Strong	<a href="#">🔄</a>
<input type="checkbox"/> IM Files	<div style="width: 100%; height: 10px; background-color: green;"></div> Strong	<a href="#">🔄</a>
<input type="checkbox"/> IM Message	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	<a href="#">🔄</a>
<input type="checkbox"/> Recording Files	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	<a href="#">🔄</a>
<input type="checkbox"/> Video Recording Files	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	<a href="#">🔄</a>
<input type="checkbox"/> Voicemail	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	<a href="#">🔄</a>

[Cancel](#)   [Save](#)

### **i** Note

Encrypting the data stored on attached storage units will prevent the user from browsing the data directly from the UCM USB/SD Card file explorer.

## Enabling Data/File Encryption

To choose which files are going to be encrypted, use the following settings to enable the encryption for specific types of data.

Encrypted storage of sensitive information/files on the device prevents leakage of sensitive information and unauthorized access to information.

Type    All    Config File    IM Files    IM Message    Recording Files  
 Video Recording Files    Voicemail

**i** Encryption of audio and video files on external storage will prevent direct opening/viewing of them outside the UCM webUI. [Decryption Tool](#) will be required to decrypt and open them. See [Instructions](#) for usage details.

*File/Data Type*

Once the user chooses which data to encrypt, the user can save the setting. This means that any data created after this configuration will be encrypted, however, all the data which has been created prior to this configuration is not encrypted. To encrypt it please see the sections below.

## Encrypting/Decrypting Files

When the user click on "Export" button, a CSV file which contains the secret key will be downloaded. This key can be stored safely and used to decrypt the data later on.

Secret Key

[Export](#)

[Update](#)

**i**

You can update the secret key using the "Update" button, this would require entering the administrator's password to allow the user to change the secret key.

**Note**

Please note that only the super administrator can change the secret key.

**Warning**

If the key has been updated after it has been exported, this will render the old key obsolete and the user will not be able to decrypt the data. We highly recommend that you do not change the encryption key after it has been backed up. In case you need to change the encryption key, please make sure to export the new one and store it safely.

In the following section, the user can view the status of the files, whether they are encrypted or not. The user can also select the different data types to encrypt. This will encrypt the existing data.

Data/File Encryption Status			
<a href="#">Encrypt</a>			
<input type="checkbox"/>	Type	Security	Options
<input type="checkbox"/>	Config File	<div style="width: 100%; height: 10px; background-color: green;"></div> Strong	
<input type="checkbox"/>	IM Files	<div style="width: 100%; height: 10px; background-color: green;"></div> Strong	
<input type="checkbox"/>	IM Message	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	
<input type="checkbox"/>	Recording Files	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	
<input type="checkbox"/>	Video Recording Files	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	
<input type="checkbox"/>	Voicemail	<div style="width: 0%; height: 10px; background-color: gray;"></div> Unencrypted	

Data/File Encryption Status

The user can select the types of stored files to encrypt, then use the [Encrypt](#) button to start the encryption. Or you can encrypt the files using the following encrypting button .

To open and play encrypted audio files outside of the UCM system, users need a decryption tool (found on the [Grandstream Tools page](#)), a key file and the password for it (set when exporting the key file).

For more information on how to use the decryption tool, please refer to the following guide :

[UCM6300/A Series IP PBX – CDR Tool Guide](#)

**Note**

- In an HA environment, the Primary UCM's key will be used as the Master Key, and this will be synced with the Secondary UCM so both UCMs will use the same key to encrypt and decrypt files.
- Files on the standby machine are not automatically encrypted so users will need to manually re-encrypt all new files that were created before the failover.

**Critical**

- Downgrading from a firmware version with data encrypted to a firmware version which does not support data encryption will require the user to perform a factory reset.
- Backing up the data of the PBX before upgrading the firmware is highly recommended to avoid the possibility of data corruption/loss.

## LDAP Server

The UCM630xA 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 UCM630xA 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 UCM630xA 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 UCM630xA, 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 UCM630xA. If the UCM630xA 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 UCM630xA 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 UCM630xA.

The screenshot shows the 'LDAP Server' configuration page with two tabs: 'LDAP Server Configurations' (selected) and 'LDAP Phonebook'. The configuration fields are as follows:

Field	Value	Suffix
* Base DN:	dc=pbx,dc=com	
PBX DN:	ou=pbx	,dc=pbx,dc=com
Root DN:	cn=admin	,dc=pbx,dc=com
* Root Password:	.....	
* Confirm Root Password:	.....	
LDAP Cert:	server.crt	
LDAP Private Key:	private.key	
LDAP CA Cert:	server.ca	

Each of the three certificate fields (LDAP Cert, LDAP Private Key, and LDAP CA Cert) has a 'Reset Certificates' button to its right.

*LDAP Server Configurations*

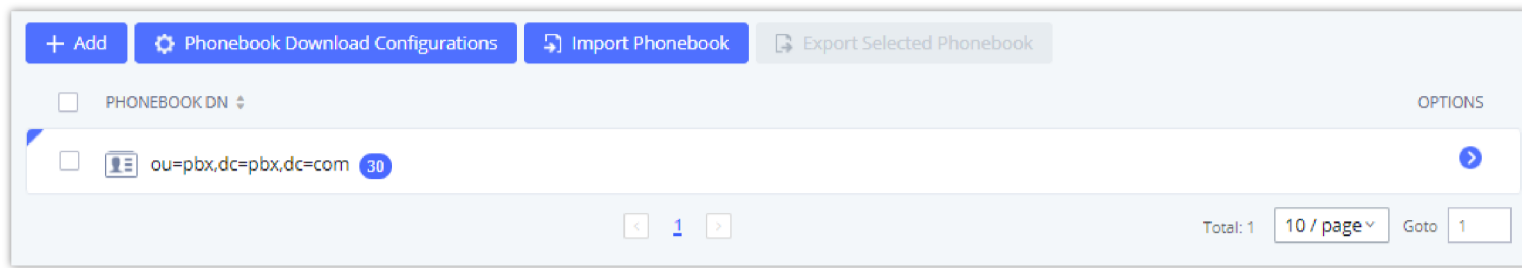
The UCM630xA LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client does not have to configure username and password to access the phonebook directory. The "Root DN" and "Root Password" here are for LDAP management and configuration where users will need provide for authentication purpose before modifying the LDAP information.

The default phonebook list in this LDAP server can be viewed and edited by clicking on

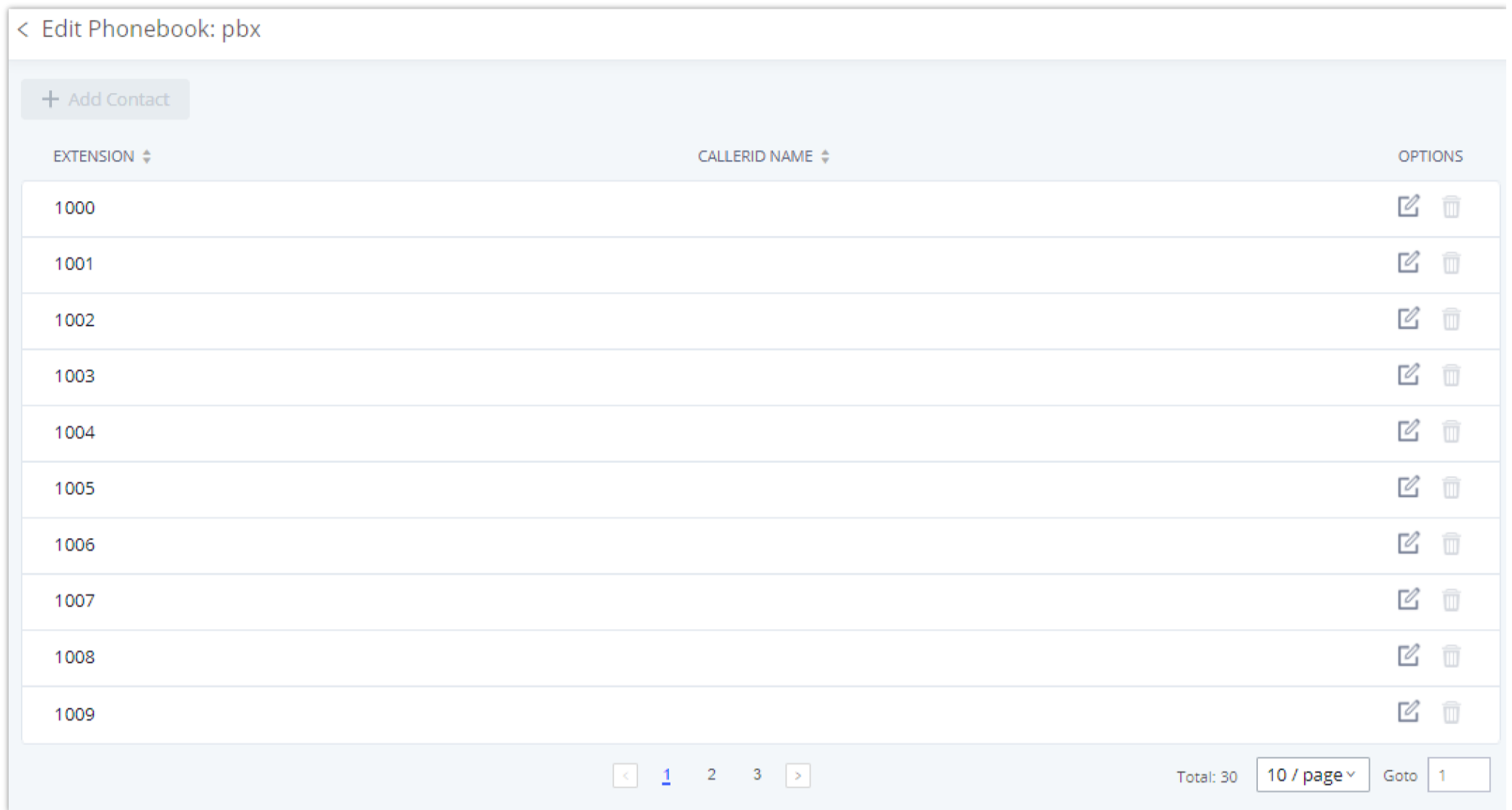


for the first phonebook under LDAP Phonebook.

The UCM630xA support secure LDAP (LDAPS) where the communication is encrypted and secure.



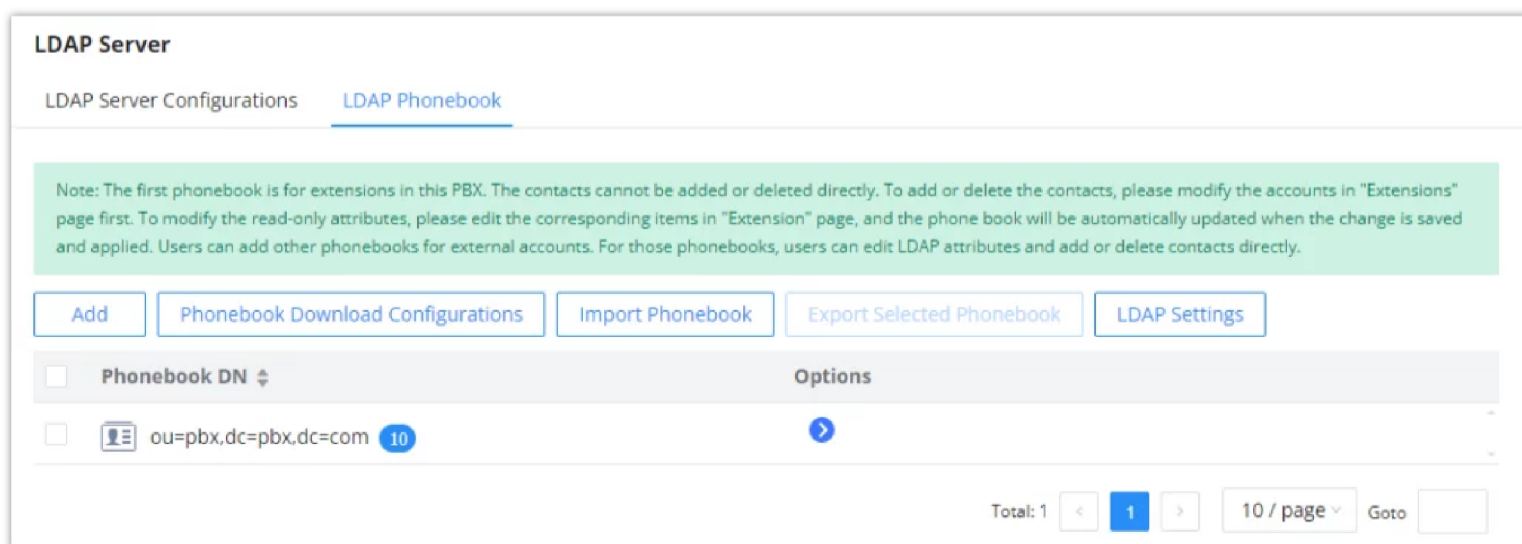
Default LDAP Phonebook DN



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.



LDAP Server → LDAP Phonebook

The user can use the search bar on the top right corner of page, please see the screenshot below.

You can enter the extension number or the name of the contact; if you are unsure about the name or the extension, the search feature supports fuzzy matching.

CallerID Name	Email	Options
Arthur Morgan	morgan.arthur@email.com	<a href="#">i</a>
Abigail Stevens		<a href="#">i</a>

LDAP Phonebook Search Bar

- o **Add new phonebook**

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

\* Phonebook Prefix:


Phonebook DN:


Cancel Save

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.

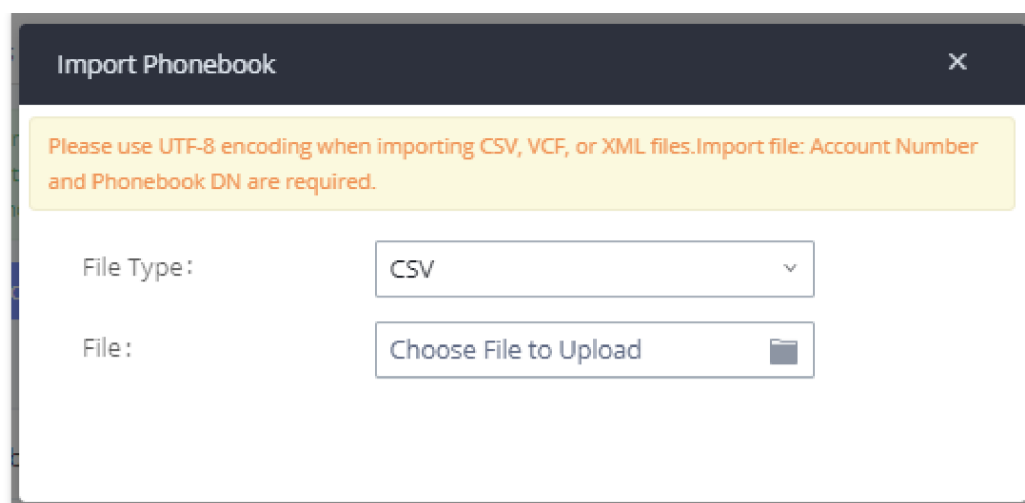
ACCOUNTNUMBER	CALLERID NAME	EMAIL	OPTIONS
062514356	Dr. Smith		<a href="#">edit</a> <a href="#">delete</a>

Total: 1 10 / page Goto 1

Edit LDAP Phonebook

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

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



Import Phonebook

The file to be imported must be a CSV, VCF 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 UCM630xA LDAP phonebook section first and use it as a sample to start with.

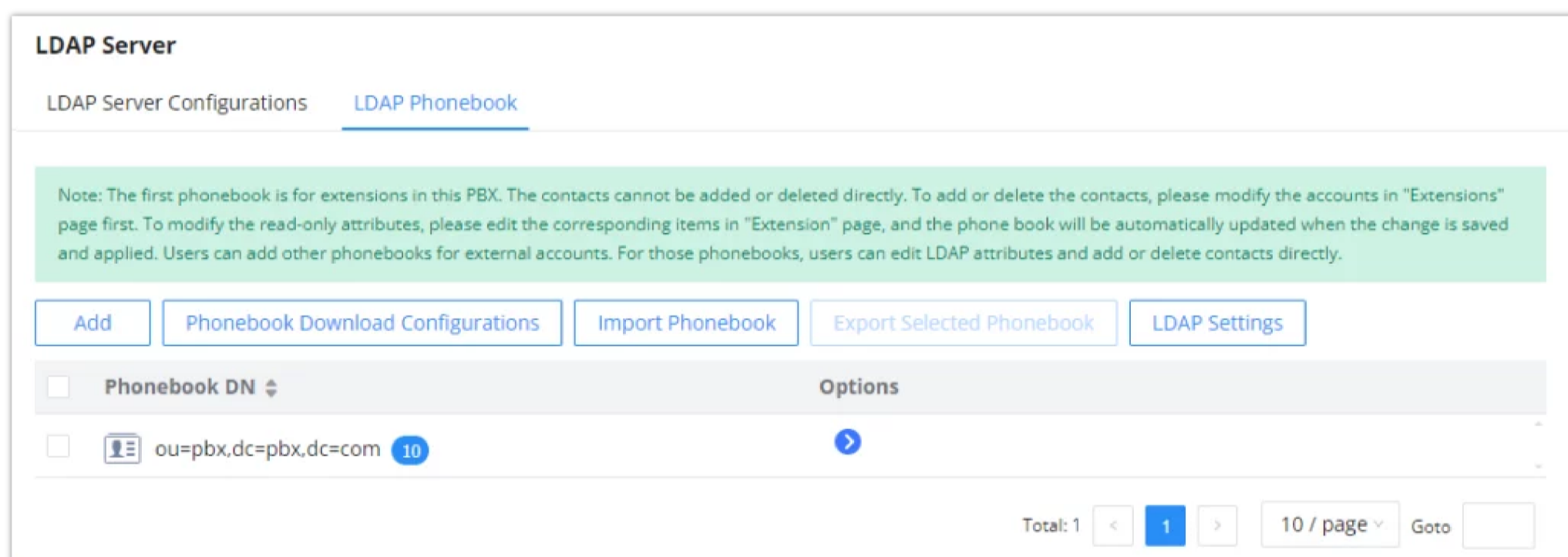
	A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	1004	1004		Accounting	1004000000			phonebook
6	Steve	Chang	1005	1005		Support	1005000000			others

Phonebook CSV File Format

The Phonebook DN field is the same "Phonebook Prefix" entry as when the user clicks on "Add" to create a new phonebook. Therefore, if the user enters "phonebook" in "Phonebook DN" field in the CSV file, the actual phonebook DN "ou=phonebook,dc=pbx,dc=com" will be automatically created by the UCM630xA 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 UCM630xA LDAP Phonebook, the contacts in the CSV file will be added into the existing phonebook. If the phonebook DN does not exist on the UCM630xA 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 UCM630xA.

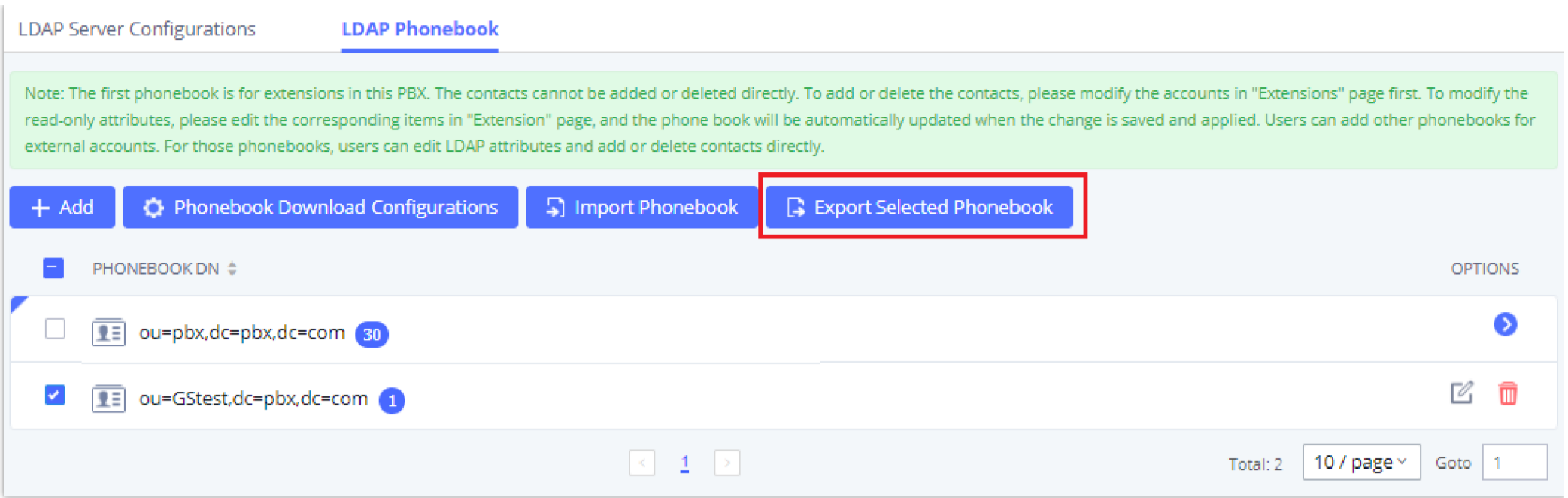


LDAP Phonebook After Import

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.

- o **Export phonebook to your computer from UCM630xA 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 UCM630xA again.



Export Selected LDAP Phonebook

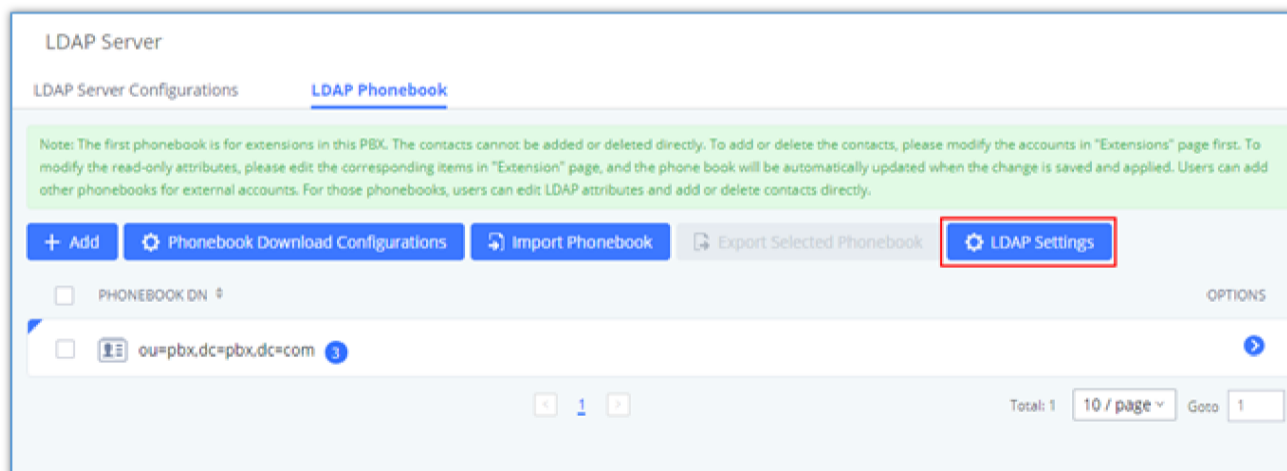
## LDAP Settings

Prerequisites to support contacts sync-up to IP Phones, UCM needs to support the following:

1. If Cloud IM is enabled, UCM can send remote UCM's contacts to each end device.
2. Contacts from remote UCM can be synced by Cloud IM or LDAP sync via trunk. The contacts data must be complete and consistent.
3. If Cloud IM is enabled, the contacts sent from UCM to end device should integrate Cloud IM contacts.
4. If Cloud IM is disabled, the contacts sent from UCM to end device should only contain contacts on the UCM.

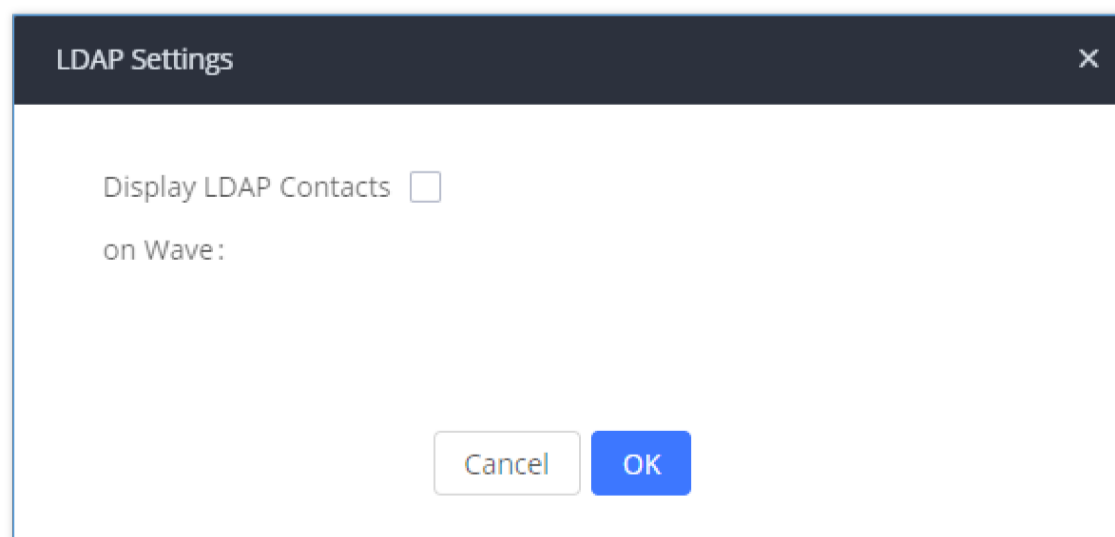
To support contacts sync-up to Wave, it allows Wave to obtain enterprise contacts from Cloud IM or LDAP. On UCM SIP peer trunk, if LDAP sync is enabled, end point can obtain remote UCM extensions' info via LDAP. Also, it will allow configuring whether to sync up LDAP contacts on Wave so that Wave doesn't receive duplicate contacts info.

Under UCM **webUI** → **System Settings** → **LDAP Server**, click on "LDAP Settings", option "Wave enable LDAP phonebook" is available for configuration. If enabled, all Wave users on this UCM will display LDAP contacts. Otherwise, it will not display.



LDAP Settings

Please note the LDAP contacts displayed on Wave will exclude the duplicate contacts from Cloud IM.



Display LDAP Contacts on Wave

## LDAP Client Configurations

The configuration on LDAP client is useful when you use other LDAP servers. Here we provide an example on how to configure the LDAP client on the UCM.

Assuming the remote server base dn is "**dc=pbx,dc=com**", configure the LDAP client as follows:

<b>Phonebook Name</b>	Enter a name for the phonebook
<b>Server Address</b>	The IP address of the LDAP server
<b>Base DN</b>	Enter the base domain name.
<b>Username</b>	Enter the username used to authenticate into the LDAP server, if authentication is required.
<b>Password</b>	Enter the password used to authenticate into the LDAP server, if authentication is required.
<b>Filter</b>	Enter the filter. Ex: ((CallerIDName=%)(AccountNumber=%))
<b>Port</b>	Enter the port number. Default port is 389
<b>LDAP Number Attributes</b>	Enter the number attributes for the remote server.
<b>Automatic Update Cycle</b>	If "None" is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
<b>LDAP Name Attributes</b>	Enter the name attributes for the remote server.
<b>Client Type</b>	Choose the client type. For encrypted data transfer please choose LDAPS.
<b>LDAP Client CA Cert</b>	LDAP Client Public Certification
<b>LDAP Client Private Key</b>	LDAP Client Private Certification

The UCM can automatically update the phonebook, by configuring the 'LDAP Automatic Update Cycle'. Available options are: 1 day/2days/7 days. It is set to 'None' by default.

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

Phonebook Download Configurations
Cancel Save

<p>* LDAP Server: <input type="text" value="LdapClient"/></p> <p>* Base DN: <input type="text" value="dc=pbx,dc=com"/></p> <p>* Password: <input type="password" value="*****"/></p> <p>* Port: <input type="text" value="389"/></p> <p>Client Type: <input type="text" value="LDAP"/></p> <p>LDAP Automatic Update Cycle: <input type="text" value="None"/></p> <p>LDAP Client CA Cert: <input type="text" value="client.ca"/> <input type="button" value="Reset Certificates"/></p> <p>LDAP Client Private Key: <input type="text" value="client.key"/> <input type="button" value="Reset Certificates"/></p>	<p>* Server Address: <input type="text" value="192.168.0.240"/></p> <p>* Username: <input type="text" value="cn=admin,dc=pbx,dc=com"/></p> <p>* Filter: <input type="text" value="(CallerIDName=%)"/></p> <p>LDAP Name Attributes: <input type="text" value="CallerIDName FirstName LastName"/></p> <p>* LDAP Number Attributes: <input type="text" value="MobileNumber HomeNumber AccountNumber"/></p>
---	---

To configure Grandstream IP phones as the LDAP clients for UCM, please refer to the following example:

- o **Server Address:** The IP address or domain name of the UCM
- o **Base DN:** dc=pbx,dc=com
- o **Username:** Please leave this field empty
- o **Password:** Please leave this field empty
- o **LDAP Name Attribute:** CallerIDName Email Department FirstName LastName
- o **LDAP Number Attribute:** AccountNumber MobileNumber HomeNumber Fax
- o **LDAP Number Filter:** (AccountNumber=%)
- o **LDAP Name Filter:** (CallerIDName=%)
- o **LDAP Display Name:** AccountNumber CallerIDName
- o **LDAP Version:** If existed, please select LDAP Version 3
- o **Port:** 389

The following figure shows the configuration information on a Grandstream GXP2170 to successfully use the LDAP server as configured in **[Figure: LDAP Server Configurations]**.

### LDAP

LDAP protocol	<input type="text" value="LDAP"/>
Server Address	<input type="text" value="192.168.40.134"/>
Port	<input type="text" value="389"/>
Base	<input type="text" value="dc=pbx,dc=com"/>
User Name	<input type="text"/>
Password	<input type="password"/>
LDAP Number Filter	<input type="text" value="(AccountNumber=%)"/>
LDAP Name Filter	<input type="text" value="(CallerIDName=%)"/>
LDAP Version	<input type="radio"/> Version 2 <input checked="" type="radio"/> Version 3
LDAP Name Attributes	<input type="text" value="CallerIDName"/>
LDAP Number Attributes	<input type="text" value="AccountNumber"/>
LDAP Display Name	<input type="text" value="AccountNumber CallerIDName"/>
Max. Hits	<input type="text" value="50"/>
Search Timeout	<input type="text" value="30"/>
Sort Results	<input checked="" type="radio"/> No <input type="radio"/> Yes
LDAP Lookup	<input checked="" type="checkbox"/> Incoming Calls <input checked="" type="checkbox"/> Outgoing Calls
Lookup Display Name	<input type="text"/>

*GXP2170 LDAP Phonebook Configuration*

**AD Client Type**

<b>Phonebook Name</b>	Enter a name for the phonebook
<b>Server Address</b>	The IP address of the AD server

<b>Base DN</b>	Enter the base domain name.
<b>Username</b>	Enter the username used to authenticate into the LDAP server, if authentication is required.
<b>Password</b>	Enter the password used to authenticate into the LDAP server, if authentication is required.
<b>Filter</b>	Enter the filter. Ex: ((CallerIDName=%)(AccountNumber=%))
<b>Port</b>	Enter the port number. Default port is 389
<b>AD Attributes</b>	AccountNumber must be included if the default configuration is used.
<b>Automatic Update Cycle</b>	If "None" is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
<b>Host Name</b>	Enter the host name of the remote AD server.

## Time Settings

### Automatic Date and Time

The current system time on the UCM630xA can be found under Web GUI→**System Status**→**Dashboard**→**PBX Status**.

To configure the UCM630xA to update time automatically, go to Web GUI→**System Settings**→**Time Settings**→**Automatic date and Time**.

**i** 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 UCM630xA for the first time to avoid service interrupt after installation and deployment in production.

<b>Time Zone</b>	Select your timezone. To update your list of timezones, please click on " <b>Update Time Zone List</b> ". <b>Note:</b> Updating the time zone list requires rebooting the UCM.
------------------	--

Remote NTP Server

Enable DHCP Option 2

Enable DHCP Option 42

\* Time Zone

*Automatic Date and Time Settings*

### Set Date and Time

To manually set the time on the UCM630xA, go to Web GUI→**System Settings**→**Time Settings**→**Set Date and Time**. The format is YYYY-MM-DD HH:MM:SS.

### Time Settings

Automatic Date and Time    **Set Date and Time**    NTP Server    Office Time    Holiday

Cancel    Save

---

Current Date and Time:       

Date Format:   

Time Format:   

*Set Time Manually*

**i** Manually setup time will take effect immediately after saving and applying change in the Web GUI. If users would like to reboot the UCM630xA 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 UCM630xA can be used as an NTP server for the NTP clients to synchronize their time with. To configure the UCM630xA 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 UCM630xA IP address or host name to use the UCM630xA as the NTP server.

### Office Time

On the UCM630xA, 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.

*Create New Office Time*

<b>Start Time</b>	Configure the start time for office hour.
<b>End Time</b>	Configure the end time for office hour
<b>Week</b>	Select the workdays in one week.
<b>Show Advanced Options</b>	Check this option to show advanced options. Once selected, please specify "Month" and "Day" below.

<b>Month</b>	Select the months for office time.
<b>Day</b>	Select the workdays in one month.

*Create New Office Time*

Select "Start Time", "End Time" and the day for the "Week" for the office time. The system administrator can also define month and day of the month as advanced options. Once done, click on "Save" and then "Apply Change" for the office time to take effect. The office time will be listed in the web page as the figure shows below.



**Time Settings**

Automatic Date and Time    Set Date and Time    NTP Server    **Office Time**    Holiday

[+ Add](#)
[Delete](#)

	INDEX	TIME	WEEK	MONTH	DAY	OPTIONS
<input type="checkbox"/>	1	09:00-18:00	Mon Tue Wed Thu Fri	Default	Default	<a href="#">✎</a> <a href="#">🗑</a>

*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 UCM630xA, 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.

## Create New Holiday

\* Name:

Holiday Memo:

Year:

Month: 

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sept	Oct	Nov	Dec

Day: 

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Show Advanced

Options:

Week: 

Sun	Mon	Tue	Wed
Thu	Fri	Sat	

Time:  -

Create New Holiday

<b>Name</b>	Specify the holiday name to identify this holiday.
<b>Holiday Memo</b>	Create a note for the holiday.
<b>Month</b>	Select the month for the holiday.
<b>Year</b>	Select the Year for the holiday. <b>Note:</b> In the "Year" option, select "All" to set annual fixed holiday information.
<b>Day</b>	Select the day for the holiday.
<b>Show Advanced Options</b>	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
<b>Week</b>	Select the days as holiday in one week.
<b>Time</b>	Select the time on which the holiday starts.

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.

Time Settings



Automatic Date and Time    Set Date and Time    NTP Server    Office Time    **Holiday**

[+ Add](#)   [Delete](#)   [Import](#)   [Export](#)

<input type="checkbox"/>	NAME	WEEK	YEAR	MONTH	DAY	TIME	HOLIDAY MEMO	OPTIONS
<input type="checkbox"/>	Custom	Sun Sat	2022	Mar	21,22	00:00-23:59	Enjoy your holiday	<a href="#">Edit</a> <a href="#">Delete</a>

Total: 1    10 / page

*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.

## Custom Time Groups

Users can create custom time frames which can be used as a routing condition in the inbound routes. Multiple time ranges can be added and the frequency can be customized to be every specific weekday or every specific day/week of the selected months.

**Note:**

Users can also export and import these custom time groups in CSV format for easier management.

To access Custom Time Groups, please navigate to **System Settings > Time Settings > Custom Time Groups**

Time Settings > Create New Custom Time Groups

\* Name


Description

**Time Groups**

Time  -

Frequency  By Week  By Month

Sun	Mon	Tue	Wed
Thu	Fri	Sat	

Time	Week	Month	Day	Options
				

Custom Time Groups

Parameter	Description
<b>Name</b>	Enter the name of the time group.
<b>Description</b>	Enter the description of the time group.
<b>Time Groups</b>	
<b>Time</b>	Select the time period for this group.
<b>Frequency</b>	Select the frequency of this group per week/month.

**Email Settings**

**Email Settings**

The Email application on the UCM630xA can be used to send out alert event Emails, Voicemail (Voicemail-To-Email) etc. The configuration parameters can be accessed via **System Settings > Email Settings > Email Settings**.

Parameter	Description
-----------	-------------

<b>Mail Server Providers</b>	<p>Select the mail server provider type.</p> <ul style="list-style-type: none"> <li>● <b>Common:</b> Select this option when integrating email service such as Gmail and on-premise email servers.</li> <li>● <b>Microsoft:</b> Select this option when integrating email service provided by Microsoft Outlook.</li> </ul> <p><b>Note:</b> The settings below appear when selecting "Common".</p>
<b>TLS Enable</b>	If enabled, TLS will be used when forwarding emails to the SMTP server.
<b>Type</b>	<ul style="list-style-type: none"> <li>● <b>MTA:</b> Mail Transfer Agent. The configured domain will be used in the sender address. Warning: Emails sent by MTA may be considered spam by the destination SMTP server.</li> <li>● <b>Client:</b> Send emails to the configured SMTP server, which will then forward the emails to the destination address.</li> </ul>
<b>Email Template Sending Format</b>	Select the email template format to be sent. The "HTML" format is compatible with most mail clients and is recommended. If the mail client does not support the "HTML" format, please select the "Plain Text" format.
<b>SMTP Server</b>	<p>Enter the SMTP server.</p> <p>For example, smtp.mydomain.com:587. Port number is optional.</p>
<b>Enable SASL Authentication</b>	Toggles SASL authentication. If disabled, IPPBX will not use the username and password for email client authentication. Most email servers require login authentication while private email servers may allow anonymous login. If using Microsoft Exchange Server or if credentials are not required, please disable this option.
<b>Username</b>	Enter the username of the email account.
<b>Password</b>	Enter the password of the email account. It is highly recommended to use HTTPS when saving and applying password changes.
<b>Enable Email-to-Fax</b>	Monitors the inbox of the configured email address for the specified subject. If detected, the IPPBX will get a copy of the attachment from the email and send it to the XXX extension by fax. The attachment must be in PDF/TIF/TIFF format.
<b>Email-to-Fax Blocklist/Allowlist</b>	The user can enable the Email-to-Fax Blacklist or Email-to-Fax Whitelist.
<b>Email-to-Fax Subject Format</b>	Select the email subject format to use for emails to fax. XXX refers to the extension that the fax will be sent to. This extension can only contain numbers.
<b>Fax Sending Success/Failure Confirmation</b>	If enabled, the UCM will send an email notification to the sender about the fax sending result.
<b>Internal Block/Allowlist</b>	<p>Email address blacklist/whitelist for local extensions.</p> <p>This option is displayed after enabling <b>Email-to-Fax Blocklist/Allowlist</b>.</p>
<b>External Blocklist/Allowlist</b>	<p>Email address blacklist/whitelist for non-local contacts. Separate multiple addresses with semicolon (;) (i.e. "xxx;yyy").</p> <p>This option is displayed after enabling <b>Email-to-Fax Blocklist/Allowlist</b>.</p>
<b>POP/POP3 Server Address</b>	Enter the IP address of the POP/POP3 server.
<b>POP/POP3 Server Port</b>	Enter the port of the POP/POP3 server.
<b>Display Name</b>	Enter the name of the PBX that will be displayed in sent emails.
<b>Sender</b>	Enter the email used to send the emails.

<b>Email Settings</b>	Use "Test" button to test if the email integration is working correctly. <b>Note:</b> Before running the test, please save the configuration first by clicking on "Save" then "Apply Changes".
Parameter	Description
<b>Mail Server Providers</b>	Select the mail server provider type.  <ul style="list-style-type: none"> <li>• <b>Common:</b> Select this option when integrating email service such as Gmail and on-premise email servers.</li> <li>• <b>Microsoft:</b> Select this option when integrating email service provided by Microsoft Outlook.</li> </ul> <b>Note:</b> The settings below appear when selecting "Microsoft".
Server Authorization	
<b>Redirect URIs</b>	Enter a redirect URI which will receive the OAuth2 token. Make sure that the URI is secure and is accessible.
<b>Tenant ID</b>	Enter the ID of the tenant of the directory in Microsoft Entra
<b>Username</b>	Enter Microsoft Entra login username.
<b>Application (Client) ID</b>	Enter the ID of the application created on Microsoft Entra
<b>Client Password</b>	Enter the client secret of the application created on Microsoft Entra.
Email Delivery Settings	
<b>Email Template Sending Format</b>	Select the email template format to be sent. The "HTML" format is compatible with most mail clients and is recommended. If the mail client does not support the "HTML" format, please select the "Plain Text" format.
<b>Display Name</b>	Enter the name of the PBX that will be displayed in sent emails.
<b>Email Settings</b>	Use "Test" button to test if the email integration is working correctly. <b>Note:</b> Before running the test, please save the configuration first by clicking on "Save" then "Apply Changes".

The following figure shows a sample Email setting on the UCM630xA.

**Email Settings**

[Email Settings](#)   [Email Template](#)   [Email Footer Hyperlink](#)   [Email Send Log](#)

---

Mail Server Providers:

TLS Enable:

Type:

Email Template Sending Format:

\* Mail Server Domain:

\* SMTP Server:

Enable SASL Authentication:

\* Username:

ⓘ The email server must allow 3rd party email clients to use the SMTP service.

\* Password:

Enable Email-to-Fax:

Email-to-Fax Blocklist/Allowlist:

Email-to-Fax Subject Format:

Fax Sending Success/Failure Confirmation:

UCM630xA 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 UCM630xA.

The Email templates on the UCM630xA can be used for email notification, the configuration parameters can be accessed via Web GUI→**Settings**→**Email Settings**→**Email Templates**.

## Email Templates

Users can customize email templates for password reset, voicemail, meeting scheduling, extensions, fax, meeting report, PMS, CDR, emergency call, missed calls, alert events, call queue statistics and etc.

- Click on



icon to edit the template.

Email Settings				
TYPE	NAME	TIME	OPTIONS	
Multimedia Meeting Schedule	mcm_template.html	2022-04-19 17:29:59 UTC+01:00		
SLA Alert	callqueuesla_template.html	2022-03-31 13:07:37 UTC+01:00		
Wave Welcome	welcome_template.html	2022-03-31 13:07:37 UTC+01:00		
Remote Registration	register_template.html	2022-03-31 13:07:37 UTC+01:00		
Extension	account_template.html	2022-03-31 13:07:37 UTC+01:00		
CDR	cdr_template.html	2011-12-03 11:30:03 UTC+01:00		
Fax	fax_template.html	2011-12-03 11:30:03 UTC+01:00		
Missed Calls	missedcall_template.html	2011-12-03 11:30:03 UTC+01:00		
Voicemail	voicemail_template.html	2011-12-03 11:30:03 UTC+01:00		
Call Queue Statistics	callqueuestatistics_template.html	2011-12-03 11:30:03 UTC+01:00		
Fax Sending	sendfax_template.html	2011-12-03 11:30:03 UTC+01:00		
Emergency Calls	emergency_template.html	2011-12-03 11:30:03 UTC+01:00		
Meeting Report	conferencereport_template.html	2011-12-03 11:30:03 UTC+01:00		

Email Template

## Email Footer Hyperlink

Under UCM Web GUI → System Settings → Email Settings → Email Footer Hyperlink, users could edit the text and URL to modify the email footer hyperlink.

Email Footer Hyperlink

## Email Send Log

Under UCM Web GUI → System Settings → Email Settings → Email Send Log, users could search, filter and check whether the Email is sent out successfully or not. This page will also display the corresponding error message if the Email is not sent out successfully.

Email Send Log

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 them with comma and no spaces.

Field	Description
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: <ul style="list-style-type: none"> <li>○ All Modules</li> <li>○ Extension</li> <li>○ Voicemail</li> <li>○ Meeting Schedule</li> <li>○ User Password</li> <li>○ Alert Events</li> <li>○ CDR</li> <li>○ Test</li> </ul>

*Email Log – Display Filter*

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	<a href="#">i</a>
2020-12-21 18:00:04	Video Conference Schedule	m.g@gmail.com	12-21 18:00:06	m.g@gmail.com	sent	250	<a href="#">i</a>
2020-12-20 18:00:04	Video Conference Schedule	m.g@gmail.com	12-20 18:00:07	m.g@gmail.com	sent	250	<a href="#">i</a>
2020-12-19 18:00:03	Video Conference Schedule	m.g@gmail.com	12-19 18:00:06	m.g@gmail.com	sent	250	<a href="#">i</a>
2020-12-18 18:00:03	Video Conference Schedule	m.g@gmail.com	12-18 18:00:06	m.g@gmail.com	sent	250	<a href="#">i</a>
2020-12-17 18:00:03	Video Conference Schedule	m.g@gmail.com	12-17 18:00:06	m.g@gmail.com	sent	250	<a href="#">i</a>

Total: 32    10 / page    Goto 1

*Email Logs*

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

Code	Description
<b>250</b>	Mail sent successfully
<b>501</b>	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.
<b>535</b>	The user name and password verification in the client mode is incorrect. Please check whether the user name and password are configured correctly.
<b>550</b>	<p>Possible reasons:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>
<b>552</b>	The sent email is too large or the email attachment type is prohibited
<b>553</b>	The sender and the email account are inconsistent, please configure the sender as your email account correctly.
<b>554</b>	The email was identified as spam. Please reduce the sending frequency or try again the next day

Code	Description
	Indicates that there is no return code.
<b>none</b>	<p>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.</p> <p>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".</p>

Email Codes

## SMS Settings

### SMS Configuration

Configuring the SMS feature on the UCM6300 series allows the administrators to enable two-factor authentication and to send alerts and meeting notices.

**SMS Settings > SMS Settings**

[SMS Settings](#)    SMS Template    SMS Delivery Log

Enable SMS

\* SMS Carrier

Region

\* Account ID

\* Secret

\* From

SMS Settings

<b>Enable SMS</b>	Tick this box to enable SMS service.
<b>SMS Carrier</b>	Choose the SMS carrier: <ul style="list-style-type: none"> <li>● Amazon</li> <li>● Twilio</li> </ul>
<b>Region</b>	Choose the region.
<b>Account ID</b>	Enter the ID of the account created at the carrier.
<b>Secret</b>	Enter the secret code.
<b>Account ID</b>	Configures Twilio account ID.

<b>Auth Token</b>	The key of the Twilio account.
<b>Messages Server ID</b>	Twilio SMS Server ID
<b>From</b>	Enter the number phone allocated for the UCM.

## SMS Template

The template of the SMS can be modified in "SMS Template" tab. Please note that carriers may require to pre-register the templates for SMS that the UCM will send. Refer to the [Amazon](#) and [Twilio](#) documentation for more information.

**SMS Settings > SMS Settings**

SMS Settings    SMS Template    SMS Delivery Log

SMS templates are subject to carrier specifications, and carriers may require senders to pre-register templates for each type of message they plan to send. Please refer to the operator's requirements for details. More details can be found here: [Amazon](#), [Twilio](#)

TYPE	TEMPLATE CONTENT	OPTIONS
Verification Code	[UCM] Your verification code is <span style="color: orange;">\${code}</span> . It will expire in 10 minutes.	
Alarm Notification	[UCM] <span style="color: orange;">\${hostName}(\${macAddr})</span> system event: <span style="color: orange;">\${content}</span>	

© 2023 Grandstream Networks, Inc.

*SMS Template*

## SMS Delivery Log

All the SMS messages sent will be logged in the following tab.

**SMS Settings**

SMS Settings    SMS Template    SMS Delivery Log

Show All Logs    Clear    Delete Search Result(s)    Display Filter ▾

SEND RESULT ▾	RECIPIENT ▾	SMS CATEGORY ▾	SEND TIME ▾
No data			

© 2023 Grandstream Networks, Inc.

SMS Delivery Log

## HA

Dual-system hot standby provides a highly reliable and fault-tolerant solution for enterprises using the UCM6300 series/UCM6300A series. Based on two UCM devices of the same product model and software version, one of them is in the "Active" working state in real-time, and the other is in the "Standby" working state. The daily data on the host server will be synchronized to the standby machine in real-time, and the standby machine always monitors the running status of the host. When the host fails, including hardware failures and severe software failures, the standby machine will immediately take over the business and enter the "Active" working state, and Upgrade to a host to ensure that the business is not interrupted, and the call will automatically resume.

The HA function provides two modes of operating. The first mode of function is **Local Hot Standby**, which offers a deployment that switches dynamically when the primary UCM encounters an issue. The second mode is **Remote Disaster Recover**, it offers deploying a back up UCM remotely, this offers an architecture that would not be affected by any disaster that might occur on the geolocation of the primary UCM.

### Important Note

In order to set HA, both UCMs should have static IP addresses.

## HA settings

The users can configure the HA under **System Settings** → **HA settings** page.

When setting up an HA dual-system, please keep the models and versions of the two devices forming the HA consistent, otherwise database compatibility problems may occur.  
 If you need to connect an external USB device, it is recommended to use USB3.0 for both computers. Please ensure that the specifications are consistent, otherwise it will cause an exception.  
 When enabling HA IPv6 support, it is highly recommended to reboot both UCMs at the same time after completing the HA configuration.

High Available Enable

HA Mode  Local Hot Standby <sup>?</sup>  Remote Disaster Recovery <sup>?</sup>

Force Switch

\* Hot Standby Station Type

\* Hot Standby Cluster IP

\* Hot Standby Peer IP

\* Hot Standby Peer MAC Address

\* Heartbeat Port

\* Heartbeat Timeout Period (s)

Software Fault Switch

Hardware Fault Switch  FXO1

Enable IPv6

Scan External Storage Files

Get more information about HA Settings at [HA User Guide](#)

HA Settings

Parameter	Description
<b>Force Switch</b>	Enables/disables the HA functionality. By default, is Disabled.
<b>Force Switch</b>	Clicking the button will immediately force a switchover to the standby UCM.
<b>Hot Standby Station Type</b>	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the initial active device. If set to Secondary, the peer UCM system will be assigned as the initial standby device. The roles of the UCM systems may change as HA switchovers occur.
<b>Hot Standby Cluster IP</b>	To use this service, the active and standby UCM systems need to use the same static IP address.
<b>Hot Standby Peer IP</b>	Local IP address of Hot Standby peer device.
<b>Hot Standby Peer MAC Address</b>	The MAC address of Hot Standby peer device.
<b>Heartbeat Port</b>	The number of the heartbeat port should be consistent with the peer heartbeat port.
<b>Heartbeat Timeout Period (s)</b>	Upon timeout, the Standby UCM will take over services.

<b>Software Fault Switch</b>	Enable Software Fault Switch
<b>Hardware Fault Switch</b>	If issues are detected with the selected connection interfaces, the backup UCM6510 will take over services after the master/slave handover. If not checked, UCM will send only a fault alarm.
<b>Enable IPv6</b>	If enabled, HA on UCM can be used with IPv6 while compatible with IPv4.
<b>Scan External Storage Files</b>	<p>Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page.</p> <p>It is recommended to configure external storage data synchronization when forming HA for the first time, If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.</p>

*Local Hot Standby*

Parameter	Description
<b>Network Port Domain Name</b>	<ul style="list-style-type: none"> <li>● WAN</li> <li>● LAN</li> </ul>
<b>Force Switch</b>	Clicking the button will immediately force a switchover to the standby UCM.
<b>Remote Disaster Recovery Station Type</b>	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the initial active device. If set to Secondary, the peer UCM system will be assigned as the initial standby device. The roles of the UCM systems may change as HA switchovers occur.
<b>Remote Disaster Recovery Peer MAC Address</b>	The MAC address of Remote Disaster Recovery peer device
<b>Heartbeat Port</b>	The heartbeat port should be the same as the peer device's heartbeat port.
<b>Heartbeat Timeout Period (s)</b>	Upon timeout, the Standby UCM will take over services.
<b>Local Heartbeat IP</b>	Fill in the IP address of the heartbeat port of the local site, in the format: xxx.xxx.xxx.xxx, which is used for the peer end to detect the local machine status, heartbeat negotiation, and communication address for data synchronization.
<b>Local Heartbeat Gateway IP</b>	Fill in the IP address of the local heartbeat gateway for remote disaster recovery, in the format: xxx.xxx.xxx.xxx
<b>Local Heartbeat Address Subnet Mask</b>	Fill in the subnet mask of the heartbeat address of the remote disaster recovery local end, in the format: xxx.xxx.xxx.xxx, such as: 255.255.255.0.
<b>Peer Heartbeat IP</b>	Fill in the IP address of the heartbeat port of the peer site, in the format: xxx.xxx.xxx.xxx, which is used to detect peer status, heartbeat negotiation, and communication address for data synchronization.
<b>Scan External Storage Files</b>	<p>Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page.</p> <p>It is recommended to configure external storage data synchronization when forming HA for the first time, If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.</p>

## HA Status

Once the HA is configured, the user can view its status under **System Settings → HA → HA Status** as shown below

HA	
HA Settings	HA Status
HA Mode	Local Hot Standby
Hot Standby Status	Dual
Hot Standby Full Backup Status	No backup
MAC Address of Current UCM	C0:74:AD:7D:B3:7A
Role of Current UCM	Active
GDMS HA Abnormal Status	No Primary UCM has been added to GDMS

HA Status

## HA Log

The user can view the HA log through the **system settings → HA → HA log** page. The HA log effectively records the execution results of past full backup actions, as well as the historical records that triggered the active/standby switchover.

### Note

The UCM63xx series supports SNMP to be able to use 3rd party monitoring tools to monitor both UCMs in HA setup.

## SNMP

UCM63xx supports SNMP in case the system administrator chooses to use third party monitoring tools. These are the options available when setting up SNMP.

## SNMP Settings

SNMP
Cancel Save

SNMP Settings
SNMP Community
SNMP Trap Destinations
SNMP V3 Users
SNMP Trap Proxy

SNMP service uses port 161 by default. Please make sure port 161 is not occupied before enabling SNMP.

Enable:

Device Name:

Device Location:

Contact Email Address:

Enable SNMP Trap Proxy:

SNMP Trap Proxy Listening Port:

SNMP Settings

**Enable**

Tick this box to enable SNMP.

<b>Device Name</b>	Enter the device name.
<b>Location</b>	Enter the location.
<b>Contact Email Address</b>	Enter the email address used to send the SNMP alerts to.
<b>Enable SNMP Trap Proxy</b>	Tick this box to enable a proxy for SNMP Trap.
<b>SNMP Trap Proxy Listening Port</b>	The port number on which the SNMP Trap Proxy is listening on.

## SNMP Community

You can also create SNMP communities and affect a certain level of access. An SNMP community is a group created to aggregate many management stations. The community name is used to authenticate and identify these machines in the NMS (Network Management System).

*SNMP Community*

<b>Name</b>	Enter a name for the community
<b>Access Level</b>	<p>Select an access level:</p> <ul style="list-style-type: none"> <li>• <b>Read Only:</b> The SNMP community will be able only to read SNMP messages.</li> </ul>

## SNMP Trap Destinations

SNMP Traps is a very useful feature when there are many network components to manage. Instead of sending requests to all the machines in the network in order to view their SNMP logs risking slowing down or bringing the network to a complete halt, SNMP Traps can be configured so these machines can send unrequested messages to the manager to notify it about critical events and general failures.

*SNMP Trap Destinations*

<b>Name</b>	Enter a name of your SNMP Trap destination.
<b>IP Address</b>	Enter the SNMP Trap destination's IP address.

<b>Port</b>	Enter the port of the SNMP Trap destination.
<b>Community</b>	Select the community that you want
<b>Type</b>	<p>Select the type of SNMP:</p> <ul style="list-style-type: none"> <li>• <b>Trapsink:</b> Select this option if you want to send SNMP v1 traps.</li> <li>• <b>Trap2sink:</b> Select this option if you want to send SNMP v2 traps.</li> <li>• <b>Informsink:</b> Select this option if you want to send "Inform" notifications only.</li> </ul>

### SNMP Version 3

UCM 63xx also supports SNMP v3 in case the system administrator decides to add more security to the monitoring process. SNMP v3 is a very good solution to monitor devices that interface directly with Internet. SNMP v3 offers more security than its predecessors by hashing the authentication information, encrypting the SNMP messages exchanged between the managed devices and the network management system which prevent eavesdropping. Also, it prevents any data tampering which protects the integrity of the data exchanged.

SNMP v3

<b>Name</b>	Set the user's name
<b>Authentication Protocol</b>	<p>Select the authentication protocol:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul>
<b>Authentication Password</b>	Set the authentication password.
<b>Privacy Protocol</b>	<p>Select the protocol to use to encrypt the data</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES-128</li> <li>• AES-192</li> <li>• AES-256</li> </ul>
<b>Privacy Password</b>	Set the privacy password.
<b>Group Level</b>	<p>Set the group level:</p> <ul style="list-style-type: none"> <li>• Read Only.</li> <li>• Read/Write.</li> </ul>

## SNMP Trap Proxy

Create New SNMP Trap Proxy
Cancel Save

\* Name:

\* IP Address:

\* Port:

SNMP Trap Proxy

<b>Name</b>	Enter a name for the proxy server.
<b>IP Address</b>	Enter the proxy server's IP address.
<b>Port</b>	Enter the proxy server's port.

## RADIUS

The UCM6300 offers Radius-based authentication for the super administrator and other administrators. This requires configuring a Radius server then enabling Radius client on the UCM6300 which can be found under **System Settings** → **RADIUS**

### Radius

Supports configuring two types of account privileges on the Radius server: Super Administrator and Administrator.

Enable Radius Web Access Control

As Default Login Method

\* Radius Auth Server Address

\* Radius Auth Server Port

\* Radius Shared Secret

\* Maximum Number of Retransmission

\* Radius Timeout (s)

RADIUS

<b>Enable Radius Web Access Control</b>	Enable or disable Radius.
<b>As Default Login Method</b>	Enable Radius as the default login method to the web UI of the UCM
<b>Radius Auth Server Address</b>	Enter the IP address/hostname of Radius server.
<b>Radius Auth Server Port</b>	Enter the port of radius server Default port number is: 1812

<b>Radius Shared Secret</b>	Enter Radius Shared Secret
<b>Maximum Number of Retransmission</b>	Enter the number of retransmissions. The interval is 1 to 5.
<b>Radius Timeout (s)</b>	The maximum seconds before a session expires if there is no response from the server. The interval is between 1 to 30 seconds.

## TR-069

To configure TR-069 on Grandstream devices, set following parameters:

Parameter	Description
<b>Enable TR-069</b>	Toggle it on to enable TR-069. It is enabled by default
<b>ACS URL</b>	URL for TR-069 Auto Configuration Servers (ACS), e.g., <a href="http://myacs.grandstream.com">http://myacs.grandstream.com</a>
<b>TR-069 Username</b>	ACS username for TR-069 must be the same as in the ACS configuration.
<b>TR-069 Password</b>	ACS password for TR-069 must be the same as in the ACS configuration.
<b>Verify ACS Server</b>	Enables verification of the server certificate when interacting with GDMS. For security purposes, it is recommended to enable this option. However, verification is not needed for self-signed certifications.
<b>Enable Periodic Inform</b>	If enabled, <i>Inform messages</i> will be sent periodically based on the <b>Inform Interval</b> value.
<b>Enable Periodic Inform</b>	Enables periodic inform. If set to Yes, the device will send inform packets to the ACS.
<b>Inform Interval (s)</b>	A periodic time when PBX will send inform packets to TR-069 ACS server This option is specified in seconds. The default value is 86400.
<b>ACS Connection Request Username</b>	The username for the ACS to connect to PBX.
<b>ACS Connection Request Password</b>	The password for the ACS to connect to the PBX.
<b>ACS Connection Request Port</b>	Port for incoming connection requests. The default value is 7547.
<b>CPE Cert File</b>	The Cert file for PBX to connect to the ACS via SSL.
<b>CPE Cert Key</b>	The Cert key for PBX 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 UCM630xA 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 UCM630xA. The settings for this feature can be accessed via Web GUI > **Device Management** > **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.

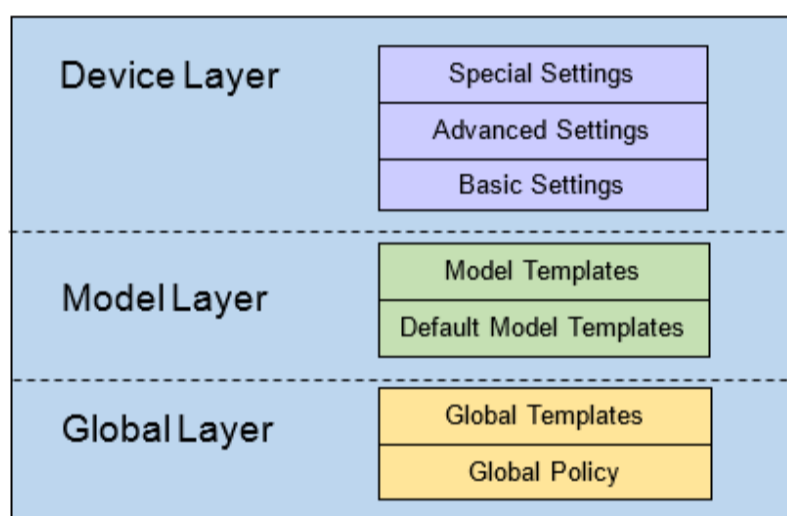
- **Model**

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]**.



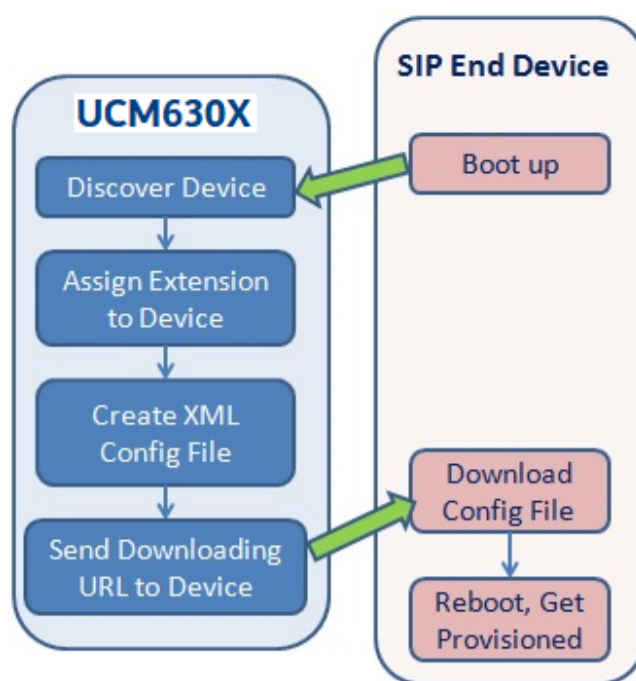
*Zero Config Configuration Architecture for End Point Device*

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 UCM630xA 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 UCM630xA for auto provisioning. Three methods of auto provisioning are used.



UCM630xA Zero Config

- o **SIP SUBSCRIBE**

When the phone boots up, it sends out SUBSCRIBE to a multicast IP address in the LAN. The UCM630xA 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 UCM630xA and take the new configuration.

- o **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 UCM630xA 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 UCM630xA.

- o **mDNS**

When the phone boots up, it sends out mDNS query to get the TFTP server address. The UCM630xA will respond with its own address. The phone will then send TFTP request to download the XML config file from the UCM630xA.

To start the auto provisioning process, under Web GUI > **Device Management** > **Zero Config** > **Zero Config Settings**, fill in the auto provision information.

**Basic Settings**Enable Zero Config: Enable Automatic Configuration 

Assignment:

**Extension Assignment**

Auto provision automatically provides an extension to the device.

There are two methods of auto provision: SIP SUBSCRIBE and DHCP Option 66.

For example, when the device boots up, it will send SIP SUBSCRIBE multicast in the LAN. The PBX will find it, create an account and return a URL of the config file for the device to download.

Auto Assign Extension: Zero Config Extension Segment: 5000 - 6299 [Zero Config Extension Segment](#)

Segment:

Enable Pick Extension: Pick Extension Segment: 4000 - 4999 [Pick Extension Segment](#)Pick Extension Period (hour): **Network Settings**Subnet Whitelist:  ⊖[Add Subnet Whitelist](#) ⊕**Save***Auto Provision Settings*

<b>Enable Zero Config</b>	Enable or disable the zero-config feature on the PBX. The default setting is enabled.
<b>Enable Automatic Configuration Assignment</b>	By default, this is disabled. If disabled, when SIP device boots up, the UCM630xA 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 UCM630xA.  <b>Note:</b> When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the UCM630xA which will include the XML config file URL for the SIP device to download.
<b>Auto Assign Extension</b>	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.
<b>Zero Config Extension Segment</b>	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 → <b>PBX Settings</b> → <b>General Settings</b> → <b>General</b> page → Extension Preference section: "Auto Provision Extensions".
<b>Enable Pick Extension</b>	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.
<b>Pick Extension Segment</b>	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 → <b>PBX Settings</b> → <b>General Settings</b> → <b>General</b> page → Extension Preference section: "Pick Extensions".
<b>Pick Extension Period (hour)</b>	Specify the number of minutes to allow the phones being provisioned to pick extensions.

<b>Subnet Whitelist</b>	<p>This feature allows the UCM to provision devices in different subnets other than UCM network.</p> <p>Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is <b>&lt;IP&gt;/&lt;CIDR&gt;</b>.</p> <p>Examples:</p> <p>10.0.0.1/8</p> <p>192.168.6.0/24</p> <p><b>Note:</b> Only private IP ranges (10.0.0.0   172.16.0.0   192.168.0.0) are supported.</p>
-------------------------	--

*Auto Provision Settings*

Please make sure an extension is manually assigned to the phone or "Automatically Assign Extension" is enabled during provisioning. After the configuration on the UCM630xA Web GUI, click on "Save" and "Apply Changes". Once the phone boots up and picks up the config file from the UCM630xA, 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 > **Device Management** > **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 UCM630xA. 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 UCM630xA Web GUI > **Device Management** > **Zero Config** > **Auto Provisioning Settings**.

Auto Discover
×

The PBX can automatically discover new devices via ARP, PING or SIP Message by scanning the entire network segment or a single IP address.

PBX LAN/LAN1	192.168.5.147
Address:	
Network Segment:	192.168.5.0 - 192.168.5.255
Broadcast IP:	192.168.5.255
Scan Method:	<input type="text" value="SIP-Message"/>
Subnet Whitelist:	<input type="text" value="Local Subnet Only"/>
Scan IP:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="5"/> . <input type="text" value="137"/>

*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 Web GUI) are displayed in the list.

MAC ADDRESS	IP ADDRESS	EXTENSION	VERSION	VENDOR	MODEL	CREATE CONFIG	OPTIONS
<input type="checkbox"/> 000B82000001	<a href="#">192.168.2.111</a>	1000	unknown	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/> 000B8227FB15	<a href="#">192.168.2.108</a>	--	1.0.3.208	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/> 000B82A46ACE	<a href="#">192.168.2.106</a>	--	1.0.0.36	GRANDSTREAM	--	--	
<input type="checkbox"/> 000B82D33AC4	<a href="#">192.168.2.105</a>	--	20.19.10.30	GRANDSTREAM	--	--	
<input type="checkbox"/> 000B82F66470	<a href="#">192.168.2.107</a>	--	10.19.9.26	GRANDSTREAM	--	--	

Discovered Devices

When the UCM is set to "Dual" network method, the user will be able to choose which LAN interface to use for Auto-Discovery.

**Auto Discover**

The PBX can automatically discover new devices via ARP, PING or SIP Message by scanning entire network segment or a single IP address.

Interface:

PBX Network Interface IP Address:

Network Segment:

Auto Discover LAN1/LAN2

## Firmware

In Firmware tab, users can upload to and manage firmware for endpoints. Additionally, firmware upload size limit has been increased from 300MB to 1GB.

**Zero Config**

< [Model Templates](#) [Model Update](#) **[Firmware](#)** [Zero Config Settings](#) >

---

Firmware Storage Path :  Local

**Firmware List**

NAME	MODEL	FIRMWARE VERSION	DATE	SIZE	STATUS	OPTIONS
No Data						

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

Firmware Storage

Upload New Firmware

- **Enable:** toggles whether the UCM will provision this firmware to endpoints if they are using the UCM as the firmware server. If not enabled, the UCM will reject requests from endpoints for this firmware.
- **Model:** The device model for which this firmware is intended for. Only for self-reference and has no effect on provisioning.
- **Firmware:** The firmware version of the file being uploaded. Only for self-reference and has no effect on provisioning.
- **Remark:** Add a comment about the uploaded firmware. Only for self-reference and has no effect on provisioning.
- **Choose File to Upload:** Select the firmware file to upload from the user's PC. The file name must match the firmware file name requested by the endpoint.

## 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_sec	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	===== Device Start =====													
5	===== Device Start =====													
6	config_name	vendor	state	ip	account_sec	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	===== Device Start =====													
9	===== Device Start =====													
10	config_name	vendor	state	ip	account_sec	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

Device List – CSV file Sample

### Note

Please ensure that the .csv file is encoded in UTF-8 to be able to import the devices correctly into the UCM.

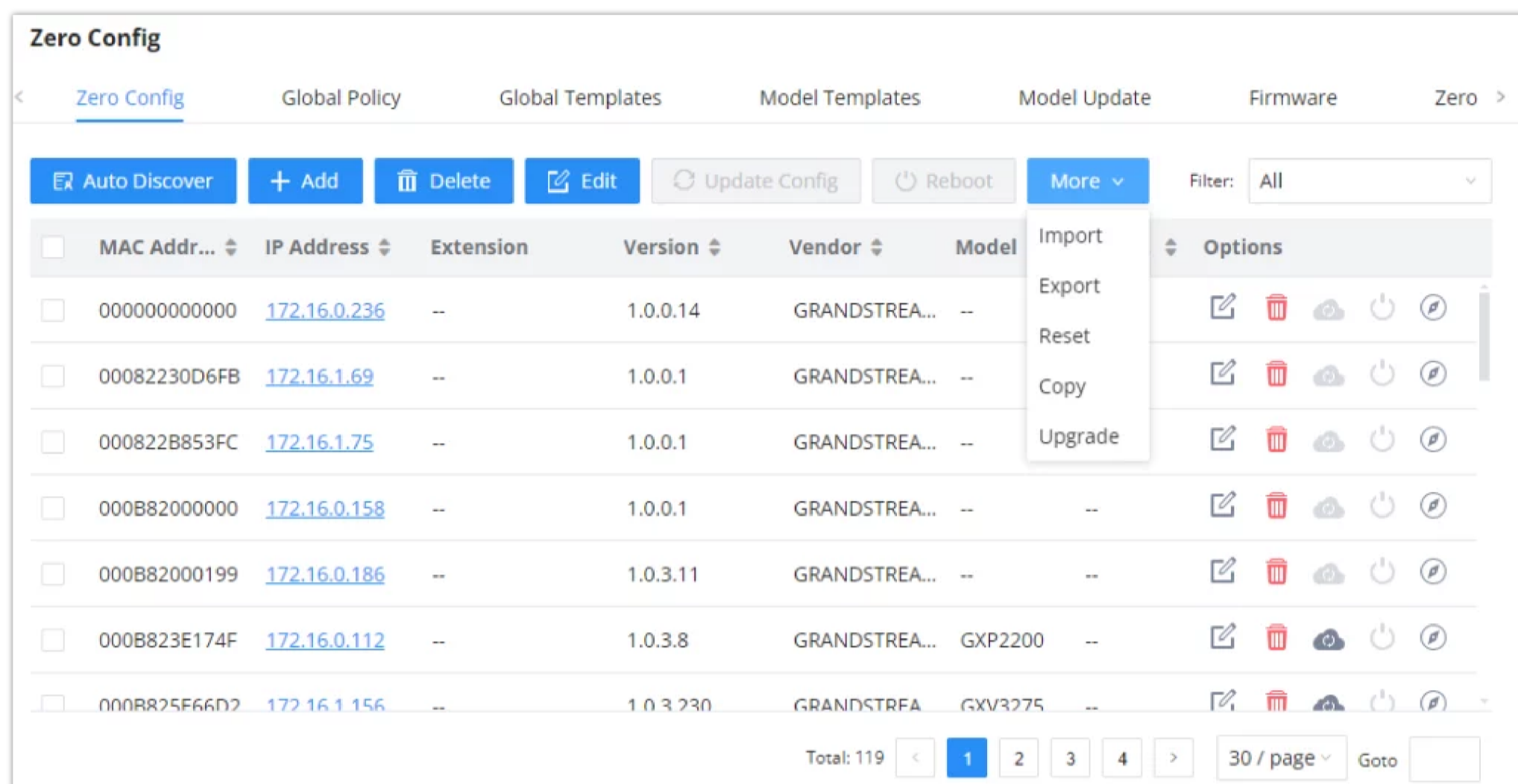
## Managing Discovered Devices

- **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: Display all discovered devices.
  - Scan Results: Display only manually discovered devices. [Discovery]

- o IP Address: Enter device IP and press Search button.
- o MAC Address: Enter device MAC and press Search button.
- o Model: Enter a model name and press Search button. Example: GXP2130.
- o Extension: Enter the extension number and press Search button.



Managing Discovered Devices

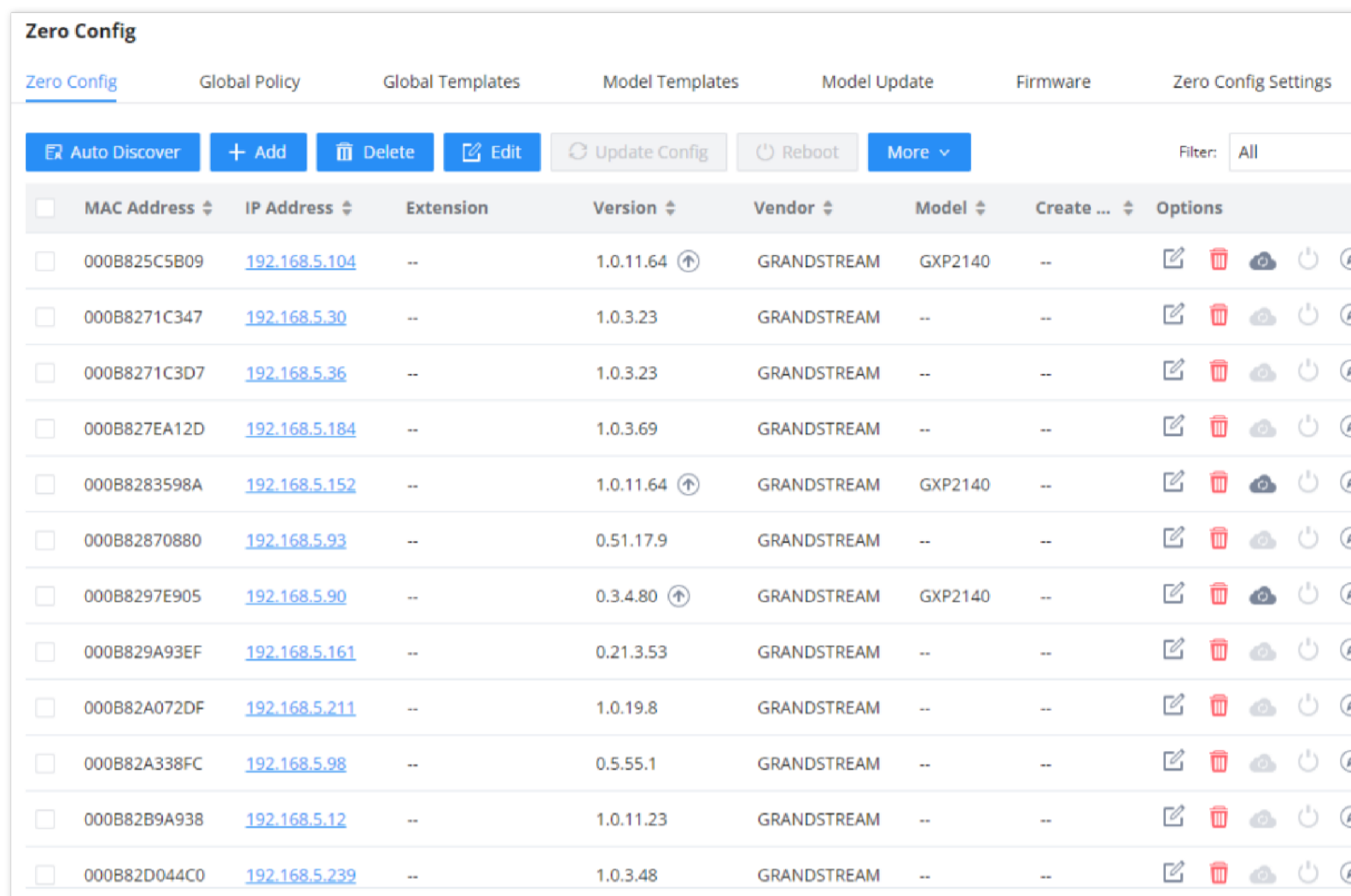
From the main menu of zero config, users can perform the following operations:
































































- o Click on **Auto Discover** in order to access to the discovery menu as shown on [Discovery] section.
- o Click on **Add** to add a new device to zero config database using its MAC address.
- o Click on **Delete** to delete selected devices from the zero-config database.
- o Click on **Edit** to modify selected devices.
- o 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.
- o 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).
- o Click on **More** to perform the following additional actions:
  - o **Import:** Import list of devices.
  - o **Export:** Export the list of the discovered devices. Select the devices to export before clicking this button. In case no devices were selected, all the discovered devices will be exported.
  - o **Reset:** Reset the discovered devices. Select the devices to reset before clicking this button. In case no devices were selected all the discovered devices will be reset to their initial configuration.

- **Copy:** Copy the configuration across devices.
- **Upgrade:** Upgrade the software of the discovered devices to the latest version. Select the devices which you want to upgrade. In case when no devices were selected, all the discovered devices will be upgraded to the latest firmware version.

All these operations will be detailed on the next sections.

When a new firmware is detected for the discovered devices, an upgrade icon  will appear next to the firmware version installed on the device.



MAC Address	IP Address	Extension	Version	Vendor	Model	Create ...	Options
<input type="checkbox"/> 000B825C5B09	<a href="#">192.168.5.104</a>	--	1.0.11.64 	GRANDSTREAM	GXP2140	--	    
<input type="checkbox"/> 000B8271C347	<a href="#">192.168.5.30</a>	--	1.0.3.23	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B8271C3D7	<a href="#">192.168.5.36</a>	--	1.0.3.23	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B827EA12D	<a href="#">192.168.5.184</a>	--	1.0.3.69	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B8283598A	<a href="#">192.168.5.152</a>	--	1.0.11.64 	GRANDSTREAM	GXP2140	--	    
<input type="checkbox"/> 000B82870880	<a href="#">192.168.5.93</a>	--	0.51.17.9	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B8297E905	<a href="#">192.168.5.90</a>	--	0.3.4.80 	GRANDSTREAM	GXP2140	--	    
<input type="checkbox"/> 000B829A93EF	<a href="#">192.168.5.161</a>	--	0.21.3.53	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B82A072DF	<a href="#">192.168.5.211</a>	--	1.0.19.8	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B82A338FC	<a href="#">192.168.5.98</a>	--	0.5.55.1	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B82B9A938	<a href="#">192.168.5.12</a>	--	1.0.11.23	GRANDSTREAM	--	--	    
<input type="checkbox"/> 000B82D044C0	<a href="#">192.168.5.239</a>	--	1.0.3.48	GRANDSTREAM	--	--	    

Zero Config

## Global Configuration

Global configuration will apply to all the connected Grandstream SIP end point devices in the same LAN with the UCM630xA no matter what the Grandstream device model it is. It is divided into two levels:

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

 Global Templates configuration has higher priority to Global Policy configuration.

## Global Policy

Global Policy can be accessed in Web GUI>**Device Management**>**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.



*Global Policy Categories*

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

<b>Language settings</b>	
<b>Language</b>	Select the LCD display language on the SIP end device.
<b>Date and Time</b>	
<b>Date Format</b>	Configure the date display format on the SIP end device's LCD.
<b>Time Format</b>	Configure the time display in 12-hour or 24-hour format on the SIP end device's LCD.
<b>Enable NTP</b>	To enable the NTP service.
<b>NTP Server</b>	Configure the URL or IP address of the NTP server. The SIP end device may obtain the date and time from the server.
<b>NTP Update Interval</b>	Configure the NTP update interval.
<b>Time Zone</b>	Configure the time zone used on the SIP end device.
<b>Enable Daylight Saving Time</b>	Select either to enable or disable the DST.

*Global Policy Parameters – Localization*

<b>Default Call Settings</b>	
<b>Dial Plan</b>	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.
<b>Enable Call Features</b>	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.
<b>Use # as Dial Key</b>	If set to "Yes", pressing the number key "#" will immediately dial out the input digits.
<b>Auto Answer by Call-info</b>	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.
<b>NAT Traversal</b>	Configure if NAT traversal mechanism is activated.
<b>User Random Port</b>	If set to "Yes", this parameter will force random generation of both the local SIP and RTP ports.
<b>General Settings</b>	

<b>Call Progress Tones</b>	<p>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:</p> <p>f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]];</p> <ul style="list-style-type: none"> <li>○ Frequencies are in Hz and cadence on and off are in 10ms).</li> <li>○ "on" is the period (in ms) of ringing while "off" is the period of silence. Up to three cadences are supported.</li> <li>○ Please refer to user manual of the SIP devices to be provisioned for more details</li> </ul>
<b>HEADSET Key Mode</b>	<p>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.</p>

*Global Policy Parameters – Phone Settings*

<b>LDAP Phonebook</b>	
<b>Source</b>	<p>Select "Manual" or "PBX" as the LDAP configuration source.</p> <ul style="list-style-type: none"> <li>○ If "Manual" is selected, the LDAP configuration below will be applied to the SIP end device.</li> <li>○ If "PBX" is selected, the LDAP configuration built-in from UCM630xA Web GUI→<b>System Settings</b>→<b>LDAP Server</b> will be applied.</li> </ul>
<b>Address</b>	<p>Configure the IP address or DNS name of the LDAP server.</p>
<b>Port</b>	<p>Configure the LDAP server port. The default value is 389.</p>
<b>Base DN</b>	<p>This is the location in the directory where the search is requested to begin.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>○ dc=grandstream, dc=com</li> <li>○ ou=Boston, dc=grandstream, dc=com</li> </ul>
<b>Username</b>	<p>Configure the bind "Username" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.</p>
<b>Password</b>	<p>Configure the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.</p>
<b>Number Filter</b>	<p>Configure the filter used for number lookups. Please refer to user manual for more details.</p>
<b>Name Filter</b>	<p>Configure the filter used for name lookups. Please refer to user manual for more details.</p>
<b>Version</b>	<p>Select the protocol version for the phone to send the bind requests. The default value is 3.</p>
<b>Name Attribute</b>	<p>Specify the "name" attributes of each record which are returned in the LDAP search result.</p> <p>Example:</p> <p>gn</p> <p>cn sn description</p>

<b>Number Attribute</b>	<p>Specify the “number” attributes of each record which are returned in the LDAP search result.</p> <p>Example:</p> <p>telephoneNumber</p> <p>telephoneNumber Mobile</p>
<b>Display Name</b>	<p>Configure the entry information to be shown on phone’s LCD. Up to 3 fields can be displayed.</p> <p>Example:</p> <p>%cn %sn %telephoneNumber</p>
<b>Max Hits</b>	<p>Specify the maximum number of results to be returned by the LDAP server. Valid range is 1 to 3000. The default value is 50.</p>
<b>Search Timeout</b>	<p>Specify the interval (in seconds) for the server to process the request and client waits for server to return.</p> <p>Valid range is 0 to 180. Default value is 30.</p>
<b>Sort Results</b>	<p>Specify whether the searching result is sorted or not. Default setting is No.</p>
<b>Incoming Calls</b>	<p>Configure to enable LDAP number searching when receiving calls. The default setting is No.</p>
<b>Outgoing Calls</b>	<p>Configure to enable LDAP number searching when making calls. The default setting is No.</p>
<b>Lookup Display Name</b>	<p>Configures the display name when LDAP looks up the name for incoming call or outgoing call.</p> <p>It must be a subset of the LDAP Name Attributes.</p>
<b>XML Phonebook</b>	
<b>Phonebook XML Server</b>	<p>Select the source of the phonebook XML server.</p> <ul style="list-style-type: none"> <li>○ <b>Disable</b></li> </ul> <p>Disable phonebook XML downloading.</p> <ul style="list-style-type: none"> <li>○ <b>Manual</b></li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>○ <b>Local UCM Server</b></li> </ul> <p>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.</p>
<b>Phonebook Download Interval</b>	<p>Configure the phonebook download interval (in Minute). If set to 0, automatic download will be disabled. Valid range is 5 to 720.</p>
<b>Remove manually edited entries on download</b>	<p>If set to “Yes”, when XML phonebook is downloaded, the entries added manually will be automatically removed.</p>

<b>Firmware Source</b>	<p>Firmware source via ZeroConfig provisioning could a URL for external server address, local UCM directory or USB media if plugged in to the UCM630xA. Select a source to get the firmware file:</p> <ul style="list-style-type: none"> <li>○ <b>URL</b></li> </ul> <p>If select to use URL to upgrade, complete the configuration for the following four parameters: "Upgrade Via", "Server Path", "File Prefix" and "File Postfix".</p> <ul style="list-style-type: none"> <li>○ <b>Local UCM Server</b></li> </ul> <p>Firmware can be uploaded to the UCM630xA 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.</p> <ul style="list-style-type: none"> <li>○ <b>Local USB Media</b></li> </ul> <p>If selected, the USB storage device needs to be plugged into the UCM630xA and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory.</p> <ul style="list-style-type: none"> <li>○ <b>Local SD Card Media</b></li> </ul> <p>If selected, an SD card needs to be plugged into the UCM630xA and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory.</p>
<b>Upgrade via</b>	When URL is selected as firmware source, configure upgrade via TFTP, HTTP or HTTPS.
<b>Server Path</b>	When URL is selected as firmware source, configure the firmware upgrading server path.
<b>File Prefix</b>	Configure the Config Server Path.
<b>Config Server Path</b>	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.
<b>Allow DHCP Option 43/66</b>	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
<b>Automatic Upgrade</b>	<p>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.</p> <ul style="list-style-type: none"> <li>○ <b>By week</b></li> </ul> <p>Once selected, specify the day of the week to check HTTP/TFTP server for firmware upgrades or configuration files changes.</p> <ul style="list-style-type: none"> <li>○ <b>By day</b></li> </ul> <p>Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes.</p> <ul style="list-style-type: none"> <li>○ <b>By minute</b></li> </ul> <p>Once selected, specify the interval <b>X</b> that the SIP end device will request for new firmware every <b>X</b> minutes.</p>
<b>Firmware Upgrade Rule</b>	Specify how firmware upgrading and provisioning request to be sent.
<b>Zero Config</b>	Select either to enable or disable zero config.
<b>Web Access</b>	
<b>Admin Password</b>	Configure the administrator password for admin level login.
<b>End-User Password</b>	Configure the end-user password for the end user level login.
<b>Web Access Mode</b>	Select HTTP or HTTPS as the web access protocol.

<b>Web Server Port</b>	Configure the port for web access.  The valid range is 1 to 65535.
<b>RTSP Port</b>	Configure the RTSP Port.
<b>Enable UPnP Discovery</b>	Select either to enable or disable Enable UPnP Discovery
<b>Login Settings</b>	Configure the login settings.
<b>User Login Timeout</b>	Configure User Login Timeout.
<b>Maximum Consecutive Failed Login Attempts</b>	Configure Maximum Consecutive Failed Login Attempts.
<b>Login Error Lock Time</b>	Configure Login Error Lock Time.
<b>Security</b>	
<b>Disable Telnet/SSH</b>	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.
<b>Syslog</b>	
<b>Syslog Server</b>	Configure the URL/IP address for the syslog server.
<b>Syslog Level</b>	Select the level of logging for syslog.
<b>Send SIP Log</b>	Configure whether the SIP log will be included in the syslog message.

*Global Policy Parameters – Maintenance*

<b>Basic Settings</b>	
<b>IP Address</b>	Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected. <ul style="list-style-type: none"> <li>○ <b>DHCP</b></li> </ul> 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. <ul style="list-style-type: none"> <li>○ <b>PPPoE</b></li> </ul> Once selected, users need specify the Account ID, Password and Service Name for PPPoE.
<b>Host Name</b>	Specifies the name of the client. This field is optional but may be required by Internet Service Providers.
<b>Vendor Class ID</b>	Used by clients and servers to exchange vendor class ID.
<b>Account ID</b>	Enter the PPPoE account ID.
<b>Password</b>	Enter the PPPoE Password.
<b>Service Name</b>	Enter the PPPoE Service Name.
<b>Advanced Setting</b>	
<b>Layer 3 QoS</b>	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0-63.
<b>Layer 3 QoS For RTP</b>	Assign the priority value of the Layer 3 QoS for RTP packets.  Valid range is 0 -63.
<b>Layer 3 QoS For SIP</b>	Assign the priority value of the Layer 3 QoS for SIP packets.  Valid range is 0 -63.

<b>Layer 2 QoS Tag</b>	Assign the VLAN Tag of the Layer 2 QoS packets.  Valid range is 0 -4095.
<b>Layer 2 QoS Priority Value</b>	Assign the priority value of the Layer 2 QoS packets.  Valid range is 0-7.
<b>STUN Server</b>	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
<b>Keep Alive</b>	Select either to enable or disable Keep Alive.
<b>Keep Alive Interval</b>	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.
<b>Register Expiration</b>	Specify the Register Expiration.
<b>Local SIP Port</b>	Configure Local SIP Port.
<b>Local RTP Port</b>	Configure Local RTP Port.
<b>Auto On-Hook Timer(s)</b>	Configure Auto On-Hook Timer(s).
<b>Ring Timeout</b>	Configure Ring Timeout.
<b>SIP Transport</b>	Select either UDP, TCP or TLS/TCP as SIP transport protocol.
<b>Direct IP Call</b>	Select either to disable or enable Direct IP Call support.
<b>SIP Proxy Compatibility Mode</b>	Select either to disable or enable SIP Proxy Compatibility Mode.
<b>Unregister On Reboot</b>	Select either to disable or enable Unregister On Reboot.
<b>Whitelist</b>	
<b>Whitelist</b>	Select either to enable or disable Whitelist
<b>SIP Phone Number Whitelist</b>	Configure the SIP Phone Number Whitelist.

*Global Policy Parameters – Network Settings*

<b>Wallpaper</b>	
<b>Screen Resolution 1024 x 600</b>	<p>Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> <li>○ <b>Source</b></li> </ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> <li>○ <b>File</b></li> </ul> <p>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 UCM630xA.</p>

<p><b>Screen Resolution 800 x 400</b></p>	<p>Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> <li>○ <b>Source</b></li> </ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> <li>○ <b>File</b></li> </ul> <p>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 UCM630xA.</p>
<p><b>Screen Resolution 480 x 272</b></p>	<p>Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> <li>○ <b>Source</b></li> </ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> <li>○ <b>File</b></li> </ul> <p>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 UCM630xA.</p>
<p><b>Screen Resolution 320 x 240</b></p>	<p>Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> <li>○ <b>Source</b></li> </ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> <li>○ <b>File</b></li> </ul> <p>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 UCM630xA.</p>

*Global Policy Parameters – Customization*

**Email Settings**

<p><b>SMTP Settings</b></p>	<p>Check this option to configure the email settings that will be sent to the provisioned phones:</p> <ul style="list-style-type: none"> <li>◦ <b>Server</b> IP address of the SMTP server</li> <li>◦ <b>Port</b> SMTP server port</li> <li>◦ <b>From E-Mail address</b> Email address</li> <li>◦ <b>Sender Username</b> Username of the sender</li> <li>◦ <b>Password Recovery Email</b> Email where recovered password will be sent</li> <li>◦ <b>Alarm receive Email 1</b> Email address where alarms notifications will be sent</li> <li>◦ <b>Alarm receive Email 1</b> Email address where alarms notifications will be sent</li> <li>◦ <b>Enable SSL</b> Enable SSL protocol for SMTP</li> </ul>
<p><b>FTP</b></p>	
<p><b>FTP</b></p>	<p>Check this option to configure the FTP settings that will be sent to the provisioned phones:</p> <ul style="list-style-type: none"> <li>◦ <b>Storage Server Type</b> Either FTP or Central Storage</li> <li>◦ <b>Server</b> FTP server address</li> <li>◦ <b>Port</b> FTP port to be used</li> <li>◦ <b>Username</b> FTP username</li> <li>◦ <b>Path</b> FTP Directory path</li> </ul>


Global Templates can be accessed in Web GUI>**Device Management**>**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.

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



*Create New 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.

*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 > **Device Management** > **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 **Device Management** > **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 UCM630xA.

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.


<b>Model</b>	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
<b>Template Name</b>	Create a name for the model template.
<b>Description</b>	Enter a description for the model template. This is optional.
<b>Default Model Template</b>	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.
<b>Active</b>	Check this option to enable the model template.


#### *Create New 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 <https://www.grandstream.com/support/tools>

## Edit Model Templates: GRP2613\_template

\* Model: GRANDSTREAM GRP2613

\* Template Name: GRP2613\_template

Description:

Default Model Template:

Active:

Options:

Custom Parameters

Custom Parameters

Please enter P-values into the Name fields. Example: To configure Language to English, enter "P1362" into the Name field and "en\_US" into the Value field.

	P1362	en	Description	Possible Match Exists
--	-------	----	-------------	-----------------------

+ Add New Field

### Edit Model Template

- o Click on Save when done. The model template will be displayed on Web GUI > **Device Management** > **Zero Config** > **Model Templates** page.
- o Click on to delete the model template or click on "Delete Selected Templates" to delete multiple selected templates at once.
- o Click on "Toggle Selected Template(s)" to toggle the status between enabled/disabled for the selected model templates.
- o Click the "Copy Template" button to copy the configuration items of the selected model template to another template, thereby reducing template editing work. Note: The model template only supports copying between devices of the same model.
- o Click the "Import/Export" button to upload/export the model template list in .CSV format.

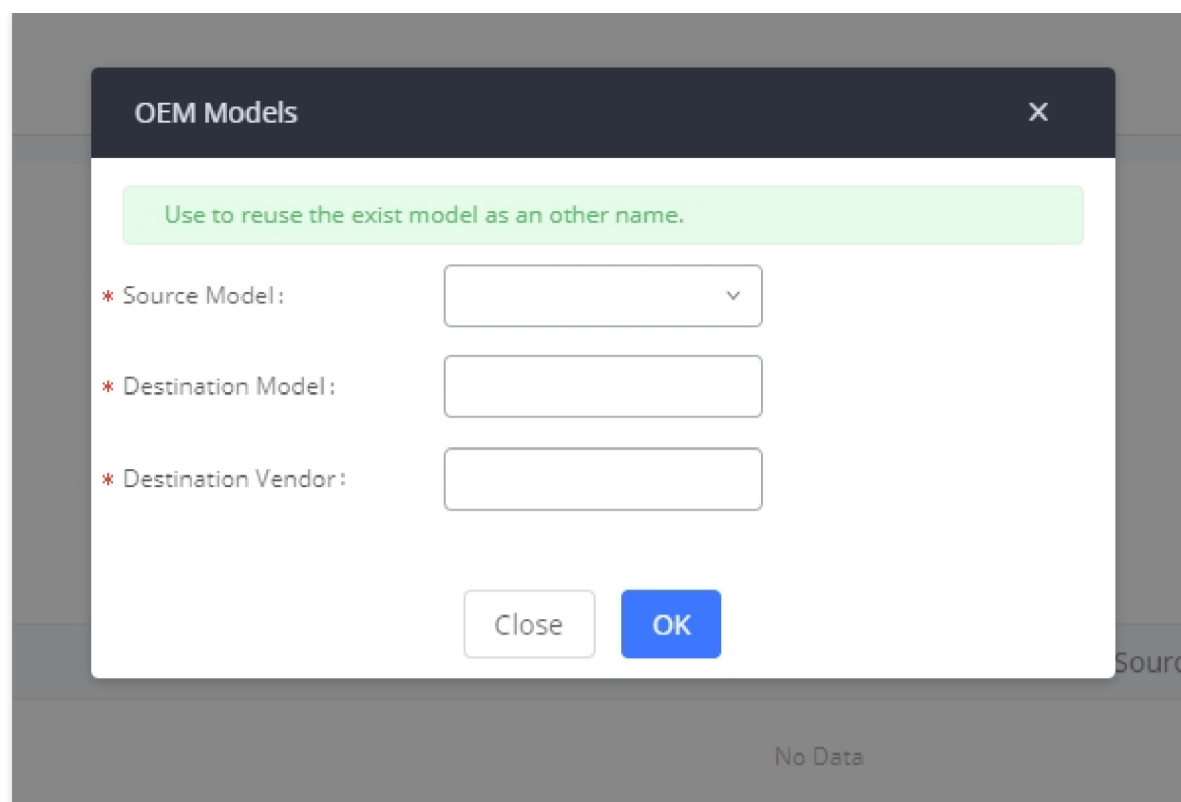
## Model Update

UCM630xA 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.



