

Grandstream Networks, Inc.

UCM630x Audio Series - User Manual



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.

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

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

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

PRODUCT OVERVIEW

Technical Specifications

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

Interfaces	
Analog Telephone FXS Ports	UCM6300A: None UCM6302A: 2 RJ11 ports UCM6304A: 4 RJ11 ports UCM6308A: 8 RJ11 ports All ports have lifeline capability in case of power outage.
PSTN Line FXO Ports	UCM6300A: None UCM6302A: 2 RJ11 ports UCM6304A: 4 RJ11 ports UCM6308A: 8 RJ11 ports All ports have lifeline capability in case of power outage
Network Interfaces	Three self-adaptive Gigabit ports (switched, routed or dual card mode) with PoE+
NAT Router	Yes (supports router mode and switch mode)
Peripheral Ports	UCM6300A: 1x USB 3.0, and 1x SD card interface UCM6302A: 1x USB 2.0, 1x USB 3.0, and 1x SD card interface UCM6304A/6308A: 2x USB 3.0 and 1x SD card interface
LED Indicators	UCM6300A/6302A/UCM6304A: None UCM6308A: Power 1/2, FXS, FXO, LAN, WAN, Heartbeat
LCD Display	UCM6300A/6302A/6304A: 320*240 LCD with touch screen for Shortcut Keys and Scroll Bar. UCM6308A: 128x32 dot matrix graphic LCD with DOWN and OK buttons

Reset Switch	Yes, long press for factory reset and short press for reboot
Voice Capabilities	
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711, NetEQ, FEC 2.0, jitter resilience up to 50% audio packet loss
Voice and Fax Codecs	Opus, G.711 A-law/U-law, G.722, G722.1 G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Signalling and Control	
API	Full API available for third-party platform and application integration.
DTMF Methods	Inband, RFC4733, and SIP INFO
Provisioning Protocol and Plug-and-Play	Mass provisioning using AES encrypted XML configuration file, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66 multicast SIP SUBSCRIBE mDNS), eventlist between local and remote trunk
Network Protocols	TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay (pending), IPv6, OpenVPN(R)
Disconnect Methods	Busy/Congestion/Howl Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect
Security	
Media Encryption	SRTP, TLS1.2, HTTPS, SSH, 802.1x
Physical	
Universal Power Supply	UCM6300A/6302A: Input: 100 ~ 240VAC, 50/60Hz; Output: DC 12V, 1.5A UCM6304A: 1x DC 12V Power Jack Input: 100~240VAC, 50/60Hz;Output: DC 12V, 2A UCM6308A: 2x DC 12V Power Jack Input: 100~240VAC,50/60Hz; Output: DC12V, 2A
Dimensions	UCM6300A/6302A/6304A: 270mm(L) x 175mm(W) x 36mm(H) UCM6308A: 485mm(L) x 187.2mm(W) x 46.2mm(H)
Weight	UCM6300A: Unit weight 705g, Package weight 1131g UCM6302A: Unit weight 725g, Package weight 1221g UCM6304A: Unit weight 775g, Package weight 1621g UCM6308A: Unit weight 2538g, Package weight 3463g
Temperature & Humidity	Operating: 32 - 113oF / 0 ~ 45oC, Humidity 10 - 90% (non-condensing) Storage: 14 - 140oF / -10 ~ 60oC, Humidity 10 - 90% (non-condensing)
Mounting	UCM6300A/6302A/6304A: Wall mount and desktop. UCM6308A: Rack mount and desktop.
Additional Features	
Multi-language Support	Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech, Turkish Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Polish, Portuguese, Russian, Swedish, Turkish, Ukrainian, Hebrew, Arabic, Nederlands Customizable language pack to support any other languages
Caller ID	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 - BT, NTT
Polarity Reversal/ Wink	Yes, with enable/disable option upon call establishment and termination
Call Center	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/workload, in-queue announcement
Customizable Auto Attendant	Up to 5 layers of IVR (Interactive Voice Response) in multiple languages
Telephony Operating System	Based on Asterisk version 16

Maximum Call Capacity	UCM6300A: Users: 250 Concurrent calls (G.711): 50 Max concurrent SRTP calls: 50 UCM6302A: Users: 500 Concurrent calls (G.711): 75 Max concurrent SRTP calls: 75 UCM6304A: Users: 1000 Concurrent calls (G.711): 150 Max concurrent SRTP calls: 120 UCM6308A: Users: 1500 Concurrent calls (G.711): 200 Max concurrent SRTP calls: 150
Maximum Attendees of Meeting Bridges	UCM6300A: 3 Meeting rooms and up to 50 parties UCM6302A: 5 Meeting rooms and up to 75 parties UCM6304A: 7 Meeting rooms and up to 120 parties UCM6308A: 9 Meeting rooms and up to 150 parties
Wave App	Free; Available for desktop (Windows 10+, Mac OS 10+), web (Firefox and Chrome Browsers) and mobile (Android & iOS), allows users to join UCM-hosted meetings, communicate with other users/solutions and make/receive calls using SIP accounts registered to a UCM6300 Audio series IP PBX
Call Features	Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, fax to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice conference, video conference, eventlist, feature codes, busy camp-on/call completion, voice control, post-meeting reports, virtual fax sending/receiving, email to fax
Firmware Upgrade	Supported by Grandstream Device Management System (GDMS), a zero-touch cloud provisioning and management system. It provides a centralized interface to provision, manage, monitor, and troubleshoot Grandstream products
Internet Protocol Standards	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028, RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550
Compliance	FCC: Part 15 (CFR 47) Class B, Part 68 CE: EN 55032, EN 55035, EN61000-3-2, EN61000-3-3, EN 62368.1, ES 203 021, ITU-T K.21 IC: ICES-003, CS-03 Part I Issue 9 RCM: AS/NZS CISPR 32, AS/NZS 62368.1, AS/CA S002, AS/CA S003.1/.2 Power adapter: UL 60950-1 or UL 62368-1

Technical Specifications

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

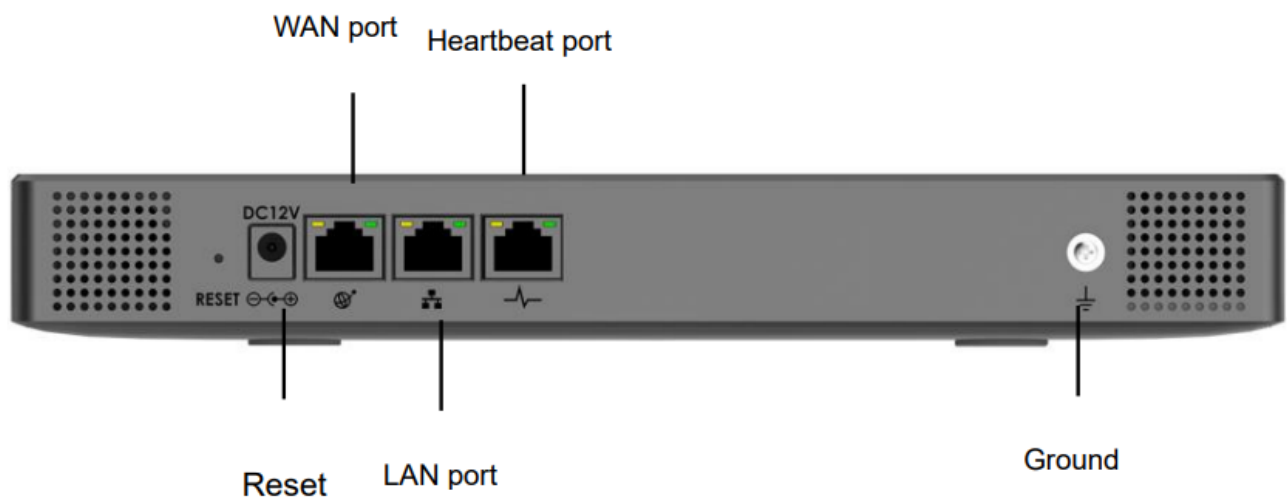
Before deploying and configuring the UCM630xA series, the device needs to be properly powered up and connected to a network. This section describes detailed information on installation, connection, and warranty policy of the UCM630xA series.

Equipment Packaging

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

UCM630xA Equipment Packaging

UCM6300A front and back view

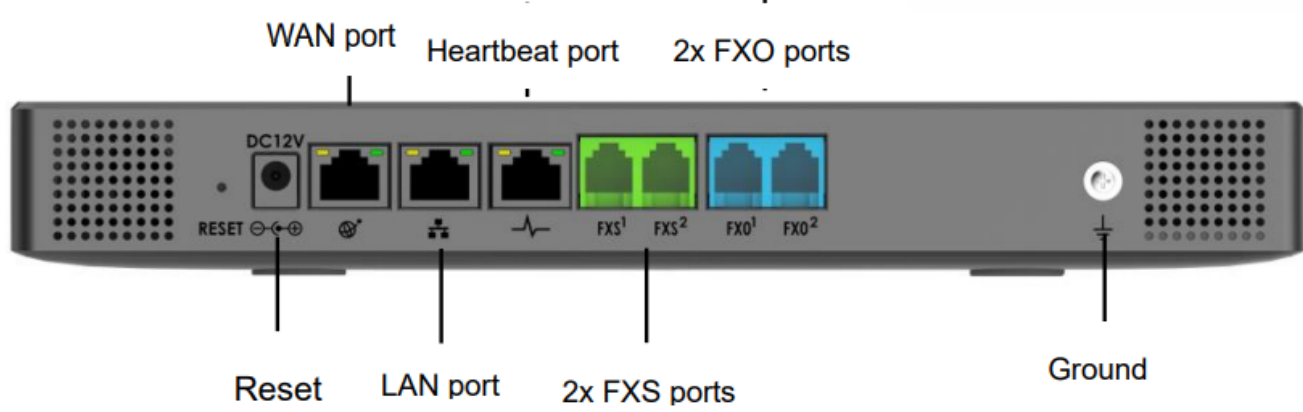


UCM6300A Back View



UCM6300A Front View

UCM6302A front and back view

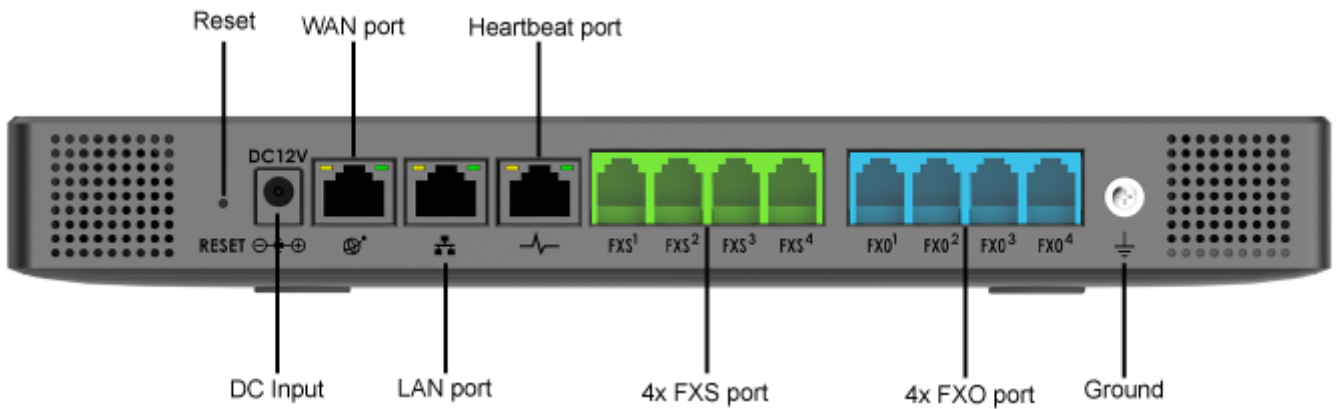


UCM6302A Back View



UCM6302A Front View

UCM6304A front and back view

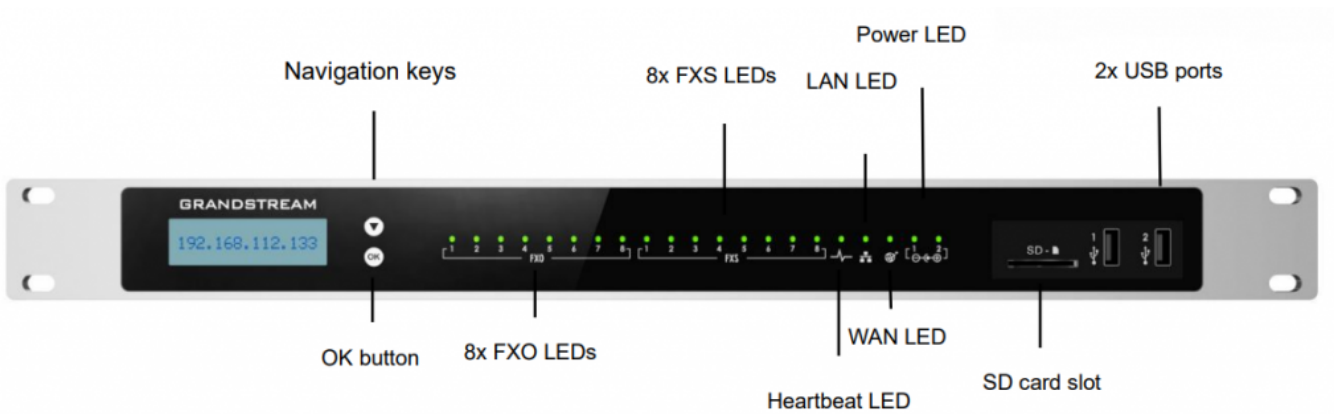


UCM6304A Front View

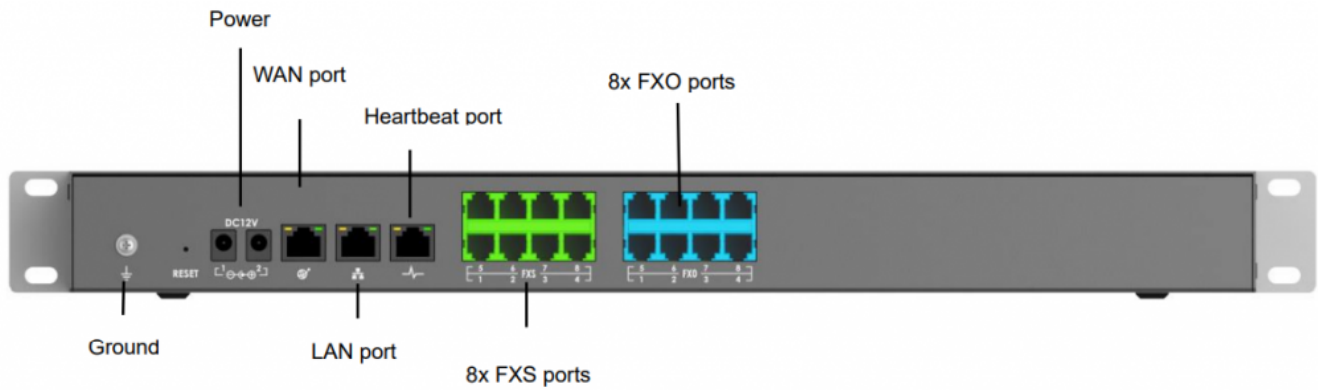


UCM6304A Back View

UCM6308A front and back view



UCM6308A Front View



UCM6308A Back View

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.