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













OEM Models

## Model Template Package List

Templates for most of the Grandstream models are built in with the UCM630xA already. Templates for Grandstream Wave and Grandstream surveillance products require users to download and install under Web GUI→**Device Management**>**Zero Config**>**Model Update** first before they are available in the UCM630xA for selection. After downloading and installing the model template to the UCM630xA, 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 UCM630xA.

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			


Total: 37    10 / page 

Template Management

## Upload Model Template Package

In case the UCM630xA 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.

**Upload Model Template Package**

Choose Model Package to Choose File to Upload

Upload:

*Upload Model Template Manually*

**Device Configuration**

On Web GUI, page **Device Management>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 UCM630xA. 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.

Cancel Update Save

---

**Model:** GRANDSTREAM GXV3350

**MAC Address:** c074ad112233

**IP Address:**

**Version:**

---

**Basic Settings**    Advanced Settings

**Accounts**

<input type="checkbox"/>	Account 1:	<input type="text" value="+123456789"/>
<input type="checkbox"/>	Account 2:	<input type="text" value="+123456789"/>
<input type="checkbox"/>	Account 3:	<input type="text" value="+123456789"/>
<input type="checkbox"/>	Account 4:	<input type="text" value="+123456789"/>
<input type="checkbox"/>	Account 5:	<input type="text" value="+123456789"/>

*Create New Device*

**Manage Devices**

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

<input type="checkbox"/>	MAC ADDRESS	IP ADDRESS	EXTENSION	VERSION	VENDOR	MODEL	CREATE CONFIG	OPTIONS
<input type="checkbox"/>	000B82000001	<a href="#">192.168.2.111</a>	1000	unknown	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/>	000B8227FB15	<a href="#">192.168.2.108</a>	--	1.0.3.208	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/>	000B82A46ACE	<a href="#">192.168.2.106</a>	--	1.0.0.36	GRANDSTREAM	--	--	
<input type="checkbox"/>	000B82D33AC4	<a href="#">192.168.2.105</a>	--	20.19.10.30	GRANDSTREAM	--	--	
<input type="checkbox"/>	000B82F66470	<a href="#">192.168.2.107</a>	--	10.19.9.26	GRANDSTREAM	--	--	

*Manage Devices*

- o Click on

to access the Web GUI of the phone.

- o 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.

**Edit Device: 000B8273C559**

**Model:** GRANDSTREAM GXP2130

**MAC Address:** 000B8273C559

**IP Address:** 192.168.5.197

**Version:** 1.0.9.127

Basic Settings **Advanced Settings**

**5 Custom Device Settings** **Preview**

[Modify Custom Settings](#)

**4 Model Templates**

0 item Idle | 0 Selected

None | None

**3 Default Model Template**

*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 → **Device Management** > **Zero Config** > **Global Policy** will be applied here. Clicking on “Modify Global Policy” to redirect to page **Device Management** > **Zero Config** > **Global Policy**.

### 2. Global Templates

Select a global template 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



. 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>**Device Management>Zero Config>Model Templates** page. Please see default model template option in **[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



. 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.

Model:	Grandstream GXP2170
MAC Address:	000B82A95F94
IP Address:	192.168.5.115
Version:	1.0.9.132

Custom Fields

Please use P-values for the Name fields. <br />Example: To configure Language, enter "P1362" into the Language Value field.

	P1362	en	Description	Possible Match Exists
--	-------	----	-------------	-----------------------

[+ Add New Field](#)

*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 [https://content.grandstream.com/hubfs/Grandstream\\_Feb\\_2021/Zip%20File/config-template.zip?hsLang=en](https://content.grandstream.com/hubfs/Grandstream_Feb_2021/Zip%20File/config-template.zip?hsLang=en)

- o Select multiple devices that need to be modified and then click on “Update Config” to batch modify devices.

If selected devices are of the same model, the configuration dialog is like the following figure. Configurations in five levels are all available for users to modify.

Modify Selected Devices Cancel Save

**WARNING: Performing a batch operation will override all the existing device configurations on this page.**



\* Model:

MAC Address:

---

**Basic Settings**    Advanced Settings

**Programmable MPK Settings**

	MPK 1:	Speed Dial	Description	Value
<input type="checkbox"/>	MPK 2:	Speed Dial	Description	Value
<input type="checkbox"/>	MPK 3:	Speed Dial	Description	Value
<input type="checkbox"/>	MPK 4:	Speed Dial	Description	Value
<input type="checkbox"/>	MPK 5:	Speed Dial	Description	Value
<input type="checkbox"/>	MPK 6:	Speed Dial	Description	Value

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.

Modify Selected Devices Cancel Save

**WARNING: Performing a batch operation will override all the existing device configurations on this page.**



<
>

\* Model:

MAC Address:

---

Basic Settings    **Advanced Settings**

**5 Custom Device Settings**

Available only for single model

**4 Model Templates**

**Preview**

Preview prepared for 000B8227FB15

Modify Selected Devices – Different Models

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

After the above configurations, save the changes and go back to Web GUI > **Device Management** > **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.

Zero Config

[Zero Config](#) [Global Policy](#) [Global Templates](#) [Model Templates](#) [Model Update](#) [Zero Config Settings](#)

Filter:

<input type="checkbox"/>	MAC ADDRESS	IP ADDRESS	EXTENSION	VERSION	VENDOR	MODEL	CREATE CONFIG	OPTIONS
<input type="checkbox"/>	000B82000001	<a href="#">192.168.2.111</a>	1000	unknown	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/>	000B8227FB15	<a href="#">192.168.2.108</a>	--	1.0.3.208	GRANDSTREAM	GXV3275	--	
<input type="checkbox"/>	000B82A46ACE	<a href="#">192.168.2.106</a>	--	1.0.0.36	GRANDSTREAM	--	--	
<input type="checkbox"/>	000B82A95F94	<a href="#">192.168.5.115</a>	--	1.0.9.132	GRANDSTREAM	GXP2170	--	
<input type="checkbox"/>	000B82D33AC4	<a href="#">192.168.2.105</a>	--	20.19.10.30	GRANDSTREAM	--	--	
<input type="checkbox"/>	000B82F66470	<a href="#">192.168.2.107</a>	--	10.19.9.26	GRANDSTREAM	--	--	

Total: 6    30 / page    Goto 1

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>**Device Management**>**Zero Config**>**Zero Config Settings**, select "Enable Zero Config".
2. Go to Web GUI>**Device Management**>**Zero Config**>**Global Policy**, configure Date Format, Time Format and Firmware Source as follows.

Localization

---

**Language Settings**

\* Language: English

---

**Date and Time**

Date Format: yyyy-mm-dd

Time Format: 12-hour Clock

Enable NTP: Disabled

NTP Server:

NTP Update Interval: 1440

Time Zone: GMT+08:00 (Beijing, Taipei, Kuala Lu...

Enable Daylight Saving Time: Disabled

---

> Phone Settings

> Contact List

---

Maintenance

---

**Upgrade and Provision**


Firmware Source: Source: URL

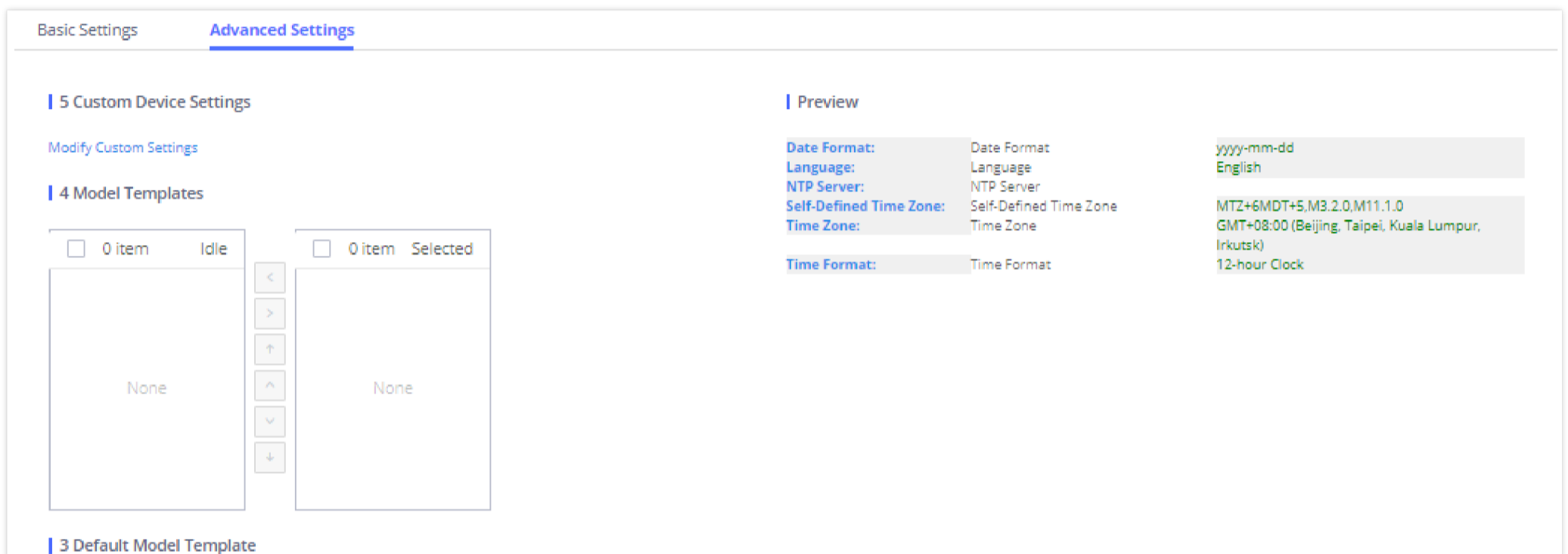
Upgrade via: TFTP

Server Path: fm.grandstream.com/gs

File Prefix:

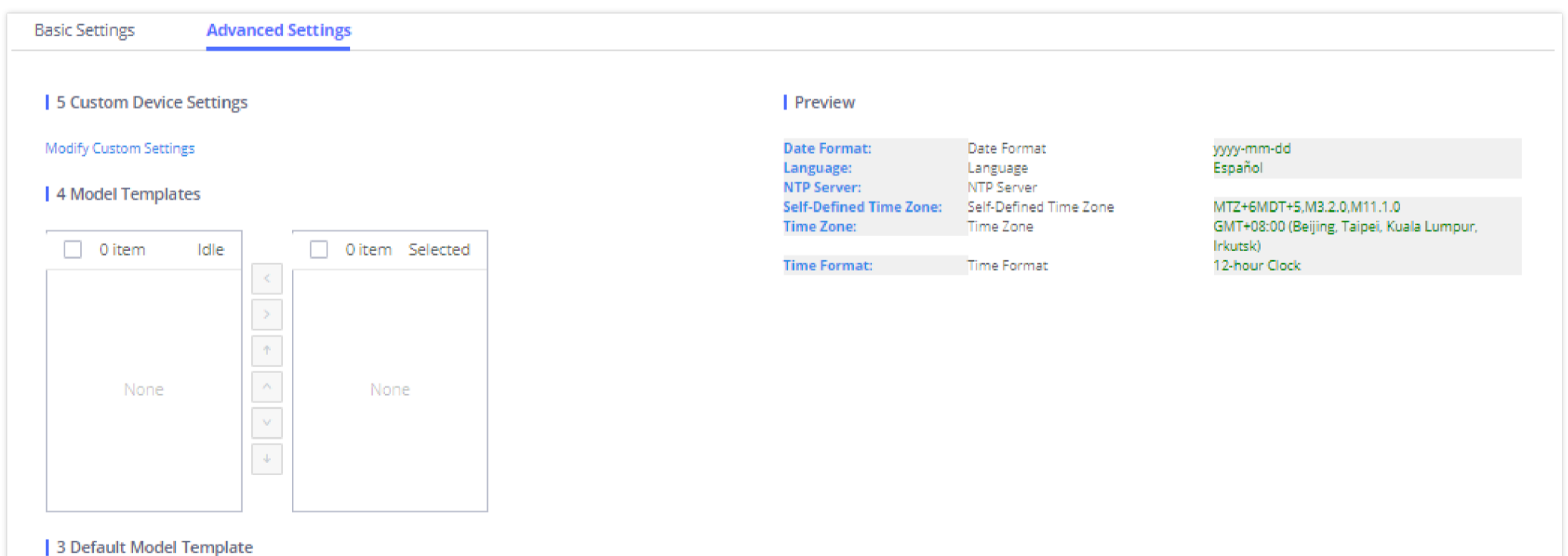
File Postfix:

- Go to Web GUI>**Device Management**>**Zero Config**>**Model Templates**, create a new model template “English Support Template” for GXP2170. Add option “Language” and set it to “English”. Then select the option “Default Model Template” to make it the default model template.
- Go to Web GUI>**Device Management**>**Zero Config**>**Model Templates**, create another model template “Spanish Support Template” for GXP2170. Add option “Language” and set it to “Español”.
- 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>**Device Management**>**Zero Config**>**Zero Config**.
- On Web GUI>**Device Management**>**Zero Config**>**Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on  to edit the device settings.
- 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.



Zero Config Sample – Device Preview 1

- 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.



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.

- 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.

Basic Settings **Advanced Settings**

**5 Custom Device Settings**

Modify Custom Settings

**4 Model Templates**

0 item Idle

None

0 item Selected

None

< > ↑ ↓

**3 Default Model Template**

**Preview**

**Date Format:** Date Format yyyy-mm-dd

**Language:** Language English

**NTP Server:** NTP Server

**Self-Defined Time Zone:** Self-Defined Time Zone MTZ+6MDT+5,M3.2.0,M11.1.0

**Time Zone:** Time Zone GMT+08:00 (Beijing, Taipei, Kuala Lumpur, Irkutsk)

**Time Format:** Time Format 12-hour Clock

Zero Config Sample – Device Preview 3

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

11. On the Web GUI > **Device Management** > **Zero Config** > **Zero Config** page, click on



to send NOTIFY to trigger the device to download config file from UCM630xA.

Now all the 9 phones in the network will be provisioned with a unique extension registered on the UCM630xA. 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.

Create New Extension

Basic Settings   Media   Features   Specific Time   Follow Me   Cancel Save

\* Select Extension Type: SIP Extension

Select Add Method: Single

---

**General**

\* Extension: 1005   CallerID Number:

\* Privilege: Internal   \* SIP/IAX Password: %27JbN@r8

AuthID:    Voicemail: Local Voicemail

\* Voicemail Password: 1161554273   Skip Voicemail Password Verification:

Send Voicemail Email Notification: Default   Attach Voicemail to Email: Default

Keep Voicemail after Emailing: Default

Enable Keep-alive:    \* Keep-alive Frequency: 60

Disable This Extension:    Enable SCA:

Emergency CID:    Enable Wave:

Sync Contact:

**User Settings**

First Name:    Last Name:

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.

General	
<b>Extension</b>	The extension number associated with the user.
<b>CallerID Number</b>	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.
<b>Call Privileges</b>	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". <b>Note:</b> Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
<b>SIP/IAX Password</b>	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.

<b>Auth ID</b>	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
<b>Voicemail</b>	Configure Voicemail. There are three valid options, and the default option is "Enable Local Voicemail". <ul style="list-style-type: none"> <li>• <b>Disable Voicemail:</b> Disable Voicemail.</li> <li>• <b>Enable Local Voicemail:</b> Enable voicemail for the user.</li> <li>• <b>Enable Remote Voicemail:</b> Forward the notify message from the remote voicemail system for the user, and the local voicemail will be disabled. Note: Remote voicemail feature is used only for Infomatec (Brazil).</li> </ul>
<b>Voicemail Password</b>	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
<b>Skip Voicemail Password Verification</b>	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
<b>Send Voicemail Email Notification</b>	Configures whether to send emails to the extension's email address to notify of a new voicemail.
<b>Attach Voicemail to Email</b>	Configures whether to attach a voicemail audio file to the voicemail notification emails. Note: When set to "Default", the global settings in <b>Basic Call Features</b> → <b>Voicemail</b> → <b>Voicemail Email Settings</b> will be used.
<b>Keep Voicemail after Emailing</b>	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 <b>Basic Call Features</b> → <b>Voicemail</b> → <b>Voicemail Email Settings</b> will be used.
<b>Enable Keep-alive</b>	If enabled, an empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is "No".
<b>Keep-alive Frequency</b>	Configure the Keep-alive interval (in seconds) to check if the host is up. The default setting is 60 seconds.
<b>Enable SCA</b>	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 <b>Advanced Call Features</b> → <b>SCA</b> page.
<b>Emergency CID Name</b>	CallerID name that will be used for emergency calls and callbacks.
<b>Disable This Extension</b>	If selected, this extension will be disabled on the PBX. <b>Note:</b> The disabled extension still exists on the PBX but cannot be used on the end device.
<b>Sync Contact</b>	If enabled, this extension number will be displayed in the Wave contact, otherwise, it will not be displayed, and it cannot be found in the chat, but the user can still dial this number.
<b>User Settings</b>	
<b>First Name</b>	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
<b>Last Name</b>	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
<b>Email Address</b>	Fill in the Email address for the user. Voicemail will be sent to this Email address.
<b>User/Wave Password</b>	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes. The password must respect the following criteria: <ul style="list-style-type: none"> <li>• At least one lower case letter</li> <li>• At least one upper case letter</li> <li>• At least one number</li> <li>• At least one special character</li> </ul>

	<ul style="list-style-type: none"> <li>• At least 8 total characters</li> </ul>
<b>User Portal/Wave Privileges</b>	<p>Change User Portal/Wave Privileges.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> Setting this privilege will grant the standard Wave privileges.</li> <li>• <b>Wave Administrator:</b> Setting this privilege will grant the user access to Management Portal on Wave.</li> </ul>
<b>Language</b>	<p>Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under <b>Web GUI→PBX Settings→Voice Prompt→Language Settings</b>. The dropdown list shows all the currently available voice prompt languages on the PBX. To add more languages to the list, please download the voice prompt package by selecting "Check Prompt List" under <b>Web GUI→PBX Settings→Voice Prompt→Language Settings</b>.</p>
<b>Concurrent Registrations</b>	<p>The maximum endpoints which can be registered to this extension. For security concerns, the default value is 3. <b>Note:</b> The user can configure up to 10 registrations per extensions.</p>
<b>Mobile Phone Number</b>	<p>Configure the phone number for the extension, user can type the related star code for the phone number followed by the extension number to directly call this number. For example, the user can type *881000 to call the mobile number associated with extension 1000.</p>
<b>Department</b>	<p>Configure the user's department. The department can be configured in <b>User Management-&gt;Address Book Management-&gt;Department Management</b>. <b>Job Title:</b> The user's department position.</p>
<b>Contact Privileges</b>	
<b>Same as Department Contact Privileges</b>	<p>When enabled, The extension will inherit the same privilege attributed to the department it belongs to.</p>
<b>Contact View Privileges</b>	<p>Select the privileges regarding the contact view in SIP endpoints and Wave.</p>

*SIP Extension Configuration Parameters → Basic Settings*

<b>SIP Settings</b>	
<b>NAT</b>	<p>Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is a one-way audio issue, usually it is related to NAT configuration or the Firewall's support of SIP and RTP ports. The default setting is enabled.</p>
<b>Enable Direct Media</b>	<p>By default, the PBX will route the media streams from SIP endpoints through itself. If this option is enabled, the PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. <b>Note:</b> It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing.</p>
<b>DTMF Mode</b>	<p>Select DTMF mode for the user to send DTMF. The default setting is "RFC4733". If "Info" is selected, the SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, RFC4733 will be used if offered, otherwise "Inband" will be used. <b>Note:</b> The default DTMF mode selected is RFC4733.</p>
<b>TEL URI</b>	<p>If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". The "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.</p>
<b>Alert-Info</b>	<p>When present in an INVITE request, the alert-Info header field specifies an alternative ring tone to the UAS.</p>
<b>Enable T.38 UDPTL</b>	<p>Enable or disable T.38 UDPTL support.</p>
<b>TURN Relay</b>	<p>Enable this option if the following are true:</p>

	<ol style="list-style-type: none"> <li>1. PBX is deployed on a private network.</li> <li>2. There are remote endpoints outside the PBX's network registering to it via its public IP address.</li> <li>3. The network's firewall is not configured for media port forwarding.</li> <li>4. Media NAT penetration is required.</li> </ol> <p>Once a TURN server is configured, media will be forwarded to it. This configuration does not affect endpoints that are registered via the PBX's RemoteConnect address.</p>
<b>Codec Preference</b>	Select audio and video codec for the extension. The available codecs are: <b>PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.</b>
<b>Jitter Buffer</b>	<p>Select the jitter buffer method.</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> Jitter buffer will not be used.</li> <li>• <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of "jitter buffer size")</li> <li>• <b>Adaptive:</b> Jitter buffer with an adaptive size (no more than the value of "max jitter buffer").</li> <li>• <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.</li> </ul>
<b>Packet Loss Retransmission</b>	<p>Configure to enable Packet Loss Retransmission.</p> <ul style="list-style-type: none"> <li>• <b>NACK</b></li> <li>• <b>NACK+RTX(SSRC-GROUP)</b></li> <li>• <b>OFF</b></li> </ul>
<b>Video FEC</b>	Check to enable Forward Error Correction (FEC) for Video.
<b>Audio FEC</b>	Check to enable Forward Error Correction (FEC) for Audio.
<b>Silence Suppression</b>	If enabled, the PBX will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the PBX will send DTX packets instead.
<b>FECC</b>	Configure to enable Remote Camera Management.
<b>ACL Policy</b>	<p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> <li>• <b>Allow All:</b> Any IP address can register to this extension.</li> <li>• <b>Local Network:</b> Only IP addresses in the configured network segments can register to this extension. Press "Add Local Network Address" to add more IP segments.</li> </ul>
<b>SRTP</b>	<p>Enable SRTP for the call. The default setting is disabled.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>Enabled and Enforced:</b> SRTP will be necessary to transmit media traffic. If the IP phone of this extension has SRTP disabled, calls cannot be established.</li> <li>• <b>Optional:</b> The PBX will negotiate whether to use SRTP or not. If the SIP endpoint has SRTP enabled, SRTP will be used. If it is disabled, SRTP will not be used.</li> </ul>
<b>SRTP Crypto Suite</b>	<p>SRTP encryption suite used by the PBX for outbound calls. Priority is based on order of configuration. The following encryption algorithms can be used to encrypt an RTP stream.</p> <ul style="list-style-type: none"> <li>• AES_CM_128_HMAC_SHA1_80 (This is the default algorithm used)</li> <li>• AES_256_CM_HMAC_SHA1_80</li> <li>• AEAD_AES_128_GCM</li> <li>• AEAD_AES_256_GCM</li> </ul>
<b>ZRTP</b>	<p>ZRTP, also known as Media Path Key Agreement for Secure RTP, is an encryption protocol which allows negotiating the encryption key for RTP traffic. ZRTP uses Diffie-Hellman exchange to establish an encrypted and secure connection between the PBX and the SIP endpoint.</p> <p>If the SIP endpoint has both SRTP and ZRTP enabled, ZRTP will always be prioritized.</p>

<b>Call Transfer</b>	
<b>Presence Status</b>	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].
<b>Internal Calls &amp; External Calls</b>	
<b>Call Forward Unconditional</b>	<p>Enable and configure the Call Forward Unconditional target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>• <b>"None"</b>: Call forward deactivated.</li> <li>• <b>"Extension"</b>: Select an extension from the dropdown list as CFU target.</li> <li>• <b>"Custom Number"</b>: Enter a customer number as a target. For example: *97.</li> <li>• <b>"Voicemail"</b>: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension.</li> <li>• <b>"Ring Group"</b>: Select a ring group from the dropdown list as CFU target.</li> <li>• <b>"Queues"</b>: Select a queue from the dropdown list as CFU target.</li> <li>• <b>"Voicemail Group"</b>: Select a voicemail group from the dropdown list as CFU target.</li> <li>• <b>Custom Prompt</b>: The call will be forwarded to a custom prompt.</li> </ul> <p>The default setting is "None".</p>
<b>CFU Time Condition</b>	<p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>• Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li> <li>• Office Time and Holiday could be configured on page <b>System Settings</b>→<b>Time Settings</b>→<b>Office Time/Holiday</b> page.</li> </ul>
<b>Call Forward No Answer</b>	<p>Configure the Call Forward No Answer target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>• <b>"None"</b>: Call forward deactivated.</li> <li>• <b>"Extension"</b>: Select an extension from the dropdown list as CFN target.</li> <li>• <b>"Custom Number"</b>: Enter a customer number as a target. For example: *97.</li> <li>• <b>"Voicemail"</b>: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension.</li> <li>• <b>"Ring Group"</b>: Select a ring group from the dropdown list as CFN target.</li> <li>• <b>"Queues"</b>: Select a queue from the dropdown list as CFN target.</li> <li>• <b>"Voicemail Group"</b>: Select a voicemail group from the dropdown list as CFN target.</li> <li>• <b>Custom Prompt</b>: The call will be forwarded to a custom prompt.</li> </ul> <p>The default setting is "None".</p>
<b>CFN Time Condition</b>	<p>Select time condition for Call Forward No Answer. The available time conditions are 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>• Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li> <li>• Office Time and Holiday could be configured on page <b>System Settings</b>→<b>Time Settings</b>→<b>Office Time/Holiday</b> page.</li> </ul>
<b>Call Forward Busy</b>	<p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>• <b>"None"</b>: Call forward deactivated.</li> <li>• <b>"Extension"</b>: Select an extension from the dropdown list as CFB target.</li> <li>• <b>"Custom Number"</b>: Enter a customer number as a target. For example: *97</li> <li>• <b>"Voicemail"</b>: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension.</li> <li>• <b>"Ring Group"</b>: Select a ring group from the dropdown list as CFB target.</li> <li>• <b>"Queues"</b>: Select a queue from the dropdown list as CFB target.</li> <li>• <b>"Voicemail Group"</b>: Select a voicemail group from dropdown list as CFB target.</li> </ul>

	<ul style="list-style-type: none"> <li>● <b>Custom Prompt:</b></li> </ul> <p>The default setting is <b>"None"</b>.</p>
<b>CFB Time Condition</b>	<p>Select time condition for Call Forward Busy. The available time conditions 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<b>Do Not Disturb</b>	<p>If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.</p>
<b>DND Time Condition</b>	<p>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".</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li> </ul> <p>Office Time and Holiday could be configured on page <b>System Settings→Time Settings→Office Time/Holiday</b> page.</p>
<b>DND Whitelist</b>	<p>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.</p> <ul style="list-style-type: none"> <li>● <b>Z</b> match any digit from 1-9.</li> <li>● <b>N</b> match any digit from 2-9.</li> <li>● <b>X</b> match any digit from 0-9.</li> </ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> <li>● <b>Z</b> match any digit from 1-9.</li> <li>● <b>N</b> match any digit from 2-9.</li> <li>● <b>X</b> match any digit from 0-9.</li> </ul>
<b>CC Settings</b>	
<b>Enable CC</b>	<p>If enabled, the PBX will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.</p>
<b>CC Mode</b>	<p>Two modes for Call Completion are supported:</p> <ul style="list-style-type: none"> <li>● <b>Normal:</b> This extension is used as an ordinary extension.</li> <li>● <b>For Trunk:</b> This extension is registered from a PBX.</li> </ul> <p>The default setting is "Normal".</p>
<b>CC Max Agents</b>	<p>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.</p> <p>The minimum value is 1.</p>
<b>CC Max Monitors</b>	<p>Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time.</p> <p>The minimum value is 1.</p>
<b>Ring Simultaneously</b>	
<b>Ring Simultaneously</b>	<p>Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.</p>

<b>External Number</b>	Set the external number to ring simultaneously. '-' is the connection character that will be ignored. This field accepts only letters, numbers, and special characters + = * #.
<b>Time Condition for Ring Simultaneously</b>	Ring the external number simultaneously along with the extension based on this time condition.
<b>Use callee DOD on FWD or RS</b>	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
<b>Monitor privilege control</b>	
<b>Call Monitoring Whitelist</b>	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
<b>Allow Operator Panel Monitoring</b>	Configure whether this extension can be monitored by the Operator Panel administrator.
<b>Seamless transfer privilege control</b>	
<b>Allowed to seamless transfer</b>	Any extensions on the PBX can perform a seamless transfer. When using the Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform a seamless transfer to the edited extension.
<b>PMS Remote Wakeup Whitelist</b>	
<b>Select the extensions that can set wakeup service for other extensions</b>	Selected extensions can set a PMS wakeup service for this extension via feature code.
<b>Other Settings</b>	
<b>Ring Timeout</b>	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the PBX. The valid range is between 5 seconds and 600 seconds. <b>Note:</b> If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
<b>Auto Record</b>	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under <b>Web GUI→CDR→Recording Files</b> .
<b>Skip Trunk Auth</b>	<ul style="list-style-type: none"> <li>• If set to "yes", users can skip entering the password when making outbound calls.</li> <li>• If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.</li> <li>• If set to "No", users will be asked to enter the password when making outbound calls.</li> </ul>
<b>Time Condition for Skip Trunk Auth</b>	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering the password when making outbound calls.
<b>Dial Trunk Password</b>	Configure personal password when making outbound calls via the trunk.
<b>Support Hot-Desking Mode</b>	Check to enable Hot-Desking Mode on the extension. Hot-Desking allows using the same endpoint device and logs in using extension/password combination. This feature is used in scenarios where different users need to use the same endpoint device during a different time of the day for instance. If enabled, SIP Password will accept only alphabet characters and digits. Auth ID will be changed to the same as Extension.
<b>Enable LDAP</b>	If enabled, the extension will be added to the LDAP Phonebook PBX list. Default is enabled.

<b>Use MOH as IVR ringback tone</b>	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
<b>Music On Hold</b>	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
<b>Call Duration Limit</b>	Check to enable and set the call limit the duration.
<b>Maximum Call Duration (s)</b>	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
<b>The Maximum Number of Call Lines</b>	The maximum number of simultaneous calls that the extension can have. 0 indicates no limit.
<b>Outgoing Call Frequency Limit</b>	If enabled, if the number of outbound calls exceed the configured threshold within the specified period, further outbound calls will be not be allowed.
<b>Send PCPID Header</b>	If enabled, this extension's SIP INVITE messages will contain the P-Called-Party-ID (PCPID) header if the callee is a SIP device.
<b>Period (m)</b>	The period of outgoing call frequency limit. The valid range is from 1 to 120. The default value is 1.
<b>Max Number of Calls</b>	Set the maximum number of outgoing calls in a period. The valide tange is from 1 to 20. The default value is 5.
<b>Enable Auto-Answer Support</b>	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
<b>Call Waiting</b>	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.
<b>Stop Ringing</b>	If enabled, when the extension has concurrent registrations on multiple devices, upon incoming call or meeting invite ringing, if one end device rejects the call, the rest of the devices will also stop ringing. By default, it's disabled.
<b>Email Missed Call Log</b>	If enabled, the log of missed calls will be sent to the extension's configured email address.
<b>Missed Call Type</b>	<p>If <b>Email Missed Calls</b> enabled, users can select the type of missed calls to be sent via email, the available types are:</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> All missed calls will be sent in email notifications.</li> <li>• <b>Missed Internal Call:</b> Only missed local extension-to-extension calls will be sent in email notifications.</li> <li>• <b>Missed External Call:</b> Only missed calls from trunks will be sent in email notifications.</li> </ul>

*SIP Extension Configuration Parameters → Features*

<b>Specific Time</b>	
<b>Time Condition</b>	Click to add Time Condition to configure specific time for this extension.

*SIP Extension Configuration Parameters → Custom Time*

<b>Normal</b>	
<b>Enable Wave</b>	Enable Wave for the specific extension.

<b>Allow Concurrent Logins from the Same Client Type</b>	<p>Enables/disables the ability to login to Wave from different sessions on the same type of client</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Concurrent Registrations limit for the SIP extension will still apply.</li> <li>• When this option is enabled, Concurrent Registrations cannot be configured as "1 (Allowed to Seize)"</li> <li>• This option is disabled by default.</li> </ul>
<b>Multi-Factor Authentication</b>	<p>When this option is enabled, the extension user will be prompted to configure multi-factor authentication on their account when they log in using Wave.</p> <p>To ensure enabling multi-factor authentication successfully, please refer to the minimum version required below for Wave on each platform</p> <ul style="list-style-type: none"> <li>• <b>Wave Web:</b> 1.0.27.12 and later</li> <li>• <b>Wave Desktop:</b> 1.27.10 and later</li> <li>• <b>Wave App for Android™:</b> 1.0.27.18 and later</li> <li>• <b>Wave App for iOS™:</b> 1.27.24 and later</li> </ul>
<b>Wave Welcome Email</b>	Wave Welcome Email template.
<b>Wave Permission Settings</b>	Clicking the path will direct you to Wave Permission configuration.
<b>Wave</b>	
<b>Download Link</b>	<a href="https://fw.gdms.cloud/wave/download/">https://fw.gdms.cloud/wave/download/</a>

*SIP Extension Configuration Parameters → Wave Client*

<b>Follow Me</b>	
<b>Enable</b>	Configure to enable or disable Follow Me for this user.
<b>Skip Trunk Auth</b>	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.
<b>Music On Hold Class</b>	Configure the Music On Hold class that the caller would hear while tracking the user.
<b>Confirm When Answering</b>	If enabled, call will need to be confirmed after answering.
<b>Enable Destination</b>	Configure to enable destination
<b>Default Destination</b>	The call will be routed to this destination if no one in the Follow Me answers the call.
<b>Use Callee DOD for Follow Me</b>	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
<b>Play Follow Me Prompt</b>	If enabled, the Follow Me prompt tone will be played
<b>New Follow Me Number</b>	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.
<b>Dialing Order</b>	This is the order in which the Follow Me destinations will be dialed to reach the user.

*SIP Extension Configuration Parameters → Follow Me*

## Create New IAX Extension

The UCM630xA 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.

General	
<b>Extension</b>	The extension number associated with the user.
<b>CallerID Number</b>	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.
<b>Privilege</b>	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". <b>Note:</b> Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
<b>SIP/IAX Password</b>	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.
<b>Voicemail</b>	Configure Voicemail. There are three valid options, and the default option is "Enable Local Voicemail". <ul style="list-style-type: none"> <li>• <b>Disable Voicemail:</b> Disable Voicemail.</li> <li>• <b>Enable Local Voicemail:</b> Enable voicemail for the user.</li> </ul>
<b>Voicemail Password</b>	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
<b>Skip Voicemail Password Verification</b>	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
<b>Send Voicemail Email Notification</b>	Configures whether to send emails to the extension's email address to notify of a new voicemail.
<b>Attach Voicemail to Email</b>	Configures whether to attach a voicemail audio file to the voicemail notification emails.
<b>Keep Voicemail after E-mailing</b>	Only applies if extension-level or global Send Voicemail to Email is enabled.
<b>Disable This Extension</b>	If selected, this extension will be disabled on the UCM630X. <b>Note:</b> The disabled extension still exists on the PBX but cannot be used on the end device.
User Settings	
<b>First Name</b>	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
<b>Last Name</b>	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
<b>Email Address</b>	Fill in the Email address for the user. Voicemail will be sent to this Email address.
<b>User Password</b>	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.
<b>Language</b>	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under <b>Web GUI→PBX Settings→Voice Prompt→Language Settings</b> . The dropdown list shows all the currently available voice prompt languages on the UCM630X. To add more languages to the list, please download the voice prompt package by selecting "Check Prompt List" under <b>Web GUI→PBX Settings→Voice Prompt→Language Settings</b> .
<b>Mobile Phone Number</b>	Configure the Mobile number of the user.

IAX Settings	
<b>Max Number of Calls</b>	Configure the maximum number of calls allowed for each remote IP address.
<b>Require Call Token</b>	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".
<b>SRTP</b>	Enable SRTP for the call. The default setting is disabled.
<b>ACL Policy</b>	<p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> <li>● <b>Allow All:</b> Any IP address can register to this extension.</li> <li>● <b>Local Network:</b> Only IP addresses in the configured network segments can register to this extension.</li> </ul>
<b>Codec Preference</b>	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.

Call Transfer	
<b>Call Forward Unconditional</b>	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
<b>CFU Time Condition</b>	<p>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".</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page <b>System Settings→Time Settings→Office Time/Holiday</b> page.</li> </ul>
<b>Call Forward No Answer</b>	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
<b>CFN Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page <b>System Settings→Time Settings→Office Time/Holiday</b> page.</li> </ul>
<b>Call Forward Busy</b>	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
<b>CFB Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> </ul> <p>Office Time and Holiday could be configured on page <b>System Settings→Time Settings→Office Time/Holiday</b> page.</p>

<b>Do Not Disturb</b>	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
<b>DND Time Condition</b>	The time condition of DND. The DND will take effect while the time condition is satisfied.
<b>DND Whitelist</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Z</b> match any digit from 1-9.</li> <li>• <b>N</b> match any digit from 2-9.</li> <li>• <b>X</b> match any digit from 0-9.</li> </ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> <li>• <b>Z</b> match any digit from 1-9.</li> <li>• <b>N</b> match any digit from 2-9.</li> <li>• <b>X</b> match any digit from 0-9.</li> </ul>
<b>Ring Simultaneously</b>	
<b>Ring Simultaneously</b>	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
<b>External Number</b>	Set the external number to ring simultaneously. '-' is the connection character that will be ignored.
<b>Time Condition for Ring Simultaneously</b>	Ring the external number simultaneously along with the extension based on this time condition.
<b>Use callee DOD on FWD or RS</b>	Use the callee's DOD number as CallerID on Outgoing Forwarding or Ring Simultaneously calls.
<b>Monitor Privilege Control</b>	
<b>Call Monitoring Whitelist</b>	Members of the list can spy on this extension via feature codes.
<b>Seamless transfer privilege control</b>	
<b>Allowed to seamless transfer</b>	Members of the list can seamlessly transfer via feature code.
<b>Other Settings</b>	
<b>Ring Timeout</b>	<p>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.</p> <p><b>Note:</b> If the endpoint also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
<b>Auto Record</b>	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under <b>Web GUI→CDR→Recording Files</b> .
<b>Skip Trunk Auth</b>	<ul style="list-style-type: none"> <li>• If set to "Yes", users can skip entering the password when making outbound calls.</li> <li>• If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.</li> <li>• If set to "No", users will be asked to enter the password when making outbound calls.</li> </ul>

<b>Time Condition for Skip Trunk Auth</b>	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering the password when making outbound calls.
<b>Dial Trunk Password</b>	Configure personal password when making outbound calls via the trunk.
<b>Enable LDAP</b>	If enabled, the extension will be added to LDAP Phonebook PBX lists.
<b>Music On Hold</b>	Configure the Music On Hold class to suggest to the bridged channel when putting them on hold.
<b>Use MOH as IVR ringback tone</b>	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
<b>Call Duration Limit</b>	Check to enable and set the call limit the duration.
<b>Maximum Call Duration (s)</b>	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
<b>Email Missed Calls</b>	Send a log of missed calls to the extension's email address.
<b>Missed Call Type</b>	<p>If <b>Email Missed Calls</b> enabled, users can select the type of missed calls to be sent via email, the available types are:</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> All missed calls will be sent in email notifications.</li> <li>• <b>Missed Internal Call:</b> Only missed local extension-to-extension calls will be sent in email notifications.</li> <li>• <b>Missed External Call:</b> Only missed calls from trunks will be sent in email notifications.</li> </ul>

<b>Specific Time</b>	
<b>Time Condition</b>	Click to add Time Condition to configure a specific time for this extension.

<b>Follow Me</b>	
<b>Enable</b>	Configure to enable or disable Follow Me for this user.
<b>Skip Trunk Auth</b>	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.
<b>Music On Hold Class</b>	Configure the Music On Hold class that the caller would hear while tracking the user.
<b>Confirm When Answering</b>	If enabled, call will need to be confirmed after answering.
<b>Enable Destination</b>	Configure to enable destination.
<b>Default Destination</b>	The call will be routed to this destination if no one in the Follow Me answers the call.
<b>Use Callee DOD for Follow Me</b>	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
<b>Play Follow Me Prompt</b>	If enabled, the Follow Me prompt tone will be played.
<b>New Follow Me Number</b>	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.
<b>Dialing Order</b>	This is the order in which the Follow Me destinations will be dialed to reach the user.

## Create New FXS Extension

The UCM630xA supports Foreign eXchange Subscriber (FXS) interface. FXS is used when user needs to connect analog phone lines or FAX machines to the UCM630xA.

### Note

Please note that the UCM6300A does not offer FXS extensions.

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.

General	
<b>Extension</b>	The extension number associated with the user.
<b>Analog Station</b>	Select the FXS port to be assigned for this extension.
<b>Caller ID Number</b>	Configure the CallerID Number that would be applied for outbound calls from this user. <b>Note:</b> The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
<b>Privilege</b>	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”. <b>Note:</b> Users need to have the same level as or higher level than an outbound rule’s privilege to make outbound calls using this rule.
<b>Voicemail</b>	Configure Voicemail. There are three valid options, and the default option is “Enable Local Voicemail”. <ul style="list-style-type: none"><li>• <b>Disable Voicemail:</b> Disable Voicemail.</li><li>• <b>Enable Local Voicemail:</b> Enable voicemail for the user.</li></ul>
<b>Voicemail Password</b>	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
<b>Skip Voicemail Password Verification</b>	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
<b>Send Voicemail Email Notification</b>	Configures whether to send emails to the extension’s email address to notify of a new voicemail.
<b>Attach Voicemail to Email</b>	Configures whether to attach a voicemail audio file to the voicemail notification emails.
<b>Keep Voicemail after Emailing</b>	Only applies if extension-level or global Send Voicemail to Email is enabled.
<b>Emergency CID Name</b>	CallerID name that will be used for emergency calls and callbacks.
<b>Disable This Extension</b>	If selected, this extension will be disabled on the UCM630X. <b>Note:</b> The disabled extension still exists on the PBX but cannot be used on the end device.

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

Analog Settings	
<b>Call Waiting</b>	Configure to enable/disable call waiting feature. The default setting is "No".
<b>User '#' as SEND</b>	If configured, the # key can be used as SNED key after dialing the number on the analog phone. The default setting is "Yes".
<b>RX Gain</b>	Configure the RX gain for the receiving channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.
<b>TX Gain</b>	Configure the TX gain for the transmitting channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.
<b>Min RX Flash</b>	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.
<b>Max RX Flash</b>	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.
<b>Enable Polarity Reversal</b>	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".
<b>Echo Cancellation</b>	Specify "ON", "OFF" or a value (the power of 2) from 32 to 1024 as the number of taps of cancellation. <b>Note:</b> 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.
<b>3-Way Calling</b>	Configure to enable/disable the 3-way calling feature on the user. The default setting is enabled.
<b>Send CallerID After</b>	Configure the number of rings before sending CID. The default setting is 1.
<b>Fax Mode</b>	For the FXS extension, there are three options available in Fax Mode. The default setting is "None". <ul style="list-style-type: none"> <li>● <b>None:</b> Disable Fax.</li> <li>● <b>Fax Gateway:</b> If selected, the UCM630X can support the conversation and processing of Fax data from T.30 to T.38 or T.38 to T.30. only for FXS ports.</li> </ul>

- **Fax Detection:** During a call, the fax signal from the user/trunk will be detected, and the received fax will be sent to the email address configured for the user. If an email address has been configured for the user, the fax will be sent to the Default Email Address configured in **Fax/T.38->Fax Settings**.

Call Transfer	
<b>Call Forward Unconditional</b>	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
<b>CFU Time Condition</b>	<p>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".</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page <b>System Settings-&gt;Time Settings-&gt;Office Time/Holiday page</b>.</li> </ul>
<b>Call Forward No Answer</b>	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
<b>CFN Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page <b>System Settings-&gt;Time Settings-&gt;Office Time/Holiday page</b>.</li> </ul>
<b>Call Forward Busy</b>	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
<b>CFB Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>● Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time.</li> <li>● Office Time and Holiday could be configured on page <b>System Settings-&gt;Time Settings-&gt;Office Time/Holiday page</b>.</li> </ul>
<b>Do Not Disturb</b>	<p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p>
<b>DND Time Condition</b>	The time condition of DND. The DND will take effect while the time condition is satisfied.
<b>DND Whitelist</b>	<p>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.</p> <ul style="list-style-type: none"> <li>● <b>Z</b> match any digit from 1-9.</li> <li>● <b>N</b> match any digit from 2-9.</li> <li>● <b>X</b> match any digit from 0-9.</li> </ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded.</p> <p>Pattern matching is supported.</p> <ul style="list-style-type: none"> <li>● <b>Z</b> match any digit from 1-9.</li> <li>● <b>N</b> match any digit from 2-9.</li> </ul>

- **X** match any digit from 0-9.

### CC Settings

#### Enable CC

If enabled, UCM630X will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason.

### Ring Simultaneously

#### Ring Simultaneously

Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.

#### External Number

Set the external number to ring simultaneously. '-' is the connection character that will be ignored.

#### Time Condition for Ring Simultaneously

Ring the external number simultaneously along with the extension based on this time condition.

#### Use callee DOD on FWD or RS

Use the callee's DOD number as CallerID on Outgoing Forwarding or Ring Simultaneously calls.

### Hotline

#### Enable Hotline

If enabled, a hotline dialing plan will be activated, a pre-configured number will be used according to the selected Hotline Type.

#### Hotline Number

Configure the Hotline Number

#### Hotline Type

Configure the Hotline Type:

- **Immediate Hotline:** When the phone is off-hook, UCM630X will immediately dial the preset number
- **Delay Hotline:** When the phone is off hook, if there is no dialing within 5 seconds, UCM630X will dial the preset number.

#### Monitor privilege control

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 endpoint also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.

#### Auto Record

Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under **Web GUI→CDR→Recording Files**.

#### Skip Trunk Auth

- If set to "Yes", users can skip entering the password when making outbound calls.
- If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.
- If set to "No", users will be asked to enter the password when making outbound calls.

<b>Time Condition for Skip Trunk Auth</b>	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering a password when making outbound calls.
<b>Dial Trunk Password</b>	Configure personal password when making outbound calls via the trunk.
<b>Enable LDAP</b>	If enabled, this extension will be added to the LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
<b>Use MOH as IVR ringback tone</b>	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
<b>Music On Hold</b>	Select which Music On Hold class to suggest to the extension when putting the active call on hold.
<b>Call Duration Limit</b>	Check to enable and set the call limit the duration.
<b>Maximum Call Duration (s)</b>	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
<b>Email Missed Calls</b>	Send a log of missed calls to the extension's email address.
<b>Missed Call Type</b>	<p>If <b>Email Missed Calls</b> enabled, users can select the type of missed calls to be sent via email, the available types are:</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> All missed calls will be sent in email notifications.</li> <li>• <b>Missed Internal Call:</b> Only missed local extension-to-extension calls will be sent in email notifications.</li> <li>• <b>Missed External Call:</b> Only missed calls from trunks will be sent in email notifications.</li> </ul>

<b>Specific Time</b>	
<b>Time Condition</b>	Click to add Time Condition to configure a specific time for this extension.

<b>Follow Me</b>	
<b>Enable</b>	Configure to enable or disable Follow Me for this user.
<b>Skip Trunk Auth</b>	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.
<b>Music On Hold Class</b>	Configure the Music On Hold class that the caller would hear while tracking the user.
<b>Confirm When Answering</b>	If enabled, call will need to be confirmed after answering.
<b>Enable Destination</b>	Configure to enable destination.
<b>Default Destination</b>	The call will be routed to this destination if no one in the Follow Me answers the call.
<b>Use Callee DOD for Follow Me</b>	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
<b>Play Follow Me Prompt</b>	If enabled, the Follow Me prompt tone will be played.
<b>New Follow Me Number</b>	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.
<b>Dialing Order</b>	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.

General	
<b>Create Number</b>	Specify the number of extensions to be added. The default setting is 5.
<b>Extension Incrementation</b>	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,..... <b>Note:</b> Up to 3 characters.
<b>Extension</b>	Configure the starting extension number of the batch of extensions to be added.
<b>Permission</b>	<p>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”.</p> <p><b>Note:</b> Users need to have the same level as or higher level than an outbound rule’s privilege to make outbound calls from this rule.</p>
<b>Voicemail</b>	<p>Configure Voicemail.</p> <p>There are three valid options and the default option is “Enable Local Voicemail”.</p> <ul style="list-style-type: none"><li>○ <b>Disable Voicemail:</b> Disable Voicemail.</li><li>○ <b>Enable Local Voicemail:</b> Enable voicemail for the user.</li><li>○ <b>Enable Remote Voicemail:</b> 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).</li></ul>
<b>SIP/IAX Password</b>	<p>Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"><li>○ User Random Password.</li></ul> <p>A random secure password will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"><li>○ Use Extension as Password.</li><li>○ Enter a password to be used on all the extensions in the batch.</li></ul>
<b>Voicemail Password</b>	<p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"><li>○ User Random Password.</li></ul> <p>A random password in digits will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"><li>○ Use Extension as Password.</li></ul> <p>Enter a password to be used on all the extensions in the batch.</p>
<b>Send Voicemail to Email</b>	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.

<b>Keep Voicemail after Emailing</b>	Only applies if extension-level or global Send Voicemail to Email is enabled.
<b>CallerID Number</b>	<p>Configure CallerID Number when adding Batch Extensions.</p> <ul style="list-style-type: none"> <li>○ Use Extension as Number</li> <li>○ Users can choose to use the extension number as CallerID</li> <li>○ Use as Number</li> <li>○ Users can choose to set a specific number instead of using the extension number.</li> </ul>
<b>Skip Voicemail Password Verification</b>	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.
<b>Enable Keep-alive</b>	If enabled, the PBX will regularly send SIP OPTIONS to check if host device is online.
<b>Keep-alive Frequency</b>	Configure the keep-alive interval (in seconds) to check if the host is up.
<b>Disable This Extension</b>	Check this box to disable this extension.
<b>Enable SCA</b>	If enabled, (1) Call Forward, Call Waiting and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Advanced Call Features->SCA page.
<b>Emergency Calls CID</b>	CallerID number that will be used when calling out and receiving direct callbacks.
<b>Enable Wave</b>	If enabled, this extension number can register, log in and use Wave normally, otherwise it will not be able to use Wave, but the phone function will still be retained.
<b>Sync Contact</b>	If enabled, this extension number will be displayed in the Wave contact, otherwise it will not be displayed, and it cannot be found in the chat, but the user can still dial this number.
<b>Language</b>	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.
<b>Media</b>	
<b>NAT</b>	<p>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.</p> <p>The default setting is enabled.</p>
<b>Enable Direct Media</b>	By default, the PBX will route the media streams 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".
<b>DTMF Mode</b>	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.
<b>Alert-info</b>	When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS.
<b>SRTP</b>	Enable/disable SRTP for RTP stream encryption.
<b>Packet Loss Retransmission</b>	<p>Configure to enable Packet Loss Retransmission.</p> <ul style="list-style-type: none"> <li>○ NACK</li> <li>○ NACK+RTX(SSRC-GROUP)</li> <li>○ OFF</li> </ul>
<b>Video FEC</b>	Check to enable Forward Error Correction (FEC) for Video.
<b>FECC</b>	Configure to enable FECC
<b>Audio FEC</b>	Check to enable Forward Error Correction (FEC) for Audio.

<b>ACL Policy</b>	<p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> <li>○ Allow All: Any IP address can register to this extension.</li> <li>○ 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.</li> </ul>
<b>Jitter Buffer</b>	<p>Select jitter buffer method.</p> <ul style="list-style-type: none"> <li>○ Disable: Jitter buffer will not be used.</li> <li>○ Fixed: Jitter buffer with a fixed size (equal to the value of "jitter buffer size")</li> <li>○ Adaptive: Jitter buffer with an adaptive size (no more than the value of "max jitter buffer").</li> <li>○ NetEQ: Dynamic jitter buffer via NetEQ.</li> </ul>
<b>Codec Preference</b>	<p>Configure the codecs to be used.</p>
<b>Call Transfer</b>	
<b>Presence Status</b>	<p>Select which presence status to set for the extension and configure call forward conditions for each status. Six possible options are possible: <b>"Available"</b>, <b>"Away"</b>, <b>"Chat"</b>, <b>"Custom"</b>, <b>"DND"</b> and <b>"Unavailable"</b>. More details at [PRESENCE].</p>
<b>Call Forward Unconditional</b>	<p>Enable and configure the Call Forward Unconditional target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>○ <b>"None"</b>: Call forward deactivated.</li> <li>○ <b>"Extension"</b>: Select an extension from dropdown list as CFU target.</li> <li>○ <b>"Custom Number"</b>: Enter a customer number as target. For example: *97.</li> <li>○ <b>"Voicemail"</b>: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension.</li> <li>○ <b>"Ring Group"</b>: Select a ring group from dropdown list as CFU target.</li> <li>○ <b>"Queues"</b>: Select a queue from dropdown list as CFU target.</li> <li>○ <b>"Voicemail Group"</b>: Select a voicemail group from dropdown list as CFU target.</li> </ul> <p>The default setting is "None".</p>
<b>CFU Time Condition</b>	<p>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".</p> <p>Note:</p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>

<p><b>Call Forward No Answer</b></p>	<p>Configure the Call Forward No Answer target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>○ <b>"None"</b>: Call forward deactivated.</li> <li>○ <b>"Extension"</b>: Select an extension from dropdown list as CFN target.</li> <li>○ <b>"Custom Number"</b>: Enter a customer number as target. For example: *97.</li> <li>○ <b>"Voicemail"</b>: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension.</li> <li>○ <b>"Ring Group"</b>: Select a ring group from dropdown list as CFN target.</li> <li>○ <b>"Queues"</b>: Select a queue from dropdown list as CFN target.</li> <li>○ <b>"Voicemail Group"</b>: Select a voicemail group from dropdown list as CFN target.</li> </ul> <p>The default setting is "None".</p>
<p><b>CFN Time Condition</b></p>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<p><b>Call Forward Busy</b></p>	<p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"> <li>○ <b>"None"</b>: Call forward deactivated.</li> <li>○ <b>"Extension"</b>: Select an extension from dropdown list as CFB target.</li> <li>○ <b>"Custom Number"</b>: Enter a customer number as target. For example: *97.</li> <li>○ <b>"Voicemail"</b>: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension.</li> <li>○ <b>"Ring Group"</b>: Select a ring group from dropdown list as CFB target.</li> <li>○ <b>"Queues"</b>: Select a queue from dropdown list as CFB target.</li> <li>○ <b>"Voicemail Group"</b>: Select a voicemail group from dropdown list as CFB target.</li> </ul> <p>The default setting is "None".</p>
<p><b>CFB Time Condition</b></p>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<p><b>Do Not Disturb</b></p>	<p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p>

<b>DND Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> </ul> <p>Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</p>
<b>DND Whitelist</b>	<p>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.</p> <ul style="list-style-type: none"> <li>○ Z match any digit from 1-9</li> <li>○ N match any digit from 2-9</li> <li>○ X match any digit from 0-9.</li> </ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> <li>○ Z match any digit from 1-9</li> <li>○ N match any digit from 2-9</li> <li>○ X match any digit from 0-9.</li> </ul>
<b>CC Settings</b>	
<b>Enable CC</b>	<p>If enabled, UCM630xA 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.</p>
<b>CC Mode</b>	<p>Two modes for Call Completion are supported:</p> <ul style="list-style-type: none"> <li>○ <b>Normal:</b> This extension is used as ordinary extension.</li> <li>○ <b>For Trunk:</b> This extension is registered from a PBX.</li> </ul> <p>The default setting is "Normal".</p>
<b>CC Max Agents</b>	<p>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.</p>
<b>CC Max Monitors</b>	<p>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.</p>
<b>Ring Simultaneously</b>	
<b>Ring Simultaneously</b>	<p>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.</p>
<b>External Number</b>	<p>Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p>
<b>Time Condition for Ring Simultaneously</b>	<p>Ring the external number simultaneously along with the extension on the basis of this time condition.</p>
<b>Use callee DOD on FWD or RS</b>	<p>Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.</p>
<b>Monitor privilege control</b>	

<b>Allowed to call-barging</b>	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
<b>Seamless transfer privilege control</b>	
<b>Allowed to seamless transfer</b>	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.
<b>Other Settings</b>	
<b>Ring Timeout</b>	<p>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 UCM630xA, 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.</p> <p><b>Note:</b> If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
<b>Auto Record</b>	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.
<b>Skip Trunk Auth</b>	<ul style="list-style-type: none"> <li>○ If set to "yes", users can skip entering the password when making outbound calls.</li> <li>○ If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.</li> <li>○ If set to "No", users will be asked to enter the password when making outbound calls.</li> </ul>
<b>Time Condition for Skip Trunk Auth</b>	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
<b>Dial Trunk Password</b>	Configure personal password when making outbound calls via trunk.
<b>Enable LDAP</b>	If enabled, the extension will be added to LDAP Phonebook PBX list.
<b>Bind PMS Room</b>	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.
<b>Music On Hold</b>	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
<b>Call Duration Limit</b>	The maximum duration of call-blocking.
<b>Maximum Call Duration</b>	The maximum call duration (in seconds). The default value 0 means no limit.
<b>Call Waiting</b>	<p>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.</p> <p><b>Note:</b> the option only works when the caller dials the extension directly.</p>

*Batch Add SIP Extension Parameters*

## 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.

<b>General</b>	
<b>Create Number</b>	Specify the number of extensions to be added. The default setting is 5.
<b>Extension Incrementation</b>	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,.....
<b>Extension</b>	The extension number associated with this particular user/phone.

<b>Permission</b>	<p>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".</p> <p><b>Note:</b> 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.</p>
<b>CallerID Number</b>	<p>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.</p>
<b>Voicemail</b>	<p>Configure Voicemail. There are three valid options and the default option is "Enable Local Voicemail".</p> <p>Disable Voicemail: Disable Voicemail.</p> <p>Enable Local Voicemail: Enable voicemail for the user.</p>
<b>SIP/IAX Password</b>	<p>Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"> <li>○ User Random Password.</li> </ul> <p>A random secure password will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> <li>○ Use Extension as Password.</li> <li>○ Enter a password to be used on all the extensions in the batch.</li> </ul>
<b>Voicemail Password</b>	<p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"> <li>○ User Random Password.</li> </ul> <p>A random password in digits will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> <li>○ Use Extension as Password.</li> <li>○ Enter a password to be used on all the extensions in the batch.</li> </ul>
<b>Send Voicemail to Email</b>	<p>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-&gt;Voicemail Email Settings.</p>
<b>Keep Voicemail after Emailing</b>	<p>Only applies if extension-level or global Send Voicemail to Email is enabled.</p>
<b>Auto Record</b>	<p>Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→<b>CDR</b>→<b>Recording Files</b>.</p>
<b>Skip Voicemail Password Verification</b>	<p>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.</p>
<b>Disable This Extension</b>	<p>Check this box to disable this extension.</p>
<b>Language</b>	<p>Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.</p>
<b>IAX Settings</b>	
<b>Max Number of Calls</b>	<p>Configure the maximum number of calls allowed for each remote IP address.</p>

<b>Require Call Token</b>	<p>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.</p> <p>The default setting is "Yes".</p>
<b>SRTP</b>	<p>Enable/disable SRTP for RTP stream encryption.</p>
<b>ACL Policy</b>	<p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> <li>○ <b>Allow All:</b> Any IP address can register to this extension.</li> <li>○ <b>Local Network:</b> Only IP addresses in the configured network segments can register to this extension.</li> </ul>
<b>Codec Preference</b>	<p>Configure the codecs to be used.</p>
<b>Call Transfer</b>	
<b>Call Forward Unconditional</b>	<p>Enable and configure the Call Forward Unconditional target number.</p>
<b>CFU Time Condition</b>	<p>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".</p> <p>Note:</p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<b>Call Forward No Answer</b>	<p>Configure the Call Forward No Answer target number.</p>
<b>CFN Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<b>Call Forward Busy</b>	<p>Configure the Call Forward Busy target number.</p>
<b>CFB Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>

<b>Do Not Disturb</b>	<p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p>
<b>DND Time Condition</b>	<p>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".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>○ "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.</li> <li>○ Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time.</li> <li>○ Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</li> </ul>
<b>DND Whitelist</b>	<p>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.</p> <ul style="list-style-type: none"> <li>○ Z match any digit from 1-9,</li> <li>○ N match any digit from 2-9,</li> <li>○ X match any digit from 0-9.</li> </ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> <li>○ Z match any digit from 1-9,</li> <li>○ N match any digit from 2-9,</li> <li>○ X match any digit from 0-9.</li> </ul>
<b>Ring Simultaneously</b>	
<b>Ring Simultaneously</b>	<p>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.</p>
<b>External Number</b>	<p>Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p>
<b>Time Condition for Ring Simultaneously</b>	<p>Ring the external number simultaneously along with the extension on the basis of this time condition.</p>
<b>Use callee DOD on FWD or RS</b>	<p>Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.</p>
<b>Monitor privilege control</b>	
<b>Allowed to call-barging</b>	<p>Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.</p>
<b>Seamless transfer privilege control</b>	
<b>Allowed to seamless transfer</b>	<p>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.</p>
<b>Other Settings</b>	

<b>Ring Timeout</b>	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 UCM630xA, 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.  <b>Note:</b> If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
<b>Auto Record</b>	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.
<b>Skip Trunk Auth</b>	<ul style="list-style-type: none"> <li>○ If set to "yes", users can skip entering the password when making outbound calls.</li> <li>○ If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.</li> <li>○ If set to "No", users will be asked to enter the password when making outbound calls.</li> </ul>
<b>Time Condition for Skip Trunk Auth</b>	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
<b>Dial Trunk Password</b>	Configure personal password when making outbound calls via trunk.
<b>Enable LDAP</b>	If enabled, the extension will be added to LDAP Phonebook PBX list.
<b>Music On Hold</b>	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
<b>Call Duration Limit</b>	Check to enable and set the call limit the duration.
<b>Maximum Call Duration (s)</b>	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds

#### *Batch Add IAX Extension Parameters*

## Batch Extension Resetting Functionality

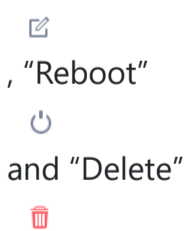
Users can select multiple extensions and reset their settings to default by pressing the reset button



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 UCM630xA 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"



are available per extension. User can search an extension by specifying the extension number to find an extension quickly.

Extensions									
<span>+ Add</span> <span>Edit</span> <span>Delete</span> <span>Edit All SIP</span> <span>E-mail Notification</span> <span>More</span> <input type="text" value="Extension Number or Name"/> <span>Search</span>									
<input type="checkbox"/>	STATUS	PRESENC...	EXTENSION	NAME	MESSAGE	TYPE	IP AND PORT	EXTENSION I...	OPTIONS
<input type="checkbox"/>	● Unavailable Available		1000		0/0/0	SIP(WebRT...	--		
<input type="checkbox"/>	● Idle	Available	1001		0/1/0	SIP(WebRT...	192.168.5.10...		
<input type="checkbox"/>	● Unavailable Available		1002		0/0/0	SIP(WebRT...	--		
<input type="checkbox"/>	● Unavailable Available		1003		0/0/0	SIP(WebRT...	--		
<input type="checkbox"/>	● Unavailable Available		1004		0/0/0	SIP(WebRT...	--		

Total: 5  Goto

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

### Manage Extensions

#### o 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)

#### o Edit single extension

Click on



to start editing the extension parameters.

#### o 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.

#### **i** Note

This is the expected behavior when you reset an extension:

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

- **Reboot the user**

Click on



to send NOTIFY reboot event to the device which has an UCM630xA extension already registered. To successfully reboot the user, "Zero Config" needs to be enabled on the UCM630xA Web GUI → **Device Management** → **Zero Config** → **Zero Config Settings**.

- **Delete single extension**

Click on



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

**Notes**

This is the expected behavior when you delete an extension:

- The system will delete all the data of the extension except the CDR and meetings record. All the data on the user side will be erased.
- The extension will be removed from group chats and the messages sent previously by the extension will be kept. However, only other users can search through those messages while the new user of the extension cannot.
- If the extension was in a meeting schedule, the meeting will still be present. The extension will be removed from the meeting and will not be notified about the meeting.

- **Modify selected extensions**

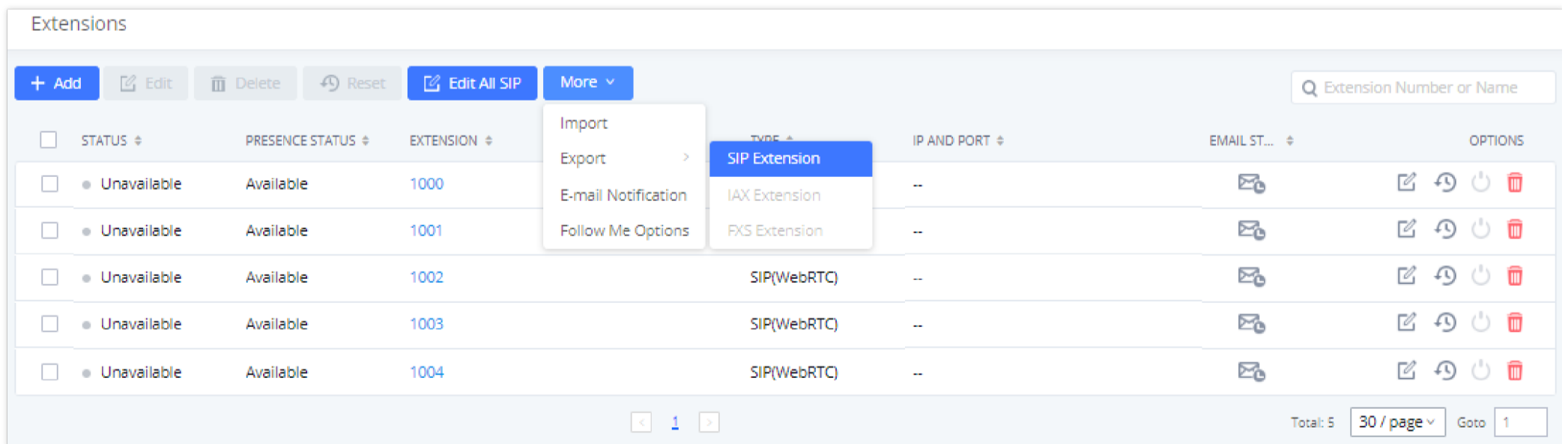
Select the checkbox for the extension(s). Then click on "Edit" to edit the extensions in a batch.

- **Delete selected extensions**

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

## Export Extensions

The extensions configured on the UCM630xA 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.



Export Extensions

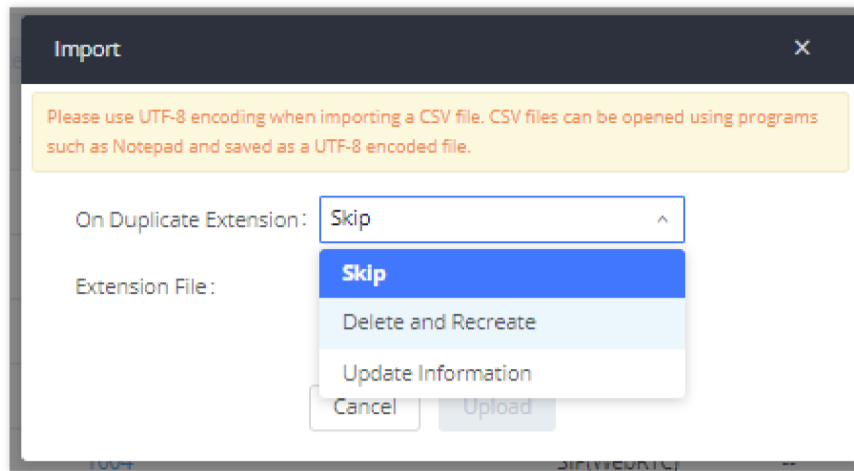
The exported csv file can serve as a template for users to fill in desired extension information to be imported to the UCM630xA.

## Import Extensions

The capability to import extensions to the UCM630xA provides users flexibility to batch add extensions with similar or different configuration quickly into the PBX system.

1. Export extension csv file from the UCM630xA 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.



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.
  - o **Skip:** Duplicate extensions in the csv file will be skipped. The PBX will keep the current extension information as previously configured without change.
  - o **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.
  - o **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 UCM630xA.

Example of file to import:

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

Import File

Field	Supported values
<b>Extension</b>	Digits
<b>Technology</b>	SIP/SIP(WebRTC)
<b>Enable Voicemail</b>	yes/no/remote
<b>CallerID Number</b>	Digits
<b>SIP/IAX Password</b>	Alphanumeric characters
<b>Voicemail Password</b>	Digits
<b>Skip Voicemail Password Verification</b>	yes/no
<b>Ring Timeout</b>	Empty/ 3 to 600 (in second)
<b>SRTP</b>	yes/no
<b>Strategy</b>	Allow All/Local Subnet Only/A Specific IP Address
<b>Local Subnet 1</b>	IP address/Mask
<b>Local Subnet 2</b>	IP address/Mask
<b>Local Subnet 3</b>	IP address/Mask
<b>Local Subnet 4</b>	IP address/Mask
<b>Local Subnet 5</b>	IP address/Mask
<b>Local Subnet 6</b>	IP address/Mask
<b>Local Subnet 7</b>	IP address/Mask

<b>Local Subnet 8</b>	IP address/Mask
<b>Local Subnet 9</b>	IP address/Mask
<b>Local Subnet 10</b>	IP address/Mask
<b>Specific IP Address</b>	IP address
<b>Skip Trunk Auth</b>	yes/no/bytime
<b>Codec Preference</b>	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
<b>Permission</b>	Internal/Local/National/International
<b>NAT</b>	yes/no
<b>DTMF Mode</b>	RFC4733/info/inband/auto
<b>Insecure</b>	Port
<b>Enable Keep-alive</b>	Yes/no
<b>Keep-alive Frequency</b>	Value from 1-3600
<b>AuthID</b>	Alphanumeric value without special characters
<b>TEL URI</b>	Disabled/user=phone/enabled
<b>Call Forward Busy</b>	Digits
<b>Call Forward No Answer</b>	Digits
<b>Call Forward Unconditional</b>	Digits
<b>Support Hot-Desking Mode</b>	Yes/no
<b>Dial Trunk Password</b>	Digits
<b>Disable This Extension</b>	Yes/no
<b>CFU Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFN Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFB Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Music On Hold</b>	Default/ringbacktone_default
<b>CC Agent Policy</b>	If CC is disabled use: never  If CC is set to normal use: generic  If CC is set to trunk use: native
<b>CC Monitor Policy</b>	Generic/never
<b>CCBS Available Timer</b>	3600/4800
<b>CCNR Available Timer</b>	3600/7200
<b>CC Offer Timer</b>	60/120
<b>CC Max Agents</b>	Value from 1-999
<b>CC Max Monitors</b>	Value from 1-999
<b>Ring simultaneously</b>	Yes/no
<b>External Number</b>	Digits
<b>Time Condition for Ring Simultaneously</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Time Condition for Skip Trunk Auth</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Enable LDAP</b>	Yes/no
<b>Enable T.38 UDPTL</b>	Yes/no
<b>Max Contacts</b>	Values from 1-10
<b>Enable Wave</b>	Yes/no

<b>Alert-Info</b>	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
<b>Do Not Disturb</b>	Yes/no
<b>DND Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Custom Auto answer</b>	Yes/no
<b>Do Not Disturb Whitelist</b>	Empty/digits
<b>User Password</b>	Alphanumeric characters.
<b>First Name</b>	Alphanumeric without special characters.
<b>Last Name</b>	Alphanumeric without special characters.
<b>Email Address</b>	Email address
<b>Language</b>	Default/en/zh
<b>Phone Number</b>	Digits
<b>Call-Barging Monitor</b>	Extensions allowed to call barging
<b>Seamless Transfer Members</b>	Extensions allowed to seamless transfer

*SIP extensions Imported File Example*

<b>Field</b>	<b>Supported values</b>
<b>Extension</b>	Digits
<b>Technology</b>	IAX
<b>Enable Voicemail</b>	yes/no
<b>CallerID Number</b>	Digits
<b>SIP/IAX Password</b>	Alphanumeric characters
<b>Voicemail Password</b>	Digits
<b>Skip Voicemail Password Verification</b>	yes/no
<b>Ring Timeout</b>	Empty/ 3 to 600 (in second)
<b>S RTP</b>	yes/no
<b>Strategy</b>	Allow All/Local Subnet Only/A Specific IP Address
<b>Local Subnet 1</b>	IP address/Mask
<b>Local Subnet 2</b>	IP address/Mask
<b>Local Subnet 3</b>	IP address/Mask
<b>Local Subnet 4</b>	IP address/Mask
<b>Local Subnet 5</b>	IP address/Mask
<b>Local Subnet 6</b>	IP address/Mask
<b>Local Subnet 7</b>	IP address/Mask
<b>Local Subnet 8</b>	IP address/Mask
<b>Local Subnet 9</b>	IP address/Mask
<b>Local Subnet 10</b>	IP address/Mask
<b>Specific IP Address</b>	IP address
<b>Skip Trunk Auth</b>	yes/no/bytime
<b>Codec Preference</b>	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
<b>Permission</b>	Internal/Local/National/International
<b>NAT</b>	yes/no
<b>Call Forward Busy</b>	Digits
<b>Call Forward No Answer</b>	Digits
<b>Call Forward Unconditional</b>	Digits
<b>Require Call Token</b>	Yes/no/auto

<b>Max Number of Calls</b>	Values from 1-512
<b>Dial Trunk Password</b>	Digits
<b>Disable This Extension</b>	Yes/no
<b>CFU Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFN Time Condition</b>	
<b>CFB Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Music On Hold</b>	Default/ringbacktone_default
<b>Ring simultaneously</b>	Yes/no
<b>External Number</b>	Digits
<b>Time Condition for Ring Simultaneously</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Time Condition for Skip Trunk Auth</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Enable LDAP</b>	Yes/no
<b>Limit Max time (s)</b>	empty
<b>Do Not Disturb</b>	Yes/no
<b>DND Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Do Not Disturb Whitelist</b>	Empty/digits
<b>User Password</b>	Alphanumeric characters.
<b>First Name</b>	Alphanumeric without special characters.
<b>Last Name</b>	Alphanumeric without special characters.
<b>Email Address</b>	Email address
<b>Language</b>	Default/en/zh
<b>Phone Number</b>	Digits
<b>Call-Barging Monitor</b>	Extensions allowed to call barging
<b>Seamless Transfer Members</b>	Extensions allowed to seamless transfer

*IAX extensions Imported File Example*

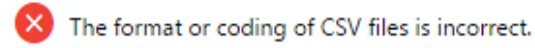
<b>Field</b>	<b>Supported values</b>
<b>Extension</b>	Digits
<b>Technology</b>	FXS
<b>Analog Station</b>	FXS1/FXS2
<b>Enable Voicemail</b>	yes/no
<b>CallerID Number</b>	Digits
<b>Voicemail Password</b>	Digits
<b>Skip Voicemail Password Verification</b>	yes/no
<b>Ring Timeout</b>	Empty/ 3 to 600 (in second)
<b>Auto Record</b>	yes/no
<b>Fax Mode</b>	None/Fax Gateway/Fax Detection
<b>Skip Trunk Auth</b>	Yes/no/bytime
<b>Permission</b>	Internal/Local/National/International
<b>Call Forward Busy</b>	Digits
<b>Call Forward No Answer</b>	Digits
<b>Call Forward Unconditional</b>	Digits

<b>Call Waiting</b>	Yes/no
<b>Use # as SEND</b>	Yes/no
<b>RX Gain</b>	Values from -30→6
<b>TX Gain</b>	Values from -30→6
<b>MIN RX Flash</b>	Values from: 30 – 1000
<b>MAX RX Flash</b>	Values from: 40 – 2000
<b>Enable Polarity Reversal</b>	Yes/no
<b>Echo Cancellation</b>	On/Off/32/64/128/256/512/1024
<b>3-Way Calling</b>	Yes/no
<b>Send CallerID After</b>	1/2
<b>Dial Trunk Password</b>	digits
<b>Disable This Extension</b>	Yes/no
<b>CFU Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFN Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFB Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Music On Hold</b>	Default/ringbacktone_default
<b>CC Agent Policy</b>	If CC is disabled use: never  If CC is set to normal use: generic  If CC is set to trunk use: native
<b>CC Monitor Policy</b>	Generic/never
<b>CCBS Available Timer</b>	3600/4800
<b>CCNR Available Timer</b>	3600/7200
<b>CC Offer Timer</b>	60/120
<b>CC Max Agents</b>	Value from 1-999
<b>CC Max Monitors</b>	Value from 1-999
<b>Ring simultaneously</b>	Yes/no
<b>External Number</b>	Digits
<b>Time Condition for Ring Simultaneously</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Time Condition for Skip Trunk Auth</b>	
<b>Enable LDAP</b>	Yes/no
<b>Enable Hotline</b>	Yes/no
<b>Hotline Type</b>	Immediate hotline/delay hotline
<b>Hotline Number</b>	digits
<b>Limit Max time (s)</b>	empty
<b>Do Not Disturb</b>	Yes/no
<b>DND Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Do Not Disturb Whitelist</b>	Empty/digits
<b>User Password</b>	Alphanumeric characters.
<b>First Name</b>	Alphanumeric without special characters.
<b>Last Name</b>	Alphanumeric without special characters.

<b>Email Address</b>	Email address
<b>Language</b>	Default/en/zh
<b>Phone Number</b>	Digits
<b>Call-Barging Monitor</b>	Extensions allowed to call barging
<b>Seamless Transfer Members</b>	Extensions allowed to seamless transfer

*FXS Extensions Imported File Example*

The CSV file should contain all the above fields, if one of them is missing or empty, the UCM630xA will display the following error message for missing fields.



The format or coding of CSV files is incorrect.

*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.

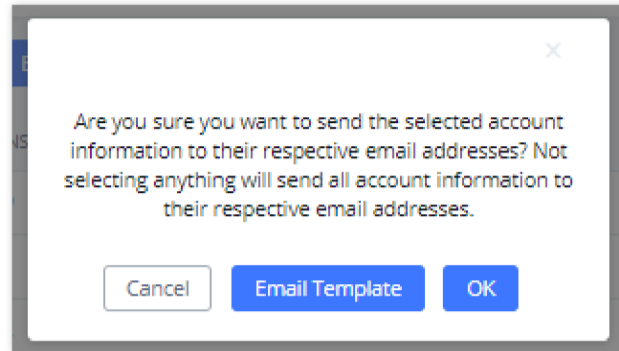
OPTIONS	VALUE
Extension	1000
Status	● Unavailable
Presence Status	Available
Terminal Type	SIP(WebRTC)
CallerID Name	
Message	0/0/0
IP and Port	--
Email Status	To Be Sent
Ring Group	
Call Queue	
Call Queue(Dynamic)	

*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 UCM630xA 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.



*E-mail Notification – Prompt Information*

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

General Settings	
Server Address	<a href="https://192.168.5.147:5060">192.168.5.147:5060</a>
Account Name	Mia
SIP User ID	1000
Authenticate ID	1000
Authenticate Password	pas1

*Account Registration Information*

GSWave Settings	
Login URL	<a href="https://192.168.5.147:8090/#/">https://192.168.5.147:8090/#/</a>
Login URL for Public	<a href="https://c074ad0a8c94-10671.b.gdms.cloud/#/">https://c074ad0a8c94-10671.b.gdms.cloud/#/</a>
Login Name	1000
Login Password	pas1

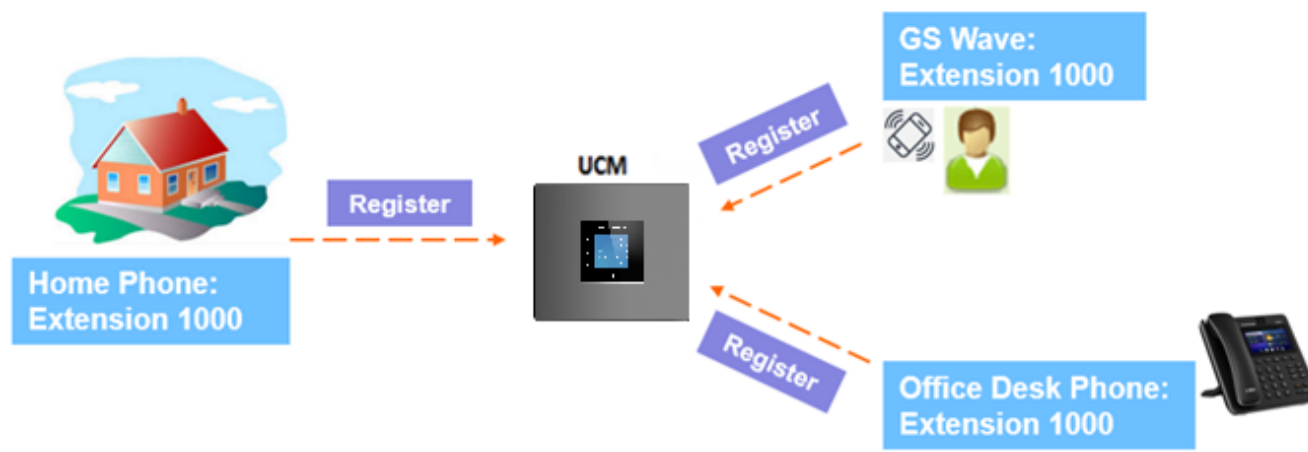


Use Web App to scan qr code and log in

*Grandstream Wave Settings and QR Code*

## Multiple Registrations per Extension

UCM630xA supports multiple registrations per extension so that users can use the same extension on devices in different locations.



Multiple Registrations per Extension

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

Edit Extension: 1000

Basic Settings   Media   Features   Specific Time   Follow Me   Cancel   Save

---

**General**

* Extension: <input type="text" value="1000"/>	CallerID Number: <input type="text" value="1000"/>
* Permission: <input type="text" value="Internal"/>	* SIP/IAX Password: <input type="password" value="*****"/>
AuthID: <input type="text"/>	Voicemail: <input type="text" value="Local Voicemail"/>
* Voicemail Password: <input type="password" value="*****"/>	Skip Voicemail Password: <input type="checkbox"/>
Send Voicemail to Email: <input type="text" value="Default"/>	Verification: <input type="text"/>
Enable Keep-alive: <input type="checkbox"/>	Keep Voicemail after Emailing: <input type="text" value="Default"/>
Disable This Extension: <input type="checkbox"/>	* Keep-alive Frequency: <input type="text" value="60"/>
Emergency Calls CID: <input type="text"/>	Enable SCA: <input type="checkbox"/>

**User Settings**

First Name: <input type="text"/>	Last Name: <input type="text"/>
Email Address: <input type="text"/>	* User Password: <input type="password" value="*****"/>
* Language: <input type="text" value="Default"/>	* Concurrent Registrations: <input type="text" value="3"/>
Mobile Phone Number: <input type="text"/>	

Extension – Concurrent Registration

## SMS Message Support

The UCM630xA provides built-in SIP SMS message support. For SIP end devices such as Grandstream GXP or GXV phones that supports SIP message, after an UCM630xA 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.



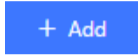


SMS Message Support

# EXTENSION GROUPS

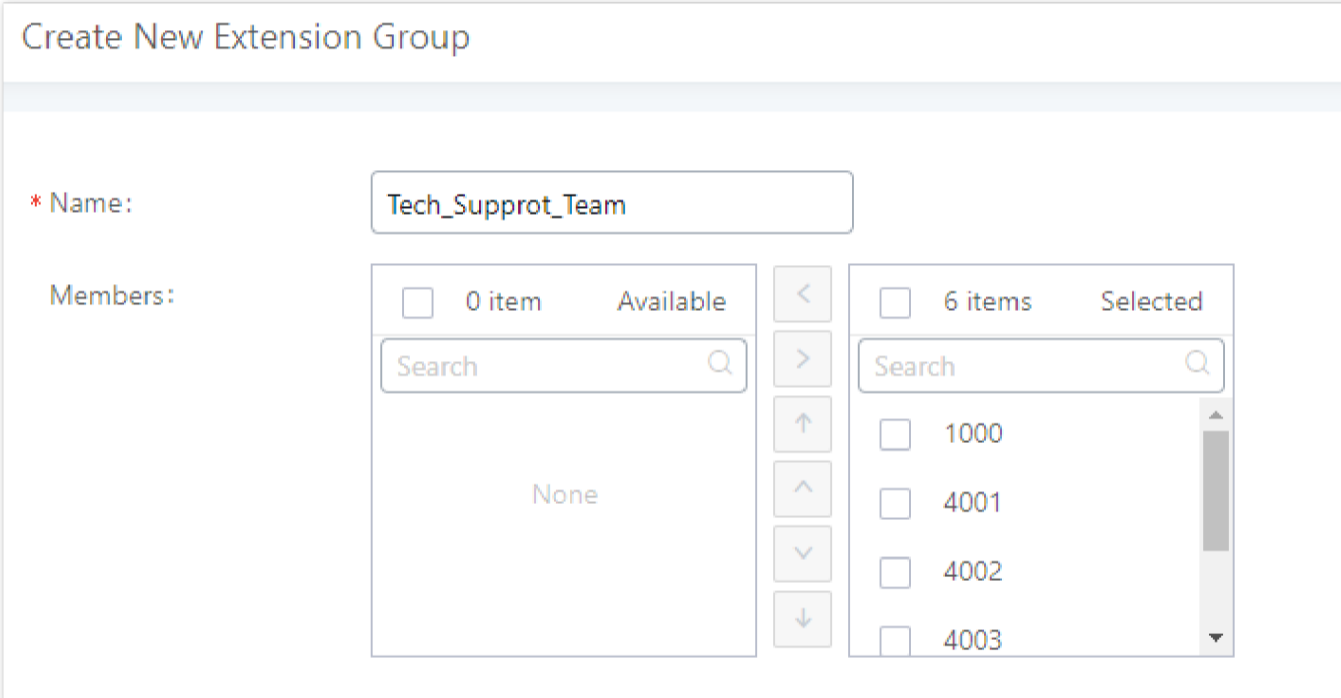
The UCM630xA extension group feature allows users to assign and categorize extensions in different groups to better manage the configurations on the UCM630xA. For example, when configuring "Enable Filter on Source Caller ID", users could select a group instead of each person's extension to assign. This 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  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.



*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.

**General**

\* Calling Rule Name:

\* Pattern:

PIN Groups:

Password:

Disable This Route:

Privilege Level:

PIN Groups with Privilege Level:

**Enable Filter on Source Caller ID**

Enable Filter on Source Caller

ID:

Outbound Route CID:



Custom Dynamic Route:

Available Extensions/Extension Groups:

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.

Parameter	Description
<b>FXO Port</b>	Select the channel for the analog trunk. <ul style="list-style-type: none"> <li>● UCM6301: 1 channel</li> <li>● UCM6302: 2 channels</li> <li>● UCM6304: 4 channels</li> <li>● UCM6308: 8 channels</li> </ul>
<b>Trunk Name</b>	Specify a unique label to identify the trunk when listed in outbound rules, incoming rules, etc.
<b>Advanced Options</b>	
<b>Disable This Trunk</b>	If selected, the trunk will be disabled, and incoming/Outgoing calls via this trunk will not be possible.
<b>SLA Mode</b>	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.
<b>Barge Allowed</b>	The barge option specifies whether other stations can join a call in progress on this trunk. If enabled, the other stations can press the line button to join the call. The default setting is Yes. This option appears when <b>SLA Mode</b> is enabled.

<b>Hold Access</b>	<p>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.</p> <p>The default setting is Yes.</p>
<b>Enable Polarity Reversal</b>	<p>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".</p>
<b>Polarity on Answer Delay (ms)</b>	<p>When the FXO port answers the call, FXS may send a Polarity Reversal. If this interval is shorter than the value of "Polarity on Answer Delay", the Polarity Reversal will be ignored. Otherwise, the FXO will On-hook to disconnect the call. The default setting is 600ms.</p>
<b>Current Disconnect Threshold (ms)</b>	<p>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.</p>
<b>Ring Timeout (ms)</b>	<p>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.</p>
<b>RX Gain</b>	<p>Configure the RX gain for the receiving channel of the analog FXO port. The valid range is from -13.5 (dB) to +12.0 (dB). The default setting is 0.</p>
<b>TX Gain</b>	<p>Configure the TX gain for the transmitting channel of the analog FXO port. The valid range is from -13.5 (dB) to +12.0 (dB). The default setting is 0.</p>
<b>Use CallerID</b>	<p>Configure to enable CallerID detection.</p> <p>The default setting is "Yes".</p>
<b>Caller ID Scheme</b>	<p>Select the Caller ID scheme for this trunk.</p> <ul style="list-style-type: none"> <li>● Bellcore/Telcordia</li> <li>● ETSI-FSK During Ringing</li> <li>● ETSI-FSK Prior to Ringing with DTAS</li> <li>● ETSI-FSK Prior to Ringing with LR</li> <li>● ETSI-FSK Prior to Ringing with RP</li> <li>● ETSI-DTMF During Ringing</li> <li>● ETSI-DTMF Prior to Ringing with DTAS</li> <li>● ETSI-DTMF Prior to Ringing with LR</li> <li>● ETSI-DTMF Prior to Ringing with RP</li> <li>● SIN 227-BT</li> <li>● NTT Japan</li> <li>● Auto-Detect</li> </ul> <p>If you are not sure which scheme to choose, please select "Auto Detect". The default setting is "Bellcore/Telcordia".</p>
<b>Fax Mode</b>	<p>Configures how faxes to this extension will be handled.</p> <ul style="list-style-type: none"> <li>● <b>None:</b> Faxes will not be processed.</li> <li>● <b>Fax Gateway:</b> Faxes to this extension will be processed and converted from T.30 to T.38 or vice-versa. FXS/FXO ports only.</li> </ul> <p>The default setting is None.</p>
<b>FXO Dial Delay (ms)</b>	<p>Configure the time interval between off-hook and first dialed digit for outbound calls.</p>
<b>Auto Record</b>	<p>Enable automatic recording for the calls using this trunk. The default setting is disabled. The recording files can be accessed under Web GUI &gt; <b>CDR &gt; Recording Files</b>.</p>
<b>Speed Dial Out</b>	<p>If enabled, a # sign will be automatically added to the end of the called number for outgoing calls to improve dialing efficiency. If the FXS gateway does not support #, it may cause outgoing calls to fail. After activation,</p>

	the SLA mode will be disabled.
<b>Direct Callback</b>	<p>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.</p>
<b>DAHDI Out Line Selection</b>	<p>This is to implement an analog trunk outbound line selection strategy. Three options are available:</p> <ul style="list-style-type: none"> <li>● <b>Ascend:</b> 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).</li> <li>● <b>Poll:</b> 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.</li> <li>● <b>Descend:</b> 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).</li> </ul> <p>The default setting is “Ascend” mode.</p>
<b>Max Outgoing Calls</b>	The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit.
<b>Echo Cancellation Mode</b>	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>Default:</b> The NLP limits the signal level to the background noise level when active, and the background noise level adjustment is low.</li> <li>● <b>High Noise Level Adjustment:</b> The NLP limits the signal level to the background noise level when active, and the background noise level adjustment is high.</li> <li>● <b>Noise Masking:</b> The NLP sends sign noise when active, and the background noise level adjustment is high.</li> <li>● <b>White Noise Injection:</b> 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.</li> </ul>
<b>Max Incoming Calls</b>	The max allowed number of concurrent incoming calls through the trunk. Default is 0 (no limit).
<b>Noise Cancellation RX Frequency (Hz)</b>	<p>Prevents interference from low-frequency signals; when enabled, the RX frequency will only allow signals above this configured value to pass. These are the supported values:</p> <ul style="list-style-type: none"> <li>● OFF</li> <li>● 20</li> <li>● 40</li> <li>● 60</li> <li>● 200</li> </ul> <p>The default value is "OFF".</p>
<b>Noise Cancellation TX Frequency (Hz)</b>	<p>Prevents interference from low-frequency signals; when enabled, the TX frequency will only allow signals above this configured value to pass. These are the supported values:</p> <ul style="list-style-type: none"> <li>● OFF</li> <li>● 20</li> <li>● 40</li> <li>● 60</li> <li>● 200</li> </ul> <p>The default value is "OFF".</p>
<b>Enable Total Time Limit For Outbound Calls</b>	If enabled, a limit will be placed on the cumulative duration of outbound calls within a specified period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.

<b>Period</b>	Configure the cumulative period for the total duration of outgoing calls. After reaching the next cycle, the accumulated time will be cleared, and it will start to accumulate again from 0. At the same time, the limit of the time-out trunk will be automatically lifted. If By Month is selected, the cycle will be one natural month, if Quarterly is selected, the cycle will be three months from the current month.
<b>Total Time (m)</b>	Configure the maximum allowed cumulative duration of outbound calls allowed by this trunk within the configured period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.
<b>Tone Settings</b>	
<b>Busy Detection</b>	Busy Detection is used to detect far-end Hangup or for detecting busy signal. The default setting is "Yes".
<b>Busy Tone Count</b>	If "Busy Detection" is enabled, users can specify the number of busy tones to be played before hanging up. The default setting is 2. Better results might be achieved if set to 4, 6, or even 8. Please note that the higher the number is, the more time is needed to Hangup the channel. However, this might lower the probability to get a random Hangup.
<b>Congestion Detection</b>	Congestion detection is used to detect far-end congestion signal. The default setting is "Yes".
<b>Congestion Count</b>	If "Congestion Detection" is enabled, users can specify the number of congestion tones to wait for. The default setting is 2.
<b>Tone Country</b>	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)".
<b>Busy Tone</b>	<p><b>Syntax:</b>  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.</p> <p><b>Default value:</b>  f1=480@-50,f2=620@-50,c=500/500</p>
<b>Congestion Tone</b>	<p><b>Syntax:</b>  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.</p> <p><b>Default value:</b>  f1=480@-50,f2=620@-50,c=250/250</p>
<b>PSTN Detection</b>	Click on "Detect" to detect the busy tone, Polarity Reversal, and Current Disconnect by PSTN. Before the detection, please make sure there is more than one channel configured and working properly. If the detection has a busy tone, the "Tone Country" option will be set as "Custom".

**Note**

Please note that the UCM6300A model does not support analog trunks.

## PSTN Detection

The UCM630xA 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 UCM630xA settings.

1. Go to UCM630xA 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.

*UCM630xA FXO Tone Settings*

4. Click on “Detect” to start PSTN detection.

*UCM630xA 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.

The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The settings are as follows:

- Detect model: Auto Detect (dropdown menu)
- Source Channel (to be detected): 1 (dropdown menu)
- Destination Channel: 2 (dropdown menu)
- \* Destination Number: 123654 (text input field)
- Dump Call Progress Tone:
- File: (empty text input field)

At the bottom, there is a "Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please follow the page prompt that pops out in the test." Below the note are two buttons: "Cancel" and "Detect".

UCM630xA PSTN Detection: Auto Detect

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

The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The settings are as follows:

- Detect model: Semi-auto Detect (dropdown menu)
- Source Channel (to be detected): 1 (dropdown menu)
- \* Destination Number: 123654 (text input field)
- Dump Call Progress Tone:
- File: (empty text input field)

At the bottom, there is a "Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please follow the page prompt that pops out in the test." Below the note are two buttons: "Cancel" and "Detect".

UCM630xA 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 UCM630xA 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 UCM630xA settings.

<b>Detect Model</b>	<p>Select "Auto Detect" or "Semi-auto Detect" for PSTN detection.</p> <ul style="list-style-type: none"> <li>○ <b>Auto Detect</b></li> </ul> <p>Please make sure two or more channels are connected to the UCM630xA 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 UCM630xA will control the call to be established and hang up between caller and callee to finish the detection.</p> <ul style="list-style-type: none"> <li>○ <b>Semi-auto Detect</b></li> </ul> <p>Semi-auto detection requires answering or hanging up the call manually. Please make sure one channel is connected to the UCM630xA 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.</p> <p>The default setting is "Auto Detect".</p>
<b>Source Channel</b>	Select the channel to be detected.
<b>Destination Channel</b>	Select the channel to help detect when "Auto Detect" is used.
<b>Destination Number</b>	Configure the number to be called to help the detection.
<b>Dump Call Progress Tone File</b>	Choose whether to save the calling tone file, it is not checked by default.

*PSTN Detection for Analog Trunk*





**i**

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

## VOIP TRUNKS

### VoIP Trunk Configuration

VoIP trunks can be configured in UCM630xA 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.

<https://documentation.grandstream.com/knowledge-base/sip-trunks-guide/>

The VoIP trunk options are listed in the table below.

<b>Type</b>	<p>Select the VoIP trunk type.</p> <ul style="list-style-type: none"> <li>• Peer SIP Trunk</li> <li>• Register SIP Trunk</li> </ul>
<b>Provider Name</b>	Configure a unique label (up to 64 characters) to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Host Name</b>	Configure the IP address or URL for the VoIP provider's server of the trunk.
<b>Transport</b>	<p>Configure the SIP Transport method. Using TCP requires local TCP support. Using TLS Requires local TLS support.</p> <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS</li> </ul>
<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded.
<b>Keep Original CID</b>	Keep the CID from the inbound call when dialing out. This setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line.
<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>NAT</b>	Turn on this setting when the PBX is using public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall.
<b>Disable This Trunk</b>	<p>If checked, the trunk will be disabled.</p> <p>Note: If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.</p>
<b>TEL URI</b>	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.
<b>Caller ID Number</b>	<p>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.</p> <p>Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: From the user (Register Trunk Only) → CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID.</p>
<b>CallerID Name</b>	Configure the new name of the caller when the extension has no CallerID Name configured.
<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded.
<b>Auth ID</b>	Enter the Authentication ID for the "Register SIP Trunk" type.

<b>Direct Callback</b>	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.
<b>RemoteConnect Mode</b>	If enabled, the RemoteConnect related parameters will be set synchronously. Please make sure the trunk host is allocated by GDMS or supports TLS.
<b>Limit Concurrent Calls</b>	If enabled and when the number of concurrent calls exceeds any trunk's configured concurrent call thresholds, an alarm notification will be generated. Note: Please make sure the system alert event "Trunk Concurrent Calls" is enabled.
<b>Concurrent Call Threshold</b>	Threshold of all incoming and outgoing concurrent calls through this trunk.
<b>Outgoing Concurrent Calls Threshold</b>	Threshold of all outgoing concurrent calls passing through this trunk.
<b>Incoming Concurrent Calls Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.
<b>Total Time Limit For Outbound Calls</b>	
<b>Enable Total Time Limit For Outgoing Calls</b>	When this setting is activated, the user can set a time limit before calls cannot be initiated through this trunk
<b>Period</b>	This setting defines how long until the time allowed for outgoing calls is reset.  <ul style="list-style-type: none"> <li>• <b>Monthly:</b> The time allowed will reset every month.</li> <li>• <b>Quarterly:</b> The time allowed will reset every 3 months.</li> </ul> <b>Example:</b> If the time limit has been set to 4320 minutes, the allowed time will always revert back to 4320 after a month or 3 month based on the period configured.
<b>Total Time</b>	Total time allowed in minutes

*Create New SIP Trunk*

## Account SIP Trunk

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

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

<b>Basic Settings</b>	
<b>Provider Name</b>	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Transport</b>	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP".  <ul style="list-style-type: none"> <li>• <b>UDP</b></li> <li>• <b>TCP</b></li> <li>• <b>TLS</b></li> </ul>
<b>Keep Original CID</b>	Keep the CID from the inbound call when dialing out. This setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line.

<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>NAT</b>	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall.
<b>Disable This Trunk</b>	If selected, the trunk will be disabled. <b>Note:</b> If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
<b>TEL URI</b>	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.
<b>CallerID Number</b>	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 / Register Trunk Username (Keep Trunk CID enabled) >>> DOD CID >>> Extension CID >>> Trunk CID / Register Trunk Username (Keep Trunk CID disabled) >>> Global Outbound CID. <b>Note 1:</b> Certain providers may ignore this CID. <b>Note 2:</b> If this CID contains asterisk (*), call recordings from this trunk may be lost when saving them to NAS storage.
<b>CallerID Name</b>	Configure the new name of the caller when the extension has no CallerID Name configured.
<b>Username</b>	Enter the username to register to the trunk from the provider when the "Register SIP Trunk" type is selected.
<b>Password</b>	Enter the password to register to the trunk when "Register SIP Trunk" is selected.
<b>AuthID</b>	Enter the Authentication ID for the "Register SIP Trunk" type.
<b>Auto Record</b>	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 <b>Web GUI</b> → <b>CDR</b> → <b>Recording Files</b> .
<b>Direct Callback</b>	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.
<b>Monitor Concurrent Calls</b>	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
<b>Outgoing Concurrent Calls Threshold</b>	Threshold of all outgoing concurrent calls passing through this trunk.
<b>Incoming Concurrent Calls Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.
<b>Advanced Settings</b>	
<b>Codec Preference</b>	Select the audio 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 and ADPCM.
<b>Packet Loss Retransmission NACK+RTX(SSRC-GROUP)</b>	Configure to enable Packet Loss Retransmission.

<b>Audio FEC</b>	Configure to enable Forward Error Correction (FEC).
<b>Video FEC</b>	Video FEC
<b>ICE Support</b>	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.
<b>TURN Relay</b>	TURN servers are used for media NAT traversal and will be prioritized if ICE is also enabled.
<b>FECC</b>	Remote Camera Management
<b>SRTP</b>	Toggle encryption of RTP streams.
<b>SRTP Crypto Suite</b>	SRTP encryption suite used by UCM for outbound calls. Priority is based on order of configuration.
<b>ZRTP Encryption Mode</b>	If disabled, UCM will not support ZRTP encryption. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.
<b>Enable T.38 UDPTL</b>	Enable or disable T.38 UDPTL support.
<b>Special Attributes</b>	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. These attributes may cause incompatibility when interconnecting with other devices.
<b>Send PPI Header</b>	<p>If enabled, the SIP INVITE message sent to the trunk will contain PPI (P-Preferred-Identity) header. The default setting is "No".</p> <p><b>Note:</b> "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.</p>
<b>PPI Mode</b>	<p><b>Default</b> – Include the trunk's preferred CID (configured in Basic Settings) in the PPI Header.</p> <p><b>Original CID</b> – Include the original CID in the PPI Header.</p> <p><b>DOD Number</b> – 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.</p>
<b>Send PAI Header</b>	<p>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".</p> <p><b>Note:</b> "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.</p>
<b>PAI Header</b>	<p>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.</p> <p><b>Note:</b> "Send PAI Header" needs to be enabled to use this feature</p>
<b>Send Anonymous</b>	If checked, the "From" header in the outgoing INVITE message will be set to anonymous.
<b>DOD As From Name</b>	<p>If enabled and "From User" is configured, the INVITE's From header will contain the DOD number.</p> <p><b>Note:</b></p>
<b>Passthrough PAI Header</b>	If checked and the option "Send PAI Header" is not checked, the PAI header will be passthrough from one side to the other side.
<b>Send PANI Header</b>	If checked, the INVITE and REGISTER sent to the trunk will contain the P-Access-Network-Info header.

<b>Access Network Info</b>	The access network information is in the P-Access-Network-Info header.
<b>Send Anonymous</b>	If checked, the "From" header in the outgoing INVITE message will be set to anonymous.
<b>Outbound Proxy Support</b>	Select to enable outbound proxy in this trunk. The default setting is "No".
<b>Outbound Proxy</b>	When outbound proxy support is enabled, enter the IP address or URL of the outbound proxy.
<b>Remove OBP from Route</b>	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".
<b>DID Mode</b>	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".
<b>GIN Registration</b>	If enabled, the UCM will send a GIN REGISTER (generate implicit numbers).
<b>DTMF Mode</b>	Configure the default DTMF mode when sending DTMF on this trunk. <ul style="list-style-type: none"> <li>• <b>Default:</b> The global setting of DTMF mode will be used. The global setting for the DTMF Mode setting is under <b>Web GUI→PBX Settings→SIP Settings→ToS</b>.</li> <li>• <b>RFC4733:</b> Send DTMF using RFC4733.</li> <li>• <b>Info:</b> Send DTMF using SIP INFO message.</li> <li>• <b>Inband:</b> Send DTMF using inband audio. This requires a 64-bit codec, i.e., PCMU and PCMA.</li> <li>• <b>Auto:</b> Send DTMF using RFC4733 if offered. Otherwise, an inband will be used.</li> </ul>
<b>Enable Heartbeat Detection</b>	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".
<b>Heartbeat Frequency</b>	When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
<b>The Maximum Number of Call Lines</b>	The maximum number of concurrent calls using the trunk. The default setting is 0, which means no limit.
<b>STIR/SHAKEN</b>	Configure this feature to prevent call spoofing, robocalls and spam calls. <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>Outgoing Attest:</b> The UCM will only authenticate the caller ID.</li> <li>• <b>Incoming Verify:</b> The UCM will only verify if the caller ID is authenticated</li> <li>• <b>Both:</b> The UCM will authenticate the outgoing calls as well as verify if the incoming calls are authenticated.</li> </ul>
<b>CC Settings</b>	
<b>Enable CC</b>	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.
<b>CC Max Agents</b>	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.
<b>CC Max Monitors</b>	Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

## Register SIP Trunk

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

Basic Settings	
<b>Provider Name</b>	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Host Name</b>	Configure the IP address or URL for the VoIP provider's server of the trunk.
<b>Auto Record</b>	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→ <b>CDR</b> → <b>Recording Files</b> .
<b>Keep Original CID</b>	Keep the CID from the inbound call when dialing out, this setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line.
<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>NAT</b>	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall.
<b>Disable This Trunk</b>	If selected, the trunk will be disabled. <b>Note:</b> If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
<b>TEL URI</b>	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.
<b>Caller ID Number</b>	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. <b>Important Note:</b> When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call:  <ul style="list-style-type: none"> <li>• CID from inbound call (<b>Keep Original CID Enabled</b>) → Trunk Username/CallerID (<b>Keep Trunk CID Enabled</b>) → DOD → Extension CallerID Number → Trunk Username/CallerID (<b>Keep Trunk CID Disabled</b>) → Global Outbound CID.</li> </ul>
<b>CallerID Name</b>	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
<b>Transport</b>	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP".  <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS</li> </ul>
<b>RemoteConnect Mode</b>	If enabled, the RemoteConnect related parameters will be set synchronously. Please make the trunk host is allocated by GDMS or it supports TLS.
<b>Direct Callback</b>	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	
<b>Codec Preference</b>	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p and VP8.
<b>Packet Loss Retransmission</b>	Configure to enable Packet Loss Retransmission.

<b>Audio FEC</b>	Configure to enable Forward Error Correction (FEC) for audio.
<b>Video FEC</b>	Configure to enable Forward Error Correction (FEC) for video.
<b>ICE Support</b>	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.
<b>TURN Relay</b>	TURN servers are used for media NAT traversal and will be prioritized if ICE is also enabled.
<b>FECC</b>	Configure to enable Far-end Camera Control
<b>Silence Suppression</b>	If enabled, the UCM will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the UCM will send DTX packets instead.
<b>SRTP</b>	Enable SRTP for the VoIP trunk. The default setting is "No".
<b>SRTP Crypto Suite</b>	SRTP encryption suite used by UCM for outbound calls. Priority is based on order of configuration.
<b>IPVT Mode</b>	Similar to Enable Direct Media. The PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. Primarily for use with trunks to IPVT.
<b>Enable T.38 UDPTL</b>	Enable or disable T.38 UDPTL support.
<b>Special attributes</b>	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. These attributes may cause incompatibility when interconnecting with other devices.
<b>Send PPI Header</b>	If checked, the invite message sent to trunks will contain PPI (P-Preferred-Identity) Header.
<b>Send PAI Header</b>	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.
<b>DOD as From Name</b>	If enabled and "From User" is configured, the INVITE's From header will contain the DOD number.
<b>Passthrough PAI Header</b>	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the UCM.
<b>Send PANI Header</b>	If checked, the INVITE and REGISTER sent to the trunk will contain P-Access-Network-Info header.
<b>Send Anonymous</b>	If checked, the "From" header in outgoing INVITE message will be set to anonymous.
<b>Outbound Proxy Support</b>	Enable to send outbound signal to the proxy instead of the devices directly.
<b>DID Mode</b>	Configure to obtain the destination ID of an incoming SIP call from SIP Request-line or To header.
<b>GIN Registration</b>	If enabled, the UCM will send a GIN REGISTER (generate implicit numbers).
<b>DTMF Mode</b>	<p>Configure the mode for sending the DTMF.</p> <ul style="list-style-type: none"> <li>● <b>RFC4833</b> (default): DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream. Backwards-compatible with RFC2833.</li> <li>● <b>DTMF</b> is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs</li> <li>● <b>Info</b>: DTMF is transmitted separately from the media streams.</li> <li>● <b>RFC4733_info</b>: DTMF is transmitted through both RFC4733 and SIP INFO</li> <li>● <b>Auto</b>: DTMF mode will be negotiated with the remote peer, only supports RFC4733 and inband. RFC4733 will be used by default unless the remote peer does not indicate support.</li> </ul>

<b>Enable Heartbeat detection</b>	If enabled, the PBX will regularly send SIP OPTIONS to check if the device is online.
<b>The Maximum Number of Call Lines</b>	The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit.
<b>Sync LDAP Enable</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Sync LDAP Password:</b> Password used for LDAP phonebook encryption and decryption. The password must be the same for both peers to ensure successful syncing.</li> <li>• <b>LDAP Outbound Rule:</b> Specify an outbound rule. The PBX system will automatically modify the remote contacts by adding prefix parsed from this rule.</li> <li>• <b>LDAP Dialed Prefix:</b> System will automatically modify the remote contacts by adding this prefix</li> <li>• <b>LDAP Sync Method:</b> Specifies the sync method of the UCM. When an LDAP sync request is received, the UCM will send the phonebook data via the specified method.</li> <li>• <b>LDAP Last Sync Date:</b> The last successful sync date.</li> </ul>
<b>STIR/SHAKEN</b>	<p>Block Spam Calls.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Disable STIR/SHAKEN.</li> <li>• <b>Outgoing Attest:</b> Enable STIR/SHAKEN attestation for outgoing calls.</li> <li>• <b>Incoming Verify:</b> Enable STIR/SHAKEN verification for incoming calls.</li> <li>• <b>Both:</b> Enable STIR/SHAKEN for both outgoing and incoming calls</li> </ul>
<b>Enable CC</b>	Check this box to allow the system to automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. If the Call Waiting is disabled, the CC service will take effect only for unanswered and timeout calls.

## Peer SIP Trunk

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

<b>Basic Settings</b>	
<b>Provider Name</b>	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Host Name</b>	Configure the IP address or URL for the VoIP provider's server of the trunk.
<b>Transport</b>	<p>Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP".</p> <ul style="list-style-type: none"> <li>• <b>UDP</b></li> <li>• <b>TCP</b></li> <li>• <b>TLS</b></li> </ul>
<b>SIP URI Scheme When Using TLS</b>	When TLS is selected as Transport for register trunk, users can select between SIP and SIPS URI scheme
<b>Keep Original CID</b>	Keep the CID from the inbound call when dialing out. This setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line.
<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>NAT</b>	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall.

<b>Disable This Trunk</b>	<p>If selected, the trunk will be disabled.</p> <p><b>Note:</b> If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.</p>
<b>TEL URI</b>	<p>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.</p>
<b>Need Registration</b>	<p>Select whether the trunk needs to register on the external server or not when the "Register SIP Trunk" type is selected. The default setting is No.</p>
<b>Allow outgoing calls if registration failure</b>	<p>If enabled outgoing calls even if the registration to this trunk fails will still be able to go through. Note that if we uncheck the "Need Registration" option, this option will be ignored.</p>
<b>CallerID Name</b>	<p>Configure the new name of the caller when the extension has no CallerID Name configured.</p>
<b>From Domain</b>	<p>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.</p>
<b>From User</b>	<p>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.</p>
<b>Username</b>	<p>Enter the username to register to the trunk from the provider when the "Register SIP Trunk" type is selected.</p>
<b>Password</b>	<p>Enter the password to register to the trunk when "Register SIP Trunk" is selected.</p>
<b>Auth ID</b>	<p>Enter the Authentication ID for the "Register SIP Trunk" type.</p>
<b>Auth Trunk</b>	<p>If enabled, the UCM will send a 401 response to the incoming call to authenticate the trunk.</p>
<b>Auto Record</b>	<p>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 <b>Web GUI→CDR→Recording Files</b>.</p>
<b>RemoteConnect Mode</b>	<p>If enabled, the RemoteConnect related parameters will be set synchronously. Please make the trunk host is allocated by GDMS or it supports TLS.</p>
<b>Direct Callback</b>	<p>Allows external numbers the option to get directed to the extension that last called them.</p> <p>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.</p>
<b>Enable Concurrent Call Alert</b>	<p>If enabled, the "Trunk Concurrent Calls" system event will monitor the number of concurrent calls in this trunk. When the number of concurrent calls in a certain period exceeds the set threshold, an alarm message will be generated. Note: Please turn on the alert for the "Trunk Concurrent Calls" event first.</p>
<b>Two-way Concurrent Calls Threshold</b>	<p>Threshold of all incoming and outgoing concurrent calls through this trunk.</p>
<b>Outgoing Concurrent Calls Threshold</b>	<p>Threshold of all outgoing concurrent calls passing through this trunk.</p>
<b>Incoming Concurrent Calls Threshold</b>	<p>Threshold of all incoming concurrent calls passing through this trunk.</p>

Advanced Settings	
<b>Codec Preference</b>	Select the audio 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 and ADPCM.
<b>Packet Loss Retransmission NACK+RTX(SSRC-GROUP)</b>	Configure to enable Packet Loss Retransmission.
<b>Audio FEC</b>	Configure to enable Forward Error Correction (FEC).
<b>Video FEC</b>	Video FEC
<b>ICE Support</b>	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.
<b>TURN Relay</b>	TURN servers are used for media NAT traversal and will be prioritized if ICE is also enabled.
<b>FECC</b>	Remote Camera Management
<b>SRTP</b>	<p>Enable SRTP for the call. The default setting is disabled.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>Enabled and Enforced:</b> SRTP will be necessary to transmit media traffic. If the IP phone of this extension has SRTP disabled, calls cannot be established.</li> <li>• <b>Optional:</b> The UCM will negotiate whether to use SRTP or not. If the SIP endpoint has SRTP enabled, SRTP will be used. If it is disabled, SRTP will not be used.</li> </ul>
<b>SRTP Crypto Suite</b>	<p>SRTP encryption suite used by UCM for outbound calls. Priority is based on order of configuration. The following encryption protocols can be used to encrypt an RTP stream.</p> <ul style="list-style-type: none"> <li>• AES_CM_128_HMAC_SHA1_80 (This is the default used protocol)</li> <li>• AES_256_CM_HMAC_SHA1_80</li> <li>• AEAD_AES_128_GCM</li> <li>• AEAD_AES_256_GCM</li> </ul>
<b>ZRTP Encryption Mode</b>	If disabled, UCM will not support ZRTP encryption. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.
<b>Enable T.38 UDPTL</b>	Enable or disable T.38 UDPTL support.
<b>Special Attributes</b>	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. These attributes may cause incompatibility when interconnecting with other devices.
<b>Send PPI Header</b>	<p>If enabled, the SIP INVITE message sent to the trunk will contain PPI (P-Preferred-Identity) header. The default setting is "No".</p> <p><b>Note:</b> "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.</p>
<b>PPI Mode</b>	<p><b>Default</b> – Include the trunk's preferred CID (configured in Basic Settings) in the PPI Header.</p> <p><b>Original CID</b> – Include the original CID in the PPI Header.</p> <p><b>DOD Number</b> – 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.</p>
<b>Send PAI Header</b>	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".

	<p><b>Note:</b> "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.</p>
<b>PAI Header</b>	<p>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.</p> <p><b>Note:</b> "Send PAI Header" needs to be enabled to use this feature</p>
<b>Send Anonymous</b>	<p>If checked, the "From" header in the outgoing INVITE message will be set to anonymous.</p>
<b>Passthrough PAI Header</b>	<p>If checked and the option "Send PAI Header" is not checked, the PAI header will be passthrough from one side to the other side.</p>
<b>Send PANI Header</b>	<p>If checked, the INVITE and REGISTER sent to the trunk will contain the P-Access-Network-Info header.</p>
<b>Access Network Info</b>	<p>The access network information is in the P-Access-Network-Info header.</p>
<b>Send Anonymous</b>	<p>If checked, the "From" header in the outgoing INVITE message will be set to anonymous.</p>
<b>Outbound Proxy Support</b>	<p>Select to enable outbound proxy in this trunk. The default setting is "No".</p>
<b>Outbound Proxy</b>	<p>When outbound proxy support is enabled, enter the IP address or URL of the outbound proxy.</p>
<b>Remove OBP from Route</b>	<p>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".</p>
<b>DID Mode</b>	<p>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".</p>
<b>GIN Registration</b>	<p>If enabled, the UCM will send a GIN REGISTER (generate implicit numbers).</p>
<b>DTMF Mode</b>	<p>Configure the default DTMF mode when sending DTMF on this trunk.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> The global setting of DTMF mode will be used. The global setting for the DTMF Mode setting is under <b>Web GUI→PBX Settings→SIP Settings→ToS</b>.</li> <li>• <b>RFC4733:</b> Send DTMF using RFC4733.</li> <li>• <b>Info:</b> Send DTMF using SIP INFO message.</li> <li>• <b>Inband:</b> Send DTMF using inband audio. This requires a 64-bit codec, i.e., PCMU and PCMA.</li> <li>• <b>Auto:</b> Send DTMF using RFC4733 if offered. Otherwise, an inband will be used.</li> </ul>
<b>Enable Heartbeat Detection</b>	<p>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".</p>
<b>Heartbeat Frequency</b>	<p>When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.</p>
<b>The Maximum Number of Call Lines</b>	<p>The maximum number of concurrent calls using the trunk. The default setting is 0, which means no limit.</p>
<b>STIR/SHAKEN</b>	<p>Configure this feature to prevent call spoofing, robocalls and spam calls.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>Outgoing Attest:</b> The UCM will only authenticate the caller ID.</li> <li>• <b>Incoming Verify:</b> The UCM will only verify if the caller ID is authenticated</li> <li>• <b>Both:</b> The UCM will authenticate the outgoing calls as well as verify if the incoming calls are authenticated.</li> </ul>

CC Settings	
<b>Enable CC</b>	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.
<b>CC Max Agents</b>	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.
<b>CC Max Monitors</b>	Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

#### Create New IAX Trunk

<b>Type</b>	Select the VoIP trunk type. <ul style="list-style-type: none"> <li>• Peer IAX Trunk</li> <li>• Register IAX Trunk</li> </ul>
<b>Provider Name</b>	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Host Name</b>	Configure the IP address or URL for the VoIP provider's server of the trunk.
<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>Username</b>	Enter the username to register to the trunk from the provider when the "Register IAX Trunk" type is selected.
<b>Password</b>	Enter the password to register to the trunk from the provider when the "Register IAX Trunk" type is selected.
<b>Disable This Trunk</b>	If selected, the trunk will be disabled.
<b>Caller ID Number</b>	The number that the trunk will try to use when making outbound calls. CID priority from highest to lowest is as follows: <b>From User</b> (register trunk only) >>> <b>Inbound Call CID</b> (if Keep Original CID is enabled and the call is originally from another trunk) >>> <b>Trunk CID</b> (Keep Trunk CID enabled) >>> DOD CID >>> <b>Extension CID</b> >>> <b>Register Trunk Username</b> (Keep Trunk CID disabled) >>> <b>Global Outbound CID</b> . <b>Note 1:</b> Certain providers may ignore this CID. <b>Note 2:</b> If this CID contains an asterisk (*), call recordings from this trunk might be lost when saving them to NAS storage.
<b>CallerID Name</b>	Configure the new name of the caller when the extension has no CallerID Name configured.

[IAX Peer Trunk](#)

[IAX Register Trunk](#)

Basic Settings	
<b>Provider Name</b>	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
<b>Host Name</b>	Configure the IP address or URL for the VoIP provider's server of the trunk.

<b>Keep Trunk CID</b>	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
<b>Disable This Trunk</b>	If selected, the trunk will be disabled.
<b>Caller ID</b>	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. <b>Important Note:</b> When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call. From the user (Register Trunk Only) → CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID.
<b>CallerID Name</b>	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
<b>Username</b>	Enter the username to register to the trunk from the provider.
<b>Password</b>	Enter the password to register to the trunk from the provider.
<b>Advanced Settings</b>	
<b>Codec Preference</b>	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p and VP8.
<b>Enable Heartbeat Detection</b>	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".
<b>Heartbeat Frequency</b>	When the "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
<b>Maximum Number of Call Lines</b>	The maximum number of concurrent calls using the trunk. The default setting is 0, which means no limit.

## Trunk Groups

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


VoIP Trunks

VoIP Trunks [Trunk Group](#)

[+ Add Trunk Group](#)

NAME ↕	TERMINAL TYPE	HOSTNAME/IP ↕	USERNAME	OPTIONS
No Data				

*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.

Cancel Save

### Create New Trunk Group

If the host is not a numeric IP address, but the port number is present in the URI, the UCM performs an A or AAAA record lookup of the domain name. If a domain is configured without a port number, the UCM will do an SRV record lookup.

Type: Register SIP Trunk

\* Provider Name: Please select a provider

\* Host Name:

Transport: UDP

Keep Original CID:

Keep Trunk CID:

NAT:

Disable This Trunk:

TEL URI: Disabled

Need Registration:

Allow outgoing calls if registration fails:

CallerID Name:

\* Trunk Registration Number: Trunk Registration Number / Password / AuthID +

[Add Username](#) +

Line Selection Strategy: Linear

AuthTrunk:

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

#### Trunk Group Configuration

<b>Type</b>	Register Trunk
<b>Provider Name</b>	Configure a unique label to identify the trunk when listed in outbound rules and incoming rules.
<b>Host Name</b>	Enter the IP address or hostname of the VoIP provider's server.
<b>Transport</b>	Configure the SIP Transport method. Using TCP requires local TCP support; using TLS requires local TLS support.
<b>Keep Original CID</b>	Keep CID from the inbound call when dialing out even if option "Keep Trunk CID" is enabled. Please make sure the peer PBX at the other end supports matching user entry using the "username" field from the authentication line.
<b>Keep Trunk CID</b>	Always use trunk CID if specified even if extension has DOD number or CID configured.
<b>NAT</b>	Enable this setting if the IPPBX is using public IP and communicating with devices behind NAT. Note 1: This setting will overwrite the Contact header of received messages, which may affect the ability to establish calls when behind NAT. Consider changing settings in PBX Settings → SIP Settings → NAT instead.
<b>Disable This Trunk</b>	Check this box to disable this trunk
<b>TEL URI</b>	if "Enabled" option is selected, TEL URI and remove OBP from Route cannot be enabled at the same time. If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". A "User=Phone" parameter will 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.
<b>Need Registration</b>	Whether to register on the external server.

<b>Allow outgoing calls if registration fails</b>	Uncheck to block outgoing calls if registration fails. If "Need Registration" option is unchecked, this setting will be ignored.
<b>CallerID Name</b>	To display the caller ID name of the trunk, you must configure the caller ID number of the trunk.
<b>Trunk Registration Number</b>	The number used to register with the provider server, and the VoIP provider will authenticate the number based on the trunk registration number.
<b>Line Selection Strategy</b>	Linear: Select lines in list order and make Outbound calls. Round Robin: Rotary line selection with memory and making Outbound calls.
<b>AuthTrunk</b>	If enabled, the IPPBX will send a 401 response to the incoming call to authenticate the trunk.
<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded.
<b>Direct Callback</b>	Allows external numbers the option to get directed to the extension that last called them.
<b>RemoteConnect Mode</b>	If enabled, RemoteConnect-related options will be automatically configured. Please confirm the trunk has a GDMS-assigned address or supports TLS.
<b>Monitor Concurrent Calls</b>	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
<b>Concurrent Call Threshold</b>	Threshold of all incoming and outgoing concurrent calls in this trunk.
<b>Outgoing Concurrent Call Threshold</b>	Threshold of all outgoing concurrent calls passing through this trunk.
<b>Incoming Concurrent Call Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.
<b>Enable Total Time Limit For Outbound Calls</b>	If enabled, a limit will be placed on the cumulative duration of outbound calls within a specific period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.

## WebRTC Trunks

WebRTC, Web Real-Time Communication, is a real time audio/video chatting framework that allows real-time audio/video chatting through the web browser. WebRTC usually does not refer to the web application itself but to the set of protocols and practices bundled with a graphical interface. Our UCM63xx supports creating WebRTC trunks to use exclusively with web application, this allows the users to join calls and meetings just by clicking a link to a web page.

Below is a figure that shows the options to configure when setting up this feature:

* Trunk Name :	<input type="text" value="GS_WebRTC_Trunk"/>
Disable This Trunk :	<input type="checkbox"/>
Auto Record :	<input checked="" type="checkbox"/>
Enable Concurrent Call Threshold :	<input checked="" type="checkbox"/>
* Incoming Concurrent Call Threshold :	<input type="text" value="150"/>
WebRTC Inbound Link Address :	Automatically generated after saving

<b>Trunk Name</b>	Create a unique label to easily identify the trunk for inbound route configuration.
<b>Disable This Trunk</b>	Check this box to disable this trunk.
<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded.
<b>Jitter Buffer</b>	Select jitter buffer method for temporary accounts such as meeting participants who joined via link. <b>Disable:</b> Jitter buffer will not be used. <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of "Jitter Buffer Size") <b>Adaptive:</b> Jitter buffer with a adaptive size that will not exceed the value of "Max Jitter Buffer"). <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.
<b>Monitor Concurrent Calls</b>	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
<b>Incoming Concurrent Call Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.
<b>WebRTC Inbound Link Address</b>	This link can be embedded onto a web page. Clicking the link will connect to a pre-configured WebRTC trunk destination. You can also enter this link in the browser address bar to directly access and test WebRTC calls.

### Important Note

Please note that in order to use WebRTC Trunk feature, you need to have a paid RemoteConnect plan enabled.



## Direct Outward Dialing (DOD)

The UCM630xA 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 UCM630xA:

1. To setup DOD go to UCM630xA 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.

Create DOD
✕

\*DOD Number:

DOD Name:

Add Extension:

15 items
Available

- 1000
- 1001 "John Snow"
- 1002 "Jack Doe"
- 1003 "Marc Hugzman"
- 1004 "Pieter Rozfield"

0 item
Selected

None

<
>

Cancel
Save

*DOD extension selection*

1. 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.

< DOD

Direct Outward Dialing (DOD) 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.

+ Add DOD
↻ Import
↵ Export

DOD ↕	DOD NAME ↕	EXTENSIONS ↕	OPTIONS
918273645	Test	<div style="display: flex; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">1000</div> <div style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">1001</div> <div style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">1002</div> </div>	<div style="display: flex; gap: 5px;"> <span style="font-size: 1.2em;">✎</span> <span style="font-size: 1.2em;">✖</span> </div>

<
1
>

Total: 1
 10 / page
Goto
1

*Edit DOD*

**Note**

Users can import and export DOD files.

## SLA STATION

The UCM630xA 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 UCM630xA is like BLF but SLA is used to monitor external line i.e., analog trunk on the UCM630xA. 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 UCM630xA.

### Create/Edit SLA Station

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

SLA Station			
<input type="button" value="+ Add"/> <input type="button" value="Delete"/>			
<input type="checkbox"/> STATION NAME	STATION	ASSOCIATED SLA TRUNKS	OPTIONS
<input type="checkbox"/> FXO1	1000	test	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Total: 1    10 / page    Goto 1

### SLA Station

- Click on  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.

### SLA Station Configuration Parameters

<b>Station Name</b>	Configure a name to identify the SLA Station.
<b>Station</b>	Specify a SIP extension as a station that will be using SLA.
<b>Available SLA Trunks</b>	Existing Analog Trunks with SLA Mode enabled will be listed here.
<b>Associated SLA Trunks</b>	<p>Select a trunk for this SLA from the Available SLA Trunks list. Click on <input type="button" value="Up"/> <input type="button" value="Down"/> 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.</p>
<b>SLA Station Options</b>	
<b>Ring Timeout</b>	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.
<b>Ring Delay</b>	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.
<b>Hold Access</b>	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

- On the UCM630xA, 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.

\* FXO Port:  1  2

\* Trunk Name:

Advanced Options

SLA Mode:

Enable SLA Mode for Analog Trunk

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

Analog Trunks				
Analog Trunks <span>Call Progress Tone File List</span>				
TRUNKS	DISABLE	TRUNK MODE	ANALOG PORTS	OPTIONS
test	no	sla	1	

Total: 1  / page

Analog Trunk with SLA Mode Enabled

1. On the UCM630xA, 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".

STATION NAME	STATION	ASSOCIATED SLA TRUNKS	OPTIONS
FXO1	1000	test	

Total: 1  / page

SLA Example – SLA Station

1. On the SIP phone 1, configure to register UCM630xA extension 1002. Configure the MPK as BLF mode and the value must be set to "extension\_trunkname", which is 1002\_fxo1 in this case.
2. On the SIP phone 2, configure to register UCM630xA extension 1005. Configure the MPK as BLF mode and value must be set to "extension\_trunkname", which is 1005\_fxo1 in this case.

Mode	Account	Description	Value
MPK 1	Busy Lamp Field (BLF)	Account 2	1005_fxo1

SLA Example – MPK Configuration

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

- o **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.

- o **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.

- o **Answering call using LINE key**

When the station is ringing, pressing the LINE key to answer the incoming call.

- o **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


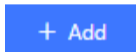


### Outbound Routes

In the following sections, we will discuss the steps and parameters used to configure and manage outbound rules in UCM630xA, 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 UCM630xA, 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  to add a new outbound route.
-  Click on to edit the outbound route.
-  Click on to delete the outbound route.

On the UCM630xA, the outbound route priority is based on "Best matching pattern". For example, the UCM630xA 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.

### Outbound Route Configuration Parameters

<b>Outbound Rule Name</b>	Configure the name of the calling rule (e.g., local, long_distance, and etc.). Letters, digits, _ and – are allowed.
<b>Pattern</b>	<p>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:</p> <ul style="list-style-type: none"> <li>○ [12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 is allowed.</li> <li>○ N ... Any digit from 2-9.</li> <li>○ . ... Wildcard, matching one or more characters.</li> <li>○ ! ... Wildcard, matching zero or more characters immediately.</li> <li>○ X ... Any digit from 0-9.</li> <li>○ Z ... Any digit from 1-9.</li> <li>○ – ... Hyphen is to connect characters and it will be ignored.</li> <li>○ [] Contain special characters ([x], [n], [z]) represent letters x, n, z.</li> </ul>
<b>Disable This Route</b>	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.
<b>Password</b>	Configure the password for users to use this rule when making outbound calls.
<b>Local Country Code</b>	If your local country code is affected by the outbound blacklist, please enter it here to bypass the blacklist.

<b>Call Duration Limit</b>	Enable to configure the maximum duration for the call using this outbound route.
<b>Maximum Call Duration</b>	Configure the maximum duration of the call (in seconds). The default setting is 0, which means no limit.
<b>Warning Time</b>	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.
<b>Auto Record</b>	If enabled, calls using this route will automatically be recorded.
<b>Warning Repeat Interval</b>	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.
<b>PIN Groups</b>	Select a PIN Group
<b>PIN Groups with Privilege Level</b>	If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied.
<b>Privilege Level</b>	<p>Select privilege level for the outbound rule.</p> <ul style="list-style-type: none"> <li>○ <b>Internal:</b> The lowest level required. All users can use this rule.</li> <li>○ <b>Local:</b> Users with Local, National, or International level can use this rule.</li> <li>○ <b>National:</b> Users with National or International level can use this rule.</li> <li>○ <b>International:</b> The highest level required. Only users with international level can use this rule.</li> <li>○ <b>Disable:</b> The default setting is "Disable". If selected, only the matched source caller ID will be allowed to use this outbound route.</li> </ul> <p>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.</p>
<b>Enable Filter on Source Caller ID</b>	<p>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".</p> <p>The following two methods can be used at the same time to define the extensions as the source caller ID.</p> <ol style="list-style-type: none"> <li>1. Select available extensions/extension groups from the list. This allows users to specify arbitrary single extensions available in the PBX.</li> <li>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.</li> </ol> <ul style="list-style-type: none"> <li>○ All patterns are prefixed with the "_".</li> <li>○ Special characters:</li> </ul> <p><b>X:</b> Any Digit from 0-9.</p> <p><b>Z:</b> Any Digit from 1-9.</p> <p><b>N:</b> Any Digit from 2-9.</p> <p><b>.":</b> Wildcard. Match one or more characters.</p> <p><b>!:</b> Wildcard. Match zero or more characters immediately.</p> <p>Example: [12345-9] – Any digit from 1 to 9.</p> <p>Note: Multiple patterns can be used. Patterns should be separated by comma ",". Example: _X. , _NNXXNXXXXX , _818X.</p>
<b>Outbound Route CID</b>	Attempt to use the configured outbound route CID. This CID will not be used if DOD is configured.
<b>Send This Call Through Trunk</b>	

<b>Trunk</b>	Select the trunk for this outbound rule.
<b>Strip</b>	<p>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.</p> <p>Example:</p> <p>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.</p>
<b>Prepend</b>	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.
<b>Use Failover Trunk</b>	
<b>Failover Trunk</b>	<p>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.</p> <p>UCM630xA support up to 10 failover trunks.</p> <p>Example:</p> <p>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.</p>
<b>Strip</b>	<p>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.</p> <p>Example:</p> <p>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.</p>
<b>Prepend</b>	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.
<b>Time Condition</b>	
<b>Time Condition Mode</b>	<p>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.</p> <p>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.</p>

## Failover Trunk Toggles

An outgoing calling rule associates an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks. For example, "local" allows 7-digit dialed through FXO port while "long distance" allows 10-digit dialed through a low-cost SIP trunk. A failover trunk can be set up to be used when the primary trunk fails. Note: This panel only manages individual outgoing calling rules.

[+ Add](#) [Scheduled Sync](#) [Outbound Blacklist](#) [PIN Groups](#) **[Failover Trunk Toggles](#)** [Import](#) [Export](#)

SEQUENCE	NAME	PATTERN	PRIVILEGE LEVEL	OPTIONS
1	out	_2X. _9X.	Internal	
2	Outbound	_X.	Local	

Failover Trunk Toggles

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

< Failover Trunk Toggles [Cancel](#) [Save](#)

\* No-Failover Response Codes :

6 items Available

Search

- 403
- 404
- 408
- 480
- 503
- 603

1 item Selected

Search

- 486

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

No-Failover Response Codes

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

### Note

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

## Outbound Routes DOD

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

Outbound Routes

An outgoing calling rule associates an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks. For example, "local" allows 7-digit dialed through FXO port while "long distance" allows 10-digit dialed through a low-cost SIP trunk. A failover trunk can be set up to be used when the primary trunk fails. Note: This panel only manages individual outgoing calling rules.

[+ Add](#) [Scheduled Sync](#) [Outbound Blacklist](#) [PIN Groups](#) [Import](#) [Export](#)

SEQUENCE	NAME	PATTERN	PRIVILEGE LEVEL	OPTIONS
1	gd_out	_9X.	Internal	
2	Again_out	_X.	Internal	

Total: 2 / page: 10 / page: 1

Outbound Routes Page

< DOD: go\_out

When both the Outbound route and the Trunk are configured with DOD, the priority is: Outbound route>Trunk.

Direct Outward Dialing (DOD) 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.

[+ Add DOD](#) [Import](#) [Export](#)

DOD	DOD NAME	EXTENSIONS
369369	first dod	1000 1001 1002

---

< DOD: Again\_Out

When both the Outbound route and the Trunk are configured with DOD, the priority is: Outbound route>Trunk.

Direct Outward Dialing (DOD) 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.

[+ Add DOD](#) [Import](#) [Export](#)

DOD	DOD NAME	EXTENSIONS
852582	second DOD	1000 1001 1002

*DOD Configuration by Outbound Route*

## Outbound Blacklist

The UCM630xA 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.

< Outbound Blacklist

The blacklist (based on CalleID) is used for all outbound routes.

Country Codes:

- North America
- South America
- Europe
- Asia and the Middle East
- Africa
- Oceania

- North America
  - Anguilla 1264
  - Antigua and Barbuda 1268
  - Bahamas 1242
  - Barbados 1246
  - Bermuda 1441
  - Canada 1204 1226 1236 1249 ...

**Blacklist Manage**

\* Add Blacklist Rule:  [Add](#)

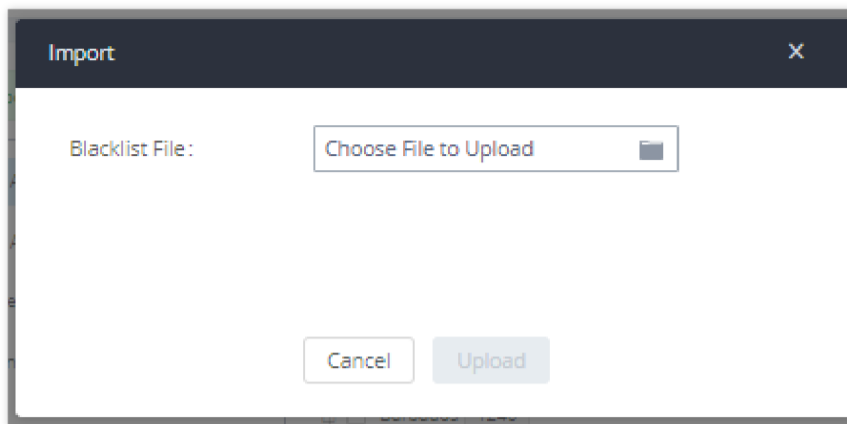
Blacklist list

[Clear](#) [Delete](#) [Import](#) [Export](#)

CONTINENT	COUNTRY	BLACKLIST RULE	OPTIONS
<p>No Data</p>			

*Country Codes*

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

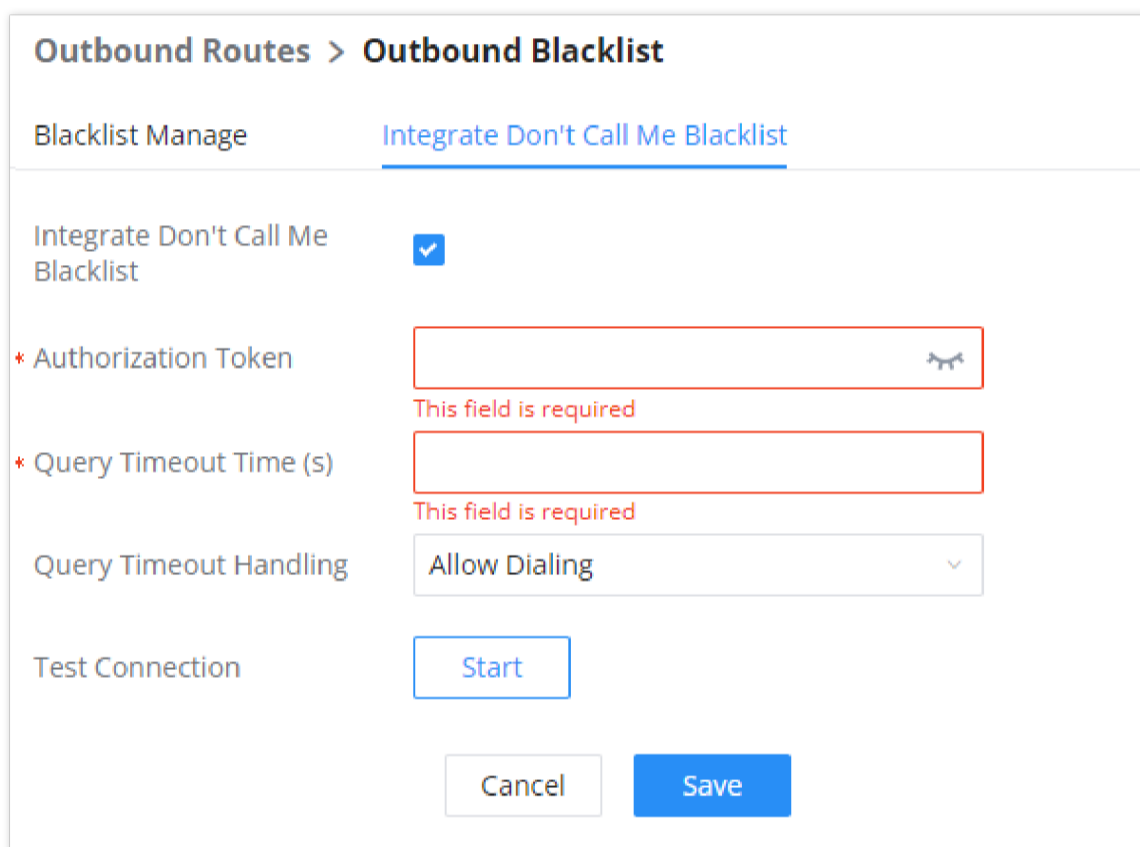


Blacklist Import/Export

### Don't Call Me Blacklist Integration

Don't Call Me database is a database on which people can register their numbers to prevent being called by marketers and salespersons. When the UCM6300 Series is integrated with this database and one of the extensions dials a phone number, it will be verified in the database. In case the number exists in the database, the call will not be permitted.

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



Don't Call Me Database Integration

Parameter	Description
<b>Integrate Don't Call Me Blacklist</b>	Enable or disable Don't Call Me integration
<b>Authorization Token</b>	Enter the authorization token generated by the Don't Call Me database.
<b>Query Timeout (s)</b>	Enter the duration after which the query is considered timed out.
<b>Query Timeout Handling</b>	Select the action to perform after the query timeout. <ul style="list-style-type: none"> <li>• <b>Allow Dialing:</b> If the query times out, the call will be allowed.</li> <li>• <b>Prohibit Dialing:</b> If the query times out, the call will be prohibited.</li> </ul>
<b>Test Connection</b>	Click on this button to test that the integration is working as intended. <b>Note:</b> If the database or Internet access is momentarily down, this test will fail.

## Scheduled Sync

The UCM630xA allows users to synchronize the outbound routes, this feature can be found on the Web GUI→**Extension/Trunk**→**Outbound Routes**→ **Scheduled Sync**.

Outbound Routes/Scheduled Sync

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

## PIN Groups

The UCM630xA 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**.

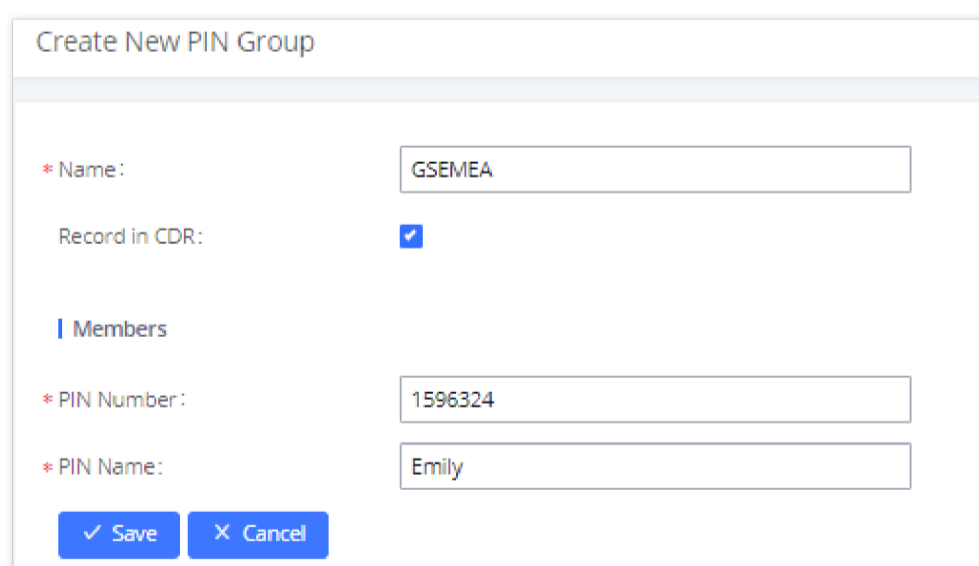
Outbound Routes/PIN Group

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

Once user click on

[PIN Groups](#)

the following figure shows to configure the new PIN.



Create New PIN Group

\* Name: GSEMEA

Record in CDR:

Members

\* PIN Number: 1596324

\* PIN Name: Emily

Create New PIN Group

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

< PIN Groups

[+ Add](#) [Upload](#)

NAME	RECORD IN CDR	OPTIONS						
GSEMEA	yes	<a href="#">Edit</a> <a href="#">Download</a> <a href="#">Delete</a>						
<table border="1"> <thead> <tr> <th>PIN NUMBER</th> <th>PIN NAME</th> </tr> </thead> <tbody> <tr> <td>125478963</td> <td>Dao</td> </tr> <tr> <td>1596324</td> <td>Emily</td> </tr> </tbody> </table>			PIN NUMBER	PIN NAME	125478963	Dao	1596324	Emily
PIN NUMBER	PIN NAME							
125478963	Dao							
1596324	Emily							

Total: 1 | 10 / page | Goto 1

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.

**General**

\* Calling Rule Name:       Disable This Route:

\* Pattern:       Privilege Level:

PIN Groups:       PIN Groups with Privilege Level:

Password:

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.

CDR [Display Filter](#)

By default, this page displays the CDR entries from the current month. Use the "Filter" button to specify a time range.

[Delete All](#) [Delete Search Result \(s\)](#) [Download All Records](#) [Download Search Result \(s\)](#) [Automatic Download](#)

STATUS	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
	5555	99856352 [Tr...	DIAL	2019-12-04 10:57:47	0:00:08	0:00:08	Emily/GSEMEA	-
	1000	*36	DIAL	2019-12-03 10:12:37	0:00:19	0:00:19	-	-

CDR Record

o 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.

< PIN Groups

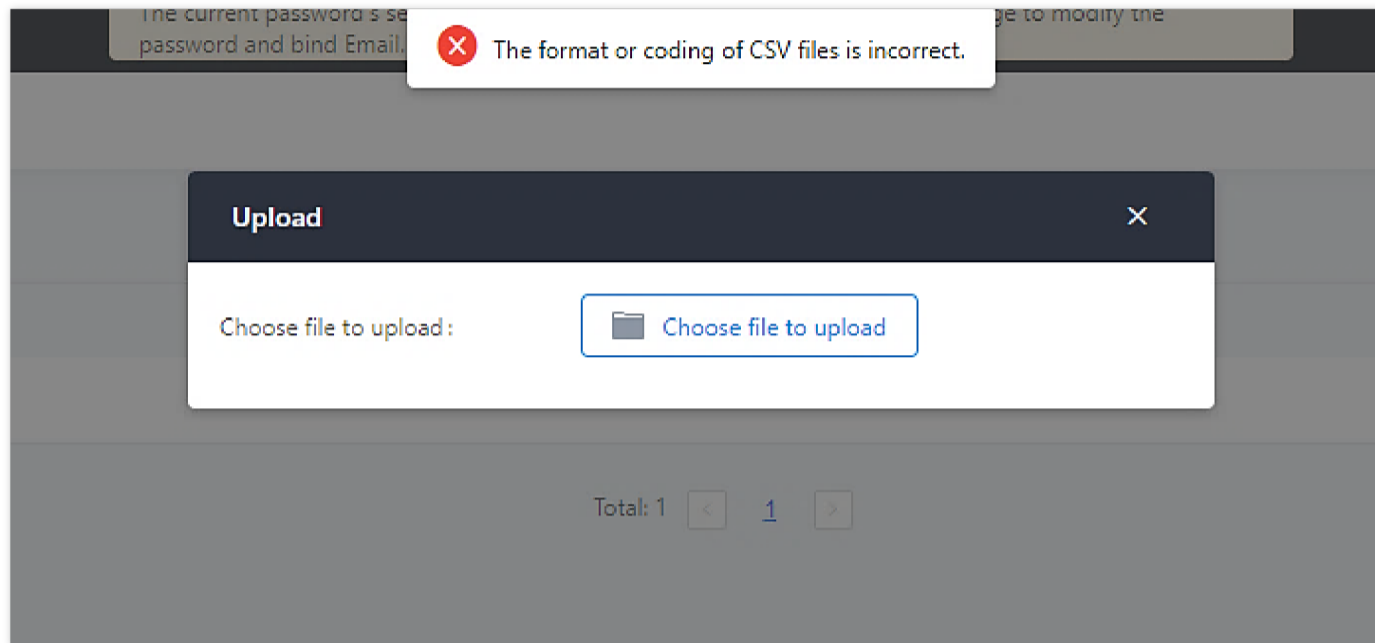
+ Add Upload

NAME	RECORD IN CDR	OPTIONS
GSEMEA	yes	

Total: 1 10 / page Goto 1

Importing PIN Groups from CSV files

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



Incorrect CSV File

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




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

CSV File Format

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

< PIN Groups

+ Add Upload

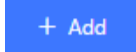


NAME ↕	RECORD IN CDR ↕	OPTIONS
GSEMEA	yes	  

Total: 1 10 / page Goto 1

CSV File Successful Upload

## Inbound Routes

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

- Click on  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

Inbound Rule Configuration Parameters

<b>Trunks</b>	Select the trunk to configure the inbound rule.
<b>Inbound Route Name</b>	Configure the name of the Inbound Route. For example, "Local", "LongDistance" etc.
<b>Pattern</b>	<p>All patterns are prefixed with the "_".</p> <p>Special characters:  <b>X</b>: Any Digit from 0-9. <b>Z</b>: Any Digit from 1-9. <b>N</b>: Any Digit from 2-9. <b>."</b>: Wildcard. Match one or more characters. <b>!"</b>: Wildcard. Match zero or more characters immediately. Example: [12345-9] – Any digit from 1 to 9.</p> <p><b>Notes:</b>            Multiple patterns can be used. Each pattern should be entered in a new line.</p> <p><b>Example:</b>            _X.            _NNXXNXXXXX /* 10-digit long distance */</p>
<b>Disable This Route</b>	After creating the inbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in the PBX. Users can enable it again when it is needed.
<b>CID Source</b>	<p>Configures the source of the CID to match with the configured CallerID Pattern.</p> <p><b>None:</b> CID is not obtained from any source. Only applicable if no CallerID Pattern is configured.</p> <p><b>DiversionID:</b> CID is obtained from the Diversion header. Only applicable to SIP trunks.</p> <p><b>CallerID:</b> If the call is from a SIP trunk, the CID is obtained from the From header. Otherwise, the CID will be obtained from other related signaling.</p>
<b>Seamless Transfer Whitelist</b>	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.
<b>Ringback tone</b>	Choose the custom ringback tone to play when the caller reaches the route.

<b>Auto Record</b>	If enabled, calls using this route will automatically be recorded.
<b>Block Collect Call</b>	If enabled, collect calls will be blocked. <b>Note:</b> Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call".
<b>Alert-Info</b>	Configure the Alert-Info, when the PBX receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.
<b>Fax Detection</b>	If enabled, fax signals from the trunk during a call will be detected.
<b>Fax Destination</b>	Configures the destination of faxes.  <ul style="list-style-type: none"> <li>• <b>Extension:</b> send the fax to the designated FXS/SIP extension (fax machine) or a FAX extension.</li> <li>• <b>Fax to Email:</b> 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-&gt;Fax/T.38-&gt;Fax Settings page.</li> </ul> <b>Note:</b> please make sure the sending email address is correctly configured in <b>System Settings-&gt;Email Settings</b> .
<b>Auto Answer</b>	If enabled, the PBX will automatically answer calls and receive faxes through the inbound route. If disabled, the PBX will not receive a fax until after the call has been answered. Enabling this option will slow down the answering of non-fax calls on the inbound route. The alert tone heard during the detection period can be customized.
<b>Block Collect Calls</b>	If enabled, collect calls will be <b>blocked</b> . <b>Note:</b> Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect <b>Call</b> ". <b>Note:</b> This is affected by Block Set Calls on the SIP Settings -> General Settings page.
<b>Prepend Trunk Name</b>	If enabled, the trunk name will be added to the caller id name as the displayed caller id name.
<b>Set Caller ID Info</b>	Manipulates Caller ID (CID) name and/or number within the call flow to help identify who is calling. When enabled two fields will show allowing to manipulate the CallerID Number and the Caller ID Name.
<b>CallerID Number</b>	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.  <ul style="list-style-type: none"> <li>• <b>`\${CALLERID(num)}`:</b> Default value which indicates the number of an incoming caller (CID). The CID will not be modified.</li> <li>• <b>`\${CALLERID(num):n}`:</b> Skips the first n characters of a CID number, where n is a number.</li> <li>• <b>`\${CALLERID(num):-n}`:</b> Takes the last n characters of a CID number, where n is a number.</li> <li>• <b>`\${CALLERID(num):s:n}`:</b> 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).</li> <li>• <b>n`\${CALLERID(num)}`:</b> Prepends n to a CID number, where n is a number.</li> </ul>
<b>CallerID Name</b>	The default string is <b>`\${CALLERID(name)}`</b> , which means the name of an incoming caller, it is a pattern-matching syntax format. <b>A`\${CALLERID(name)}`B</b> means Prepend a character 'A' and suffix a character 'B' to <b>`\${CALLERID(name)}`</b> . Not using pattern-matching syntax means setting a fixed name to the incoming caller.
<b>Enable Route-Level Inbound Mode</b>	Gives uses the ability to configure inbound mode per individual route. When enabled two fields will show allowing to set the Inbound mode and the Inbound mode Suffix. <b>Note:</b> Global inbound mode must be enabled before users can configure route-level inbound mode.
<b>Inbound Mode</b>	Choose the inbound mode for this route. <b>Note:</b> 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.
<b>Inbound Mode Suffix</b>	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.
<b>Inbound Multiple Mode</b>	Multiple mode allows users to switch between destinations of the inbound rule by feature codes. Configure related feature codes as described in [Inbound Route: Multiple Mode]. If this option is enabled, the user can use feature code to switch between different modes/destinations.
<b>CallerID Name Lookup</b>	If enabled, the callerID will be resolved to a name through local LDAP. Note, if a matched name is found, the original callerID name will be replaced. The name lookup is performed before other callerID or callerID name modifiers (e.g., Inbound Route's Set CallerID Info or Prepend Trunk Name). <b>Note:</b> Name lookup may impact system performance.
<b>Dial Trunk</b>	This option shows up only when "By DID" is selected. If enabled, the external users dialing into the trunk via this inbound route can dial outbound calls using the PBX's trunk.
<b>Privilege Level</b>	<p>This option shows up only when "By DID" is selected.</p> <ul style="list-style-type: none"> <li>● <b>Disable:</b> Only the selected Extensions or Extension Groups are allowed to use this rule when enabled Filter on Source Caller ID.</li> <li>● <b>Internal:</b> The lowest level required. All users are allowed to use this rule, checking this level might be risky for security purposes.</li> <li>● <b>Local:</b> Users with Local level, National or International level are allowed to use this rule.</li> <li>● <b>National:</b> Users with National or International Level are allowed to use this rule.</li> <li>● <b>International:</b> The highest level required. Only users with an international level are allowed to use this rule.</li> </ul>
<b>Allowed DID Destination</b>	<p>This option shows up only when "By DID" is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination is:</p> <ul style="list-style-type: none"> <li>● Extension</li> <li>● Conference</li> <li>● Call Queue</li> <li>● Ring Group</li> <li>● Paging/Intercom Groups</li> <li>● IVR</li> <li>● Voicemail Groups</li> <li>● Dial By Name</li> <li>● All</li> </ul>
<b>Default Destination</b>	<p>Select the default destination for the inbound call.</p> <ul style="list-style-type: none"> <li>● Extension</li> <li>● Voicemail</li> <li>● Conference Room</li> <li>● Call Queue</li> <li>● Ring Group</li> <li>● Paging/Intercom</li> <li>● Voicemail Group</li> <li>● DISA</li> <li>● IVR</li> <li>● External Number</li> <li>● By DID</li> </ul> <p>When "By DID" is used, the PBX will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through.</p> <ul style="list-style-type: none"> <li>● Dial By Name</li> <li>● Callback</li> </ul>
<b>Strip</b>	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.
<b>Prepend</b>	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.

<b>Time Condition</b>	
<b>Start Time</b>	Select the start time "hour:minute" for the trunk to use the inbound rule.
<b>End Time</b>	Select the end time "hour:minute" for the trunk to use the inbound rule.
<b>Date</b>	Select "By Week" or "By Day" and specify the date for the trunk to use the inbound rule.
<b>Week</b>	Select the day in the week to use the inbound rule.
<b>Destination</b>	<p>Select the destination for the inbound call under the defined time condition.</p> <ul style="list-style-type: none"> <li>● Extension</li> <li>● Voicemail</li> <li>● Conference Room</li> <li>● Call Queue</li> <li>● Ring Group</li> <li>● Paging/Intercom</li> <li>● Voicemail Group</li> <li>● DISA</li> <li>● IVR</li> <li>● By DID</li> </ul> <p>When "By DID" is used, the PBX will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through.</p> <p>Configure the number of digits to be stripped in the "Strip" option.</p> <ul style="list-style-type: none"> <li>● Dial By Name</li> <li>● External Number</li> <li>● Callback</li> </ul>

### Inbound Route: Prepend Example

UCM630xA 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, UCM630xA will strip the first 8 digits.
3. If Prepend is set to 2, UCM630xA will then prepend a 2 to the stripped number, now the number become 2163.
4. UCM630xA will now forward the incoming call to extension 2163.

\* Trunks: SIPTrunks -- test

\* Pattern: \_18005251163

Disable This Route:

Alert-info: None

Fax Detection:

Block Collect Calls:

Set CallerID Info:

Dial Trunk:

Inbound Multiple Mode:

CallerID Pattern:

Allowed to seamless transfer:

Prepend Trunk Name:

Enable Route-Level Inbound Mode:

Allowed DID Destination: Extension x

**Default Mode** Mode 1

\* Default Destination: By DID

Strip: 8

Prepend: 2

Inbound Route feature: Prepend

## Inbound Route: Multiple Mode

In the UCM630X, the user can configure an inbound route to enable multiple mode to switch between different destinations. The inbound multiple mode can be enabled under Inbound Route settings (**Global Inbound Multi-Mode** must be enabled first) .

Inbound Routes > Create New Inbound Rule

**Call Setting**

Ringback Tone: None

Alert-info: None

Auto Record:

Fax Detection:

Block Collect Calls:

**CallerID Setting**

Prepend Trunk Name:

Set CallerID Info:

CallerID Name Lookup:

**Inbound Mode**

Inbound Multi-Mode:

Custom Inbound Mode:

**Default Mode** Mode 1

\* Default Destination:

Cancel Save

Inbound Route – Inbound Multi-Mode

When Multiple Mode is enabled for the inbound route, the user can configure a "Default Destination" and up to 9 destination modes for all routes (Mode 1, Mode 2, etc). By default, 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" for example and dial feature code \*61 to switch back to "Default Destination". These feature codes can be customized under Inbound Routes Set Global Inbound Mode (please make sure they are not in conflict with other configured feature codes on the UCM630x). 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 7 PM. 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 Global Inbound Multi-Modes, click on [Set Global Inbound Mode](#) under the "Inbound Routes" page, check the "Global Inbound Multi-Mode" option, and change "Inbound Default Mode" and "Inbound Mode 1" values (By default, \*61 and \*62 respectively).

Users can also add modes by clicking on the "Add Mode" button. (Up to 8 additional modes).

### Inbound Routes > Set Global Inbound Mode

This feature can be used to change inbound modes either through the web UI or feature codes. To use this feature, please enable "Inbound Multiple Mode" and configure each mode.

Global Inbound Multi-Mode

Global Inbound Mode

BLF Subscription Number

#### Inbound Mode Toggle Feature Code

\* Default Mode

\* Mode 1

[Add Mode +](#)

*Inbound Route – Global Inbound Multi-Mode Feature Codes*

## Inbound Route: Custom Inbound Mode

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

**Inbound Routes > Create New Inbound Rule**

Block Collect Calls

**CallerID Setting**

Prepend Trunk Name  Set CallerID Info

CallerID Name Lookup

**Inbound Mode**

Inbound Multi-Mode

Inbound Mode

**Custom Inbound Mode**

\* Inbound Mode Feature Code

**Default Mode** | Mode 1

\* Default Destination

**Time Condition**

Time Condition	Time	Week	Month	Day	Destination	Options

*Inbound Route – Custom Inbound Mode*

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

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

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

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

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

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

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

To do this, please refer to the following steps:

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

## Inbound Routes > Set Global Inbound Mode

This feature can be used to change inbound modes either through the web UI or feature codes. To use this feature, please enable "Inbound Multiple Mode" and

Global Inbound Multi-Mode

Global Inbound Mode

Mode 1

BLF Subscription Number

777

### Inbound Mode Toggle Feature Code

\* Default Mode

\*61

\* Mode 1

\*62

Mode 2

\*63

Mode 3

\*64

Mode 4

\*69

Mode 5

\*70

Add Mode

Cancel

Save

Global Inbound Mode – BLF Subscription Number

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



Inbound Mode – Default Mode

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



Inbound Mode – Mode 1

## Inbound Route: Third-party Database Search

This feature allows the user to enter to integrate the UCM with a third-party database which contains the phone numbers and their matching names. When a call is received on a specific inbound route, the callerID will be checked against the database, if it's found, then the corresponding name will be displayed.

**Important Note**

This feature uses MySQL queries, therefore, it will function with MySQL databases.

**Inbound Routes**

Buttons: Add, Blacklist, Set Global Inbound Mode, **Third-party Database Search**, Import, Export, Filter

SIP Trunks -- Grandstrea

Inbound Route Name	Pattern	CallerID Pattern	Inbound Mode	Inbound Mode Function Code	Time Condition	Time	Destination	Options
No data								

*Inbound Routes*

Once the user clicks on "Third-party Database Search", it will open the configuration page, as seen in the figure below.

**Inbound Routes > Third-party Database Search**

Third-party Database Search

\* MySQL Host

\* Database

\* Username

\* MySQL Password

\* Character Set

\* Query Key

Table	Caller Name	Number
phonebook	name	number

**Info:** Enter the 3 information of the target phonebook in the database, you can contact the database administrator to get the appropriate keywords for the query. For example, if the table name is "phonebook", the caller name is "name", the number is "number", the SQL statement will be executed: `SELECT name FROM phonebook WHERE number LIKE '%[NUMBER]%'`;

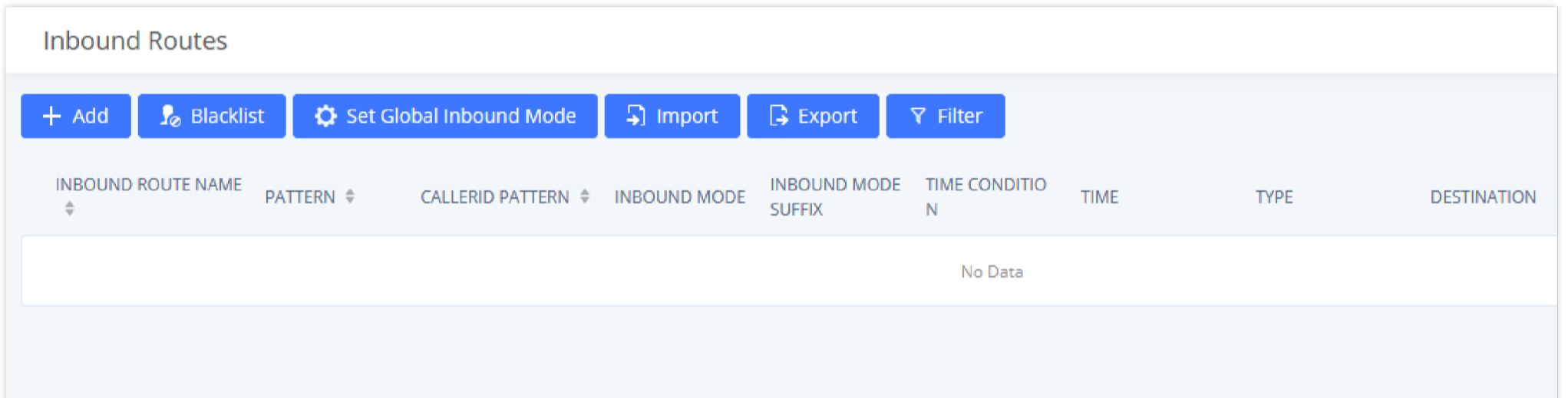
Test Connection

*Third-party Database Search Configuration*

<b>Third-party Database Search</b>	Enable or disable the feature.
<b>MySQL Host</b>	Specifies the hostname or IP address of the MySQL server.
<b>Database</b>	The name of the MySQL database that stores caller information.
<b>Username</b>	Enter the username used to connect to the MySQL database.
<b>MySQL Password</b>	Enter the password for the specified MySQL username.
<b>Character Set</b>	Specifies the character set for MySQL connections.
<b>Query Key</b>	Enter the 3 information of the target phonebook in the database, you can contact the database administrator to get the appropriate keywords for the query. For example, if the table name is "phonebook" , the caller name is "name" , the number is "number" , the SQL statement will be executed: <b>SELECT</b> name <b>FROM</b> phonebook <b>WHERE</b> number <b>LIKE</b> '%[NUMBER]%' ;
<b>Test Connection</b>	Test the connection to the database

### 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.



*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.

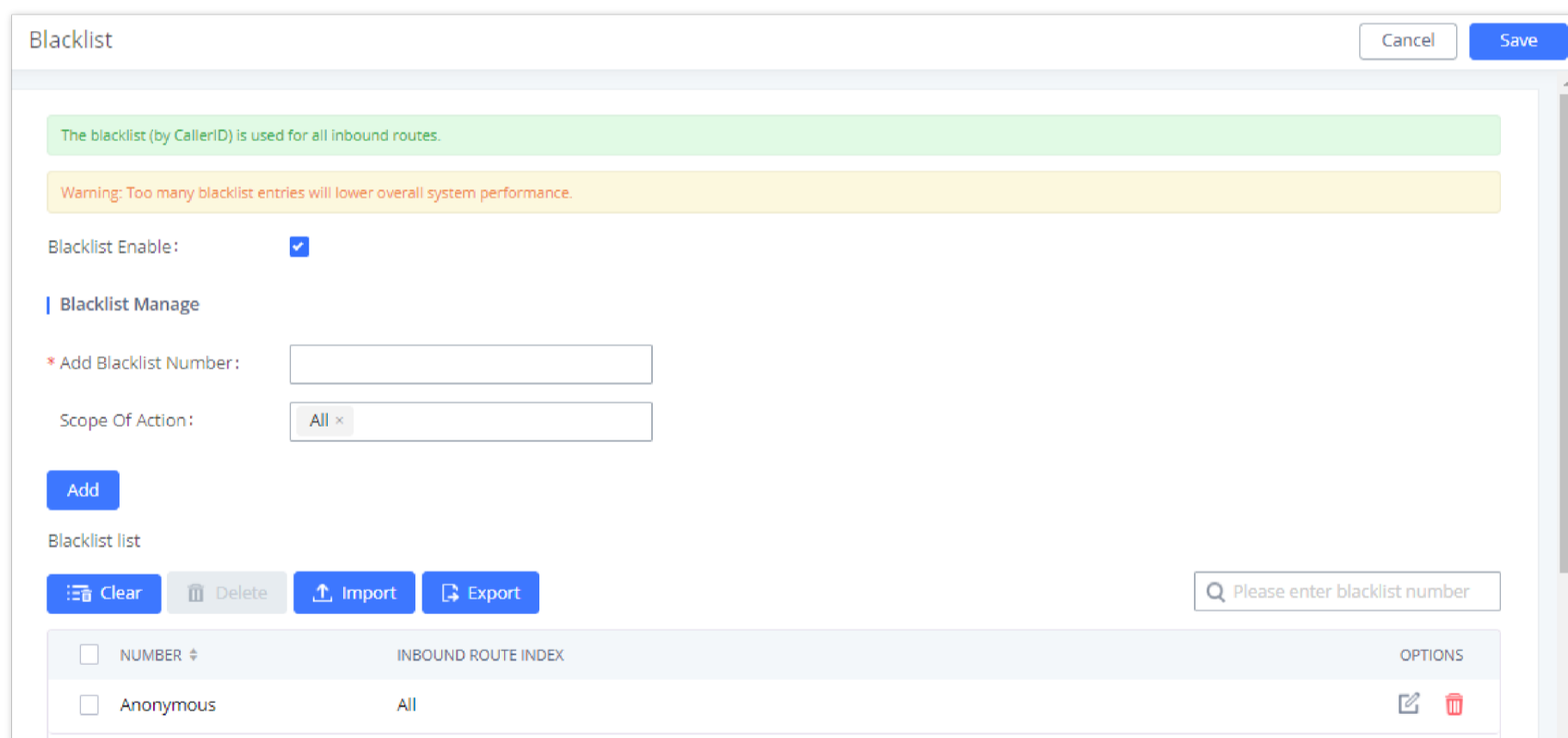
## FAX with Two Media

The UCM630xA supports Fax re-INVITE with multiple codec negotiation. If a Fax re-INVITE contains both T.38 and PCMA/PCMU codec, UCM630xA will choose T.38 codec over PCMA/PCMU.

## Blacklist Configurations

In the UCM630xA, Blacklist is supported for all inbound routes. Users could enable the Blacklist feature and manage the Blacklist by clicking on "Blacklist".

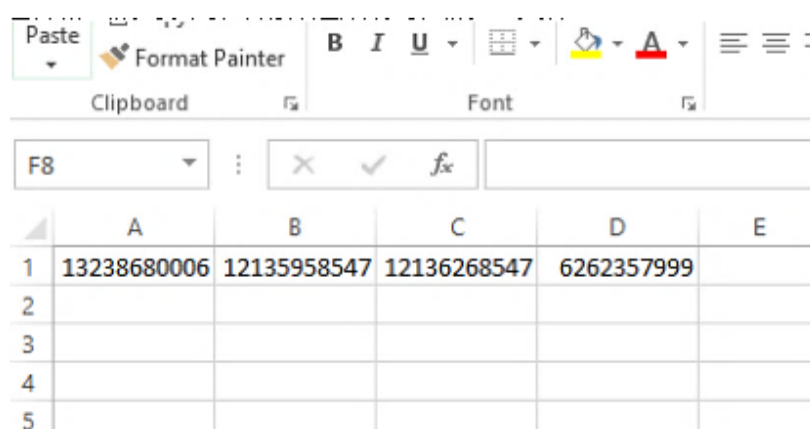
- Select the checkbox for "Blacklist Enable" to turn on Blacklist feature for all inbound routes. Blacklist is disabled by default.
- Enter a number in "Add Blacklist Number" field and then click "Add" to add to the list. Anonymous can also be added as a Blacklist Number by typing "Anonymous" in Add 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  button.



The screenshot shows the 'Blacklist' configuration window. At the top, there are 'Cancel' and 'Save' buttons. Below that, a green box states 'The blacklist (by CallerID) is used for all inbound routes.' and a yellow warning box says 'Warning: Too many blacklist entries will lower overall system performance.' The 'Blacklist Enable' checkbox is checked. Under 'Blacklist Manage', there is an 'Add Blacklist Number' field and a 'Scope Of Action' dropdown set to 'All'. An 'Add' button is below. The 'Blacklist list' section has buttons for 'Clear', 'Delete', 'Import', and 'Export', and a search bar. A table below shows one entry: 'Anonymous' with 'All' in the 'INBOUND ROUTE INDEX' column and edit/delete icons in the 'OPTIONS' column.

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.



The screenshot shows a spreadsheet with a toolbar at the top. The data is as follows:

	A	B	C	D	E
1	13238680006	12135958547	12136268547	6262357999	
2					
3					
4					
5					



Blacklist csv File

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

## FAX SERVER

The UCM6300A 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 **Advanced 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.

**Fax Settings**

- Enable Error Correction Mode:
- Maximum Transfer Rate:
- Minimum Transfer Rate:
- Max Concurrent Sending Fax:
- Fax Queue Length:
- User Information in Fax Header:
- Fax Header Information:
- Default Email Address:  [Email Template](#)
- Send PDF Files Only:
- Enable Fax Resend:
- Max Resend Attempts:
- Fax Resend Frequency:

*Fax Settings*

### FAX/T.38 Settings

<b>Enable Error Correction Mode</b>	<p>Configure to enable Error Correction Mode (ECM) for the Fax.</p> <p>The default setting is "Yes".</p>
<b>Maximum Transfer Rate</b>	<p>Configure the maximum transfer rate during the Fax rate negotiation.</p> <p>The possible values are 2400, 4800, 7200, 9600, 12000 and 14400.</p> <p>The default setting is 14400.</p>
<b>Minimum Transfer Rate</b>	<p>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.</p>

<p><b>Max Concurrent Sending Fax</b></p>	<p>Configure the concurrent fax that can be sent by UCM6300A. Two modes "Only" and "More" are supported.</p> <ul style="list-style-type: none"> <li>○ <b>Only</b></li> </ul> <p>Under this mode, the UCM6300A allows only single user to send fax at a time.</p> <ul style="list-style-type: none"> <li>○ <b>More</b></li> </ul> <p>Under this mode, the UCM6300A supports multiple concurrent fax sending by the users.</p> <p>By default, this option is set to "only".</p>
<p><b>Fax Queue Length</b></p>	<p>Configure the maximum length of Fax Queue from 6 to 10.</p> <p>The default setting is 6.</p>
<p><b>User Information in Fax Header</b></p>	<p>If enabled this this will give users the option to send a special header in SIP fax messages.</p>
<p><b>Fax Header Information</b></p>	<p>Adds fax header into the fax file.</p>
<p><b>Default Email Address</b></p>	<p>Configure the Email address to send the received Fax to if user's Email address cannot be found.</p> <p><b>Note:</b></p> <p>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.</p>
<p><b>Template Variables</b></p>	<p>Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users.</p> <p>The template variables are:</p> <ul style="list-style-type: none"> <li>○ <code>\${CALLERIDNUM}</code> : Caller ID Number</li> <li>○ <code>\${CALLERIDNAME}</code> : Caller ID Name</li> <li>○ <code>\${RECEIVEEXTEN}</code> : The extension to receive the Fax</li> <li>○ <code>\${FAXPAGES}</code> : Number of pages in the Fax</li> <li>○ <code>\${VM_DATE}</code> : The date and time when the Fax is received</li> </ul>
<p><b>Send PDF Files Only</b></p>	<p>If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.</p>
<p><b>Enable Fax Resend</b></p>	<p>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 <i>Resend</i> button will appear in the File Send Progress list in <i>OtherFeatures</i> → <i>Fax Sending</i> to allow manual resending.</p>
<p><b>Max Resend Attempts</b></p>	<p>Configures the maximum attempts number to resend the fax.</p> <p>Default value is set to 5.</p>
<p><b>Fax Resend Frequency</b></p>	<p>Configures the Fax Resend Frequency.</p> <p>Default value is set to 50.</p>

## Receiving Fax

### Example Configuration to Receive Fax from PSTN Line

The following instructions describe how to use the UCM6300A to receive fax from PSTN line on the Fax machine connected to the UCM6300A FXS port.

1. Connect Fax machine to the UCM6300A FXS port.
2. Connect PSTN line to the UCM6300A 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".

Edit Analog Trunk: FAX

\* FXO Port:  1  2

\* Trunk Name: FAX

**Advanced Options**

SLA Mode:

Enable Polarity Reversal:

Current Disconnect Threshold (ms):  200

\* RX Gain: 0dB

\* TX Gain: 0dB

Use CallerID:

Fax Mode: None

Caller ID Scheme: Bellcore/Telcordia

\* FXO Dial Delay (ms): 0

Auto Record:

Disable This Trunk:

DAHDI Out Line Selection: Ascend

\* The Maximum Number of Call Lines: 0

Echo Cancellation Mode: Default

Direct Callback:

Configure Analog Trunk

1. Go to UCM6300A Web GUI→**Extension/Trunk**→**Extensions** page.
2. 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.

Create New Extension

Basic Settings | Media | Features | Specific Time | Follow Me

Cancel Save

\* Select Extension Type: FXS Extension

Select Add Method: Single

---

General

\* Extension: 1005

CallerID Number:

Voicemail: Local Voicemail

Skip Voicemail Password Verification:

Attach Voicemail to Email: Default

Disable This Extension:

Analog Station: FXS 1

\* Privilege: Internal

\* Voicemail Password: 96902350

Send Voicemail Email Notification: Default

Keep Voicemail after Emailing: Default

Emergency Calls CID:

Configure Extension for Fax Machine: FXS Extension

Create New Extension

Basic Settings | Media | Features | Specific Time | Follow Me

Cancel Save

Analog Settings

Call Waiting:

\* RX Gain: 0dB

\* MIN RX Flash (ms): 200

Enable Polarity Reversal:

3-way Calling:

\* Fax Mode: Fax Gateway

Use '#' as SEND:

\* TX Gain: 0dB

\* MAX RX Flash: 1250

\* Echo Cancellation: ON

\* Send CallerID After: 1

Fax to Email: Yes

Configure Extension for Fax Machine: Analog Settings

1. Go to Web GUI→**Extension/Trunk**→**Inbound Routes** page.

2. Create an inbound route to use the Fax analog trunk. Select the created extension for Fax machine in step 4 as the default destination.

Create New Inbound Rule

Cancel Save

\* Trunks: AnalogTrunks -- FAX

\* Pattern: s

Disable This Route:

Alert-info: None

Fax Detection:

Prepend Trunk Name:

Enable Route-Level:

Inbound Mode:

Inbound Route Name:

CallerID Pattern:

Seamless Transfer

Whitelist:

Ringback Tone: None

Auto Record:

Set CallerID Info:

Inbound Multiple Mode:

Default Mode Mode 1

\* Default Destination: Extension 1008 "Fax Extension"

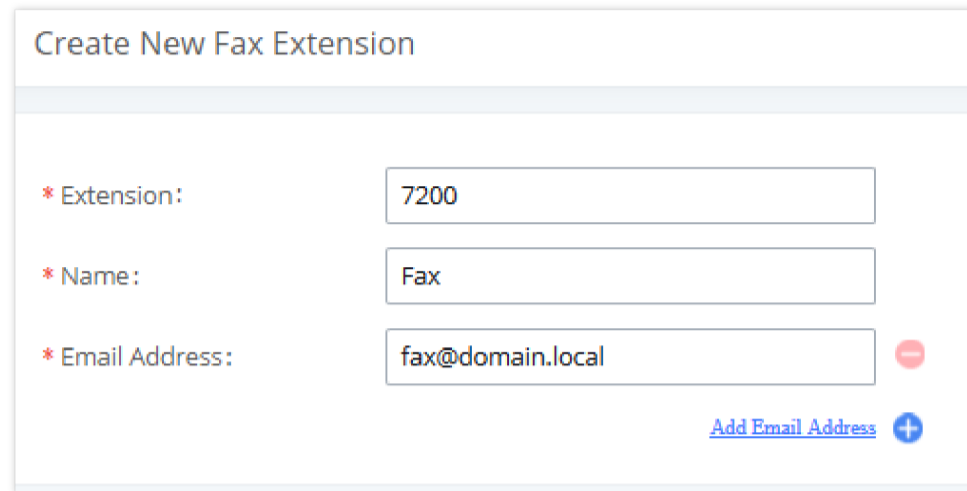
Configure Inbound Rule for Fax

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

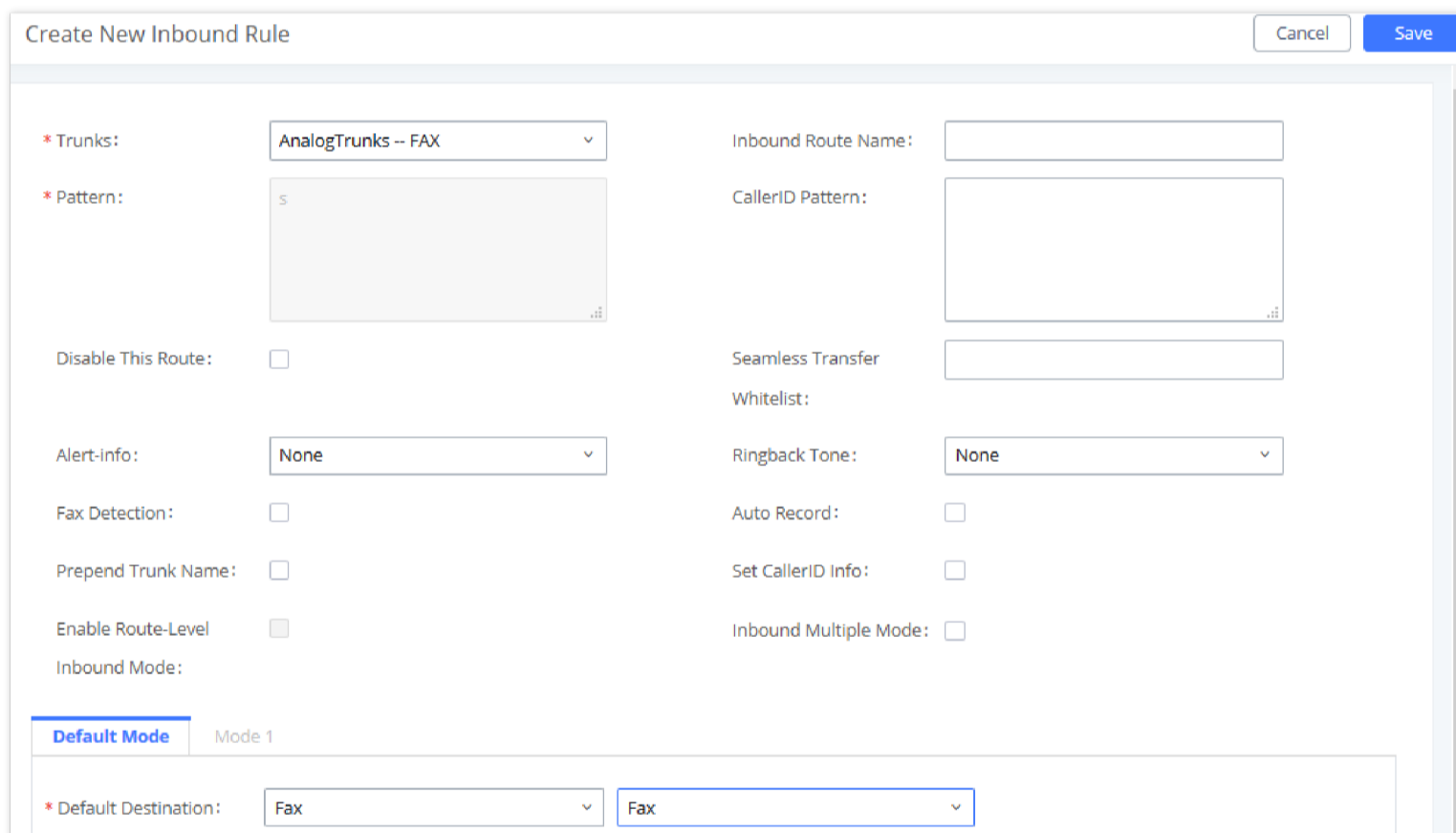
The following instructions describe a sample configuration on how to use Fax-to-Email feature on the UCM6300A.

1. Connect PSTN line to the UCM6300A FXO port.
2. Go to UCM6300A **Basic Call Feature** > **Fax/T.38** page. Create a new Fax extension.



*Create a Fax Extension*

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



*Inbound Route to a 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.

List of Fax Files				
Delete		Clear		Callee Number
NAME	DATE	SIZE	OPTIONS	
<input type="checkbox"/> VFAX-7200-20210125-112246-1611570166.49.pdf	2021-01-25 11:22:46 UTC+01:00	1.49 KB		
<input type="checkbox"/> VFAX-7200-20210125-112246-1611570166.49.tiff	2021-01-25 11:22:46 UTC+01:00	5.69 KB		

## FAX Sending

Besides the support of Fax machines, The supports also sending Fax via Web GUI access. This feature can be found on Web GUI→**Advanced Call 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 UCM6300A can reach out to PSTN numbers via the trunk, on Fax Sending page, enter the fax number and upload the file to be faxed. Then click on "Send" to start. The progress of sending fax will be displayed in Web GUI. Users can also view the sending history is in the same web page.

### Fax Sending

\* External Fax Number:

Fax File:

**File Send Progress**

*Fax Sending in Web GUI*

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

### Fax Sending

\* External Fax Number:

Fax File:

**File Send Progress**

<input type="checkbox"/>	NAME ↕	DATE ↕	SENDER ↕	EXTERNAL FAX NUMBER ↕	CURRENT PROGRESS ↕	OPTIONS
<input type="checkbox"/>	test.pdf	2021-01-25 11:29:19 UTC+01:00	admin	0123456789	Sending... 5%	<input type="button" value="Delete"/>

*Fax Send Progress*

### i Note

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



## MEETING

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

UCM630xA series	Number of meeting room	Participant limit
UCM6300A	3	50
UCM6302A	5	75
UCM6304A	7	120
UCM6308A	9	150

Below are the UCM meeting specifications supported for each model:

## Room

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

## Meeting Room Configuration Parameters

<b>Extension</b>	The number to dial to reach the meeting room.
<b>Meeting Name</b>	The name of the meeting room.
<b>Privilege</b>	Select the permission level for outgoing calls.
<b>Allow User Invite</b>	If enabled, participants can invite other users to the meeting.
<b>Allowed to Override Host Mute</b>	If enabled, participants will be able to unmute themselves if they have been muted by the host.
<b>Auto Record</b>	If enabled, the meeting audio will be recorded and saved as a .WAV file with default filename meeting- $\{Meeting\}$ Number- $\{UNIQUEID\}$ . Recordings can be downloaded from the Meeting Recordings page. <b>Note:</b> When this option has been enabled the meeting host cannot stop the recording of the meeting.
<b>Room Password</b>	If meeting room password is configured, meeting participants will need to enter a password to enter the room. Scheduling meetings will not be supported for this room.

### Note

Please note that you can't schedule meetings for the rooms which are protected by a password.

Meeting Settings contains the following options:

## Meeting Settings

<b>Enable Talk detection</b>	If enabled, the AMI will send the corresponding event when a user starts or ends talking.
------------------------------	---

<b>DSP Talking Threshold</b>	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.
<b>DSP Silence Threshold</b>	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.
<b>Audio Codec Preference</b>	Configures the preferred codecs for temporary accounts such as meeting participants who joined via link.
<b>Allow New Participants To View Chat History</b>	Configure whether new attendees joining in the middle of a Wave meeting can view the chat content already in the meeting.
<b>Jitter Buffer</b>	<p>Select jitter buffer method for temporary accounts such as meeting participants who joined via link.</p> <ul style="list-style-type: none"> <li>● <b>Disable:</b> Jitter buffer will not be used.</li> <li>● <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of "Jitter Buffer Size")</li> <li>● <b>Adaptive:</b> Jitter buffer with an adaptive size that will not exceed the value of "Max Jitter Buffer").</li> <li>● <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.</li> </ul>

## Schedule Meeting

Meeting Schedule can be found under UCM **Basic Call Features**→**Multimedia Meeting**→**Meeting Schedule**. Users can create, edit, view, and delete a Meeting Schedule.

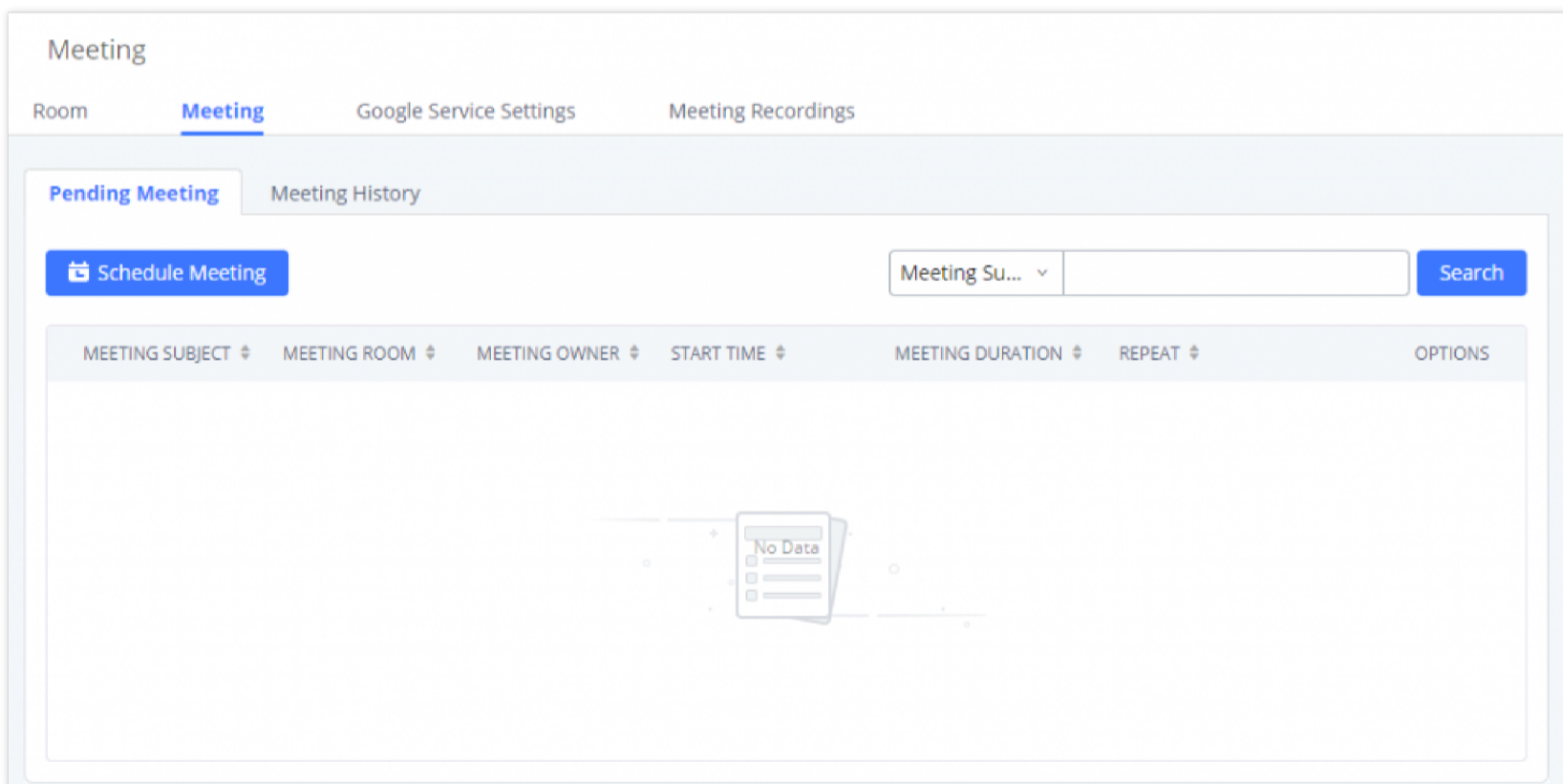
- Click on "Add" to add a new Meeting Schedule.
- Click on the scheduled meeting to edit or delete the event.