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.

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.

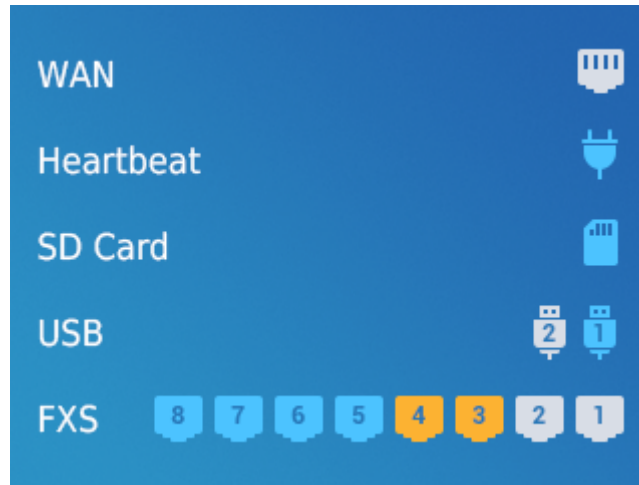
The following table summarizes the layout of the LCD menu of UCM630x.

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

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.

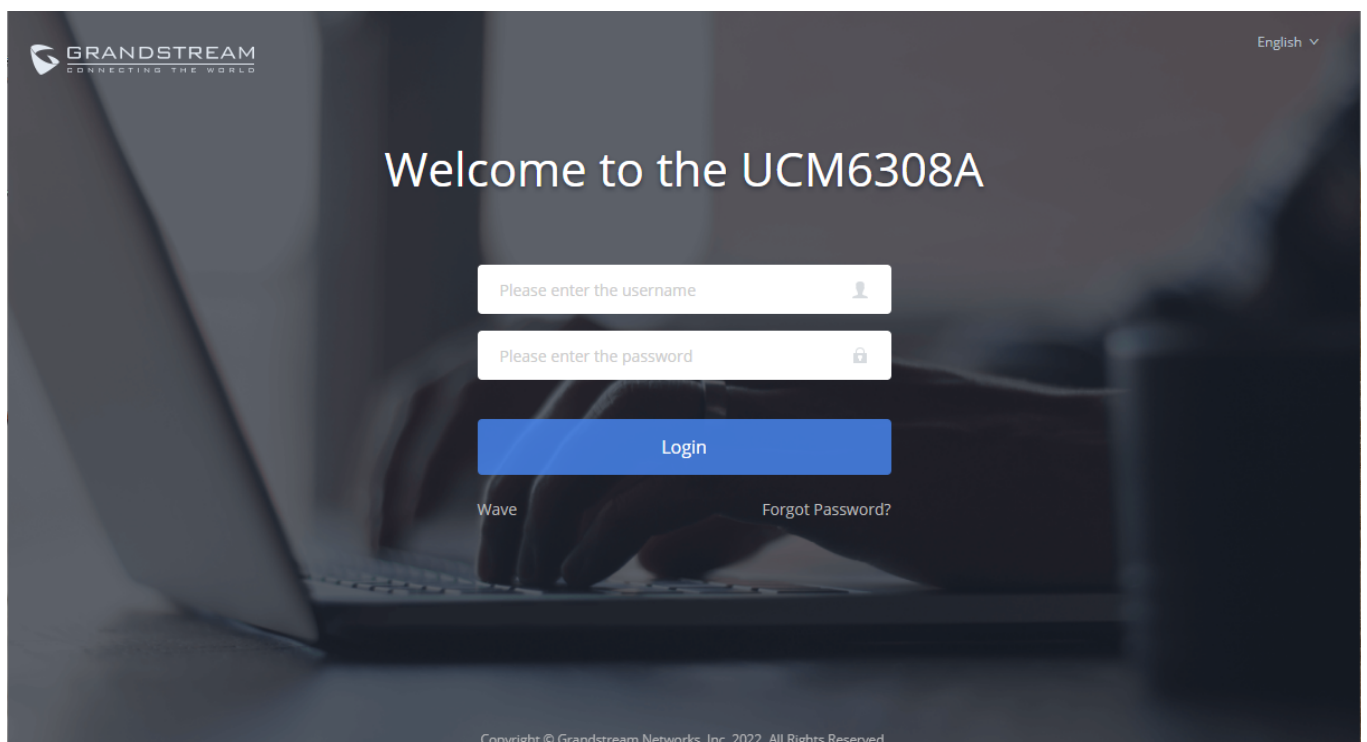
LED Indicator	LED Status
Power 1/Power 2 PoE LAN WAN USB SD FXS ports FXO ports	Solid: Connected Fast Blinking: Data Transferring Slow Blinking: Trying to connect OFF: Not Connected

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



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

By default, the 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.

Setup Wizard

1 Change Password — 2 Network Settings — 3 Select Time Zone — 4 Extensions — 5 Trunks / Routes — 6 Summary

Change Password

Enter Old Password:

Enter New Password:

Re-enter New Password:

Email Address:

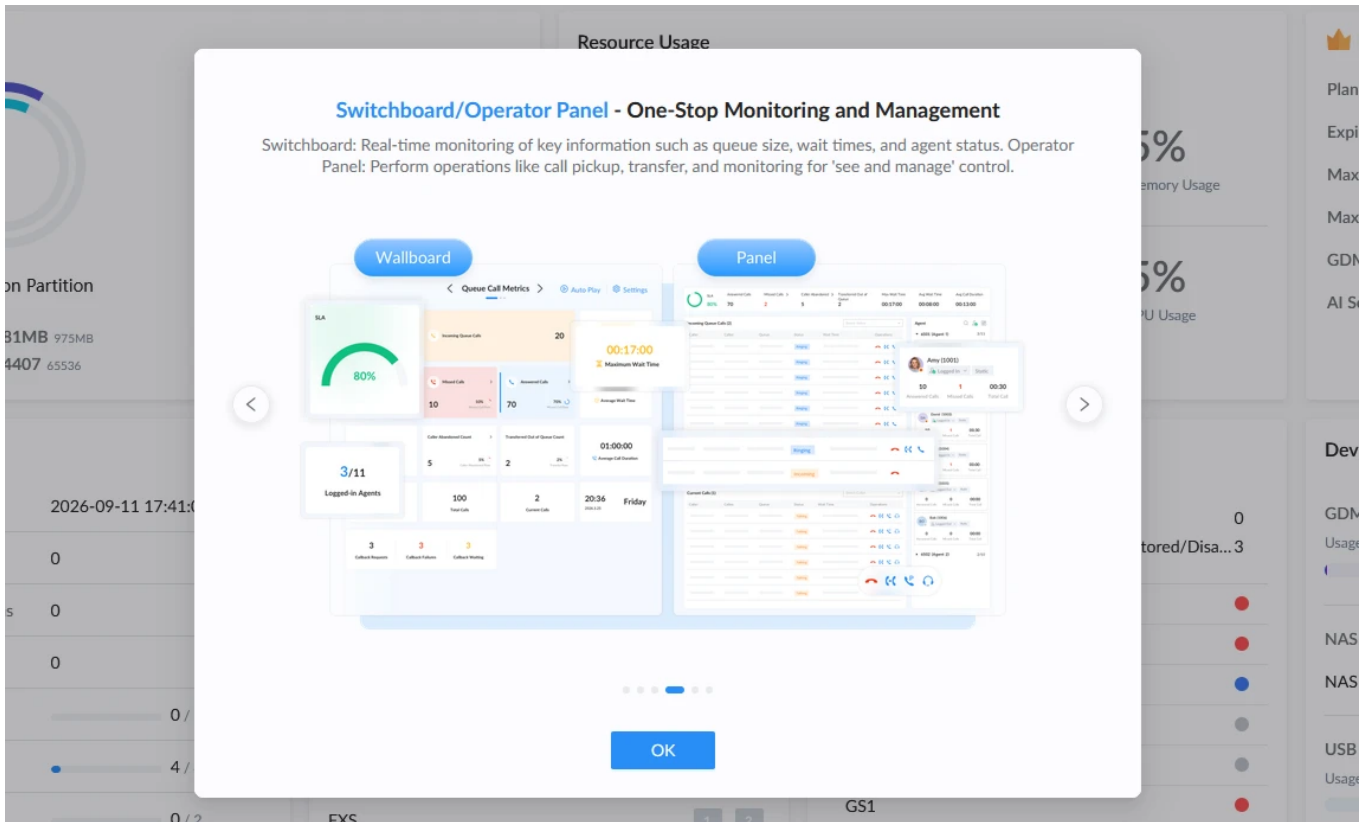
Next

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.

New Feature Guide

The UCM630xA includes an interactive **New Feature Guide** to inform administrators of major platform updates upon upgrading system firmware. When logging in for the first time following a firmware upgrade, an illustrated modal window automatically appears to highlight the key enhancements and value-added capabilities introduced in the new release.

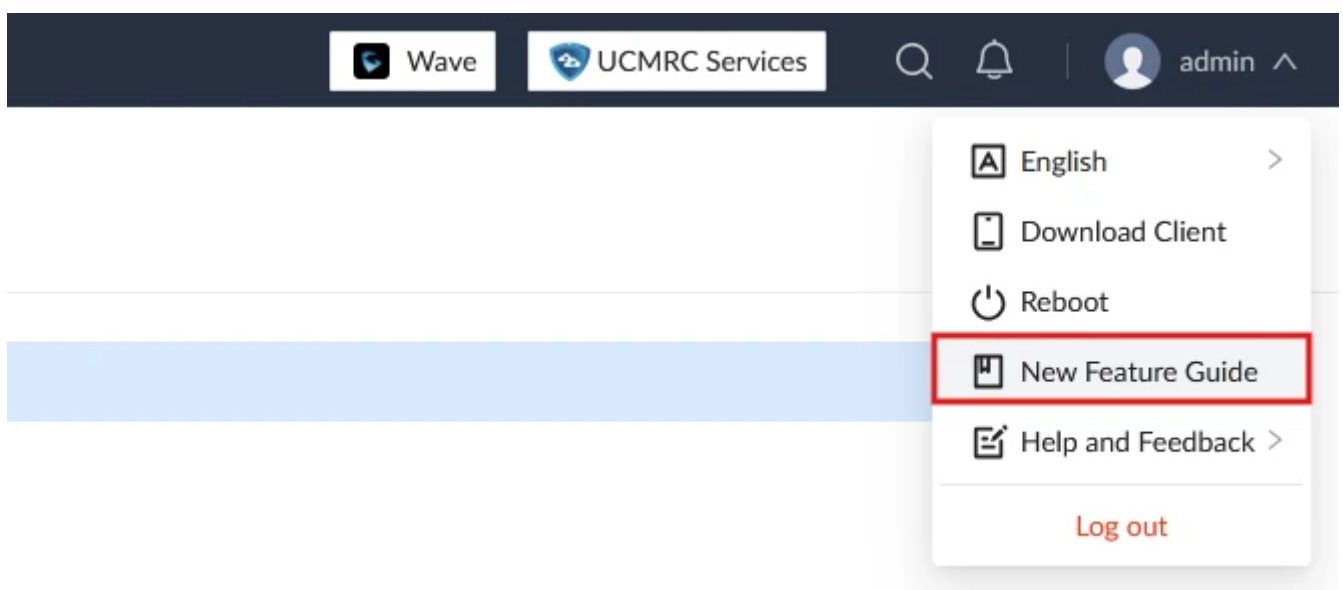


Interactive New Features Guide Modal

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

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

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

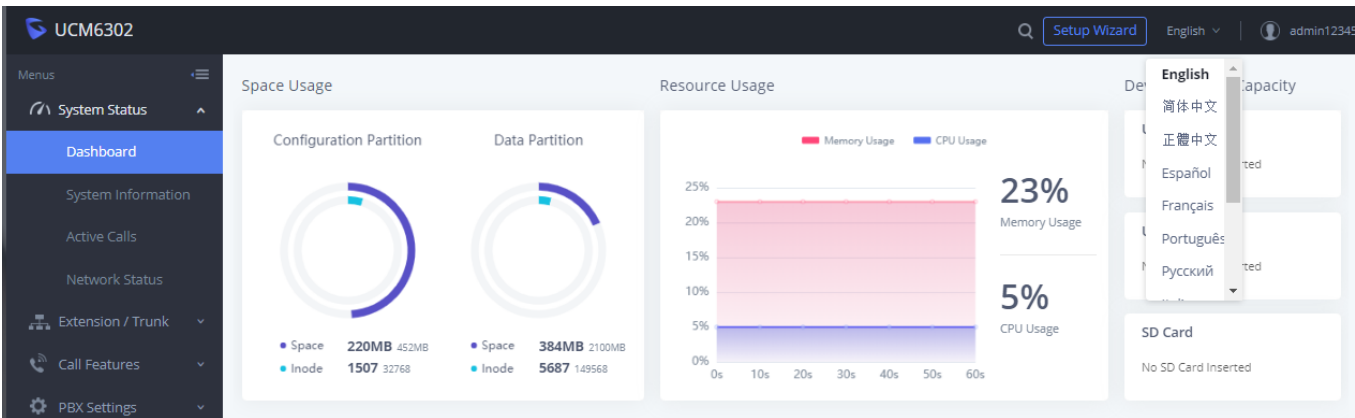
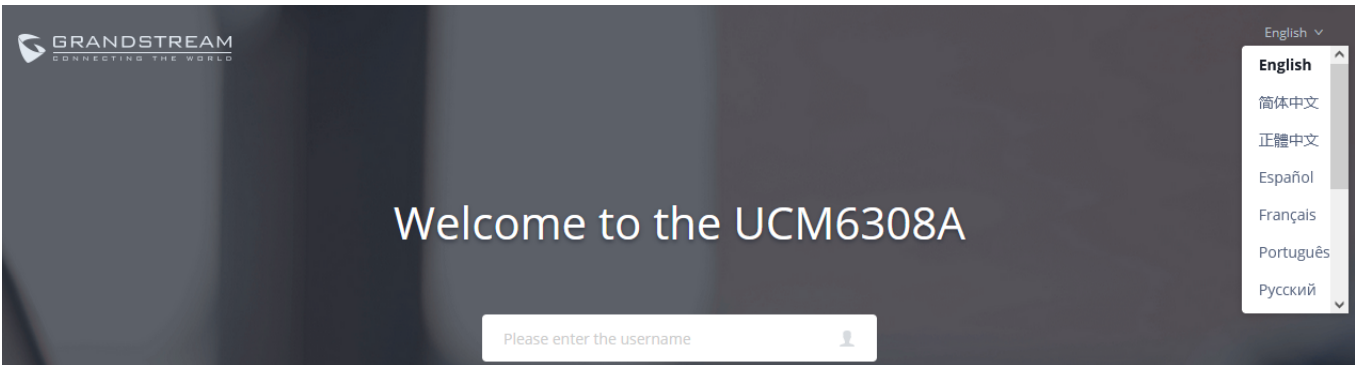


Accessing New Feature Guide via Top Header Menu

Web GUI Languages

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

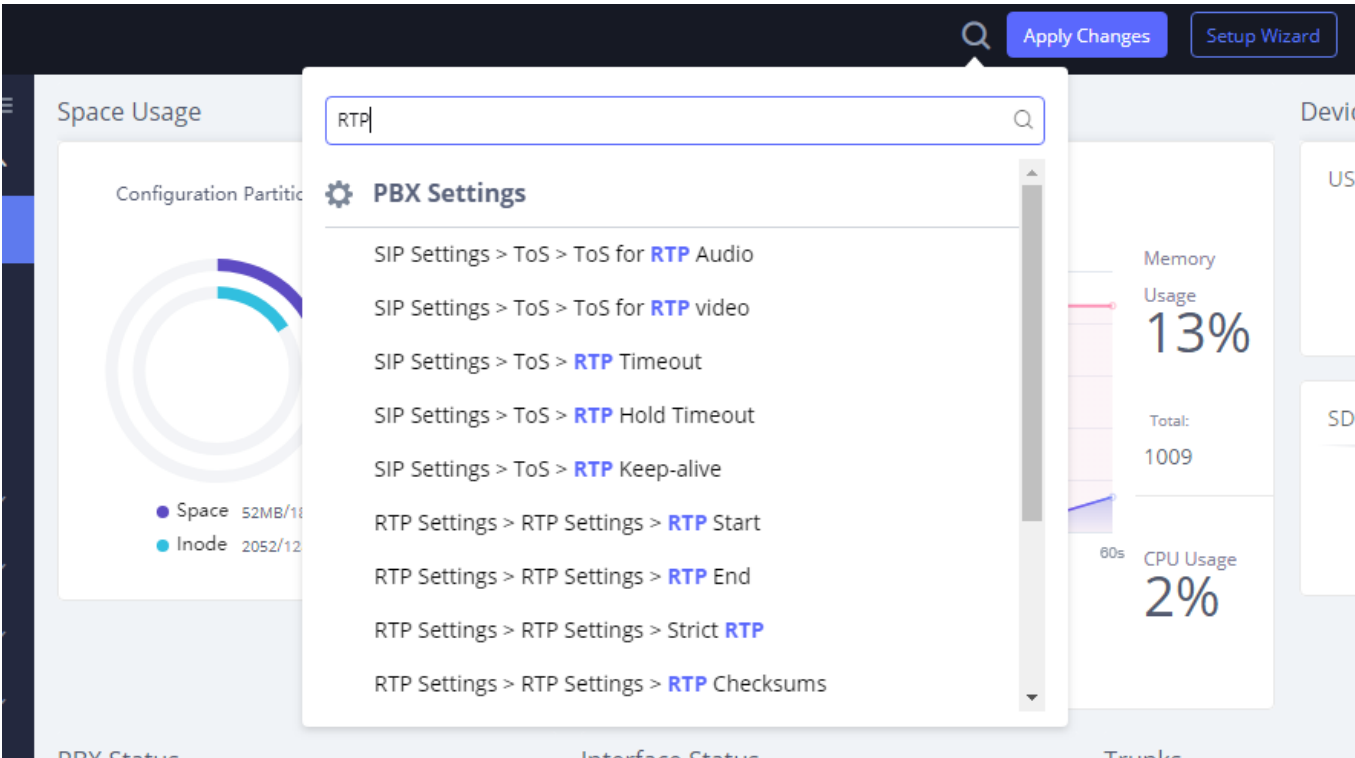
Users can select the UCM's web UI display language in the top-right corner of the page.



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.



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

90%

▼

Threshold :

Data Partition Write

90%

▼

Threshold :

General Settings Interface

General Settings	
Device Name	Configure the name of the UCM.
Enable CPU Flow Control	Enables the CPU flow control.
CPU Flow Control Threshold	Used to set the threshold generated by the CPU Flow Control. When the system CPU reaches the threshold, it will prohibit the new calls. Default value is 90%.
Data Partition Write Threshold	Used to set a threshold to stop writing data partition. When the disk data partition reaches the threshold configured, the data partition writing will be stopped. Default value is 90%.

General Settings Parameters

IM Settings

IM Settings

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

IM Settings

IM Settings

Cloud IM Service

IM Server

Read Receipts ⓘ



Notify Inactive Users of New Messages ⓘ



[Email Template](#)

* Max File Size Upload (MB) ⓘ

50

Message Deletion Period ⓘ

24 hour(s)



Cancel

Save

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

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

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.

IM Settings

Cloud IM Service

IM Server

Cancel

Save

Enable Cloud IM: ☒

Local Proxy: ☐

Cloud IM Server Address:

To view the external CloudIM server address, please go to [RemoteConnect](#)

* Service ID:

* Key:

* Department Name:

Trusted User:

Prepend:

Sync Local Chat Data: ☐

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

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

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

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**.

Redirect From Port 80	Toggles automatic redirection to UCM's web portal from port 80. If disabled, users will need to manually add the UCM's configured HTTPS port to the server address when accessing the UCM web portal via browser. Default is "Enabled".
External Host	Configure a URL and port (optional) used to access the UCM web portal if the UCM is behind NAT.

Port	Specifies the port number used to access the UCM HTTP server. Default is "8089".
Enable IP Address Allowlist	IP Allowlist restricts all IP addresses except for those in the allowlist from accessing the device via HTTP(S) (i.e., web portal, ZeroConfig, CTI apps).
Permitted IP(s)	List of addresses that can access the UCM web portal.Ex: 192.168.6.233 / 255.255.255.255
Wave Settings	
Cross-origin Address Allowlist	The UCM will accept cross-server requests from addresses in the whitelist, which should be formatted as https://domain, https://ip:port or *. Entering * will allow cross-server requests from all addresses.Note: This option allow third parties to embed a Wave portal into their websites. This allows the users to log into wave using their extension numbers and use limited Wave features.For more details, please refer to the following link: https://doc.grandstream.dev/WAVE-SDK/EN/#api-Quick%20Start-Over view
External Host	Specifies the public domain name or IP address (and port, if required) used by Wave clients to access UCM services when the UCM is behind NAT or accessed from an external network. This address is synchronized to Wave and used for external service access, including high-availability and disaster recovery scenarios.Note: When a RemoteConnect plan is enabled, this field is automatically populated with the Wave external host address provided by GDMS. Please ensure that Automatically Update the External Host Address for Wave is disabled to prevent the external host from being reset by GDMS.
Port	The port to access Wave Web and Wave Mobile. If behind NAT, please make sure to map the external port to this port.
Certificate Settings	
Default Certificate Auto Renewal	If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected.
Options	Selects the method of acquiring SSL certificates for the UCM web server. Two methods are currently available:Upload Certificate: Upload the appropriate files from one's own PC.Request Certificate: Enter the domain for which to request a certificate for from "Let's Encrypt".
TLS Cert	Upload the certificate for the HTTP server used for TLS connections. It contains the client's private key and the server's signed certificate. Once uploaded, the file will automatically be saved as "certificate.pem".Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The file size must not exceed 2MB.
TLS Private Key	Upload the private key for the HTTP server. Once uploaded, the file will automatically be saved as "private.pem".Notes:Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca.DER-formatted certificates are supported and will automatically be converted to PEM format upon upload.The file size must not exceed 2MB.

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.

- 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.

Method	Select "Route", "Switch" or "Dual" mode on the network interface of UCM630X. The default setting is "Switch". Route: WAN port will be used for the uplink connection. LAN port will function similarly to a regular router port. Switch: WAN port will be used for the uplink connection. LAN port will be used as a bridge for connections. Dual: Both WAN and LAN ports will be used for uplink connections labeled as LAN2 and LAN1, respectively. The port selected as the Default Interface will need to have a gateway IP address configured if it is using a static IP.
MTU	Specifies the maximum transmission unit value. Default is 1492.
IPv4 Address	
Preferred DNS Server	If configured, this will be used as the Primary DNS server.
WAN (when "Method" is set to "Route")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
Username	Enter the username to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for the WAN port.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for the WAN port.
Enable VoIP VLAN	If enabled, the following VLAN settings will be added to achieve VoIP data diversion.
IP Method	The UCM's address type.Static IP: Manual configuration of address information.
IP Address	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
Subnet Mask	Enter the subnet mask. For example, "255.255.255.0".
Gateway IP	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
Layer 2 QoS 802.1Q/VLAN Tag	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.
Layer 2 QoS 802.1p Priority Value	This assigns priority value for Layer 2 QoS packets.
LAN (when Method is set to "Route")	
IP Address	Enter the IP address assigned to the LAN port. The default setting is 192.168.2.1.
Subnet Mask	Enter the subnet mask. The default setting is 255.255.255.0.
DHCP Server Enable	Enable or disable DHCP server capability. The default setting is "Yes".
DNS Server 1	Enter DNS server address 1. The default setting is 8.8.8.8.
DNS Server 2	Enter DNS server address 2. The default setting is 208.67.222.222.

Allow IP Address From	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.
LAN (when Method is set to "Switch")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
Username	Enter the username to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for the LAN port. The accepted range is 2-4094.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for the LAN port. The default value is 0.
Enable VoIP VLAN	If enabled, the following VLAN settings will be added to achieve VoIP data diversion.
IP Method	The UCM's address type.Static IP: Manual configuration of address information.
IP Address	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
Subnet Mask	Enter the subnet mask. For example, "255.255.255.0".
Gateway IP	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
Layer 2 QoS 802.1Q/VLAN Tag	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.
Layer 2 QoS 802.1p Priority Value	This assigns priority value for Layer 2 QoS packets.
LAN 1 / LAN 2 (when Method is set to "Dual")	
Default Interface	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.
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings when the port is assigned as the default interface. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
Username	Enter the username to connect via PPPoE.
Password	Enter the password to connect via PPPoE.

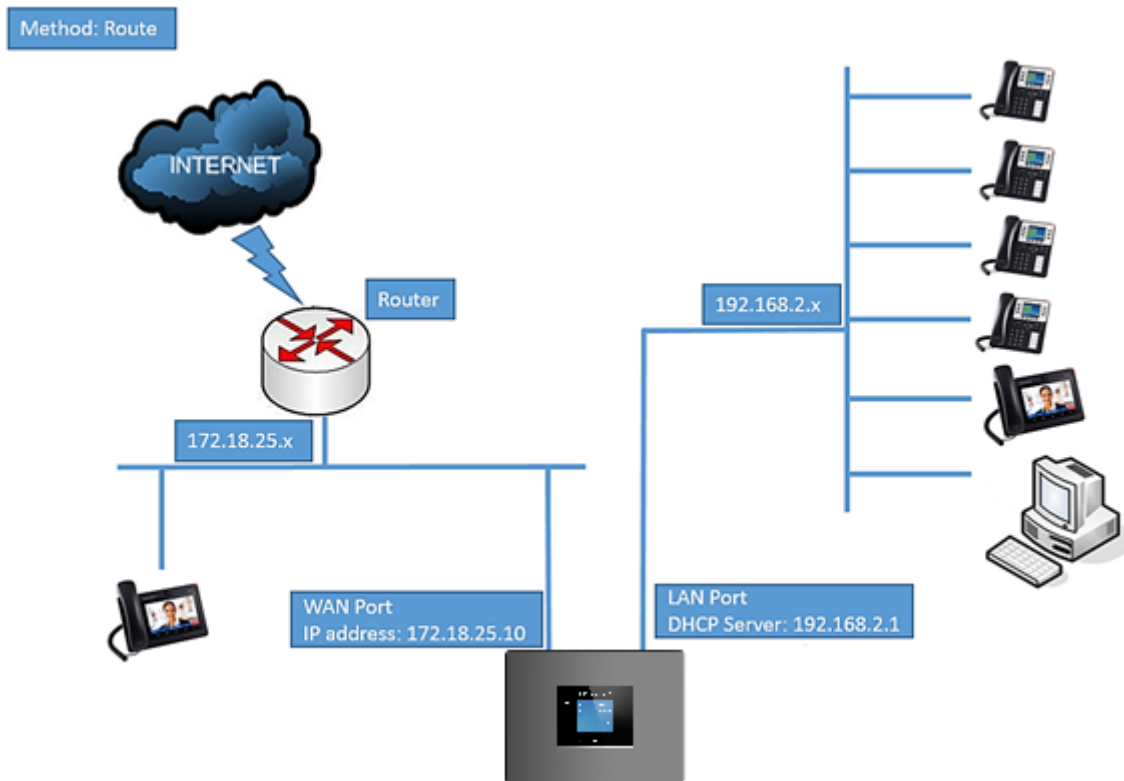
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for the LAN port. The accepted range is 2-4094.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for the LAN port. The default value is 0.
IP Method	The UCM's address type. Static IP: Manual configuration of address information.
IP Address	The IPv4 address of the device, format: xxx.xxx.xxx.xxx.
Subnet Mask	Enter the subnet mask. For example, "255.255.255.0".
Gateway IP	Enter the gateway IP address. Format: "xxx.xxx.xxx.xxx".
Layer 2 QoS 802.1Q/VLAN Tag	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.
Layer 2 QoS 802.1p Priority Value	This assigns priority value for Layer 2 QoS packets.
IPv6 Address	
WAN (when "Method" is set to "Route")	
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
LAN (when Method is set to "Route")	
DHCP Server	Select Disable, Auto, or DHCPv6. Disable: the DHCPv6 server is disabled. Auto: Stateless address auto configuration using NDP protocol. DHCPv6: Stateful address auto configuration using DHCPv6 protocol. The default setting is Disabled.
DHCP Prefix	Enter DHCP prefix. (Default is 2001:db8:2:2::)
DHCP prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings. Default is (2001:4860:4860::8888)
DNS Server 2	Enter the DNS server 2 address for static settings. Default is (2001:4860:4860::8844)
Allow IP Address From	Configure starting IP address assigned by the DHCP prefix and DHCP prefixlen.
Allow IP Address To	Configure the ending IP address assigned by the DHCP Prefix and DHCP prefixlen.
Default IP Lease Time	Configure the lease time (in second) of the IP address.
LAN (when Method is set to "Switch")	
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
LAN 1 / LAN 2 (when Method is set to "Dual")	
Default Interface	Users will need 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.

IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
Network Port Traffic Control	
LAN (when Method is set to "Switch")	
Enable Network Port Traffic Storm Alert	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. Note: To enable this feature email or HTTP notification should be set up correctly In Maintenance ?? System Events.
Ignore Safe Operational Flow	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.
Network Port Receiving Traffic Control	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.
LAN 1 & LAN 2 (when Method is set to "Dual")	
Enable Network Port Traffic Storm Alert	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. Note: To enable this feature email or HTTP notification should be set up correctly In Maintenance ?? System Events.
Ignore Safe Operational Flow	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.
LAN1 & LAN2- Network Port Receiving Traffic Control	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.
LAN & WAN (When Method is set to Route Mode)	
Enable Network Port Traffic Storm Alert	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. Note: To enable this feature email or HTTP notification should be set up correctly In Maintenance ?? System Events.
Ignore Safe Operation Flow	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.
WAN:Network Port Receiving Traffic Control	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.
LAN:Network Port Receiving Traffic Control	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.

- Method: Route

When the UCM630xA has, method set to Route in network settings, WAN port interface is used for uplink

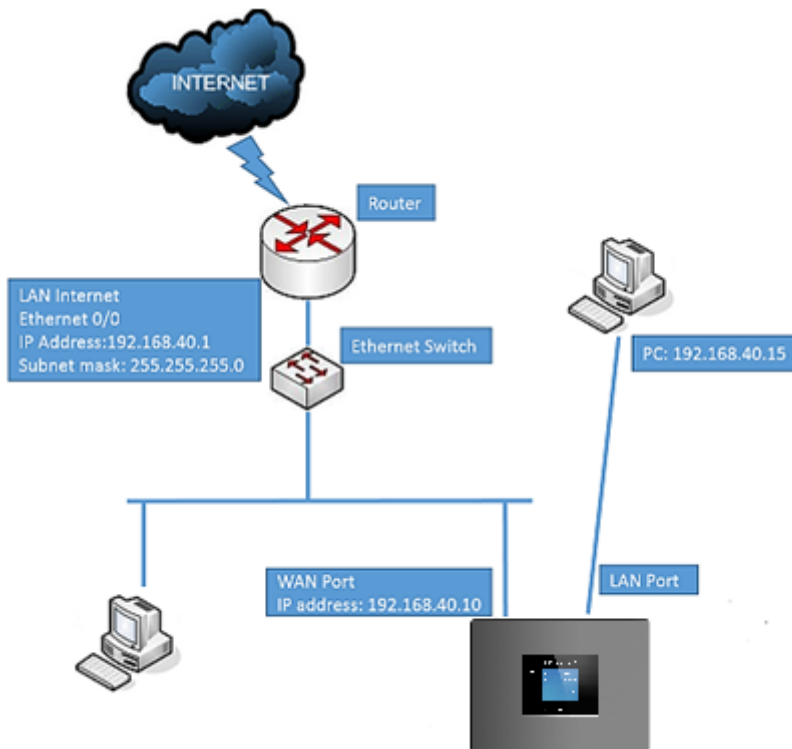
connection and LAN port interface is used as a router. Please see a sample diagram below.



UCM6302A Network Interface Method Route

- Method: Switch

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

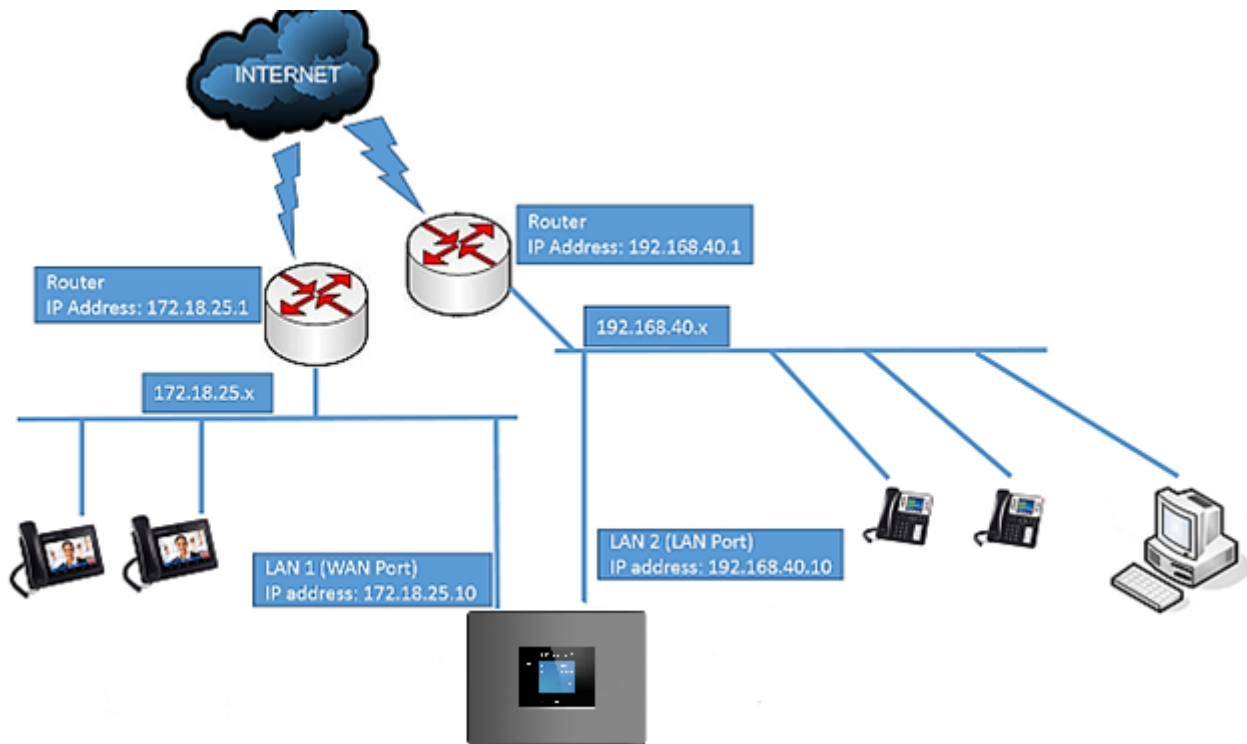


UCM6302A Network Interface Method: Switch

- Method: Dual

Both WAN port and LAN port are used for uplink connection. Users will need assign LAN 1 or LAN 2 as the

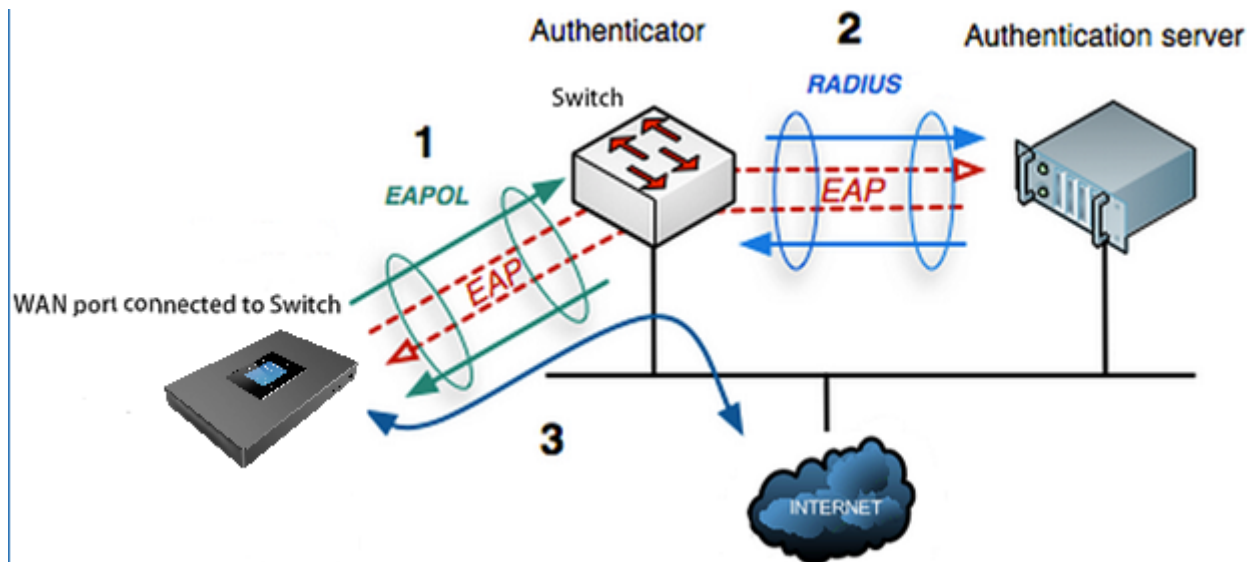
default interface in option "Default Interface" and configure "Gateway IP" if static IP is used for this interface.



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 8021X as Client

Network Settings

Basic Settings

802.1X Settings

Static Routes

Port Forwarding

802.1X Mode :

EAP-MD5

* Identity :

8021xxUCM6302

* MD5 Password :

.....

UCM630xA Using 8021X 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.

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

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.

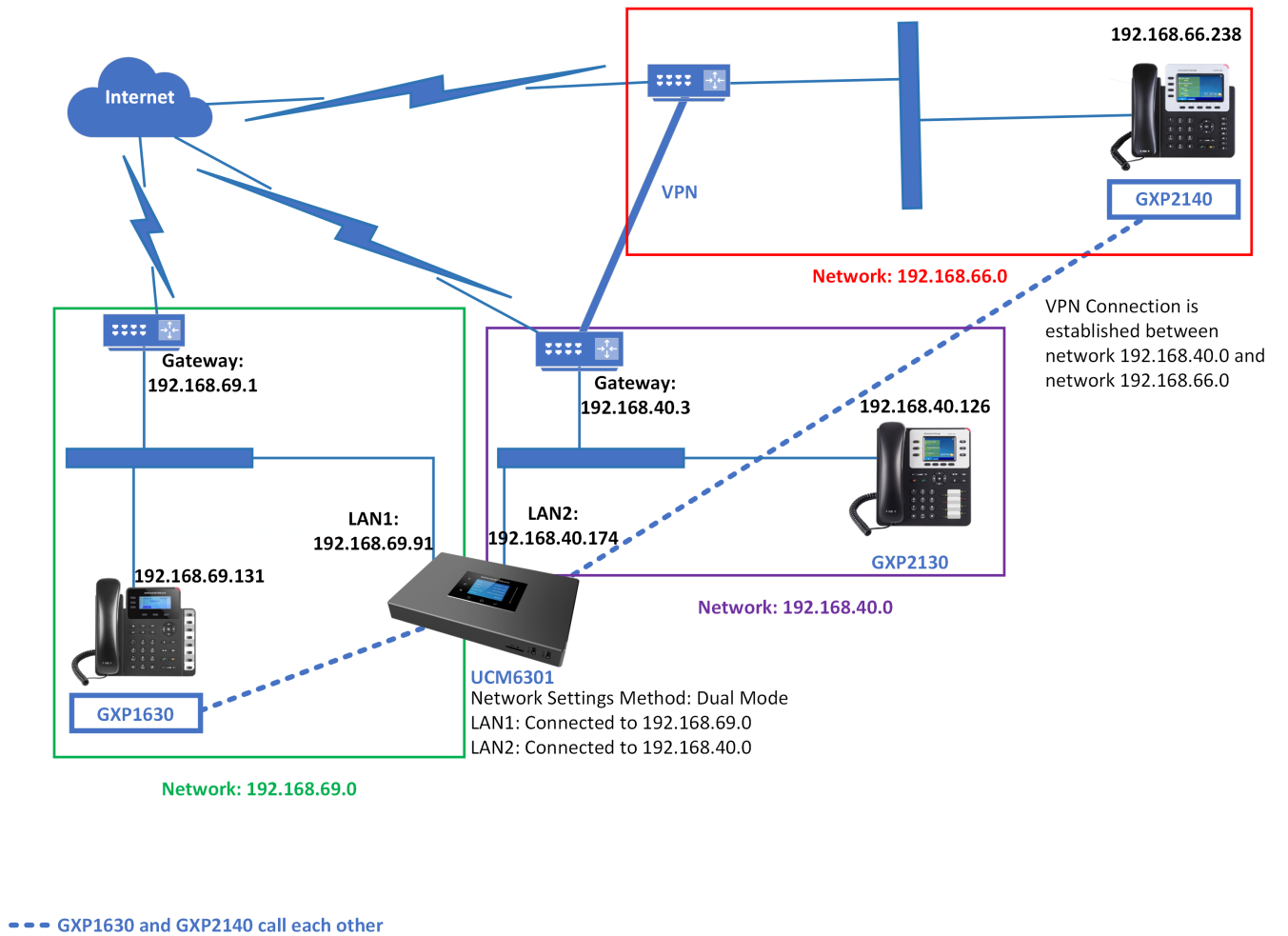
- Click on **"Add IPv4 Static Route"** to create a new IPv4 static route or click on **"Add IPv6 Static Route"** to create a new IPv6 static route. The configuration parameters are listed in the table below.
- Once added, users can select
 - to edit the static route.
- Select
 - to delete the static route.