### Meeting Schedule Parameters

Schedule Options	
<b>Meeting Subject</b>	Configure the name of the scheduled meeting. Letters, digits, some special characters are also supported. Characters ` % # ? < > @ \$ ^ ~   are not allowed.
<b>Meeting Room</b>	Choose which room to have this scheduled meeting. If this option has been enabled, please select an existing room for this meeting. If this option has not been enabled, a new meeting room will be created.
<b>Time</b>	Configure the meeting date and time.
<b>Time Zone</b>	Select the meeting time zone.
<b>Password</b>	Configure the meeting's login password.
<b>Host Password</b>	Configure the Host Password. <b>Note:</b> It is randomly generated when first creating a new meeting Schedule.
<b>Host</b>	Configure Host.
<b>Repeat</b>	<p>Choose when to repeat a scheduled meeting.</p> <ul style="list-style-type: none"> <li>● <b>No Repeat</b></li> <li>● <b>Every Day</b></li> <li>● <b>Weekly</b></li> <li>● <b>Monthly</b></li> <li>● <b>Custom:</b> it specifies how often the meeting is repeated per days/weeks. E.g., every 3 days/weeks.</li> </ul>

<b>Allow User Invite</b>	If enabled, participants will be able to invite others to the meeting by pressing 1 on their keypad or by clicking the Participants->Invite option.
<b>Call Participant</b>	If enabled, the invited participants will be called upon meeting start time.
<b>Allowed to Override Host Mute</b>	If enabled, participants will be able to unmute themselves if they have been muted by the host.
<b>Email Reminder (m)</b>	Check to enable scheduled meeting email reminder. Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-120. 60 is the default value. <b>Note:</b> After editing the time of a single recurrence of a scheduled meeting, a cancellation email will be sent out followed by a meeting update email.
<b>Auto Record</b>	If selected, the meeting will be recorded and saved as either a .WAV or .MKV file. The default filename is meeting- $\{Meeting\ Number\}$ - $\{UNIQUEID\}$ . Recordings can be downloaded from either the Meeting Recordings or the Meeting Video Recordings page. Video recordings require external storage to be available. When recording a screen share, only the screen share and meeting audio will be recorded. <b>Note:</b> Please note that UCM63XX Audio Series doesn't support Screen Sharing, Whiteboard, or PDF file sharing.
<b>Enable Google Calendar</b>	Select this option to sync scheduled meeting with Google Calendar. <b>Note:</b> Google Service Setting OAuth2.0 must be configured on the IPPBX. Please refer to section <b>[Google Service Settings Support]</b> .
<b>Meeting Agenda</b>	Enter information about the meeting, e.g., the purpose of the meeting or the subjects that will be discussed in the meeting.
<b>Invitees</b>	Local extensions, remote extensions, and special extensions are supported.

Once created, at the scheduled meeting time, UCM630xA will send INVITE to the extensions that have been selected for meeting.



Meeting Schedule

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

Unstarted Meeting		Historical Meeting					Schedule Meeting	
CONFERENCE SUBJECT	CONFERENCE ROOM	CONFERENCE OWNER	START TIME	MEETING DURATION	REPEAT	OPTIONS		
test <span>Ongoing</span>	6301	lili	Today 15:50 Etc/GMT-1	00:15:00	No Repeat			

< 1 >

Total: 1 10 / page

*Meeting Scheduled-Ongoing*

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

Unstarted Meeting		Historical Meeting						
CONFERENCE SUBJECT	CONFERENCE ROOM	CONFERENCE OWNER	START TIME	MEETING DURATION	REPEAT	OPTIONS		
test	6301	lili	2021-01-20 15:50	00:15:00	No Repeat			

< 1 >

Total: 1 10 / page

*Meeting 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


- 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).


## Meeting Recordings

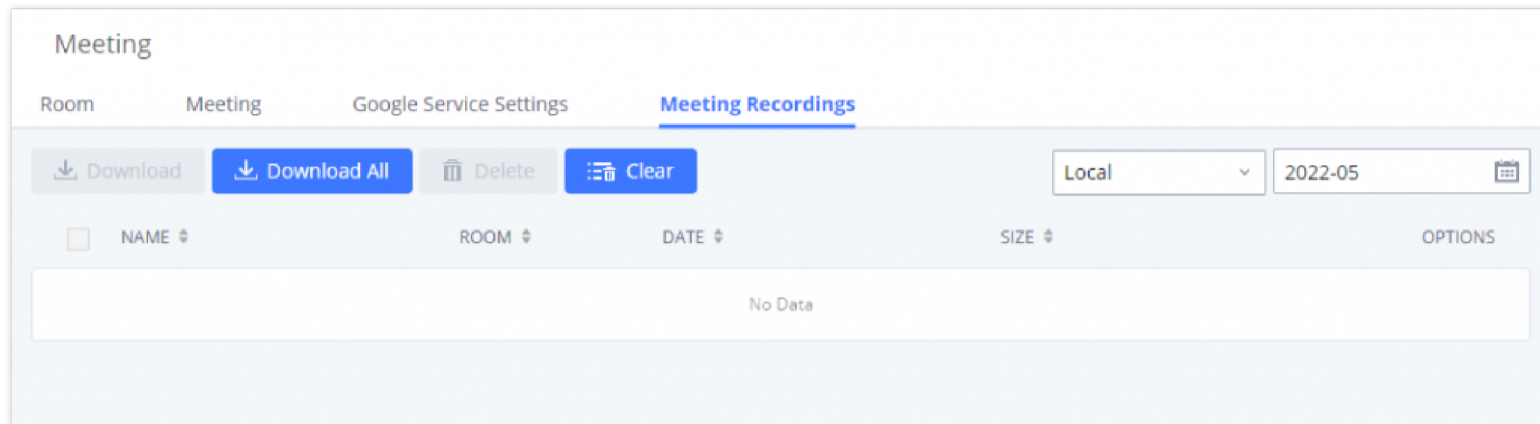
The UCM630xA allows users to record the meeting call and retrieve the recording from Web GUI → **Basic Call Features** → **Multimedia Meeting** → **Meeting Recordings**.

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

The recording files will be listed as below once available. Users could click on

 to download the recording or click on

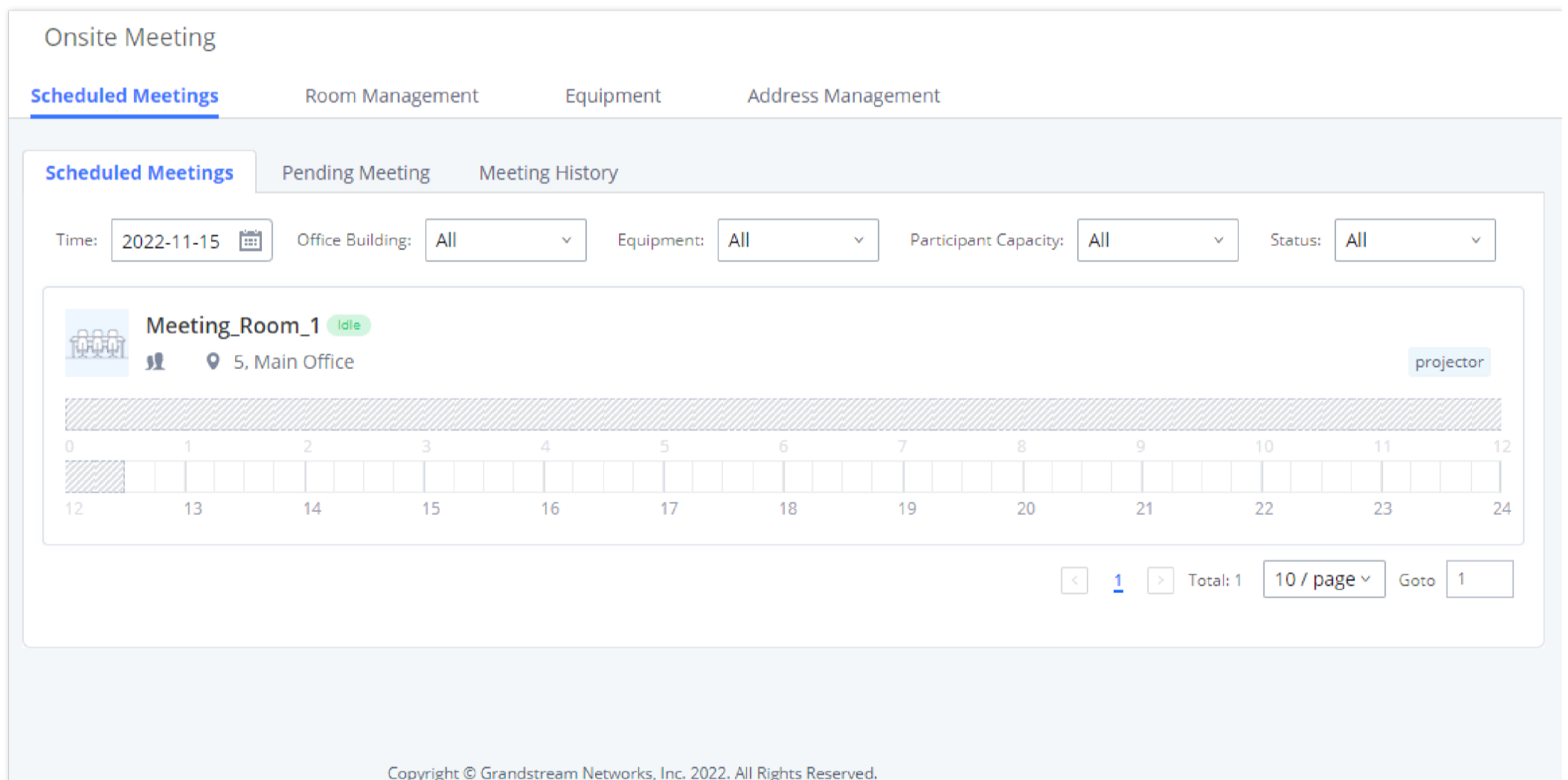
 to delete the recording. Users could also delete all recording files by clicking on “Delete All Recording Files” or delete multiple recording files at once by clicking on “Delete” after selecting the recording files.



Meeting Recordings

## ONSITE MEETING

For workplaces that require employees to return to physical offices for work, Grandstream UCM offers the Onsite Meeting feature, a new way to stay organized and keep up-to-date with in-person meetings. This feature allows administrators to create and manage onsite meeting rooms, specify meeting room locations, schedule meetings, and add conferencing equipment. The new feature can be found under the **Device Management > Onsite Meeting** page. The first page that appears is the **Scheduled Meetings** page and tab page, which provide an overview of all created meeting rooms. It provides information about the rooms’ meeting schedules for the day, their locations, their member capacity, and their equipment.



Scheduled Onsite Meeting

The **Pending Meeting** tab and **Meeting History** tab show detailed information about upcoming meetings and previous meetings respectively. From the **Pending Meeting** tab, users can delete upcoming meetings and extend the duration of ongoing meetings. **The Meeting History** tab will display the last 6 months of onsite meeting.

Onsite Meeting

Scheduled Meetings Room Management Facility Address Management

Scheduled Meetings Pending Meeting Meeting History

Schedule Meeting Meeting Subject Search

MEETING SUBJECT #	MEETING ROOM #	MEETING OWNER #	START TIME #	MEETING DURATION #	REPEAT #	OPTIONS
Quick Meeting <span>Starting soon</span>	BackupRoom		Today 20:00 Etc/GMT+8	00:30:00	No Repeat	
Recent Events	BackupRoom		2022-11-24 07:00 Etc/GMT+8	01:00:00	No Repeat	
Yearly Reports	Primary-Meeting-Room		2022-12-29 13:00 Etc/GMT+8	01:00:00	No Repeat	

Pending Onsite Meeting

When a meeting is scheduled the invitees will receive an invitation via email which contains all the information regarding the onsite meeting. The email will be attached with an .ics file which can be imported to a calendar to mark your calendar of the onsite meeting, please see the screenshot below.

**GRANDSTREAM**  
CONNECTING THE WORLD

**You have been invited to attend the following meeting.**

**Weekly\_Meeting**

Time 2024-03-29 15:00 -- 2024-03-29 16:00

Time Zone Etc/GMT-1 (GMT+01:00)

Host 1003

Room Meeting\_Room\_1

Address 2nd,Main Office,1640 Riverside Drive, Hill Valley, CA

Company Info | Contact Us  
© 2024 Grandstream Networks, Inc.

This is an automatically generated email. Please do not reply.

One attachment • Scanned by Gmail ⓘ

Meeting-33f96e39-8ff4-4bf5-9821-8bf1ba35bbba.ics [Download](#)

Onsite Meeting Email Invitation

## IVR

### Configure IVR

IVR configurations can be accessed under the UCM630xA Web GUI → **Basic Call Features** → **IVR**. Users could create, edit, view, and delete an IVR.

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

### Create New IVR

Basic Settings
Key Pressing Events

**Name :**

**Extension :**

Dial Trunk:

Auto Record:

Dial Other Extensions:  All  Extension  Audio Conference  Video Conference  Call Queue  
 Ring Group  Paging/Intercom Groups  Voicemail Groups  Fax Extension  
 Dial By Name

**IVR Black/Whitelist:**

Replace Display Name:

Return to IVR Menu:

Alert-info:

**Prompt:**  [Upload Audio File](#)

[Add Prompt](#) +

**Digit Timeout (s):**

**Response Timeout:**

**Response Timeout Prompt:**  [Upload Audio File](#)

**Invalid Input Prompt:**  [Upload Audio File](#)

**Response Timeout Prompt Repeats:**

**Invalid Input Prompt Repeats:**

Language:

*Create New IVR*

#### IVR Configuration Parameters

<b>Basic Settings</b>	
<b>Name</b>	Configure the name of the IVR. Letters, digits, _ and – are allowed.
<b>Extension</b>	Enter the extension number for users to access the IVR.
<b>Dial Trunk</b>	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”.
<b>Auto Record</b>	If enabled, calls to this IVR will automatically be recorded.
<b>Permission</b>	<p>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.</p> <p>The default setting is “Internal”. If the user tries to dial outbound calls after dialing into the IVR, the UCM630xA will compared the IVR’s permission level with the outbound route’s privilege level.</p> <p>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.</p>

<b>Dial Other Extensions</b>	<p>This controls the destination that can be reached by the external caller via the inbound route. The available destinations are:</p> <ul style="list-style-type: none"> <li>○ Extension</li> <li>○ Meeting</li> <li>○ Call Queue</li> <li>○ Ring Group</li> <li>○ Paging/Intercom Groups</li> <li>○ Voicemail Groups</li> <li>○ Dial by Name</li> <li>○ All</li> </ul>
<b>IVR Black/Whitelist</b>	If enabled only numbers inside of the Whitelist or outside of the Blacklist can be called from IVR.
<b>Internal Black/Whitelist</b>	Contain numbers, either of Blacklist or Whitelist.
<b>External Black/Whitelist</b>	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...
<b>Replace Display Name</b>	If enabled, the UCM will replace the caller display name with IVR name.
<b>Return to IVR Menu</b>	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
<b>Alert Info</b>	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.
<b>Prompt</b>	Select an audio file to play as the welcome prompt for the IVR. Click on "Prompt" to add additional audio file under Web GUI→ <b>PBX Settings</b> → <b>Voice Prompt</b> → <b>Custom Prompt</b> .
<b>Digit Timeout</b>	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 UCM630xA will consider the entries complete. Default timeout is 3s.
<b>Response Timeout</b>	After playing the prompts in the IVR, the UCM630xA 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.
<b>Response Timeout Prompt</b>	Select the prompt message to be played when timeout occurs.
<b>Invalid Input Prompt</b>	Select the prompt message to be played when an invalid extension is pressed.
<b>Response Timeout Prompt Repeats</b>	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.
<b>Invalid Input Prompt Repeats</b>	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.
<b>Language</b>	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→ <b>PBX Settings</b> → <b>Voice Prompt</b> → <b>Language Settings</b> . The dropdown list shows all the current available voice prompt languages on the UCM630xA. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under Web GUI→ <b>PBX Settings</b> → <b>Voice Prompt</b> → <b>Language Settings</b> .
<b>Key Pressing Events</b>	

<p><b>Key Press Event:</b></p> <p><b>Press 0</b></p> <p><b>Press 1</b></p> <p><b>Press 2</b></p> <p><b>Press 3</b></p> <p><b>Press 4</b></p> <p><b>Press 5</b></p> <p><b>Press 6</b></p> <p><b>Press 7</b></p> <p><b>Press 8</b></p> <p><b>Press 9</b></p> <p><b>Press *</b></p>	<p>Select the event for each key pressing for 0-9, *, Timeout and Invalid. The event options are:</p> <ul style="list-style-type: none"> <li>○ Extension</li> <li>○ Voicemail</li> <li>○ Meeting Rooms</li> <li>○ Voicemail Group</li> <li>○ IVR</li> <li>○ Ring Group</li> <li>○ Queues</li> <li>○ Page Group</li> <li>○ Custom Prompt</li> <li>○ Hangup</li> <li>○ DISA</li> <li>○ Dial by Name</li> <li>○ External Number</li> <li>○ Callback</li> </ul> <p>For each key event, time condition can be configured. At the configured time condition, this IVR key event can be triggered. Office time, holiday time or specific time can be configured for time condition. Up to 5 time conditions can be added for each key.</p> <p>The available time conditions are 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday' and 'Specific Time'. If 'Specific Time' is selected, a new window will prompt for admin to configure start time, end time and frequency.</p>
<p><b>Timeout</b></p>	<p>When exceeding the number of defined answer timeout, IVR will enter the configured event when timeout. If not configured, then it will Hangup.</p>
<p><b>Invalid</b></p>	<p>Configure the destination when the Invalid Repeat Loop is done.</p>
<p><b>Time Condition</b></p>	<p>Configure the time condition for each key press event, so that it goes to the corresponding destination within a specified time.</p>

Edit IVR: test

Basic Settings **Key Pressing Events** Cancel Save

**Press 0**

Destination: Extension 3001 Time Condition: Specific Time +

TIME	WEEK	MONTH	DAY	OPTIONS
08:00-11:00	Sun Mon Tue Wed Thu Fri Sat	Default	Default	<a href="#">+</a>

[Add](#) +

**Press 1**

Destination: Select an Option Time Condition: All Time +

[Add](#) +

**Press 2**

Destination: Select an Option Time Condition: All Time +

[Add](#) +

**Press 3**

Destination: Select an Option Time Condition: All Time +

[Add](#) +

**Press 4**

Destination: Select an Option Time Condition: All Time +

[Add](#) +

Key Pressing Events

## Blacklist/Whitelist 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 black/whitelist.

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

- If the user selects "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.

Create New IVR

**Basic Settings**      Key Pressing Events

\* Name:

\* Extension:

Dial Trunk:

\* Permission:

Dial Other Extensions:  All  Extension  Conference  Video Conference  
 Call Queue  Ring Group  Paging/Intercom Groups  
 Voicemail Groups  Fax Extension  Dial By Name

\* IVR Black/Whitelist:

Internal Black/Whitelist:

28 items Available		2 items Selected	
<input type="checkbox"/>	1000	<input type="checkbox"/>	1001
<input type="checkbox"/>	1003	<input type="checkbox"/>	1002
<input type="checkbox"/>	1004		
<input type="checkbox"/>	1005		
<input type="checkbox"/>	1006		

External Blacklist/Whitelist:

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.

Alert-info:

\* Prompt:

[Add Prompt](#)

Click on Prompt to Create IVR Prompt

Once the IVR prompt file is successfully added to the UCM630xA, it will be added into the prompt list options for users to select in different IVR scenarios.

## Key Pressing Events

### Standard Key Event

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

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

Edit IVR: IVR-DISA

Basic Settings **Key Pressing Events** Cancel Save

**Press 0**

Destination:  Time Condition:  ⊖

Destination:  Time Condition:  ⊕

**Press 1**

Destination:  Time Condition:  ⊖

All Time ⊕

Office Time ⊖

Out of Office Time ⊕

**Holiday** ⊖

Out of Holiday ⊕

Out of Office Time or Holiday ⊕

Office Time and Out of Holiday ⊕

Key Pressing Events

**Note:**

If you select "Specific time", you need to select the start time and the end time.

The frequency supports two options: By week and By Month, by default the specific time does not include the holidays.

**Specific Time** ✕

Time:  -

Frequency:  By Week  By Month

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sept	Oct	Nov	Dec

Week  Day

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1							
2							
3							
4							
5							
6							

Excluding Holidays:

Cancel OK

Specific Time

**Custom Key Event**

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

### Create New IVR

Basic Settings
Key Pressing Events

Cancel
Save

Key Event Type:  Standard  Custom

Key Events

+ Add
Delete
Clear

Key:

🗑️

Destination:

Time Condition:

-
+

Other Settings

Timeout

Destination:

Time Condition:

-
+

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

*Key Pressing Event*

This new feature supports the following:

- Up to 100 custom key press events
- Each key combination can contain up to 8 characters (numbers and star (\*) only)
- Supports Time Conditions
- Different custom keys can have the same Destination and Time Condition

**i Note**

IVR option Dial Other Extensions will be disabled if using custom IVR keys.

## LANGUAGE SETTINGS FOR VOICE PROMPT

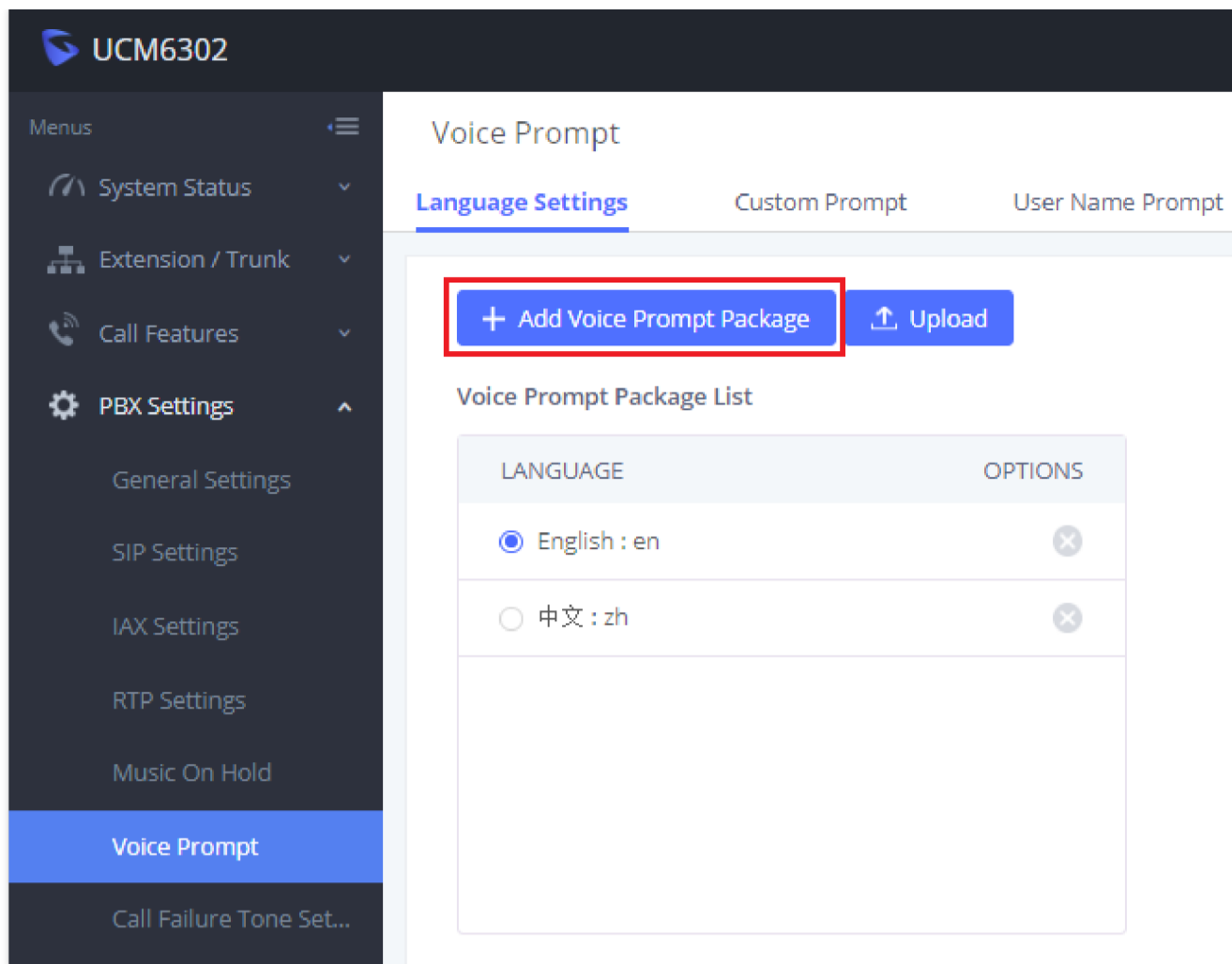
The UCM630xA supports multiple languages in Web GUI as well as system voice prompt. Currently, there are 16 languages supported in system voice prompt: British English, Deutsch, English, Spanish, Spanish (Catalonia), Spanish (Spain), Greek, French, Italian, Dutch, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Swedish, Turkish, Czech, Ukrainian, Hebrew, Arabic, and Chinese.

English (United States) and Chinese voice prompts are built in with the UCM630xA already. The other languages provided by Grandstream can be downloaded and installed from the UCM630xA Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the UCM630xA.

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 UCM630xA Web GUI, click on “Add Voice Prompt Package” button.




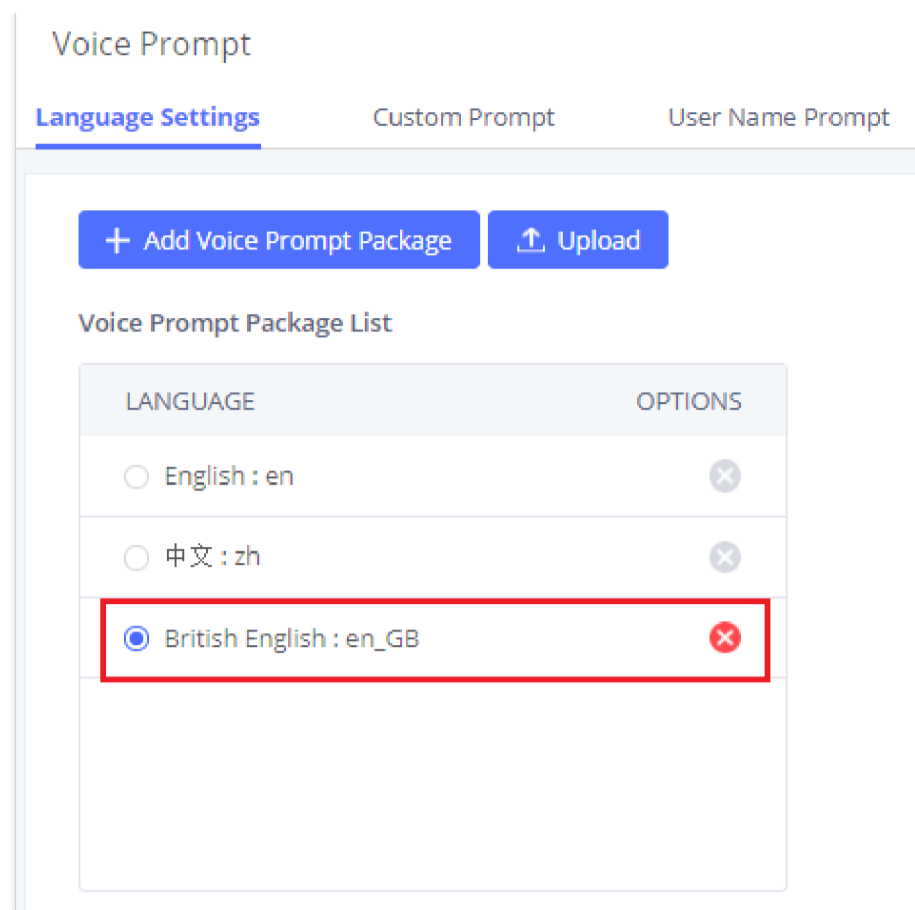
Language Settings for Voice Prompt

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



Voice Prompt Package List

Click on  to download the language to the UCM630xA. The installation will be automatically started once the downloading is finished.

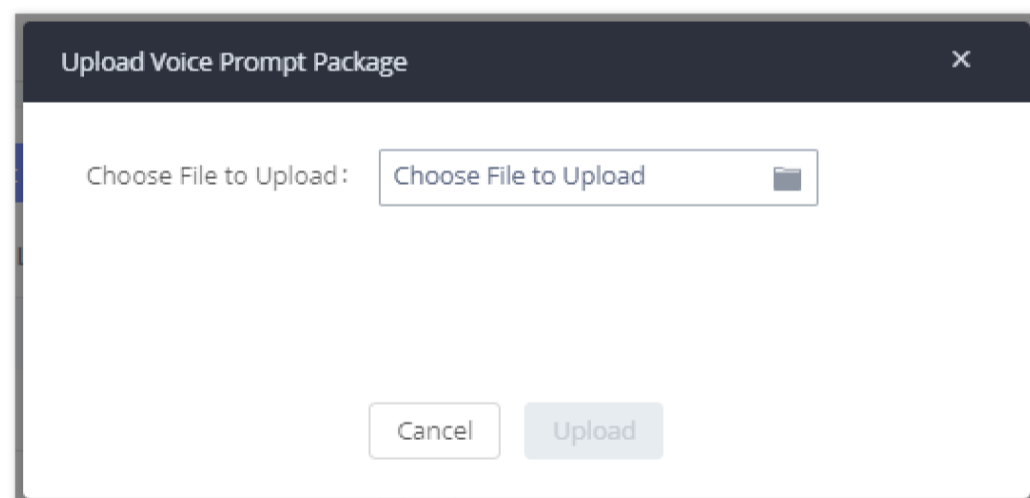


*New Voice Prompt Language Added*

A new language option will be displayed after successfully installed. Users then could select it to apply in the UCM630xA system voice prompt or delete it from the UCM630xA.

## Customize Specific Prompt

On the UCM630xA, 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.



*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.

1. Go under web GUI **PBX Settings** → **Voice Prompt** → **Username Prompt** and click on **“Upload”** button.

2. 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 UCM630xA extensions, the configurations of the voicemail can be globally set up and managed under **Basic Call Features**→**Voicemail**.

* Max Greeting Time (s):	<input type="text" value="60"/>
Dial "0" for Operator:	<input type="checkbox"/>
Operator Type:	<input type="text" value="Extension"/>
Operator Extension:	<input type="text" value="None"/>
* Max Messages Per Folder:	<input type="text" value="50"/>
Max Message Time:	<input type="text" value="15 minutes"/>
Min Effective Message Time:	<input type="text" value="3 seconds"/>
Announce Message Caller-ID:	<input type="checkbox"/>
Announce Message Duration:	<input type="checkbox"/>
Play Envelope:	<input checked="" type="checkbox"/>
Play Most Recent First:	<input type="checkbox"/>
Allow User Review:	<input type="checkbox"/>
Voicemail Remote Access:	<input type="checkbox"/>
Forward Voicemail to Peered UCMs:	<input type="checkbox"/>
Voicemail Password:	<input type="text"/>
Format:	<input type="text" value="GSM"/>

Voicemail Settings

<b>Max Greeting Time (s)</b>	Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds.
<b>Dial '0' For Operator</b>	If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator's extension.
<b>Operator Type</b>	Configure the operator type; either an extension or a ring group.
<b>Operator Extension</b>	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.
<b>Max Messages Per Folder</b>	Configure the maximum number of messages per folder in users' voicemail. The valid range 10 to 1000. The default setting is 50.
<b>Max Message Time</b>	<p>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:</p> <ul style="list-style-type: none"> <li><input type="radio"/> 1 minute</li> <li><input type="radio"/> 2 minutes</li> <li><input type="radio"/> 5 minutes</li> <li><input type="radio"/> 15 minutes</li> <li><input type="radio"/> 30 minutes</li> <li><input type="radio"/> Unlimited</li> </ul>
<b>Min Effective Message Time</b>	<p>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:</p> <ul style="list-style-type: none"> <li><input type="radio"/> No minimum</li> <li><input type="radio"/> 1 second</li> <li><input type="radio"/> 2 seconds</li> <li><input type="radio"/> 3 seconds</li> <li><input type="radio"/> 4 seconds</li> <li><input type="radio"/> 5 seconds</li> </ul> <p style="text-align: center;"><b>Note:</b> Silence and noise duration are not counted in message time.</p>
<b>Announce Message Caller-ID</b>	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".
<b>Announce Message Duration</b>	If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is "No".
<b>Play Envelope</b>	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".
<b>Play Most Recent First</b>	If enabled, it will play the most recent message first.
<b>Allow User Review</b>	If enabled, users can review the message following the IVR before sending.

<p><b>Voicemail Remote Access</b></p>	<p>If enabled, external callers routed by DID and reaching VM will be prompted by the UCM with 2 options:</p> <ul style="list-style-type: none"> <li>○ <i>Press 1 to leave a message.</i> To leave a message for the extension reached by DID.</li> <li>○ Press 2 to access voicemail management system.</li> </ul> <p>This will allow caller to access any extension VM after entering extension number and its VM password.</p> <p><b>Note:</b> This option applies to inbound call routed by DID only.</p> <p>The default setting is "Disabled".</p>
<p><b>Forward Voicemail to Peered UCMs</b></p>	<p>Enables the forwarding of voicemail to remote extensions on peered SIP trunks.</p> <p>The default setting is "Disabled".</p>
<p><b>Voicemail Password</b></p>	<p>Configures the default voicemail password that will be used when an extension is reset.</p>
<p><b>Format</b></p>	<p>Warning: WAV files take up significantly more storage space than GSM files.</p>

*Voicemail Settings*

**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 UCM630xA 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.

Main Menu	Sub Menu 1	Sub Menu 2
<p><b>1 – New messages</b></p>	<p>3 - Advanced options</p>	<p>1 - Send a reply</p>
		<p>2 - Call the person who sent this message</p>
		<p>3 - Hear the message envelop</p>
		<p>4 - Leave a message</p>
		<p>* - Return to the main menu</p>
	<p>5 - Repeat the current message</p>	
	<p>7 - Delete this message</p>	
	<p>8 - Forward the message to another user</p>	
	<p>9 – Save</p>	

	* - Help	
	# - Exit	
<b>2 – Change folders</b>	0 - New messages	
	1 - Old messages	
	2 - Work messages	
	3 - Family messages	
	4 - Friend messages	
	# - Cancel	
<b>3 – Advanced options</b>	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	
<b>0 – Mailbox options</b>	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		

### ✔ Tips

- While listening to the voicemail, press \* or # to rewind and forward the voice message, respectively. Each press will forward or rewind 3 seconds.
- Rewind can go back to the beginning of the message while forward will not work when there are 3 seconds or less left in the voice message.
- Voice guidance will be automatically played when the voicemail is done playing.

## 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 press 1 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 UCM630xA can be configured to send the voicemail as attachment to Email. Click on “Voicemail Email Settings” button to configure the Email attributes and content.

<b>Send Voicemail to Email</b>	If enabled, voicemail will be sent to the user’s email address. Note: SMTP server must be configured to use this option.
<b>Keep Voicemail after Emailing</b>	Enable this option if you want to keep recording files after the Email is sent. The default setting is Enable.
<b>Email Template</b>	<p>Fill in the “Subject:” and “Message:” content, to be used in the Email when sending to the user.</p> <p>The template variables are:</p> <ul style="list-style-type: none"><li>◦ \t: TAB</li><li>◦ \${VM_NAME}: Recipient’s first name and last name</li><li>◦ \${VM_DUR}: The duration of the voicemail message</li><li>◦ \${VM_MAILBOX}: The recipient’s extension</li><li>◦ \${VM_CALLERID}: The caller ID of the person who has left the message</li><li>◦ \${VM_MSGNUM}: The number of messages in the mailbox</li><li>◦ \${VM_DATE}: The date and time when the message is left</li></ul>

### Voicemail Email Settings

#### Voicemail Email Settings

Send Voicemail to Email:

Keep Voicemail after Emailing:

Emailing:

Email Template: [Email Template](#)

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

## Configure Voicemail Group

The UCM630xA 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 → **Basic Call Features** → **Voicemail** → **Voicemail Group**. Click on "Add" to configure the group.

**Voicemail > Create New Voicemail Groups**

\* Extension: 6600

\* Name: Name

\* Method:  Forwarded  Shared

Voicemail Password: Voicemail Password

Email Address: Email Address

Shared Voicemail Status:

Members:

- Available (5 Items): 5000, 5001, 5002, 5003, 5004
- Selected (0 Item): None

Voicemail prompt will be played to callers entering voicemail. Priority: Temporary Prompt > Unavailable Prompt > Name Prompt  
The audio file must be less than 30 MB in file size with a file extension of .mp3/.wav/.ulaw/.alaw/.gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate.

Buttons: Cancel, Save

Voicemail Group

<b>Extension</b>	Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members.
<b>Name</b>	Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed.
<b>Method</b>	Select the preference for receiving and managing group voicemail. <ul style="list-style-type: none"> <li>● <b>Forwarded:</b> Voicemail will be stored in the group voicemail box, and each voicemail group member will be forwarded a copy of it.</li> <li>● <b>Shared:</b> Voicemail will be stored in the group voicemail box, and voicemail status will be shared among all voicemail group members. If a member deletes a voicemail, it will also be deleted for all members. Likewise, if one member reads a voicemail, it will be considered read for the entire group.</li> </ul>
<b>Voicemail Password</b>	Configure the voicemail password for the users to check voicemail messages.
<b>Email Address</b>	Configure the Email address for the voicemail group extension.
<b>Shared Voicemail Status</b>	If enabled, voicemail group status can be monitored via BLF. Green indicates no unread voicemail, and red indicates existing unread voicemail.
<b>Members</b>	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.

<b>Greet Prompt</b>	<p>This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Temporary Prompt</b>	<p>This voicemail prompt will be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Unavailable Prompt</b>	<p>This voicemail prompt will be played when user enters voicemail. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>

## RING GROUP

The UCM630xA supports ring group feature with different ring strategies applied to the ring group members. This section describes the ring group configuration on the UCM630xA.

### Configure Ring Group

Ring group settings can be accessed via Web GUI→**Basic Call Features**→**Ring Group**.

EXTENSION	NAME	STRATEGY	MEMBERS	MESSAGE	OPTIONS
6400	TechSupport	Ring in Order	1000 1001 1002 1003 1004	Messages: 0/0/0	

Ring Group

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

<b>Ring Group Name</b>	Configure ring group name to identify the ring group. Letters, digits, _ and – are allowed.
<b>Extension</b>	Configure the ring group extension.
<b>Members</b>	Select available users from the left side to the ring group member list on the right side. Click on ▲ ▼ to arrange the order.
<b>LDAP Phonebook</b>	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.
<b>Ring Strategy</b>	Select the ring strategy. The default setting is “Ring in order”.

	<ul style="list-style-type: none"> <li>● <b>Ring Simultaneously:</b> 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.</li> <li>● <b>Ring in Order:</b> 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.</li> </ul>
<b>Music On Hold</b>	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.
<b>Custom Prompt</b>	<p>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.</p> <p><b>Note:</b> Users can also refer to the page <b>PBX Settings</b>→ <b>Voice Prompt</b>→ <b>Custom Prompt</b>, where they could record new prompt or upload prompt files.</p>
<b>Ring Timeout on Each Member</b>	<p>Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 60 seconds.</p> <p><b>Note:</b> The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.</p>
<b>Auto Record</b>	If enabled, calls on this ring group will be automatically recorded. The default setting is No. The recording files can be accessed from WebGUI→ <b>CDR</b> → <b>Recording Files</b> .
<b>Endpoint Call Forwarding Support</b>	<p>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.</p> <p>However, this feature has the following limitations:</p> <ul style="list-style-type: none"> <li>● This feature will work only when call forwarding is configured on endpoints, not on the UCM.</li> <li>● 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.</li> <li>● 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.</li> <li>● If the forwarded call hits voicemail, the other ring group members will no longer receive the call.</li> </ul>
<b>Replace Display Name</b>	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.
<b>Skip Busy Agent</b>	If enabled, skip busy agents regardless of call waiting settings.
<b>Enable Destination</b>	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.
<b>Default Destination</b>	<p>The call would be routed to this destination if no one in this ring group answers the call.</p> <p><b>Note:</b> 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.</p>
<b>Voicemail</b>	Whether to enable the voicemail for the ring group or not.
<b>Voicemail Password</b>	Configure the voicemail password (only numbers).
<b>Email Address</b>	Fill in the user's Email address (s), the voice message will be sent to this address (s).
<b>Busy Prompt</b>	<p>This voicemail prompt will be played when the callee is in another call or is in DND mode. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>

<p><b>Greet Prompt</b></p>	<p>This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<p><b>Temporary Prompt</b></p>	<p>This voicemail prompt will be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<p><b>Unavailable Prompt</b></p>	<p>This voicemail prompt will only be played when the callee's extension is unregistered. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>

**Create New Ring Groups**

\* Ring Group Name:

\* Extension:

Members:

<input type="checkbox"/> 27 items Available	<input type="checkbox"/> 3 items Selected
<input type="text" value="Search"/> <ul style="list-style-type: none"> <li><input type="checkbox"/> 1000</li> <li><input type="checkbox"/> 1001</li> <li><input type="checkbox"/> 1005</li> <li><input type="checkbox"/> 1006</li> <li><input type="checkbox"/> 1007</li> </ul>	<input type="text" value="Search"/> <ul style="list-style-type: none"> <li><input type="checkbox"/> 1002</li> <li><input type="checkbox"/> 1003</li> <li><input type="checkbox"/> 1004</li> </ul>

LDAP Phonebook:

<input type="checkbox"/> 0 item Available	<input type="checkbox"/> 0 item Selected
<input type="text" value="Search"/> <p style="text-align: center;">None</p>	<input type="text" value="Search"/> <p style="text-align: center;">None</p>

**Ring Group Options**

Ring Strategy:

Music On Hold:

Custom Prompt:  [Upload Audio File](#)

*Ring Group Configuration*

## Remote Extension in Ring Group

Remote extensions from the peer trunk of a remote UCM630xA 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 UCM630xA\_A and UCM630xA\_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 UCM630xA\_A update remote LDAP server automatically from peer UCM630xA\_B. In addition, Sync LDAP Password must match for UCM630xA\_A and UCM630xA\_B to sync LDAP contact automatically. Port number can be anything between 0~65535, and use the outbound rule created in step 1 for the LDAP Outbound Rule option.

Sync LDAP Enable:

\* Sync LDAP Password:

\* Sync LDAP Port:

LDAP Outbound Rule:

\* LDAP Dialed Prefix:

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 UCM630xA.

VoIP Trunks

VoIP Trunks Trunk Group

+ Add SIP Trunk + Add IAX Trunk

PROVIDER NAME	TERMINAL TYPE	TYPE	HOSTNAME/IP	USERNAME	OPTIONS
Gstest	SIP	peer	192.168.5.112		

Total: 1 10 / page Goto 1

Manually Sync LDAP Server

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

5. If LDAP server is synced correctly, Available LDAP Numbers box will display available remote extensions that can be included in the current ring group. Please also make sure the extensions in the peer UCM630xA can be included into that UCM630xA's LDAP contact.

Create New Ring Group

\* Ring Group Name:

\* Extension:

Members:

Available Extensions:  106  1000  1001  1002  1003

Selected Extensions:  0

LDAP Phonebook:  15

Available LDAP:  5000(ou=ucm6510,dc=pbx,dc=com)  5001(ou=ucm6510,dc=pbx,dc=com)  5002(ou=ucm6510,dc=pbx,dc=com)  5003(ou=ucm6510,dc=pbx,dc=com)

Selected LDAP:  0

Ring Group Options

Ring Group Remote Extension

## RESTRICT CALLS

Restrict calls is a feature that can be used to restrict calls between internal extensions besides those in the Allowed List.

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

Create New Restrict Calls

Name:

Restrict Calls between Extension:

Members:



Available	Selected
<input type="checkbox"/> 1 item <input type="checkbox"/> 1001	<input type="checkbox"/> 1 item <input type="checkbox"/> 1000

Allowed List:

Available	Selected
<input type="checkbox"/> 1 item <input type="checkbox"/> 1000	<input type="checkbox"/> 1 item <input type="checkbox"/> 1001

Restrict Calls

## Configure Restrict Calls

- Click on "Add" to add a rule for restrict calls.
- Click on  to edit the rule of restrict calls.
- Click on  to delete the rule of restrict calls.

<b>Name</b>	Configure Restrict call's name
<b>Restrict Calls between extensions</b>	When enabled, members of the group cannot dial other extension, only the numbers in the Allowed List. <b>Note:</b> It's enabled by default.
<b>Members</b>	Configure the members that will not be able to call any extensions besides those in the Allowed List.
<b>Allowed list</b>	Select the extensions that the Members list can be able to call.

## PAGING/INTERCOM

Paging and Intercom Group can be used to make an announcement over the speaker on a group of phones. Targeted phones will answer immediately using speaker. The UCM630xA paging and intercom can be used via feature code to a single extension or a paging/intercom group. This section describes the configuration of paging/intercom group under Web GUI → **Basic Call Features** → **Paging/Intercom**.

### Paging/Intercom Groups

#### 2-way Intercom

**Paging/Intercom > Create New Paging/Intercom Group**

Disable

\* Name

\* Strategy

\* Extension

Private Intercom

Auto Record

Replace Display Name

\* Maximum Call Duration (s)

Custom Prompt  [Upload Audio File](#)

Play Prompt to Caller

\* Members

5 items Available

Search

1000

1001

1002

0 item Selected

Search

None

*2-way Intercom*

Parameter	Configuration
<b>Disable</b>	If disabled, the real-time and scheduled paging/intercom will not be triggered.
<b>Name</b>	Enter a name for the intercom
<b>Type</b>	Choose "Private Intercom".
<b>Extension</b>	Configure the intercom group extension.
<b>Auto Record</b>	Enable this option to record in WAV format.
<b>Replace Display Name</b>	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
<b>Maximum Call Duration (s)</b>	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).
<b>Custom Prompt</b>	This option sets a custom prompt to be used as an announcement to the person receiving a paging/intercom call. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add additional record.
<b>Members</b>	Selected members will receive paging/intercom calls to this paging/intercom group.

<b>Paging/Intercom Whitelist</b>	Only selected extensions will be able to use this paging /intercom group. If none is selected, all extensions will be able to use this paging/intercom group.
----------------------------------	---

### Private Intercom

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

**Paging/Intercom > Create New Paging/Intercom Group**

Disable

\* Name

\* Strategy

\* Extension

**Private Intercom**

Auto Record

Replace Display Name

\* Maximum Call Duration (s)

Custom Prompt  [Upload Audio File](#)

Play Prompt to Caller

\* Members  5 items Available  0 item

Private Intercom

Parameter	Configuration
<b>Disable</b>	If disabled, the real-time and scheduled paging/intercom will not be triggered.
<b>Name</b>	Enter a name for the intercom
<b>Type</b>	Choose "Private Intercom".
<b>Extension</b>	Configure the intercom group extension.
<b>Auto Record</b>	Enable this option to record in WAV format.
<b>Replace Display Name</b>	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
<b>Maximum Call Duration (s)</b>	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).
<b>Custom Prompt</b>	This option sets a custom prompt to be used as an announcement to the person receiving a paging/intercom call. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add additional record.

<b>Members</b>	Selected members will receive paging/intercom calls to this paging/intercom group.
<b>Paging/Intercom Whitelist</b>	Only selected extensions will be able to use this paging /intercom group. If none is selected, all extensions will be able to use this paging/intercom group.

## 1-way Paging

**Paging/Intercom > Create New Paging/Intercom Group**

Disable

\* Name

\* Strategy

\* Extension

Video Broadcast

Auto Record

Replace Display Name

Delayed Paging

\* Maximum Call Duration (s)

Announcement File  [Upload Audio File](#)

Play Prompt to Caller

\* Members

5 items Available

0 item

1-way Paging

Parameter	Description
<b>Disable</b>	If disabled, the real-time and scheduled paging/intercom will not be triggered.
<b>Name</b>	Configure paging/intercom group name.
<b>Strategy</b>	Select "1-way Paging".
<b>Extension</b>	Configure the paging/intercom group extension.
<b>Video Broadcast</b>	If checked, video paging will be supported. If the caller sends a video page, the paging group members will be able to receive and view the video.
<b>Auto Record</b>	Enable this option to record in WAV format (audio) and MKV format (video).
<b>Replace Display Name</b>	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
<b>Delayed Paging</b>	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved,

	and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the prerecorded message will be played, and the call will end after it is finished playing.
<b>Maximum Call Duration</b>	Specify the maximum call duration in seconds. The default value 0 means no limit.
<b>Announcement File</b>	Configures an audio/video file to play to the paging members. This can be used to play preconfigured audio/video at the beginning of paging calls or to simply notify members that it is a paging/intercom call.
<b>Play Prompt to Caller</b>	Play the prompt to the caller.
<b>Members</b>	Select available users from the left side to the paging/intercom group member list on the right.
<b>Paging/Intercom Whitelist</b>	Select which extensions are allowed to use the paging/intercom feature for this paging group.

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

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

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

## Multicast Paging

Paging/Intercom > Create New Paging/Intercom Group

Disable

\* Name

\* Strategy

\* Extension

Delayed Paging

\* Maximum Call Duration (s)

Custom Prompt  [Upload Audio File](#)

Play Prompt to Caller

\* Prompt Playback Count

\* Multicast Address/Port   +

[Add Multicast IP Address](#) +

Paging/Intercom Allowlist  Selected  All

0 item Available

5 items Selected  
  
 1000

Multicast Paging

<b>Paging/Intercom</b>	Select existing paging/intercom groups and multicast communities.
<b>Name</b>	Enter the name of the scheduled Intercom/Paging.
<b>Caller</b>	Once a caller is selected, and the specified start time is reached, the system will contact the caller. If this call is rejected, the page/intercom will be cancelled. If caller is set to None, the system will call all group members and play the configured prompt.
<b>Start Date</b>	Select the date of the start of the paging/intercom.
<b>Start Time</b>	Select the start time of the paging/intercom.
<b>Repeat</b>	<p>Select the repeat interval of the paging/intercom.</p> <ul style="list-style-type: none"> <li>• <b>No Repeat:</b> The intercom/paging will play once on the scheduled date and time.</li> <li>• <b>Everyday:</b> The intercom/paging will play daily starting from the scheduled day and on the time scheduled every day.</li> <li>• <b>Weekly:</b> The intercom/paging will play weekly on the selected day(s) of the week.</li> <li>• <b>Monthly:</b> The intercom/paging will play monthly on the selected date of the month.</li> </ul>
<b>Include Holidays</b>	<p>When Every day, Weekly, or Monthly is selected. This option will appear.</p> <p>If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.</p>

### Sync to Google Calendar

This feature cannot be used if Google Services have not been authorized. Please resolve this in the **Integrations > Google Services** page.

## Multicast Community

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

### Paging/Intercom > Create New Multicast Community

\* Name

\* Extension

Delayed Paging

\* Maximum Call Duration (s)

Custom Prompt  [Upload Audio File](#)

Play Prompt to Caller

\* Prompt Playback Count

\* Multicast Paging Group

0 Available

0 Selected

Paging/Intercom  Selected  All

Multicast Community Parameters

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

	<ul style="list-style-type: none"> <li>• <b>No Repeat:</b> The intercom/paging will play once on the scheduled date and time.</li> <li>• <b>Everyday:</b> The intercom/paging will play daily starting from the scheduled day and on the time scheduled every day.</li> <li>• <b>Weekly:</b> The intercom/paging will play weekly on the selected day(s) of the week.</li> <li>• <b>Monthly:</b> The intercom/paging will play monthly on the selected date of the month.</li> </ul>
<b>Include Holidays</b>	<p>When Every day, Weekly, or Monthly is selected. This option will appear.</p> <p>If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.</p>
<b>Sync to Google Calendar</b>	<p>This feature cannot be used if Google Services have not been authorized. Please resolve this in the <b>Integrations &gt; Google Services</b> page.</p>

## Scheduled Paging/Intercom

### Pending Paging/Intercom


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


**Paging/Intercom > Create New Scheduled Paging/Intercom**

\* Paging/Intercom

\* Name

\* Caller

\* Start Date  

\* Start Time   -

[Add Start Time](#) +

Repeat

Sync to Google Calendar  [Google Services](#)

<b>Paging/Intercom</b>	Select existing paging/intercom groups and multicast communities.
<b>Name</b>	Enter the name of the scheduled Intercom/Paging.
<b>Caller</b>	Once a caller is selected, and the specified start time is reached, the system will contact the caller. If this call is rejected, the page/intercom will be cancelled. If caller is set to None, the system will call all group members and play the configured prompt.
<b>Start Date</b>	Select the date of the start of the paging/intercom.
<b>Start Time</b>	Select the start time of the paging/intercom.
<b>Repeat</b>	<p>Select the repeat interval of the paging/intercom.</p> <ul style="list-style-type: none"> <li>• <b>No Repeat:</b> The intercom/paging will play once on the scheduled date and time.</li> <li>• <b>Everyday:</b> The intercom/paging will play daily starting from the scheduled day and on the time scheduled every day.</li> <li>• <b>Weekly:</b> The intercom/paging will play weekly on the selected day(s) of the week.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Monthly:</b> The intercom/paging will play monthly on the selected date of the month.</li> </ul>
<b>Include Holidays</b>	When Every day, Weekly, or Monthly is selected. This option will appear. If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.
<b>Sync to Google Calendar</b>	This feature cannot be used if Google Services have not been authorized. Please resolve this in the <b>Integrations &gt; Google Services</b> page.

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

Name	Caller	Paging/Intercom Extension	Paging/Intercom Name	Strategy	Start Time	Repeat	Options
Multicast_Group	1000	1077	Multicast_Group	Multicast Paging	2024-03-07 15:00	No Repeat 15:00	
Paging	1003	1055	Paging	1-way Paging	2024-03-07 18:00	No Repeat 18:00	
Multicast_Group	1006	1077	Multicast_Group	Multicast Paging	2024-03-20 11:00	Wed, Tue, Thu, Fri, Mon 11:00	

### Paging/Intercom Schedule

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

**Paging/Intercom Groups**

Paging/Intercom Groups    Multicast Community    Scheduled Paging/Intercom

Pending Paging/Intercom    Paging/Intercom Schedule

2024    Mar    Today    < >    Mar 1 – 31, 2024    Day    Week    Month

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	01	02	03	04	05	06

Calendar events shown:

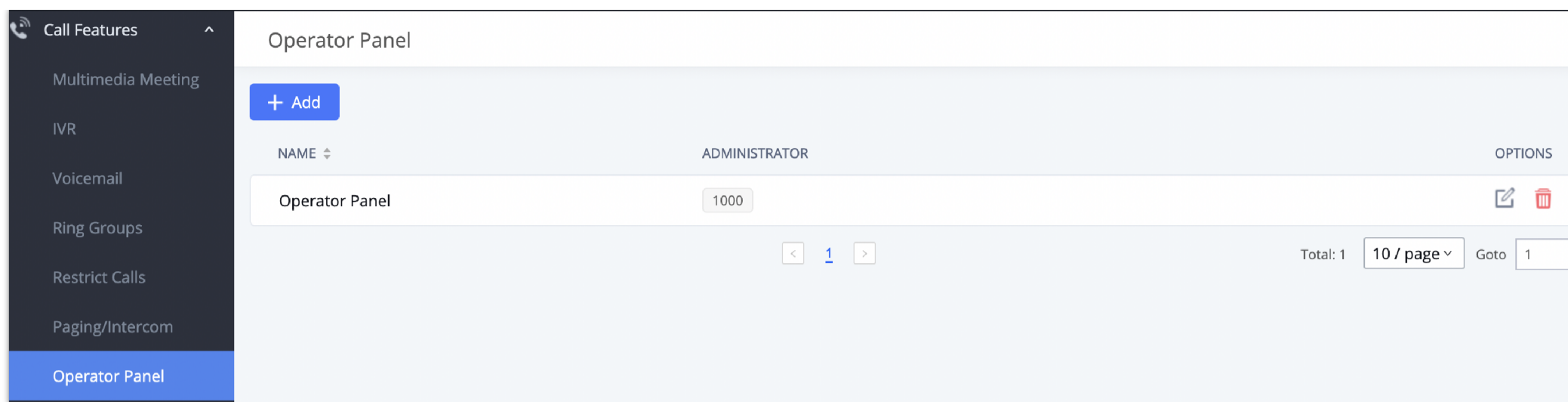
- 03:00 Multicast\_C
- 06:00 Paging
- 11:00 Multicast\_C
- 11:00 Multicast\_C
- 11:00 Multicast\_C

## OPERATOR PANEL



### Configure Operator Panel

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

The UCM630xA supports operator panel so that UCM extension can be used as admin to manage calls and activities such as extension status, call queue status, transfer, barge-in, hangup and etc. On Grandstream Wave client, it can display the extensions, ring group, voicemail, call queue, call park status under the management of the extension. This section describes how to configure operator panel.



Operator Panel Configuration Page

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

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

Operator Panel Settings

## 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→ **BasicCall Features**→**Call Queue**.

### Add Call Queue

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

Call Queue							
<a href="#">Call Queue</a>	<a href="#">Queue Recordings</a>	<a href="#">Queue Switchboard</a>	<a href="#">Call Queue Statistics</a>				
<a href="#">Add</a>	<a href="#">Global Queue Settings</a>						
Extension	Name	Strategy	Queue Chairman	Members			Options
6500	Help_Desk	Ring All	1005	1000	1001	1002	
6501	Sales	Ring All	1005	1003	1004	1005 1002	
6502	Marketing	Ring All	4005	4000	4001	4002 4003 4004	
6503	Support	Ring All	5009	5001	5002	5003 5004 5006	

Total: 4 < 1 > 10 / page Goto

Call Queue Page

- Click on "Add" to add call queue.
- Click on to edit the call queue.
- Click on to delete the call queue.

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

Basic Settings	
<b>General</b>	
<b>Extension</b>	Configure the call queue extension number.
<b>Name</b>	Configure the call queue name to identify the call queue.
<b>Strategy</b>	<p>Select the strategy for the call queue.</p> <ul style="list-style-type: none"> <li>● <b>Ring All:</b> Ring all available Agents simultaneously until one answers.</li> <li>● <b>Linear:</b> Ring agents in the specified order.</li> <li>● <b>Least Recent:</b> Ring the agent who has been called the least recently.</li> <li>● <b>Fewest Calls:</b> Ring the agent with the fewest completed calls.</li> <li>● <b>Random:</b> Ring a random agent.</li> <li>● <b>Round Robin:</b> Ring the agents in Round Robin scheduling with memory.</li> </ul> <p>The default setting is "Ring All".</p>
<b>Music On Hold</b>	<p>Select the <b>Music On Hold</b> class for the call queue.</p> <p><b>Note:</b> Music On Hold classes can be managed from <b>Web GUI→PBX Settings→Music On Hold</b>.</p>
<b>Max Queue Length</b>	Configure the maximum number of calls to be queued at once. This number does not include calls that have been connected with agents, only calls that are still in queue. When this maximum value is exceeded, the caller will hear a busy tone and be forwarded to the configured failover destination. Default value is 0 (unlimited).
<b>Agent Rest Time (s)</b>	Configure the amount of time in seconds after ending a call where the agent will not receive additional calls. Once this time has passed, the agent will be able to receive calls again. If set to 0, agents can receive additional calls immediately after ending a call. Default value is 10 seconds.
<b>Retry Time (s)</b>	Configure the number of seconds to wait before ringing the next agent. The minimum is 1 and the default setting is 5 seconds. Since only 3 digits can be entered, the max value is 999.
<b>Agent Ring Time</b>	Configure the number of seconds to ring an agent. The minimum is 5 and the default setting is 30 seconds. Since only 3 digits can be entered, the max value is 999.
<b>Auto Record</b>	<p>If enabled, the calls on the call queue will be automatically recorded. The recording files can be accessed in <b>Queue Recordings</b> under <b>Web GUI→Call Features→Call Queue</b>.</p> <p>Users can choose whether to automatically record only internal calls, external calls or all calls. By default, Auto Record is disabled.</p>

<b>Welcome Prompt</b>	
<b>Enable</b>	Enable the welcome prompt.
<b>Custom Prompt</b>	Choose the initial tone that plays when the user dials the queue number. <b>Note:</b> The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
<b>Play Full Welcome Prompt</b>	If enabled, queue agents will not be rung until after the welcome prompt is done playing. Otherwise, queue agents will be rung while the welcome prompt is being played to the caller.
<b>Satisfaction Survey Prompt</b>	
<b>Custom Prompt</b>	After a queue agent hangs up a call, a prompt will play asking the caller to rate their satisfaction on a scale of 1 to 5, with 5 being the highest. <b>Notes:</b> The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw <ul style="list-style-type: none"> <li>• The user can upload a custom prompt directly from this parameter.</li> <li>• Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw</li> <li>• Super administrator, administrators and queue chairmen can access agent satisfaction statistics by going to <b>Call Queue Statistics → Overview → Agent Satisfaction Statistics/Queue Satisfaction Statistics</b>.</li> <li>• The service satisfaction information can also be downloaded from <b>Call Queue Statistics</b>.</li> </ul>
<b>Max Wait Time</b>	
<b>Max Wait Time</b>	Configures the amount of time (in seconds) a caller will be kept in queue before the the call is automatically routed to the configured Max Wait Time Destination. If set to 0, callers will be kept in queue indefinitely. Default is 60 seconds.
<b>Destination</b>	The call will be routed to this destination if no one in this queue answers after the max wait time expires.
<b>Reset Agent Call Counter</b>	
<b>Enable</b>	Specifies the frequency at which the agent call counter will be reset. This will affect counter data used for agent ring strategies and the queue switchboard data.
<b>Repeat</b>	Set the repeat frequency to One-time, Daily, Weekly or Monthly.
<b>Date/Time</b>	Set the date and time.
<b>Destination Prompt Cycle</b>	
<b>Enable</b>	If enabled, the callers will hear the configured custom prompt at set intervals while waiting. If they press "1," they are immediately routed to a predefined failover destination.
<b>Destination Prompt Cycle</b>	Configure the voice prompt cycle (in seconds) of this call queue. When playing the voice prompt, you can press 1 to transfer to failover destination.
<b>Custom Prompt</b>	When playing a custom prompt, press 1 to enter the failover destination. Otherwise, continue waiting in queue. <b>Note:</b> The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
<b>Destination</b>	After the specified amount of time, the caller will be prompted to press 1 to immediately get redirected to the configured failover destination.
<b>Advanced Settings</b>	

<b>Virtual Queue</b>	
<b>Enable Virtual Queue</b>	If enabled, the system will activate a virtual queue for users, allowing them to opt for a callback instead of waiting. Callers will be prompted to either remain in the queue or choose a number that the PBX will use to reach them, ensuring they retain their position in line.
<b>Virtual Queue Mode</b>	<ul style="list-style-type: none"> <li>• <b>DTMF mode:</b> pressing 2 will manually trigger virtual queue and callers will hear a prompt to manually set a callback number.</li> <li>• <b>Timeout mode:</b> virtual queue will automatically be triggered when the configured Virtual Queue Period has passed and the users can choose a callback number.</li> <li>• <b>Auto mode:</b> virtual queue will automatically be triggered when the configured Virtual Queue Period has passed but the callback number will automatically be set to the caller's detected CID number.</li> </ul>
<b>Virtual Queue Period (s)</b>	The amount of time in seconds that must pass before virtual queue is offered to callers when using <b>Timeout mode</b> or <b>Auto mode</b> .
<b>Virtual Queue Outbound Prefix</b>	System will add this prefix to dialed numbers when calling back users.
<b>Enable Virtual Queue Position Announcement</b>	If enabled, the system will inform callers waiting in the queue of their positions in line.
<b>Enable Virtual Queue Wait Time Announcement</b>	If enabled, the estimated wait time for the call to get answered will periodically be announced to the caller.
<b>Enable Virtual Queue Callback Timeout</b>	If enabled, agents will have a set amount of time to answer a virtual queue callback.
<b>Write Timeout</b>	The amount of time in seconds that agents will have to answer a virtual queue callback. If the value is less than the Agent Ring Time, then the Agent Ring Time will take effect.
<b>Virtual Queue Welcome Prompt</b>	Upload the file of your welcome prompt of the virtual queue. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
<b>Queue Announcement</b>	
<b>Enable Position Announcement</b>	If enabled, the system will inform callers waiting in the queue of their positions in line.
<b>Enable Wait Time Announcement</b>	If enabled, the estimated wait time for the call to get answered will periodically be announced to the caller. <b>Note:</b> Wait time will not be announced if less than one minute.
<b>Announcement Interval</b>	The interval at which caller positions and estimated wait times will be announced. Valid range is between 20 and 600 seconds. Default value is 20.
<b>Agent ID Announcement</b>	If enabled, a system prompt containing the agent ID will be played to the caller when answered by an agent.
<b>Custom Announcement</b>	
<b>Custom Prompt</b>	The system will periodically play this announcement to callers that enter the queue. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
<b>Announcement Interval (s)</b>	Configures the interval for playing the queue's custom announcement. Valid range is between 20 and 600 seconds. Default value is 60.

<b>Empty Queue</b>	
<b>Leave When Empty</b>	<p>Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict".</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> Callers will be disconnected from the queue if all agents are paused or invalid.</li> <li>• <b>No:</b> Never disconnect the callers from the queue when the queue is empty.</li> <li>• <b>Strict:</b> Callers will be disconnected from the queue if all agents are paused, invalid or unavailable.</li> </ul>
<b>Dial in Empty Queue</b>	<p>Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No".</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> Callers can always dial into a call queue.</li> <li>• <b>No:</b> Callers cannot dial into a queue if all agents are paused or invalid.</li> <li>• <b>Strict:</b> Callers cannot dial into a queue if the agents are paused, invalid or unavailable.</li> </ul>
<b>Failover Destination</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Play Sound.</li> <li>• Extension.</li> <li>• Voicemail.</li> <li>• Queues.</li> <li>• Ring Group.</li> <li>• Voicemail Group.</li> <li>• IVR</li> <li>• External Number.</li> </ul>
<b>CTI</b>	
<b>Enable Agent Login</b>	Enabling agent login will cause the dynamic agents to be unavailable.
<b>Queue Chairman</b>	The queue chairman can log into his web portal to operate the queue.
<b>Service Level Agreement (SLA)</b>	
<b>Enable SLA</b>	<p>Toggles Service Level Agreement (SLA), which is percentage measurement of the queue group's ability to answer incoming calls within a defined amount of time. If a queue group's calculated SLA percentage is below the configured threshold value, alerts will be generated and sent out via email to the specified recipients.</p> <p><b>Example:</b> The SLA goal is 80% of calls (Threshold) within 20 seconds (SLA Time). If less than 80% of queue calls are answered within 20 seconds, the specified users will be notified of it.</p>
<b>SLA Time (s)</b>	Configures the amount of time in seconds that agents must answer incoming queue calls within to satisfy service quality requirements. Answering calls past this time will negatively affect the SLA measurement, and an alert will be generated once it hits below the specified SLA alert threshold. Supported values are 1 to 180. Default value is 20.
<b>SLA Alert Email Notification</b>	Enable SLA alert email notification.
<b>Alert Threshold (%)</b>	Configures the SLA alert threshold. If the percentage of queue calls answered within the configured SLA Time go below this value, an alert email will be generated and sent to the configured recipients. Supported values are 1 to 100. Default value is 80.
<b>SLA Alert Interval (m)</b>	Configures the minimum amount of time (in minutes) between alert sending. If a new alert is generated within this period, it will not be sent to recipients until the next alert interval. The valid range is from 1 to 120. The default value is 120.
<b>SLA Alert Email Template</b>	The template of the SLA alert email notifications.

<b>Alert Email Recipients</b>	Send SLA alert notifications to the configured alert email recipients. If a recipient does not have an email address configured, they will not receive the alert notifications.
<b>Other Settings</b>	
<b>Report Hold Time</b>	If enabled, the PBX 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".
<b>Replace Display Name</b>	If enabled, the PBX will replace the caller display name with the Call Queue name so that the caller knows the call is incoming from a Call Queue.
<b>Enable Feature Codes</b>	Enable feature codes option for call queue. For example, *83 is used for "Agent Pause"
<b>Autofill</b>	Enable/Disable the Autofill feature which distributes calls automatically to available agents as soon as they become free instead of having callers wait in a traditional queue.
<b>Dynamic Login Password</b>	If enabled, the configured PIN number is required for dynamic agent to log in. The default setting is disabled.
<b>Alert-Info</b>	When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS.
<b>Call Memory</b>	If enabled, the system will remember the last agent a caller has talked to. If the caller enters the queue again within the configured Retrieval Time (Days), the remembered agent will be prioritized for answering the call.
<b>Memory Retention Time (Days)</b>	Sets the amount of time that callers will be remembered for Call Memory agent matching. Calls to the queue after this period of time will no longer prioritize the caller's last agent. Valid range is 1 to 30 days. Default value is 7.
<b>Agents</b>	
<b>Static Agents</b>	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 ◀ or ▶ to choose. And use UP and Down arrow to select the order of the agent within the call queue.

## Static and Dynamic Agents

There are two types of agents that can be part of a call queue: static agents, manually added when configuring the queue, and dynamic agents, which can login and log out from the call queue anytime by using preset codes.

Static can be configured on **Basic Call Features**→**Call Queue**→**Edit Queue**→**Agents**. While dynamic agents only need a Login and Logout suffix to be able to join a queue.

These codes can be found under **Basic Call Features**→**Call Queue**→**Global Queue Settings**→**Dynamic Agent Login Setting** as shown below:

## Call Queue > Global Queue Settings

**Note:** Wave Mobile users may experience delays in receiving calls due to app wakeup processes or wireless network latency. As this may

### Dynamic Agent Login Settings

Agent Login Code Suffix

Agent Logout Code Suffix

Example

If 6500 is the queue extension,

Agent Login Extension Suffix is **\***,

Agent Logout Extension Suffix is **\*\***,

dial **6500\*** to log in and **6500\*\*** to log out.

Note: Removing the suffix while there are active sessions will prevent the agents from logging out.

*Dynamic Agent Login Settings*

#### **Note:**

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

To guarantee a high level of audio quality with the call queue feature, UCMs will limit the number of 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 agents for each UCM model:

UCM Model	Maximum Number of Agents in Call Queue
UCM6300A	25
UCM6302A	50
UCM6304A	80
UCM6308A	160

## Call Queue Feature Codes

Users can leverage feature codes to perform different call queue related actions by accessing **Basic Call Features**→**Feature Codes**→**Feature Codes**, below is the description of each code along with their default values:

- **Agent Pause (\*83):** Allows agents to pause their activity in all queues for a specific reason. Once the code is dialed, the agent will be prompted to enter a pause reason represented by a digit from 0 to 9. Another way to do this is to dial the feature code and the reason code number together. (e.g. dialing \*831 to directly set the pause status as "Lunchtime" (1)).
- **Agent Unpause (\*84):** This code is used by the agent to resume activity in all queues.

#### **Note:**

Users can configure up to 10 pause reason when the Agent Pause Reason Settings are set to "Custom". However, there only 5 pause reasons on the default settings: (1) Lunch, (2) Hourly Break, (3) Backoffice, (4) Email, and (5) Wrap.

- **Dynamic Agent Logout (\*85):** Agents can dial this code to log out from all queues.

## Queue Recordings

Queue recordings are shown under **Basic Call Features**→**Call Queue**→**Queue Recordings**.

Name	Caller	Call Queue	Date	Size	Options
q6502-4000-20241023-171020-1729 699819.28-5009.wav	4000	6502	2024-10-23 17:10:19	9.57 MB	10:27
q6503-1002-20241023-170556-1729 699555.15-5009.wav	1002	6503	2024-10-23 17:05:55	248.54 KB	00:16
q6500-5007-20241023-170358-1729 699436.10-5009.wav	5007	6500	2024-10-23 17:03:56	604.63 KB	00:54

Queue Recordings Page

- Click on



to download the recording file in .wav format; and on



to delete the recording file.

- Users can also download recordings in batch either by selecting specific recordings using the checkbox and clicking on [Download](#) or by downloading all files through [Download All](#) the button.

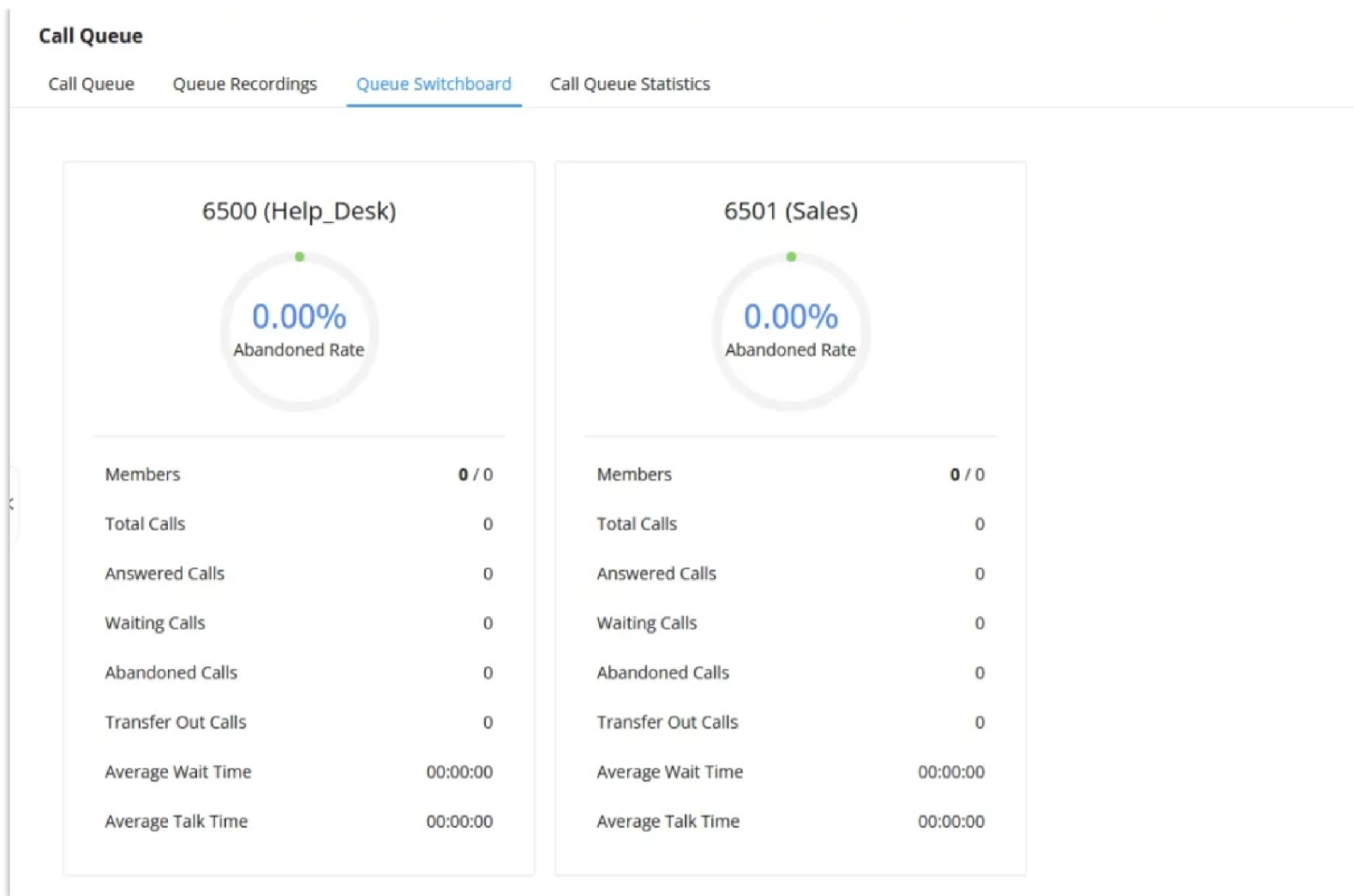
### Note:

If file data/file encryption is enabled for recording files, the Decryption Tool will be required to access the downloaded file. Instructions for using the tool can be found in this [guide](#).

## Queue Switchboard

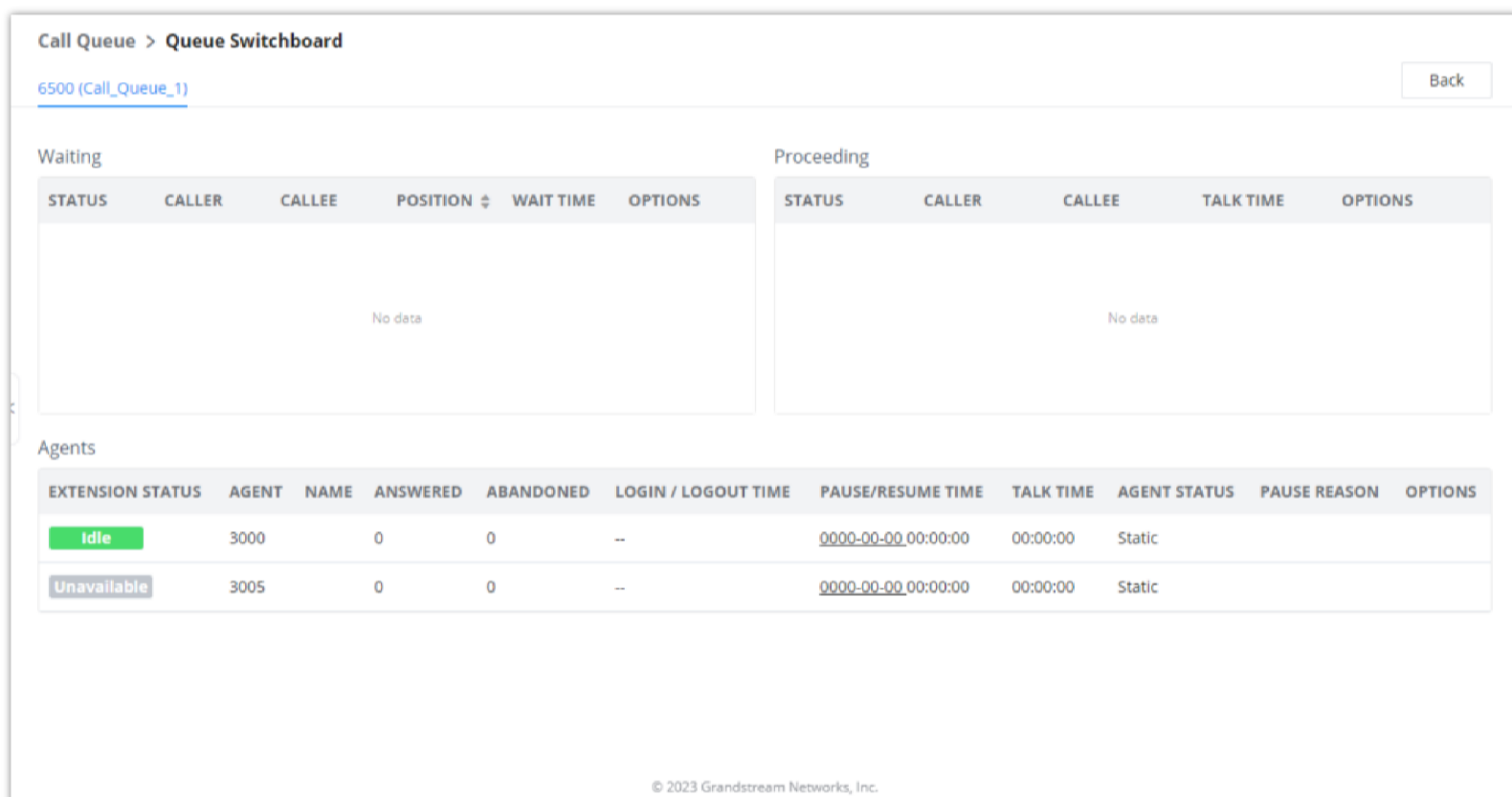
Switchboard is a Web GUI tool for call queue monitoring and management, admin can access to it from the menu **Basic Call Features**→**Call Queue** then press "Switchboard".

Following page will be displayed:



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:



Call Queue Switchboard

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

<b>Waiting</b>	Shows the current waiting calls along with the caller ID and the option to hang-up call.
<b>Proceeding</b>	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.

<b>Agents</b>	<p>Displays some basic call statistics and agent's mode (static or dynamic) along with the list of agents in the queue and the extension status:</p> <ul style="list-style-type: none"> <li>• Idle</li> <li>• Ringing</li> <li>• In Use</li> <li>• Paused</li> <li>• Unavailable</li> </ul>
---------------	---

### Queue Switchboard Privilege

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

<b>Super Admin</b>	<p>Default admin of the UCM. Call queue privileges include:</p> <ul style="list-style-type: none"> <li>• Viewing and edit all queue agents.</li> <li>• Monitor and execute actions for incoming/outgoing calls for all queues.</li> <li>• Generate Call Queue reports to track performance.</li> </ul>
<b>Queue Chairman</b>	<p>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 their extension number and assigned user password. Call Queue privileges include:</p> <ul style="list-style-type: none"> <li>• Viewing status and information related to all agents in the assigned queue.</li> <li>• Perform actions on calls such as hang-up, transfer or barge-in.</li> <li>• Manual Login/Logout of static and dynamic agents.</li> </ul>
<b>Queue Agent</b>	<p>User appointed by Super Admin to be a member of a queue extension. A queue agent can log into the UCM user portal with their extension number and assigned user password to manage their calls only.</p>

### Call 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 → **Basic Call Features**→**Call Queue** and click on "**Call Queue Statistics**", the following page will be displayed:

**Call Queue Statistics**

Call Queue Queue Recordings Queue Switchboard Call Queue Statistics

Download Reset Statistics Automatic Download 2024-10-01 to 2024-10-23 Filter

Overview Agent Details Login Record Pause Log

**Statistics Report**

- 27 Total Calls
- 70.37 % Abandoned Rate
- 00:00:18 Average Wait Time
- 00:00:51 Average Talk Time
- 1 Callback Calls

Agent Statistics Queue Statistics Agent Satisfaction Statistics Queue Satisfaction Statistics Agent Search

Agent	Name	Total Calls	Answered Calls	Answered Rate	Average Talk Time
1000	John	25	5	20.00 %	00:00:42
1001	Alice	9	0	0.00 %	00:00:00
1002	Bob	8	3	37.50 %	00:01:06
1003	Megan	0	0	0.00 %	00:00:00
1004	Mark	0	0	0.00 %	00:00:00
1005	James	0	0	0.00 %	00:00:00

Call Queue Statistics

Users can download statistics in CSV format by clicking the [Download](#) button. They can also set up automatic email deliveries of these statistics at regular intervals by clicking on [Automatic Download](#)

Additionally, users can clear the statistics using the [Reset Statistics](#) button.

**Call Queue > Automatic Download**

Automatically send call queue statistics to the configured email address at the specified frequency and time.

Automatic Download

Report Type  All  Overview  Agent Details  Login Record  Pause Log

Automatic Download Period

Email  [Email Template](#)

*Call Queue Statistics Automatic Download*

This section provides a detailed description of each tab on the **Basic Call Features→Call Queue→Call Queue Statistics** page.

## Overview Tab

The overview page shows the following information:

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

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

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

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

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

Queue Statistics Details

## Agent Details Tab

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

Time	Agent	Name	Queue	Caller ID Number	Abandoned	Wait Time	Talk Time	Service Satisfaction
2024-10-21 13:37:52	1000	John	6500	5004	Yes	00:00:10	00:00:00	Not Surveyed
2024-10-21 14:12:08	1000	John	6500	5004	Yes	00:00:10	00:00:00	Not Surveyed
2024-10-21 14:13:19	1000	John	6500	5004	Yes	00:00:20	00:00:00	Not Surveyed
2024-10-21 14:13:56	1000	John	6500	5004	Yes	00:00:15	00:00:00	Not Surveyed
2024-10-22 10:06:28	1000	John	6500	4002	No	00:00:10	00:00:59	Not Evaluated
2024-10-21 12:13:44	1001	Alice	6500	5004	Yes	00:00:11	00:00:00	Not Surveyed
2024-10-21 13:32:36	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:33:33	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:34:05	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:34:26	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed

Agent details

## Login Record Tab

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

- **Agent:** the extension that logged in and out.
- **Queue:** the queue that the extension logged in and out of.

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

Agent	Name	Queue	Login Time	Logout Time	Login Duration
1001	Alice	6500	2024-10-22 09:48:45	2024-10-22 09:50:46	00:02:01
1002	Bob	6500	2024-10-21 11:25:13	2024-10-21 13:47:01	02:21:48
1002	Bob	6500	2024-10-22 09:42:01	2024-10-22 09:53:43	00:11:42

*Login Record*

## Pause Log Tab

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

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

Agent	Name	Queue	Pause Time	Resume Time	Pause Duration	Pause Reason
1001	Alice	6500	2024-10-21 11:36:01	2024-10-21 12:12:31	00:36:30	Hourly Break
5009		6502	2024-10-24 10:18:42	2024-10-24 11:23:22	01:04:40	Lunch
5009		6503	2024-10-24 10:18:42	2024-10-24 11:23:22	01:04:40	Lunch
5009		6500	2024-10-24 10:18:42	2024-10-24 11:23:22	01:04:40	Lunch

*Pause Log*

## 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.

**Note:** Wave Mobile users may experience delays in receiving calls due to app wakeup processes or wireless network latency. As this may affect the queue call answering performance, it is not recommended to assign Wave Mobile users as agents.

**Dynamic Agent Login Settings**

Agent Login Code Suffix

Agent Logout Code Suffix

**Example** If 6500 is the queue extension,  
 Agent Login Extension Suffix is \*,  
 Agent Logout Extension Suffix is \*\*,  
 dial **6500\*** to log in and **6500\*\*** to log out.  
 Note: Removing the suffix while there are active sessions will prevent the agents from logging out.

**Agent Pause Reason**

Dial the "Agent Pause" [Feature Code](#) and the corresponding key to be paused in all queues for the selected reason, which will be logged.

Agent Pause Reason Settings

Global Queue Settings

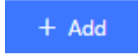


Dynamic Agent Login Settings	
<b>Agent Login Code Suffix</b>	Configure the code to dial after the queue extension to log into the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log in.
<b>Agent Logout Code Suffix</b>	Configure the code to dial after the queue extension to log out of the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log out.
Agent Pause Reason	
<b>Agent Pause Reason Settings</b>	Select the agent pause reason settings. <ul style="list-style-type: none"> <li>• Default: Use the default settings for the agent pause reason.</li> <li>• Custom: User the custom settings. These settings should be configured using they corresponding key for each status. The user can upload a custom prompt which will be played for the agent once they set the pause reason.</li> </ul>
<b>Key Settings</b>	Enter which key to press to set the different pause reasons.
Virtual Queue Callback Key Settings	
<b>Enable</b>	Select whether to enable or disable virtual queue callback feature. By default it's disabled.
<b>Call Back Current Number</b>	Press the feature key configured to set your current number as callback number.
<b>Custom Callback Number</b>	Press these feature key configured to set a custom callback number.
<b>Continue Waiting</b>	Press the feature key configured to continue waiting.

# PICKUP GROUPS

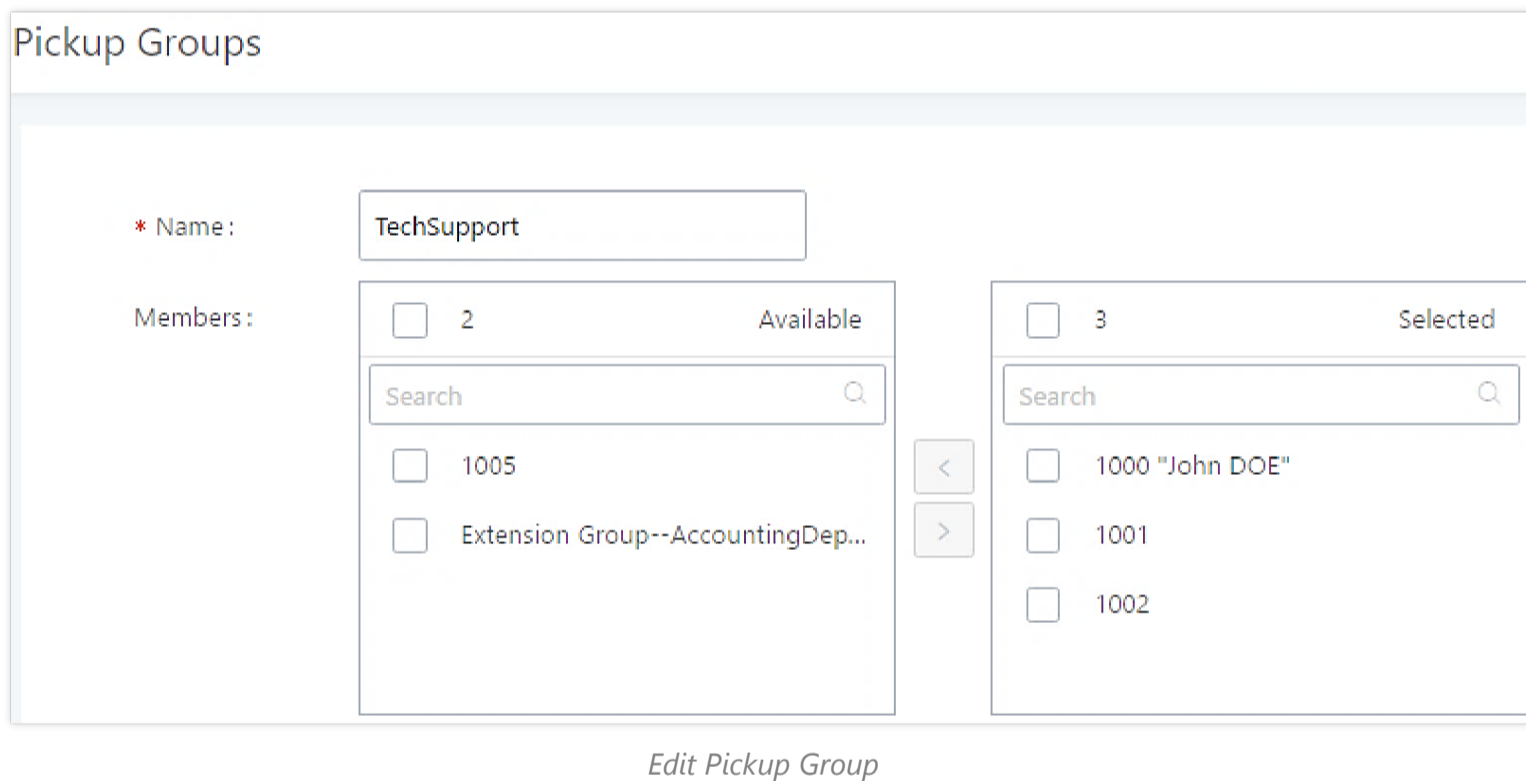
The UCM630xA supports pickup group feature which allows users to pick up incoming calls for other extensions if they are in the same pickup group, by dialing "Pickup Extension" feature code (by default \*8).

## Configure Pickup Groups

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

- Click on  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.



## Configure Pickup Feature Code

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

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

Feature Codes

Feature Maps    DND/Call Forward    **Feature Codes**

Reset All    Default All

* Voicemail Access Code:	<input type="text" value="*98"/>	<input checked="" type="checkbox"/>	* My Voicemail:	<input type="text" value="*97"/>	<input checked="" type="checkbox"/>
* Agent Pause:	<input type="text" value="*83"/>	<input checked="" type="checkbox"/>	* Agent Unpause:	<input type="text" value="*84"/>	<input checked="" type="checkbox"/>
* Paging Prefix:	<input type="text" value="*81"/>	<input checked="" type="checkbox"/>	* Intercom Prefix:	<input type="text" value="*80"/>	<input checked="" type="checkbox"/>
* Blacklist Add:	<input type="text" value="*40"/>	<input checked="" type="checkbox"/>	* Blacklist Remove:	<input type="text" value="*41"/>	<input checked="" type="checkbox"/>
* Pickup on Ringing Prefix:	<input type="text" value="**"/>	<input checked="" type="checkbox"/>	* Pickup In-call Prefix:	<input type="text" value="*45"/>	<input type="checkbox"/>
* Pickup Extension:	<input type="text" value="*8"/>	<input checked="" type="checkbox"/>	* Direct Dial Voicemail Prefix:	<input type="text" value="*"/>	<input checked="" type="checkbox"/>
* Direct Dial Mobile Phone Prefix:	<input type="text" value="*88"/>	<input checked="" type="checkbox"/>	* Call Completion Request:	<input type="text" value="*11"/>	<input checked="" type="checkbox"/>
* Call Completion Cancel:	<input type="text" value="*12"/>	<input checked="" type="checkbox"/>	Enable Spy:	<input type="checkbox"/>	
* Listen Spy:	<input type="text" value="*54"/>		* Whisper Spy:	<input type="text" value="*55"/>	
* Barge Spy:	<input type="text" value="*56"/>		* Wakeup Service:	<input type="text" value="*36"/>	<input checked="" type="checkbox"/>
* PMS Wakeup Service:	<input type="text" value="*35"/>	<input checked="" type="checkbox"/>	* Update PMS Room Status:	<input type="text" value="*23"/>	<input checked="" type="checkbox"/>
* Presence Status:	<input type="text" value="*48"/>	<input checked="" type="checkbox"/>	* Dynamic Agent Logout:	<input type="text" value="*85"/>	<input checked="" type="checkbox"/>
* Voicemail Group Access Code:	<input type="text" value="*99"/>	<input checked="" type="checkbox"/>			

*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.

Manage Music On Hold

+ Add    Download All Music On Hold

Music on Hold Playlists:

Record    Delete    Upload

<input type="checkbox"/>	DISABLED/ENABLED	SOUND FILE	OPTIONS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	macroform-cold_day.wav	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	macroform-robot_dity.wav	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	macroform-the_simplicity.wav	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	manolo_camp-morning_coffee.wav	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	reno_project-system.wav	

Total: 5    10 / page    Goto 1

*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

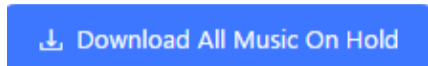
next to the selected Music On Hold class to delete this Music On Hold class.

- 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



to delete all selected Music On Hold files.

The UCM630xA allows Users to select the Music On Hold file from Web GUI to play it. The UCM630xA will initiate a call to the selected extension and play this Music On Hold file once the call is answered.

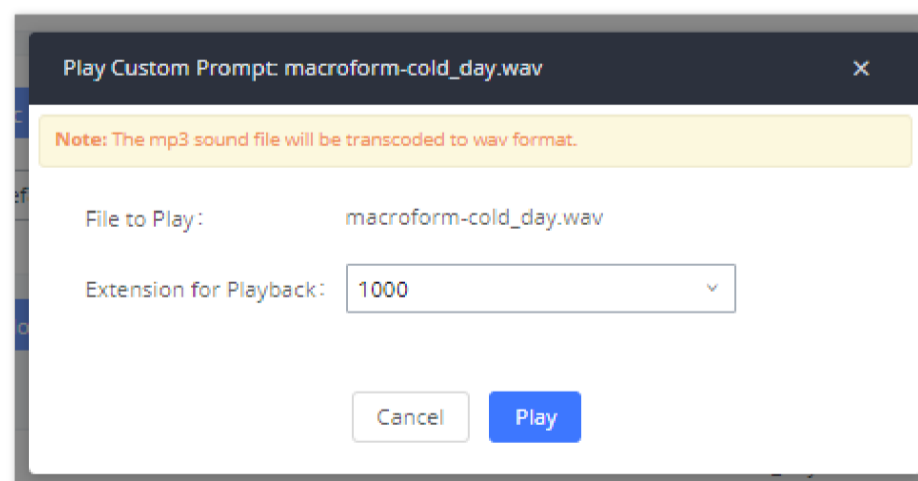
Steps to play the Music On Hold file:

1. Click on the



button for the Music On Hold file.