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



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.

WAN Port	Specify the WAN port number or a range of WAN ports. Unlimited number of ports can be configured. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
LAN IP	Specify the LAN IP address.
LAN Port	Specify the LAN port number or a range of LAN ports. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
Protocol Type	Select protocol type "UDP Only", "TCP Only" or "TCP/UDP" for the forwarding in the selected port. The default setting is "UDP Only".

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.

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 GXP2160Admin Logout | Reboot | Provision | Factory ResetEnglish


GRANDSTREAM
 CONNECTING THE WORLD

STATUSACCOUNTSSETTINGSNETWORKMAINTENANCEPHONEBOOK

Version 1.0.5.23

Status

Account Status

Network Status

System Info

Network Status

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

ARP GC Threshold 1	Minimum number of entries to keep. Garbage collector will not purge entries if there are fewer than this number. The default value is 128.
ARP GC Threshold 2	Threshold when garbage collector becomes more aggressive about purging entries. Entries older than 5 seconds will be cleared when over this number. The default value is 512.
ARP GC Threshold 3	Maximum number of non-PERMANENT neighbor entries allowed. Increase this when using large numbers of interfaces and when communicating with large numbers of directly connected peers. The default value is 1024.

ARP Settings

OpenVPN(R)

OpenVPN(R) 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(R) Feature on the UCM630xA

OpenVPN(R) Enable	Enable / Disable the OpenVPN(R) feature.
Configuration Method	Select the OpenVPN(R) configuration method. Manual Configuration: Allows to configure OpenVPN(R) settings manually. Upload Configuration File: Allows to upload .ovpn and .conf files to the UCM and to automatically configure OpenVPN(R) settings.
OpenVPN(R) Server Address	Configures the hostname/IP and port of the server. For example 192.168.1.2:22
OpenVPN(R) Server Protocol	Specify the protocol user, user should use the same settings as used on the server
OpenVPN(R) Device mode	Use the same setting as used on the server. Dev TUN: Create a routed IP tunnel. Dev TAP: Create an Ethernet tunnel.
OpenVPN(R) Use Compression	Compress tunnel packets using the LZO algorithm on the VPN link. Do not enable this unless it is also enabled in the server config file.
Enable Weak SSL Ciphers	Either to enable the Weak SSL ciphers or not.
OpenVPN(R) Encryption Algorithm	Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server.
OpenVPN(R) CA Cert	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
OpenVPN(R) Client Cert	Upload a client certificate. This file will be renamed as 'client.crt' automatically.
OpenVPN(R) Client Key	Upload a client private key. This file will be renamed as 'client.key' automatically.

Username	Username used to authenticate into the server.
Password	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:

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

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

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

Hostname Information

Hostname:	haograndstream.ddns.net	
Host Type:	☒ DNS Host (A) ☐ DNS Host (Round Robin) ☐ DNS Alias (CNAME)	
	☐ Port 80 Redirect ☐ Web Redirect	
IP Address:	1.2.3.4 Last Update: 2015-01-07 17:29:20 PST	
Assign to Group:	- No Group -   Configure Groups	
Enable Wildcard:	Wildcards are a Plus / Enhanced feature. Upgrade Now!	
Advanced Records:	TXT, SPF, and SRV records and the use of some special clients are Plus / Enhanced features. Upgrade now to use them.	

Register Domain Name on noipcom

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

UCM6302

Menus

- System Status
- Extension / Trunk
- Call Features
- PBX Settings
- System Settings**
 - HTTP Server
 - Network Settings
 - OpenVPN®
 - DDNS Settings**

DDNS Settings

DDNS Server: no-ip.com

Enable DDNS: ☒

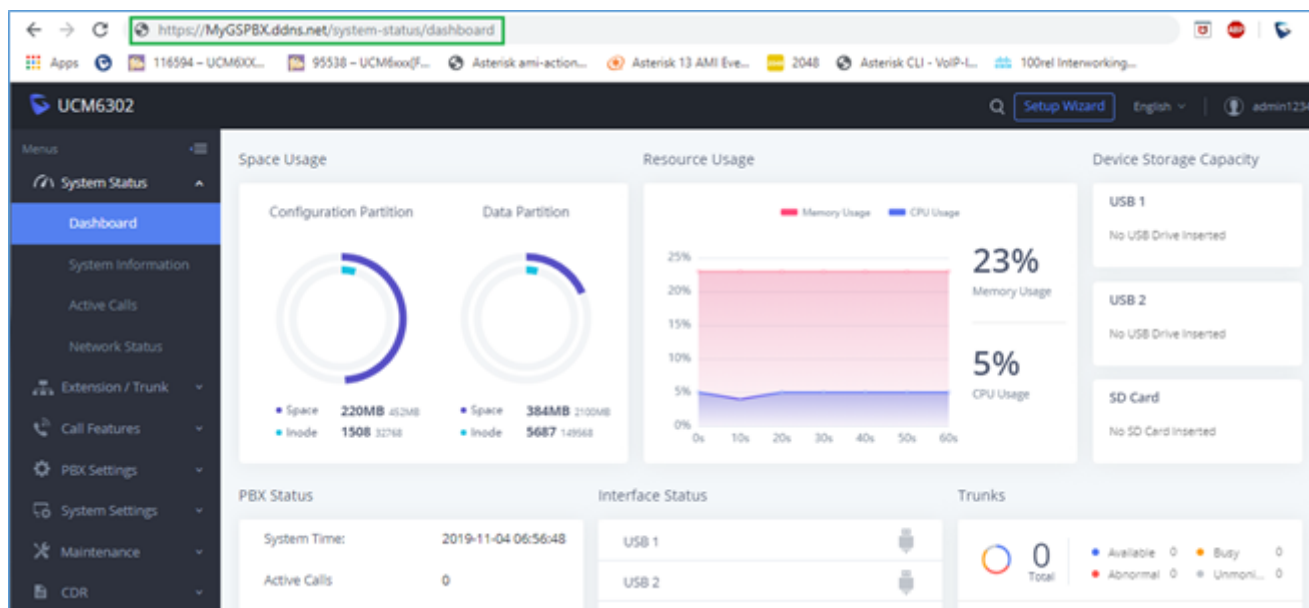
* Username: user_no_ip

* Password:

* Host Name: MyGSPBX.ddns.net

UCM630xA DDNS Setting

- 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
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.

Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping request. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (UCM630xA) interface.
SYN-Flood Defense Enable	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. eth(0)LAN defends against attacks directed to the LAN IP address of the UCM630xA. eth(1)WAN defends against attacks directed to the WAN IP address of the UCM630xA. SYN Flood Defense will limit the amount of SYN packets accepted by the UCM from one source to 10 packets per second. Any excess packets from that source will be discarded.
Ping-of-Death Defense Enable	Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (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: Reject_SSH_WAN

* Action: REJECT

* Type: IN

* Interface: WAN

* Service: SSH

Create New Firewall Rule

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. ACCEPT REJECT DROP
Type	Select the traffic type. IN If selected, users will need specify the network interface "LAN" or "WAN" (for UCM630xA) for the incoming traffic. OUT
Interface	Select the interface to use the Firewall rule.
Service	Select the service type. FTP SSH Telnet HTTP LDAP Custom If "Custom" is selected, users will need specify Source (IP and port), Destination (IP and port) and Protocol (TCP, UDP or Both) for the service. Please note if the source or the destination field is left blank, it will be used as "Anywhere".
Source IP Address and Port	Configure a source subnet and port. If set to "Anywhere" or left empty, traffic from all addresses and ports will be accepted. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
Destination IP Address and Port	Configure a destination subnet and port. If set to "Anywhere" or left empty, traffic can be sent to all addresses and ports. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
Protocol	Select the protocol for the rule to be used.

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.

Dynamic Defense Enable	Enable dynamic defense. The default setting is disabled.
Blacklist Update Interval	Configure the blacklist update time interval (in seconds). The default setting is 120.
Connection Threshold	Configure the connection threshold. Once the number of connections from the same host reaches the threshold, it will be added into the blacklist. The default setting is 100.
Dynamic Defense Whitelist	Allowed IPs and ports range, multiple IP addresses and port range. For example: 192.168.2.100-192.168.2.105, 1000:9999

The following figure shows a configuration example like this:

- If a host at IP address 192.168.5.7 initiates more than 20 TCP connections to the 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.

Static Defense **Dynamic Defense** Fail2Ban SSH Access

Dynamic Defense

Dynamic Defense Enable: ☒

* Blacklist Update Interval: 500 (s):

* Connection Threshold: 20

Dynamic Defense Whitelist: 192.168.5.100-192.168.5.200 1500:2000

Configure Dynamic Defense

Geo-IP Access Control

This feature allows administrators to control access to the UCM based on the source country or region of incoming IP addresses. When enabled, access from selected countries can be restricted for all external services, including Web GUI access, API access, SIP signaling, and extension registration.

The country/region IP database can be updated manually or automatically to ensure accurate IP-to-location mapping.

Security Settings

Static Defense Dynamic Defense Geo-IP Access Control Fail2Ban

Geo-IP Access Control  

 Does not affect intranet.

Strict Defend Mode  ☐

Update Country/Region

Scheduled Update  **Scheduled Task**

Last Detect: No update history

Country/Region Updates: -

Country/Region Allowlist

☐ Continent 	Country/Region 	Allow Access 
☐ Asia	Afghanistan	
☐ Europe	Aland Islands	
☐ Europe	Albania	
☐ Africa	Algeria	
☐ Oceania	American Samoa	
☐ Europe	Andorra	
☐ Africa	Angola	
☐ North America	Anguilla	

UCM Geo IP Access Control Page

Country/Region IP Defense supports **two enforcement methods**, which determine how and when traffic from blocked countries is handled.

- 1. Non-Strict Defend Mode:** In this mode, Country/Region IP Defense is enforced with business priority. Traffic from blocked countries is rejected at the application/service layer. The UCM returns explicit responses (for example, SIP error responses or HTTP error pages). Services remain reachable, but access is denied.
- 2. Strict Defend Mode:** In this mode, Country/Region IP Defense is enforced with security priority. Traffic from blocked countries is dropped at the network level, and no SIP, HTTP, or HTTPS response is returned. Requests do not reach the Web server, SIP stack, API services, or Wave services.

- The defense priority is: Static Defense (firewall rules) -> Country/Region IP Defense (Strict) -> Dynamic Defense -> Fail2Ban -> Extension/Service ACLs -> Country/Region IP Defense (Non-Strict).
- Strict Defend Mode is disabled by default. Enabling or disabling this option may reload the Web service and interrupt active management sessions.

Fail2ban

Fail2Ban feature on the UCM630xA provides intrusion 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 a certain period as defined in "Banned Duration". This feature helps prevent SIP brute force attacks on the PBX system.

Fail2ban is enabled by default.

Security Settings
Static Defense
Dynamic Defense
Geo-IP Access Control
Fail2Ban
SSH Access
Data/File Encryption

Basic Protection

SIP Defense
Login Attack Defense

Customer Service Protection

Customer Service System Call Defense
Live Chat Protection

Global Protection Settings

Banned Duration (s)
600
Valid range is 0-999999999. 0 indicates permanent ban

Cancel
Save

Allowlist

Add

IP
Description / Comment


No data

Blocklist

Add

Banned Type
IP
Time
Description / Comment

Fail2ban Settings

The table below describes the main parameters of the Fail2Ban feature:

SIP Defense	If enabled, which is the default setting, The UCM will monitor failed SIP registration attempts and heartbeat timeouts based on the security logs. Once the number of failed attempts from an IP address has reached SIP Defense's configured Max Retries value, the IP address will be banned for the amount of time configured in the Banned Duration field.
Login Attack Defense	When enabled, which is the default setting, once the number of login attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will be banned for the amount of time configured in the Banned Duration field.
Customer Service System Call Defense	Once the number of call attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will be banned for the amount of time configured in the Banned Duration field.
Live Chat Protection	Once the number of chat attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will be banned for the amount of time configured in the Banned Duration field.
Banned Duration (s)	Configure the duration (in seconds) that an IP address is banned. 0 indicates a permanent ban.
Fail2ban Allowlist	Configure IP address, CIDR mask or DNS host in the allowlist. Fail2ban will not ban the host with matching address in this list.
Blocklist	Users will be able to manually add or view the IPs that have been automatically blocked by the UCM.

SSH Access

SSH switch now is available via Web GUI and LCD. 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

Enable SSH Access	This option is used for system debugging. Once enabled, UCM will allow SSH access. The SSH connection requires super administrator's username and password. The default setting is "No". It is recommended to set it to "No" if there is no need for debugging.
SSH Port	Define the SSH service port.
GDMS Remote SSH	Please enter the token to request SSH data.
Access Token	Enter the token to establish SSH access.

Data/File Encryption

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

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

❗ 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



Data/File Encryption Status

Encrypt

☐ Type	Security	Options
☐ Config File	Strong	
☐ IM Files	Strong	
☐ IM Message	Unencrypted	
☐ Recording Files	Unencrypted	
☐ Video Recording Files	Unencrypted	
☐ Voicemail	Unencrypted	

Cancel

Save

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

❗ 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.

FileData 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 clicks 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

Secret Key ExportUpdate

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

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

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

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

Data/File Encryption Status

Encrypt

☐ Type	Security	Options
☐ Config File	Strong	
☐ IM Files	Strong	
☐ IM Message	Unencrypted	
☐ Recording Files	Unencrypted	
☐ Video Recording Files	Unencrypted	
☐ Voicemail	Unencrypted	

DataFile Encryption Status

The user can select the types of stored files to encrypt, then use the button to start the encryption. Or you can encrypt the files using the following encrypting button .

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

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

UCM6300/A Series IP PBX - CDR Tool Guide

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

data encryption will require the user to perform a factory reset.

- Backing up the data of the PBX before upgrading the firmware is highly recommended to avoid the possibility of data corruption/loss.

LDAP Server

The 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.

LDAP Server

LDAP Server Configurations

LDAP Phonebook

LDAP Server



 If enabled, the UCM can be used as an LDAP server.

LDAP Port

389

Range 1 - 65535

LDAPS Port

636

Range 1 - 65535

* 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 CA Cert

server.ca



Reset

TLS Compression



Private Certificate and Key

LDAP Cert

server.crt



LDAP Private Key

private.key



Cancel

Save

LDAP Server Configurations

Enable LDAP Server	Enable LDAP Server
LDAP Port	Enter the port number for LDAP service. The default port number is 389. The allowed range is 1 - 65535
LDAPS Port	LDAPS server port is predefined and cannot be set by the user. The default port number is 636. The allowed range is 1 - 65535
Base DN	Specifies the location in the directory where the search is requested to begin. It is predefined and cannot be modified.
PBX DN	Specifies the location in the directory where the search for PBX entry is requested to begin. It narrows the search scope and decreases directory lookup time.
Root DN	Specifies the location in the directory where the search for the admin user entry is requested to begin. It narrows the search scope and decreases directory lookup time.
Root Password	Defines the root password for authentication.
Confirm Root Password	Confirms the root password for authentication.
LDAP CA Cert	Upload the LDAPS certification authority certificate.
TLS Compression	If this option is enabled, compression will be performed when transmitting the data. Enabling this option is not recommended since it may present a security risk. Note: This option is disabled by default.
LDAP Cert	Upload the LDAP server certificate
LDAP Private Key	Upload the LDAP private key.
Certificate & Private Key	Click this button to reset the certificate and key configuration.

The 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.

+ Add

Phonebook Download Configurations

Import Phonebook

Export Selected Phonebook

☐ PHONEBOOK DN

OPTIONS

☐  ou=pbx,dc=pbx,dc=com 30



< 1 >

Total: 1 10 / page Goto 1

Default LDAP Phonebook DN

< Edit Phonebook: pbx

+ Add Contact

EXTENSION	CALLERID NAME	OPTIONS
1000		 
1001		 
1002		 
1003		 
1004		 
1005		 
1006		 
1007		 
1008		 
1009		 

< 1 2 3 >

Total: 30 10 / page Goto 1

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 Server Configurations [LDAP Phonebook](#)

Note: The first phonebook is for extensions in this PBX. The contacts cannot be added or deleted directly. To add or delete the contacts, please modify the accounts in "Extensions" page first. To modify the read-only attributes, please edit the corresponding items in "Extension" page, and the phone book will be automatically updated when the change is saved and applied. Users can add other phonebooks for external accounts. For those phonebooks, users can edit LDAP attributes and add or delete contacts directly.

[Add](#) [Phonebook Download Configurations](#) [Import Phonebook](#) [Export Selected Phonebook](#) [LDAP Settings](#)

☐ Phonebook DN ☐ Options

☐ ou=pbx,dc=pbx,dc=com 10

Total: 1 1 10 / page Goto

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.

ik: pbx

nal Contacts

CallerID Name	Email	Options
Arthur Morgan	morgan.arthur@email.com	
Abigail Stevens		

LDAP Phonebook Search Bar

- Add new phonebook

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

Add Phonebook

* Phonebook Prefix:

Phonebook DN:

Add LDAP Phonebook

Configure the "Phonebook Prefix" first. The "Phonebook DN" will be automatically filled in. For example, if configuring "Phonebook Prefix" as "people", the "Phonebook DN" will be filled with

"ou=people,dc=pbx,dc=com".

Once added, users can select

to edit the phonebook attributes and contact list (see figure below) or select

to delete the phonebook.

< Edit Phonebook: GStest

+ Add Contact

ACCOUNTNUMBER

CALLERID NAME

EMAIL

OPTIONS

062514356

Dr. Smith

<

1

>

Total: 1

10 / page

Goto

1

Edit LDAP Phonebook

- Import phonebook from your computer to LDAP server

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

Import Phonebook

Please use UTF-8 encoding when importing CSV, VCF, or XML files.Import file: Account Number and Phonebook DN are required.

File Type:

CSV

File:

Choose File to Upload

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 Nam	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	1004	1004		Accounting	1004000000			phonebook
6	Steve	Chang	1005	1005		Support	1005000000			others

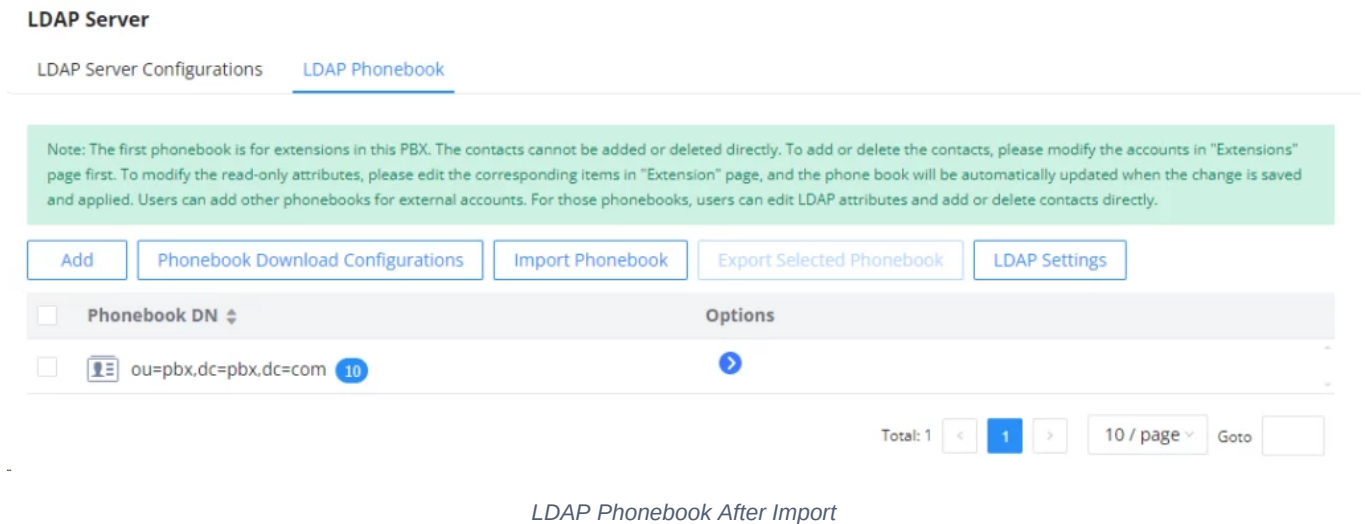
Phonebook CSV File Format

The Phonebook DN field is the same "Phonebook Prefix" entry as when the user clicks on "Add" to create a new phonebook. Therefore, if the user enters "phonebook" in "Phonebook DN" field in the CSV file, the actual phonebook DN "ou=phonebook,dc=pbx,dc=com" will be automatically created by the 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.

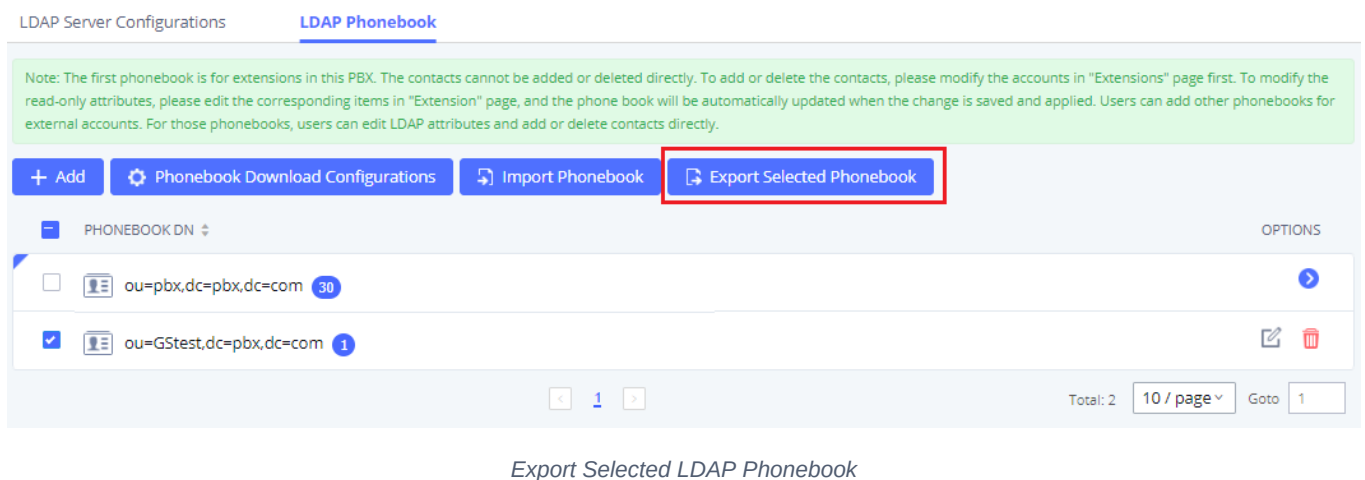
The sample phonebook CSV file in above picture will result in the following LDAP phonebook in the UCM630xA.



As the default LDAP phonebook with DN "ou=pbx,dc=pbx,dc=com" cannot be edited or deleted in LDAP phonebook section, users cannot import contacts with Phonebook DN field "pbx" if existed in the CSV file.

- Export phonebook to your computer from 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.



LDAP Settings

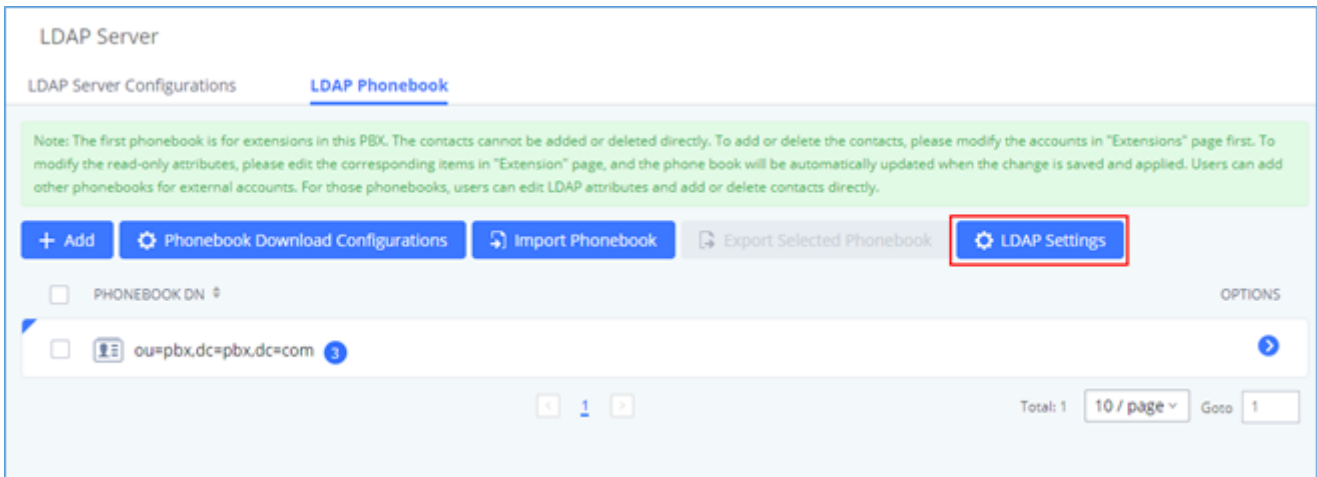
Prerequisites to support contacts sync-up to IP Phones, UCM needs to support the following:

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.