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



Play Custom Prompt

3. The selected extension will ring.

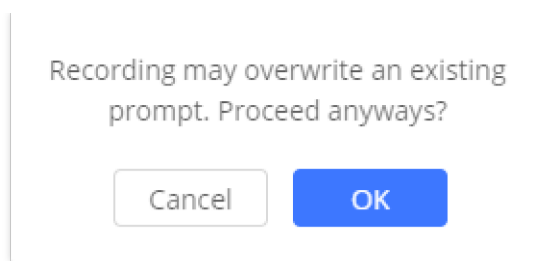
4. Answer the call to listen to the music playback.

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

1. Click on

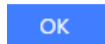


2. A message of confirmation will pop up, as shown below.

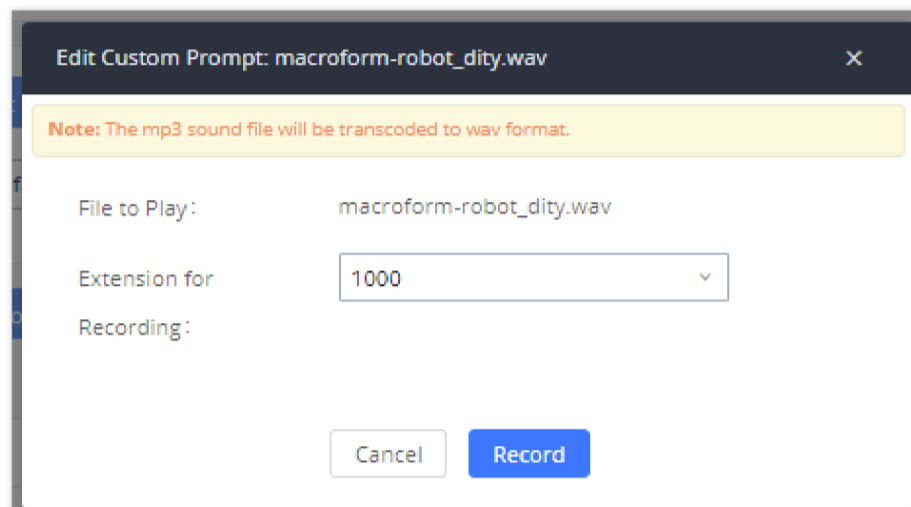


Information Prompt

3. Click



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



Record Custom Prompt

5. Answer the call and start to record your new music on hold.

6. Hang up the call and refresh Music On Hold page then you can listen to the new recorded file.

### **i** Note

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 UCM630xA 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:

<https://documentation.grandstream.com/knowledge-base/busy-camp-on-2/>

## **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.

*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:

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

*SIP Presence Status*

Another option to set the presence status and which is more practical is using the feature code from the user's phone, once 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→**Basic Call Features→Feature Codes**.

*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 = PRESENCE\_STATUS**.

STATUS	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
▶	*1000* 1000	*48	PRESENCE_STATUS	2019-12-11 17:55:33	0:00:13	0:00:13		-
▶	*admin* VFAX [T...	998653221	DIAL	2019-12-11 17:51:09	0:00:22	0:00:22		-
▶	*1000* 1000	6500	QUEUE[6500]	2019-12-11 17:32:45	0:00:04	0:00:00		-

Presence Status CDR

## FOLLOW ME

Follow Me is a feature on the UCM630xA 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.

**Edit Extension: 1000**

Basic Settings   Media   Features   Specific Time   **Follow Me**

Enable:

Skip Trunk Auth:

Music On Hold Class:

Confirm When Answering:

Use Callee DOD for Follow Me:

Enable Destination:

Default Destination:

**Follow Me Numbers**

New Follow Me Number:  Dial Local Extension    Dial External Number

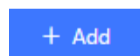
for  (seconds)

Dialing Order:  Ring after trying previous extension/number    Ring along with previous extension/number

EXTENSION	OPTIONS
1002 for 30 (seconds)	<input type="button" value="X"/> <input type="button" value="↺"/> <input type="button" value="↻"/> <input type="button" value="⬇"/> <input type="button" value="⬆"/>

Edit Follow Me

1. Click on



to add local extensions or external numbers to be called after ringing the extension selected in the first step.





2. 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:

<b>Enable</b>	Configure to enable or disable Follow Me for this user.
<b>Skip Trunk Auth</b>	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.
<b>Music On Hold Class</b>	Configure the Music On Hold class that the caller would hear while tracking users

<b>Confirm When Answering</b>	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.
<b>Enable Destination</b>	When enabled, the call will be routed to the default destination if no one in the Follow Me extensions answers the call.
<b>Default Destination</b>	Configure the destination if no one in the Follow Me extensions answers the call. The available options are: <ul style="list-style-type: none"> <li>○ Extension</li> <li>○ Voicemail</li> <li>○ Queues</li> <li>○ Ring Group</li> <li>○ Voicemail Group</li> <li>○ IVR</li> <li>○ External Number</li> </ul>
<b>Follow Me Numbers</b>	The added numbers are listed here. Click on   to arrange the order. Click on  to delete the number. Click on  to add new numbers.
<b>New Follow Me Number</b>	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.
<b>Dialing Order</b>	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.

*Follow Me Settings*

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

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

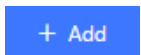
*Follow Me Options*

## SPEED DIAL

The UCM630xA 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 UCM630xA.

To enable Speed Dial, on the UCM630xA Web GUI, go to page Web GUI → **Basic Call Features** → **Speed Dial**.

User should first click on



. Then decide from one digit up to four digits combination used for Speed Dial and select a dial destination from "Default Destination". The

supported destinations include extension, voicemail, meeting room, voicemail group, IVR, ring group, call queue, page group, DISA, Dial by Name and external number.

### Create New Speed Dial

Enable

Destination:

\* Speed Dial

Extension:

Default

Destination:

*Speed Dial Destinations*

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

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

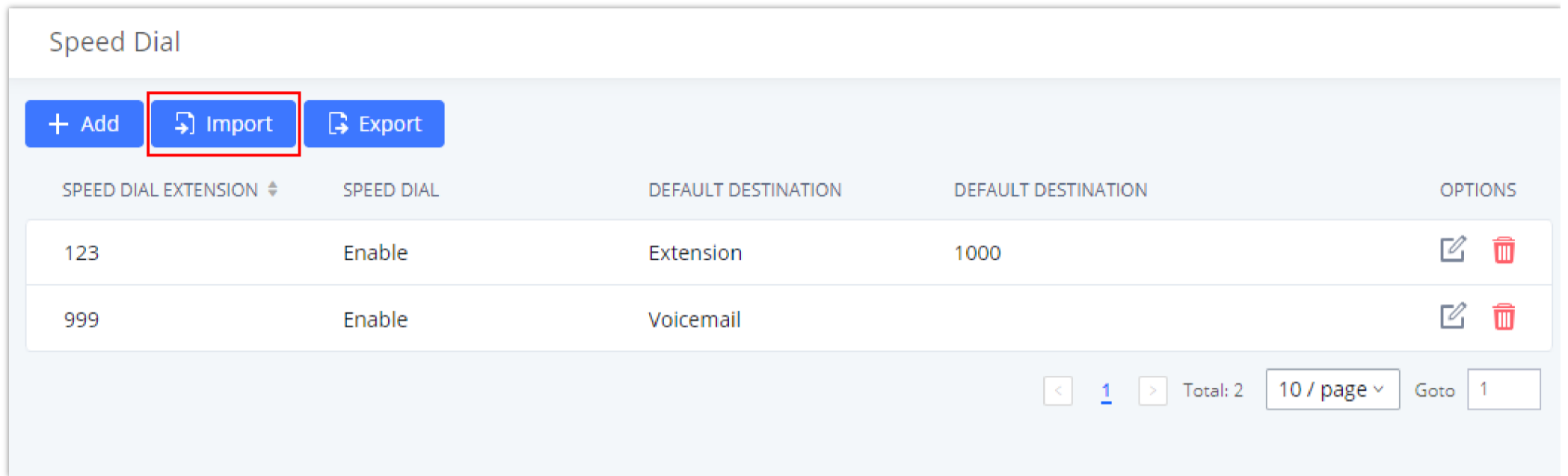
Speed Dial					
+ Add					
Extension ↕	Speed Dial	Default Destination	Default Destination	Options	
1	Enable	Extension	1000		
2	Enable	Extension	1001		
3	Enable	External Number	0016175669300		
4	Enable	Ring Group	6400		
5	Enable	Queues	6500		

Total: 5 < 1 > 10 / page ▾ Goto





*List of Speed Dial*

## Import Speed Dial

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

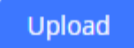


The screenshot shows the 'Speed Dial' management interface. At the top, there are three buttons: '+ Add', 'Import' (highlighted with a red box), and 'Export'. Below the buttons is a table with the following columns: 'SPEED DIAL EXTENSION', 'SPEED DIAL', 'DEFAULT DESTINATION', 'DEFAULT DESTINATION', and 'OPTIONS'. The table contains two rows of data:

SPEED DIAL EXTENSION	SPEED DIAL	DEFAULT DESTINATION	DEFAULT DESTINATION	OPTIONS
123	Enable	Extension	1000	 
999	Enable	Voicemail		 

At the bottom right of the interface, there is a pagination control showing '< 1 >' and 'Total: 2', a dropdown menu for '10 / page', and a 'Goto 1' field.

*Import Speed Dial List*

Then select the csv file of the speed dial entries and click 

### Important

Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.

### Alert

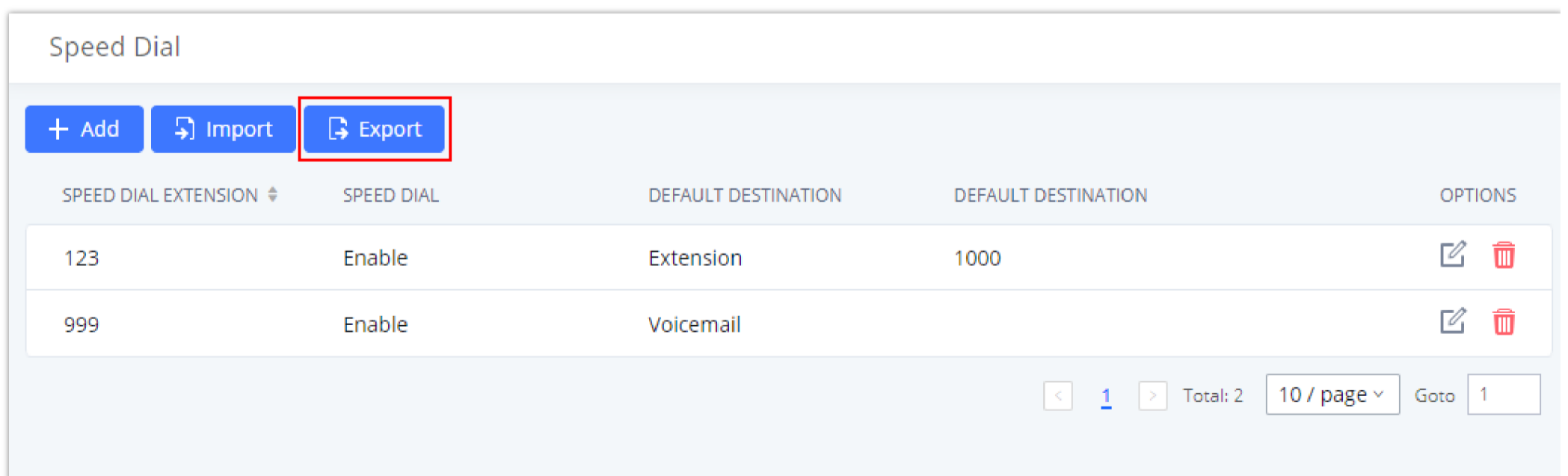
Importing speed dial entries will overwrite the existing speed dials, if you wish to import new speed dial entries to the already existing ones, you will have to export them then combine them together in one file before you import it.

### Note





The number of speed dial entries is limited to 1000.

## Export Speed Dial

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



The screenshot shows the 'Speed Dial' management interface. At the top, there are three buttons: '+ Add', 'Import', and 'Export' (highlighted with a red box). Below the buttons is a table with the following columns: 'SPEED DIAL EXTENSION', 'SPEED DIAL', 'DEFAULT DESTINATION', 'DEFAULT DESTINATION', and 'OPTIONS'. The table contains two rows of data:

SPEED DIAL EXTENSION	SPEED DIAL	DEFAULT DESTINATION	DEFAULT DESTINATION	OPTIONS
123	Enable	Extension	1000	 
999	Enable	Voicemail		 

At the bottom right of the interface, there is a pagination control showing '< 1 >' and 'Total: 2', a dropdown menu for '10 / page', and a 'Goto 1' field.

*Export Speed Dial List*

# 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 UCM630xA, the user can then dial out via the SIP trunk or PSTN trunk connected to UCM630xA as it is an internal extension.

The UCM630xA supports DISA to be used in IVR or inbound route. Before using it, create new DISA under Web GUI→**Advanced Call Features**→**DISA**.

- Click on

 + Add

to add a new DISA.

- Click on

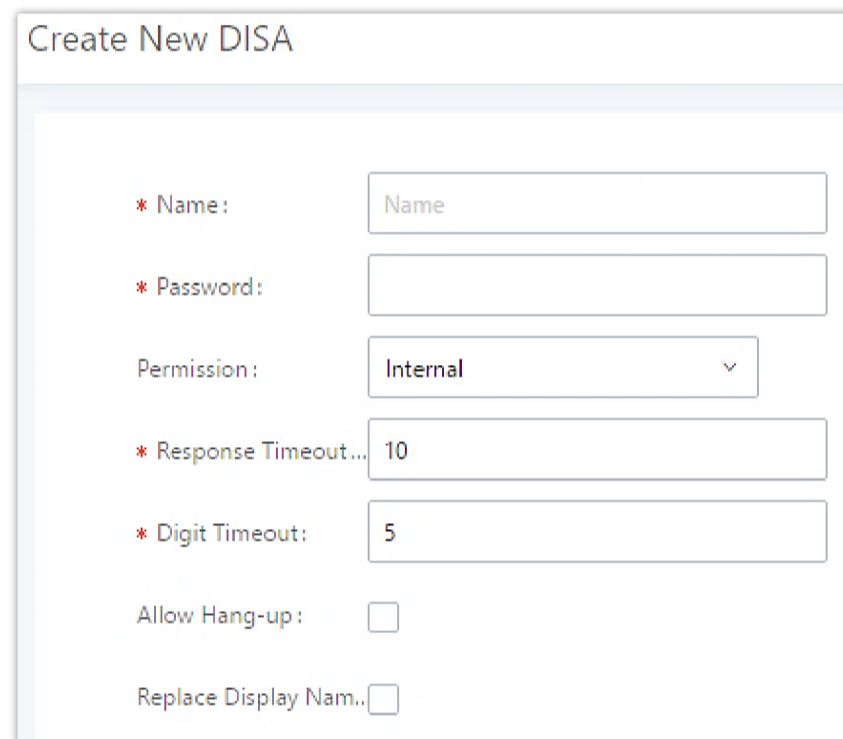


to edit the DISA configuration.

- Click on



to delete the DISA.



The screenshot shows a 'Create New DISA' form with the following fields and values:

- \* Name: [Name]
- \* Password: [ ]
- Permission: [Internal]
- \* Response Timeout...: [10]
- \* Digit Timeout: [5]
- Allow Hang-up:
- Replace Display Nam..:

*Create New DISA*

The following table details the parameters to set and configure DISA feature on UCM630xA PBX.

<b>Name</b>	Configure DISA name to identify the DISA.
<b>Password</b>	Configure the password (digit only) required for the user to enter before using DISA to dial out. <b>Note:</b> The password must be at least 4 digits.
<b>Permission</b>	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 UCM630xA 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.

<b>Response Timeout</b>	Configure the maximum amount of time the UCM630xA will wait before hanging up if the user dials an incomplete or invalid number.  The default setting is 10 seconds.
<b>Digit Timeout</b>	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
<b>Allow Hangup</b>	If enabled, during an active call, users can enter the UCM630xA 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".
<b>Replace Display Name</b>	If enabled, the UCM will replace the caller display name with the DISA name.

### *DISA Settings*

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>


<https://documentation.grandstream.com/knowledge-base/emergency-calls/>

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**"

## Emergency Calls

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

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

### Create New Emergency Call

\* Name:

\* Emergency Number:

Emergency Level:

Disable Hunt on Busy:

Custom Prompt:  [Prompt](#)

\* Use Trunks:

\* Members Notified:

11 items Available

Search

- 1001 "John Doe"
- 1002
- 1003
- 1004

1 item Selected

Search

- 1000 "James tuan"

Strip:

Prepend:

Auto Record:

Send Recording File:

Email Address:  [+](#)

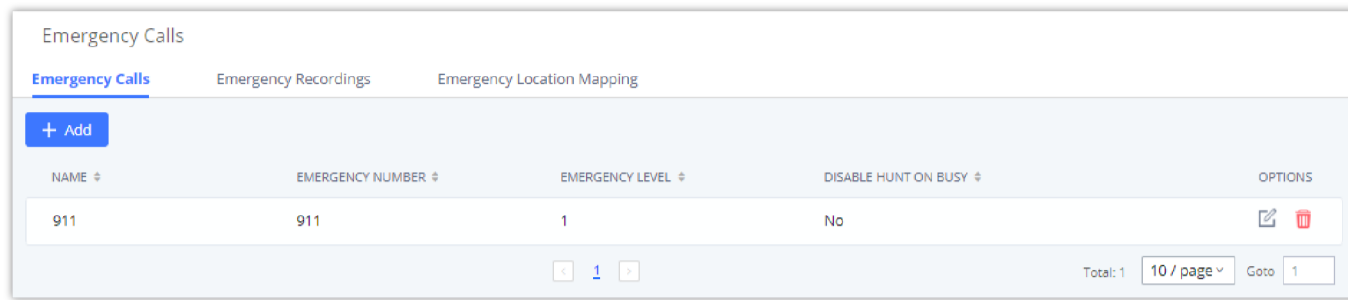
*Emergency Number Configuration*

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

<b>Name</b>	Configure the name of the emergency call.  For example, "emergency911", "emergency211" and etc.
<b>Emergency Number</b>	Config the emergency service number. For example, "911", "211" and etc.
<b>Emergency Level</b>	Select the emergency level of the number. Level "3" means the most urgent.
<b>Disable Hunt on Busy</b>	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.
<b>Custom Prompt</b>	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.
<b>Use Trunks</b>	Select the trunks for the emergency call. Select one trunk at least and select five trunks at most.
<b>Members Notified</b>	Select the members who will be notified when an emergency call occurs.
<b>Strip</b>	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.
<b>Prepend</b>	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.
<b>Auto Record</b>	When enabled, emergency call will be automatically recorded.

<b>Send Recording File</b>	When enabled recording files will be sent to the configured email address.
<b>Email Address</b>	The email address to where the recording files will be sent.

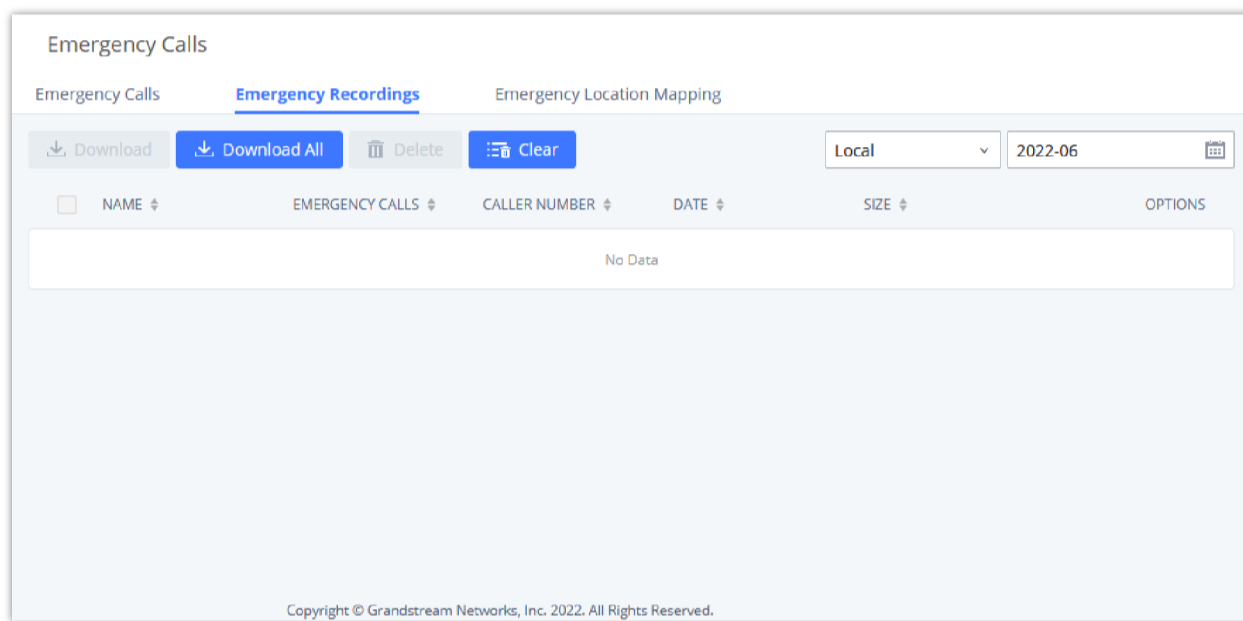
### Emergency Numbers Parameters



911 Emergency Sample

## Emergency Recordings

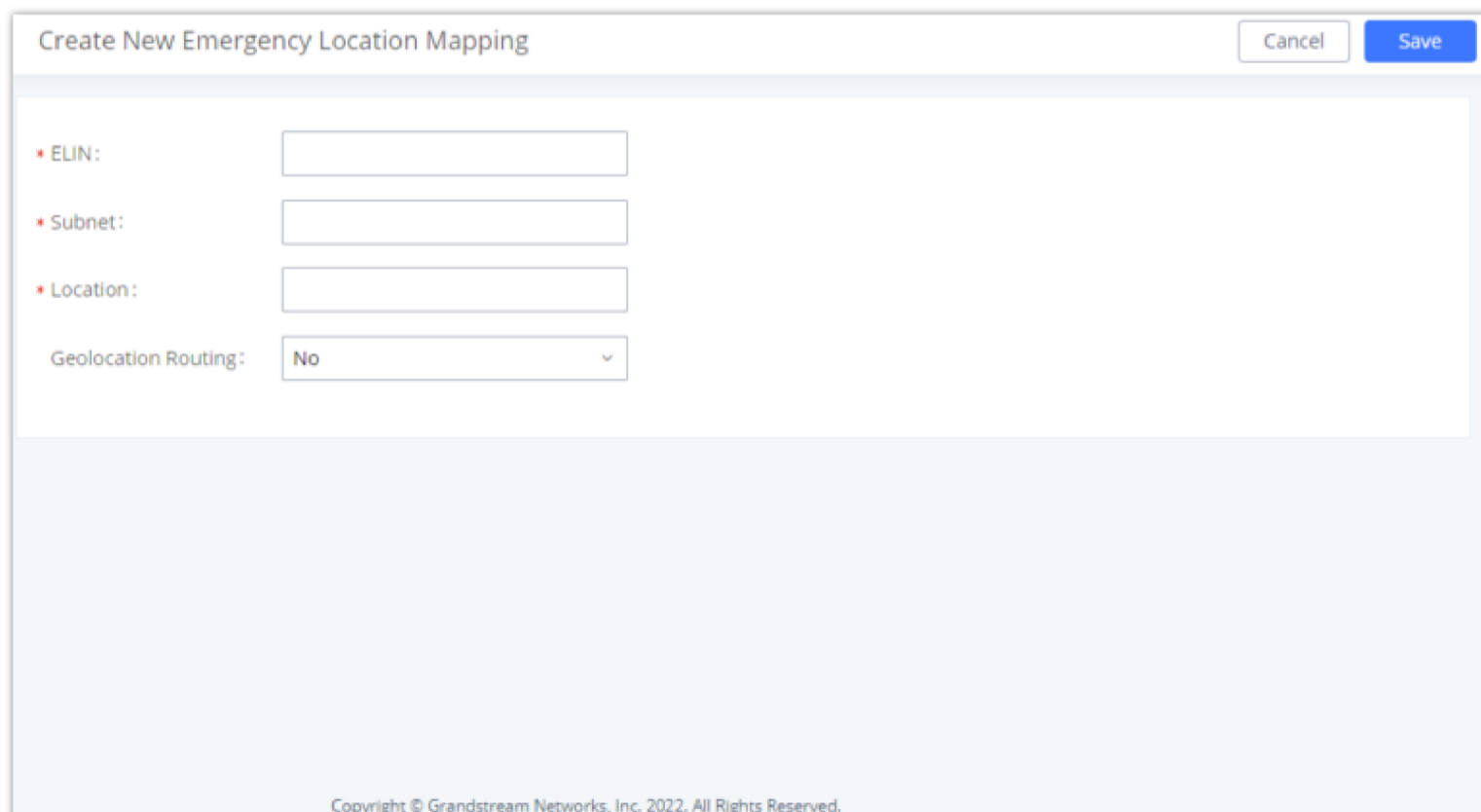
UCM6300 Series allows recording emergency calls and they can be found under WebUI → **Call Feature** → **Emergency Calls** → **Emergency Recordings**



Emergency Recordings

## Emergency Location Mapping

In compliance with Kari's Law and the Ray Baum's Act, UCM's Emergency Calls feature supports emergency location mapping. This will allow users to associate subnets with emergency location identification numbers (ELINs), which can then be used by E911 service providers for example to determine the location of callers. The new options can be found under **Advanced Call Features** → **Emergency Calls** → **Emergency Location Mapping**.



Emergency Location Mapping

- **ELIN:** The emergency location identification number registered with the E911 provider. This number will be sent out as the emergency call's CID number.
- **Subnet:** The network subnet that the ELIN will be associated with. The ELIN that is sent to E911 providers is based on the subnet that a calling endpoint is registered from. Example: "xxx.xxx.xxx.xxx/24" or "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/64".
- **Location:** Location associated with the configured subnet. This is used for the UCM administrator's reference.
- **Geolocation Routing:** Toggles whether to include the *Geolocation* header in the emergency call SIP INVITE message. The *Location* field value will be used as the *Geolocation* header value.

### **Important Note**

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

## 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 UCM630xA.
2. On the UCM630xA, 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 UCM630xA 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 UCM630xA 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 UCM630xA 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 UCM630xA, go to Web GUI → **Advanced Call Features** → **Callback** page and click on

[+ Create New Callback](#)

. Configuration parameters are listed in the following table.

### Callback Configuration Parameters

<b>Name</b>	Configure a name to identify the Callback. (Enter at least two characters)
<b>CallerID Pattern</b>	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.  <b>Note:</b> If leaving as blank, all numbers are allowed to use this callback.
<b>Outbound Prepend</b>	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.
<b>Delay Before Callback</b>	Configure the number of seconds to be delayed before calling back the user.

<b>Destination</b>	<p>Configure the destination which the callback will direct the caller to. Two destinations are available:</p> <ul style="list-style-type: none"> <li>○ IVR</li> <li>○ DISA</li> </ul> <p>The caller can then enter the desired number to dial out via UCM630xA trunk.</p>
--------------------	--

## BLF AND EVENT LIST

### BLF



The UCM630xA supports BLF monitoring for extensions, ring group, call queue, meeting 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 UCM630xA and remote extensions on the VOIP trunk can be monitored. The event list setting is under Web GUI → **Basic Call Features** → **Event List**.

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

<b>URI</b>	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 UCM630xA. The valid characters are letters, digits, _ and -.
<b>Local Extensions</b>	Select the available extensions/Extension Groups listed on the local UCM630xA to be monitored in the event list.
<b>Remote Extensions</b>	If LDAP sync is enabled between the UCM630xA and the peer UCM630xA, the remote extensions will be listed under "Available Extensions". If not, manually enter the remote extensions under "Special Extensions" field.
<b>Special Extensions</b>	Manually enter the remote extensions in the peer/register trunk to be monitored in the event list. Valid format: 5000,5001,9000

Create New Event List

\* URI:

Event Type:

Local Extensions:

<input type="checkbox"/> 9 items Available	<input type="checkbox"/> 3 items Selected
Search here <input type="text"/>	Search here <input type="text"/>
<input type="checkbox"/> 1003 "Betty"	<input type="checkbox"/> 1000 "Mia"
<input type="checkbox"/> 1004	<input type="checkbox"/> 1001 "John"
<input type="checkbox"/> 1005 "Will"	<input checked="" type="checkbox"/> 1002 "Chris"
<input type="checkbox"/> 1006 "lala"	
<input type="checkbox"/> 1007 "Kiki"	

Remote Extensions:

<input type="checkbox"/> 0 item Available	<input type="checkbox"/> 0 item Selected
Search here <input type="text"/>	Search here <input type="text"/>
None	None

Special Extensions:

Create New Event List

Remote extension monitoring works on the UCM630xA via event list BLF, among Peer SIP trunks or Register SIP trunks (register to each other). Therefore, please properly configure SIP trunks on the UCM630xA 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 UCM630xA and remote extensions are added to the list, the UCM630xA will send out SIP SUBSCRIBE to the remote UCM630xA to obtain the remote extension status. When the SIP end points register and subscribe to the local UCM630xA 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.

### **i** Notes

- To configure LDAP sync, please go to UCM630xA Web GUI→**Extension/Trunk→VoIP Trunk**. You will see "Sync LDAP Enable" option. Once enabled, please configure password information for the remote peer UCM630xA to connect to the local UCM630xA. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM630xA and remote UCM630xA need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM630xAs.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM630xA PBX. However, it might not work the other way around depending on whether the non-UCM630xA PBX supports event list BLF or remote monitoring feature.

- To configure LDAP sync, please go to UCM630xA Web GUI→**Extension/Trunk→VoIP Trunk**. You will see "Sync LDAP Enable" option. Once enabled, please configure password information for the remote peer UCM630xA to connect to the local UCM630xA. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM630xA and remote UCM630xA need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM630xAs.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM630xA PBX. However, it might not work the other way around depending on whether the non-UCM630xA 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→**Advanced Call Features**→**Dial By Name**.

**Create New Dial By Name**

\* Name:

\* Extension:

Custom Prompt:  [Upload Audio File](#)

Members:  30 items Available  0 item Selected

LDAP Phonebook:  1 item Available  0 item Selected

Options

\* Prompt Wait Time:

Query Type:  By Last Name + First Name  By First Name + Last Name

Select Type:  By Order  By Menu

*Create Dial by Name Group*

**User Settings**

First Name:  Last Name:

Email Address:

\* Language:

Mobile Phone Number:

\* User Password:

\* Concurrent Registration...:

*Configure Extension First Name and Last Name*

### 1. Name

Enter a Name to identify the Dial by Name group.

### 2. Extension

Configure the direct dial extension for the Dial By Name group.

### 3. Custom Prompt

This option sets a custom prompt for directory to announce to a caller. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add additional record.

#### 4. Available Extensions/Selected Extensions

Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have a valid first name and last name configured under Web GUI → **Extension/Trunk** → **Extensions** in order to be searchable in Dial By Name directory through IVR. By specifying the extensions here, the administrators can make sure unscreened calls will not reach the company employee if he/she does not want to receive them directly.

#### 5. Prompt Wait Time

Configure "Prompt Wait Time" for Dial By Name feature. During Dial By Name call, the caller will need to input the first letters of First/Last name before this wait time is reached. Otherwise, timeout will occur, and the call might hang up. The timeout range is between 3 and 60 seconds.

#### 6. Query Type

Specify the query type. This defines how the caller will need to enter to search the directory.

By First Name: enter the first 3 digits of the first name to search the directory.

By Last Name: enter the first 3 digits of the last name to search the directory.

#### 7. Select Type

Specify the select type on the searching result. The IVR will confirm the name/number for the party the caller would like to reach before dialing out.

By Order: After the caller enters the digits, the IVR will announce the first matching party's name and number. The caller can confirm and dial out if it is the destination party, or press \* to listen to the next matching result if it is not the desired party to call.

By Menu: After the caller enters the digits, the IVR will announce 8 matching results. The caller can press number 1 to 8 to select and call or press 9 for results in next page.

The Dial by Name group can be used as the destination for inbound route and key pressing event for IVR. The group name defined here will show up in the destination list when configuring IVR and inbound route. If Dial by Name is set as a key pressing event for IVR, user could use '\*' to exit from Dial by Name, then re-enter IVR and start a new event. The following example shows how to use this option.

The screenshot shows the 'Edit IVR: Test' configuration page with the 'Key Pressing Events' tab selected. It features three rows of configuration for key presses:

- Press 0: A dropdown menu set to 'Dial By Name' and a text input field containing 'DialByNameG...'.
- Press 1: A dropdown menu set to 'Select an Opti...'.
- Press 2: A dropdown menu set to 'Select an Opti...'.

Dial By Name Group In IVR Key Pressing Events

The screenshot shows the 'Edit Inbound Rule' configuration page with a 'Save' button in the top right corner. It contains several configuration fields:

- \* Pattern: A text input field containing '.'.
- CallerID Pattern: A text input field containing 'Separate patterns by commas, such as " \_ : '.
- Disable This Route: An unchecked checkbox.
- Prepend Trunk Name: An unchecked checkbox.
- Prepend User Defined Nam...: An unchecked checkbox and an empty text input field.
- Inbound Multiple Mode: An unchecked checkbox.
- Alert-info: A dropdown menu set to 'None'.
- Dial Trunk: An unchecked checkbox.
- Privilege Level: A dropdown menu set to 'Internal'.
- DID Destination: An empty text input field.
- Allowed to seamless transfe...: An empty text input field.
- Default Mode: A section header.
- \* Default Destination: A dropdown menu set to 'Dial By Name' and a text input field containing 'DialByNameGP1'.

Dial By Name Group In Inbound Rule

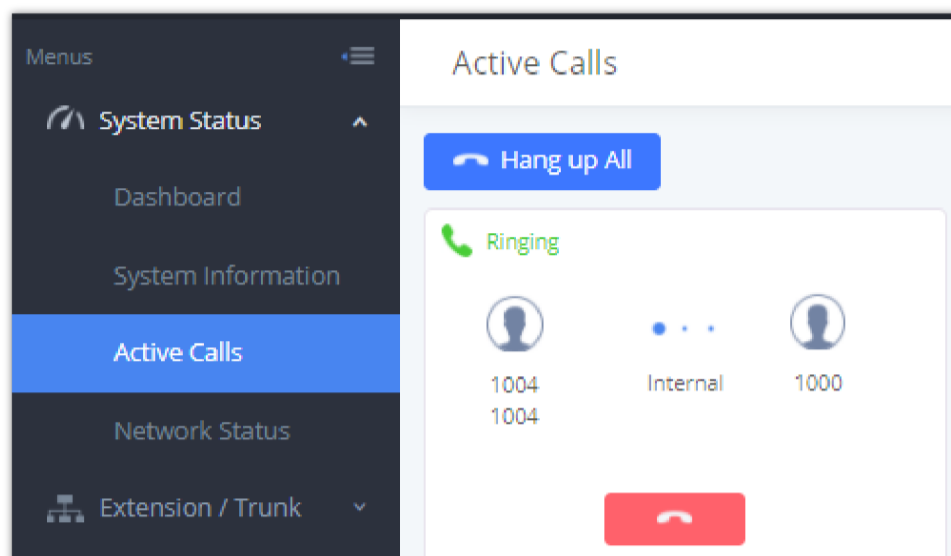
Please refer to [Username Prompt Customization] for User Name Prompt Customization.

# ACTIVE CALLS AND MONITOR

The active calls on the UCM630xA 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.

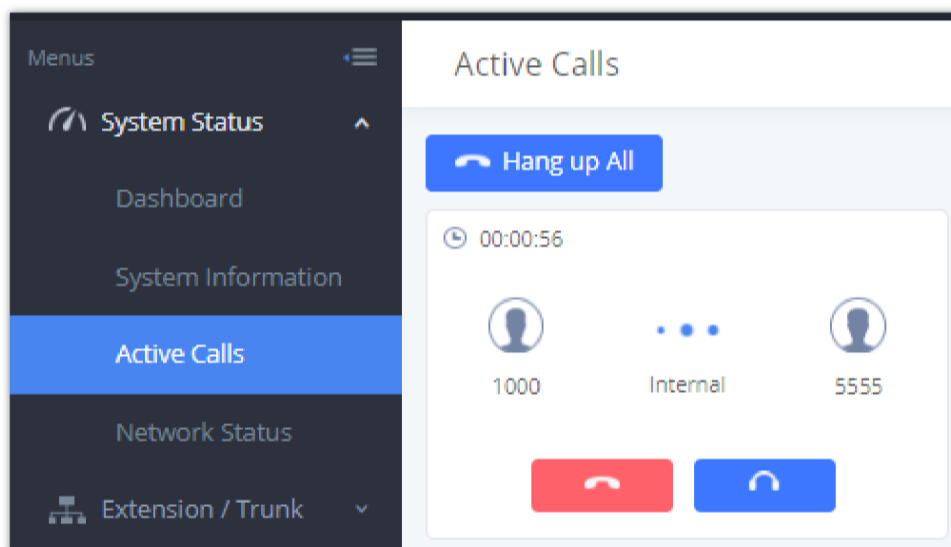
## Active Calls Status

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.



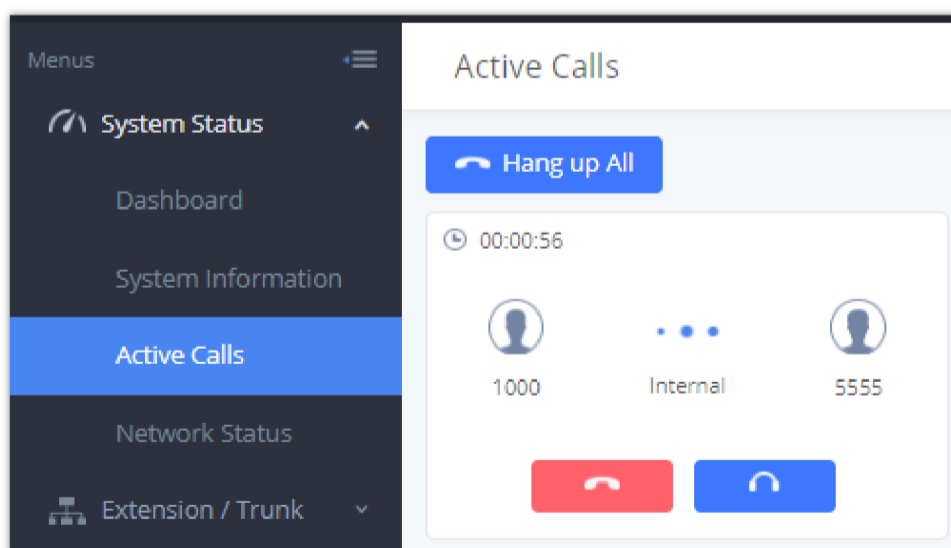
Active Calls – Call Ringing

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



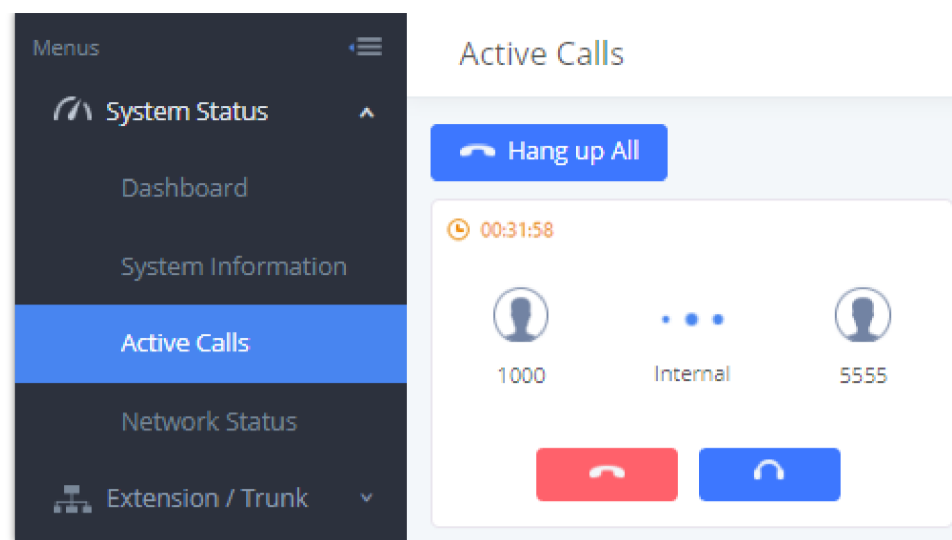
Active Calls – Call Established

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.



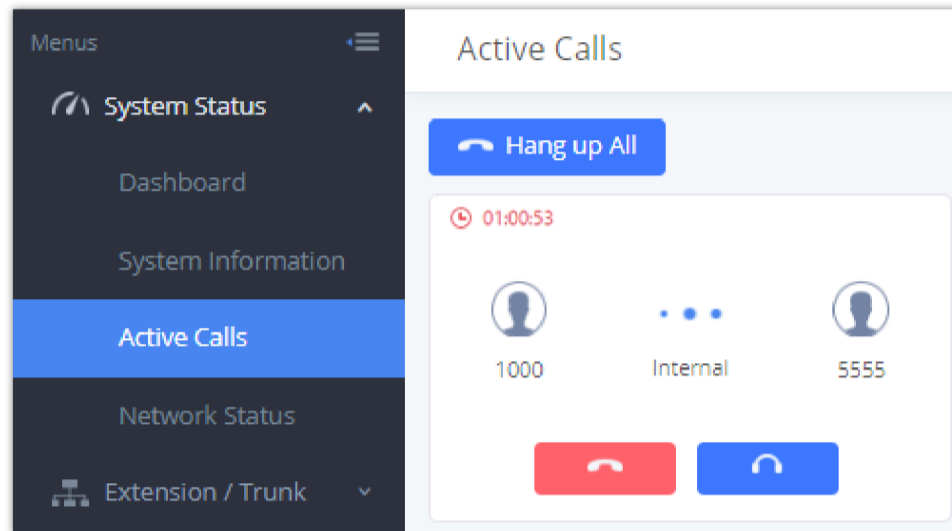
Call Duration: Less than 30 Minutes

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.



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.



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



to hang up all active calls.

## Call Monitor

During an active call, click on icon



and the monitor dialog will pop up.

**Call Barging** ✕

Monitor's Extension:

Monitored Extension:

Spy Modes:

Require Confirmation:

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 meeting.

1. 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.
2. 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 **[UCM630xA Feature Codes]** and **[Call Recording]** section for instructions.

## CALL FEATURES

The UCM630xA supports call recording, transfer, call forward, call park and other call features via feature code. This section lists all the feature codes in the UCM630xA and describes how to use the call features.

### Feature Codes

Feature codes allow users to perform certain actions such as call park or call forwarding, by dialing a configured code. For example, dialing #72 to park a call.

The UCM630xA is by default configured with feature codes for different use cases, but users can change these codes manually by accessing **Basic Call Features → Feature codes**.


#### Notes:

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


#### 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.


<p><b>Attended Transfer</b></p>	<ul style="list-style-type: none"> <li>- Default code: *2</li> <li>- 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.</li> <li>- Options: <ul style="list-style-type: none"> <li>● <b>Disable</b></li> <li>● <b>Allow Caller:</b> Enable the feature code on caller side only.</li> <li>● <b>Allow Callee:</b> Enable the feature code on callee side only.</li> <li>● <b>Allow Both:</b> Enable the feature code on both caller and callee.</li> </ul> </li> </ul>
<p><b>Transfer Dialing Timeout Period (s)</b></p>	<p>Configures the dial timeout period of blind and attended transfers.</p>
<p><b>Seamless Transfer</b></p> 	<ul style="list-style-type: none"> <li>● Default code: *44 (Disabled by default).</li> <li>● Seamless Transfer allows user to perform blind transfer using PBX feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple.</li> <li>● 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.</li> </ul> <p>(This feature code cannot be nested by other feature codes)</p>
<p><b>Disconnect</b></p>	<ul style="list-style-type: none"> <li>- Default code: *0</li> <li>- Enter the code during active call. It will disconnect the call.</li> <li>- Options: <ul style="list-style-type: none"> <li>● <b>Disable</b></li> <li>● <b>Allow Caller:</b> Enable the feature code on caller side only.</li> <li>● <b>Allow Callee:</b> Enable the feature code on callee side only.</li> <li>● <b>Allow Both:</b> Enable the feature code on both caller and callee.</li> </ul> </li> </ul>
<p><b>Call Park</b></p>	<ul style="list-style-type: none"> <li>- Default code: #72</li> <li>- Enter the code during active call to park the call.</li> <li>- Options: <ul style="list-style-type: none"> <li>● <b>Disable</b></li> <li>● <b>Allow Caller:</b> Enable the feature code on caller side only.</li> <li>● <b>Allow Callee:</b> Enable the feature code on callee side only.</li> <li>● <b>Allow Both:</b> Enable the feature code on both caller and callee.</li> </ul> </li> </ul>
<p><b>Feature Code Input Timeout (ms)</b></p>	<p>Configure the maximum interval (ms) between digits for feature code activation.</p>
<p><b>Start/Stop Call Recording</b></p>	<ul style="list-style-type: none"> <li>-Default code: *3</li> <li>- Enter the code followed by # or SEND to start recording the audio call and the PBX will mix the streams natively on the fly as the call is in progress.</li> <li>- Options: <ul style="list-style-type: none"> <li>● <b>Disable</b></li> <li>● <b>Allow Caller:</b> Enable the feature code on caller side only.</li> <li>● <b>Allow Callee:</b> Enable the feature code on callee side only.</li> <li>● <b>Allow Both:</b> Enable the feature code on both caller and callee.</li> </ul> </li> </ul>
<p><b>Enable Recording Whitelist</b></p>	<p>Enable the Recording Whitelist feature</p>
<p><b>Recording Operation Whitelist</b></p>	<p>Select extension in the whitelist that can use the *3 recording function.</p>
<p><b>Feature Code Digits Timeout</b></p>	<p>Set the maximum interval (ms) between digits for feature code activation</p>
<p><b>DND/Call Forward</b></p>	

<p><b>Call Forward Setting Type</b></p>	<ul style="list-style-type: none"> <li>• <b>Basic</b></li> <li>• <b>Advanced</b></li> </ul> <p>If <b>Advanced</b> is selected, call forwarding can be set for all calls, internal calls and external calls. To do this, users can dial one of the feature codes below and then dial <b>0, 1</b> or <b>2</b>.</p> <p>The feature code modifiers are as follow:</p> <p>→ <b>0</b> corresponds to "<b>All calls</b>".  → <b>1</b> refers to "<b>Internal calls</b>". (calls that came within the PBX)  → <b>2</b> is used for "<b>External calls</b>". (calls from outside the PBX)</p>
<p><b>Do Not Disturb (DND) Activate</b></p>	<p>Default code: <b>*77</b>  Activate DND feature to ignore any incoming calls.</p>
<p><b>Do Not Disturb (DND) Deactivate</b></p>	<p>Default code: <b>*78</b>  Deactivate DND Feature.</p>
<p><b>Call Forward Busy Enable</b></p> 	<p>Default Code: <b>*90</b>  Enables Call Forward Busy (CFB) for the dialing extension.  Assuming feature code is xxx, the following call forward setting methods are available :</p> <p><b>Method 1:</b> Dial xxx and follow the system prompts.  <b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000).  <b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000).  Methods 1 and 2 are supported in <b>Basic</b>.  Methods 1 and 3 are supported in <b>Advanced</b>.  (This feature code cannot be nested by other feature codes)</p>
<p><b>Call Forward Busy Disable</b></p>	<p>Default Code: <b>*91</b>  Disables Call Forward Busy (CFB) for the dialing extension. Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type:  <b>Basic:</b> Dial xxx.  <b>Advanced:</b> Dial xxx + 0/1/2.</p>
<p><b>Call Forward No Answer Enable</b></p> 	<p>Default Code: <b>*92</b>  Enables Call Forward No Answer (CFNA) for the dialing extension.  Assuming feature code is xxx, the following call forward setting methods are available :</p> <p><b>Method 1:</b> Dial xxx and follow the system prompts.  <b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000).  <b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000).  Methods 1 and 2 are supported in <b>Basic</b>.  Methods 1 and 3 are supported in <b>Advanced</b>.  (This feature code cannot be nested by other feature codes)</p>
<p><b>Call Forward No Answer Disable</b></p>	<p>Default Code: <b>*93</b>  Disables Call Forward No Answer (CFNA) for the dialing extension. Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type:  <b>Basic:</b> Dial xxx.  <b>Advanced:</b> Dial xxx + 0/1/2.</p>
<p><b>Call Forward Always Enable</b></p> 	<p>Default Code: <b>*72</b>  Enables Call Forward Always (CFA) for the dialing extension.  Assuming feature code is xxx, the following call forward setting methods are available :</p> <p><b>Method 1:</b> Dial xxx and follow the system prompts.  <b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000).  <b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000).  Methods 1 and 2 are supported in <b>Basic</b>.  Methods 1 and 3 are supported in <b>Advanced</b>.  (This feature code cannot be nested by other feature codes)</p>

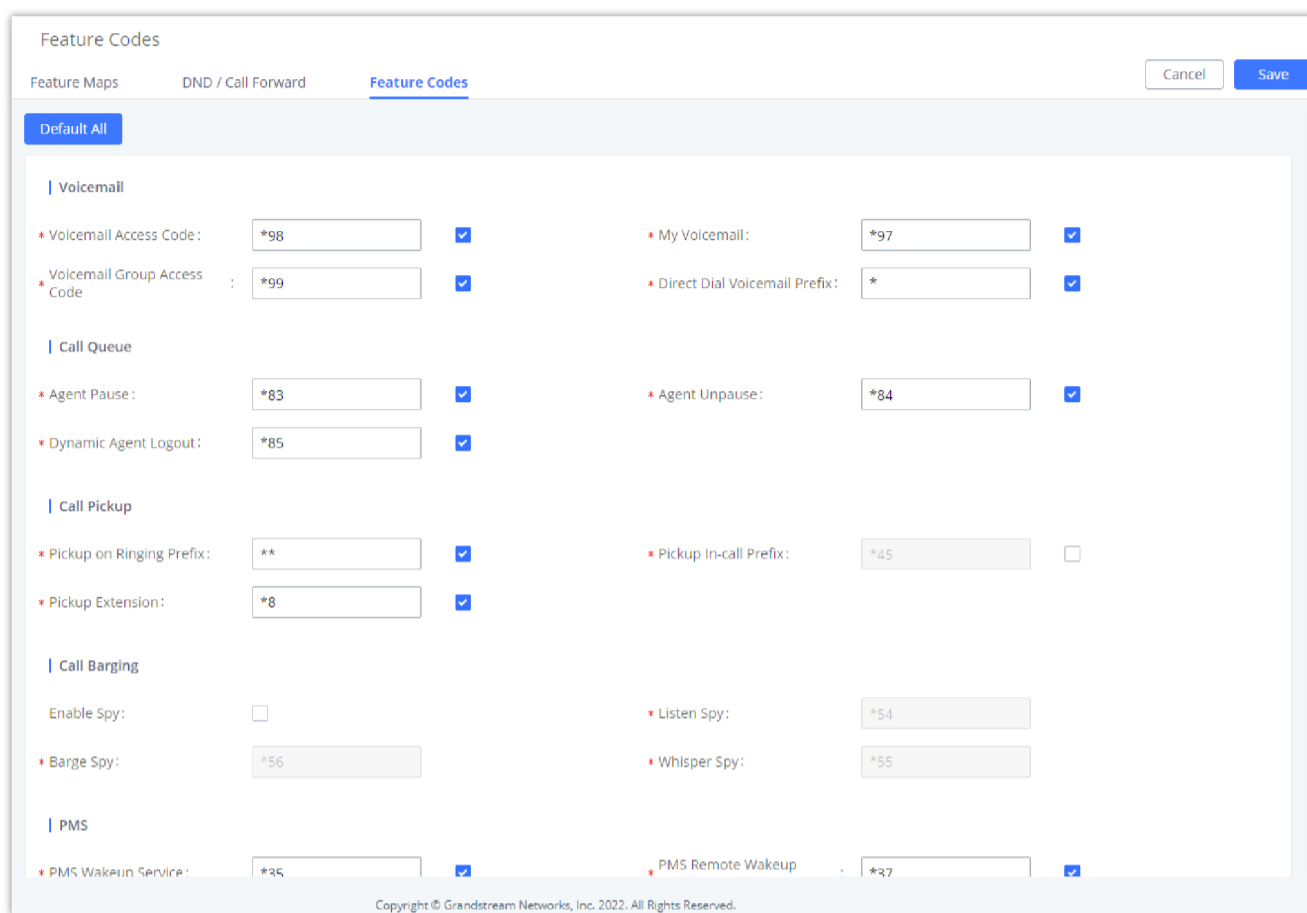
<b>Call Forward Always Disable</b>	<p>Default Code: <b>*73</b></p> <p>Disables Call Forward Always (CFA) for the dialing extension. Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type:</p> <p><b>Basic:</b> Dial xxx.</p> <p><b>Advanced:</b> Dial xxx + 0/1/2.</p>
<b>Remote Call Forward Enable</b>	<p>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.</p>
<b>Remote DND / Call Forward Settings</b>	
<b>Enable</b>	<p>Enable this option and configure the Whitelist below to allow specific extensions to dial feature codes to set DND or call forwarding for any extension.</p>
<b>Remote Call Forward Busy Enable</b>	<p>Default code: <b>*65</b></p> <p>Configures and enables CFB for any extension.</p>
<b>Remote Call Forward No Answer Enable</b>	<p>Default code: <b>*66</b></p> <p>Configures and enables CFNA for any extension.</p>
<b>Remote Call Forward Always Enable</b>	<p>Default code: <b>*67</b></p> <p>Configures and enables CFU for any extension.</p>
<b>Remote DND Enable</b>	<p>Default code: <b>*68</b></p> <p>Enables Do Not Disturb for any extension.</p>
<b>Remote Call Forward Busy Disable</b>	<p>Default code: <b>*651</b></p> <p>Disables CFB for any extension.</p>
<b>Remote Call Forward No Answer Disable</b>	<p>Default code: <b>*661</b></p> <p>Disables CFNA for any extension.</p>
<b>Remote Call Forward Always Disable</b>	<p>Default code: <b>*671</b></p> <p>Disables CFU for any extension.</p>
<b>Remote DND Disable</b>	<p>Default code: <b>*681</b></p> <p>Disables Do Not Disturb for any extension.</p>
<b>Whitelist</b>	<p>Extensions in this whitelist can configure DND or call forwarding for any extension via feature codes.</p>
<b>Feature Codes</b>	
<b>Voicemail</b>	
<b>Voicemail Access Code</b> 	<p>- Default code: <b>*98</b></p> <p>- Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>My Voicemail</b>	<p>- Default code: <b>*97</b></p> <p>- Press *97 to access the voicemail box.</p>
<b>Voicemail Group Access Code</b>	<p>Default code: <b>*99</b></p> <p>Dial this code to access group voicemail. If password is required, enter password followed by the pound (#) key.</p>

<b>Direct Dial Voicemail Prefix</b>	Prefix used to dial directly to voicemail.
<b>Call Queue</b>	
<b>Agent Pause</b> 	Default code: <b>*83</b> Pause the agent in all call queues. (This feature code cannot be nested by other feature codes)
<b>Agent Unpause</b>	Default code: <b>*84</b> Unpause the agent in all call queues.
<b>Dynamic Agent Logout</b>	Default code: <b>*85</b> Log the dynamic agent out of all queues.
<b>Call Pickup</b>	
<b>Pickup on Ringing Prefix</b> 	Picks up a ringing call for another extension. Example: If the prefix is **, and there is a call ringing ext 1008, dial **1008 from a different extension to pick up the call to 1008. (This feature code cannot be nested by other feature codes)
<b>Pickup In-call Prefix</b>	Picks up an ongoing call for another extension. Example: If the feature code is *45, and ext 1008 is in a call, dialing *45 and then 1008 following the prompt will take that call. Note: The feature code user must be in the extension's Allowed to seamless transfer list to pick up calls for it.
<b>Pickup Extension</b>	This is the feature code to pick up incoming calls for other extensions in the same pickup group. The default setting is *8.
<b>Call Barging</b>	
<b>Enable Spy</b>	Check this box to enable spy feature codes.
<b>Listen Spy</b> 	This is the feature code to listen in on a call to monitor performance. Your line will be muted, and neither party will hear you. The default setting is *54. (This feature code cannot be nested by other feature codes)
<b>Barge Spy</b> 	This is the feature code to join in on the call to assist both parties. The default setting is *56. (This feature code cannot be nested by other feature codes)
<b>Whisper Spy</b> 	This is the feature code to speak to only one party in the call. For example, you could whisper to employees to help them handle a call. Only an employee on your account will be able to hear you. The default setting is *55. (This feature code cannot be nested by other feature codes)
<b>PMS</b>	
<b>PMS Wakeup Service</b>	Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service.
<b>PMS Remote Wakeup Service</b>	Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions.
<b>Update PMS Room Status</b> 	2 methods are available: 1. Dial the room status feature code + housekeeper code, listen to the prompt and then dial the appropriate key for the desired room status. Example: The housekeeper with housekeeper code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available. 2. Dial room status feature code*housekeeper code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: Housekeeper with Housekeeper

	code 0001 dials *23*0001*1 to change room status Available. (This feature code cannot be nested by other feature codes)
<b>Misc</b>	
<b>Paging Prefix</b> 	Configure the paging prefix for paging. For example, if the Paging Prefix is set to *81, dial *816000 to initiate a paging call to extension 6000. (This feature code cannot be nested by other feature codes)
<b>Intercom Prefix</b> 	Configure the intercom prefix for intercom calls. For example, if the Intercom Prefix is set to *80, dial *806000 to initiate an intercom call to extension 6000. (This feature code cannot be nested by other feature codes)
<b>Blacklist Add</b>	Follow the voice prompt to add a caller ID to blacklist.
<b>Blacklist Last Caller</b>	Add the last inbound caller ID number to blacklist.
<b>Blacklist Remove</b>	Follow the voice prompt to remove a caller ID from blacklist.
<b>Direct Dial Mobile Phone Prefix</b> 	If calling mobile phone numbers is permitted, use this prefix plus the extension number to dial the mobile phone number of this extension directly. (This feature code cannot be nested by other feature codes)
<b>Call Completion Request</b>	If the caller wants to use CC to complete a call, he/she can dial this code. After the CC has been registered successfully, the system will start to monitor the status of the callee. The system will call back the caller when the callee's extension is available.
<b>Call Completion Cancel</b>	If the caller has requested CC successfully, and he/she doesn't need to call back anymore, he/she can dial this code to cancel the request.
<b>Presence Status</b>	Dial this feature code to set the presence status of the extension.
<b>Call Flip</b>	- Default code: <b>*46</b> - Dial this code to move the call of this extension from another device to the current device.
<b>Wakeup Service</b>	Dial this feature code to access PBX Wakeup Service. You can add, update, activate or deactivate PBX Wakeup Service.
<b>Remote Extension Privilege Update</b>	Whitelisted extensions will be able to use the Remote Extension Privilege Update feature code to remotely change any extension's outgoing call privilege. <b>Note:</b> After this function has been enabled, the extension is the whitelist can set the privilege for outgoing calls of any extension by dialing the feature code.
<b>Remote Extension Privilege Update Whitelist</b>	Remote Extension Privilege Update Whitelist <b>Procedure:</b> 1. Dial *26 on the whitelisted extension, hear the prompt "Change extension's outgoing permission level, please enter the phone number, then enter # key." 2. After the process, voice will prompt "Press 1 to set to internal, press 2 to set to local, press 3 to set to national, press 4 to set to international." 3. After selecting, it will prompt "Change extension XXXX outgoing permission to XXX", and hang up.
<b>Privileged Call</b>	Dial the feature code + extension number, for example *001002 to hang up the current call of extension 1002 with privilege, and then call extension 1002.
<b>Privileged Call Whitelist</b>	The extensions in this white list can use the feature code of the privileged call.

<b>Priority Call</b> 	<p>Makes a high priority call to a specified extension by dialing the feature + extension number. If the specified extension is an ongoing call, it will be forcibly hung up to allow the caller to ring the extension.          (This feature code cannot be nested by other feature codes)</p>
<b>Priority Call Whitelist</b>	<p>Extension in the whitelist will be allowed to use this feature code to make priority calls.</p>

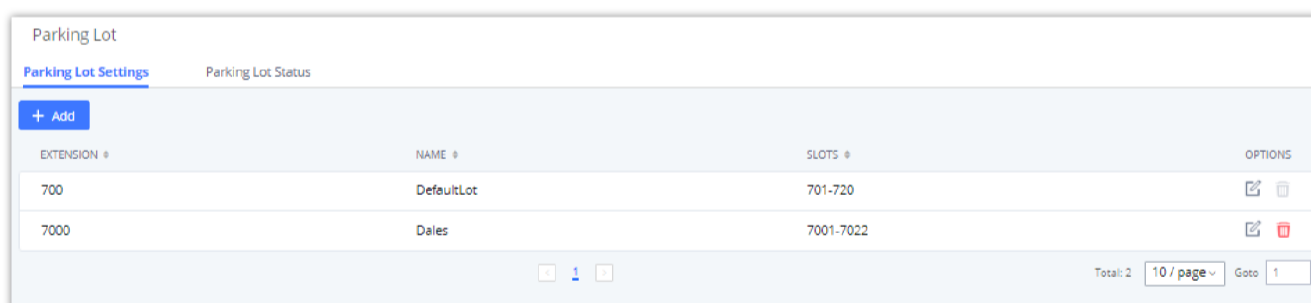
The UCM630xA also allows user to one click enable / disable specific feature code as shown below:



Enable/Disable Feature codes

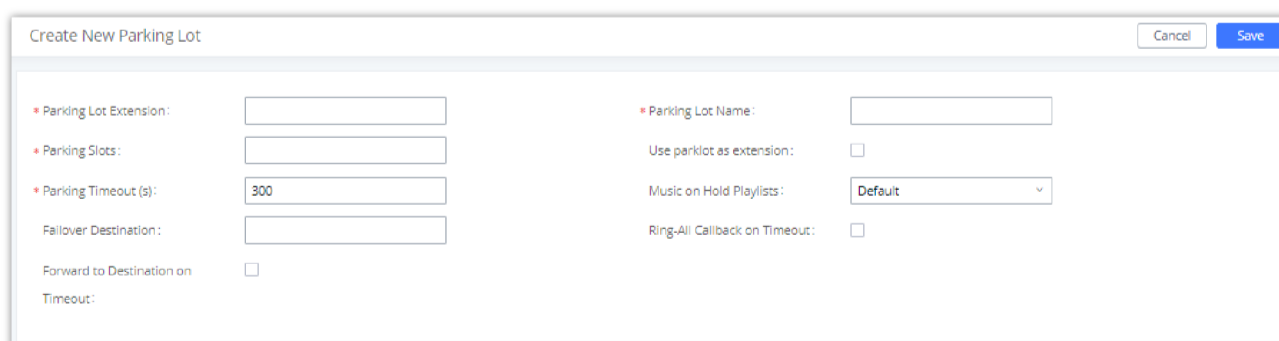
## Parking Lot

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



Parking Lot

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



New Parking Lot

## Parking Lot

<b>Parking Lot Extension</b>	<ul style="list-style-type: none"> <li>○ Default Extension: <b>700</b></li> <li>○ During an active call, initiate blind transfer and then enter this code to park the call.</li> </ul>
------------------------------	--

<b>Parking Lot Name</b>	<ul style="list-style-type: none"> <li>○ Set a name to the parking lot</li> </ul>
<b>Parked Slots</b>	<ul style="list-style-type: none"> <li>○ Default Extension: <b>701-720</b></li> <li>○ These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.</li> </ul>
<b>Use Parklot as Extension</b>	<ul style="list-style-type: none"> <li>○ 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.</li> </ul>
<b>Parking Timeout (s)</b>	<ul style="list-style-type: none"> <li>○ Default setting is <b>300</b> seconds, and the maximum limit is <b>99.999</b> seconds.</li> <li>○ 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.</li> </ul>
<b>Music On Hold Classes</b>	Select the Music on Hold Class.
<b>Failover Destination</b>	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.
<b>Ring All Callback on Timeout</b>	If enabled, all registered endpoints of the extension will ring when callback occurs. Otherwise, only the original endpoint will be called back.
<b>Forward to destination on timeout</b>	If enabled, the call will be routed to the configured destination upon timeout. Otherwise, the call will be routed back to the original caller.
<b>Timeout Destination</b>	This option appears once Forward to Destination on Timeout is enabled. Upon park timeout, the call will be routed to the configured destination.
<b>Parking Lot Timeout Alert-Info</b>	Adds an Alert-Info header to parking lot callbacks after the Parking Timeout has been reached.

## Call Park

The UCM630xA 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)





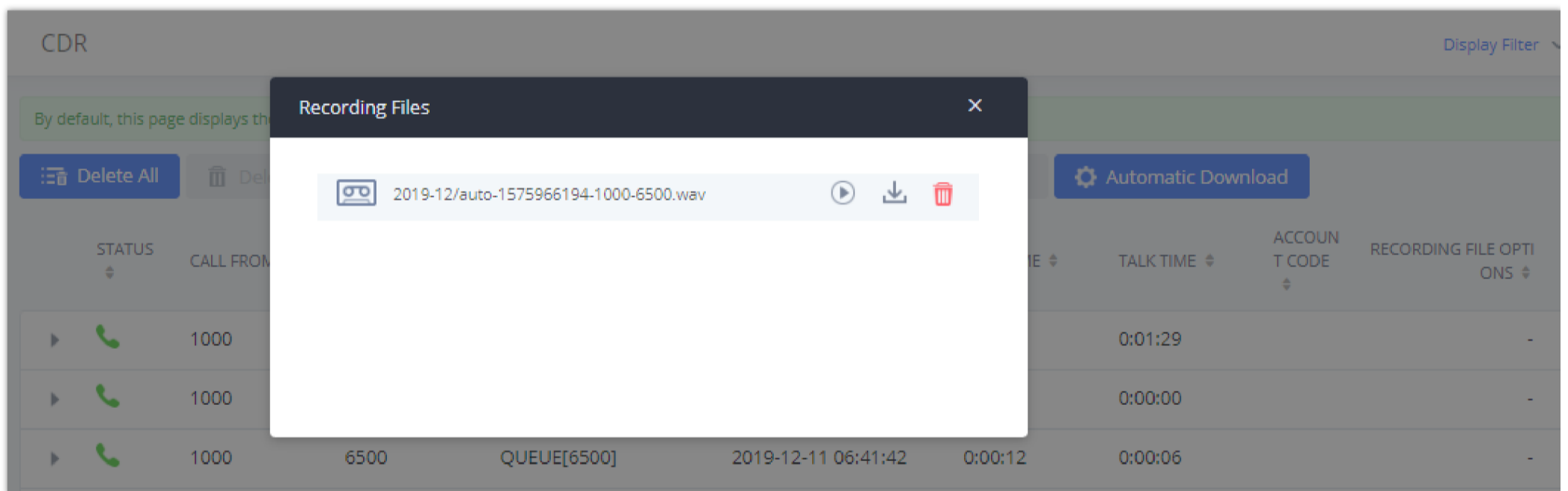
Users can see the CID name information of parked calls. VPK/MPKs must be configured as “Monitored Call Park” with the desired parking lot extension. The display will alternate between displaying the parking lot extension and the call’s CID name. There is no need to configure anything on the UCM.

## Call Recording

The UCM630xA 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.

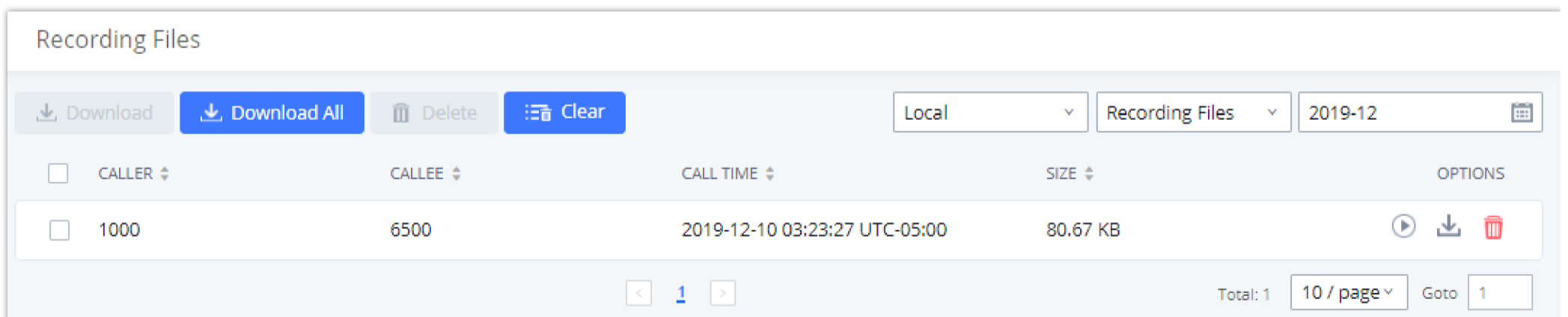
1. Make sure the feature code for “Start/Stop Call Recording” is configured and enabled.
2. After establishing the call, enter the “Start/Stop Call Recording” feature code (by default it is \*3) followed by # or SEND to start recording.
3. To stop the recording, enter the “Start/Stop Call Recording” 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.



Download Recording File from CDR Page

The above recorded call’s recording files are also listed under the UCM630xA Web GUI→**CDR**→**Recording Files**.



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

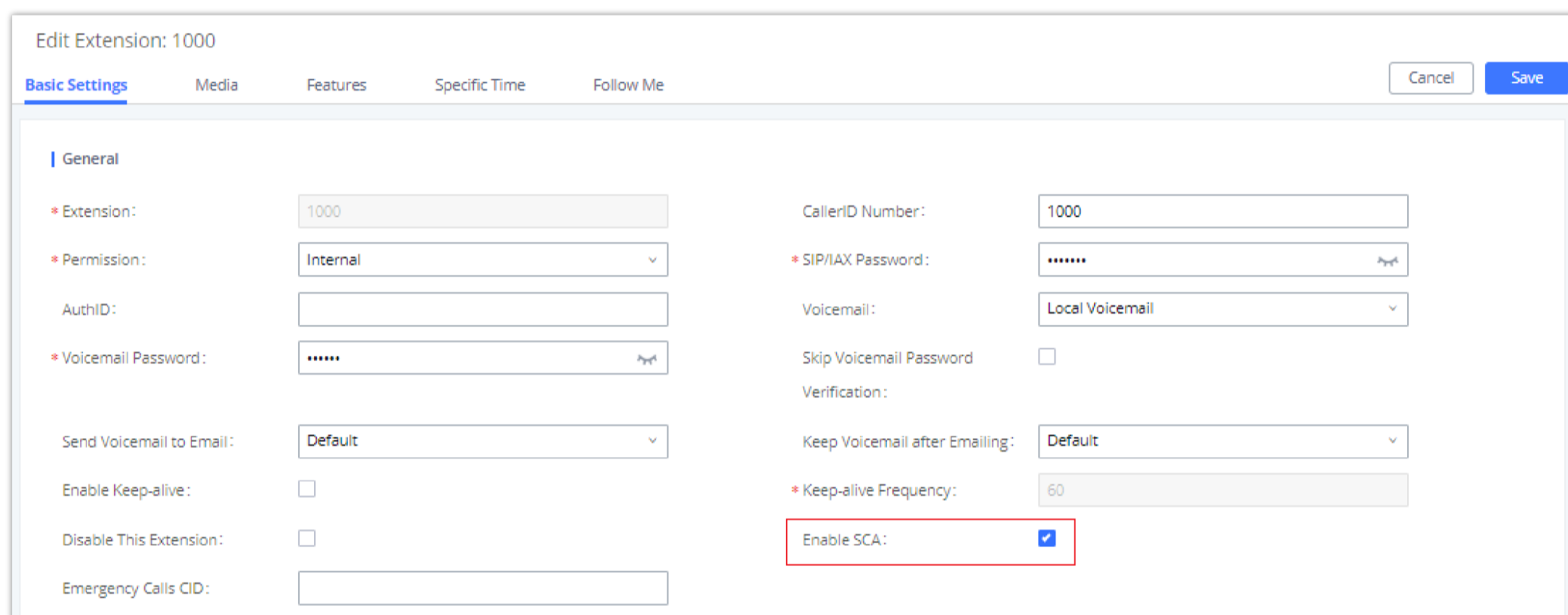
"Enable Spy" allows any user to listen to any call by feature codes. This may result in the leakage of user privacy.

## 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.



Basic Settings | Media | Features | Specific Time | Follow Me

Cancel Save

General

\* Extension: 1000

\* Permission: Internal

AuthID:

\* Voicemail Password: \*\*\*\*\*

Send Voicemail to Email: Default

Enable Keep-alive:

Disable This Extension:

Emergency Calls CID:

CallerID Number: 1000

\* SIP/IAX Password: \*\*\*\*\*

Voicemail: Local Voicemail

Skip Voicemail Password:

Verification:

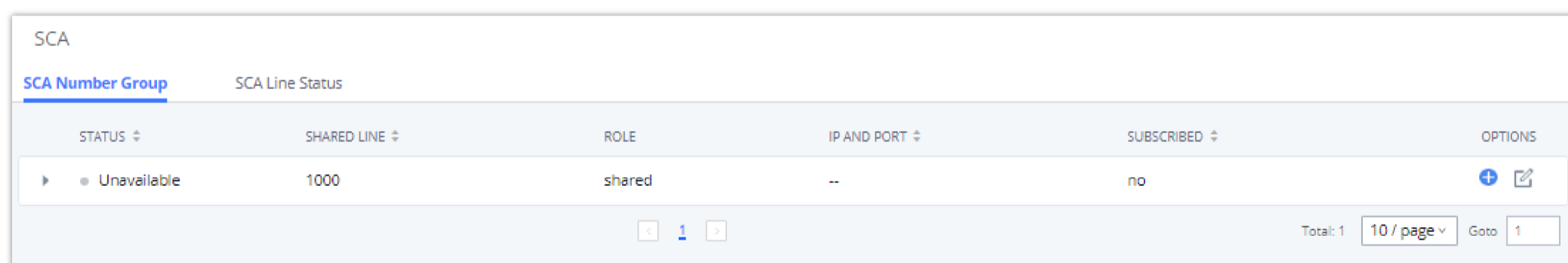
Keep Voicemail after Emailing: Default

\* Keep-alive Frequency: 60

Enable SCA:

Enabling SCA option under Extension's Settings

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



SCA

SCA Number Group | SCA Line Status

STATUS	SHARED LINE	ROLE	IP AND PORT	SUBSCRIBED	OPTIONS
Unavailable	1000	shared	--	no	+ [edit]

Total: 1 | 10 / page | Goto 1

SCA Number Configuration

3. Configure the private number as desired.

SCA Private Number Configuration

4. Once the private number has been created, users must now register a device to it. To properly register a device to the private number, use the configured private number as the SIP User ID. Auth ID and Password will be the same as the main extensions. Once registration is complete, SCA is now configured.

SCA Options

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

The following table describe the SCA Number configuration setting:

Add SCA Private Number

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

#### Editing the SCA Number

<b>Shared Line Number</b>	While SCA is enabled, this number will be the same as the extension number.
<b>Allow Call Retrieve from Another Location</b>	Allows remote call retrieval. Must be enabled in public hold. By default, it is enabled.
<b>Alert All Appearances for Group Paging Calls</b>	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.
<b>Multiple Call Arrangement</b>	Allows simultaneous calls in an SCA group. By default, it is disabled.
<b>Allow Bridging between Locations</b>	Allows location bridging for SCA group. Must be enabled when using the Barge-In feature. By default, it is disabled.
<b>Bridge Warning Tone</b>	<p>Configures the notification in the bridge when another party join.</p> <ul style="list-style-type: none"> <li>○ None: No notification sound.</li> <li>○ Barge-In only: Notification sound will play when another party join.</li> <li>○ Barge-In and Repeat: Notification sound will play when another party joins and repeat every 30 seconds.</li> </ul> <p>By default, it is set to "Barge-In Only".</p>

## Time Condition Routing

Time Condition Routing allows the user to create default destinations for calls which are based on time conditions under **Advanced Call Features**→**Time Condition Routing**.

**Time Condition Routing > Create New Time Condition Routing**

\* Name

\* Time

Create new time groups in [Time Settings -> Custom Time Groups](#).

**Time Match**

\* Default Destination

**Time Mismatch**

\* Default Destination

*Time Condition Routing*

# 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 **Advanced 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.

Create New Announcement

\* Name:

Prompt:  [Upload Audio File](#)

Default Destination:

*Announcement settings*

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

<b>Name</b>	Configure the name of the Announcement.
<b>Prompt</b>	Choose/upload the audio file to play when the call reaches this announcement.
<b>Default Destination</b>	Select the destination which the call will be forwarded to after the announce has been played.

*Announcement Parameters*

# 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 UCM630xA, 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

Internal Options/General

General Preferences	
<b>Global Outbound CID</b>	Global-level CID Number used for all outgoing calls if no other CID numbers have been configured for the calling party.
<b>Global Outbound CID Name</b>	Global-level CID Name used for all outgoing calls if no other CID names have been configured for the calling party.
<b>Ring Timeout (s)</b>	Number of seconds to ring the extension before forwarding the call to voicemail. If <b>Extensions &gt; Features &gt; Ring Timeout</b> is not configured, the ring timeout value configured in <b>General Settings &gt; Ring Timeout</b> will be

	used.
<b>Call Duration Limit</b>	Block calls for the configured duration. If <b>Extensions &gt; Features &gt; Call Duration Limit</b> and <b>Outbound Routes &gt; Call Duration Limit</b> are not configured, <b>General Settings &gt; Call Duration Limit</b> will be used. <b>Note:</b> This setting is disabled by default
<b>Recording Settings</b>	
<b>Record Prompt</b>	If enabled, the system will play voice prompt "This call will be recorded" before the recording is started. <b>Note:</b> This setting is disabled by default
<b>Allow External Numbers to Cancel Recording</b>	If enabled, external call parties will be given the option to decline the recording of calls.
<b>Merge Same Call Recordings</b>	If enabled, the system will merge all recordings created during a call regardless of how many times a user starts and stops recording during a call.
<b>Stereo Recording</b>	If enabled, the caller and callee's audio will be split into two channels during call recording. Not applicable to calls with more than 2 parties.
<b>Calling Channel</b>	Configure the audio channels for the calling party and the called party. If the caller is selected as the right channel, the callee will be used for the left channel, and vice-versa. <b>Note:</b> This option is available when "Stereo Recording" is enabled.
<b>International Call Prefix</b>	When this configuration is empty, International Call Prefix can be empty or +.
<b>Extension Preferences</b>	
<b>Enforce Strong Password</b>	If enabled, a strong password policy will be enforced. This does not affect user login passwords, which must be strong.
<b>Enable Random Password</b>	If enabled, the extension will be created with a randomly generated password.
<b>Send Extension Update Emails</b>	If enabled, an email will be sent to an extension's configured email address after creating it or modifying that extension's settings.
<b>Disable Extension Range</b>	If set to "Yes", users could disable the extension range pre-configured/configured on the IPPBX. The default setting is "No". <b>Note:</b> It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.
<b>User Extensions</b>	1000-6299 User Extensions is referring to the extensions created under <b>Web GUI &gt; Extension/Trunk &gt; Extensions</b> page.
<b>Meeting Extensions</b>	6300-6399 This extension range is used for creating meeting rooms
<b>Ring Group Extensions</b>	6400-6499 This extension range is used for ring groups
<b>Queue Extensions</b>	6500-6599 This range of extensions is used for queueing
<b>Voicemail Group Extension</b>	6600-6699 This extension range is used for voicemail groups.
<b>IVR Extensions</b>	7000-7100 This extension range is used for
<b>Dial by Name Extensions</b>	7101-7199 This extension range is used for Dial by Name feature
<b>Fax Extensions</b>	7200-8200 This extension range is used for T.38 Fax

## Zero Config Extension

<b>Pick Extensions</b>	4000-4999 This refers to the extensions that can be manually picked from end device when being provisioned by the IPPBX. 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.
<b>Auto Provision Extensions</b>	5000-6299 This sets the range for “Zero Config Extension Segment” which is the extensions can be assigned on the IPPBX to provision the end device.
<div style="border: 1px solid black; background-color: #007bff; color: white; padding: 5px; display: inline-block; border-radius: 5px;">Default Extension Segment</div>	Clicking this button will reset the extension range to their default values.

## PBX Settings/RTP Settings

### RTP Settings

#### Internal Options/RTP Settings

<b>RTP Start</b>	Configure the RTP port starting number. The default setting is 10000.
<b>RTP End</b>	Configure the RTP port ending address. The default setting is 20000.
<b>Strict RTP</b>	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".
<b>RTP Checksums</b>	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".
<b>ICE Support</b>	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.
<b>STUN Server</b>	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.
<b>BFCP UDP Start</b>	Configure BFCP UDP port starting number. The default setting is 50000.
<b>BFCP UDP End</b>	Configure BFCP UDP port ending number. The default setting is 52999.
<b>BFCP TCP Start</b>	Configure BFCP TCP port starting number. The default setting is 53000.
<b>BFCP TCP End</b>	Configure BFCP TCP port ending number. The default setting is 55999.
<b>TURN Server</b>	Configure TURN server address. TURN is an enhanced version of the STUN protocol and is dedicated to the processing of symmetric NAT problems.
<b>TURN Server Name</b>	Configure turn server account name

<b>TURN Server Password</b>	Configure turn server account password.
<b>Connection Protocol</b>	Protocol used to connect to the TURN server.
<b>Number of ICE Candidates</b>	This configures the number of pre-collected ICE candidates to gather and send to remote peers. The higher the number, the greater the network traffic consumption.

## Payload

The UCM630xA payload type for audio codecs and video codes can be configured here.

### Internal Options/Payload

<b>AAL2-G.726</b>	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112.
<b>DTMF</b>	Configured payload type for DTMF. The default setting is 101.
<b>G.721 Compatible</b>	Configure to enable/disable G.721 compatible. The default setting is Yes.
<b>G.726</b>	Configure the payload type for G.726 if "G.721 Compatible" is disabled. The default setting is 111.
<b>iLBC</b>	Configure the payload type for iLBC. The default setting is 97.
<b>OPUS</b>	Configure the payload type for OPUS. The default setting is 123.
<b>Audio FEC Payload Type</b>	Configure the Audio FEC Payload Type. The default setting is 127
<b>Audio RED Payload Type</b>	Configure the Audio RED Payload Type. Default setting is 122
<b>H.264</b>	Configure the payload type for H.264. The default setting is 99.
<b>H.263P</b>	Configure the payload type for H.263+. The default setting is 100 103.
<b>VP8</b>	Configure the payload type for VP8. The default setting is 108.
<b>Main Video FEC</b>	Configure the Main Video FEC
<b>RTP FECC</b>	Configure the RTP FECC
<b>RTX</b>	Configure the RTX
<b>G.722.1</b>	G.722.1: Low-complexity coder, 24kbps.
<b>G.722.1C</b>	G.722.1C: Low-complexity coder, 48kbps.

## PBX Settings/Voice Prompt Customization

### Record New Custom Prompt

In the UCM630xA Web GUI → **PBX Settings** → **Voice Prompt** → **Custom Prompt** page, click on "Record" and follow the steps below to record new IVR prompt.

Record New Custom Prompt
✕

**Note:** The mp3 sound file will be converted to wav format.

\* File Name:

Format:

Extension:

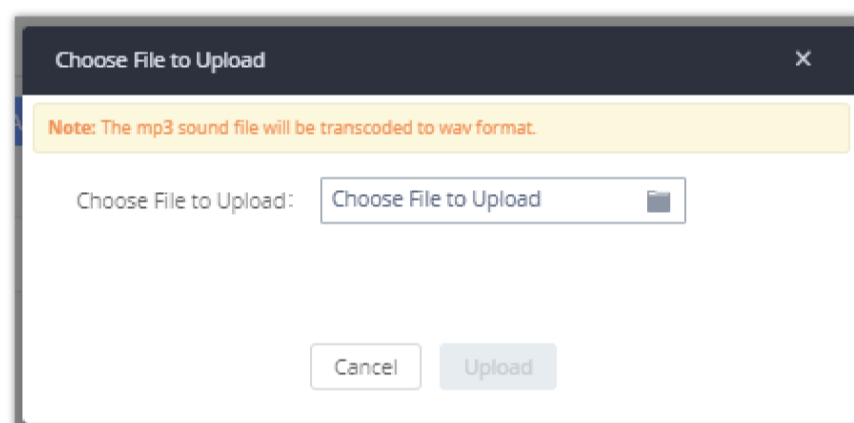
Record New Custom Prompt

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 UCM630xA to record the IVR prompt.
4. Click the "Record" button. A request will be sent to the UCM630xA. The UCM630xA 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 UCM630xA. The following are required for the IVR prompt file to be successfully uploaded and used by the UCM630xA:

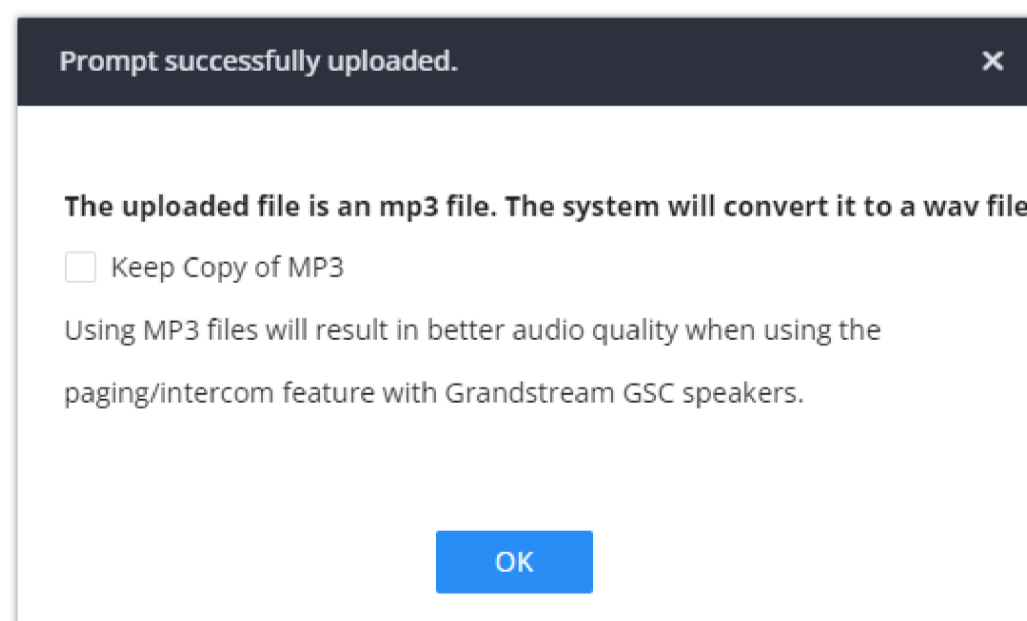
- PCM encoded.
- 16 bits.
- 8000Hz mono.
- In .mp3 or .wav format; or raw/ulaw/alaw/gsm file with .ulaw or .alaw suffix.
- File size under 5M.



*Upload Custom Prompt*

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

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



Tick "Keep Copy of MP3" to keep an mp3 copy of the file which can be diffused with certain GSC speakers. Diffusing the MP3 files result in a higher quality sound played by GCS speakers.

## Download All Custom Prompt

On the UCM630xA, the users can download all custom prompts from UCM Web GUI to local PC. To download all custom prompt, log in UCM Web GUI and navigate to **PBX Settings**→**Voice Prompt**→**Custom Prompt** and click on "Download All". The following window will pop up in order to set a name for the downloaded file.

Download All Custom Prompt

**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.

SIP Trunk Prompt Tone

## General Call Prompt Tones

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 Tones**" page as shown on the following figure:

Call Prompt Tones

SIP Trunk Prompt Tone      **General Call Prompt Tones**      Cancel      Save

Specify the tones to play for various general call scenarios.

Reset All      Default All

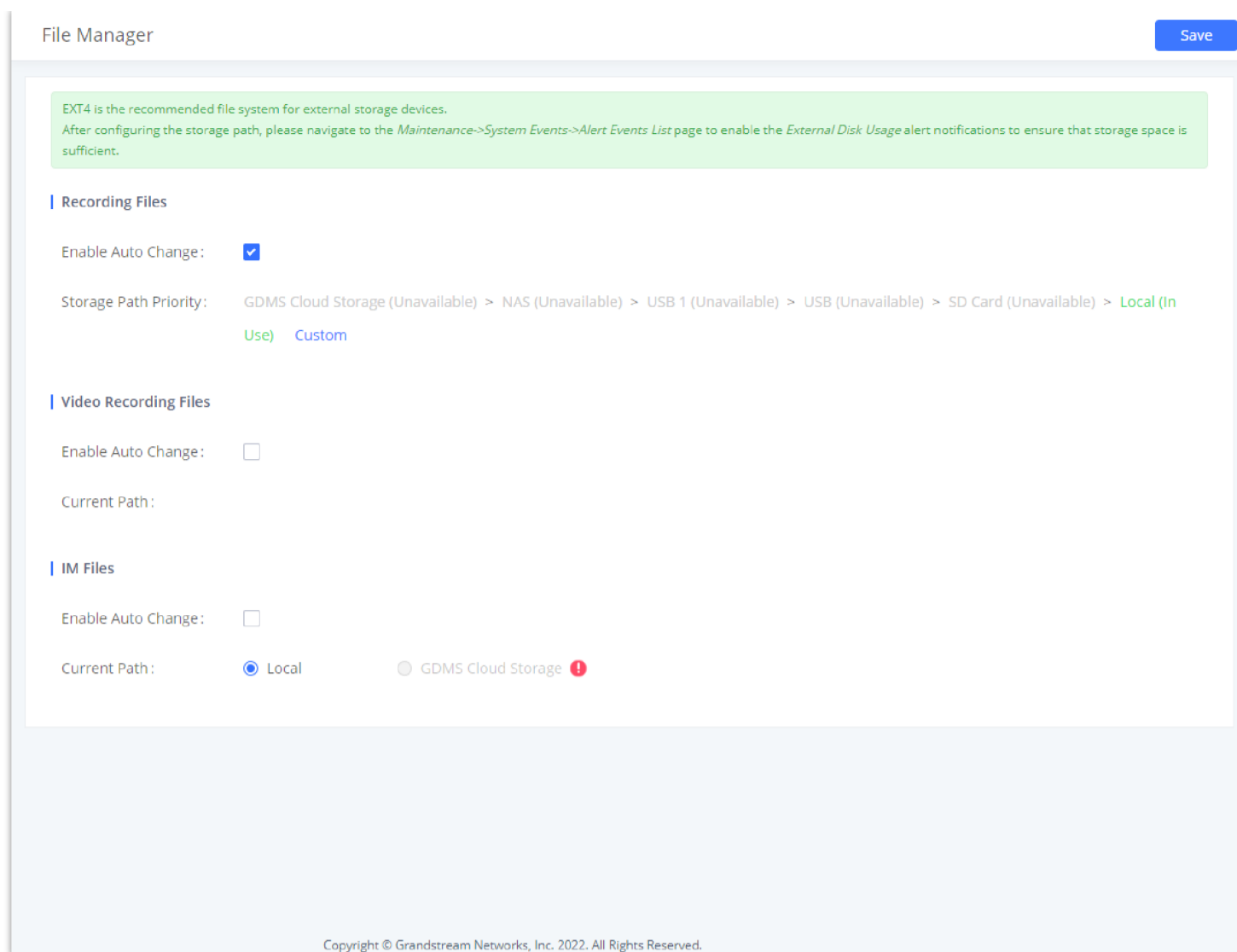
Bad Number:	wrong-number	Out Of Service:	out-of-service
User Busy:	user-busy	Trunk Busy:	trunk-busy
No Answer:	no-answer	No Permission:	no-permission
Do Not Disturb:	user-busy	General Failed:	general-failed
Call Waiting:	Default Ringback Tone		

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

General call Failure Prompts

## File Manager

UCM supports automatic or manual recording of calls and storage of IM chat files. Files are allowed to be saved in UCM local or external storage devices, and can even be stored in GDMS cloud storage. The chat files are only allowed to be saved in UCM local or external storage devices, users can go to UCM630xA Web GUI→**PBX Settings**→**File Manager** page and select whether to store the recording files in USB Disk, SD card, GDMS or locally on the UCM630xA.



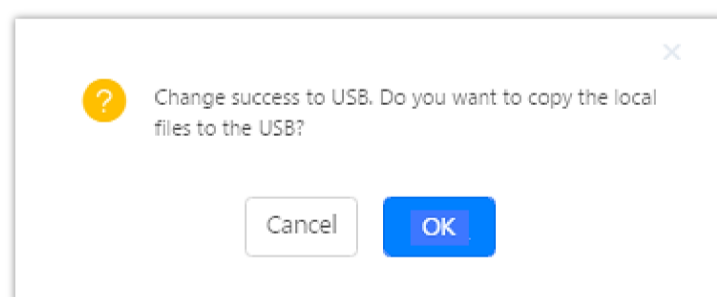
File Manager

## Note

Once a storage device has filled up, the UCM will choose the next available storage device based on the *Storage Path Priority*.

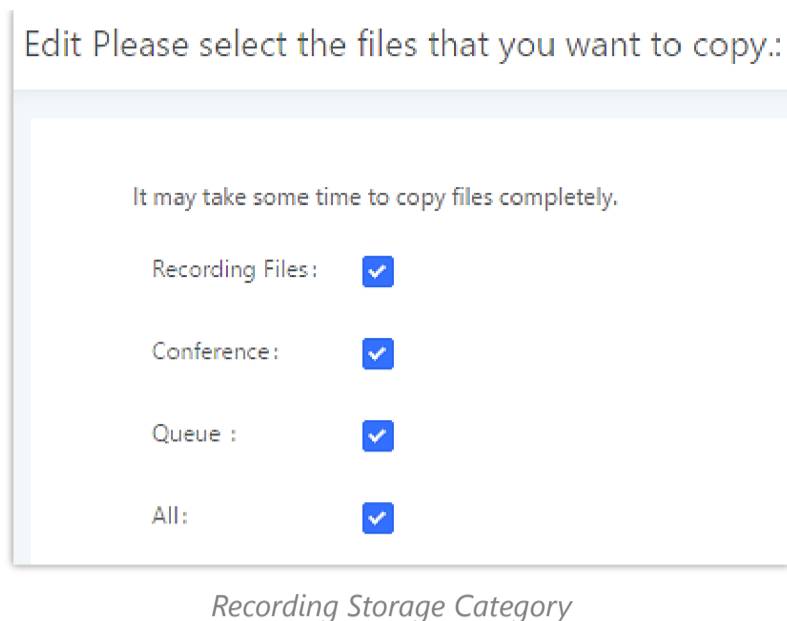
- If **“Enable Auto Change”** is selected, the files will be automatically saved in the available USB Disk or SD card plugged into the UCM630xA. If both USB Disk and SD card are plugged in, the files will be always saved in the USB Disk.
- When “Enable Auto Change” is enabled, the option **“Storage Path Priority”** will appear. It allows the user to configure the priority of each storage unit in the priority list (The storage on top of the list has the highest priority). The default priority list is *GDMS Cloud Storage > NAS > USB 1 > USB > SD Card > Local*
- If **“Local”** is selected, the files will be stored in UCM630xA internal storage.
- If **“GDMS Cloud Storage”** is selected, data will no longer be stored locally and if you need to listen to the recording, download the file to the computer side and play it offline.

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.



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.