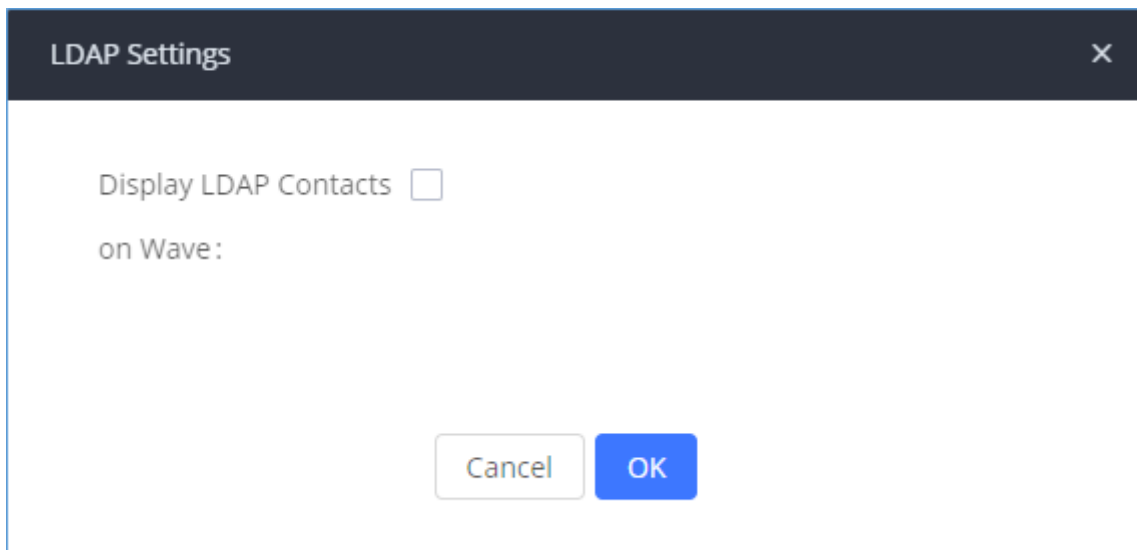
To support contacts sync-up to Wave, it allows Wave to obtain enterprise contacts from Cloud IM or LDAP. On UCM SIP peer trunk, if LDAP sync is enabled, end point can obtain remote UCM extensions' info via LDAP. Also, it will allow configuring whether to sync up LDAP contacts on Wave so that Wave doesn't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

Phonebook Name	Enter a name for the phonebook
----------------	--------------------------------

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

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

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

Phonebook Download Configurations Cancel Save

* LDAP Server:

* Base DN:

* Password:

* Port:

Client Type:

LDAP Automatic Update Cycle:

LDAP Client CA Cert: Reset Certificates

LDAP Client Private Key: Reset Certificates

* Server Address:

* Username:

* Filter:

LDAP Name Attributes:

* LDAP Number Attributes:

LDAP Client Configurations

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

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

- **Port:** 389

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

LDAP

LDAP protocol	LDAP ▼
Server Address	192.168.40.134
Port	389
Base	dc=pbx,dc=com
User Name	
Password	
LDAP Number Filter	(AccountNumber=%)
LDAP Name Filter	(CallerIDName=%)
LDAP Version	☐ Version 2 ☒ Version 3
LDAP Name Attributes	CallerIDName
LDAP Number Attributes	AccountNumber
LDAP Display Name	AccountNumber CallerIDName
Max. Hits	50
Search Timeout	30
Sort Results	☒ No ☐ Yes
LDAP Lookup	☒ Incoming Calls ☒ Outgoing Calls
Lookup Display Name	
Save Save and Apply Reset	

GXP2170 LDAP Phonebook Configuration

AD Client Type

Phonebook Name	Enter a name for the phonebook
Server Address	The IP address of the AD server
Base DN	Enter the base domain name.
Username	Enter the username used to authenticate into the LDAP server, if authentication is required.
Password	Enter the password used to authenticate into the LDAP server, if authentication is required.

Filter	Enter the filter. Ex: ((CallerIDName=%)(AccountNumber=%))
Port	Enter the port number. Default port is 389
AD Attributes	AccountNumber must be included if the default configuration is used.
Automatic Update Cycle	If "None" is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
Host Name	Enter the host name of the remote AD server.

Time Settings

Automatic Date and Time

The current system time on the 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**.

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.

Parameter	Description
Remote NTP Server	Configure the NTP server address to synchronize the time and date from.
Enable DHCP Option 2	If enabled, DHCP Option 2 will override the Time Zone setting on the PBX.
Enable DHCP Option 42	If enabled, DHCP Option 42 will override the NTP server configured on the PBX.
Time Zone	Choose the correct time zone according to your location.
Update Time Zone List	Clicking this button updates the list of timezones.
Scheduled Update	Configure schedule time zone update.

Remote NTP Server

pool.ntp.org

Enable DHCP Option 2

☒

Enable DHCP Option 42

☒

* Time Zone

(UTC+00:00) Etc/GMT-0

Update Time Zone List

Cancel

Save

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

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.

Menus

System Status

Extension / Trunk

Call Features

PBX Settings

System Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Create New Office Time

Time:

09:00

-

18:00

Week:

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Show Advanced Options:

☒

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

Create New Office Time

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

Create New Office Time

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

Time Settings

Automatic Date and Time

Set Date and Time

NTP Server

Office Time

Holiday

+ Add

Delete

☐	INDEX	TIME	WEEK	MONTH	DAY	OPTIONS
☐	1	09:00-18:00	Mon Tue Wed Thu Fri	Default	Default	

Settings→Time Settings→Office Time

- Click on

to edit the office time.
- Click on

to delete the office time.
- Click on **"Delete"** to delete multiple selected office times at once.

Holiday

On the UCM, the system administrator can define Holidays, which can be used by Inbound Routes, Call Forwarding, and other time based features such as Paging/Intercom. To configure holidays, log in to the Web GUI and navigate to System **Settings->Time Settings->Holiday**.

From this page, the administrator can:

- Configure **new** new holidays using the "Add" button.
- **Edit** existing holidays by clicking the "Edit" icon for a specific holiday.
- **Delete a single** holiday by clicking the "Delete" icon.
- **Delete multiple** holidays at once by selecting them and clicking the "Delete" button.
- **Import** holiday configurations using the "Import" button.
- **Export** holiday configurations using the "Export" button.

Time Settings

Automatic Date and Time

Set Date and Time

NTP Server

Office Time

Holiday

Custom Time Groups

The Holiday time condition comprises of the following dates and times below.

Add

Delete

Import

Export

☐	Name	Week	Year	Month	Day	Time	Description	Options
☐	New_Year	Default	All	Jan	1	00:00-23:59		

Holiday Settings

When creating/editing a holiday, users can configure the parameters described in the table below:

Time Settings > Create New Holiday

Name

New_Year

Description

Year

All

Month

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

Configuration Method ⓘ
☒ By Date ☐ By Week

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				

Time

00:00 - 23:59

Cancel

Save

Create a New Holiday Entry

Parameter	Description
Name	Specifies the name of the holiday. Used to identify the holiday in related features.
Description	Optional description for the holiday.
Custom Prompt	Selects a custom voice prompt or generate a prompt using AI to play during the holiday period for inbound calls or time-based routing rules. Custom prompts can be managed under PBX Settings -> Voice Prompt -> Custom Prompt.
Year	Specifies the year in which the holiday applies. Select All to configure a recurring annual holiday.
Month	Select the month in which the holiday occurs.
Configuration Method	Defines how the holiday date is determined. The options are: By Date: Used for holidays with a fixed calendar date. By Week: Used for holidays defined by a weekday pattern within a month (for example, the fourth Thursday of a month).
Day	Displayed when Configuration Method is "By Date". Choose one or more calendar dates within the selected month to be treated as holidays.
Sequence	Displayed when Configuration Method is "By Week". Select the occurrence of the weekday within the month, such as First, Second, Third, Fourth, or Fifth.
Week	Displayed when Configuration Method is "By Week". Select the day of the week (Sunday through Saturday).
Time	Specifies the effective time range of the holiday. The holiday is active from the start time to the end time on the configured date(s).

Custom Time Groups

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

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

Start Time

-

End Time

Frequency

☒ By Week

☐ By Month

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Add

Time	Week	Month	Day	Options

Cancel

Save

Custom Time Groups

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

Email Settings

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
Mail Server Providers	Select the mail server provider type: Common: Select this option when integrating email services such as Gmail or on-premise email servers. Microsoft: Select this option when integrating email services provided by Microsoft Outlook. Note: The settings below appear when selecting "Common".
TLS Enable	If enabled, TLS will be used when forwarding emails to the SMTP server.
Type	Select the mail processing type: MTA: Mail Transfer Agent. The configured domain will be used in the sender address. Warning: Emails sent by MTA may be considered spam by the destination SMTP server. Client: Send emails to the configured SMTP server, which will then forward the emails to the destination address.
Email Template Sending Format	Select the email template format to be sent. The "HTML" format is compatible with most mail clients and is recommended. If the mail client does not support HTML, select "Plain Text".
Mail Server Domain	Enter the domain name of the mail server (e.g., grandstream.com).
SMTP Server	Enter the SMTP server address (e.g., smtp.gmail.com:587). Port number is optional.
Enable SASL Authentication	Toggles SASL authentication. If disabled, the IPPBX will not use username and password for email client authentication. Most email servers require login authentication. If using Microsoft Exchange Server or if credentials are not required, disable this option.
Username	Enter the username of the email account.
Password	Enter the password of the email account. It is highly recommended to use HTTPS when saving and applying password changes.
Enable Email-to-Fax	Monitors the inbox of the configured email address for the specified subject. If detected, the IPPBX retrieves the attachment and sends it to the target extension by fax. The attachment must be in PDF/TIF/TIFF format.
Email-to-Fax Blocklist/Allowlist	Enable or disable the Email-to-Fax Blacklist or Whitelist.
Email-to-Fax Subject Format	Select the email subject format to use for email-to-fax. XXX refers to the target extension that the fax will be sent to.
Notify Sender of Result	If enabled, the UCM will send an email notification back to the sender containing the fax transmission result.
Notify Admin of Fax Failure	Configures a unified administrator email address. When enabled, the UCM automatically sends an email notification to this specified address whenever an Email-to-Fax transmission fails.
Internal Block/Allowlist	Email address blacklist/whitelist for local extensions. Displayed when Email-to-Fax Blocklist/Allowlist is enabled.
External Block/Allowlist	Email address blacklist/whitelist for non-local contacts. Separate multiple addresses with semicolons (;). Displayed when Email-to-Fax Blocklist/Allowlist is enabled.
POP/POP3 Server Address	Enter the IP address or domain of the POP/POP3 server.
POP/POP3 Server Port	Enter the port number of the POP/POP3 server.
Display Name	Enter the name of the PBX that will be displayed in sent emails.
Sender	Enter the email address used to send out emails from the PBX.
Email Settings (Test)	Click Test to verify if the email integration is functioning correctly. Note: Save and apply changes before running the email test.

For a step-by-step configuration of Microsoft Outlook email services, please refer to the following guide:
<https://documentation.grandstream.com/knowledge-base/grandstream-ippbx-microsoft-outlook-authentication-guide/>

The following figure shows a sample Email setting on the UCM630XA, assuming the Email is using 192.168.6.202 as the SMTP server.

Email Settings

Email Settings

Email Template

Email Footer Hyperlink

Email Send Log

Mail Server Providers

Common

TLS Enable

☒

Type

Client

Email Template Sending Format

HTML

* Mail Server Domain

example.com

* SMTP Server

smtp.mycompany.com:587

Enable SASL Authentication

☒

* Username

pbx1@mycompany.com

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

* Password

.....

Enable Email-to-Fax

☒

Email-to-Fax Blocklist/Allowlist

Disable

Email-to-Fax Subject Format

SendFaxMail To XXX

Fax Sending Success/Failure Confirmation

☐

Cancel

Save

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.

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

Email Settings **Email Template** Email Footer Hyperlink Email Send Log

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 Settings

Email Settings Email Template **Email footer hyperlink** Email Send Log

* Text:	Company Info	* URL:	https://www.grandstream.com	
* Text:	Contact Us	* URL:	https://www.grandstream.com/contact-us?	

[Add](#)

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 Settings Email Template Email footer hyperlink **Email Send Log**

■ In MTA mode, SPF authentication cannot be received. Therefore, even if an email is sent successfully, the return code of 550 will still be returned. Many email servers will place non-SPF-certified mail into the trash or spam folder. If the recipient has not received a sent email, please check to see if the sent email was placed in the recipient's trash or spam folder. In Client mode, a 250 return code indicates that the email has been sent successfully to the configured SMTP server. If emails from the UCM are not being received, please check the inbox of the configured client email address for any email bounce notifications.

■ In Client mode, a 250 return code indicates that the email has been sent successfully to the configured SMTP server. If emails from the UCM are not being received, please check the inbox of the configured client email address for any email bounce notifications.

Display Filter ▾

EMAIL GENERATED TIME	EMAIL SEND MODULE	RECEIVERS	LAST SEND TIME	LAST SEND ADDRESS	SEND RESULT	RETURN CODE	OPTIONS
No Data							

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 then with comma and no spaces.
Send Result	Enter the status of the send result to filter with
Return Code	Enter the email code to filter with
Email Send Module	Select the email module to filter with from the drop-down list, which contains: All Modules Extension Voicemail Meeting Schedule User Password Alert Events CDR Test

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	①
2020-12-21 18:00:04	Video Conference Schedule	m.g@gmail.com	12-21 18:00:06	m.g@gmail.com	sent	250	①
2020-12-20 18:00:04	Video Conference Schedule	m.g@gmail.com	12-20 18:00:07	m.g@gmail.com	sent	250	①
2020-12-19 18:00:03	Video Conference Schedule	m.g@gmail.com	12-19 18:00:06	m.g@gmail.com	sent	250	①
2020-12-18 18:00:03	Video Conference Schedule	m.g@gmail.com	12-18 18:00:06	m.g@gmail.com	sent	250	①
2020-12-17 18:00:03	Video Conference Schedule	m.p@gmail.com	12-17 18:00:06	m.p@gmail.com	sent	250	①

1
2
3
4

Total: 32 10 / page

Goto 1

Email Logs

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

Code	Description
250	Mail sent successfully
501	Address format parsing error, 501 will be returned when there are unacceptable characters in the recipient's email address in MTA mode. Please check if the recipient's email address format is correct. The "sender" configured on the client is your mail account.
535	The user name and password verification in the client mode is incorrect. Please check whether the user name and password are configured correctly.
550	Possible reasons: 1. The recipient's mailbox user name does not exist or is in a banned state, please check whether the email recipient is the correct email address. 2. The number of destination addresses sent by the sender exceeds the maximum limit per day and is temporarily blacklisted. Please reduce the sending frequency or try again the next day. 3. The sender's IP does not pass the SPF permission test of the sending domain. Emails sent in MTA mode may return this error code even if they are sent.
552	The sent email is too large or the email attachment type is prohibited
553	The sender and the email account are inconsistent, please configure the sender as your email account correctly.
554	The email was identified as spam. Please reduce the sending frequency or try again the next day

none	Indicates that there is no return code. If the sending result is "deferred", the general reason is that the mail service area is configured incorrectly. Please check whether the server configuration is correct. If the sending result is "bounced", the general reason is that the receiving email address domain name is wrong, please check whether the email recipient is the correct email address. If it is in MTA mode, please check whether the "domain" is configured to be in the same domain name as the "recipient".
------	--

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.

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

SMS Settings

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

If an extension is using the SMS feature, please ensure that it has a properly formatted mobile number configured (i.e., country code + mobile number).