On the UCM630xA, 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.
- **Meeting:** Copy the meeting 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:

### NAS Settings

<b>Enable</b>	Enabled / Disable the NAS recording functionality.
<b>Host</b>	Configure the Domain or IP address of the NAS server. <b>Note:</b> Currently, only IP addresses are supported in the Host/IP field.
<b>Folder Path</b>	Specify the name of the shared folder. <b>Example:</b> folder1/subfolder2
<b>Username</b>	Specify the account username to access the NAS server.
<b>Password</b>	Configure the account password to access the NAS server. The password can include letters, number, and special characters.
<b>Security Mode</b>	Select a security mode based on the server settings to ensure proper connection establishment. The default value is ntlmssp. <ul style="list-style-type: none"> <li>● None</li> <li>● krb5</li> <li>● krb5i</li> <li>● ntlm</li> <li>● ntlmi</li> <li>● ntlmv2</li> <li>● ntlmssp</li> <li>● ntlmsspi</li> </ul>
<b>Status</b>	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 <b>PBX Settings→Recording Storage</b> page and <b>CDR→Recording Files</b> page.

### Important

If Network Storage Device has 1GB of storage space left, it will be considered unavailable the UCM will trigger the external disk usage alert.

## SIP SETTINGS

The UCM630xA SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

### SIP Settings/General

SIP Settings/General

<b>Realm For Digest Authentication</b>	Configure the host name or domain name for the UCM630xA. Realms MUST be globally unique according to RFC3261. The default setting is Grandstream.
<b>Bind UDP Port</b>	Configure the UDP port used for SIP. The default setting is 5060.
<b>Bind IPv4 Address</b>	Configure the IPv4 address to bind to. The default setting is 0.0.0.0, which means binding to all addresses.
<b>Bind IPv6 Address</b>	Configure the IPv6 address to bind to. The default is : “[::]” and it means to bind to all IP addresses.
<b>Allow Guest Calls</b>	<p>If enabled, the UCM630xA allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is “No”.</p> <p><b>Warning:</b></p> <p>Please be aware of the potential security risk when enabling “Allow Guest Calls” as this will allow any user with the UCM630xA address to dial into the UCM630xA.</p>
<b>Allow Transfer</b>	If set to “No”, all transfers initiated by the endpoint in the UCM630xA will be disabled (unless enabled in peers or users). The default setting is “Yes”.
<b>MWI From</b>	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.
<b>Enable Diversion Header</b>	If disabled, the UCM will not forward the diversion header.
<b>Block Collect Calls</b>	<p>If enabled, collect calls will be blocked.</p> <p><b>Note:</b> Collect calls are indicated by the header “P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call”.</p>

### SIP Settings/MISC

SIP Settings/Misc

Outbound SIP Registrations	
<b>Register Timeout</b>	Configure the register retry timeout (in seconds). The default setting is 20.
<b>Register Attempts</b>	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.

<b>Trunk Register Period (s)</b>	Configures the time window within which to send initial trunk registration requests. Instead of sending out all initial trunk registration requests at once, requests will be randomly sent out within this period.
<b>Video</b>	
<b>Support SIP Video</b>	Select to enable video support in SIP calls. The default setting is "Yes".
<b>Security</b>	
<b>Reject Non-Matching INVITE</b>	If enabled, when rejecting an incoming INVITE or REGISTER request, the UCM630X will always reject with "401 Unauthorized" instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. Default setting is "No".
<b>SDP Attribute Passthrough</b>	
<b>Enable Attribute Passthrough</b>	If enable, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passthrough.
<b>Early Media</b>	
<b>Enable Use Final SDP</b>	If enabled, call negotiation will use final response SDP.
<b>Ignore 180 Response</b>	If enabled, ringing indication after 183 response will be ignored.
<b>Blind Transfer</b>	
<b>Allow callback when blind transfer fails</b>	If enabled, the UCM will call back to the transferrer when blind transfer fails (reason of failure includes busy and no answer). <b>Note:</b> This feature takes effect only on internal calls.
<b>Blind transfer timeout</b>	Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s.
<b>Hold</b>	
<b>Forward HOLD Requests</b>	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. <b>Note:</b> Enabling this option may cause hold retrieval issues and MOH to not be heard.

## SIP Settings/Session Timer

### SIP Settings/Session Timer

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

## SIP Settings/TCP and TLS

**SIP Settings**

General Session Timer **TCP/TLS** NAT ToS STIR/SHAKEN >

Cancel Save

TCP Enable

TCP Bind IPv4 Address

TCP Bind IPv6 Address

TLS Enable

TLS Bind IPv4 Address

TLS Bind IPv6 Address

TLS Do Not Verify

TLS Self-signed CA  [Reset Certificates](#)

**Private Certificate and Key**

TLS Cert  [Reset Certificates](#)

TLS Key  [Reset Certificates](#)

**Cipher Suite**


Cipher Blacklist

© 2023 Grandstream Networks, Inc.

### TCP/TLS

## SIP Settings/TCP and TLS

<b>TCP Enable</b>	Configure to allow incoming TCP connections with the PBX. The default setting is “No”.
<b>TCP Bind IPv4 Address</b>	Configure the IP address for the TCP server to bind to. “0.0.0.0” means binding to all interfaces. The port number is optional, and the default port number is 5060. For example, 192.168.1.1:5062.
<b>TCP Bind IPv6 Address</b>	Configure the IPv6 address for the TCP server to bind to. “[:]” means bind to all interfaces. The port number is optional with the default being 5060. For example, [2001:0DB8:0000:0000:0000:1428:0000]:5060.
<b>TLS Enable</b>	Configure to allow incoming TLS connections with the PBX. The default setting is “Yes”.
<b>TLS Bind IPv4 Address</b>	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.
<b>TLS Bind IPv6 Address</b>	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, [2001:0DB8:0000:0000:0000:1428:0000]: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.
<b>TLS Do Not Verify</b>	If enabled, the TLS server’s certificate will not be verified when acting as a client. The default setting is “Yes”.
<b>TLS Self-Signed CA</b>	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.
<a href="#">Reset Certificates</a>	Clicking on this button will reset the certificates.
<b>Private Certificate and Key</b>	
<b>TLS Cert</b>	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.

	<b>Note:</b> The size of the uploaded certificate file must be under 2MB.
<b>TLS Key</b>	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. <b>Note:</b> The size of the uploaded CA certificate file must be under 2MB.
	Clicking on this button will reset the certificates.
<b>Cipher Suite</b>	
<b>Restrict Cipher List</b>	By default, all SIP TLS encryption suites are in effect on the system, and when turned on, you can configure the encryption suites allowed to be used.
<b>Cipher Suite</b>	Select the encryption suites that are allowed to be used for SIP TLS connections, in the order of priority as configured.

## SIP Settings/NAT

### SIP Settings/NAT

<b>External Host</b>	Configure a static IP address and port (optional) used in outbound SIP messages if the UCM630xA is behind NAT. If it is a host name, it will only be looked up once.
<b>Use IP address in SDP</b>	If enabled, the SDP connection will use the IP address resolved from the external host.
<b>External UDP Port</b>	Configure externally mapped UDP port when the PBX is behind a static NAT or PAT.
<b>External TCP Port</b>	Configure the externally mapped TCP port when the UCM630xA is behind a static NAT or PAT.
<b>External TLS Port</b>	Configures the externally mapped TLS port when UCM630xA is behind a static NAT or PAT.
<b>Local Network Address</b>	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

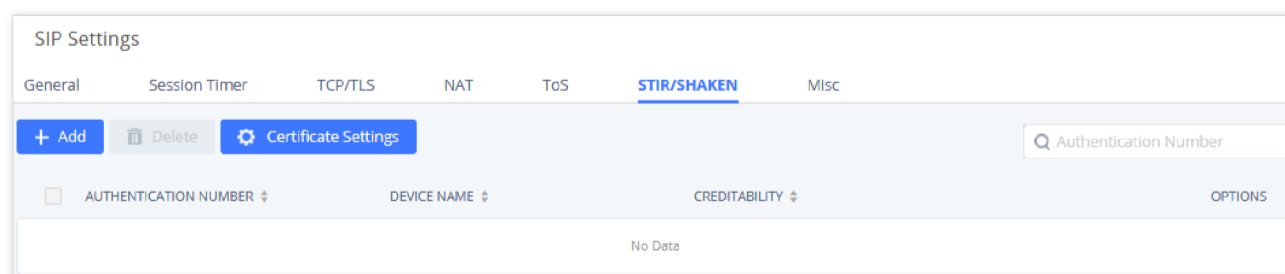
### SIP Settings/ToS

<b>ToS for SIP</b>	Configure the Type of Service for SIP packets. The default setting is None.
<b>ToS for RTP Audio</b>	Configure the Type of Service for RTP audio packets. The default setting is None.
<b>ToS for RTP Video</b>	Configure the Type of Service for RTP video packets. The default setting is None.
<b>Default Incoming/Outgoing Registration Time</b>	Configure the default duration (in seconds) of incoming/outgoing registration.  The default setting is 120.
<b>Max Registration/Subscription Time</b>	Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the UCM630xA. The default setting is 3600.
<b>Min Registration/Subscription Time</b>	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM630xA. The default setting is 60.
<b>Enable Relaxed DTMF</b>	Select to enable relaxed DTMF handling. The default setting is "No".

<b>DTMF Mode</b>	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".
<b>RTP Timeout</b>	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.  <b>Note:</b> This setting does not apply to calls on hold.
<b>RTP Hold Timeout</b>	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.
<b>RTP Keep-alive</b>	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.
<b>100rel</b>	Configure the 100rel setting on UCM630xA. The default setting is "Yes".
<b>Trust Remote Party ID</b>	Configure whether the Remote-Party-ID should be trusted. The default setting is "No".
<b>Send Remote Party ID</b>	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
<b>Generate In-Band Ringing</b>	Configure whether the UCM630xA should generate Inband ringing or not. The default setting is "Never".  <ul style="list-style-type: none"> <li>o <b>Yes:</b> The UCM630xA will send 180 Ringing followed by 183 Session Progress and in-band audio.</li> <li>o <b>No:</b> The UCM630xA 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.</li> <li>o <b>Never:</b> Whenever ringing occurs, the UCM630xA 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.</li> </ul>
<b>Server User Agent</b>	Configure the user agent string for the UCM630xA.
<b>Send Compact SIP Headers</b>	If enabled, compact SIP headers will be sent. The default setting is "No".
<b>Passthrough PAI Header</b>	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.



### STIR/SHAKEN

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

Add Authentication Number

SIP Settings/STIR/SHAKEN – Add Authentication Number Settings

<b>Authentication Number</b>	Configure the Authentication Number.
<b>Device Name</b>	Configure the device name.
<b>Credibility</b>	<p>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:</p> <ul style="list-style-type: none"> <li>○ <b>A (Full attestation)</b> – The carrier is associated with the caller and the number. There is high confidence that the CID has not been spoofed.</li> <li>○ <b>B (Partial attestation)</b> – The carrier is associated with the caller but not the number. There is uncertainty about whether the CID has been spoofed or not.</li> <li>○ <b>C (Gateway attestation)</b> – The carrier is not associated with the caller and has no confidence at all about the number. Generally used for traceback.</li> </ul>

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

Certificate Settings

SIP Settings/STIR/SHAKEN – Certificate Settings

<b>Certificate Download Time (s)</b>	Configure the public key download timeout period, the default value is 2 seconds.
<b>Signature Valid Time (s)</b>	Configure the validity period of the digital signature, the default value is 15 seconds.

<b>Private Key</b>	<p>Configure the Private key.</p> <p><b>Note:</b> 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".</p>
<b>Public Key</b>	<p>Configure the Public Key.</p> <p><b>Note:</b> 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".</p>

## Transparent Call-Info header

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

```

Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:3001@192.168.6.36:5064 SIP/2.0
Message Header
Via: SIP/2.0/UDP 192.168.6.187:5060;rport;branch=z9hG4bKpj3217e67b-e74f-4f9f-b06f-afd3dcbbe29b
From: "3002" <sip:3002@192.168.6.187>;tag=202dca4f-2b9d-4880-924c-d48cea7d0596
To: <sip:3001@192.168.6.36>
Contact: <sip:68aae6ea-f1d4-4e62-9987-446e718a2448@192.168.6.187:5060>
Call-ID: 7f66bb20-0b9f-4828-a355-698853b8d9fb
CSeq: 17559 INVITE
Allow: OPTIONS, INFO, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REGISTER, REFER
Supported: 100rel, timer, replaces, norefersub
Session-Expires: 1800
Min-SE: 90
Call-Info: <https://192.168.6.186:443/capture/8001> ;purpose=GDS-view
Max-Forwards: 70
User-Agent: Grandstream UCM6202V1.5A 1.0.13.15
Content-Type: application/sdp
Content-Length: 547
Message Body

```

*Transparent Call-Info*

## IAX SETTINGS

The UCM630xA IAX global settings can be accessed via Web GUI → **PBX Settings** → **IAX Settings**.

### IAX Settings/General

IAX Settings/General

<b>Bind Port</b>	Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569.
<b>Bind IPv4 Address</b>	Force IAX2 to bind to a specific address instead of all addresses.
<b>Bind IPv6 address</b>	Configure the IPv6 address to bind to. "[::]" means to bind to all IP addresses.
<b>IAX1 Compatibility</b>	Select to configure IAX1 compatibility. The default setting is "No".
<b>No Checksums</b>	If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this feature. The default setting is "No".
<b>Delay Reject</b>	If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is "No".
<b>ADSI</b>	Select to enable ADSI phone compatibility. The default setting is "No".
<b>Music On Hold Interpret</b>	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.

<b>Music On Hold Suggest</b>	Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold.
<b>Bandwidth</b>	Configure the bandwidth for IAX settings. The default setting is "Low".

## IAX Settings/Registration

### IAX Settings/Registration

<b>IAX Registration Options</b>	
<b>Min Reg Expire</b>	Configure the minimum period (in seconds) of registration. Default setting is 60.
<b>Max Reg Expire</b>	Configure the maximum period (in seconds) of registration. Default setting is 3600.
<b>IAX Thread Count</b>	Configure the number of IAX helper threads. The default setting is 10.
<b>IAX Max Thread Count</b>	Configure the maximum number of IAX threads allowed. The default is 100.
<b>Auto Kill</b>	If enabled and no ACK is received for new messages after the specified wait time, the connection will be terminated.
<b>Authentication Debugging</b>	If enabled, authentication traffic in debugging will not show. The default is "No".
<b>Codec Priority</b>	<p>Configure codec negotiation priority. The default setting is "Reqonly".</p> <ul style="list-style-type: none"> <li>○ <b>Caller</b> Consider the callers preferred order ahead of the host's.</li> <li>○ <b>Host</b> Consider the host's preferred order ahead of the caller's.</li> <li>○ <b>Disabled</b> Disable the consideration of codec preference all together.</li> <li>○ <b>Reqonly</b> 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.</li> </ul>
<b>Type of Service</b>	Configure ToS bit for preferred IP routing.
<b>IAX Trunk Options</b>	
<b>Trunk Frequency</b>	Configure the frequency of trunk frames (in milliseconds). The default is 20.
<b>Trunk Time Stamps</b>	If enabled, time stamps will be attached to trunk frames. The default is "No".

## IAX Settings/Security

### IAX Settings/Static Defense

<b>Call Token Optional</b>	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.
<b>Max Call Numbers</b>	Configure the maximum number of calls allowed for a single IP address.
<b>Max Unvalidated Call Numbers</b>	Configure the maximum number of Unvalidated calls for all IP addresses.
<b>Max Call Numbers</b>	Configure to limit the number of calls for a give IP address of IP range.

<b>IP or IP Range</b>	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 UCM630xA 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.

Edit Analog Ports: Signaling Preference
Cancel Update

Port 1: Loop Start ▼

Port 2: Loop Start ▼

*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 UCM630xA to automatically detect the ACIM value. The detecting value will be automatically filled into the settings.

### ACIM Setting

ACIM Detection: Detect

Detect Option: ERL ▼

Port 1:: 600 Ω ▼

Port 2:: 600 Ω ▼

*FXO Ports ACIM Settings*

### PBX Interface Settings

<b>Tone Region</b>	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)".
<b>Advanced Settings</b>	
<b>FXO Opermode</b>	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)".
<b>FXS Opermode</b>	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)".

<b>FXS TISS Override</b>	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.
<b>PCMA Override</b>	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.  <b>Note:</b>  This option requires system reboot to take effect.
<b>Boost Ringer</b>	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".
<b>Fast Ringer</b>	Configure to increase the ringing speed to 25HZ. This option can be used with "Low Power" option. The default setting is "Normal".
<b>Low Power</b>	Configure the peak voltage up to 50V during "Fast Ringer" operation. This option is used with "Fast Ringer". The default setting is "Normal".
<b>Ring Detect</b>	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".
<b>FXS MWI Mode</b>	Configure the type of Message Waiting Indicator on FXS lines. The default setting is "FSK".  <ul style="list-style-type: none"> <li>○ <b>FSK</b>: Frequency Shift Key Indicator</li> <li>○ <b>NEON</b>: Light Neon Bulb Indicator.</li> </ul>
<b>FXO Frequency Tolerance</b>	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.

The screenshot shows a web interface for configuring DAHDI settings. At the top, there's a header 'Interface Settings' with a sub-tab 'DAHDI Settings' selected. Below this, there are two settings, each with a red asterisk indicating they are required:

- \* Analog Buffers: A dropdown menu showing '32, half'.
- \* Fax Buffers Policy: A dropdown menu showing '32, half'.

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.

## CONTACTS

Address book management is under UCM web UI->Maintenance, and it has two sections "Contact Management" and "Department management".

### Contact Management

Contact management page displays extension contacts and external contacts information.

- Extension contacts

Extension contacts page shows all the extensions that has "Sync Contact" option enabled in extension settings page. The extension contacts here can be edited or deleted individually or in batch. No new extension contact can be added directly from this page. If an extension contact is deleted from this page, "Sync Contact" option is disabled from this extension. This will not delete the extension from UCM.

#### **Note**

"Delete" extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

EXTENSION	NAME	DEPARTMENT	EMAIL ADDRESSES	CONTACT PRIVILEGES	OPTIONS
1000		---		All Contacts(Same as Department)	
1001	John Doe	---		All Contacts(Same as Department)	
1002	Jane Doe	---		All Contacts(Same as Department)	
1003	Arthur Morgan	---		All Contacts(Same as Department)	
1004		---		All Contacts(Same as Department)	
1005		---		All Contacts(Same as Department)	
2000		---		All Contacts(Same as Department)	
2001		---		All Contacts(Same as Department)	
2002		---		All Contacts(Same as Department)	
2003		---		All Contacts(Same as Department)	

Extension Contacts

#### **Note**

"Delete" extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

Click Edit icon to configure name, department, email address and etc for each extension contact.

\* Extension:

First Name:

Last Name:

Department:

Job Title:

Email Address:

Mobile Phone Number:

Home Number:

Fax:

**Contact Privileges**

Same as Department

Contact Privileges:

\* Contact View:  [Add / Edit Privileges](#)

Privileges:

*Edit Extension Contact*

<b>Extension</b>	Displays extension number.
<b>First Name</b>	Configure first name for the extension contact.
<b>Last Name</b>	Configure last name for the extension contact.
<b>Department</b>	Select department for the extension contact. Department can be created in "Department Management" page.
<b>Department Title</b>	Configure the job title for the extension contact.
<b>Email Address</b>	Configure email address for the extension contact.
<b>Mobile Phone Number</b>	Configure mobile phone number for the extension contact.
<b>Home Number</b>	Configure home number for the extension contact
<b>Fax</b>	Configure Fax for the extension contact.
<b>Same as Department Contact Privileges</b>	When this option is enabled, the contact extension will inherit the same privilege as the department it belongs to.
<b>Contact View Privileges</b>	This option allows configuring privileges for the contact extension. <b>Note:</b> This option will be disabled if " <b>Same as Department Contact Privileges</b> " has been enabled.

- o External contacts

On external contacts page, the admin can create single external contact, import contacts in batch, edit contacts, delete contacts and export contacts.

Contact Management

Extension Contacts **External Contacts**

[+ Add](#) [Change Department](#) [Delete](#) [Import](#) [Export](#)  [Search](#)

<input type="checkbox"/>	MOBILE PHONE NUMBER	NAME	DEPARTMENT	EMAIL ADDRESSES	REMARK	OPTIONS
<input type="checkbox"/>	55555555	Sadie Adler	Sales	adler.s@mycompany.com		<a href="#">Edit</a> <a href="#">Delete</a>

[1](#) Total: 1 10 / page Goto 1

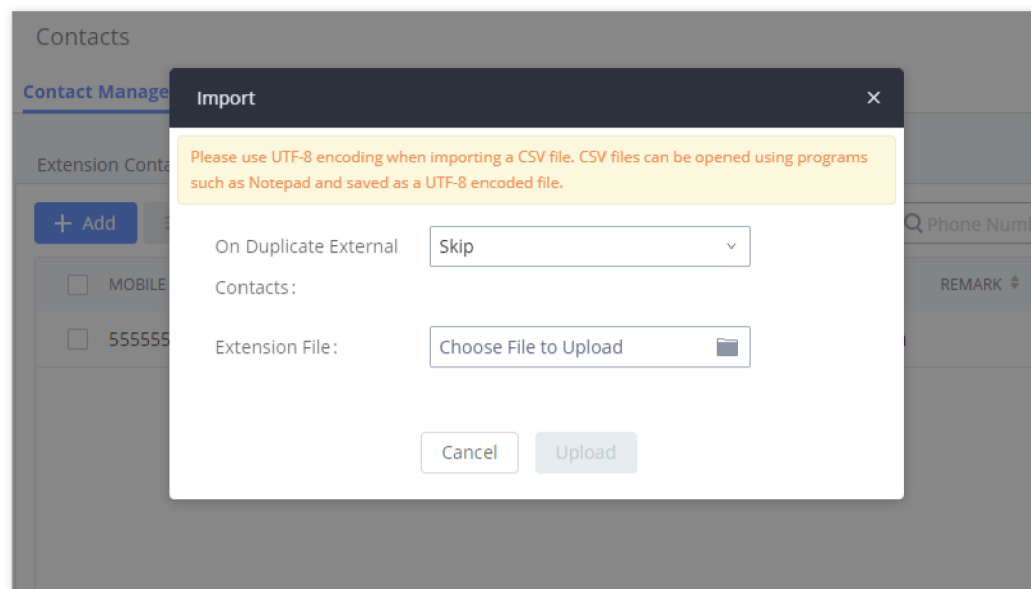
*External Contacts*

Click on "Export" icon, a CSV format file will be generated with the current external contacts.

Click on "import" icon, then follow the steps below to add external contacts in batch:

- o **Step 1:** For option "On Duplicate External Contacts", select whether to skip duplicate contact on the imported CSV file or update the duplicate UCM contact with the information in the CSV.

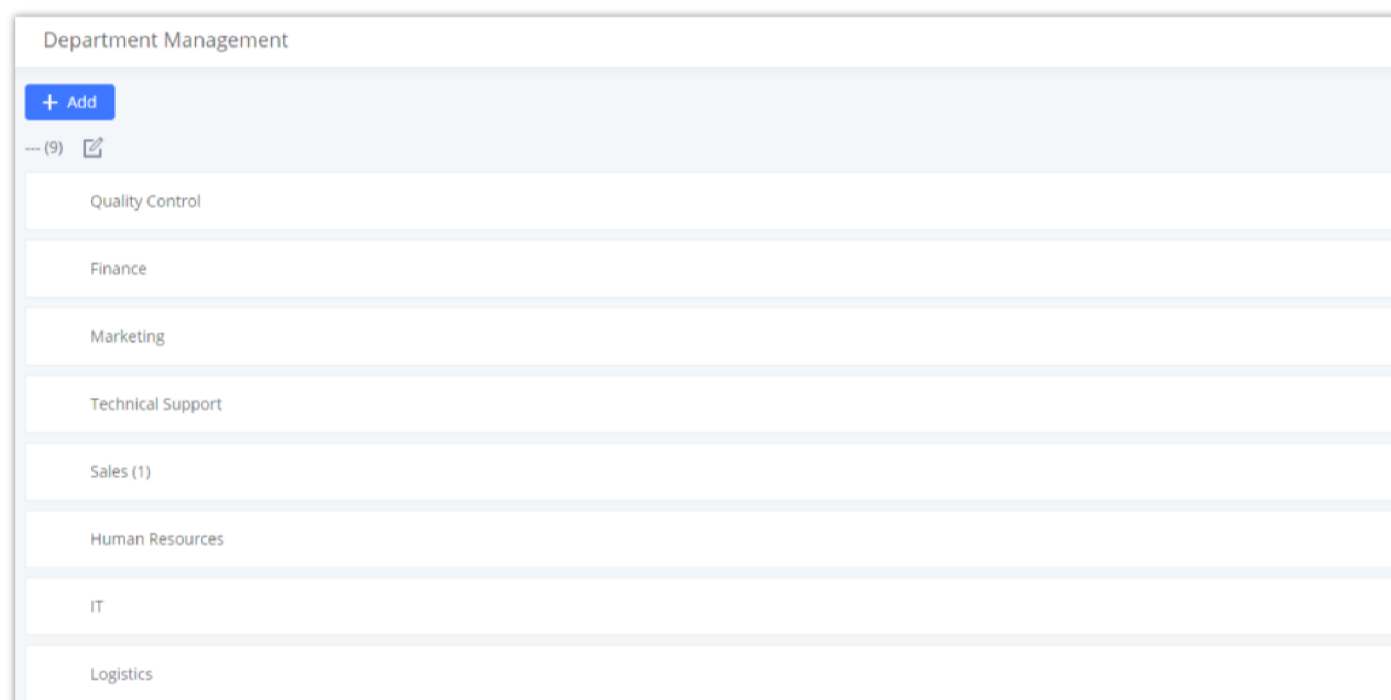
- **Step 2:** Choose file from local PC to upload.
- **Step 3:** Click on "Upload".
- **Step 4:** Click on "Apply" to complete importing external contacts.



*Import External Contacts*

## Department Management




Departments are organizational units that allows organizing extensions within groups that specify the specialty of a the extension owners within a company. This makes finding contacts easier within the UCM contact books.



*Department Management*

Click on "Add" to create a new department. Configure the department name and select the superior department. By default the superior department is the root directory. If the UCM has cloud IM configured, the root directory will be the department in cloud IM.

On the department list:

- Click on  to create sub department.
- Click on  to add member to the department.
- Click on  to edit the department.

*Edit Department*

<b>Department Name</b>	Enter the name of the department.
<b>Upper Level Department</b>	Select the upper level department if the department being created is a nested department.
<b>Contact View Privileges</b>	<ul style="list-style-type: none"> <li>• <b>All Contacts:</b> The extensions in this department will be able to see all the contacts.</li> <li>• <b>Department &amp; Sub-department Contacts:</b> The extensions in this department will only be able to see the contacts which are in the same department or in sub-departments.</li> </ul>
<b>Set as Shared Department</b>	Enable this option to share this department across the UCMs which use the same Cloud IM server. To be able to enable this option, make sure that the UCM has a RemoteConnect Plan and is correctly connected to the Cloud IM server.
<b>Share to Following Sites</b>	Pick the sites to which you want to share this specific department.

**Note**

The user can create up to 100 departments with up to 4 levels of nested departments.

**Important**

To be able to use shared department, the UCM devices will have to be subscribed to a RemoteConnect plan that offers Cloud IM service. For more information please refer to: <https://ucmrc.gdms.cloud/plans>

## Privilege Management

The user can configure custom privileges other than the default ones (All contacts, Departments and sub-departments contacts). These custom privileges allow more flexible ways of allowing contacts to view all or specific contacts from other departments.

UCM admin can add or edit Privilege Management; under UCM web UI → **Contacts Privilege Management**, there are 2 default privileges:

- Visible to all contacts.
- Only the contact person's department and sub-department contacts are visible.

When Cloud IM is enabled on the UCM, a third privilege becomes available to choose:

- Local Contacts: Restricts the contacts shown to the contacts of the local UCM.

Privilege Management		
NAME	PRIVILEGE STATUS	OPTIONS
All Contacts	<span style="color: green;">●</span> In Use	
Department & Sub-Department Contacts	<span style="color: grey;">●</span> Not Applied	

Total: 2    10 / page    Goto 1

Privilege Management — Cloud IM Disabled

## MESSAGING

### Live Chat

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

**Live Chat > Create New Live Chat**

\* Name

\* Destination Extension

Web Page Language Use Browser Language

**Visitor Information**


Require Visitor Info

Privacy Control

**Call Settings**

Allow Visitor to Call

**Customer Service Agent Information**

Avatar   
Please select a file in png, jpg, jpeg format.

\* Name

Show Agent's Real Name

Live Chat Configuration

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

### Message Broadcast

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

**Message Broadcast > Send Message Broadcast**

\* Name

\* Sender

\* Message Content

\* Recipients

Selected(0)
 

- Company Contact
- All
- Technical Support
- Quality Control
- Sales
- IT
- Marketing
- Human Resources
- Finance
- 1000 " "

© 2023 Grandstream Networks, Inc.

*Message Broadcast Configuration*

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

## DEVICE MANAGEMENT

### IPC Devices

The UCM admin can add IPC devices and edit accessible extensions so these extensions can view the surveillance streams for the IPC devices.

Click on "Add" to add IPC device.

IP Camera Devices					
<input type="button" value="+ Add"/> <input type="button" value="Edit Allowed Members"/> <input type="button" value="Delete"/> <input type="button" value="Import"/> <input type="button" value="Export"/>					
<input type="checkbox"/> STATUS	DEVICE NUMBER	DEVICE NAME	URL	OPTIONS	
<input type="checkbox"/> ● Unmonitored	4001	GSC3620	rtsp://192.168.5.74:554	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1  Total: 1 10 / page  1

*IP Camera Devices*

Edit the IPC device settings in the table below.

<b>Device Number</b>	The number that allowed members can dial to access the IP camera.
<b>Device Name</b>	Enter the name that you want to allocate for the device.
<b>Protocol</b>	The media control protocol used. <ul style="list-style-type: none"> <li>● RTSP</li> </ul>
<b>IP Address</b>	Enter the IP address of the IP camera.
<b>Port</b>	Enter the port of the IP camera. The default is 554
<b>Channel Path</b>	If you want to view the stream of the specified channel, please configure the path of this stream.
<b>Username</b>	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
<b>Password</b>	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
<b>Transmission Protocol</b>	Transport protocol of the IP camera. Default is UDP.
<b>Heartbeat Detection</b>	If enabled, the PBX will regularly send RTSP OPTIONS to check of the device is still online.
<b>Allowed Members</b>	Extensions, Extension Groups, and Departments can be selected to access this IP camera by dialling the configured Device Number.

Create New IP Camera Devices
Cancel Save

**General**

\* Device Number:

\* Device Name:

\* Protocol:

\* IP Address:

\* Port:

Channel Path:

Username:

Password:

\* Transmission Protocol:

Heartbeat Detection:

**User Settings**

\* Allowed Members:

Company Contact

- All
- 1005
- 2004
- 2003

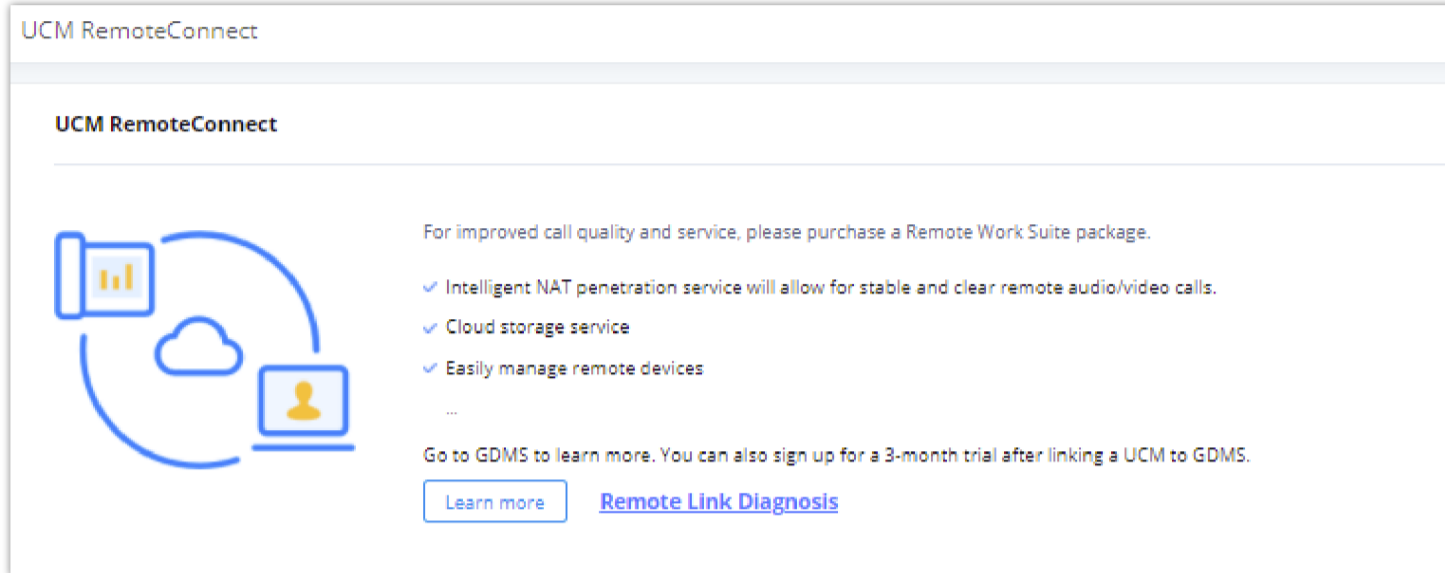
Selected(0)

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

# 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 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.

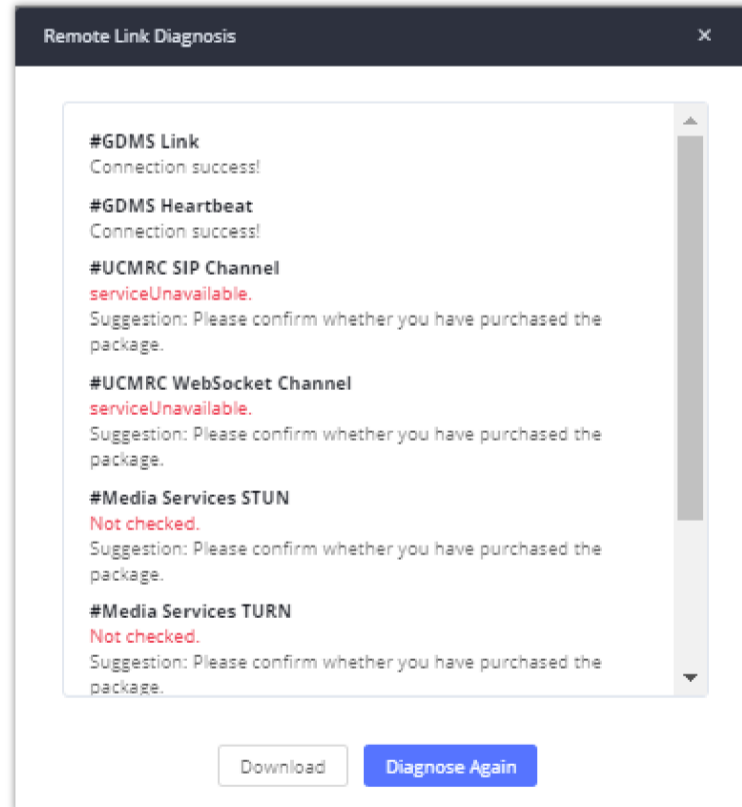
The RemoteConnect can be configured under **WebGUI→RemoteConnect** After purchasing the RemoteConnect package.



*RemoteConnect Features*

On GDMS platform, sign in and go to Device→PBX Device page, click on "Add Device" to add your UCM6300A device to GDMS system, once done an open beta plan will be assigned to the UCM.

In daily operation, the user can click the "Diagnosis" button to diagnose the remote service system. The specific diagnosis content includes media service (STUN/TURN), GDMS link and heartbeat detection, tunnel service (SIP/Web Socket), Cloud IM, UCM bandwidth speed measurement.



*Remote Diagnosis*






## RemoteConnect

**Plan**

Plan Settings

Integrated Customer Service

Enterprise UI customization

Subscription Tier:	Basic 
Subscription Period:	Permanently Active
Plan Status:	Permanently Active
Max Remote Concurrent Sessions:	2
Max Remote Users:	10
Max Time Per Remote Call/Meeting:	20 minute(s)
Max Cumulative Time for Remote Calls/Meetings Per Day:	120 minute(s)
Max Cumulative Time for Remote Calls/Meetings Per Month:	Unlimited
GDMS Cloud Storage:	0 GB <a href="#">Upgrade</a>
STUN Address:	nat-b.gdms.cloud
Wave RemoteConnect Address:	 a.gdms.cloud 
IP Endpoint/Trunk RemoteConnect Address:	 a.gdms.cloud:5061 
Wave 3rd Party Plug-ins:	Not supported by the current plan

UCM RemoteConnect – Plan

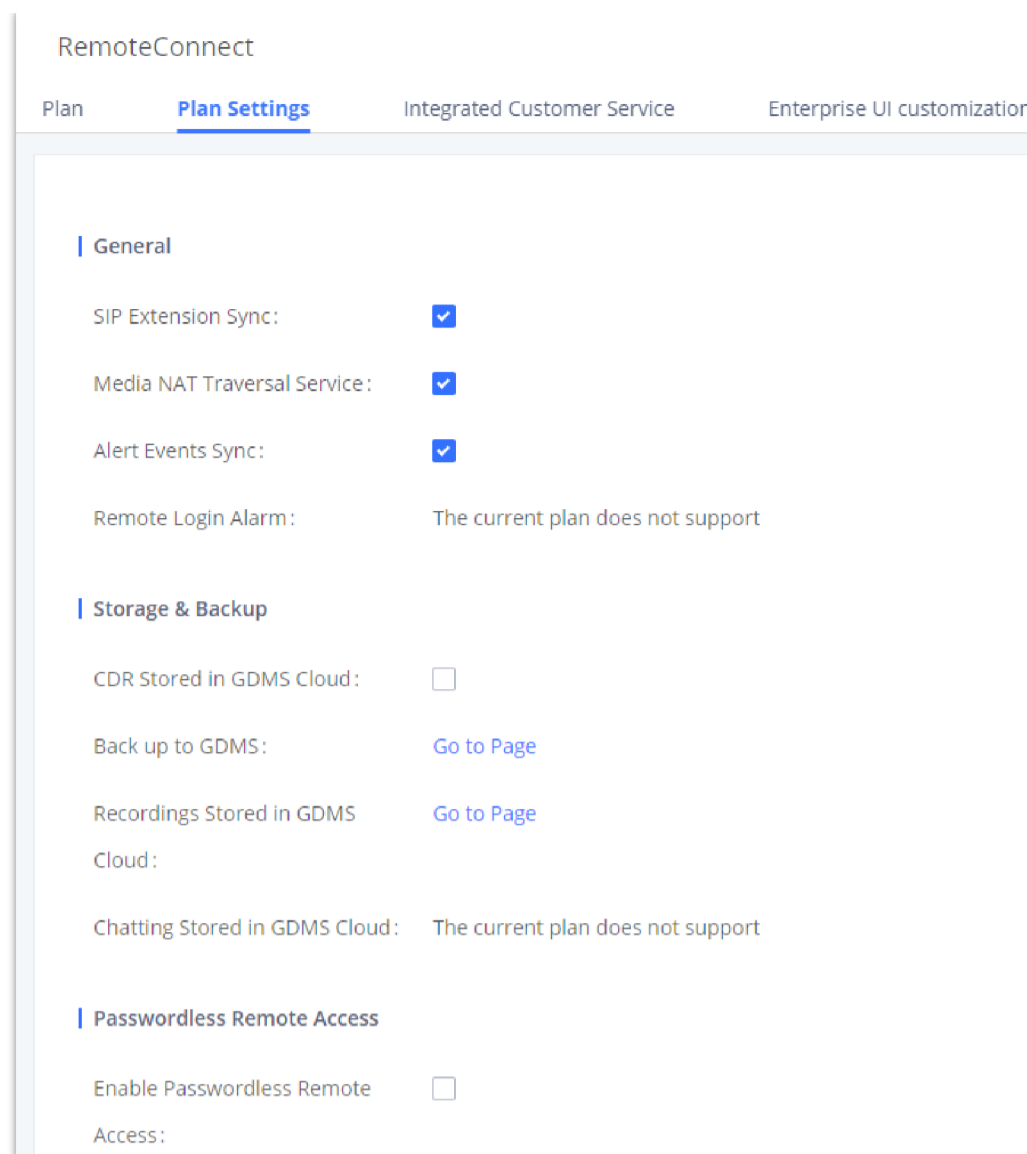
### Note

- 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.

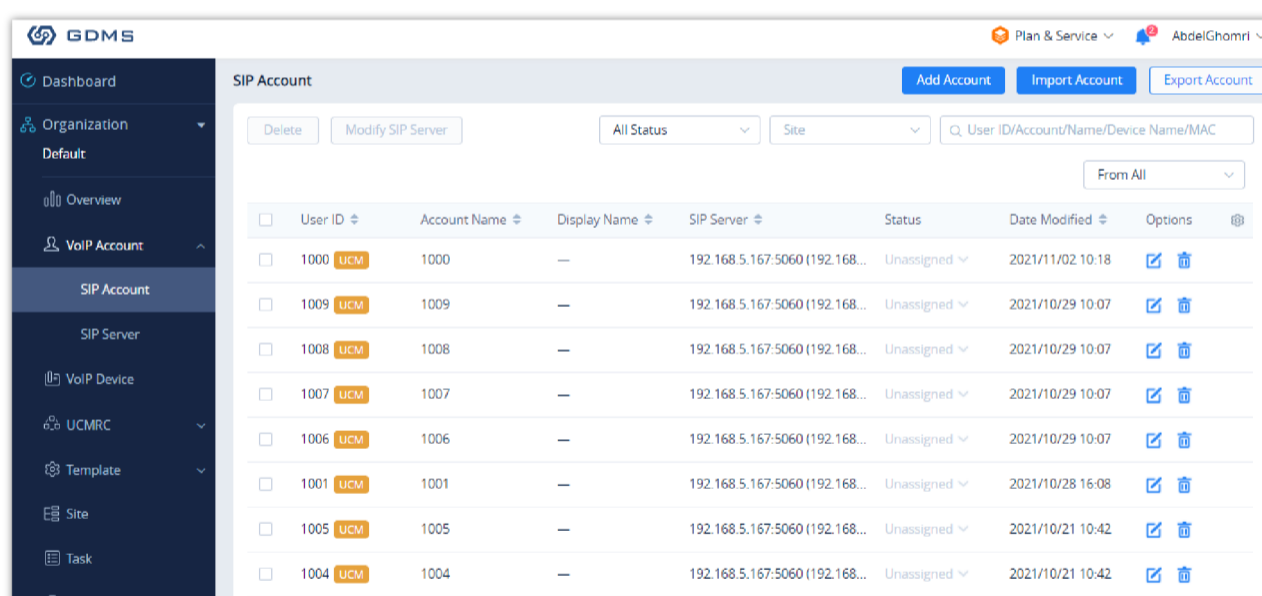
The settings are under UCM **webGUI**→**Value-added Services**→**UCM RemoteConnect**→**Plan Settings**.



UCM RemoteConnect Plan Settings

After adding UCM to the GDMS platform, UCM will synchronize all SIP extensions to the GDMS platform, this allows to use the GDMS platform for account allocation and terminal management.

The accounts synchronized to GDMS platform can be viewed on the GDMS-> VoIP Account->SIP Account page. As shown in the figure below:



UCM SIP Extensions synchronized to GDMS

The Media NAT Traversal provides a fully automatic intelligent external network penetration service to ensure that you can make normal calls/conferences on the external network.

CDR data cloud storage provides a service of dumping to GDMS to prevent CDR from continuously increasing occupying UCM storage space.

Alarm event synchronization is to synchronize the alarm information generated on UCM to the GDMS server.

UCM supports GDMS passwordless remote access. When this button is checked, GDMS remote access UCM does not need to enter the account password, and no login is required.

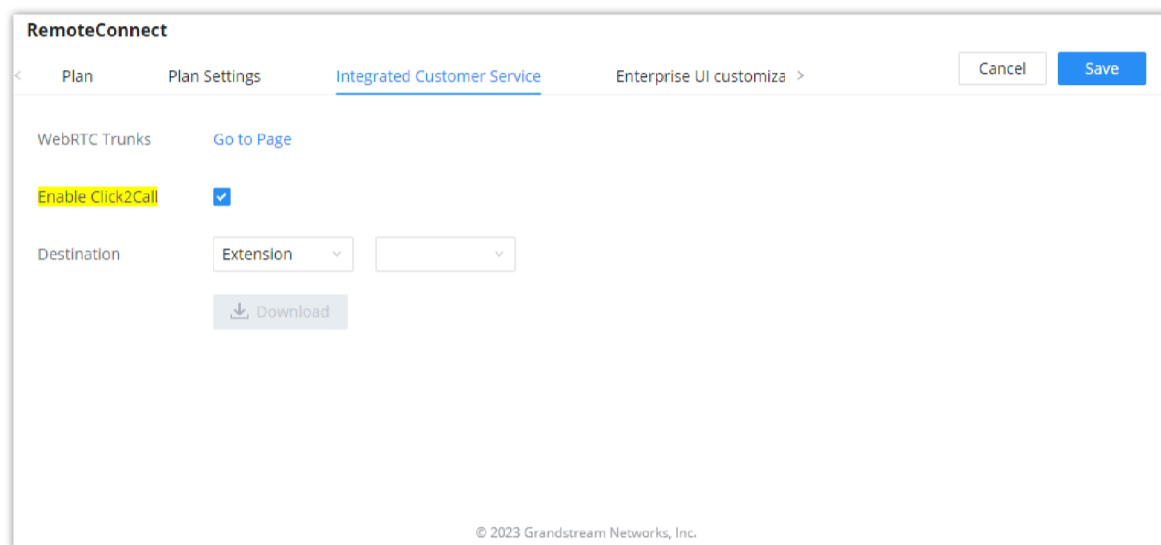
Allow the administrator/super administrator to open it. After clicking on open with an account, the subsequent passwordless login will use the account. All administrators and super administrators can see whether this UCM is enabled.

Super administrators can check and uncheck all the exemption lists; administrators can check and uncheck the exemption status of this account, and the corresponding account exemption access function will be closed after cancellation.

- Deleting an account on GDMS only removes the association between the account and the device, and does not delete the SIP account information on UCM.
- Any creation, deletion or modification of the SIP account on UCM will be automatically synchronized to the GDMS cloud platform.
- After checking the "Media NAT traversal service", the TURN service and other related traversal settings set by the user will not take effect.

## Integrated Customer Service

To configure the Integrated Customer Service SDK, go to the **RemoteConnect → Integrated Customer Service** page that allows users to download the SDK provided by the customer service system and integrate it on the website, so that the website can contact customer service for call operations. The call queue is used as the customer service number.



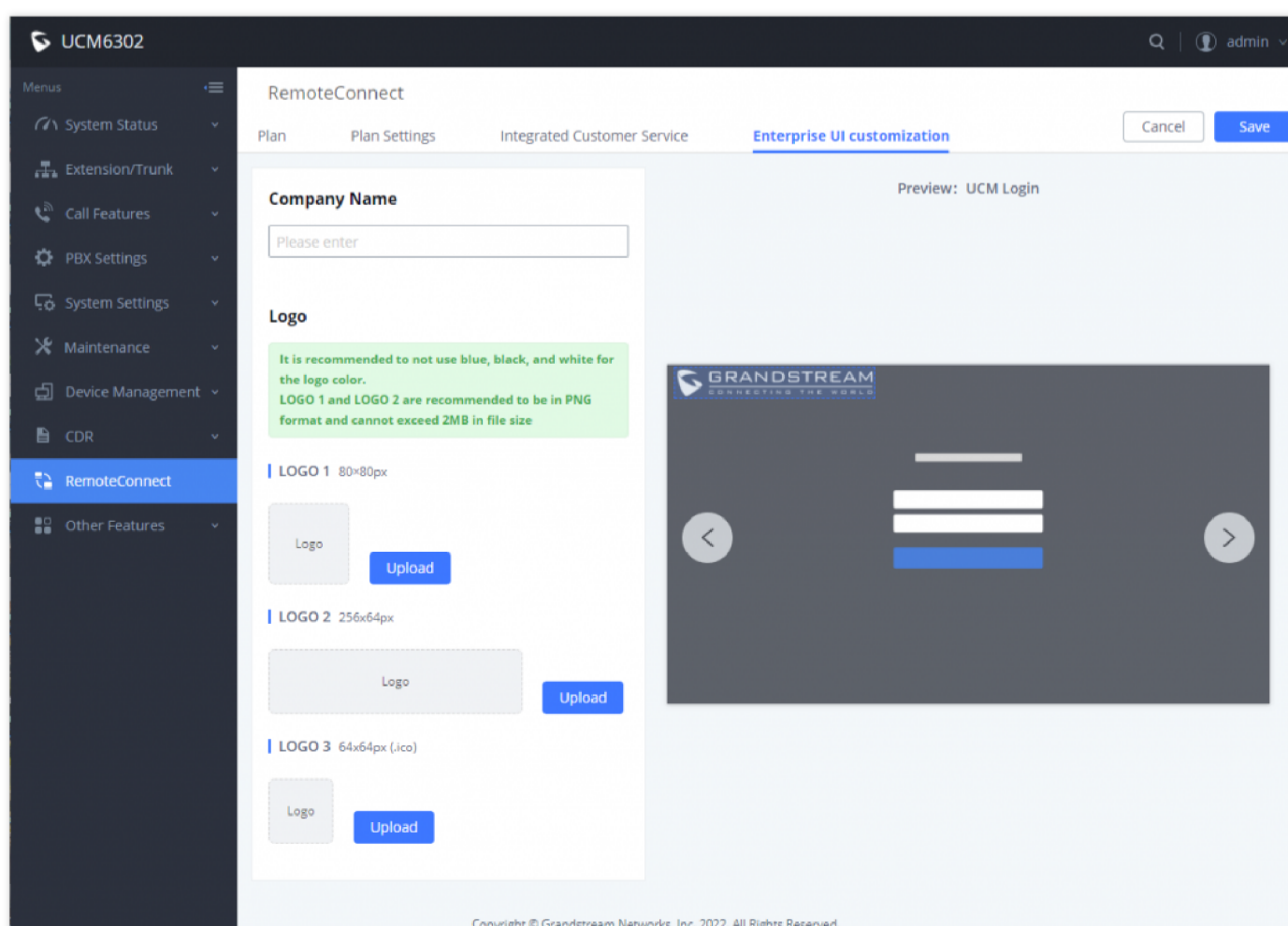
*Integrated Customer Service interface*

Enabling Click2Call will allow users to initiate a direct call from the web browser by clicking on the call button embedded on the website graphical interface. The calls initiated can be directed to call queues or a specific extension.

## Enterprise UI Customization

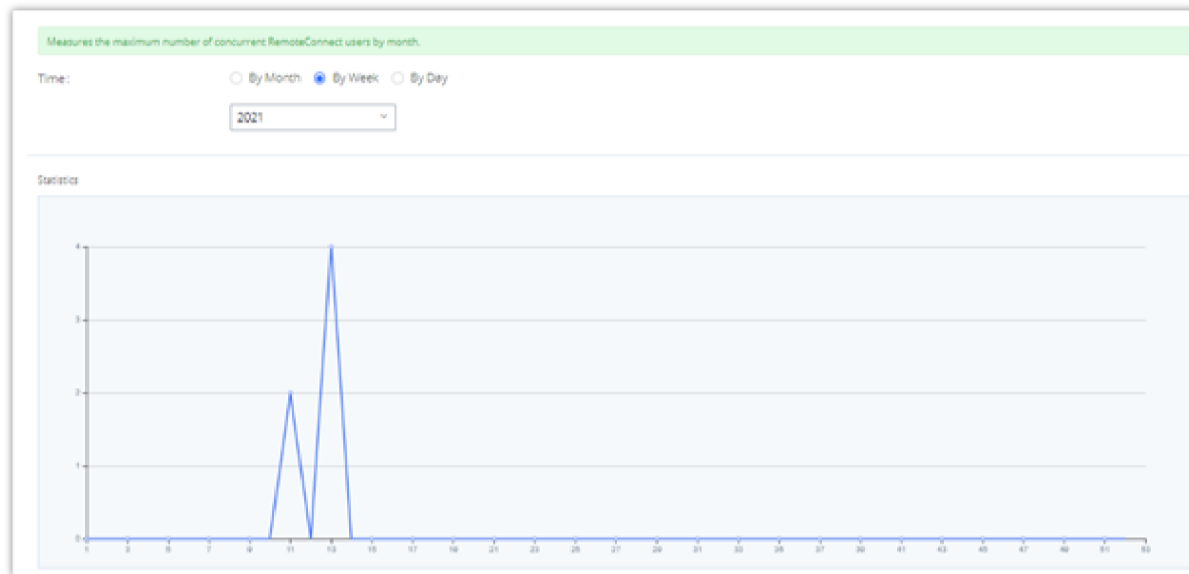
With a remote connect plan, on the value-added service → UCM RemoteConnect → UI Customization page, users can edit the company name and select a local image file as the new logo. The company name acts on the text part with the trend logo, and the pictures are in different formats and sizes according to the logo position, which are 64\*64px (only ico format is supported), 256\*256px, 80\*80px, which supports users in the "UCM management platform/login" "", "Reset Password", "Email Template", "Wave\_PC", "Wave Login", "Browser Label", "Guide Page" 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.



## 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 → **RemoteConnect** → **Statistics** page.

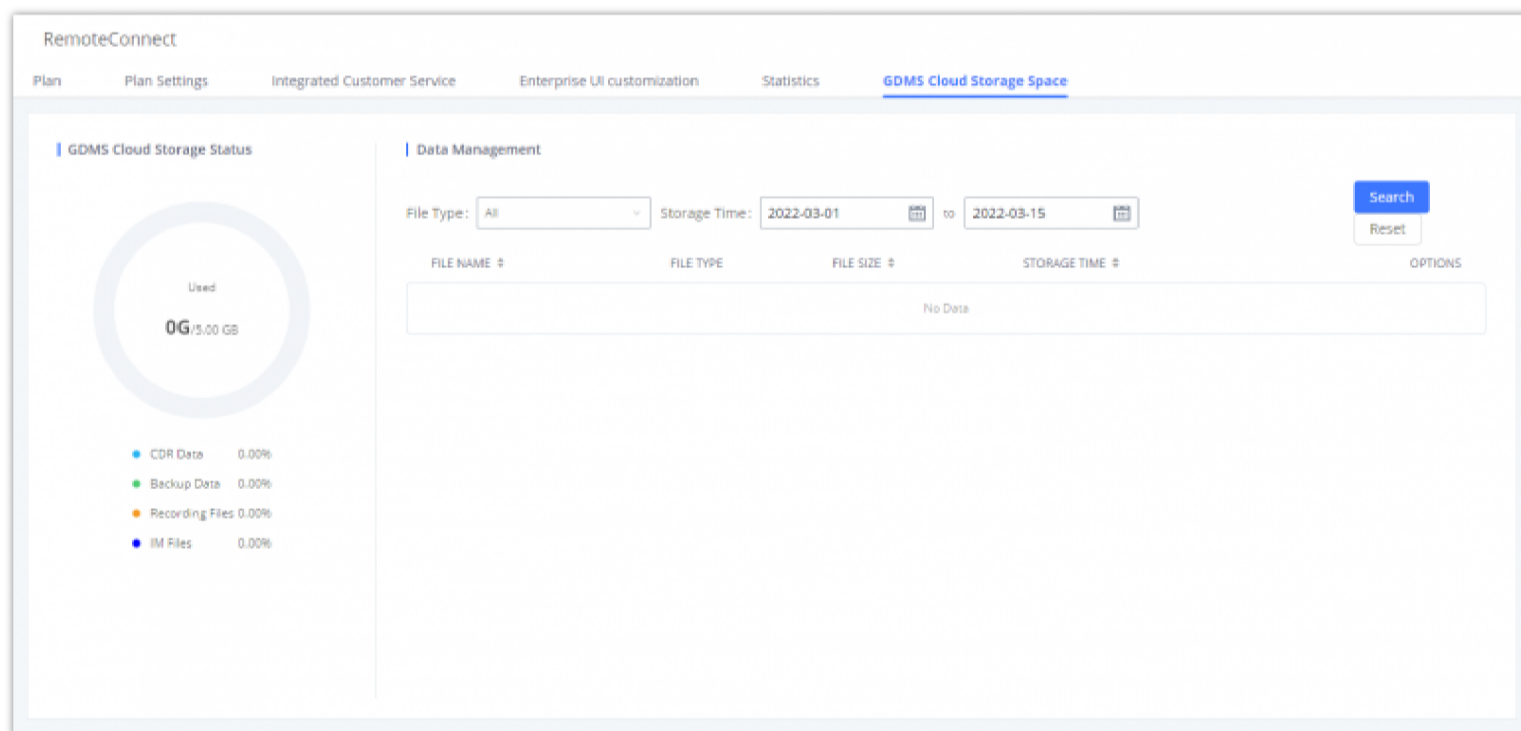


Concurrent Remote Calls

For more information, please visit <http://ucmrc.gdms.cloud/intro.html> and read our [UCM63XXA RemoteConnect guides](#)

## GDMS Cloud Storage Space

GDMS Cloud Storage Space feature on the UCM630x offers an overview about how you are using the storage space offered by RemoteConnect. It displays the amount of storage occupied, the amount of free space, also the percentage taken by each type of files. The type of files displayed are the following: CDR Data, Backup Data, Recording Files, and IM Files.



GDMS Cloud Storage Space

## API CONFIGURATION

The UCM630xA 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 UCM630xA first under **Integrations** → **API Configuration**. The API configuration parameters are listed in the table below.

**Note:** The old version of the API interface only supports cdrapi, recapi and pmsapi functions, and will be removed, please use the new HTTPS API instead.

#### Configuration Parameters (New)

HTTPS API Settings (New)	
<b>Enable</b>	Enable/Disable API. The default setting is enable.
<b>Username</b>	Configure the username for API Authentication.
<b>Password</b>	Configure the password for API Authentication.
<b>Call Control</b>	If enabled, 3 <sup>rd</sup> party applications will be able to manage inbound calls via API actions. <b>acceptCall</b> will accept incoming calls while <b>refuseCall</b> will reject them. If no actions are done within 10 seconds, calls will automatically be accepted.
<b>Permitted IP (s)</b>	Sets an IP address Access Control List (ACL) for addresses that are allowed to authenticate as this user. By default this is not set, meaning all IP addresses will be allowed. The format is: "xxx.xxx.xxx.xxx/255.255.255.255".

#### Configuration Parameters (Old)

HTTPS API Settings (Old)	
<b>Basic Settings</b>	
<b>Enable</b>	Enable/Disable API. The default setting is disabled.
<b>TLS Bind Address</b>	Configure the IP address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 8443. The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.  The default setting is 0.0.0.0:8443.
<b>Username</b>	Configure the username for TLS authentication.
<b>Password</b>	Configure the password for TLS authentication.
<b>Permitted IP(s)</b>	Specify a list of IP addresses permitted to use the API. This creates an API-specific access control list. Multiple entries are allowed.  For example, "192.168.40.3/255.255.255.255" denies access from all IP addresses except 192.168.40.3.  By default, this is blank, which indicates that no IP addresses are allowed to use this API.
<b>Other Settings</b>	
<b>TLS Private Key</b>	Upload TLS private key. The size of the key file must be under 2MB. This file will be renamed as 'private.pem' automatically.
<b>TLS Cert</b>	Upload TLS cert. The size of the certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection. This file will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.
<b>API Module</b>	
<b>CDR API</b>	Enable/disable CDR API module.
<b>REC API</b>	Enable/disable REC API module.
<b>PMS API</b>	Enable/disable PMS API module.

For more details on CDR API (Access to Call Detail Records), REC API (Access to Call Recording Files) and PMS API, please refer the document in the link here:

- <https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>

- o <https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>
- o [PMS API](#)

## API Queries Supported

The new API supports the queries listed below which will accomplish certain requests and get data about different modules on UCM630xA.

### 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
cleanTerminalChatInformation
getSIPAccountQR
getCallQueuesMemberMessage
getQueueCalling

#### API Configuration Parameters

<b>CDR Real-time Output Settings</b>	
<b>Enable</b>	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.
<b>Server Address</b>	CDR server IP address
<b>Port</b>	CDR server IP port
<b>Upload Prompts User Configuration</b>	
<b>Username</b>	Username used to upload prompts.
<b>Password</b>	Password used to upload prompts.

## Upload Voice Prompt via API

Customers now can use the "Upload Prompts User Configuration" to upload/replace voice prompt files as an alternative method to the manual upload method on UCM **PBX Settings** → **Voice Prompt** → **Custom Prompt**.

The workflow of the prompt file upload goes as:

An HTTP/HTTPS request is sent to the UCM to upload/replace a voice prompt file, the request should include authentication details to the UCM and the name of the file to be uploaded. Then the UCM will contact an FTP server that should be hosted on the same IP address of the HTTP/HTTPS requester and download the prompt file from the FTP server.

The steps and conditions to upload the voice prompt via API are listed below:

1. Configure the prompt User under **Integrations** → **API Configuration** → **Upload Prompts User Configuration**. By default, the username and password for voice prompt user are "Username: uploader; Password: uploader123".

API Configuration

HTTPS API Settings(New)    CDR Real-time Output Settings    **Upload Prompts User Configuration**    Cancel    Save

| Upload Prompts User Configuration

\* Username:

\* Password:

Upload Prompt User Configuration

1. Hash the password of the user configured to an MD5 Encryption format.
2. 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.
3. 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
```

1. 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.

## CTI SERVER

UCM does support CTI server capabilities which are designed to be a part of the CTI solution suite provided by Grandstream, including GXP21XX and GXP17XX enterprise IP phones along with GS Affinity app.

Mainly the UCM will by default listening on port TCP 8888 for the connections from GS affinity application in order to interact, modify and serve data requests by the application which includes setting call features for the connected extension as call forward and DND.

Users can change the listening port under the menu page, **Integrations → CTI Server** as shown on below screenshot:

CTI Server    Cancel    Save

\* Port:

CTI Server Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link:

<https://documentation.grandstream.com/knowledge-base/gs-affinity-user-guide/>

# ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)

The UCM630xA 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 UCM630xA **Integrations** → **AMI**. For details on how to use AMI on UCM630xA, please refer to the following AMI guide:

<https://documentation.grandstream.com/knowledge-base/ami-asterisk-management-interface/>

## Warning

Please do not enable AMI on the UCM630xA 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 UCM630xA system. Please be cautious when enabling AMI access on the UCM630xA and restrict the permission granted to the AMI user. By using AMI on UCM630xA 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 UCM630xA 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.

### Sugar CRM

Configuration page of the SugarCRM can be accessed via admin login, on the **Integrations** → **CRM**.

CRM

CRM System: SugarCRM

\* CRM Server Address: https://exasandbox.sugaropencloud.eu

\* Add Unknown Number: Leads

Contact Lookups:

1 item Available

Look up in Accounts table

2 items Selected

Look up in Contacts table



Look up in Leads table

Sugar CRM Basic Settings

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

### Sugar CRM Settings

<b>CRM System</b>	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
<b>CRM Server Address</b>	Enter the IP address of the CRM server.

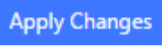
<b>Add Unknown Number</b>	Add the new number to this module if it cannot be found in the selected module.
<b>Contact Lookups</b>	Select from the " <b>Available</b> " list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Once settings on admin access are configured:

1. Click on



and



2. Logout from admin access.

3. 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



and



. The status will change from "Logged Out" to "Logged In". User can start then using SugarCRM features.

CRM User Settings

---

Enable CRM:

\* Username:

\* Password:

Login Status:

CRM User Settings

## Vtiger CRM

Configuration page of the VtigerCRM can be accessed via admin login, on the **Integrations → CRM**.

CRM

CRM System :

\* CRM Server Address:

\* Add Unknown Number:

Contact Lookups:

<input type="checkbox"/> 0 item Available	<input type="checkbox"/> 3 items Selected
None	<input type="checkbox"/> Look up in Organizatio... <input type="checkbox"/> Look up in Leads table <input type="checkbox"/> Look up in Contacts ta...

Vtiger CRM Basic Settings

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

#### Vtiger CRM Settings

<b>CRM System</b>	Select a CRM system from the dropdown menu, four CRM systems are available: Sugar CRM, Vtiger CRM, Zoho CRM (v2), Salesforce and ACT! CRM.
<b>CRM Server Address</b>	Enter the IP address of the CRM server.
<b>Add Unknown Number</b>	Add the new number to this module if it cannot be found in the selected module.
<b>Contact Lookups</b>	<p>Select from the "<b>Available</b>" list of lookups and press</p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p>to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.</p>

Once settings on admin access are configured:

1. Click on

Save

and

Apply Changes

2. Logout from admin access.

3. 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.

CRM User Settings

Enable CRM:

\* Username:

\* Password:

Login Status:

CRM User Settings

## Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI **Integrations → CRM**.

CRM

CRM System:

\* Add Unknown Number:

Contact Lookups:

1 item	Available	2 items	Selected
<input type="checkbox"/>	Look up in Leads table	<input type="checkbox"/>	Look up in Contacts table
		<input type="checkbox"/>	Look up in Accounts table

Salesforce Basic Settings

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

Once settings are configured:

2. Click on  and .
3. Logout from admin access.
4. Login to the UCM as user and navigate under "**User Portal → Other Features → CRM User Settings**".

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

CRM User Settings

Enable CRM:

\* Username:

\* Password:

\* Security Token:

Login Status:

Salesforce User Settings



## Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI **Integrations → CRM**.

Salesforce Basic Settings

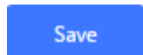
1. Select "Salesforce" from the CRM System Dropdown in order to use Salesforce CRM.

### Salesforce Settings

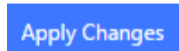
<b>CRM System</b>	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
<b>Add Unknown Number</b>	Add the new number to this module if it cannot be found in the selected module.
<b>Contact Lookups</b>	Select from the " <b>Available</b> " list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Once settings are configured:

1. Click on



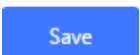
and



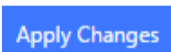
2. Logout from admin access.

3. 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



and



. The status will change from "Logged Out" to "Logged In". User can start then using Salesforce CRM features.

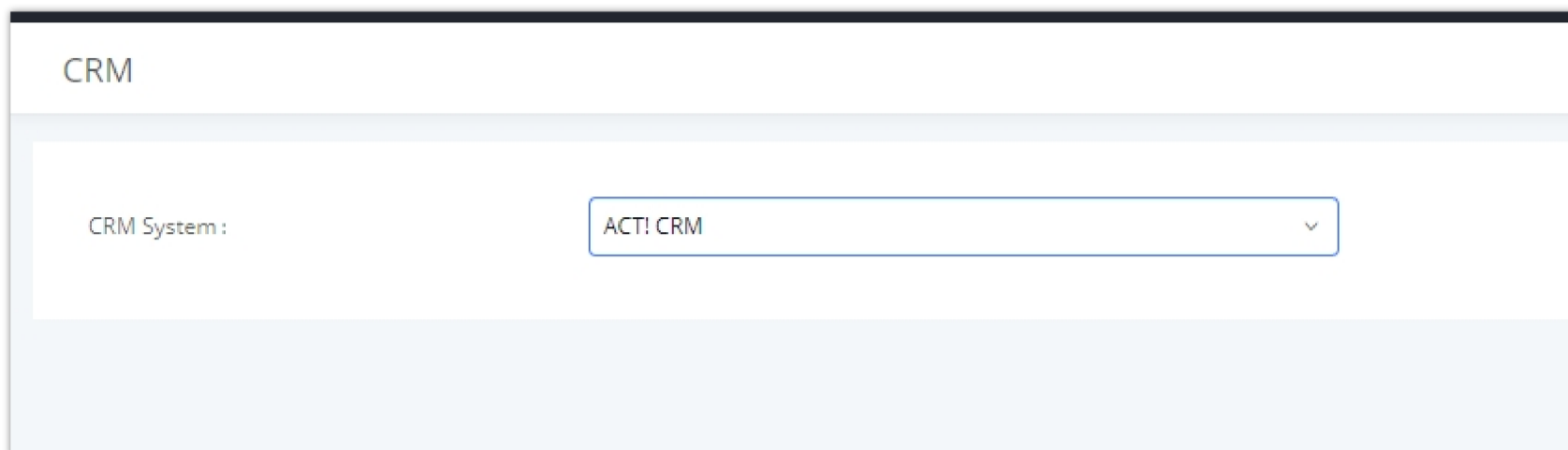
Salesforce User Settings

## ACT! CRM

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

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

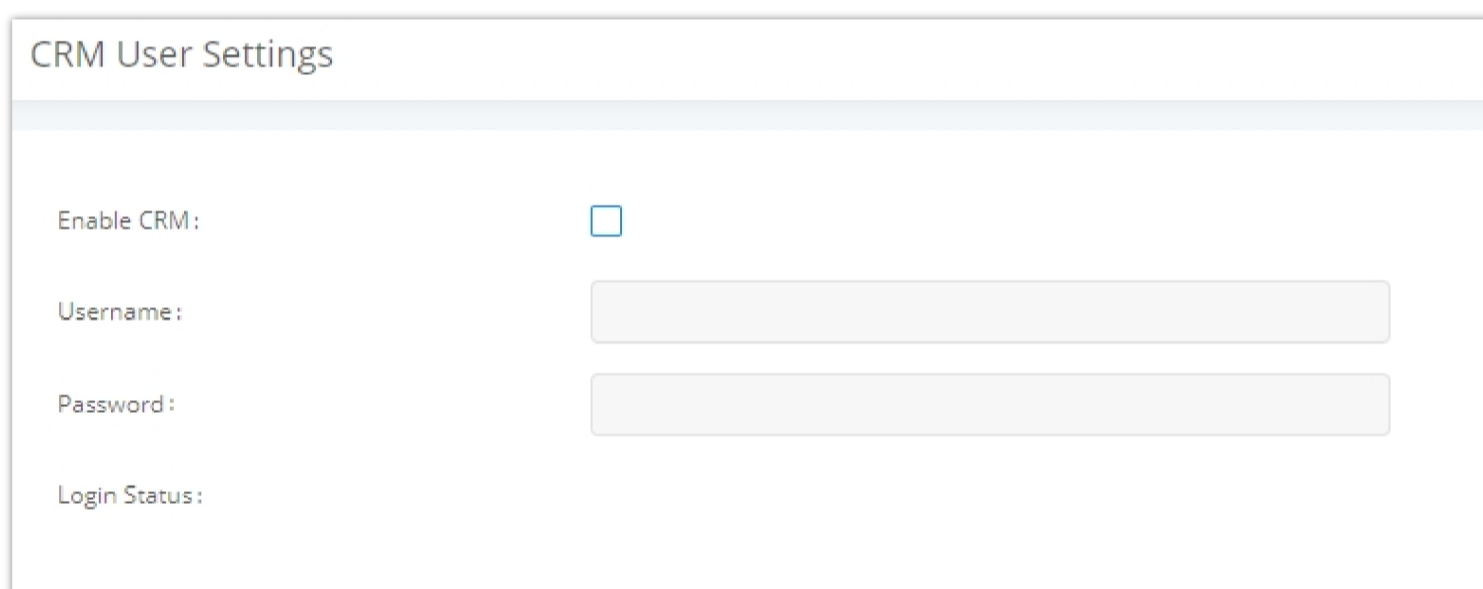
1. Navigate to **Integrations → CRM** and select the "ACT! CRM" option.



The screenshot shows a web interface titled "CRM". Below the title, there is a label "CRM System:" followed by a dropdown menu. The dropdown menu is open, and "ACT! CRM" is selected. The rest of the page is blank.

*Enabling ACT! CRM*

2. Log into the UCM as a regular user and navigate to **Other 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://www.act.com/>



The screenshot shows a web interface titled "CRM User Settings". Below the title, there is a label "Enable CRM:" followed by an unchecked checkbox. Below this, there are two input fields: "Username:" and "Password:". The "Login Status:" label is visible at the bottom but has no corresponding input field.

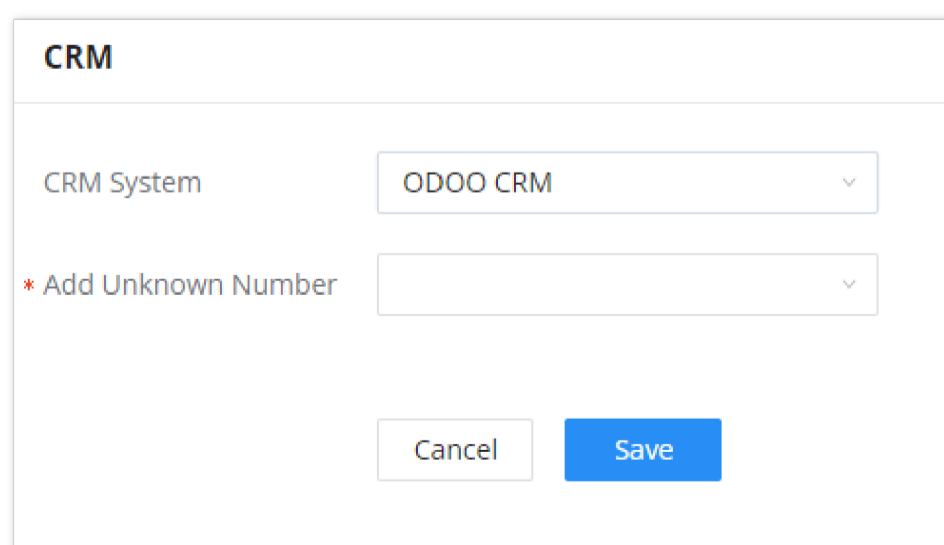
*Enabling CRM on the User Portal*

### **i** Note

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

## Odoo CRM

The UCM6300 Series supports integration with Odoo CRM. To enable Odoo CRM, please access the UCM's web UI then navigate to **Integration > CRM**.



The screenshot shows a web interface titled "CRM". Below the title, there is a label "CRM System" followed by a dropdown menu. The dropdown menu is open, and "ODOO CRM" is selected. Below this, there is a label "\* Add Unknown Number" followed by a dropdown menu. At the bottom, there are two buttons: "Cancel" and "Save".

*Odoo CRM*

Click "Save" then "Apply Changes".

Once Odoo CRM is enabled, the user can log into the user portal by access the UCM web UI and entering their username and password, then they can navigate to **Other Features > CRM User Settings**, then they configure their account using username and password created on Odoo platform.

### CRM User Settings

Enable CRM

\* Username   
This field is required

\* Password   
This field is required

\* Database   
This field is required

\* URL   
This field is required

Login Status

CRM User Settings

## PMS INTEGRATION

UCM630xA 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→**Integrations**→**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:

### PMS Supported Features

Feature	Mitel	char pmslink	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	✗	✗	✓	✗

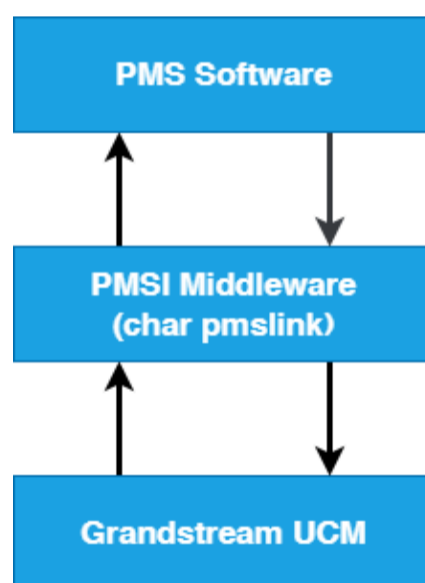
## Char PMSLink

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 char pmslink 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 (char pmslink) acting as interface between both parties.



UCM & PMS Interaction (char pmslink)

## 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

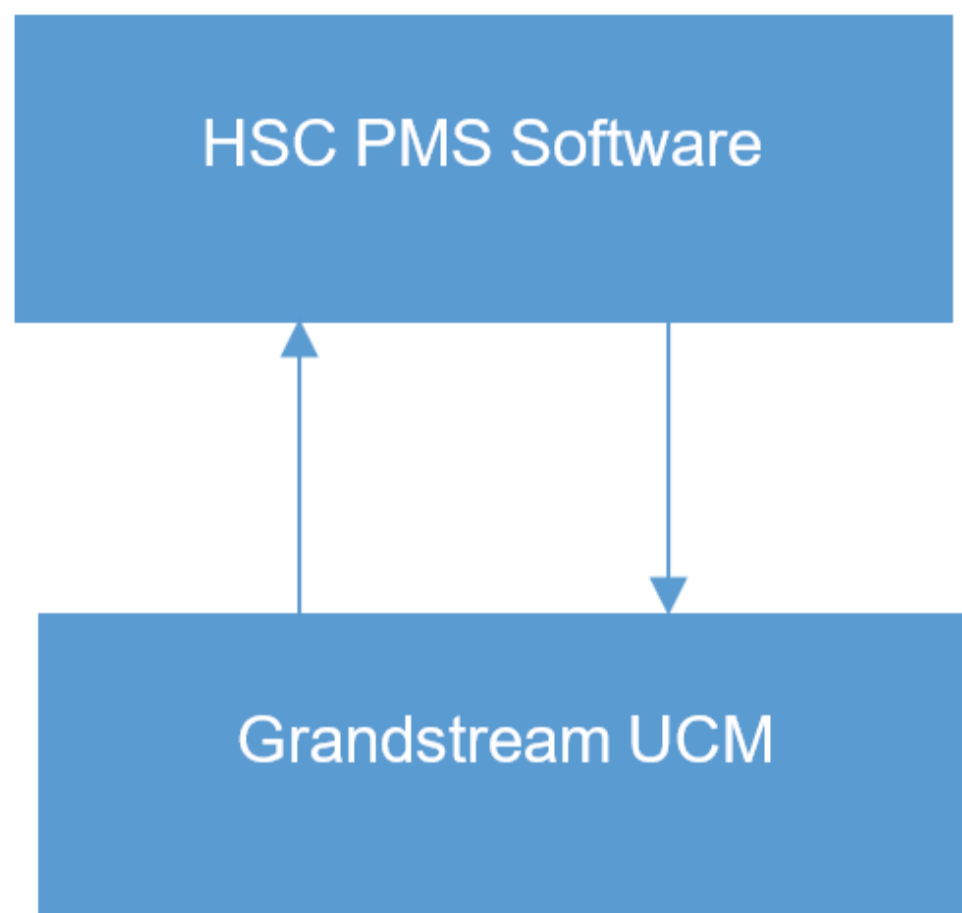
**Notes:**

1. Added support for receiving HTTP GET keep-alive messages from HSC PMS. This will allow the PMS to be aware of its connection to the UCM and take the appropriate actions such as raising alarms, sending notifications, etc.
2. Added support for HTTP GET requests from HSC PMS to retrieve UCM extension information. UCM can provide the following information:
  - extension – UCM extension number
  - name – extension display name / CID name
  - mwi – MWI state
  - permission – permission level of the extension
  - cftw – call forwarding always number
  - dnd – DND state
  - language – display language of the extension in ISO 639-1 format

The UCM should respond with either 200 OK or 404 responses.

3. Added HTTPS support

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



*UCM & HSC PMS interaction*

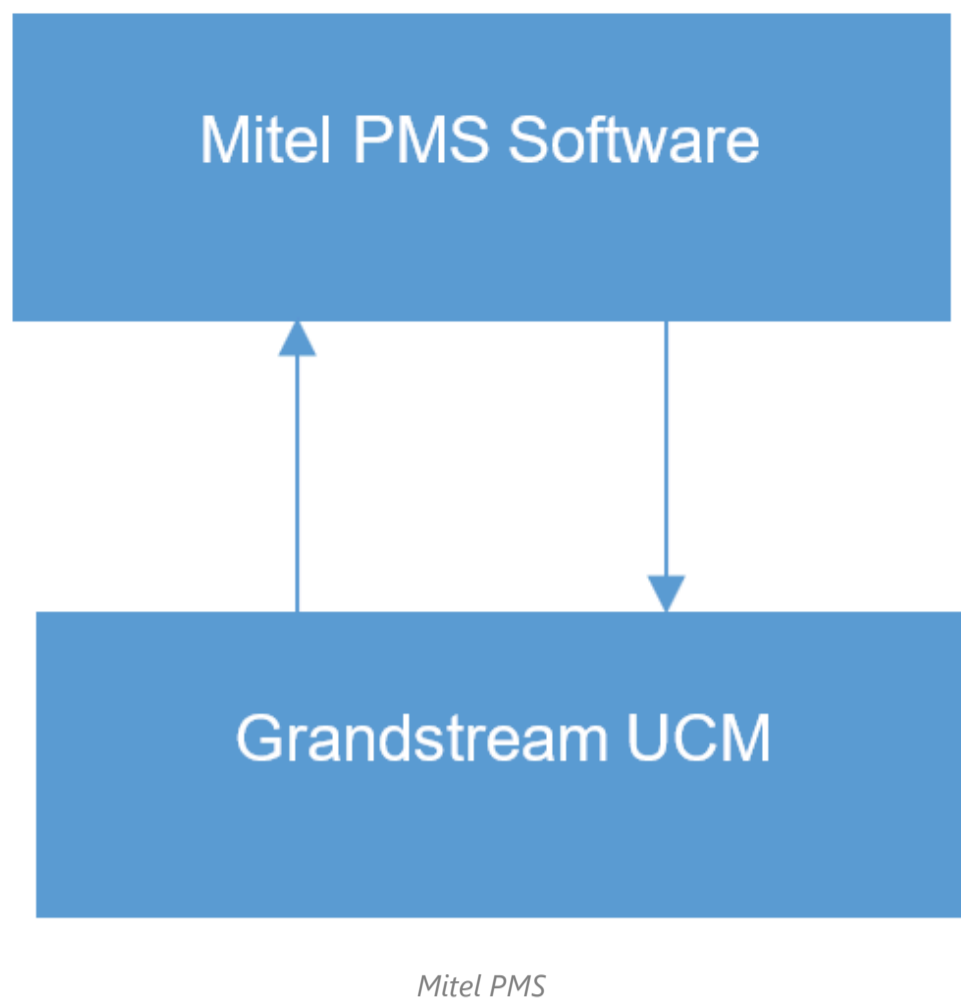
## **Mitel PMS**

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

- PMS (Property Management System)
- PBX

Grandstream 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.

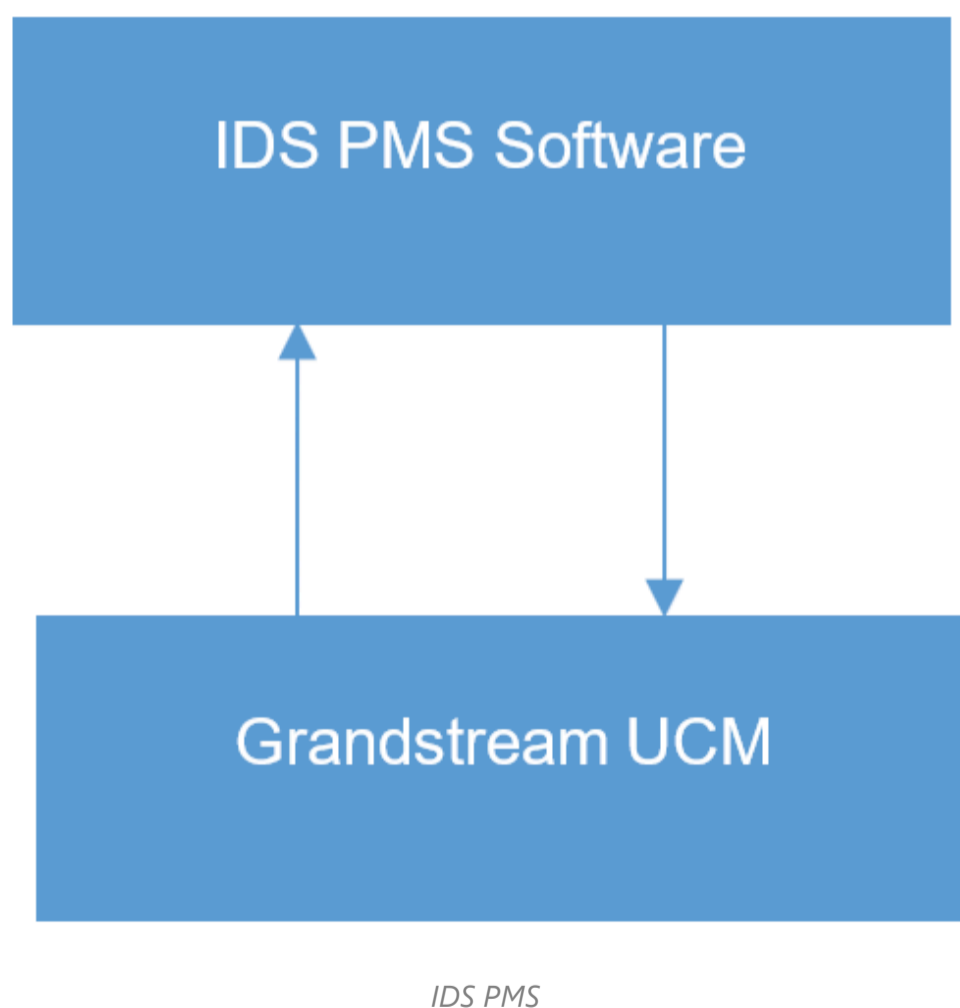


## IDS PMS

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.



## 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://documentation.grandstream.com/knowledge-base/https-api/>, Pmsapi section.

## Connecting to PMS

On the UCM WebGUI → **Other Features** → **PMS** → **Basic Settings** set the connection information for the PMS platform.

Parameter	Description
<b>PMS Module</b>	<p>Users can select the desired PMS module from the drop-down list.</p> <ul style="list-style-type: none"> <li>• char pmslink</li> <li>• Mitel</li> <li>• HSC</li> <li>• PMSAPI</li> <li>• IDSPMS</li> <li>• Local PMS</li> </ul>
<b>Protocol Type</b>	<p>Select the protocol to use for HSC PMS. Available options are:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> </ul> <p>Default is "HTTP" <b>Note:</b> Available only when "PMS Module" is set to "HSC"</p>
<b>Wakeup Prompt</b>	<p>A customized prompts that can be played when the wakeup call is answered. To customize it please navigate to <b>PBX Settings</b> → <b>Voice Prompt</b> → <b>Custom Prompt</b></p>
<b>Room Status Update Prompt</b>	<p>Choose a previously uploaded prompt or upload the prompt which will be played when the room status is changed. If the room status codes have been change, please update the Room Status accordingly.</p>
<b>PMS URL</b>	<p>Enter the server's URL address (i.e such as "http://xxx.xxx.xxx.xxx:8081/soap", "http://xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/soap" or "http://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:5060/soap"). <b>Note:</b> Available only when "PMS Module" is set to "char pmslink"</p>
<b>UCM Port</b>	<p>The port that is opened when UCM is used as PMS server. Default is 8081. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "HSC", or "IDSPMS"</p>
<b>Username</b>	<p>Enter the Username for PMS system authentication. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "HSC", or "PMSAPI".</p>
<b>Password</b>	<p>Enter the Password for PMS system authentication. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "HSC", or "PMSAPI".</p>
<b>Site</b>	<p>Enter the Site ID to identify the hotel on the PMS server. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink".</p>
<b>Back Up Voicemail Recordings</b>	<p>Back up voicemail recordings to external storage after check-out, When Enabled, The user can set the SFTP server for storage purposes by defining the following attributes :</p> <ul style="list-style-type: none"> <li>• <b>Email Address:</b> Configure the email address to send the backup to.</li> <li>• <b>Account:</b> Configures the account on the SFTP server.</li> <li>• <b>Password:</b> Defines the account password</li> <li>• <b>Server Address:</b> Defines the SFTP server address (e.g., xxx.xxx.xxx.xxx:22).</li> <li>• <b>Destination Directory:</b> Specify the directory in SFTP server to save the voicemail recordings to. Format: "xxx/xxx/xxx". If this directory does not exist, UCM will create this directory automatically.</li> <li>• <b>Test the Connection:</b> This option tests the connection to the SFTP server defined.</li> </ul> <p><b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "PMSAPI", "IDSPMS" or "Local PMS".</p>

<b>Sync Guest Name to Phone</b>	Provisions the name of the checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisionable by Zero Config.
<b>Automatically Clear Phone Call History</b>	Configures whether or not the call history of phones will be automatically cleared upon check-in or check-out. Currently only supported on Grandstream phones.  <ul style="list-style-type: none"> <li>● <b>None:</b> Call history will not be deleted after checking-in or checking-out.</li> <li>● <b>Check Out:</b> Call history will be delete when the guest checks-out.</li> <li>● <b>Check In:</b> Call history will be delete when a new guest checks-in.</li> </ul> <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "PMSAPI", "IDSPMS" or "Local PMS".
<b>Automatically Clear Wakeup Calls</b>	Scheduled wakeup calls for rooms can be cleared upon checking in or checking out.  <ul style="list-style-type: none"> <li>● <b>None:</b> The wakeup calls won't be automatically cleared.</li> <li>● <b>Check out:</b> The wake up calls assigned to the guest will be cleared when they check out.</li> <li>● <b>Check In:</b> The wake up calls assigned to a guest will be cleared when a new client checks in.</li> </ul> <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "PMSAPI", "IDSPMS" or "Local PMS".
<b>Automatically Clear Wave Chat History</b>	If enabled, room Wave chat history will be automatically cleared upon check-in or check-out. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "PMSAPI", "IDSPMS" or "Local PMS".
<b>Automatically Reset User/Wave Password</b>	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out. <b>Note:</b> Available only when "PMS Module" is set to "char pmslink", "Mitel", "PMSAPI", "IDSPMS" or "Local PMS".
<b>Review Bill at Check-Out</b>	If enabled, a pop-up window with all the charges will appear during guest check-out for reviewing purposes. <b>Note:</b> Available only when "PMS Module" is set to "Local PMS".
<b>Currency Unit</b>	The currency unit for the call rate. These are the supported options which you can choose from:  <ul style="list-style-type: none"> <li>● American Dollar</li> <li>● Euro</li> <li>● Sterling Pound</li> <li>● Yen</li> <li>● Won</li> <li>● Hong Kong Dollar</li> <li>● Australian Dollar</li> <li>● Canadian Dollar</li> <li>● Baht</li> <li>● Singapore Dollar</li> <li>● Swiss Franc</li> <li>● Swedish Krona</li> <li>● Danish Krone</li> <li>● Norwegian Krone</li> <li>● New Zealand Dollar</li> <li>● South African Rand</li> <li>● Brazilian Rial</li> <li>● Indian Rupee</li> <li>● Russian Ruble</li> <li>● Vietnamese Dong</li> <li>● Polish Zolty</li> <li>● Czech Koruna</li> <li>● Turkish Lira</li> <li>● Custom: Enter the currency unit.</li> </ul> <b>Note:</b> Available only when "PMS Module" is set to "Local PMS".

To use some PMS features please activate the feature code associated under “**Basic Call Features→Feature Codes**”

- Update PMS Room Status
- PMS Wake Up Service

## PMS Features

### Room Management

In Room Management tab, the user can create a room and affect up to two extensions to it. This will appear in Room Status tab, and from there the user can change the Check-in/Check-out

Create New Room Cancel Save

* Address:	<input type="text" value="1001"/>
* Room Number:	<input type="text" value="1001"/>
* Extension 1:	<input type="text" value="1000"/> ▼
* Extension 2:	<input type="text" value="None"/> ▼
* Call Privileges:	<input type="text" value="Internal"/> ▼

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

**Call Privileges** allows the administrator to set the level of call privilege of the room.

### Room Status

On this tab the user can check-in and check-out guests.

Check In
✕

Once a customer has checked in, please manage customer information through the PMS system. Please do not modify names, languages, or calling privileges through the UCM system.

Room Number

\* Room Status

First Name

Last Name

Guest Account

Guest Category Code

Guest Credit Money

\* Arrival Date

\* Expected Departure Date

Language

\* Call Privileges

*Check-in a Client*

After clicking "OK" the client entry will be added to the list.

PMS						
Basic Settings	Room Management	Room Status	Call Rate	Wakeup Service	Mini Bar	Housekeeper
<div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">Check-in/Check-out History</span> <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">Custom Room Status Codes</span> </div>						
Room Number	Check-In Status	Check In / Check Out	Room Status	Customer Name	Options	
1000	● Checked in	<div style="background-color: #ffc107; padding: 2px 5px; border-radius: 3px; display: inline-block;">Check Out</div>	Available		<div style="display: flex; gap: 5px;"> <span>🏠</span> <span>💰</span> </div>	
Total: 1 <span style="margin: 0 5px;">&lt;</span> <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">1</span> <span style="margin: 0 5px;">&gt;</span> <span style="margin: 0 5px;">10 / page</span> <span style="margin: 0 5px;">Goto</span> <input style="width: 30px;" type="text"/>						

*Room Status*

The user can click on **Check-in/Check-out Records** to view the history of the checked-in and checked-out guests.

**Note**

The Call Privilege configured during a guest's check-in will be reset to the room's default call privilege upon guest check-out.

### Call Rate

In Call Rate page, the user can create different call rates for different call types. For example, the user can create a call rate which applies to national calls. The call rates can be differentiated by the prefix set for each call rate, the prefix corresponds to an outbound route pattern which allows national calls. Thus, the call rate applies accordingly.

**PMS**

Basic Settings   Room Management   Room Status   Call Rate   Wakeup Service   Mini Bar   Housekeeper

[+ Add Rate](#)   [Delete Selected Rate](#)

Sequence	Prefix	Starting Cost	Starting Time (seconds)	Rate	Billing Unit (sec)	Options
No data						

PMS – Call Rate

**Add Call Rate**
✕

$Call\ Charge = Starting\ Cost + Rate \times Billing\ Unit$

Prefix

Starting Cost

Starting Time (seconds)

\* Rate

\* Billing Unit (sec)

Add Call Rate

<b>Prefix</b>	Enter the prefix to be used for outgoing calls that should correspond with an outbound route pattern. If left blank, outgoing calls will not require a prefix, and any number can be dialed.
<b>Starting Cost</b>	Configure the device role. When set as a media server, This UCM's PBX-related features will be disabled.
<b>Starting Time (seconds)</b>	Sets the starting time period for call billing. If the length of a guest's external call does not exceed the starting time, only the starting cost amount will be charged. Example: If the starting cost is set to 0.2, and the starting time is set to 60, the first 60 seconds of a call will be charged a flat amount of 0.20 dollars (or other currency). If the starting time is set to 0 instead, the first 60 seconds will be free.
<b>Rate</b>	Sets the billing rate of a call after the starting time period has ended. This is used with Billing Unit (sec) to calculate the cost of a call (Rate x Billing Unit = Telephone Cost).
<b>Billing Unit (sec)</b>	Sets the billing unit used after the starting time period has ended. This is used with Rate to calculate the cost of a call (Rate x Billing Unit = Telephone Cost). Partial units are rounded up (e.g., If the billing unit is set to 60 seconds, and the call lasted 90 seconds (1.5 units), the guest will be billed for 120 seconds (2 units)).

**Note**

The user can create up to 500 call rate entries.

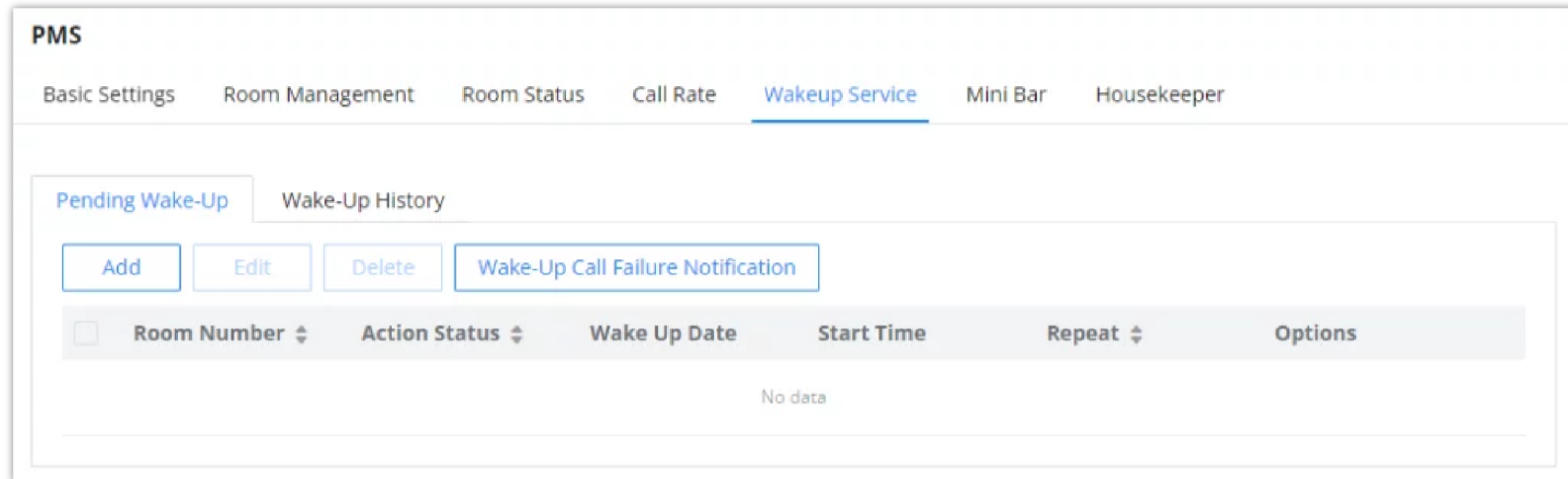
## Wakeup Service

In some cases, guests will request the hotel staff to wake them up at a specific time, you can do that by configuring a wake-up time related to the room number of the guest, where the specific IP phone on that room will ring the extension related to the room number at that specific time, this option is supported on the integrated local PMS on the UCM63XX.

## Pending Wake-Up

The settings can be defined as follows :

1. Select the wake-up service tab, click [Add](#) to create a new wake-up schedule.



Wakeup Service

2. The configuration consists of defining some attributes such as :

- o **Room number:** The room number on which the phone extension will ring at a specific time.
- o **Start Time:** Define the time and the date of the wake up call
- o **Repeat:** Select the frequency of the call: Daily, Weekly, Monthly.
- o **Number of Redials:** Configures the number of times the system will repeat the call attempt after the task has started, but the call is not connected.
- o **Redial Interval (minute):** The time interval between the end of the last call and the next initiated call when the Wake Up Call is not answered.

**PMS > Create New Wakeup Service**

\* Room Number: 1000 ×

\* Start Time: 2024-09-11 10:00

Repeat: No Repeat

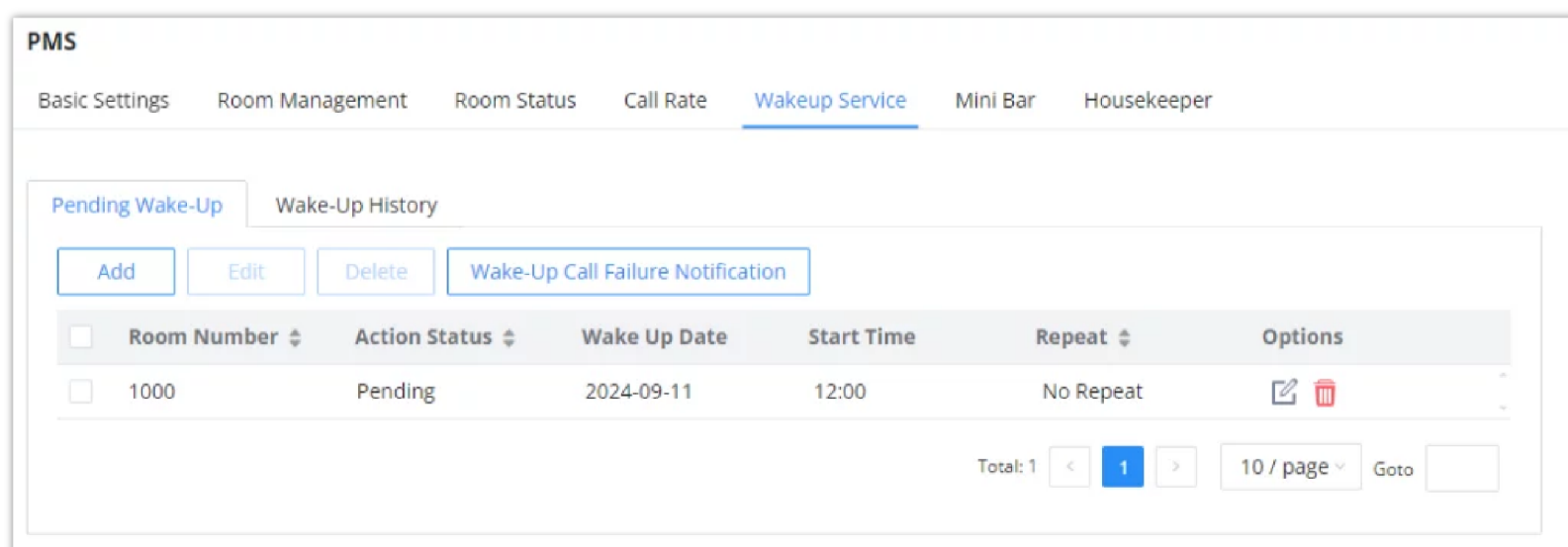
\* Number of Redials: 3

\* Redial Interval (minutes): 5

Cancel Save

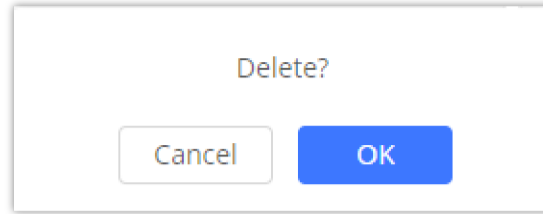
Create a New Wakeup Service

3. The newly displayed entry will be :



Canceled Wakeup Service

4. To delete a specific wake-up service, Click the icon  and confirm the deletion by Clicking "OK"



Delete Wakeup Service

The administrator can configure to send a voicemail or an email notification in case the Wake Up call is not answered.

**PMS > Wake-Up Call Failure Notification**

Voicemail Notification

Voicemail Destination Voicemail

Email Notification  Email Template

\* Receive Email  +

Add Email Address +

Delivery Method Periodic

\* Alert Sending Interval 5 minute(s)

Wake-up Call Failure Notification

The parameters of the Wake-Up Call Failure Notification page are:

<b>Voicemail Notification</b>	<p>Enable to send a notification to the configured voicemail extension/group when a wake-up call has failed, meaning it has non-answered status. Default settings is "disabled".</p> <p><b>Note:</b> No notification will be sent if no failed wake-up call has occurred.</p>
<b>Voicemail Destination</b>	Choose the voicemail/group to receive the failed wake-up call notifications.
<b>Email Notification</b>	<p>Enable to send notifications of failed wake-up calls to the email addresses configured, based on the interval chosen. Any wake-up call that is not marked as "Answered" will be included in these notifications. If there are no failed wake-up calls, no alerts will be sent. Default settings is "disabled".</p>
<b>Receive Email</b>	Configure the e-mail address to receive failed wake-up call notifications. Maximum number of allowed email addresses is 5.
<b>Delivery Method</b>	<p>Choose the delivery method of the email notifications.</p> <ul style="list-style-type: none"> <li>• <b>Real-time:</b> Notifications will be sent out immediately after alerts are generated.</li> <li>• <b>Periodic:</b> Notifications will be queued up and sent out all at once every send cycle. The interval between each send cycle can be configured via the "Alert Sending Interval" option.</li> </ul> <p>Default setting is "Periodic".</p>
<b>Alert Sending Interval</b>	The frequency of notification emails for all failed wakeup calls that happen during that cycle in minutes, hours or days. Default setting is 5 minutes.

## Wake-Up History

The Wake-Up History tab allows users to easily search for past wakeup calls by room number or answer status under a specified period. It is possible to download a CSV file containing the specific search results or a file with all historical wakeup call data.

Wake-Up History

## Mini Bar

The mini bar feature is used to track the goods which have been consumed by the guests during their stay. This feature allows to add the consumed goods to the bill. Adding the goods to the bill can be done by the housekeeper

Mini Bar

<b>Enable Mini Bar</b>	If enabled, feature codes can be used to increase and decrease usage of Mini Bar items.
<b>Increase Mini Bar Usage Code</b>	Dial this code + the item code to increase usage of the Mini Bar item for billing purposes.
<b>Decrease Mini Bar Usage Code</b>	Dial this code + the item code to reduce usage of the Mini Bar item for billing purposes.
<b>Global Tax Rate (%)</b>	Set the tax rate and configure it for an additional tax charge. If no personal tax is configured for a commodity, the global tax rate of the Mini Bar will prevail.
<b>Prompt</b>	This tone will be played when a housekeeper dials a number to enter the Mini Bar and can be used to indicate the corresponding goods code.
<b>Skip Housekeeper and Password Authentication</b>	If enabled, the default housekeeper code is 0000.
<b>Enable Multi-Item Billing</b>	If enabled, users can enter multiple goods in a single call by separating each good code with star (*).

## Local PMS

UCM6300 series offers a local Property Management System to give the user basic management features without having to purchase a PMS for the most basic property management actions. In addition to Room Management, Rooms Status for checking-in and checking-out, Wakeup Service, Mini Bar, and housekeeper functions, the UCM6300 allows several additional functions upon checking-out, like backing up voicemail recordings, clearing wakeup calls and Wave history automatically, in addition to resetting Wave's password. The user can use the Local PMS feature to check-in and check-out clients from the web user interface.

**PMS**

Basic Settings   Room Management   Room Status   Call Rate   Wakeup Service   Mini Bar   Housekeeper

PMS Module: Local PMS

Wakeup Prompt: Wake Call Upload Audio File

Room Status Update Prompt: Default Room Status Update Pro... Upload Audio File

Back Up Voicemail Recordings:

Sync Guest Name to Phone:

Automatically Clear Phone Call History: None

Automatically Clear Wakeup Calls: None

Automatically Clear Wave Chat History: None

Automatically Reset User/Wave Password:

Review Bill at Check-Out:

Currency Unit: Dollar: \$

Cancel   Save

Local PMS

Parameter	Description
<b>Wakeup Prompt</b>	A customized prompts that can be played when the wakeup call is answered. To customize it please navigate to <b>PBX Settings → Voice Prompt → Custom Prompt</b>
<b>Room Status Update Prompt</b>	Choose a previously uploaded prompt or upload the prompt which will be played when the room status is changed. If the room status codes have been change, please update the Room Status accordingly.
<b>Back Up Voicemail Recordings</b>	<p>Back up voicemail recordings to external storage after check-out, When Enabled, The user can set the SFTP server for storage purposes by defining the following attributes :</p> <ul style="list-style-type: none"> <li>● <b>Email Address:</b> Configure the email address to send the backup to.</li> <li>● <b>Account:</b> Configures the account on the SFTP server.</li> <li>● <b>Password:</b> Defines the account password</li> <li>● <b>Server Address:</b> Defines the SFTP server address (e.g., xxx.xxx.xxx.xxx:22).</li> <li>● <b>Destination Directory:</b> Specify the directory in SFTP server to save the voicemail recordings to. Format: "xxx/xxx/xxx". If this directory does not exist, UCM will create this directory automatically.</li> <li>● <b>Test the Connection:</b> This option tests the connection to the SFTP server defined.</li> </ul>
<b>Sync Guest Name to Phone</b>	Provisions the name of the checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisionable by Zero Config.
<b>Automatically Clear Phone Call History</b>	<p>Configures whether or not the call history of phones will be automatically cleared upon check-in or check-out. Currently only supported on Grandstream phones.</p> <ul style="list-style-type: none"> <li>● <b>None:</b> Call history will not be deleted after checking-in or checking-out.</li> <li>● <b>Check Out:</b> Call history will be delete when the guest checks-out.</li> <li>● <b>Check In:</b> Call history will be delete when a new guest checks-in.</li> </ul>

<b>Automatically Clear Wakeup Calls</b>	<p>Scheduled wakeup calls for rooms can be cleared upon checking in or checking out.</p> <ul style="list-style-type: none"> <li>• <b>None:</b> The wakeup calls won't be automatically cleared.</li> <li>• <b>Check out:</b> The wake up calls assigned to the guest will be cleared when they check out.</li> <li>• <b>Check In:</b> The wake up calls assigned to a guest will be cleared when a new client checks in.</li> </ul>
<b>Automatically Clear Wave Chat History</b>	If enabled, room Wave chat history will be automatically cleared upon check-in or check-out.
<b>Automatically Reset User/Wave Password</b>	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
<b>Review Bill at Check-Out</b>	If enabled, a pop-up window with all the charges will appear during guest check-out for reviewing purposes.
<b>Currency Unit</b>	<p>The currency unit for the call rate.</p> <p>These are the supported options which you can choose from:</p> <ul style="list-style-type: none"> <li>• American Dollar</li> <li>• Euro</li> <li>• Sterling Pound</li> <li>• Yen</li> <li>• Won</li> <li>• Hong Kong Dollar</li> <li>• Australian Dollar</li> <li>• Canadian Dollar</li> <li>• Baht</li> <li>• Singapore Dollar</li> <li>• Swiss Franc</li> <li>• Swedish Krona</li> <li>• Danish Krone</li> <li>• Norwegian Krone</li> <li>• New Zealand Dollar</li> <li>• South African Rand</li> <li>• Brazilian Rial</li> <li>• Indian Rupee</li> <li>• Russian Ruble</li> <li>• Vietnamese Dong</li> <li>• Polish Zolty</li> <li>• Czech Koruna</li> <li>• Turkish Lira</li> <li>• Custom: Enter the currency unit.</li> </ul>

## SCHEDULED CALL

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 UCM630xA 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→**Advanced Call Features**→**Scheduled Call**, click on "Add" to create a new scheduled call . The following window will pop up.

Create New Wakeup Service

Enable Wakeup Service:

\* Name:

Prompt:  Prompt

Custom Date:

\* Date:

\* Time:

Members:

3 items Available

Search

1002

1003

1004

2 items Selected

Search

1000

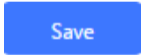
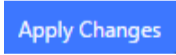
1001

Create a New Wakeup Service

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

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

Wakeup Service

1.  
Click  and  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.

UCM Model	Max members in a Wakeup Service
UCM6300A	50
UCM6302A	100
UCM6304A	150
UCM6308A	200

## Wake Up Service from User Portal

1. Login to the user portal on the UCM630xA.
2. Wake Up service can be found under “**Other 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 **Basic Call Features**→**Feature Codes**.

Feature Codes

1. Click

Save

and

Apply Changes

to apply the changes.

2. 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.

## ANNOUNCEMENT CENTER

The UCM630xA supports Announcement Center feature which allows users to pre-record and store voice message into UCM630xA 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.

Announcements Center

## Announcements Center Settings

**Announcement Center > Create New Announcement Center**

\* Name

\* Code

\* Custom Prompt

\* Ring Timeout (s)

\* Auto Answer

Announce Message Caller-ID

<b>Name</b>	Configure a name for the newly created Announcement Center to identify this announcement center.
<b>Code</b>	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. <b>Note:</b> The combination number must not conflict with any number in the system such as extension number or conference number.
<b>Custom Prompt</b>	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. <b>Note:</b> When uploading a custom, please ensure that the custom prompt file respect the following requirements. <ul style="list-style-type: none"> <li>• The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.</li> <li>• If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters -_</li> </ul>
<b>Ring Timeout</b>	Configure the ring timeout for the group members. The default value is 30 seconds.
<b>Auto Answer</b>	If set to <b>Yes</b> , the Auto answer will be enabled by the members.
<b>Announce Message Caller-ID</b>	If enabled, the caller's CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.

## Group Settings

### Group Settings

<b>Name</b>	Configure a name for the newly created group to identify the group. <b>Note:</b> Name cannot exceed 64 characters.
<b>Number</b>	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. <b>Note:</b> The combination number must not conflict with any number in the system such as extension number or conference number and cannot exceed 64 characters.
<b>Internal Members</b>	Choose the local extensions to add to the group.

<b>LDAP Members</b>	Choose the LDAP contacts to add to the group.
<b>Custom Members</b>	Enter the custom phone numbers to add to the group. <b>Note:</b> The maximum number of custom numbers which can be added are 50 custom number.

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

1. Click

[+ Add Group](#)

to add new group.

2. Give a name to the newly created group.

3. Create a group number which is used with code to send voice message.

4. Select the extensions to be included in the group, who will receive the voice message.

*Announcement Center Group Configuration*

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

1. Click

[+ Add Announcement Center](#)

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.

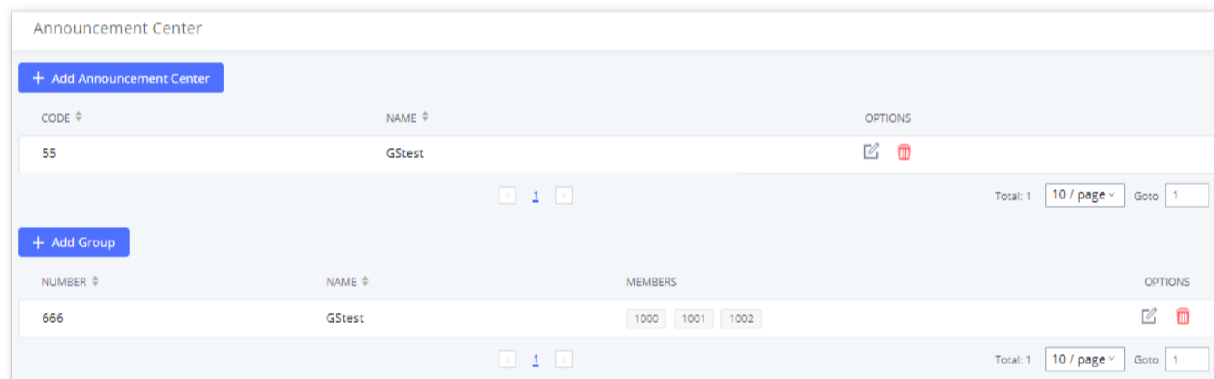
4. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click "Prompt" link and follow the instructions in that page.

*Announcements Center Code Configuration*

<b>Name</b>	Configure a name for the newly created Announcement Center to identify this announcement center.
<b>Code</b>	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

	<p>group 666.</p> <p><b>Note:</b> The combination number must not conflict with any number in the system such as extension number or conference number.</p>
<b>Custom Prompt</b>	<p>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.</p> <p><b>Note:</b> When uploading a custom, please ensure that the custom prompt file respect the following requirements.</p> <ul style="list-style-type: none"> <li>• The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.</li> <li>• If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters -_</li> </ul>
<b>Ring Timeout</b>	Configure the ring timeout for the group members. The default value is 30 seconds.
<b>Auto Answer</b>	If set to <b>Yes</b> , the Auto answer will be enabled by the members.
<b>Announce Message Caller-ID</b>	If enabled, the caller's CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the UCM630xA. All the members in group 666 which are extension 1000, 1001 and 1002 will receive this voice message after they pick up the call.



*Announcements Center Example*

## QUEUOMETRICS

QueueMetrics docking tool provides an interface for UCM system and QM docking. Pass the UCM call queue report to QueueMetrics in a richer form. QueueMetrics is a call center control platform that supports login and logout of frequently used agents in the call center, provides call reports, real-time queue monitoring and other functions.

The screenshot shows the 'QueueMetrics' configuration form. It has the following fields and values:
 

- Enable QueueMetrics Integration:**
- \* QueueMetrics URL:** [Blurred text]
- \* Username:** webqloader
- \* Webqloader Password:** [Masked with dots]
- Partition:** [Empty text box]
- Outbound Call Tracking:**

 At the bottom of the form are two buttons: 'Cancel' and 'Save'.

*QueueMetrics*

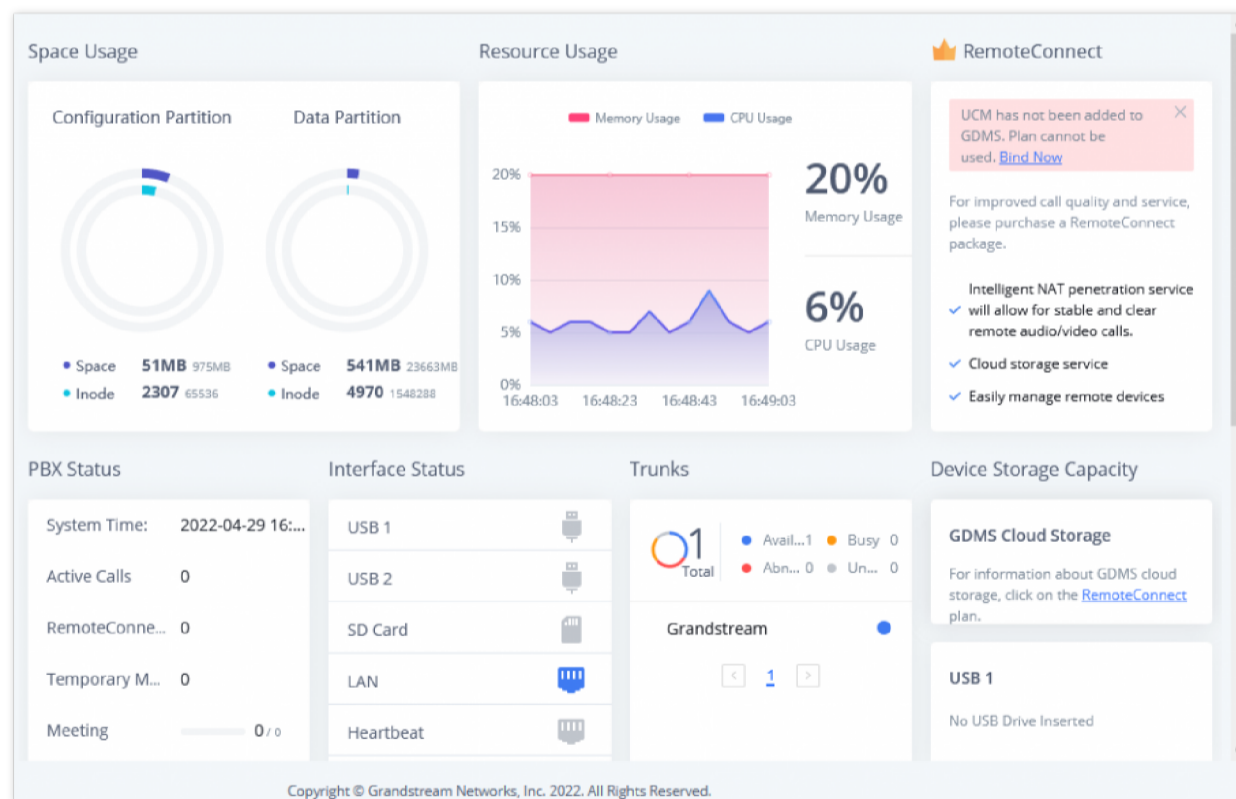
Parameter	Description
<b>Enable QueueMetrics Integration</b>	Tick this box to enable QueueMetrics integration module.
<b>QueueMetrics URL</b>	Enter the URL of the QueueMetrics on-premise server you have installed. (i.e. http://xxx.xxx.xxx.xxx:8080/queuemetrics.).
<b>Username</b>	Please enter the username used to interface with QueueMetrics. This is typically the QueueMetrics webqloader user. Please confirm that the user is enabled to avoid connection failure.
<b>Webqloader Password</b>	Please enter the webqloader password.
<b>Partition</b>	Enter the data storage partition identifier
<b>Outbound Call Tracking</b>	If enabled, QueueMetrics will track the outgoing calls of all extensions. <b>Note:</b> Outbound Call Tracking is available only on the PBX.

Queue Metrics configuration parameters

## STATUS AND REPORTING

### PBX Status

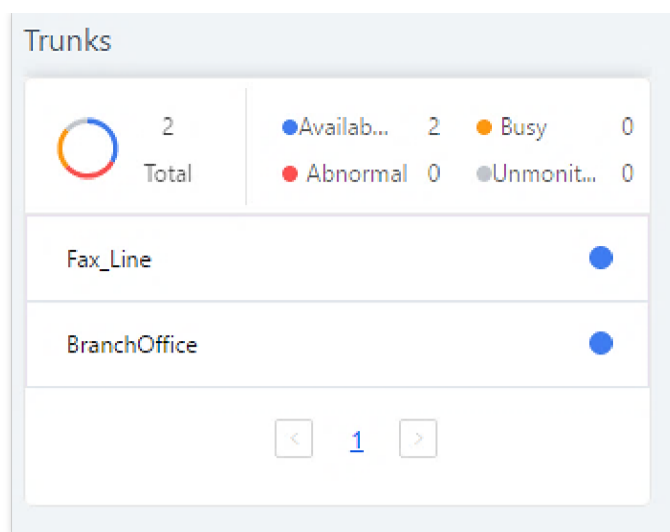
The UCM630xA monitors the status for Trunks, Extensions, Queues, Meeting Rooms, Interfaces and Parking lot. It presents administrators the real-time status in different sections under Web GUI→**System Status**→**Dashboard**.



Status→PBX Status

### Trunks

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



Trunk Status

<b>Status</b>	<p>Display trunk status.</p> <ul style="list-style-type: none"> <li>○ Analog trunk status: <ul style="list-style-type: none"> <li><b>Available</b></li> <li><b>Busy</b></li> <li><b>Unavailable</b></li> <li><b>Unknown Error</b></li> </ul> </li> <li>○ SIP Peer trunk status: <ul style="list-style-type: none"> <li><b>Unreachable:</b> The hostname cannot be reached.</li> <li><b>Unmonitored:</b> Heartbeat feature is not turned on to be monitored.</li> <li><b>Reachable:</b> The hostname can be reached.</li> </ul> </li> <li>○ SIP Register trunk status: <ul style="list-style-type: none"> <li><b>Registered</b></li> <li><b>Unrecognized Trunk</b></li> </ul> </li> </ul>
<b>Trunks</b>	Display trunk name
<b>Type</b>	<p>Display trunk Type:</p> <ul style="list-style-type: none"> <li>○ Analog</li> <li>○ SIP</li> <li>○ IAX</li> </ul>
<b>Username</b>	Display username for this trunk.
<b>Port/Hostname/IP</b>	Display Port for analog trunk, or Hostname/IP for VoIP (SIP/IAX) trunk.

Trunk Status

## 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.

STATUS	PRESENCE STA...	EXTENSION	NAME	TYPE	IP AND PORT	EMAIL...	OPTIONS
<input type="checkbox"/> Ringing	Available	1000		SIP(WebRTC)	192.168.5.199:5070		
<input type="checkbox"/> Unavailable	Available	1001		SIP(WebRTC)	--		
<input type="checkbox"/> In Use	Available	5555		SIP(WebRTC)	192.168.5.199:63827		

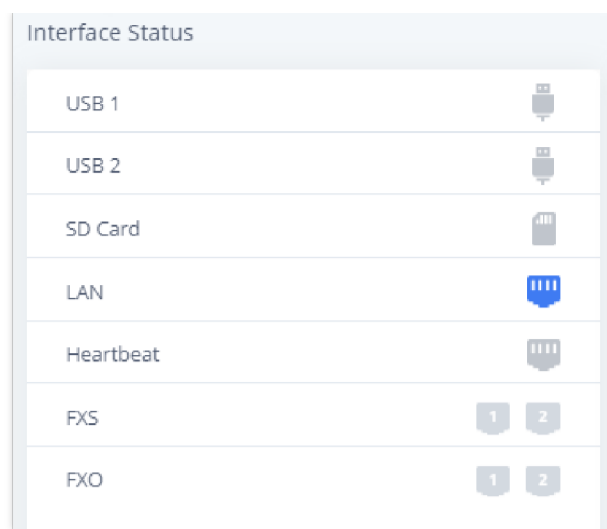
### Extension Status

<b>Status</b>	<p>Display extension number (including feature code). The color indicator has the following definitions.</p> <ul style="list-style-type: none"> <li>○ <span style="color: green;">●</span> Green: Free</li> <li>○ <span style="color: blue;">●</span> Blue: Ringing</li> <li>○ <span style="color: yellow;">●</span> Yellow: In Use</li> <li>○ <span style="color: grey;">●</span> Grey: Unavailable</li> </ul>
<b>Presence Status</b>	Display the presence status of the extension.
<b>Extension</b>	Display the extension number.
<b>Name</b>	First name and last name of the extension.
<b>IP and Port</b>	Display the IP and port number of the registered device.
<b>Email</b>	<p>Display Email Notification status for the extension.</p> <p>When notification is waiting for be sent, shows </p> <p>and once sent it will display </p>
<b>Terminal Type</b>	<p>Displays extension type.</p> <ul style="list-style-type: none"> <li>○ SIP User</li> <li>○ IAX User</li> <li>○ Analog User</li> <li>○ Ring Groups</li> <li>○ Voicemail Groups</li> </ul>

### Extension Status

## Interfaces Status

This section displays interface/port connection status on the UCM630xA. The following example shows the interface status for UCM6304A with USB, WAN port, FXS1, FXS2 and FXO1 connected.



UCM6304A Interfaces Status

	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.

Interface Status Indicators

## System Status

The UCM630xA 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 UCM630xA. Please see details in the following table.

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

<b>Lang</b>	Lang version
<b>Wave</b>	Grandstream Wave version

*System Status → General*

## Network

Under Web GUI → **System Status** → **System Information** → **Network**, users could check the network information for the UCM630xA. Please see details in the following table.

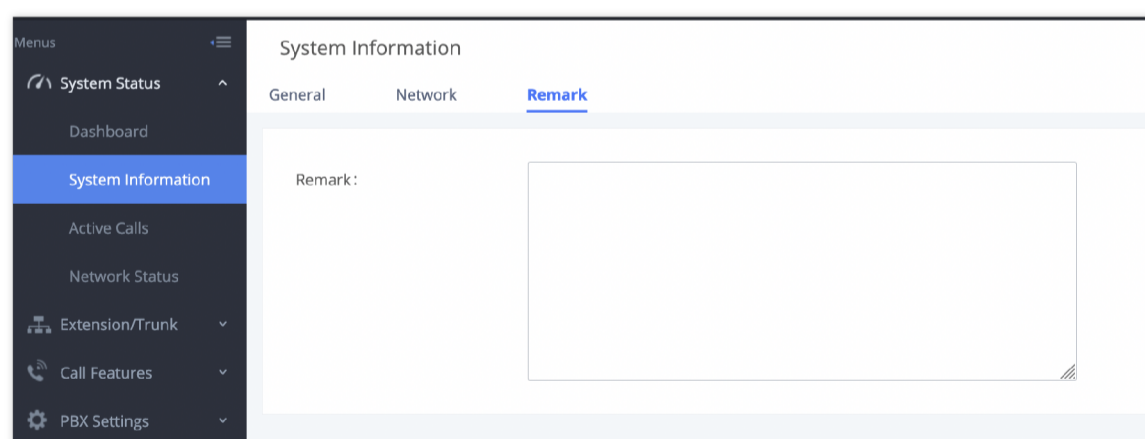
<b>System Status → System Status → Network</b>	
<b>MAC Address</b>	Global unique ID of device, in HEX format. The MAC address can be found on the label coming with original box and on the label located on the bottom of the device.
<b>IPv4 Address</b>	IPv4 address.
<b>IPv6 Address Link</b>	IPv6 address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

*System Status → Network*

## Remark

The UCM admin could add remark on UCM web UI → System Status → System Information → Remark to log any necessary information for the UCM such as location, technical contacts, important topology information and etc. This could be useful for UCM admin especially when there are multiple UCMs to be managed.

If this UCM has UCMRC service, the remark will also be sync up to GDMS. If this information is edited on GDMS, it will also be updated to the UCM web UI.



*System Status → System Information → Remark*

## 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**

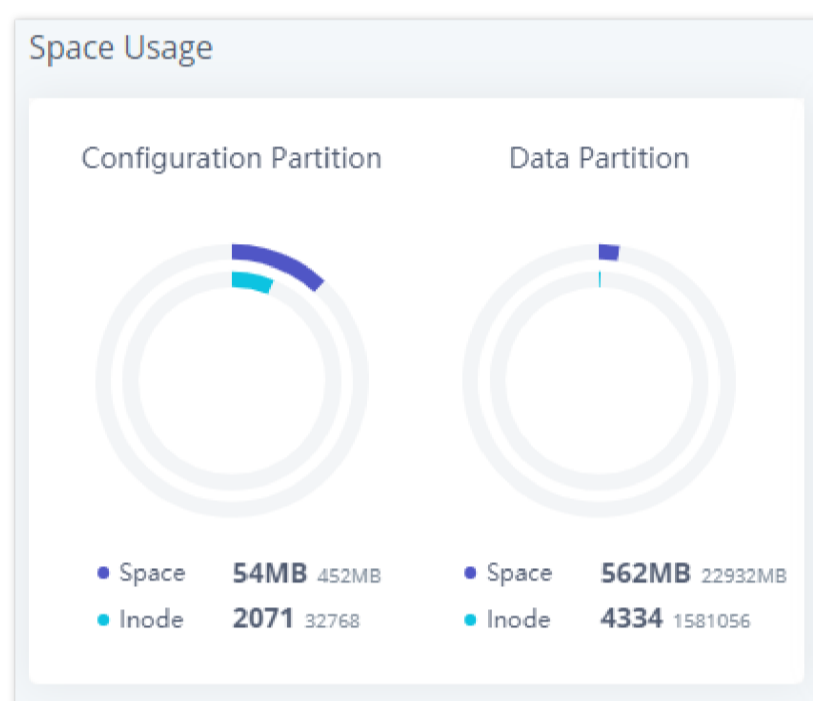
SD Card will display if connected.

Inode Usage includes:

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

**Note:**

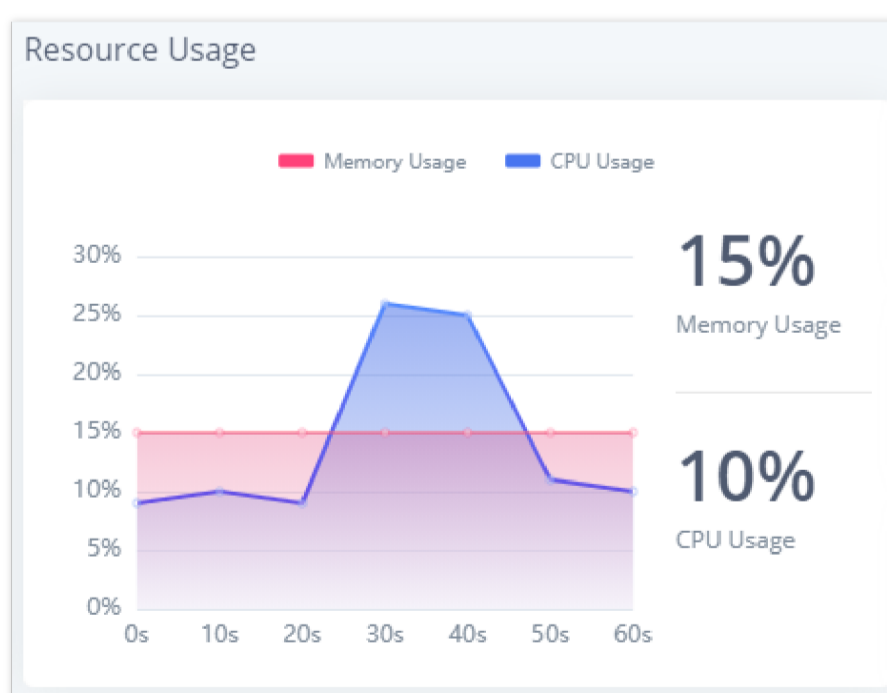
Inode is the pointer used for file reference in the system. The system usually has limited resources of pointers



System Status → Storage Usage

### Resource Usage

When configuring and managing the UCM630xA, 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.



System Status → Resource Usage

### System Events

The UCM630xA 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 UCM630xA which will have alert and/or Email generated if occurred:

EVENT NAME	ALERT	EMAIL NOTIFICATION	HTTP NOTIFICATION	PARAMETER SETTINGS
Fail2ban Blocking	OFF	OFF	OFF	
Flood Attacks	OFF	OFF	OFF	
Network Traffic Storm	OFF	OFF	OFF	
User Login Banned	OFF	OFF	OFF	
Remote Login	OFF	OFF	OFF	
User Login Success	OFF	OFF	OFF	
User Login Failed	OFF	OFF	OFF	
System Crash	ON	OFF	OFF	
Restore Config	OFF	OFF	OFF	
System Update	OFF	OFF	OFF	
System Reboot	OFF	OFF	OFF	
CPU Usage Call Control	OFF	OFF	OFF	
Memory Usage	OFF	OFF	OFF	
TLS Cert Expiration	ON	OFF	OFF	
HA failure warning	OFF	OFF	OFF	
Cloud IM abnormal	OFF	OFF	OFF	

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. <https://documentation.grandstream.com/knowledge-base/ucm-remoteconnect-user-guide>

Click on



to configure the parameters for each event. See descriptions below.

Alert Events	Definitions
<b>Fail2ban Blocking</b>	If the system Fail2ban is blocking, the event will be recorded in the alert log.
<b>Flood Attacks</b>	An alert will be generated in case a DDoS attack attempt is detected by the UCM. The event will be registered in the alert log and it will be pushed to the GDMS.
<b>Network Traffic Storm</b>	An alert will be generated in case there is an excessive amount of packets on the LAN. Network Traffic Storms consume the resources of the network components and saturate the bandwidth, which will bring the whole network to a halt. This event will be registered in events log and a notification will be pushed to the GDMS.
<b>User Login Banned</b>	If user login is blocked, the event will be recorded in the alert log.
<b>Remote Login</b>	An alert will be generated upon a remote login.
<b>User Login Success</b>	Successful user login events will be recorded in the alert log.
<b>User Login Failed</b>	User login failure events will be recorded in the alert log.
<b>System Crash</b>	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.

<b>Restore Config</b>	Once the system configuration is restored, the configuration restoration event will be recorded in the alert log.
<b>System Update</b>	Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
<b>System Reboot</b>	<p>UCM will detect the system restart and will send an alert for it. Users can see the device's MAC address, the reason for the reboot and the initiator of the reboot. There are two kinds of reboots that the UCM detects:</p> <ul style="list-style-type: none"> <li>● <b>Manual restart:</b> refers to when the administrator reboots the system through the Web U or when the device is restarted via the LCD or through GDMS.</li> <li>● <b>Automatic restart:</b> this reboot is done automatically due to several reasons some of which are firmware upgrade, HA switchover, factory reset, power failure, change of certain settings, etc.</li> </ul>
<b>CPU Usage Call Control</b>	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.
<b>Memory Usage</b>	If the detected value exceeds the configured threshold (in percentage), the UCM630X system will send the alert.
<b>TLS Cert Expiration</b>	Starting 7 days before the HTTP Server TLS certificate in the UCM device expires, an expiration countdown notification is sent every day; the certificate has expired, an expiration notification is sent; after the alarm notification is generated, a valid new certificate is uploaded, and a notification to restore the TLS certificate is generated.
<b>HA Failure</b>	After the HA dual-system hot backup disaster recovery function is enabled in the UCM device, the HA fault alarm is automatically turned on. When the device has a software and hardware related fault, an HA fault alarm is generated.
<b>HA Switch</b>	Once a switch between primary UCM device and secondary UCM has been detected, an alert event will be sent.
<b>HA Data Sync Failure</b>	In case of Data Sync failure in HA deployment, the UCM device will generate an alert event.
<b>Cloud IM Abnormal</b>	An alert message will be generated if the Cloud IM encounters any issue or exhibits any abnormal behavior.
<b>Modify Super Admin Password</b>	Once the super administrator password is modified, the system will record the password modification event in the alarm log.
<b>Data Sync Backup</b>	If the system performs data synchronization and backup abnormalities, the event will be recorded in the alert log.
<b>Local Disk Usage</b>	<p>The UCM630X will perform the Local disk usage detection based on a configured cycle. If the detected value exceeds the threshold (in percentage), the UCM630X system will send the alert.</p> <p><b>Note:</b> If the threshold is exceeded, any behavior of operating the disk will be rejected, including stopping file upload, IM writing, recording and CDR recording.</p>
<b>External Disk Usage</b>	The UCM630X will perform the External disk usage detection based on a configured cycle. If the detected value exceeds the threshold (in

	percentage), the UCM630X system will send the alert.
<b>External Disk Status</b>	If the external disk of the system is Connected/Disconnected, the event will be recorded in the alarm log.
<b>Switching File Storage Path</b>	Once the file storage path on the UCM device is changed, an alert will be sent.
<b>Emergency Calls</b>	If the system generates an emergency call, the event will be recorded in the alert log.
<b>SIP Outgoing Call through Trunk Failure</b>	If the system SIP trunk outgoing call fails, the event will be recorded in the alert log.
<b>SIP Internal Call Failure</b>	If the system SIP extension call fails within the office, the event will be recorded in the alert log.
<b>Remote Concurrent Calls</b>	If the remote concurrent call fails, the event will be recorded in the alert log.
<b>Excessive Outbound Calls</b>	When an extension initiates calls frequently, an alert will be logged in the alert log and a notification will be pushed.
<b>Trunk Outbound Call Duration Usage</b>	When the system detects that the number of concurrent calls of a certain relay exceeds the threshold set by the relay within a certain period of time, the event will be recorded in the alarm log. Calls are not restricted if the threshold is exceeded.
<b>Trunk Concurrent Calls</b>	If the threshold of all incoming and outgoing concurrent calls through a trunk is exceeded, the UCM will generate an alert event.
<b>Register SIP trunk failed</b>	The UCM will detect the failure of SIP trunk registration at a set interval.
<b>SIP Peer Trunk Status</b>	If the SIP peer trunks status is abnormal, the event will be recorded in the alert log.
<b>Register SIP failed</b>	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.
<b>SIP Lost Registration</b>	If System SIP extension registration is lost, the event will be recorded in the alert log.

## 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 reboot alert logs.

System Events			
<a href="#">Alert Log</a> <a href="#">Alert Events List</a> <a href="#">Alert Contact</a>			
<input type="button" value="Delete Search Result(s)"/> <input type="button" value="Clear"/>		<a href="#">Display Filter</a> ▼	
Time ↕	Event Name ↕	Type ↕	Content
2024-10-14 08:20:23	System Reboot	Generate Alert	MAC: C0:74:AD:38:38:38 - System has rebooted due to unidentifiable reasons. Reboot time: 2024-10-14 08:19:29.
2024-10-11 13:10:02	System Reboot	Generate Alert	MAC: C0:74:AD:38:38:38 - System has been rebooted by John via WebUI. Reboot time: 2024-10-11 13:09:09.
2024-10-01 12:16:20	Register SIP failed	Generate Alert	SIP registration failed! The remote address is: IPV4/UDP/192.168.1.100, account ID is: 4001

Total: 13   <   1   2   >   10 / page   Goto

System Events → Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on

. Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.
2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

User could filter out alert logs of "Generate Alert" or "Restore to Normal" by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of "Restore to Normal".

Start Time:	<input type="text" value="2020-11-03"/> <input type="button" value="Calendar"/>	<input type="text" value="00:00"/> <input type="button" value="Clock"/>
End Time:	<input type="text" value="2020-11-10"/> <input type="button" value="Calendar"/>	<input type="text" value="14:31"/> <input type="button" value="Clock"/>
Event Name:	<input type="text" value="All"/> ▼	
Type:	<input type="text" value="All"/> ▼	
<input type="button" value="Reset"/>		<input type="button" value="Filter"/>

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.

<b>Super Admin Email</b>	Configure the email addresses to send alert notifications to.  Up to 10 email addresses can be added.
<b>Admin Email</b>	Configure the email addresses to send alert notifications to.  Up to 10 email addresses can be added.
<b>Email Template</b>	Please refer to section <b>Email Templates</b>
<b>Protocol</b>	Protocol used to communicate with the server. HTTP or HTTPS.  Default one is <b>HTTP</b> .
<b>HTTP Server</b>	The IP address or FQDN of the HTTP/HTTPS server.

<b>HTTP Server Port</b>	HTTP/HTTPS port
<b>Warning Template</b>	<p>Customize the template used for system warnings.</p> <p>By default: <code>{"action":"\${ACTION}","mac":"\${MAC}","content":"\${WARNING_MSG}"}</code></p>
<b>Notification Template</b>	<p>Customize the notification template to receive relevant alert information.</p> <p>By default:  <code>{"action":"\${ACTION}","cpu":"\${CPU_USED}","memory":"\${MEM_USED}","disk":"\${DISK_USED}","external_disk":"\${EXTERNAL_DISK_USED}"}</code></p> <p><b>Note:</b> The notification message with "<b>action:0</b>" will be sent periodically if Notification Interval is set.</p>
<b>Notification Interval</b>	<p>Modifies the frequency at which notifications are sent in seconds.</p> <p>No notifications will be sent if the value is "0". Default value: <b>20</b></p>
<b>Template Variables</b>	<p><code>\${MAC}</code> : MAC Address</p> <p><code>\${WARNING_MSG}</code> : Warning message</p> <p><code>\${TIME}</code> : Current System Time</p> <p><code>\${CPU_USED}</code> : CPU Usage</p> <p><code>\${MEM_USED}</code> : Memory Usage</p> <p><code>\${ACTION}</code> : Message Type. Refer to [Alert Events]</p> <p><code>\${DISK_USED}</code> : Disk Usage</p> <p><code>\${EXTERNAL_DISK_USED}</code> : Disk Usage</p>

*Alert Contact*

## Task Management

The user can schedule a task in this section to be performed once. The user can schedule 4 possible tasks, Scheduled Paging/Intercom, Scheduled Backup, Scheduled Data Sync, and Scheduled Cleaner.

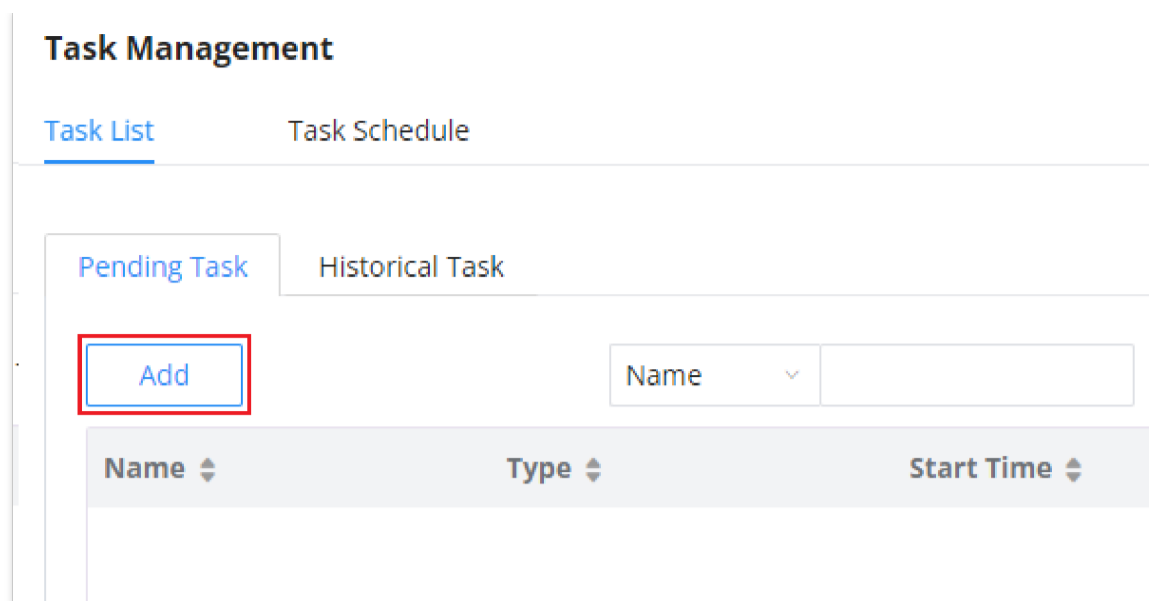
The task which can be scheduled are the following:

- Paging/Intercom
- Backup
- Data Sync
- Cleaner (CDR, Reports, IM Data, Files)

## Task List

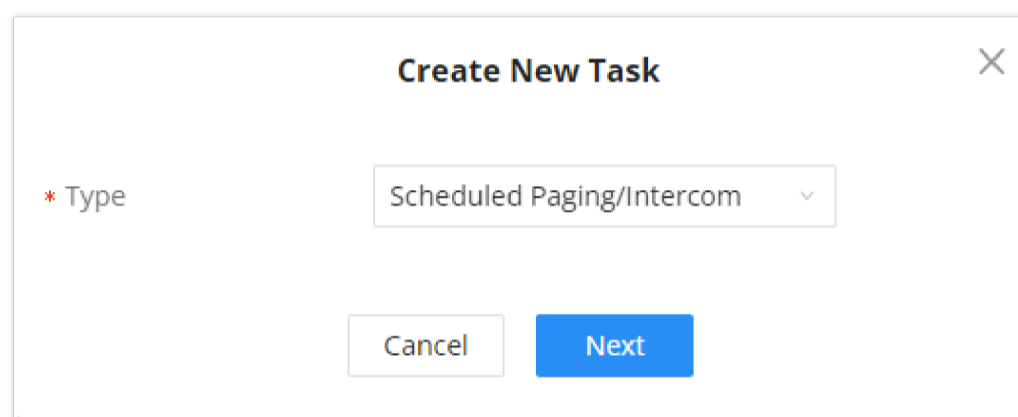
The user can schedule a task in this section to be performed once. The user can schedule 4 possible tasks, Scheduled Paging/Intercom, Scheduled Backup, Scheduled Data Sync, and Scheduled Cleaner.

To schedule a task, please navigate to **Maintenance > Task Management > Task List > Pending Task**, then click on Add button.



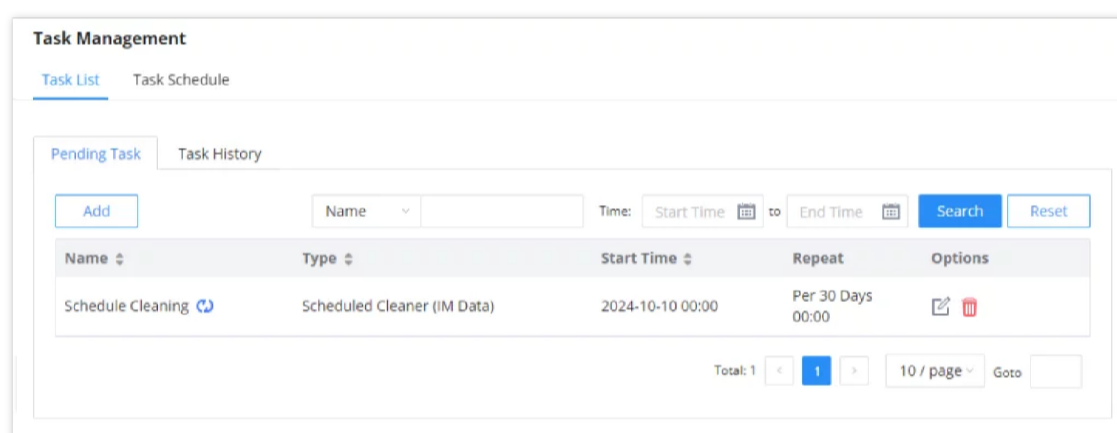
Add Task

Then select the type of the task from the drop-down menu.



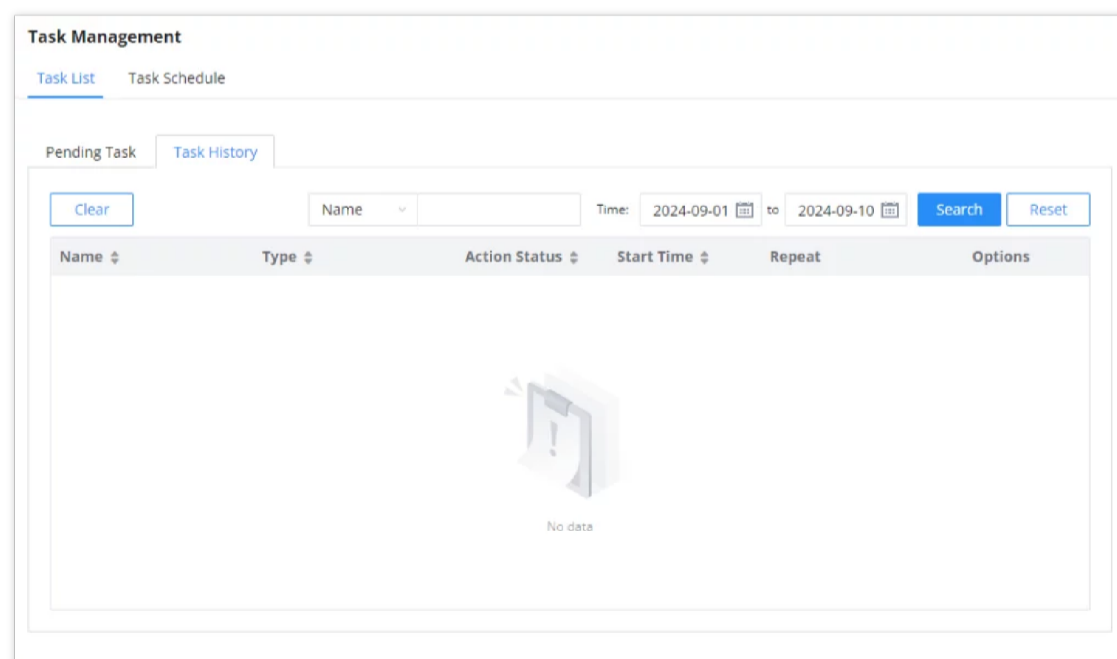
Create New Task

Click "Next" and then set the needed parameters accordingly.



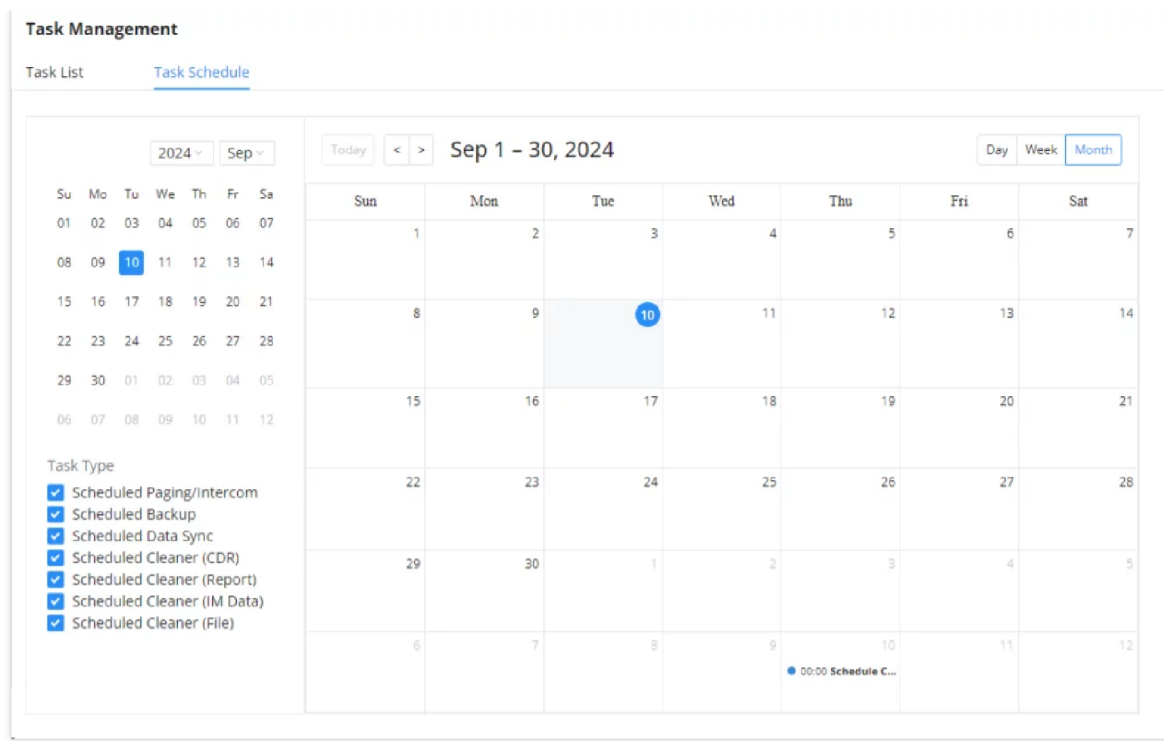
Pending Tasks

The user can check the log of the tasks which have been performed in "Task History"



## Task Schedule

To get an overview about all the tasks which have been scheduled, the user can click on **Task Schedule** tab to view the full schedule.



Task Schedule

## 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 UCM630xA, 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.

The screenshot shows the 'CDR Filter' interface. It contains the following fields and options:

- Start Time:** Select date and Select time
- End Time:** Select date and Select time
- Caller Number:** Text input field
- Caller Name:** Text input field
- Callee Number:** Text input field
- Account Code:** Text input field
- Source Trunk Name:** Text input field
- Destination Trunk Name:** Text input field
- Action Type:** Text input field
- Export File Data:** Text input field
- Extension Group:** Dropdown menu
- Call Type:**
  - Inbound Calls
  - Outbound Calls
  - Internal Calls
  - External Calls
- Status:**
  - Answered
  - No Answer
  - Busy
  - Failed

At the bottom, there are 'Filter' and 'Reset' buttons. A green banner at the bottom states: "By default, this page displays the CDR entries from the current month. Use the 'Filter' button to specify a time range."

CDR Filter

<p><b>Call Type</b></p>	<p>Groups the following:</p> <ul style="list-style-type: none"> <li>○ Inbound calls: Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension.</li> <li>○ Outbound calls: Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension.</li> <li>○ Internal calls: Internal calls are calls from one internal extension to another extension, which are not sent over a trunk.</li> <li>○ External calls: External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension.</li> </ul>
<p><b>Status</b></p>	<p>Filter with the call status, the available statuses are the following:</p> <ul style="list-style-type: none"> <li>○ Answered</li> <li>○ No Answer</li> <li>○ Busy</li> <li>○ Failed</li> </ul>

<b>Source Trunk Name</b>	Select source trunk(s) and the CDR of calls going through inbound the trunk(s) will be filtered out.
<b>Destination Trunk Name</b>	Select destination trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.
<b>Action Type</b>	<p>Filter calls using the Action Type, the following actions are available:</p> <ul style="list-style-type: none"> <li>○ Announce</li> <li>○ Announcement page</li> <li>○ Dial</li> <li>○ Announcements</li> <li>○ Callback</li> <li>○ Call Forward</li> <li>○ Meeting</li> <li>○ DISA</li> <li>○ Follow Me</li> <li>○ IVR</li> <li>○ Page</li> <li>○ Parked Call</li> <li>○ Queue</li> <li>○ Ring Group</li> <li>○ Transfer</li> <li>○ VM</li> <li>○ VMG</li> <li>○ VQ_Callback</li> <li>○ Wakeup</li> <li>○ Emergency Call</li> <li>○ Emergency Notify</li> <li>○ SCA</li> </ul>
<b>Extension Group</b>	Specify the Extension Group name to filter with.

<p><b>Export File Data</b></p>	<p>Select the fields that will be exported, the following fields are available:</p> <ul style="list-style-type: none"> <li>○ Account Code</li> <li>○ Session</li> <li>○ Premier caller</li> <li>○ Action type</li> <li>○ Source trunk name</li> <li>○ Destination trunk name</li> <li>○ Caller number</li> <li>○ Caller ID</li> <li>○ Caller name</li> <li>○ Callee number</li> <li>○ Answer by</li> <li>○ Context</li> <li>○ Start time</li> <li>○ Answer time</li> <li>○ End time</li> <li>○ Call time</li> <li>○ Talk time</li> <li>○ Source channel</li> <li>○ Dest channel</li> <li>○ Call status</li> <li>○ Dest channel extension</li> <li>○ Last app</li> <li>○ Last data</li> <li>○ AMAFLAGS</li> <li>○ UIQUEID</li> <li>○ Call type</li> <li>○ NAT</li> </ul>
<p><b>Account Code</b></p>	<p>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.</p>
<p><b>Start Time</b></p>	<p>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.</p>
<p><b>End Time</b></p>	<p>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.</p>
<p><b>Caller Number</b></p>	<p>Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out.</p> <p>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.</p> <p>For example:</p> <p><b>3XXX:</b> It will filter out CDR that having caller number with leading digit 3 and of 4 digits' length.</p> <p><b>3.:</b> It will filter out CDR that having caller number with leading digit 3 and of any length.</p>
<p><b>Caller Name</b></p>	<p>Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.</p>

<b>Callee Number</b>	<p>Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out.</p> <p><b>Note:</b> The "Callee Number" filter field supports specifying Pattern (example: 3XXX) or using Leading digits (example: 3.) as filtering options.</p>
----------------------	---

*CDR Filter Criteria*

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	ACCOUNT CODE	RECORDING FILE OPTIONS
	5555	5555	1000	DIAL	2019-12-11 09:53:03	0:00:11		-

*Call Report*

The CDR report has the following data fields:

- o **Start Time**

Format: 2019-12-11 09:53:03

- o **Action Type**

Example:

IVR

DIAL

WAKEUP

- o **Call From**

Example format: 5555

- o **Call To**

Example format: 1000

- o **Call Time**

Format: 0:00:11

- o **Talk Time**

Format: 0:00:06

- o **Account Code**

Example format:

Grandstream/Test

- o **Status**

Answered, Busy, No answer or Failed.

Users could perform the following operations on the call report.

- o **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**

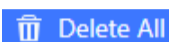
Click on "Download Search Result(s)" to export the records filtered out to a .csv file.

- **Download All Records**

Click on "Download All Records" to export all the records to a .csv file.

- **Delete All**

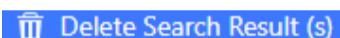
Click on



button to remove all the call report information.

- **Delete Search Result**

On the bottom of the page, click on



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



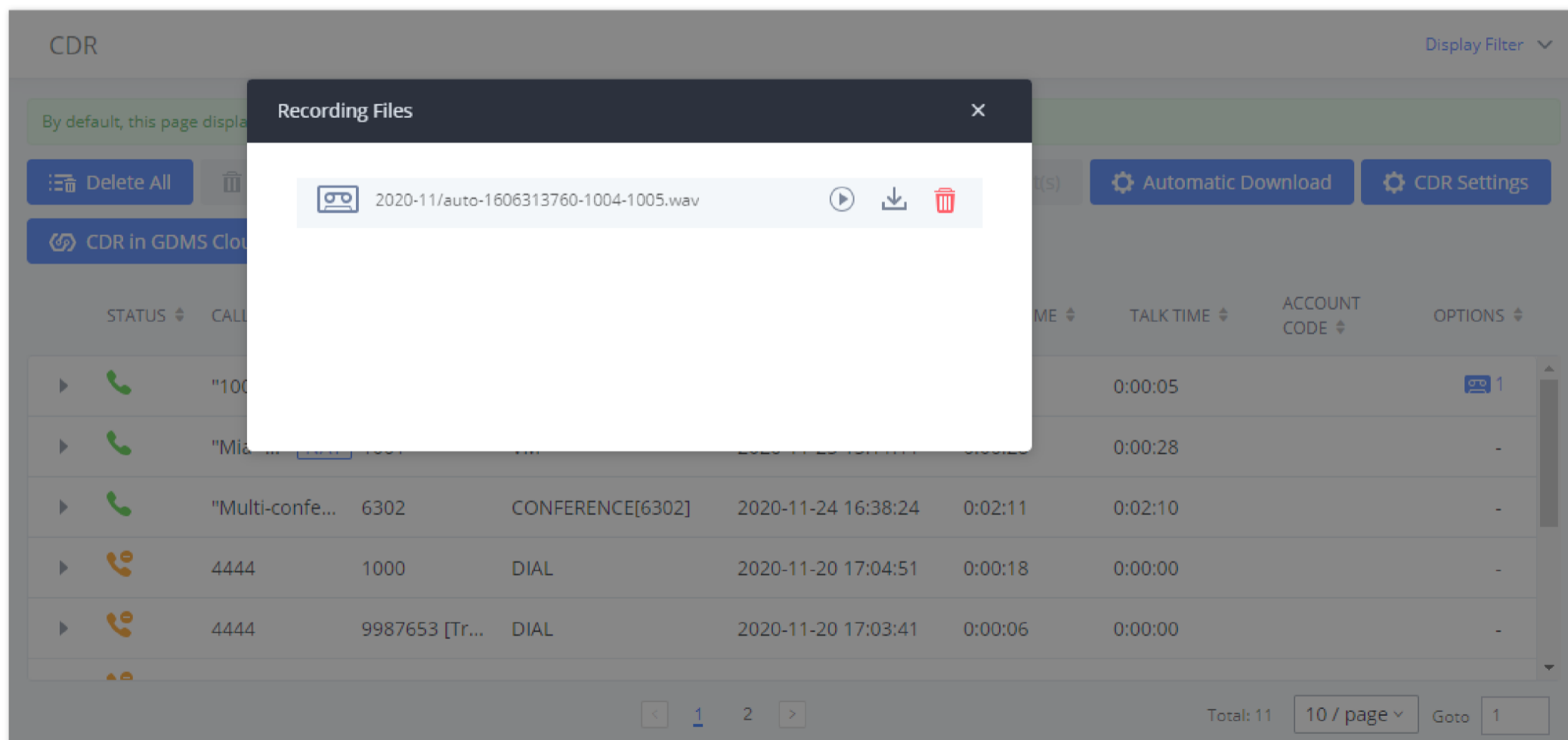
to play the recording file; click on



to download the recording file in .wav format; click on



to delete the recording file (the call record entry will not be deleted).



Call Report Entry with Audio Recording File

- **Automatic Download CDR Records**

User could configure the UCM630xA 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.

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 UCM630xA 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		-

CDR Report

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

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

Downloaded CDR File Sample

o **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.

o **Source Channel, Dest Channel**

**Sample 1:**

caller number	callee number	context	calerid	source channel	dest channel	disposition
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	ANSWERED

Downloaded CDR File Sample – Source Channel and Dest Channel 1

- o DAHDI means it is an analog call, FXO or FXS.
- o For UCM6302A, DAHDI/(1-2) are FXO ports, and DAHDI(3-4) are FXS ports.
- o For UCM6304A, DAHDI/(1-4) are FXO ports, and DAHDI(5-6) are FXS ports.
- o For UCM6308A, DAHDI/(1-8) are FXO ports, and DAHDI(9-10) are FXS ports.

**Sample 2:**

caller number	callee number	context	calerid	source channel	dest channel	lastapp
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial

Downloaded CDR File Sample – Source Channel and Dest Channel 2

- o "SIP" means it is a SIP call. There are three format:
- o (a) **PJSIP/NUM-XXXXXX**, where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.
- o (c) **PJSIP/trunk\_X/NUM**, where trunk\_X is the internal trunk name, and NUM is the number to dial out through the trunk.
- o (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.

End Time:

Caller Name:

Account Code:

Destination Trunk Name:

Export File Data:

Outbound Calls  Internal Calls

No Answer  Busy

Use the "Filter" button to specify a time range.

type Start Time Call Time Talk Time Account Code Recording File

CDR Export File data

## CDR in GDMS Cloud

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

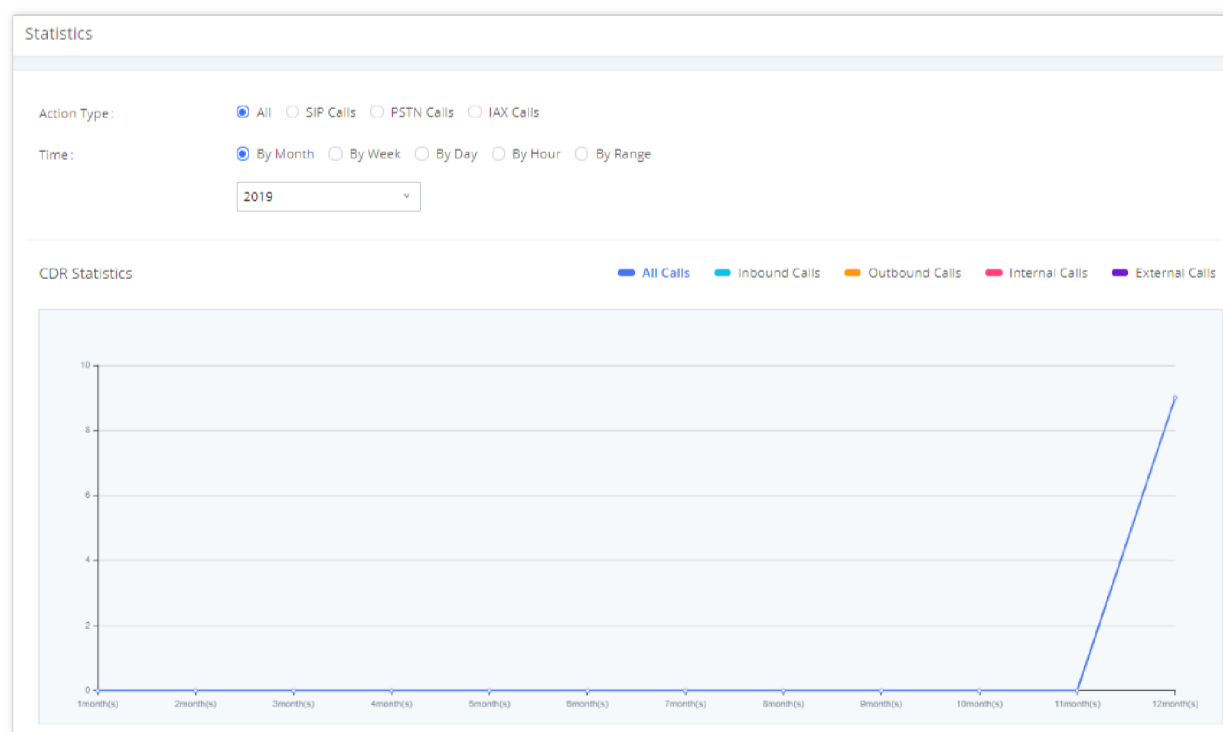
CDR in GDMS Cloud

NAME	DATE	SIZE	OPTIONS
No Data			

CDR in GDMS Cloud

## Statistics

CDR Statistics is an additional feature on the UCM630xA 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.



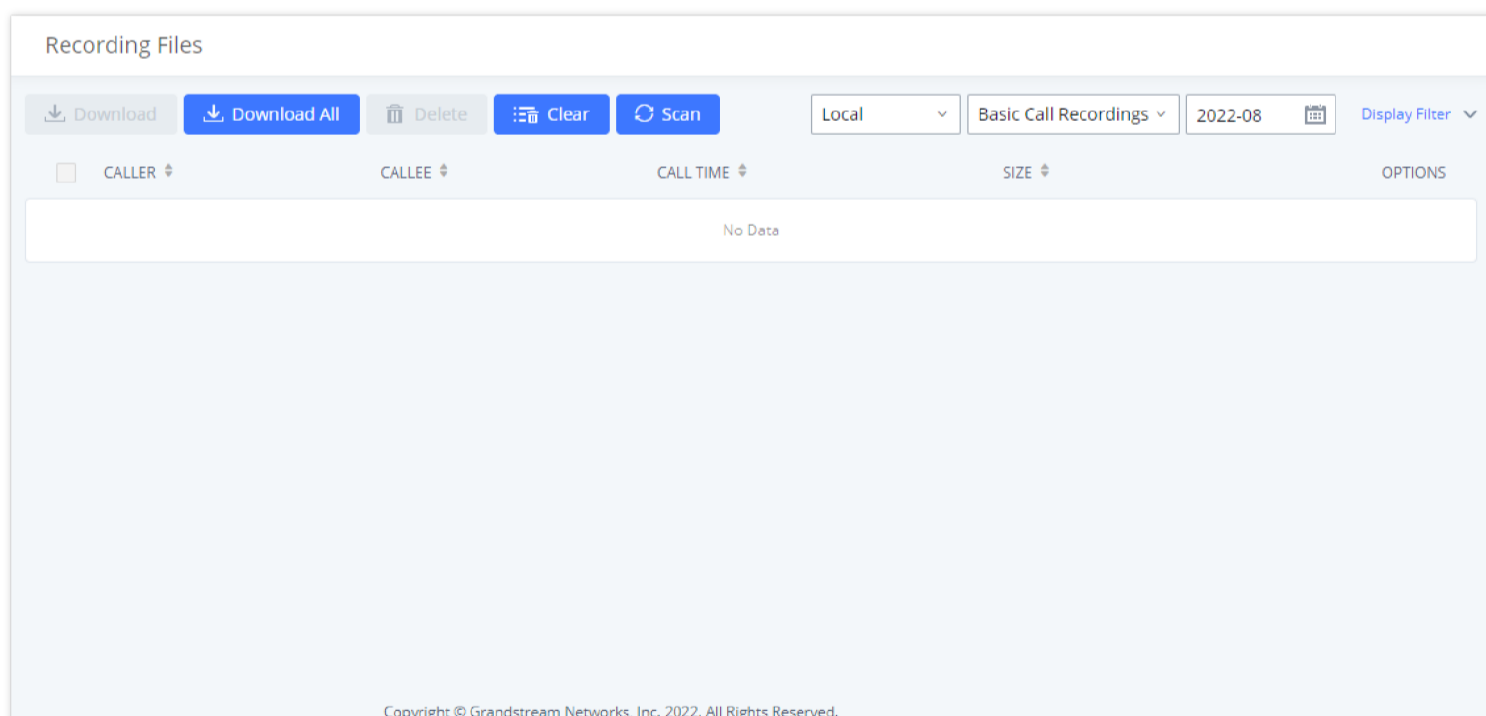
CDR Statistics

<b>Trunk Type</b>	<p>Select one of the following trunk type.</p> <ul style="list-style-type: none"> <li>○ All</li> <li>○ SIP Calls</li> <li>○ PSTN Calls</li> </ul>
<b>Call Type</b>	<p>Select one or more in the following checkboxes.</p> <ul style="list-style-type: none"> <li>○ Inbound calls</li> <li>○ Outbound calls</li> <li>○ Internal calls</li> <li>○ External calls</li> <li>○ All calls</li> </ul>
<b>Time Range</b>	<ul style="list-style-type: none"> <li>○ By month (of the selected year).</li> <li>○ By week (of the selected year).</li> <li>○ By day (of the specified month for the year).</li> <li>○ By hour (of the specified date).</li> <li>○ By range. For example, 2016-01 To 2016-03.</li> </ul>

*CDR Statistics Filter Criteria*



## 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 UCM630xA.



*CDR → Recording Files*

- Click on "**Download**" to batch-download the selected recording files.
- Click on "**Download All**" to download all the recording files.
- Click on "**Delete**" to batch-delete the selected recording files.
- Click on "**Clear**" to delete all the recording files.

- Click on **"Scan"** to retrieve the file information and display all the recording files on external storage. The UCM automatically retrieves the info of the first 5000 files from external storage already. This button can be used when the number of files stored on the external storage exceeds 5000 files and it requires manual file scanning.
- Select either **"USB Disk"** or **"Local"** to show recording files stored on external or internal storage, depending on the 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.

**Note:**

If Data/File encryption is enabled for audio call recordings, scanning the external storage for recordings via the Scan button will automatically encrypt all the found recordings.

## USER PORTAL

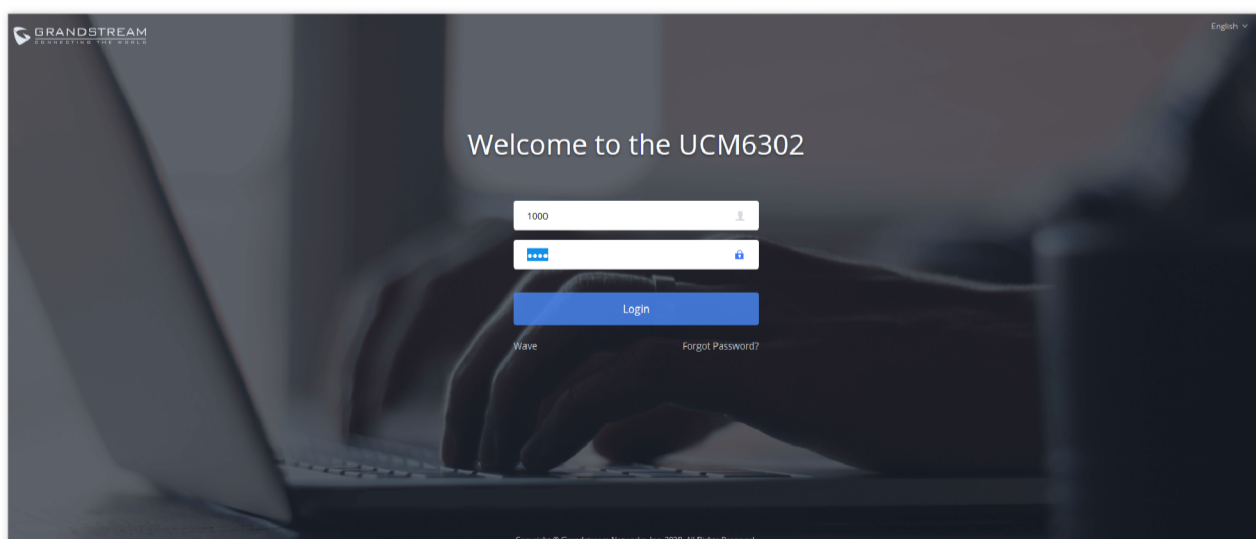
Users could log into their web GUI portal using the extension number and user password. When an extension is created in the UCM630xA, the corresponding user account for the extension is automatically created. The user portal allows access to a variety of features which include user information, extension configuration and CDR as well as settings and managing other 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.

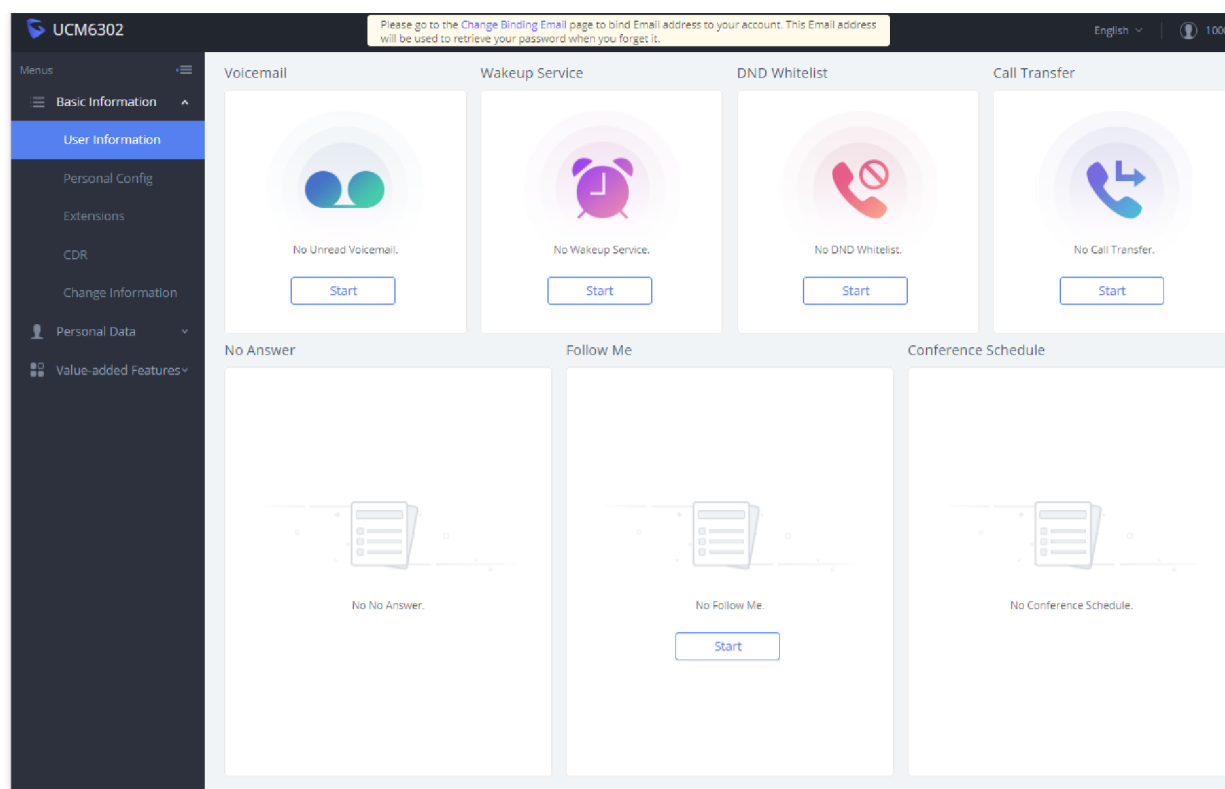
*Edit User Information by Super Admin*

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



*User Portal Login*

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



*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.

## Other Features

On this section, the user has access to manage and use all rich 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 [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 UCM630xA 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.

USERNAME	PRIVILEGE	LAST OPERATION TIME	OPTIONS
admin	Super Administrator	2021-11-05 13:02:11	

User Management Page Display

## User Information

When logged in as Super Admin, click on "Add" to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.

Create a New User

<b>Username</b>	Configure a username to identify the user which will be required in Web GUI login. Letters, digits, and underscore are allowed in the username.
<b>User Password</b>	Configure a password for this user which will be required in Web GUI login. English input is allowed without space, ' and ".
<b>Privilege</b>	This is the role of the Web GUI user. When super admin creates new user, "Administrator" or customized privilege can be selected.
<b>Multi-Factor Authentication</b>	If this authentication is enabled, the user account needs to be verified with an MFA code every time it logs in to enhance the security of the product.
<b>Email Address</b>	Configure the email address for the user. This is optional.

User Management → Create New User

Once created, the Super Admin can edit the users by clicking on



or delete the user by clicking on



USERNAME	PRIVILEGE	LAST OPERATION TIME	OPTIONS
admin	Super Administrator	2021-11-05 13:08:50	
John	Administrator	--	

User Management – New Users

## Multi-Factor Authentication

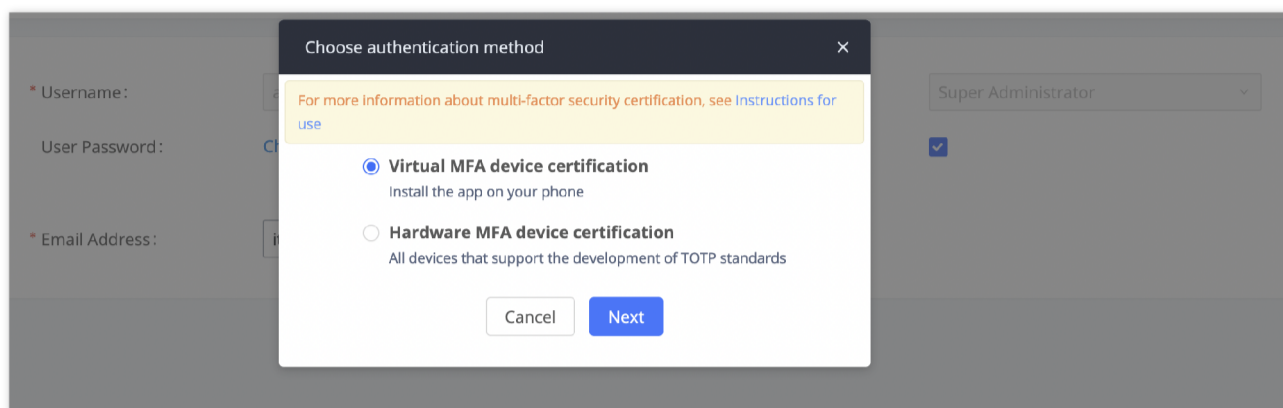
To enhance the security for UCM, super admin and admin can select to use multi-factor authentication method for login to protect the login information. Virtual MFA and hardware MFA are supported and can be selected. Once enabled, the user must use MFA code to verify before login.

### Notes:

- The user cannot enable or disable MFA for another different user.

- Super admin can edit user settings for admin but cannot edit Multi-Factor Authentication option. MFA option is only viewable for super admin when super admin edits other users.
- When the user sees MFA enabled, only this user can disable or enable it again.
- Email address and email settings are required before enabling Multi-Factor Authentication. Please ensure email setting has "Client" type configured. Otherwise, MFA cannot be enabled.

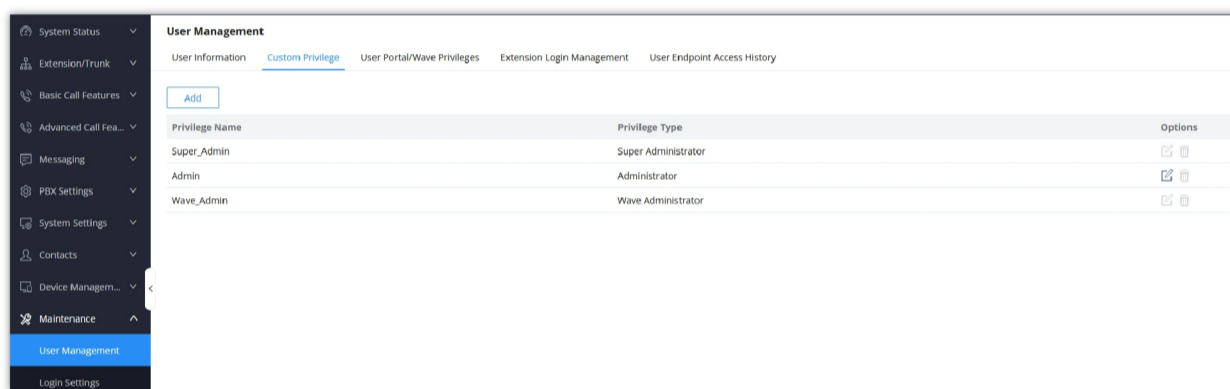
Please refer to MFA how to guide [here](#) for more information.



MFA Settings

## Custom Privilege

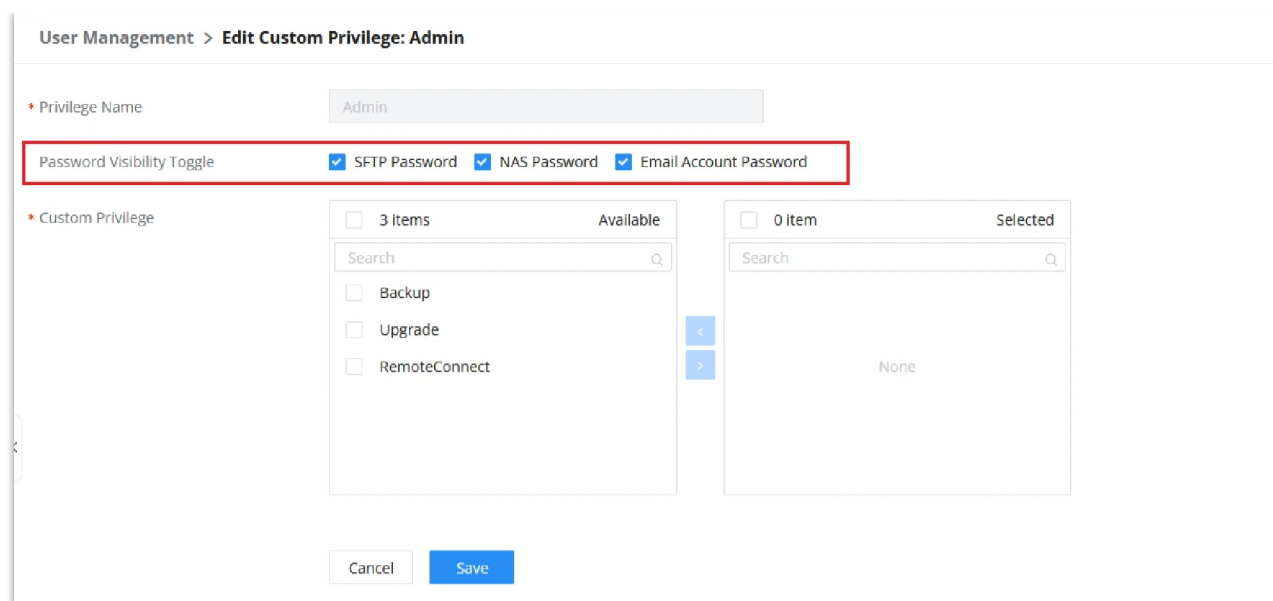
By default, three levels are supported: **Super Administrator, Administrator, Wave Administrator:**



Custom Privilege

## 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**
- The Super Admin can allow administrators to view SFTP, NAS and Email Account passwords by changing the settings on *Password Visibility Toggle*.



Custom Privilege: Admin

## Administrator


- Users with "Admin" privilege can only be created by "Super Admin" user.
- "Admin" privilege users cannot create new users for login.
- "Admin" privilege users are by default not allowed to access the following pages:

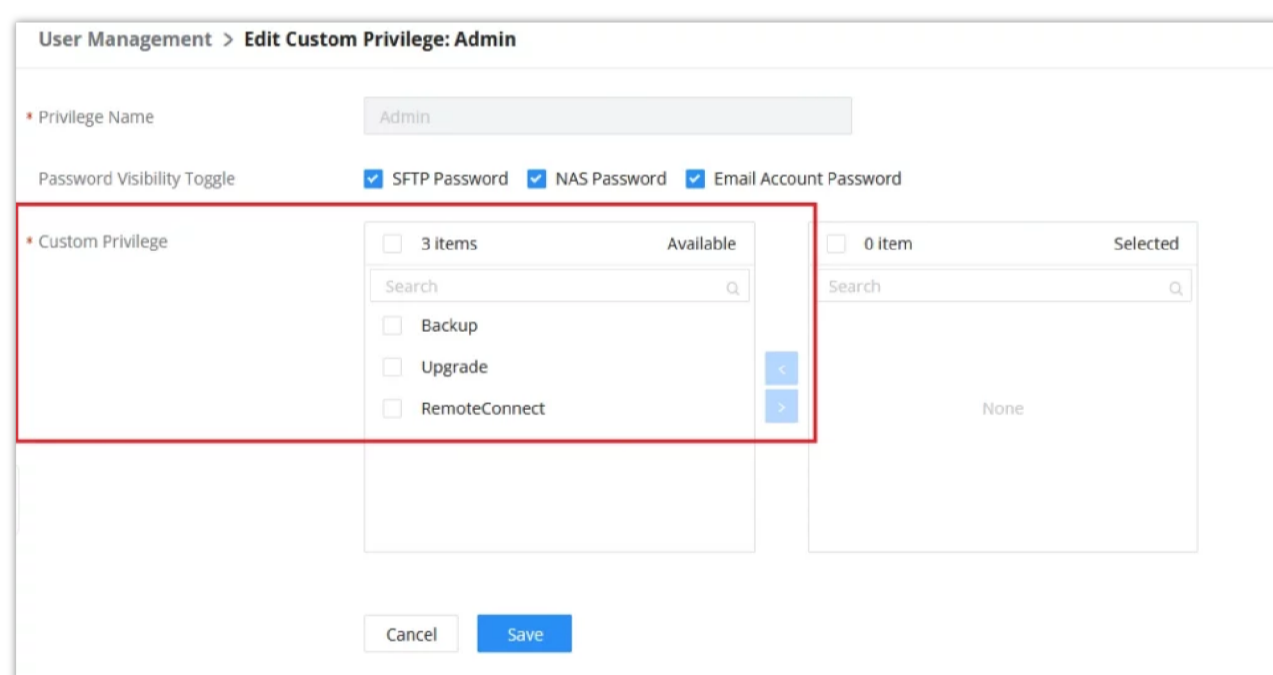
### Maintenance → Backup

### Maintenance → Upgrade

### RemoteConnect

### Settings → User Management → Operation Log

**Note:** By default, administrator accounts are not allowed to access backup menu, but this can be assigned to them by editing the option "**Maintenance > User Management > Custom Privilege**" then press  to edit the "Admin" account and include backup operation permission for these types of users.



Assign Backup permission to "Admin" users

## Wave Administrator

- This permission type does not support editing or deletion.
- This includes management of Wave-related function settings only and does not involve access to the UCM module.
- Users can set the Wave Admin privilege for specific extension under **Extension/Trunk → Extensions → Edit Extension**.

For more information, please refer to the [Wave Administrator Guide](#) guide.

Extensions > Edit Extension: 1000

Basic Settings Media Features Voicemail Custom Time Wave Client Follow Me Advanced Settings

AuthID  Concurrent Registrations 3

Disable This Extension

**User Settings**

First Name  Last Name

Email Address  User/Wave Password \*\*\*\*\*

User Portal/Wave Privileges Wave Administrator  Mobile Number +1

[Add / Edit Privileges](#)

Department Enterprise Root Directory  job Title

**Contact Privileges**

Same as Department Contact Privileges  Contact View Privileges All Contacts [Add / Edit Privileges](#)

Sync Contact

Cancel Save

Extension Settings

## Add Custom Privilege

**User Management**

User Information Custom Privilege User Portal/Wave Privileges Extension Login Management User Endpoint Access History

Add

Privilege Name	Privilege Type	Options
Super_Admin	Super Administrator	<input type="checkbox"/> <input type="checkbox"/>
Admin	Administrator	<input type="checkbox"/> <input type="checkbox"/>
Wave_Admin	Wave Administrator	<input type="checkbox"/> <input type="checkbox"/>

Add Custom Privilege

The Super Admin user can create users with different privileges. 41 items are available for privilege customization.

1. API Configuration
2. Backup
3. Callback
4. Call Queue
5. Queue Statistics
6. Queue Recordings
7. CDR Recordings
8. CDR Records
9. CDR Statistics
10. Dial By Name
11. DISA
12. Emergency Calls
13. Event List
14. Extensions
15. Extension Groups
16. Outbound Routes
17. Inbound Routes
18. Fax/T.38
19. Fax Sending
20. Feature Codes
21. IVR
22. Paging/Intercom
23. Parking Lot

- 24. Pickup Groups
- 25. PMS – Wakeup Service
- 26. Ring Groups
- 27. Restrict Calls
- 28. SCA
- 29. Speed Dial
- 30. System Status
- 31. System Events
- 32. LDAP Server
- 33. Time Settings
- 34. Multimedia Meeting
- 35. Voicemail
- 36. Voice Prompt
- 37. Schedule Call
- 38. PMS – Wakeup Service
- 39. Zero Config
- 40. Announcement
- 41. UCM RemoteConnect

**User Management > Create New Custom Privilege**

\* Privilege Name

\* Custom Privilege

<input type="checkbox"/> 40 Available	<input type="checkbox"/> 0 Selected
<input style="width: 95%;" type="text" value="Search"/>	<input style="width: 95%;" type="text" value="Search"/>
<input type="checkbox"/> API Configuration <input type="checkbox"/> Backup <input type="checkbox"/> Callback <input type="checkbox"/> Call Queue <input type="checkbox"/> Queue Statistics <input type="checkbox"/> Queue Recordings	None

*Create New Custom Privilege*

Log in UCM630xA as super admin and go to **Maintenance→User Management→Custom Privilege**, create privilege with customized available modules.

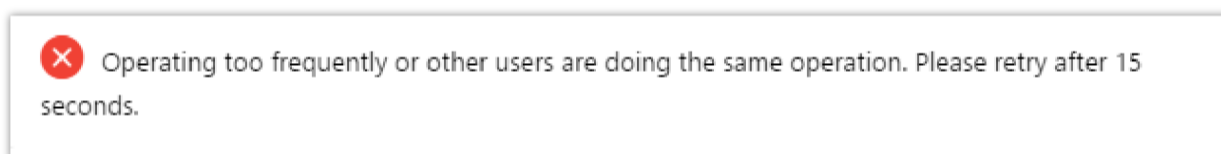
When you add CDR Records and CDR Recording Files custom privileges, additional privileges will appear (All Deletion of CDR and Allow Deletion of DCR Recordings , respectively). This offers more flexibility on the privileges that the admin assigns to the user.

Allow Deletion of CDR and CDR Recordings

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 UCM630xA. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on “Apply Changes”), a prompt will pop up as shown in the following figure.



Multiple User Operation Error Prompt

### User Portal/Wave Privileges

The user can create customize privileges related to an extension’s User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.

User Portal/Wave Privileges

### Wave Permissions

- **Chat:** Toggles ability to use the Wave Chat feature.
  - **Delete Chat:** Toggles support for Wave to delete chats and chat history. This data will only be deleted on the Wave client side.
  - **Send File:** Toggles file/image sending support in Wave chat. If disabled, users will still be able to download, view and forward chat files.
  - **Download Chat Logs:** If enabled, chat logs will be downloadable from the Wave client, including chat logs from Wave/WhatsApp/Telegram/LiveChat sessions.
- **End-to-End Encrypted Chat\*:** Toggles ability to use the Wave End-to-End Encrypted Chat feature.
- **Video Call:** Toggles ability to use the Wave Video Call feature.
- **Meeting:** Toggles ability to use the Wave Meeting feature.
  - **Start Video During Meeting:** Toggles ability to use the Wave Start During Meeting feature.
- **Online Status:** Toggles ability to set Wave online status such as "Busy", "Appear Away", "Do Not Disturb", "Appear Offline", etc. If unchecked, the status will be displayed as only either "Online" or "Idle".
- **Remote Logout:** If enabled, Wave users will be able to log out of their accounts from other logged-in devices.
- **Clear Recent Call History:** Toggles ability to delete recent call history entries and entire recent call history on Wave.
- **Application:** Toggles ability to access the "Applications" page under Wave Desktop and Wave Web.
- **Smart Devices:** Toggling off privileges will hide the corresponding pages and options in Wave.
  - **Door System**
  - **Monitor**
  - **Call Device (CTI)**
- **3rd Party Applications**
  - **App Store:** Toggles ability to access the Wave App Store. If unchecked, the App Store will be hidden, but installed apps can still be used.
  - **Pre-installed Apps\*:** Configure Wave pre-installed add-ins and related settings.

#### User Portal/Wave Privileges

- **Account Settings:** If unchecked, the *User Portal -> Basic Information -> Account Settings* page and the *Wave -> Sidebar -> User -> Account Settings* option will be hidden.
- **Extension Settings:** If unchecked, the extension's *User Portal->Basic Information->Extensions* page and the *Wave->Sidebar->User->Call Settings* option will be hidden.
  - **Do Not Disturb:** Toggles ability to set DND through the User Portal.
  - **SIP/IAX Password & AuthID:** Toggles ability to access the **SIP/IAX Password** and **AuthID** settings under the *User Portal->Basic Information->Extensions->Basic Settings* page.
  - **Configuration Voicemail**
- **Manage Recordings:** Toggles ability to view recordings through the User Portal and Wave, including the recordings in call logs, meeting details, and Wave application.
  - **Deleting Recordings:** Toggles ability to delete recordings through the User Portal and Wave. For Wave, this includes the ability to delete call logs, meeting details, and recordings.
- **Personal Data:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - CDR
  - Follow Me
  - Voicemail
  - Recordings files
  - Fax Files
  - SCA
- **Other Features:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - Fax Sending
  - Call Queue
  - Schedule Call

\*: Features which are marked by an asterisk are a part of RemoteConnect plans.

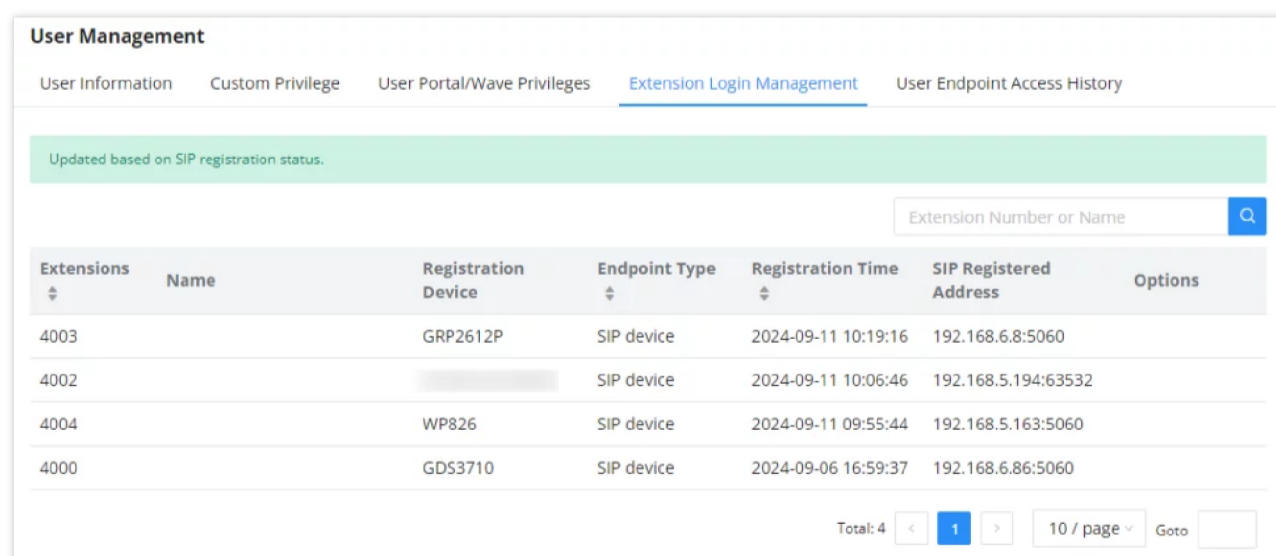
## User Portal/Wave Privileges

- **Account Settings:** If unchecked, the *User Portal > Basic Information > Account Settings* page and the *Wave > Sidebar > User > Account Settings* option will be hidden.
- **Extension Settings:** If unchecked, the extension's *User Portal->Basic Information->Extensions* page and the *Wave > Sidebar > User > Call Settings* option will be hidden.
  - **Do Not Disturb:** Toggles ability to set DND through the User Portal.
  - **SIP/IAX Password & AuthID:** Toggles ability to access the **SIP/IAX Password** and **AuthID** settings under the *User Portal > Basic Information > Extensions > Basic Settings* page.
  - **Configuration Voicemail**
- **Manage Recordings:** Toggles ability to view recordings through the User Portal and Wave, including the recordings in call logs, meeting details, and Wave Application tab.
  - **Delete Recordings:** Toggles ability to delete recordings through the User Portal and Wave. For Wave, this includes the ability to delete call logs, meeting details, and recordings.
- **Personal Data:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - CDR
  - Follow Me
  - Voicemail
  - Recordings files
  - Fax Files
  - SCA
- **Other Features:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - Fax Sending
  - Call Queue
  - Schedule Call

\*: Features which are marked by an asterisk are a part of RemoteConnect plans.

## Extension Login Management

Extension Login Management allows the administrator to review the logged-in sessions of SIP devices and Wave.



Extensions	Name	Registration Device	Endpoint Type	Registration Time	SIP Registered Address	Options
4003		GRP2612P	SIP device	2024-09-11 10:19:16	192.168.6.8:5060	
4002			SIP device	2024-09-11 10:06:46	192.168.5.194:63532	
4004		WP826	SIP device	2024-09-11 09:55:44	192.168.5.163:5060	
4000		GDS3710	SIP device	2024-09-06 16:59:37	192.168.6.86:5060	

Extension Login Management

For Wave sessions, the administrator can click on  to terminate a Wave session. SIP sessions cannot be logged out.

## User Endpoint Access History

The User Endpoint Access History tab allows the administrator to view the access history of all extensions, the time on which the access has occurred, the IP addresses from which the extensions were accessed, and whether they were accessed from the User Portal, Wave Web/Desktop, or mobile. Extension access from the SIP endpoints won't be logged in this page.

User Management					
User Information	Custom Privilege	User Portal/Wave Privileges	User Endpoint Access History		
EXTENSIONS	NAME	EXTENSION TYPE	TERMINAL TYPE	LAST OPERATION TIME	IP ADDRESS
1000		SIP(WebRTC)	Android/iOS	2022-11-14 18:15:35	192.168.5.137
1001	Arthur Morgan	SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-11-11 10:18:22 2022-11-14 16:10:37 2022-08-10 09:26:40	192.168.5.119 192.168.5.76 192.168.5.111
1002	Bonnie MacFarlan	SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-11-11 10:18:22 2022-11-14 16:53:03 2022-08-23 15:49:30	192.168.5.93 192.168.5.79 192.168.5.111
1003	Catherine Braitwaite	SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-10-18 14:14:12 2022-11-14 20:34:59 2022-11-17 09:19:44	192.168.5.111 192.168.5.76 192.168.5.168
1004	John Marston	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-08-16 15:32:37 2022-11-16 11:26:44	192.168.5.111 192.168.5.91
1005	Abigail Roberts	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-11-16 17:42:47 2022-11-16 18:11:34	192.168.5.79
1006	Mary-Beth Gaskill	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-11-16 16:21:14 2022-11-16 17:37:50	192.168.5.165 192.168.5.79
1007	Hosea Matthews	SIP(WebRTC)	Wave Web/Desktop	2022-11-16 17:50:35	192.168.5.63

Total: 8    10 / page    Goto 1

Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.

## Login Settings

### Change Password

After logging in the UCM630xA 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.

Login Settings

[Change Password / Email](#)    Login Security

---

\* Enter Old Password:

**Change Password**

Change Password:

\* Enter New Password:

\* Re-enter New Password:

**Change Username**

Change Username:

**Change Binding Email**

\* Email Address:  [Email Template](#)

<b>Enter Old Password</b>	Enter the Old Password for UCM630xA
<b>Change Password</b>	Enable Change Password
<b>Enter New Password</b>	Enter the New Password for UCM630xA

<b>Re-enter New Password</b>	Retype the New Password for UCM630xA
<b>Change Username</b>	Enable Change Username
<b>Please enter the username</b>	Enter the Username
<b>Email Address</b>	The Email address is the User Email Address. It is used for receiving password information if the user forgets his password.

*Change Password*

## Change Username

UCM630xA allows users now to change Super Administrator username.

**Change Username**

Change Username:

\* Please enter the username:

*Change Username*

## Change binding Email

UCM630xA allows user to configure binding email in case login password is lost. UCM630xA login credential will be sent to the designated email address. The feature can be found under Web GUI → **Maintenance** → **Login Settings** → **Change Password / Email**

**Change Binding Email**

\* Email Address:  [Email Template](#)

*Change Binding Email*

<b>Email Address</b>	Email Address is used to retrieve password when password is lost
----------------------	--

*Change Binding Email option*

## Login Security

After the user logs in the UCM630X Web GUI, the user will be automatically logged out after certain timeout, or he/she can be banned for a specific period if the login timeout is exceeded. Those values can be specified under UCM630X 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.

### Login Settings

Change Password / Email [Login Security](#) Remote Login

---

#### Login Settings

\* Login Timeout (m)  0 indicates no automatic logout.

SMS OTP Login

#### Login Security Policy

Enable Login Security

\* Max Login Attempts (IP)

\* Maximum number of login attempts

\* Ban Period (m)  0 indicates a permanent ban after exceeding the max number of failed login attempts.

#### Login Banned IP/User List

[Banned](#) [Ban History](#)

IP Address	Username	Banned Time	Estimated Ban Lift Time	Options
No data				

#### Login Allowlist

---

*Login Timeout Settings*

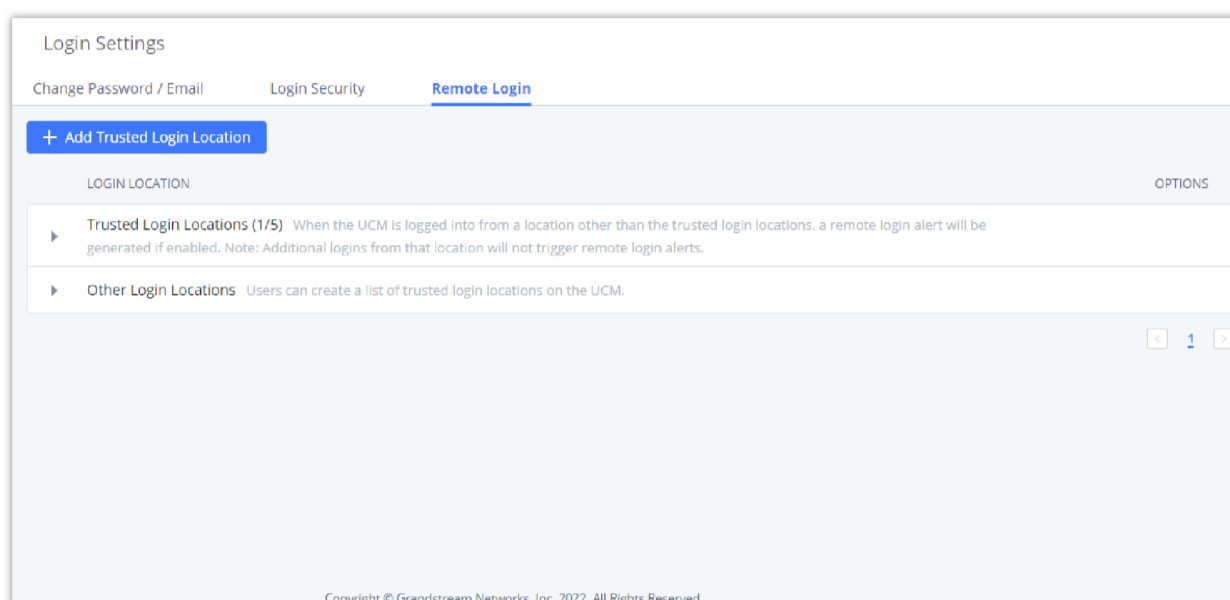
Login Settings	
<b>Login Timeout (m)</b>	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. If set to 0, the user will not be logged out automatically. Valid range is 0 to 60 and default value is 0.
<b>SMS OTP Login</b>	If enabled, users will be able to log in and reset password via SMS verification code. Mobile phone numbers will need to be configured for administrators and extensions.
Login Security Policy	
<b>Enable Login Security</b>	Enable login security measure to prevent authentication attacks.
<b>Max Login Attempts (per IP address)</b>	The max allowed number of consecutive failed login attempts from an IP address. Once exceeded, no users will be able to log in from that IP address. <b>Note:</b> The valid range is between 5 to 100 attempts.
<b>Maximum number of login attempts (per user)</b>	The maximum number of consecutive failed login attempts. When exceeded, the user will not be able to log in for the amount of time specified in "User ban period". <b>Note:</b> The valid range is between 1 to 100 attempts.
<b>Ban Period (m)</b>	The amount of minutes that a user will be banned for after exceeding the maximum allowed number of consecutive failed login attempts. <b>Note:</b> The valid range is between 0 and 10000 minutes, with 0 indicating a permanent ban.
<b>Login Banned User List</b>	List of IP addresses which are banned from making any further login attempts.
<b>Login Whitelist</b>	List of IP addresses which can make unlimited login attempts.

## Remote Login

This feature allows the user to manage trusted login locations, also, verifying where login sessions were initiated from, this is very important since, in this type of scenario, the UCM6300 would be directly connected to the Internet, and the public IP address would be used for the remote login. This feature adds a layer of visibility and control, thus enhancing the security of the UCM.

In this tab there are two types of lists of locations:

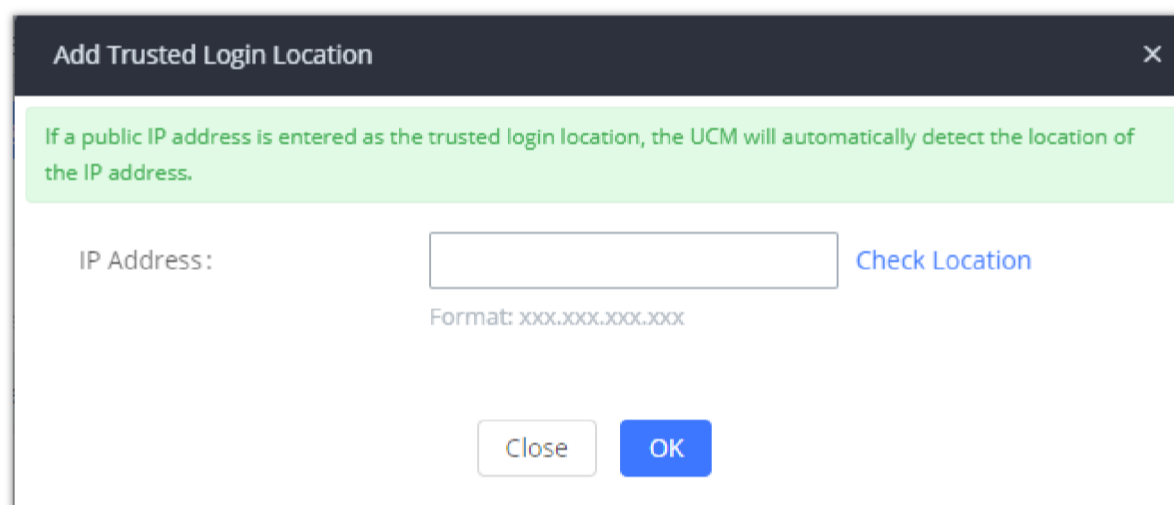
- Trusted Login Locations: These are the trusted login locations that are added manually by the admin. Any added trusted login location will not generate any remote login alert upon the first time login.
- Other Login Location: This list will show all the remote login locations that are not trusted, logging in for the first time from an untrusted login location will generate an alert, but the subsequent remote logins from the same location will not generate alerts.



*Remote Login*

To add a trusted login location, the user must click on

[+ Add Trusted Login Location](#)



*Trusted Login Location Address*

Then add the public IP address of the location, click on "**Check Location**" to verify if it's the correct location then click "**OK**".

#### **Note**

The system administrator can add up to 5 Trusted Login Locations, while Other Login Locations can have an unlimited number of entries.

## Operation Log

Super Admin has the authority to view operation logs on UCM630xA 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".

DATE	USERNAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
2022-08-04 15:48:02	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 15:47:53	admin	192.168.5.111	Wrong account or password!	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 15:47:43	admin	192.168.5.111	Wrong account or password!	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 15:17:52	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 14:44:19	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 14:26:53	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 14:14:39	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2022-08-04 12:26:36	admin	192.168.5.111	This trusted login location already exists.	addCommonLoginAddr	Details	<a href="#">Click to modify notes</a>
2022-08-04 12:26:26	admin	192.168.5.111	This trusted login location already exists.	addCommonLoginAddr	Details	<a href="#">Click to modify notes</a>
2022-08-04 12:15:54	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>

### 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.

### Operation Log Column Header

<b>Date</b>	The date and time when the operation is executed.
<b>Username</b>	The username of the user who performed the operation
<b>IP Address</b>	The IP address and geographical location from which the operation has been made.
<b>Results</b>	The result of the operation.
<b>Page Operation</b>	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
<b>Specific Operation</b>	Click on the hyperlinked operation detail to reveal more details.
<b>Remark</b>	Allows users to add notes and remarks to each operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on "Display Filter".

Operation Log

Start Time: 2019-12-10 00:00

End Time: 2019-12-11 00:00

IPv4/IPv6 Address:

User Name: admin

[Filter](#) [Reset](#)

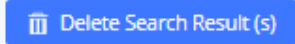
[Delete Search Result \(s\)](#) [Clear](#) [Download Search Result \(s\)](#) [Download All Log](#)

DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
No Data						

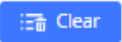
### Operation Logs Filter

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



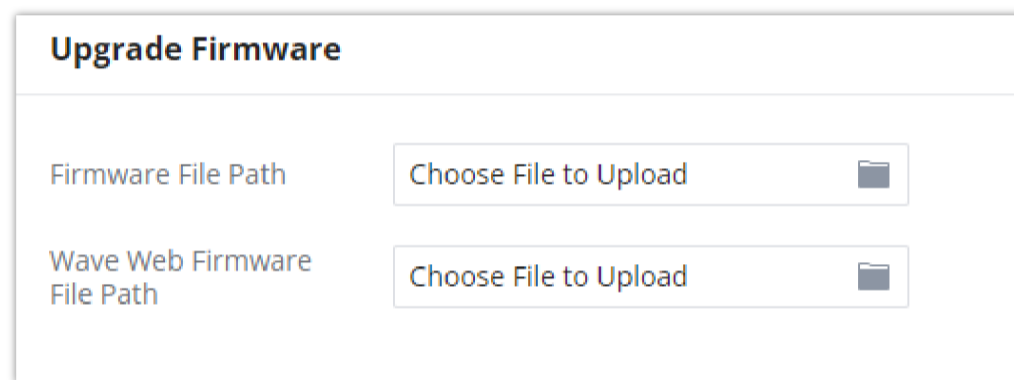
to delete all operation logs at once.

## Upgrading

During its lifetime, the UCM6300 Audio Series models will receive regular updates. These updates include new features and functionalities, bug fixes, security patches, and general improvements to the security and performance of the device. It is highly recommended that you keep the firmware of your UCM up to date.

Before proceeding with the firmware upgrade, please visit <https://www.grandstream.com/support/firmware> and download the latest firmware available for the UCM. Once the file has been download, please decompress the file, you will get a .bin file, that's the file which will uploaded to the UCM.

To upgrade the firmware of the UCM6300 Audio Series, please access the web UI of the UCM, then navigate to **Maintenance** → **Upgrade**



*Upgrade Firmware*

1. Click on "Choose File to Upload" field in front of "Firmware File Path"
2. Use the window to navigate to where the firmware file is located then select it.
3. Once the firmware file has been selected, the file will be uploaded to the UCM and the upgrade will begin.
4. A prompt will appear to reboot the device to finalize the upgrade.

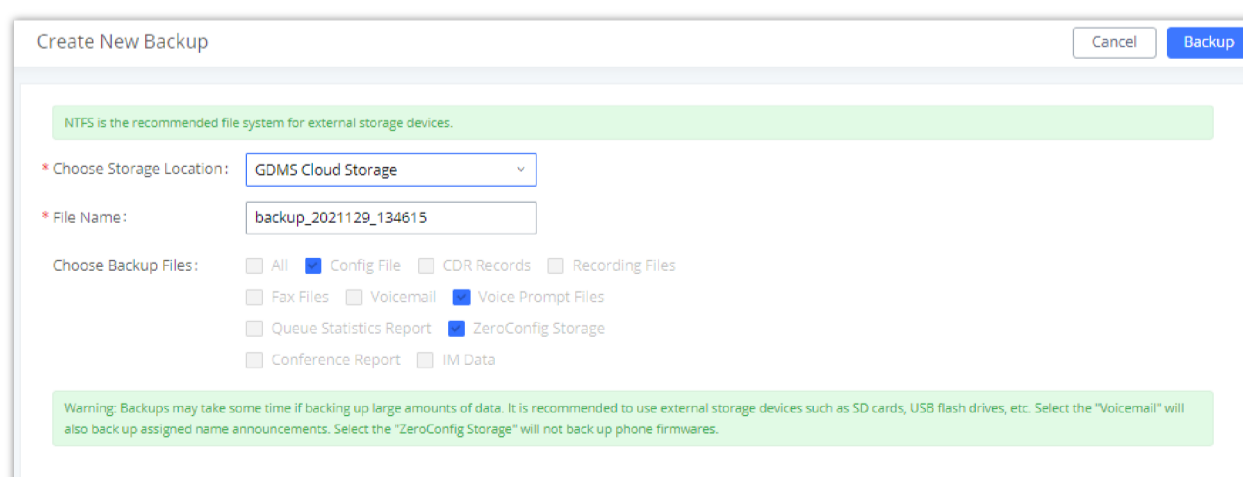
## Backup

The UCM630xA configuration can be backed up locally or via network. The backup file will be used to restore the configuration on UCM630xA when necessary.

## Backup/Restore

Users could backup the UCM630xA 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.






*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, SFTP, 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 UCM630xA internal storage or the external device.

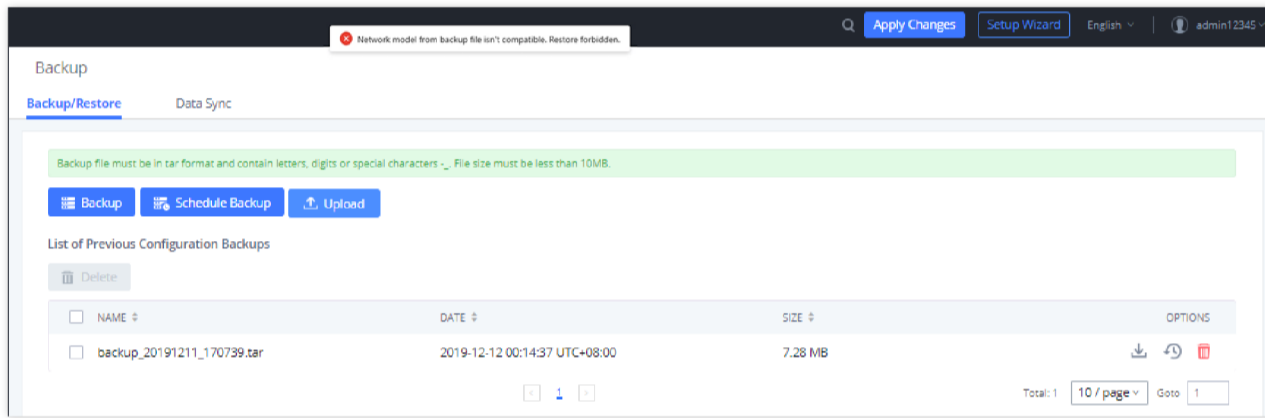
Click on



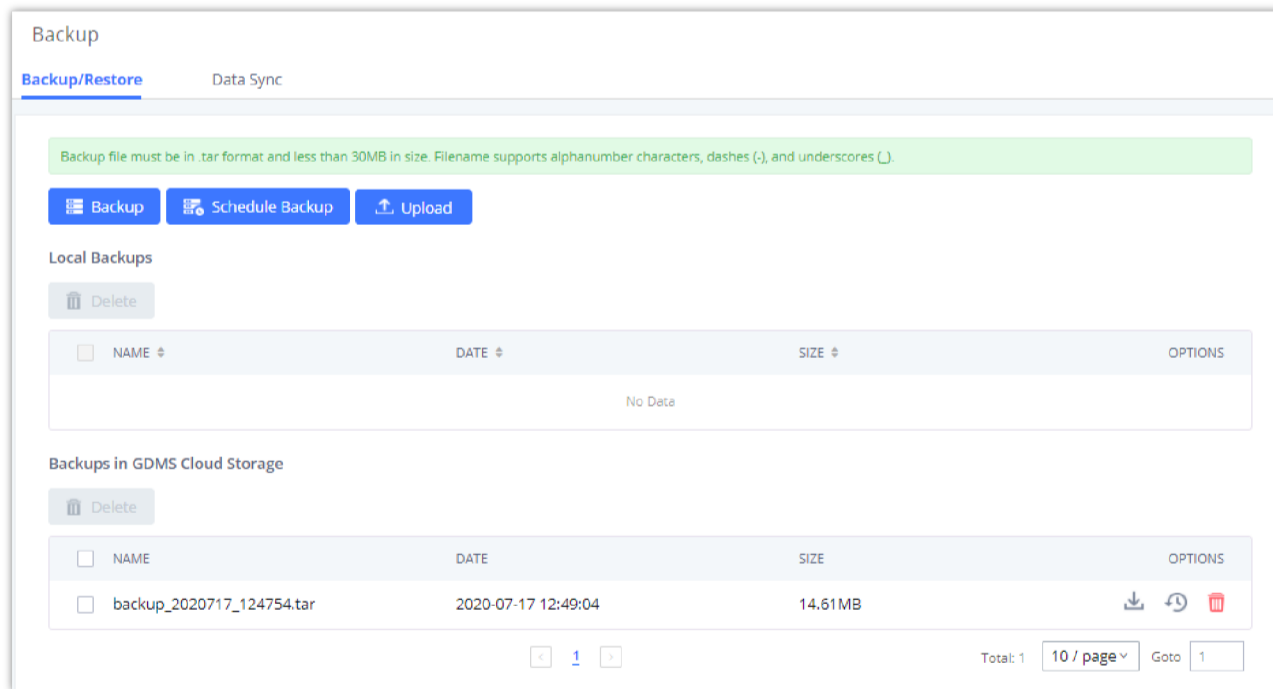
to upload backup file from the local device to UCM630xA. The uploaded backup file will also be displayed in the web page and can be used to restore the UCM630xA.

**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 meeting rooms are compactable before restoring to another UCM model. Otherwise it will prompt a warning and stop the restore process as shown below:

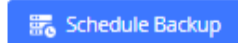


*Restore Warning*



*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.

Schedule Backup

NTFS is the recommended file system for external storage devices.

Enable Scheduled Backup:

Choose Storage Location: SFTP Server

\* Account:

Password:

\* Server Address:

Destination Directory:

\* Backup Time: 00:00

\* Backup Frequency: 1

Choose Backup Files:

All  Config File  CDR Records  Recording Files

Voicemail  Voice Prompt Files  Queue Statistics Report

ZeroConfig Storage  Conference Report

+ Test Connection

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, UCM630xA will create the directory automatically

Backup

Backup/Restore **Data Sync**

Use SFTP to automatically sync CDR, recordings, voicemail, CDR, and fax every day.

Data Sync Configuration

Enable Data Sync:

Choose Data Sync Files:

CDR Records  Recording Files

Voice Mail  Fax

\* Account: test@domain.local

Password:

\* Server Address: 192.168.5.121

Destination Directory:

\* Sync Time: 05:00

+ Test Connection + Synchronize All Data

Data Sync Log

Clean

No record to view

Data Sync

### Data Sync Configuration

<b>Enable Data Sync</b>	Enable the auto data sync function. The default setting is "No".
<b>Account</b>	Enter the Account name on the SFTP backup server.
<b>Password</b>	Enter the Password associate with the Account on the SFTP backup server.
<b>Server Address</b>	Enter the SFTP server address.

<b>Destination Directory</b>	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.
<b>Sync Time</b>	Enter 0-23 to specify the backup hour of the day.

Before saving the configuration, users could click on

[+ Test Connection](#)

. The UCM630xA will then try connecting the server to make sure the server is up and accessible for the UCM630xA. 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 UCM630xA 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 UCM630xA.

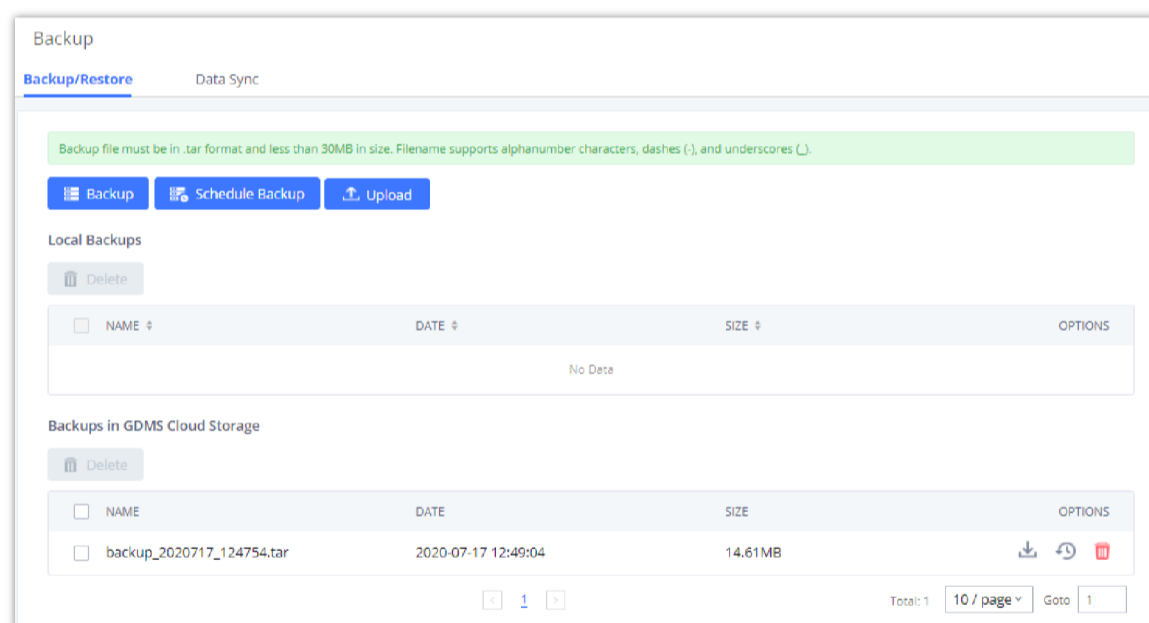
- If the backup was stored on GDMS, it will be displayed under Backups GDMS Cloud Storage, that can be restored by clicking on



- If users have other backup files on PC to restore on the UCM630xA, click on "Upload Backup File" first and select it from local PC to upload on the UCM630xA. 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.



Restore UCM630xA from Backup File

### Note

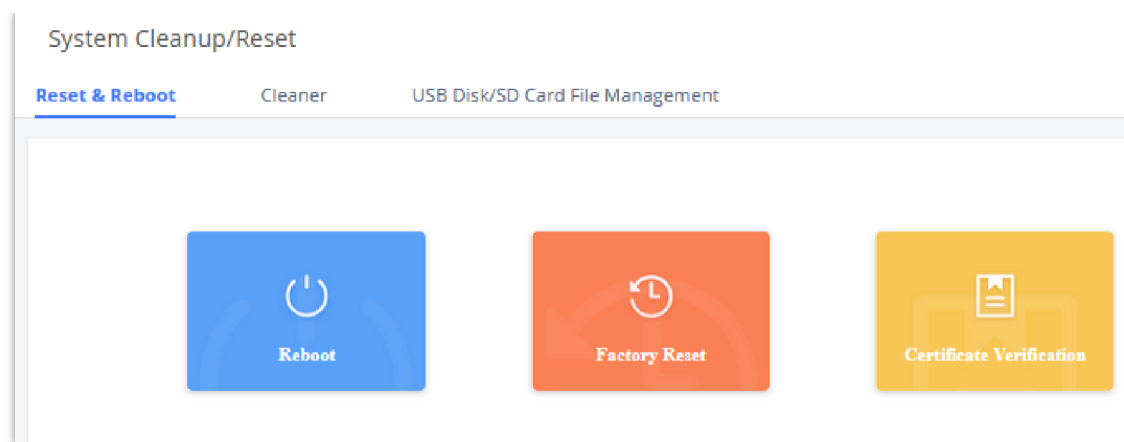
The uploaded backup file must be a tar file with no special characters like \*,!,#,@,&,\$,%,^,(,),/, \space in the file name. The uploaded back file size must be under 10MB.

## 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.



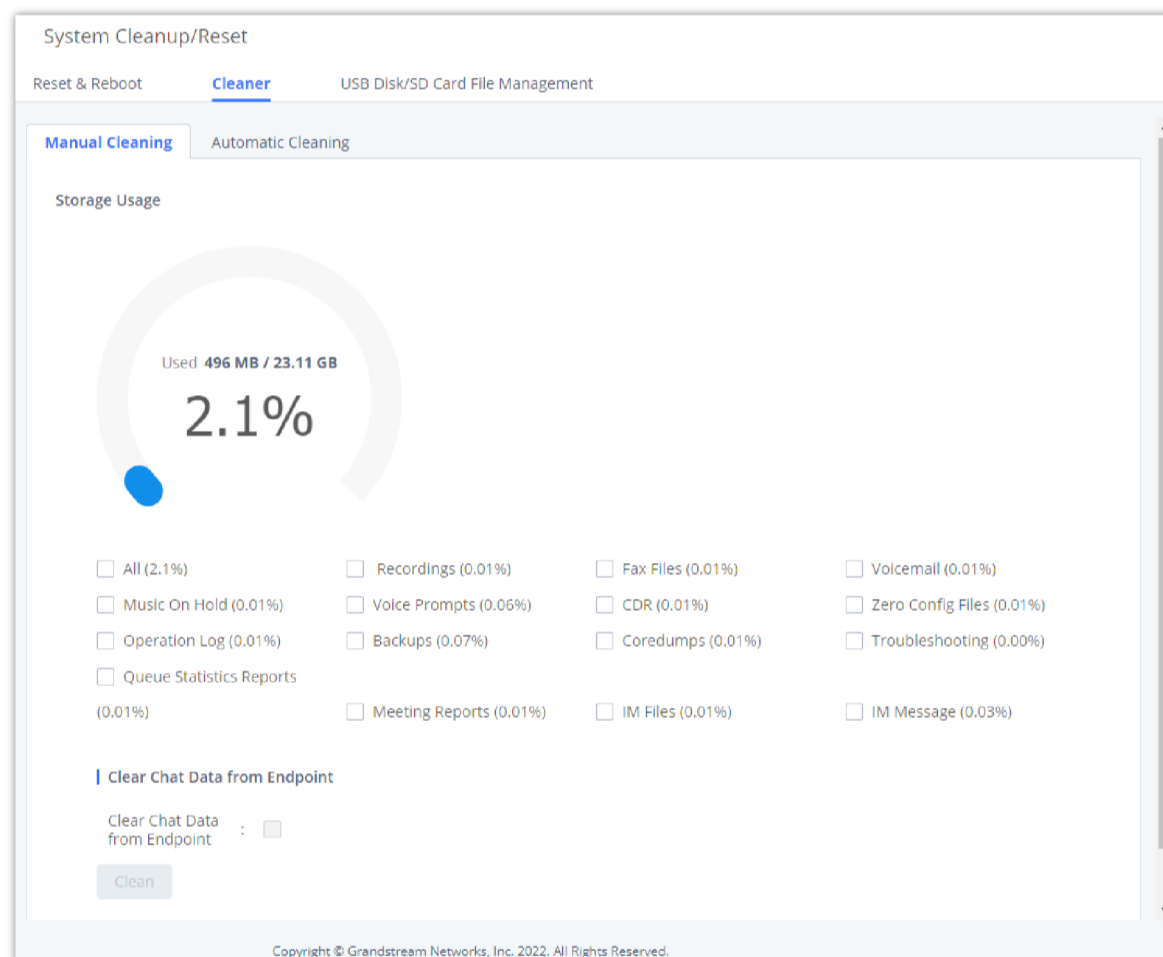
*Reset and Reboot*

- 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 UCM630xA.



*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, Meeting 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 UCM630xA.

Manual Cleaning | **Automatic Cleaning**

Clean CDR, recordings, voicemail, and fax automatically.

**CDR Cleaner**

Enable Cleaner:

Clean Time:

Cleaning Conditions:

Clean Interval (d):

**Report Cleaner**

Enable Cleaner:

Cleanup Type:  Queue Statistics Report  Conference Call Statistics Report

Clean Time:

Cleaning Conditions:

Clean Interval (d):

**IM Data Cleaner**

Enable Cleaner:

Cleanup Type:  IM Message  IM Share Files

Clean Time:

Cleaning Conditions:

File Clean Interval (d):

**File Cleaner**

Enable Cleaner:

Clean Files in External Storage:

Choose Cleaner Files:  Basic Call Recording Files  Audio Conference Recording Files  
 Call Queue Recording Files  Voicemail Files  
 Emergency Calls Recording Files  Fax  
 Backup Files  SCA Recording Files

Clean Time:

Cleaning Conditions:

File Clean Threshold:

Keep Last X Days:

**Cleaner Log**

Automatic Cleaning

Automatic Cleaning Configuration

<b>Enable CDR Cleaner</b>	Enable the CDR Cleaner function.
<b>CDR Clean Time</b>	Enter 0-23 to specify the hour of the day to clean up CDR.
<b>Cleaning Conditions</b>	<p><b>By Schedule:</b> If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.</p> <p><b>Keep Last X Records:</b> 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.)</p> <p><b>Keep Last X Days:</b> Delete all entries older than X days.</p>
<b>Clean Interval</b>	Enter 1-30 to specify the day of the month to clean up CDR when <b>By Schedule</b> is selected as <b>Cleaning Conditions</b> .

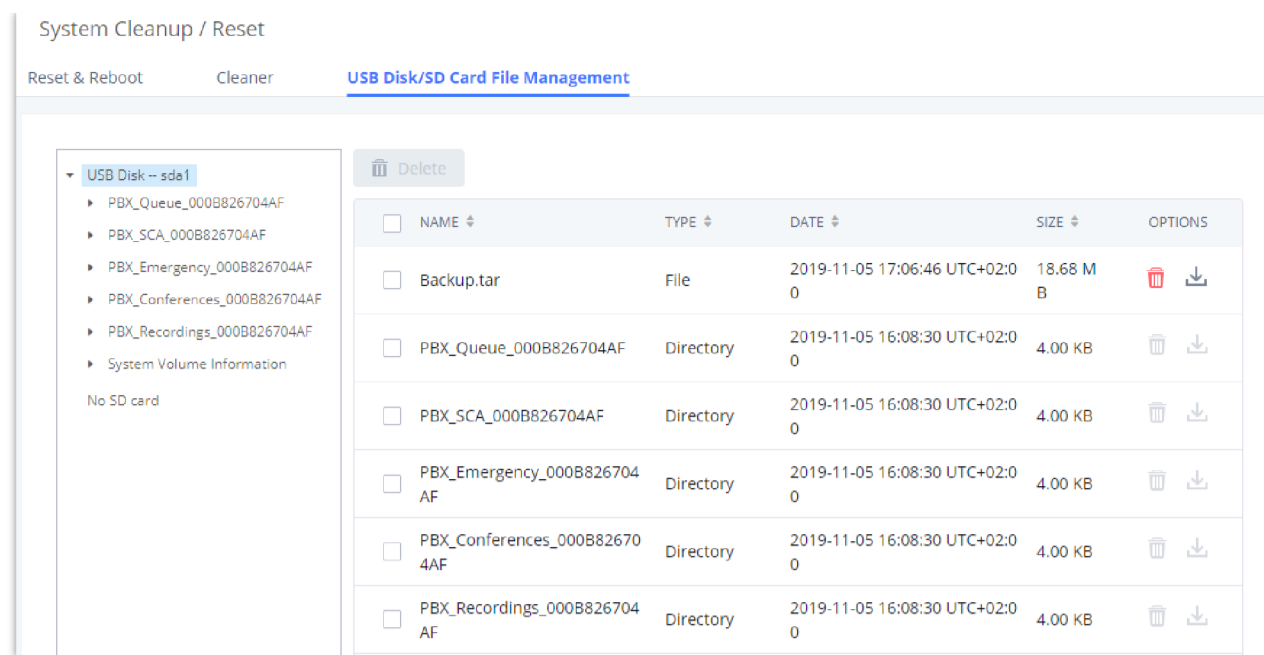
<b>Max Entries</b>	Set the maximum number of CDR entries to keep when <b>Keep Last X Records</b> is selected as <b>Cleaning Conditions</b> .
<b>Keep Last X Day</b>	Enter the number of days of call log entries to keep when <b>Keep Last X days</b> is selected as <b>Cleaning Conditions</b> .
<b>Enable Queue Statistics</b>  <b>Report Cleaner</b>	Enable scheduled queue log cleaning. By default, is disabled.
<b>Queue Statistics Report Cleaner Clean Time</b>	Enter the hour of the day to start the cleaning. The valid range is 0-23.
<b>Cleaning Conditions</b>	<p><b>By Schedule:</b> If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.</p> <p><b>Keep Last X Records:</b> 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.)</p> <p><b>Keep Last X Days:</b> Delete all entries older than X days.</p>
<b>Clean Interval</b>	Enter how often (in days) to clean queue logs when <b>By Schedule</b> is selected as <b>Cleaning Conditions</b> . The valid range is 1-30.
<b>Max Entries</b>	Set the maximum number of Queue Statistics entries to keep when <b>Keep Last X Records</b> is selected as <b>Cleaning Conditions</b> .
<b>Keep Last X Day</b>	Enter the number of days of call log entries to keep when <b>Keep Last X days</b> is selected as <b>Cleaning Conditions</b> .
<b>Enable Meeting Statistics</b>  <b>Report Cleaner</b>	Enable scheduled Meeting log cleaning. By default, is disabled.
<b>Cleaning Conditions</b>	<ul style="list-style-type: none"> <li>○ 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.</li> <li>○ Keep Last X Records: If the max number of Meeting Statistics Report has been reached, Meeting 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.)</li> <li>○ Keep Last X Days: Delete all entries older than X days.</li> </ul>

<b>Clean Interval</b>	Enter how often (in days) to clean queue logs when <b>By Schedule</b> is selected as <b>Cleaning Conditions</b> . The valid range is 1-30.
<b>Max Entries</b>	Set the maximum number of Meeting Statistics Report entries to keep when <b>Keep Last X Records</b> is selected as <b>Cleaning Conditions</b> .
<b>Keep Last X Day</b>	Enter the number of days of call log entries to keep when <b>Keep Last X days</b> is selected as <b>Cleaning Conditions</b> .
<b>Enable File Cleaner</b>	Enter the Voice Records Cleaner function.
<b>Clean Files in External Device</b>	If enabled the files in external device (USB/SD card) will be atomically cleaned up as configured.
<b>Choose Cleaner File</b>	Select the files for system automatic clean. <ul style="list-style-type: none"> <li>○ Basic Call Recording Files.</li> <li>○ Meeting Recording Files.</li> <li>○ Call Queue Recording Files.</li> <li>○ Voicemail Files.</li> <li>○ Backup Files.</li> </ul>
<b>Clean time</b>	Enter the hour of the day to start the cleaning. The valid range is 0-23.
<b>Cleaning Conditions</b>	<ul style="list-style-type: none"> <li>○ By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to delete all files.</li> <li>○ 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.</li> <li>○ Keep Last X Days: Delete all files older than X days.</li> </ul>
<b>File Clean Interval</b>	Enter 1-30 to specify the day of the month to clean up the files.
<b>File Clean Threshold</b>	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.
<b>Keep Last X Days</b>	Automatically delete all recordings older than this x days when the threshold is reached. If not set, all data is cleared
<b>Cleaner Log</b>	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**.



USB/SD Card Files Cleanup

### USB/SD Card Files Cleanup

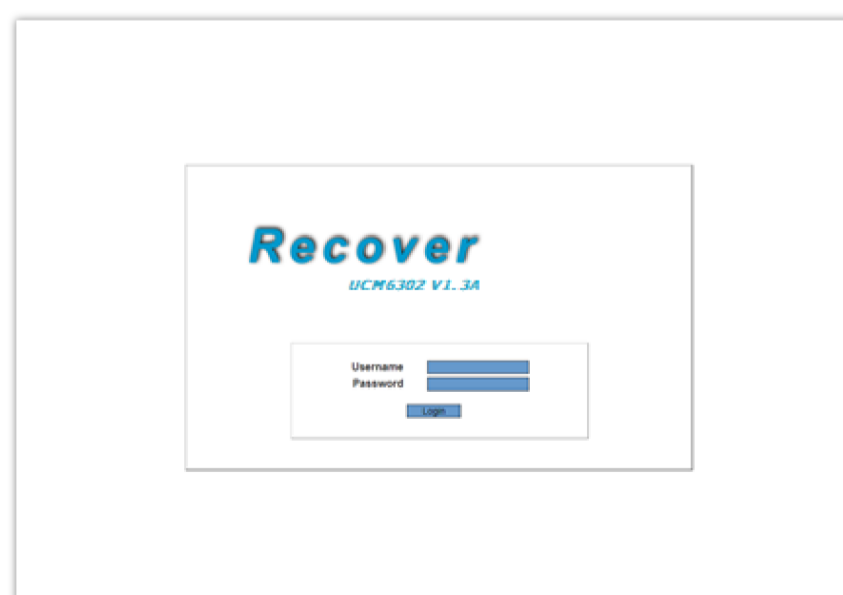
<b>Current Path</b>	Displays the current path.
<b>Directory</b>	Select the directory user want to clean.
<b>Delete Selected File</b>	Select multiple entries to delete from USB or SD card.

## 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.

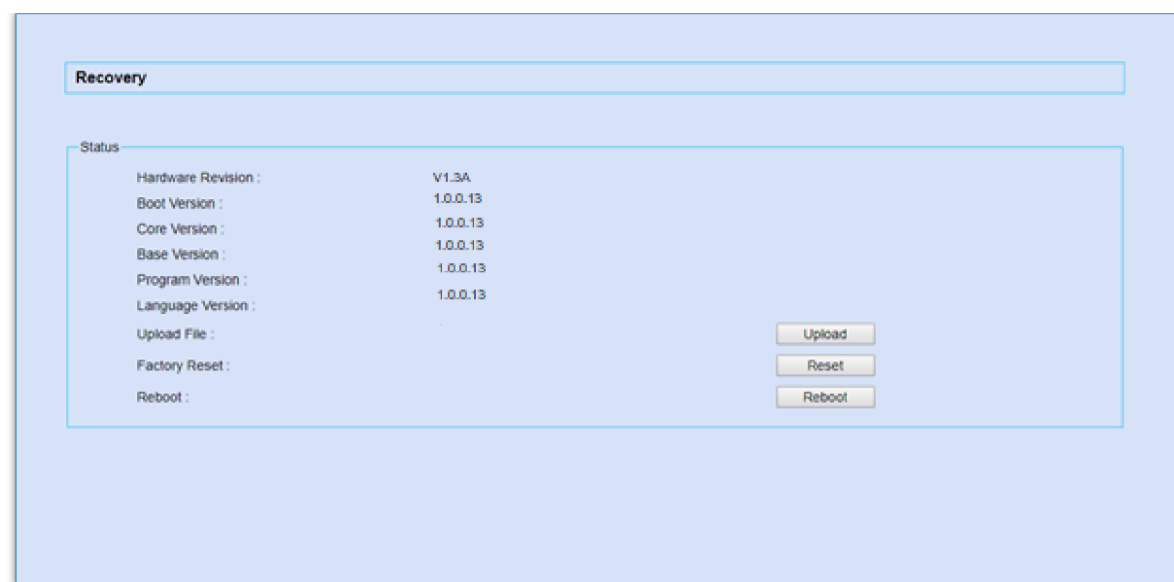
1. To access recovery mode on UCM, please follow below steps:
2. Remove the power from the unit and keep the network cable connected.
3. Press using a PIN the reset button and keep holding.
4. Plug back the power supply while maintaining the reset button pressed.
5. Wait for couple of seconds until you 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:



UCM6302A Recovery Web Page

Make sure to enter the correct admin password, and press login to access the recovery mode page :



Recovery Mode

From here, the user can either upload a firmware file, factory reset or just reboot the device.

## Syslog

On the UCM630xA, 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 UCM630xA settings because it can be helpful to locate the issues when errors happen.

Some typical modules for UCM630xA 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).

### **i** 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 UCM630xA, 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

Ethernet Capture allows capturing the traffic of the UCM for troubleshooting purposes. To access Ethernet Capture feature, please navigate to **Maintenance** → **Network Troubleshooting** → **Ethernet Capture**

**Network Troubleshooting**

[Ethernet Capture](#) | [IP Ping](#) | [Traceroute](#) | [Record Meeting for Diagnosis](#)

EXT4 is the recommended file system for external storage devices.

SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

**Regular Debugging**

Capture Type:

Interface Type:

Capture Filter:

Storage Location:

TLS Key:

**Output Result**

The file has been deleted or does not exist.

**S RTP Debugging**

Enable S RTP Debugging:

*Ethernet Capture*

The capture packets can be stored locally and downloaded for analysis. However, if the user is diagnosing a randomly-occurring issue, he/she can run a continuous packet capture which can be limited by the size of the packet capture and the number of packet capture instances

**Important**

When the maximum packet capture file size is reached, a new packet capture file will be created. When the maximum number of capture files number is reached, then the UCM will delete the oldest file created file and replace it with the new one.

Parameter	Description
<b>Capture Type</b>	Ethernet Capture: Gets a packet capture of all network traffic going through the device. WebSocket Capture: Gets a packet capture of WebSocket protocol. Mainly used for troubleshooting Wave Web calling and conferencing issues.
<b>Interface Type</b>	Select the network interface to monitor.
<b>Capture Filter</b>	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto...).
<b>Storage Location</b>	<ul style="list-style-type: none"> <li>● <b>Local:</b> Store the captured packets in the local storage.</li> <li>● <b>SFTP Server:</b> Save the capture trace to a SFTP server. Please make sure that SFTP is correctly configured under <b>PBX Settings -&gt; Online Storage -&gt; SFTP Server</b></li> <li>● <b>External Storage:</b> Save the capture trace in a usb flash drive or an SD card. This requires that a USB flash drive or SD card to be plugged into the PBX. File formats supported are FAT32 and ExFat.</li> </ul>
<b>Save to External Storage</b>	When or more external storage units are connected to the PBX, the user will be able to pick which one to use. <b>Note:</b> This option is available only when you choose "External Storage" as the storage destination of the capture trace.
<b>Destination Directory</b>	When SFTP is selected, this option will appear. Please enter the directory path in which you would like to store the captured packets.
<b>Packet Capture Size</b>	This option appears only when "External Storage" or "SFTP" options are selected. Define the packet capture size, the option available are: 50MB, 100MB, and 200MB.
<b>Number of Packet Capture</b>	Define the maximum number of the packets captured. The available options are 5, 10, and 20 packets.

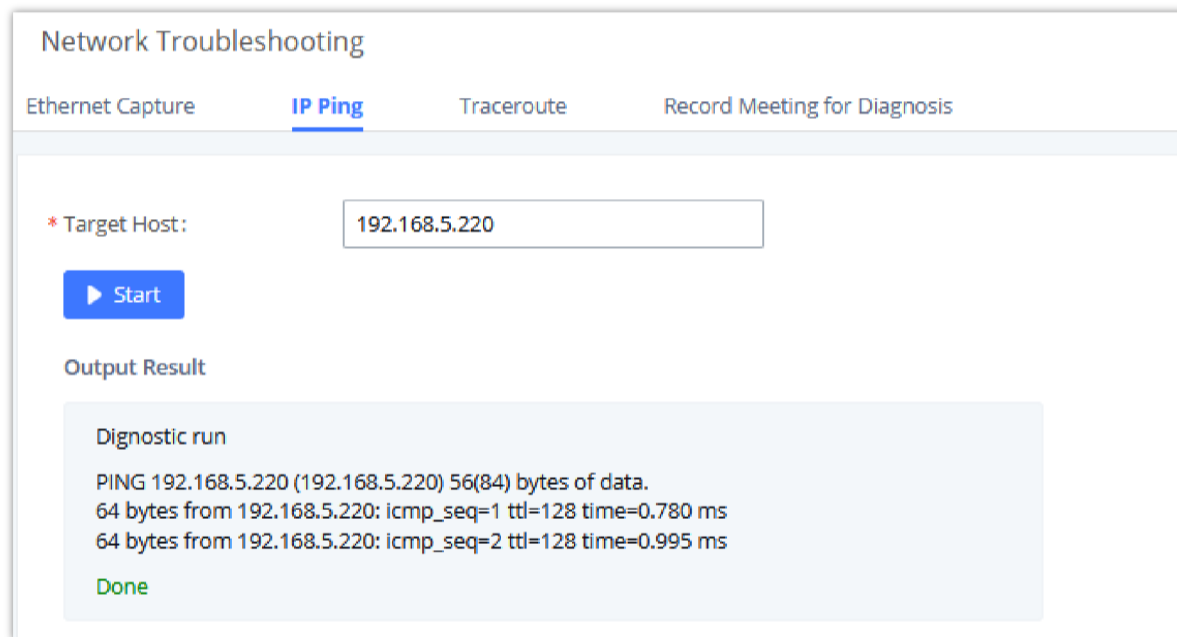
<b>TLS Key</b>	SSL/TLS packets can be decrypted through Wireshark. The packet capture must contain the TLS handshake process.
<b>Start</b>	Start capturing network traffic.
<b>Stop</b>	Stop capturing network traffic.
<b>Download</b>	Download the captured packets. This option can only be used when the captured packets are stored locally.
<b>Enable SRTP Debugging</b>	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.

**i** Capture files saved on external devices will now have "capture" prepended to file names.

## IP Ping

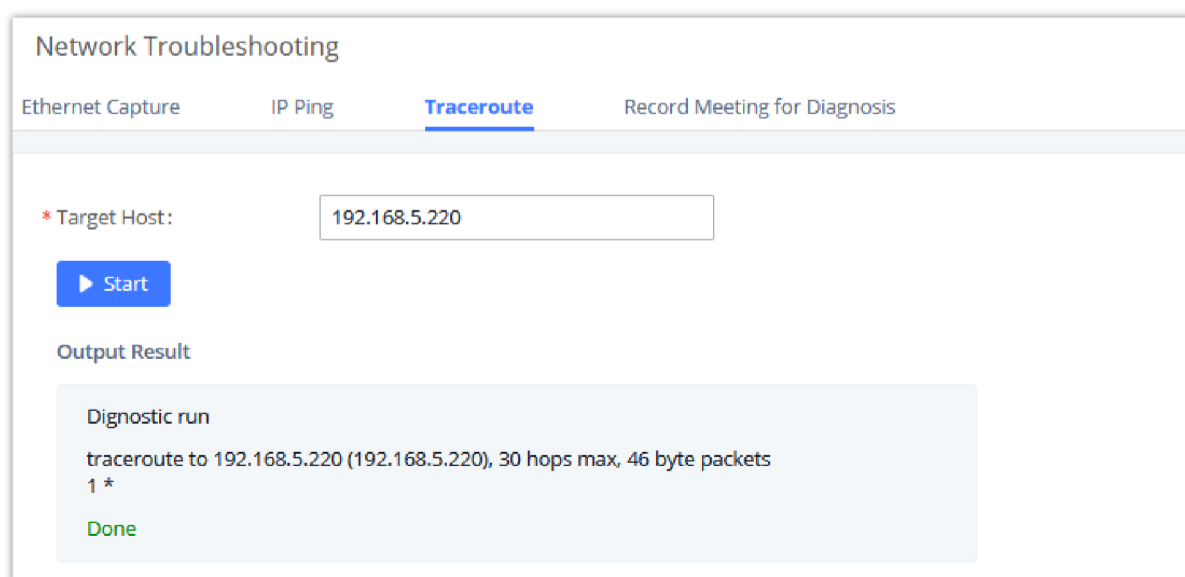
Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



*Ping*

## Traceroute

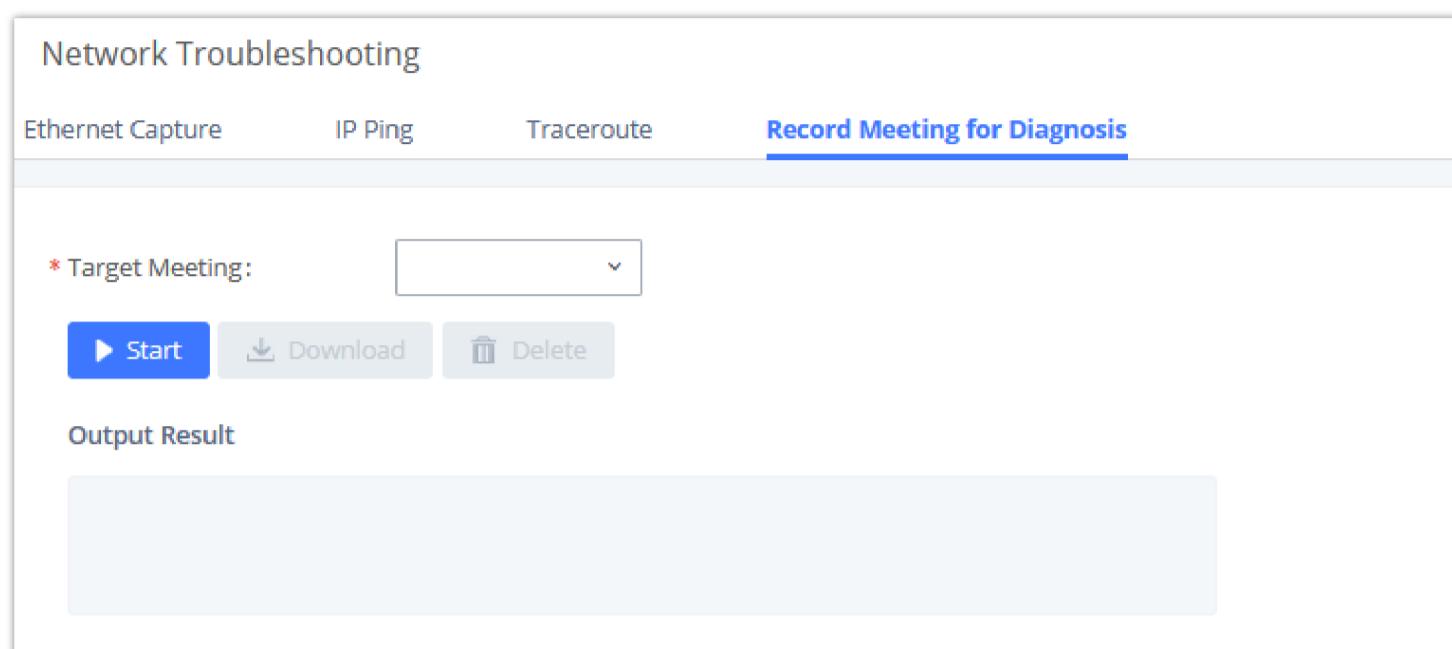
Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



*Traceroute*

## Record Meeting for Diagnosis

Enter the target meeting, support the ongoing meeting, and then click the "Start" button to capture the recording diagnosis of the meeting members in progress. The output result will be automatically displayed below, click the "download" button to download to the local. After the download is complete, immediately click the "Delete" button to clear the system content.



The screenshot shows a web interface titled "Network Troubleshooting". It has four tabs: "Ethernet Capture", "IP Ping", "Traceroute", and "Record Meeting for Diagnosis" (which is selected and underlined). Below the tabs, there is a form with a label "\* Target Meeting:" followed by a dropdown menu. Below the dropdown are three buttons: "Start" (blue with a play icon), "Download" (grey with a download icon), and "Delete" (grey with a trash icon). Below the buttons is a section labeled "Output Result" with a large, empty light blue rectangular area.

*Record Meeting for Diagnosis*

## Signaling Troubleshooting

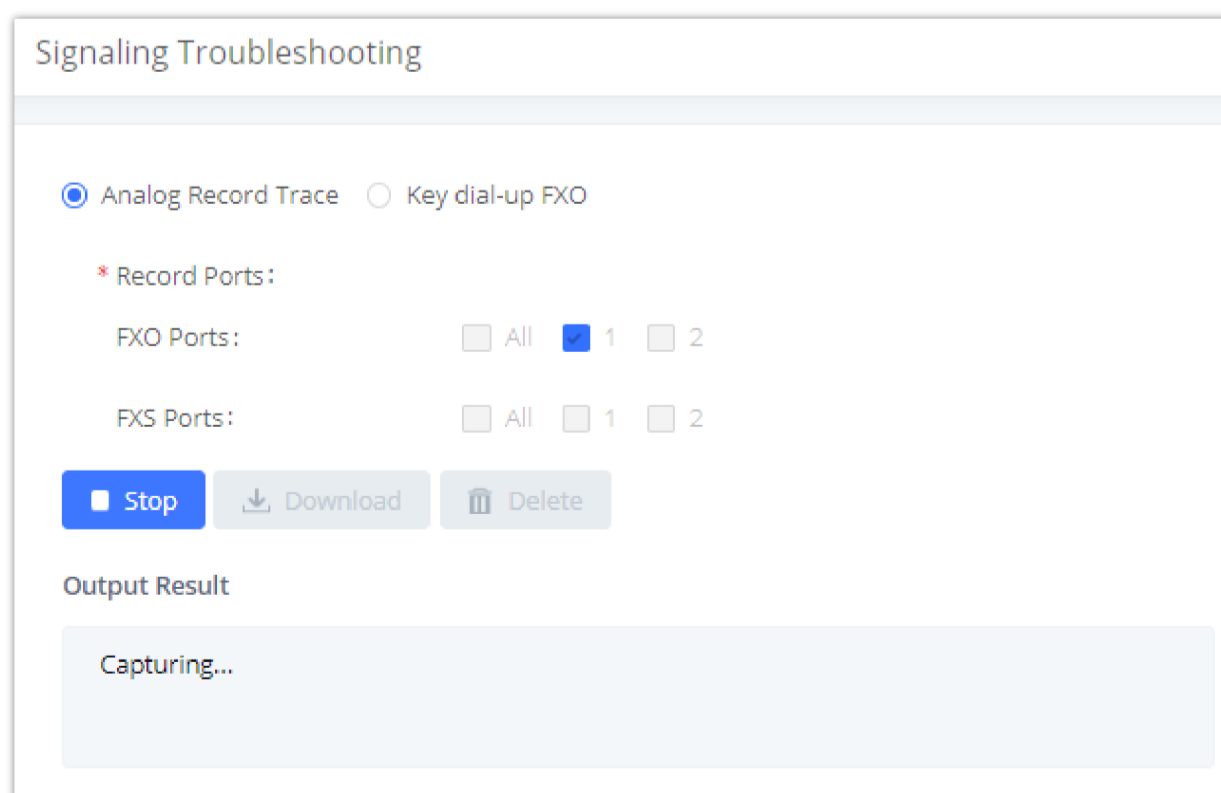
### Analog Record Trace

- **Analog Record Trace**

Analog record trace can be used to troubleshoot analog trunk issue, for example, the UCM630xA user has caller ID issue for incoming call from Analog trunk. Users can access analog record trace 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.



The screenshot shows a web interface titled "Signaling Troubleshooting". It has two radio buttons: "Analog Record Trace" (selected) and "Key dial-up FXO". Below this is a section labeled "\* Record Ports:". Under "FXO Ports:", there are three checkboxes: "All", "1" (checked), and "2". Under "FXS Ports:", there are three checkboxes: "All", "1", and "2". Below the checkboxes are three buttons: "Stop" (blue with a square icon), "Download" (grey with a download icon), and "Delete" (grey with a trash icon). Below the buttons is a section labeled "Output Result" with a large, light blue rectangular area containing the text "Capturing...".

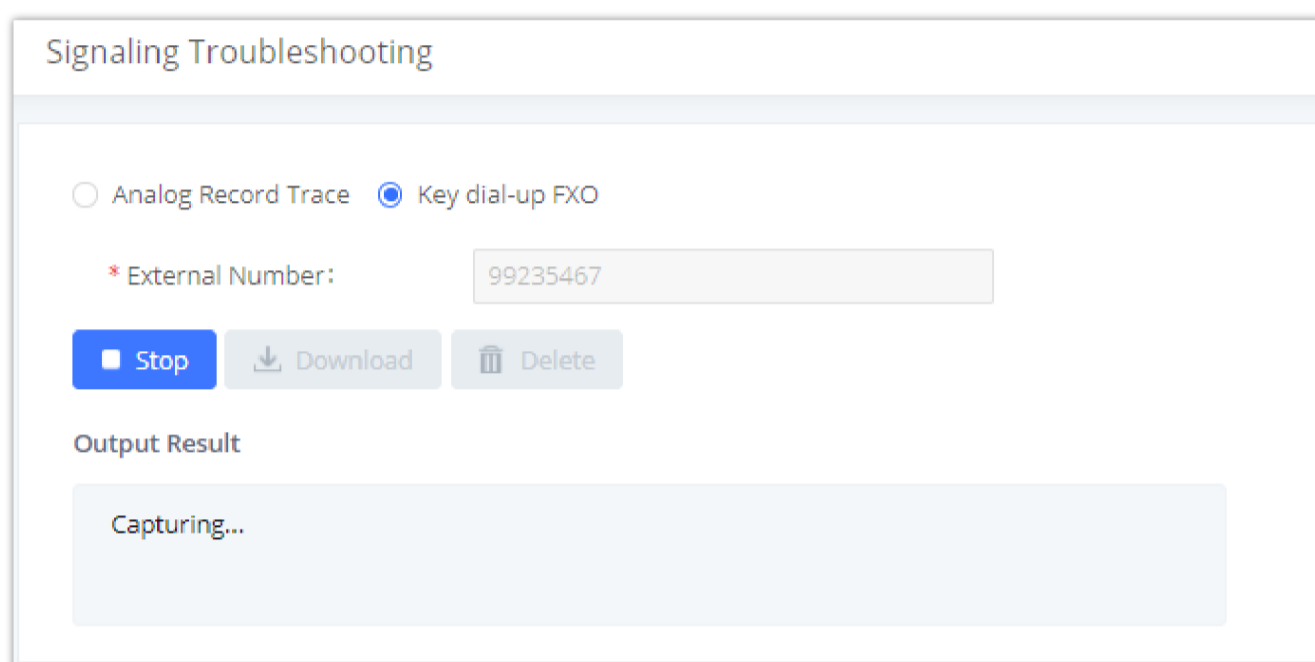
*Troubleshooting Analog Trunks*

- o A key Dial-up FXO

Users can directly set a PSTN number on the “**External Extension**” text box to troubleshoot issues related to the analog trunk easily, the following steps shows how to use this feature:

1. Configure analog trunk on UCM, including outbound route.
2. Enter a reachable external number in “**External Extension**”.
3. Press “**Start**” button. The call will be initiated to the external number.
4. Answer and finish the call before pressing “Stop” button.

The trace will be available for analysis to download after output result shows “Done! Click on Download to download the captured packets”.



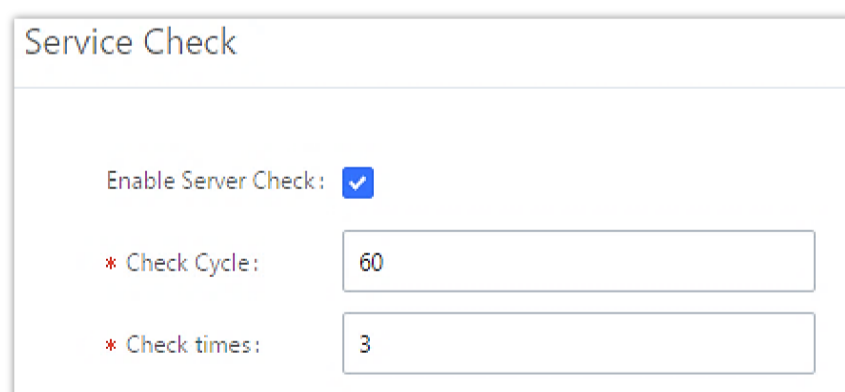
A Key Dial-up FXO

**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.

1. After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream
2. Technical support in the following link for further assistance if the issue is not resolved. <https://www.grandstream.com/support>

## Service Check

Enable Service Check to periodically check UCM630xA. 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 UCM630xA. The default setting is 3. If there is no response from UCM630xA after 3 attempts (default) to check, current status will be stored and the internal service in UCM630xA will be restarted.



Service Check

## Network Status

In UCM630xA Web GUI→**System Status**→**Network Status**, the users can view active Internet connections. This information can be used to troubleshoot connection issue between UCM630xA and other services.



Network Status

## APPENDIX A: RFC STANDARDS USED IN THE UCM6300 AUDIO SERIES

- **RFC 3261** SIP: Session Initiation Protocol
- **RFC 3262** Reliability of Provisional Responses in SIP
- **RFC 3263** Session Initiation Protocol (SIP): Locating SIP Servers
- **RFC 3264** An Offer/Answer Model with the Session Description Protocol
- **RFC 3515** The Session Initiation Protocol (SIP) Refer Method
- **RFC 3311** The Session Initiation Protocol (SIP) UPDATE Method
- **RFC 4028** Session Timers in the Session Initiation Protocol (SIP)
- **RFC 2976** The SIP INFO Method
- **RFC 3842** A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- **RFC 3892** The Session Initiation Protocol (SIP) Referred-By Mechanism
- **RFC 3428** Session Initiation Protocol (SIP) Extension for Instant Messaging
- **RFC 4733** RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
- **RFC 4566** SDP: Session Description Protocol
- **RFC 2617** HTTP Authentication; Basic and Digest Access Authentication
- **RFC 3856** A Presence Event Package for the Session Initiation Protocol (SIP)
- **RFC 3711** The Secure Real-time Transport Protocol (SRTP)
- **RFC 5245** Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- **RFC 5389** Session Traversal Utilities for NAT (STUN)
- **RFC 5766** Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- **RFC 6347** Datagram Transport Layer Security Version 1.2
- **RFC 6455** The WebSocket Protocol
- **RFC 8860** Sending Multiple Types of Media in a Single RTP Session
- **RFC 4734** Definition of Events for Modem, Fax, and Text Telephony Signals
- **RFC 3665** Session Initiation Protocol (SIP) Basic Call Flow Examples
- **RFC 3323** A Privacy Mechanism for the Session Initiation Protocol (SIP)
- **RFC 3550** RTP: A Transport Protocol for Real-Time Applications

# CHANGELOG

This section documents significant changes from previous versions of the UCM630xA 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 1.0.27.23

- Hmobile PMS option has been named to char pmslink.

## Firmware Version 1.0.27.20

- Added support for Microsoft Outlook SMTP OAuth2 authentication. [[Email Settings](#)]

## Firmware Version 1.0.27.15

- No major change

## Firmware Version 1.0.27.10

- Added QR code to email template for quick SIP registration [[Email Templates](#)]
- Added Account SIP Trunk [[Account SIP Trunk](#)]
- Added VoIP VLAN [[Network Settings](#)]
- Added support for searching CallerID in a third-party MySQL database [[Inbound Route: Third-party Database Search](#)]
- Added support for integration with Don't Call Me database [[Don't Call Me Blacklist Integration](#)]
- Added support for ZRTP on the extensions level [[Create New SIP Extension](#)]
- Added support for ZRTP on the trunk level [[VoIP Trunk Configuration](#)]
- Added support for enabling multiple Wave session on the same platform [[Create New SIP Extension](#)]
- Added support for verifying ACS [[TR-069](#)]
- Added support for Tx and Rx Noise Cancellation in Analog Trunks [[Analog Trunk Configuration](#)]
- Added Task Management feature [[Task Management](#)]
- Added support for search function in LDAP server phonebooks [[LDAP Phonebook](#)]
- Added support for data encryption on the local storage and attached storage [[Data/File Encryption](#)]
- Added *Merge Same Call Recordings* [[PBX Settings](#)]
- Added support for adding suffix to Call Forward Enable/Disable feature [[Feature Codes](#)]
- Added icons next to feature codes to indicate whether they can be nested by other feature codes [[Feature Codes](#)]
- Added support for Time Condition Routing [[TIME CONDITION ROUTING](#)]
- Added support for Custom Time Groups [[Custom Time Groups](#)]
- Added support for custom announcement for Call Queue [[Configure Call Queue](#)]
- Added Reset Agent Call Counter to Call Queue [[Configure Call Queue](#)]
- Added number and percentage of transferred calls in the Call Queue Switchboard [[Configure Call Queue](#)]
- Added Call Memory in Call Queue [[Configure Call Queue](#)]
- Updated Wake-up Service by adding call failure notification [[Wakeup Service](#)]
- Added Wake-Up Call Service Failure email template. [[Email Templates](#)]
- Room status can now be modified using the API
- Odoo CRM has been added [[Odoo CRM](#)]
- Added custom repeating setting when scheduling meetings [[Schedule Meeting](#)]
- Added Extension Login Management module. [[Extension Login Management](#)]
- Added Wave Administrator privilege [[Create New SIP Extension](#)][[Custom Privilege](#)]
- Added Download Chat Logs privilege [[User Portal/Wave Privileges](#)]

- Added Remote Logout Wave Privilege [[User Portal/Wave Privileges](#)]
- Added API support to retrieve recording filename
- Added *Password Visibility Toggle* [[Super Administrator](#)]
- Added enable/disable setting for Paging/Intercom [[Paging/Intercom](#)]
- Added support for displaying the voicemail group name on the voicemail page on Wave
- Added support for configuring custom agent pause reason with a custom prompt [[Global Queue Settings](#)]
- Added TLS key download in Ethernet Capture diagnosis tool [[Ethernet Capture](#)]
- Login Security options have been improved [[Login Security](#)]
- External Host address will be automatically pushed to Wave clients when the UCM is deployed in a Remote Disaster Recovery setup. [[HTTP Server](#)]
- UCM reboot event alerts and logs will now contain the reboot reason and the name of the user who initiated the reboot (if applicable) [[System Reboot](#)]
- Increased members notified for Emergency Calls from 10 to 30 [[Emergency Calls](#)]

#### **Firmware Version 1.0.25.9**

- Add Portugal Portuguese voice prompt support. [[LANGUAGE SETTINGS FOR VOICE PROMPT](#)]
- Add Wi-Fi related settings to GHP-W series template.

#### **Firmware Version 1.0.25.7**

- Multicast Community has been added. [[Multicast Community](#)]
- Scheduled Paging UI has been reworked. [[Scheduled Paging/Intercom](#)]
- Added support for playing MP3 files over GSC35XX devices. [[Upload Custom Prompt](#)]
- Added support for PMS billing system for Local PMS. [[Call Rate](#)]
- Mini bar has been improved. [[Mini Bar](#)]
- Added ability to set a Feature Code as a the Default Destination. [[Speed Dial](#)]
- Added ability to add External Number and LDAP numbers on Announcement Center. [[Announcement](#)]
- Added Fax Sending privilege when creating custom privileges. [[Custom Privilege](#)]
- Added enabling TURN Relay for a specific extension. [[Create New SIP Extension](#)]
- HA Data Sync Failure alert event has been added to the Alert Events List. [[Alert Events List](#)]
- SIP endpoints firmware can now be updated using the Zero Config page. [[Managing Discovered Devices](#)]
- Clearing the call history upon guest check-in or check-out has been added. [[Local PMS](#)]
- Onsite Meeting email invitations will include now an ics file. [[Onsite Meeting](#)]
- "Send File" Wave privilege has been added. [[User Portal/Wave Privilege](#)]

#### **Firmware Version 1.0.23.17**

- No major change.

#### **Firmware Version 1.0.23.15**

- Increased Fail2Ban list limit to 50 entries. [[Fail2ban](#)]
- NAS password field now supports special characters "&,\$'^`>|", [[PBX Settings/NAS](#)]
- Speed Dial limit has been increased to 1000. [[Speed Dial](#)]

#### **Firmware Version 1.0.23.12**

- Added support for limiting chat history viewing for newly added participants. [[Room](#)]
- Added support for including company number when scheduling a meeting. [[Meeting Schedule](#)]
- Added support for tracking outbound calls for QueueMetrics.

- Added support for displaying call queue names on GRP phones.
- Added support for auto answer on inbound route level to detect fax call. [[Inbound Rule Configurations](#)]
- Added support for updating the call forwarding status when enabled via feature code. [[Feature Codes](#)]
- Added support for controlling diversion header. [[SIP Settings](#)]
- Added "Extension Group" as a custom privilege. [[Custom Privilege](#)]
- Added ability to retrieve recording files saved on NAS/GDMS cloud through API.
- Added support for manually backing up the UCM configuration to SFTP. [[Backup/Restore](#)]
- Added disaster recovery for High Availability. [[HA](#)]
- Added feature code to blacklist last called number. [[Feature Codes](#)]
- Added ability to share voicemail to group members. [[VOICEMAIL](#)]
- Added ability to delete voicemails for all voicemail group from one member. [[VOICEMAIL](#)]
- Added ability to monitor voicemail groups with voicemail key on endpoints. [[VOICEMAIL](#)]
- Added "Ignore Safe Operational Flow" to Network Port Traffic Control. [[Network Settings](#)]
- Added support for domains in API ACL.
- Added support for configuring chat filesize limit. [[IM Settings](#)]
- Added support for "announce message caller-ID" in Announcement Center. [[Announcement Center Settings](#)]
- Added support for preventing Wave chat deletion. [[User Portal/Wave Privilege](#)]
- Added "Priority Call" feature code. [[Feature Codes](#)]
- Added support for updating time zones under Time Settings. [[Time Settings](#)]
- Added Live Chat feature. [[Live Chat](#)]
- Added Message Broadcast feature. [[Message Broadcast](#)]

#### **Firmware Version 1.0.21.9**

- Added SMS service support. [[SMS Settings](#)]
- Added support for creating shared departments. [[Department Management](#)]
- Added support for RADIUS login. [[RADIUS](#)]
- Added support for private intercom. [[Configure Private Intercom](#)]
- Added support for setting an extension as the default destination in Click2call. [[Integrated Customer Service](#)]
- Added support for SIP TLS cipher suite. [[SIP Settings/TCP and TLS](#)]
- Added support for continuous packet capture when using USB/SD card storage or SFTP. [[Ethernet Capture](#)]
- Added support for resetting TLS certificates to the default ones. [[SIP Settings/TCP and TLS](#)]
- Added support for SSH token. [[SSH Access](#)]
- Added support for subscribing to a voicemail group. [[Configure Voicemail Group](#)]
- Added support for setting separate call forwarding conditions for external and internal calls. [[Create New SIP Extension](#)]
- Added support for forwarding calls to a custom prompt. [[Create New SIP Extension](#)]
- Added support for external numbers to opt out of being recorded when calling into the UCM. [[PBX Settings](#)]
- Added support for caller name look up. [[Inbound Routes](#)]
- The name of the agent will now be displayed in the switchboard. [[Switchboard](#)]
- Agent pause can now be performed quickly by dialing the respective feature code and the corresponding pause reason without having to interact with the IVR. [[Configure Call Queue](#)]
- Agent pause reason will now be displayed in the switchboard. [[Switchboard](#)]
- Added support for enabling the welcome prompt to be played simultaneously with background music while the agent phone is ringing. [[Configure Call Queue](#)]

#### **Firmware Version 1.0.19.10**

- Specific Time configuration is now included in the extension exports

## Firmware Version 1.0.19.9

- Optimized various system processes
- Added Onsite Meeting feature. [[Onsite Meeting](#)]
- Added ability to customize extension call waiting tone [[General Call Prompt Tones](#)]
- Updated Zoho CRM authentication process [[Zoho Telephony](#)]
- {VM\_DATE} date value format has been changed to MM/dd/yyyy hh:mm:ss from DDD yyyy MMM hh:mm:ss. [[Configure Fax/T.38](#)] [[Voicemail Email Settings](#)]
- Added Device Name \${DEVICE\_NAME} variable to Alert Events and Emergency Calls email templates
- Added Geolocation header support [[Emergency Location Mapping](#)]
- Added P-Called-Party-ID header option to the *Add/Edit Extension* -> *Features* page [[Create New SIP Extension](#)]
- Added *Allow Operator Panel Monitoring* extension option to toggle whether the Operator Panel can monitor the extension. [[Create New SIP Extension](#)]
- Added *Basic* extension export option [[Export Extensions](#)]
- *Allow Call-barging Extension List* option changed to *Call Monitoring Whitelist* [[Create New SIP Extensions](#)] [[Create New IAX Extension](#)]
- Added *Silence Suppression* option to *Extensions/VoIP Trunks* page [[Create New SIP Extension](#)] [[VoIP Trunk Configuration](#)]
- If a storage device is full, the UCM will mark it as unavailable and automatically change file storage path to the next available location based on the *Storage Path Priority*. Previously, UCM would change the file storage path to its own local storage if external storage was full. [[File Manager](#)]
- Added new commands related to call queue and Wave [[API Configuration Parameters](#)]
- Added support for multiple API (new) users [[API Configuration Parameters](#)]
- Added the *Default Certificate Auto Renewal* option. If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected. [[HTTP Server](#)]
- Added ability to sync local IM data to Cloud IM [[Cloud IM Service](#)]
- Added ability create custom IVR key presses [[Custom Key Event](#)]
- Added *Chat Data from Endpoint* option to the Maintenance -> System Cleanup/Reset -> Cleaner page. If enabled, this option will clean out chat data from Wave clients at the same time as the UCM's server-side automatic/manual cleaning of chat data. [[Cleaner](#)]
- Added support for meeting room passwords. However, meetings cannot be scheduled for rooms with meeting password enabled. [[Room](#)]
- Meeting kick warning interval has been changed from 30 mins to 20 mins. Note: This kick warning will only play when there is only 1 person in a meeting room, and if they do not opt to stay in the meeting room after the warning, they will be removed from the meeting room after 5 minutes.
- ARP will now be used instead of ping to check NAS connectivity.
- Upgrade logs will now contain firmware version information.
- Queue chairmen can now log out dynamic agents
- Added option to automatically reset user/Wave password upon check-in/check-out. [[Local PMS](#)]
- Added option to clear Wave chat history automatically upon check-in or check-out. [[Local PMS](#)]
- Added Local PMS functionality [[Local PMS](#)]
- Check-out will no longer reset the "Skip Voicemail Password Verification" extension setting
- Added ability to assign two extensions to a room [[Room Management](#)]
- Added option to clear scheduled wakeup calls on both check-in and check-out. [[Local PMS](#)]
- Added the ability to change the default call privilege of a room. A room's privilege will be reset to this value after a guest checks out of it.
- Added support for stereo audio recording [[General Settings](#)]
- Added option to route calls based on a caller's Diversion header value [[Inbound Rule Configuration](#)]
- Added ability to control whether to use failover trunks based on the call response codes [[Failover Trunk Toggles](#)]
- Added support for H.264 with multiple payload types in SDP
- When receiving an INVITE with no SDP, following INVITEs with SDP will offer H.264 1080p resolution by default.

- In the scenario where an inbound external call is forwarded from an extension to an external number, the Contact header will now use the CID of the forwarding extension instead of the caller's CID.
- Removed *External Device Usage Threshold* option. If a connected NAS has only 1GB remaining available storage space, it will be considered unavailable and trigger the external disk usage alert. [[NAS](#)]
- Added *User Endpoint Access History* page [[User Endpoint Access History](#)]
- Added User Portal/Wave privilege control [[User Portal/Wave Privilege](#)]
- *Dial Trunk* option has been renamed to *Dial External Number* and moved to the *Dial Other Extensions* section
- The Wave Welcome email will now use the port number configured in System Settings->HTTP Server->Wave Settings->Port if the Wave Settings->External Host value is not a RemoteConnect address or does not contain a port number.
- Added links to relevant online documentation to various pages of the UCM webUI.
- Added Phonebook VMPK mode to GRP261x template
- Added Firmware tab for improved firmware management [[Firmware](#)]
- Added ability delete downloaded base model templates in the Model Update page
- Added ability to search for templates via the device model name
- Added ability to select either LAN1 or LAN2 to scan for devices on when using dual network method

### **Firmware Version 1.0.17.11**

- Several system process optimizations

### **Firmware Version 1.0.17.8**

- Updated python version to 3.8 and related processes.
- Improved speed of applying changes
- Updated lighttpd version to 1.4.61.
- The Privilege Name field now supports parenthesis ().
- The Contacts page has been moved to its own category in the sidebar.
- Added <https://www.zohoapis.in> option to CRM Server Address list.
- Added Channel Path option for accessing specific IP camera channels via URL. [[Device Management](#)]
- Improved alert email sending process.
- Updated Remote Registration email template.
- Emergency calls will no longer be restricted by the RemoteConnect call limit.
- The default highest priority codec is now G.722.
- Added Remote Extension Privilege Update feature code and Remote Extension Privilege Update Whitelist field to allow specified users to remotely change extensions' privileges. [[Feature Codes](#)]
- Automatic file migration after file storage path failure to the next storage location in the storage priority path.
- Users can now customize the storage path priority for recordings, and IM files. [[File Manager](#)]
- FXO FSK CID detection now uses spandsp.
- If SIP extensions synced from UCMs are deleted on GDMS, they will no longer be synced again.
- If HA is enabled, the HA cluster IP address will now be provisioned as the config server to endpoints instead of the active UCM's IP address.
- Added support for configuring inbound route blacklist via HTTPS API.
- If dialing into a Dial by Name directory, the call will end automatically after failing 3 times.
- Added Server Type option to the LDAP Server→LDAP Phonebook→Phonebook Download Configurations page. Users can select between LDAP and Active Directory. [[LDAP Server](#)]
- Added Department field to LDAP phonebook contacts. [[LDAP Server](#)]
- Added meeting room extensions to LDAP phonebooks. [[LDAP Server](#)]
- External Contacts created from the Contacts page will now be added to the system's internal LDAP phonebook. [[LDAP Server](#)]
- Added Remote Login tab to the Maintenance→Login Settings page. [[Maintenance](#)]

- Created new Meetings Settings page under the Multimedia Meetings page and moved several meeting-related options to it. [[Multimedia Meeting](#)]
- Regular meeting participants can now invite other members to join the meeting by dialing 1 if "Allow User Invite" is enabled. [[Multimedia Meeting](#)]
- Meetings will become "Pending" after rescheduling.
- Pending meetings are now sorted by start time by default.
- Added the Allowed to Override Host Mute option to the Edit Meeting Room and Schedule Meeting pages to allow participants to unmute themselves even after the meeting host mutes them. [[Multimedia Meeting](#)]
- Added support for user authentication. [[OpenVPN](#)]
- Operation Log entries will now contain the IP address and location information from which the operation originated. [[Operation Log](#)]
- Added option Automatically Clear Wakeup Calls for deleting scheduled wakeup calls after either guest check-in and check-out. [[PMS Features](#)]
- Users can now dial the Update PMS Room Status feature code, the maid code, and the room status code all at once to change room status. [[PMS Features](#)]
- Added a Scan button to manually retrieve the list of recordings on external storage. The UCM automatically displays up to 5000 recordings on attached external storage, but pressing this button will allow the UCM to display more. [[Recording Files](#)]
- Added ability to batch delete cloud storage files.
- If IP endpoints cannot connect to the GDMS TURN server via UDP, UCM will use TCP to connect them.
- Added Trunk Registration Period (s) option to SIP Settings->Misc. [[SIP Settings](#)]
- Added option Special Attributes to the Extension/Trunk→VoIP Trunks→Edit SIP Trunk→Advanced Settings page. If enabled, the following attributes will be included in the SIP SDP: ssrc, msid, mid, ct, as, tias, record. Enabling this may cause compatibility issues with non-Grandstream devices. [[VoIP Trunk Configuration](#)]
- Added CEI msid for audio calls.
- Added trickle-ice param to SIP OPTION's 200 OK.
- profile-level-id will be added to 200 OK when receiving INVITEs without SDP.
- Added ability to import/export speed dials. [[Speed Dial](#)]
- Improved processes to avoid duplicate alerts for the following events: Registered SIP Trunk failed, Local Disk Usage and External Disk Usage.
- Separated Allow Deletion of CDR and Recordings option to Allow Deletion of CDR and Allow Deletion of CDR Recordings. [[User Management](#)]
- Added the Call Waiting option to the User Portal.
- Added support for voicemail message seeking. When listening to voicemail, users can press star (\*) to rewind 3 seconds or pound (#) to fast forward 3 seconds. [[Voicemail](#)]
- Added Line Selection Strategy option for Trunk Groups. [[VoIP Trunks](#)]
- Changed register trunk Username field name to Trunk Registration Number. [[VoIP Trunks](#)]
- [Web] General web UI improvements
- [Web] Added Help option under the username dropdown menu that will redirect to the UCM6300 Series FAQ.
- [Web] Updated some tooltips.
- [Web] Optimized search functionality
- [Zero Config] Added GMT+2:00 (Israel) option to Time Zone drop down list in all Zero Config pages.
- [ZeroConfig] Added support for WP22 and WP825 model templates.

### **Firmware Version 1.0.15.13**

- Added SNMP monitoring feature. [[SNMP](#)]
- Added support to configure the time of a holiday. [[Holiday](#)]
- Added ability to determine the maximum total call duration per trunk for outbound calls. [[VoIP Trunk Configuration](#)]
- Added contact viewing privilege (independent from Department Contact Privilege). [[Contact Management](#)]
- Added support for agent ID announcement. [[Configure Call Queue](#)]
- Added support for Service Level Agreement for Call Queue. [[Service Level Agreement](#)]
- Added support for changing the Meeting room's name. [[Room](#)]

- Added WebRTC Trunk feature. [[WebRTC Trunks](#)]
- Extension data cleaning has been improved. [[Search and Edit an Extension](#)]
- Added support for SRTP Crypto Suite. [[VoIP Trunk Configuration](#)]
- STIR/SHAKEN has been improved. [[STIR/SHAKEN](#)]
- Added support for displaying the extension that initiated an emergency call in the emergency email notification. [[EMERGENCY](#)]
- Added support for collecting ICE candidates when an RTP connection is requested. [[RTP Settings](#)]
- Flood Attacks and Network Traffic Storm alerts have been added to the Alert Events List. [[Alert Events List](#)]
- Added support for Network Port Traffic Control for the ports of the UCM63xx Audio Series. [[Network Settings](#)]
- Added Support for limiting the frequency of calls that can be made in a period of time. [[Create New SIP Extension](#)]
- Added support for storing the local chat files in the GDMS. [[File Manager](#)]
- UCM RemoteConnect plan expiry screen has been improved.
- GDMS Cloud Storage Space details can now be viewed in the RemoteConnect menu. [[GDMS Cloud Storage Space](#)]

#### **Firmware Version 1.0.13.9**

- Added option to enable/disable DND status remotely for an extension. [[CALL FEATURES](#)]
- Added local proxy in IM settings. [[Cloud IM Service](#)]
- Added support for enabling/disabling auto audio recording for meeting. [[Auto Record](#)]
- Added privilege management for contacts. [[Privilege Management](#)]
- Improved fail2ban blacklist display. [[Fail2ban](#)]
- Improved email template for scheduling meeting. [[Email Templates](#)]
- Contacts sync-up between UCM and end points (wave/IP phones). [[LDAP Settings](#)]
- Added ability to specify DOD number based on outbound route. [[Outbound Routes DOD](#)]
- Fixed an issue where updating model templates will result in deleting the existing ones.
- Added support to use TURN Relay as an option to allow hosts behind NAT firewalls to communicate. [[VoIP Trunk Configuration](#)]

#### **Firmware Version 1.0.11.10**

- Added Operator Panel. [[OPERATOR PANEL](#)]
- Added time condition support for IVR key events. [[Key Press Event](#)]
- Added cloud IM abnormal alert event. [[Alert Events List](#)]
- Support setting to choose whether to play Follow Me.
- Add Fail2Ban whitelist comment information. [[Fail2ban](#)]
- Support Call Flip feature code. [[Feature Codes](#)]
- Added Multi-Factor Authentication for UCM login. [[Multi-Factor Authentication](#)]
- Added support for IoT device management. [[DEVICE MANAGEMENT](#)]
- Added option to enable and disable password-less remote access. [[UCM RemoteConnect Plan Settings](#)]
- Added option "Stop Ringing". [[Stop Ringing](#)]
- Add option "Email Missed Call Log". [[Email Missed Call Log](#)]
- Added remark for UCM system status. [[Remark](#)]
- Added option to enable and disable virtual queue call back keys settings. [[Virtual Queue Callback Key Setting](#)]
- Added Contacts section. [[Contacts](#)]
- Add option "Security Mode" for NAS settings. [[Security Mode](#)]
- Removed display for consumer users in user management page. [[User Management](#)]
- Support custom ignoring 180 response after 183 response. [[SIP Settings/MISC](#)]
- Added option to enable IPv6 for HA settings. [[Enable IPv6](#)]

### **Firmware Version 1.0.9.10**

- Added Support for import/export Zero Config. [[Global Policy](#)]
- Added support for enable Wave and Sync Contact under the extension. [[Create New SIP Extension](#)]
- Added support for Custom time supplement time conditions. [[Create New SIP Extension](#)]
- Added support for Call Restriction. [[RESTRICT CALLS](#)]
- Added support for Queue Metrics. [[QUEUE METRICS](#)]
- Added support for CDR API add whitelist. [[Permitted IP \(s\)](#)]
- Added support for Call queue satisfaction survey. [[Queue Statistics](#)].
- The old API Configuration is reopened for use. [[HTTPS API Settings \(Old\)](#)]
- Custom permissions support the function of deleting CDR and recording files. [[Custom Privilege](#)]
- Added support to adjust recording file storage path. [[File Manager](#)]
- Added support to High Availability feature on UCM6300A series. [[HA](#)]
- Paging/Intercom supports delayed paging. [[Configure Paging/Intercom](#)]
- UCMRC remote service diagnosis. [[Remote Diagnosis](#)]
- Support LDAP to automatically update the phone book. [[LDAP Automatic Update Cycle](#)]
- Support meeting room automatic gain control. [[Meeting AGC](#)]

### **Firmware Version 1.0.7.12**

- - Added support for email reminder when editing the time of a scheduled meeting. [[Email Reminder \(m\)](#)]
- Improved extension status syncing process to the IM server.

### **Firmware Version 1.0.7.9**

- This is the initial version.