Enable SMS

☒

* SMS Carrier

Region

* Account ID

* Secret

* From

+1

Cancel

Save

Save and Test

SMS Settings

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

SMS Carrier	Parameter	Description
Twilio	Account ID	The Account SID provided in your Twilio Console dashboard used to authenticate API requests.
	Auth Token	The secret authentication token associated with your Twilio Account SID.
	Messages Server ID	The Messaging Service SID created within Twilio for handling outgoing message pools.
	From	The authorized Twilio phone number (including country code) assigned to send outbound SMS messages.
Amazon	Region	The AWS region where your instance is hosted (e.g., us-east-1).

Amazon	Account ID	The AWS Access Key ID generated from the AWS IAM console for API access.
	Secret	The AWS Secret Access Key corresponding to the Access Key ID used for request signing.
VoiceMeUp	Account ID	The primary account or username credential assigned by VoiceMeUp for portal and API access.
	Auth Token	The API authentication token generated within the VoiceMeUp portal under API settings.
	From	The SMS-enabled VoiceMeUp DID or phone number configured as the originating sender ID.
Voxtelesys	API Key	The bearer/API authorization key generated in the Voxtelesys Portal under API Credentials.
	From	The SMS-enabled Voxtelesys phone number assigned to your account used as the sender ID.

SMS Template

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

SMS Settings > SMS Settings

SMS Settings SMS Template SMS Delivery Log

ⓘ SMS templates are subject to carrier specifications. Please refer to the operator's requirements. More details can be found here: [Amazon](#) [Twilio](#) [VoiceMeUp](#) [Voxtelesys](#)

System SMS Templates

Type	Template Content	Options
Verification Code	<code>\$DEVICE_ID</code> Your verification code is <code>\$code</code> . It will expire in 10 minutes.	
Alarm Notification	<code>\$DEVICE_ID</code> <code>\$userName</code> <code>\$newAddr</code> system event: <code>\$content</code>	

Custom SMS Templates

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

ⓘ This template is only supported for use in IVR services.

Type	Template Content	Options
Template1	Official Website: https://marketing.org	

Total: 1 10 / page

SMS Templates are categorized into two sections:

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

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

IVR > Edit IVR: IVR-SC1-French

Basic Settings Key Pressing Events

Key Event Type Standard Custom

Key Events

Key 0

Destination	SMS	Template1	Time Condition	All Time
-------------	-----	-----------	----------------	----------

SMS Delivery Log

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

SMS Settings

SMS SettingsSMS TemplateSMS Delivery Log

Show All LogsClearDelete Search Result(s)Display Filter

SEND RESULT	RECIPIENT	SMS CATEGORY	SEND TIME
No data			

}

HA

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

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

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

HA settings

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

HA

HA Settings

HA Log

① When setting up an HA dual-system, please ensure that the models and firmware versions of the two devices used for HA are the same. Otherwise database compatibility issues may occur.
When connecting external USB devices, it is recommended to use USB3.0 for both machines. Please ensure that the specifications for both USB devices are the same. Otherwise, you may experience abnormal behavior.
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 

☒

Local Hot Standby 

☐ Remote Disaster Recovery 

Force Switch 

Switch

* Hot Standby Station Type 

Secondary

* Hot Standby Cluster IP 

192.168.0.10

* Hot Standby Peer IP 

192.168.0.11

* Hot Standby Peer MAC Address 

C0:74:AD:AA:AA:AA

* Heartbeat Port 

9527

* Heartbeat Timeout Period (s) 

7

Network Detection 

☒

* Network Detection Node 

IP Address

Software Fault Switch

☐

Hardware Fault Switch 

☐ FXO1

☐ FXO2

Enable IPv6 

☐

Sync External Storage Files 

Sync

Learn more about HA Settings with the [HA Local Standby User Guide](#) | [HA Remote Disaster Recovery User Guide](#)

Local Hot Standby Settings

This table describes parameters used when configuring local HA between two UCM systems within the same site.

Parameter	Description
High Available Enable	Enables/disables the HA functionality. By default, it's disabled.
Force Switch	Clicking the button will immediately force a switchover to the standby UCM.
Hot Standby Station Type	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the 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.
Hot Standby Cluster IP	Used in single-NIC mode. This is the shared virtual IP address used by both active and standby UCMs. The IP must be static and must not match the local IP of either device.
Hot Standby Cluster IP 1	Displayed in Dual-NIC mode. Cluster virtual IP used for the LAN1 subnet. Mandatory. Must not match the local LAN1 IP and must be unique.
Hot Standby Cluster IP 2	Displayed in Dual-NIC mode. Cluster virtual IP used for the LAN2 subnet. Mandatory. Must not match the local LAN2 IP and must be unique.
Hot Standby Peer IP	Local IP address of Hot Standby peer device.
Hot Standby Peer MAC Address	The MAC address of Hot Standby peer device.

Heartbeat Port	The number of the heartbeat port should be consistent with the peer heartbeat port.
Heartbeat Timeout Period (s)	Upon timeout, the Standby UCM will take over services.
Network Detection	Enable/Disable Network Detection feature. When enabled, the active device continuously checks reachability to the configured detection node(s). If the active device loses connectivity to any configured detection node a switchover is triggered and the standby device assumes the active role. Note: HA settings on both the active and standby UCM must be consistent. In case of inconsistency, the settings on the active device will be prioritized.
Network Detection Node	Displayed in Switch and Route mode. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on active and standby devices.
Network Detection Node 1	Displayed in Dual mode. This detection node associated with Cluster IP1 / LAN1. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 2	Displayed in Dual mode. Detection node associated with Cluster IP2 / LAN2. If configured, loss of connectivity to this node on the active device will also trigger a switchover. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Software Fault Switch	Enable Software Fault Switch.
Hardware Fault Switch	If issues are detected with the selected connection interfaces, the backup UCM will take over services after the master/slave handover. If not checked, UCM will send only a fault alarm.
Enable IPv6	If enabled, HA on UCM can be used with IPv6 while compatible with IPv4.
Scan External Storage Files	Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page. It is recommended to configure external storage data synchronization when forming HA for the first time. If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.

Local Hot Standby

The table below describes parameters used for Remote Disaster Recovery HA, where two UCM systems are deployed at different sites.

HA

[HA Settings](#)
[HA Log](#)

① When setting up an HA dual-system, please ensure that the models and firmware versions of the two devices used for HA are the same. Otherwise database compatibility issues may occur. When connecting external USB devices, it is recommended to use USB3.0 for both machines. Please ensure that the specifications for both USB devices are the same. Otherwise, you may experience abnormal behavior.

High Available Enable ①
☒

HA Mode ①

☐ Local Hot Standby ②
☒ Remote Disaster Recovery ②

*Network Port Domain Name

LAN

Force Switch ①

Switch

*Remote Disaster Recovery Station Type ①

Secondary

*Remote Disaster Recovery Peer MAC Address ①

C0:74:AD:AA:AA:AA

*Heartbeat Port ①

9527

*Heartbeat Timeout Period (s) ①

7

*Local Heartbeat IP ①

198.51.100.88

*Local Heartbeat Gateway IP ①

*Local Heartbeat Address Subnet Mask ①

*Peer Heartbeat IP ①

198.51.100.66

Network Detection ①
☒

*Network Detection Node ①

IP Address

Sync External Storage Files ①

Sync

Learn more about HA Settings with the [HA Local Standby User Guide](#) | [HA Remote Disaster Recovery User Guide](#)

Remote Disaster Recovery Settings

Parameter	Description
Network Port Domain Name	Selects the network domain used for remote disaster recovery. In single NIC mode, available options are WAN and LAN. In dual NIC mode, available options are LAN1 and LAN2, corresponding to the two physical LAN interfaces.
Force Switch	Clicking the button will immediately force a switchover to the standby UCM.
Remote Disaster Recovery Station Type	Used for the initial assignment of the HA active/standby role of the UCM system. If set to Primary, the current UCM system will be assigned as the 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.
Remote Disaster Recovery Peer MAC Address	The MAC address of Remote Disaster Recovery peer device
Heartbeat Port	The heartbeat port should be the same as the peer device's heartbeat port.
Heartbeat Timeout Period (s)	Upon timeout, the Standby UCM will take over services.
Local Heartbeat IP	Fill in the IP address of the heartbeat port of the local site, in the format: xxx.xxx.xxx.xxx, which is used for the peer end to detect the local machine status, heartbeat negotiation, and communication address for data synchronization.
Local Heartbeat Gateway IP	Fill in the IP address of the local heartbeat gateway for remote disaster recovery, in the format: xxx.xxx.xxx.xxx

Local Heartbeat Address Subnet Mask	Fill in the subnet mask of the heartbeat address of the remote disaster recovery local end, in the format: xxx.xxx.xxx.xxx, such as: 255.255.255.0.
Peer Heartbeat IP	Fill in the IP address of the heartbeat port of the peer site, in the format: xxx.xxx.xxx.xxx, which is used to detect peer status, heartbeat negotiation, and communication address for data synchronization.
Network Detection	Enable/Disable Network Detection feature. When enabled, the active device continuously checks reachability to the configured detection node(s). If the active device loses connectivity to any configured detection node a switchover is triggered and the standby device assumes the active role.Note: HA settings on both the active and standby UCM must be consistent. In case of inconsistency, the settings on the active device will be prioritized.
Network Detection Node	Displayed in Switch and Route mode. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 1	Displayed in Dual mode. This detection node associated with Cluster IP1 / LAN1. If connectivity to this node is lost on the active device, a switchover is triggered. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Network Detection Node 2	Displayed in Dual mode. Detection node associated with Cluster IP2 / LAN2. If configured, loss of connectivity to this node on the active device will also trigger a switchover. Notes:The standby device does not initiate switchover on its own.Only IP addresses are supported.For correct operation, this setting must be configured identically on both devices.
Scan External Storage Files	Only applicable if there are more than 5000 UCM files in external storage such as SD card, USB, or NAS. Users can click this button to scan those paths in order to display all available files on the UCM web UI. Configured file storage paths can be viewed on the File Manager page.It is recommended to configure external storage data synchronization when forming HA for the first time, If HA is configured, files created after HA setup will be automatically displayed on the UCM web UI and do not need to be scanned for.

Remote Disaster Recovery

HA Status

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

HA

HA Settings	HA Status	HA Log
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.

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:

162

SNMP Settings

Enable	Tick this box to enable SNMP.
--------	-------------------------------

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

SNMP Community

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

Create New SNMP Community

CancelSave

* Name:

* Access Level:

Read Only

SNMP Community

Name	Enter a name for the community
Access Level	Select an access level: Read Only: The SNMP community will be able only to read SNMP messages.

SNMP 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.

Create New SNMP Trap Destinations

CancelSave

* Name:

* IP Address:

* Port:

162

* Community:

Public

* Type:

Trapsink

SNMP Trap Destinations

Name	Enter a name of your SNMP Trap destination.
IP Address	Enter the SNMP Trap destination's IP address.
Port	Enter the port of the SNMP Trap destination.
Community	Select the community that you want

Type	Select the type of SNMP: Trapsink: Select this option if you want to send SNMP v1 traps. Trap2sink: Select this option if you want to send SNMP v2 traps. Informsink: Select this option if you want to send "Inform" notifications only.
------	---

SNMP Version 3

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.

Create New SNMP V3 Users

[Cancel](#)
[Save](#)

* Name:	
* Authentication Protocol:	MD5 v
* Authentication Password:	
* Privacy Protocol:	DES v
* Privacy Password:	
* Group Level:	Read Only v

SNMP v3

Name	Set the user's name
Authentication Protocol	Select the authentication protocol: MD5 SHA
Authentication Password	Set the authentication password.
Privacy Protocol	Select the protocol to use to encrypt the data DES AES-128 AES-192 AES-256
Privacy Password	Set the privacy password.
Group Level	Set the group level: Read Only. Read/Write.

SNMP Trap Proxy

Create New SNMP Trap Proxy

[Cancel](#)
[Save](#)

* Name:	
* IP Address:	
* Port:	

SNMP Trap Proxy

Name	Enter a name for the proxy server.
------	------------------------------------

IP Address	Enter the proxy server's IP address.
Port	Enter the proxy server's port.

RADIUS

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

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	1812
* Radius Shared Secret	
* Maximum Number of Retransmission	5
* Radius Timeout (s)	3

RADIUS

Enable Radius Web Access Control	Enable or disable Radius.
As Default Login Method	Enable Radius as the default login method to the web UI of the UCM
Radius Auth Server Address	Enter the IP address/hostname of Radius server.
Radius Auth Server Port	Enter the port of radius serverDefault port number is: 1812
Radius Shared Secret	Enter Radius Shared Secret
Maximum Number of Retransmission	Enter the number of retransmissions. The interval is 1 to 5.
Radius Timeout (s)	The maximum seconds before a session expires if there is no response from the server. The interval is between 1 to 30 seconds.

TR-069

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

Parameter	Description
Enable TR-069	Toggle it on to enable TR-069. It is enabled by default

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

ZERO CONFIG

Overview

Grandstream SIP Devices can be configured via Web interface as well as via configuration file through TFTP/HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file and XML format configuration file.

The UCM630xA provides a Plug and Play mechanism to auto-provision the SIP devices in a zero-configuration manner by generating an XML config file and having the device download it within the LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

Zero Config supports centralized provisioning for Grandstream SIP devices and selected third-party enterprise SIP phones. Supported third-party devices can be discovered, configured, and managed using the same Zero Config workflow, except where explicitly limited.

To provision a phone, three steps are involved, i.e., discovery, configuration, and provisioning. This section explains how Zero Config works on the UCM630xA. The settings for this feature can be accessed via **Device Management->Zero Config**.

Zero Config Supported Devices

The following table lists all Grandstream and third-party SIP device series that support Zero Config.

Availability of specific models depends on whether the corresponding model template package is installed.

Vendor	Supported Device Series & Models
Grandstream	GXP Series
	GRP Series
	GXV Series

Grandstream	GHP Series
	GVC Series
	GAC Series
	GSC Series
	GDS Series
	GXW Series
	HT Series
	DP Series
	WP Series
Avaya	J100 Series
Cisco	CP-3905
	CP-6921
	CP-78xx Series
	CP-88xx Series
	DP-98xx Series
Poly	Edge-E Series
	Edge-B Series
	VVX Series (non-OBi)
Yealink	AX Series
	T4 Series
	T5 Series
	T7 Series
	T8 Series

Third-party enterprise device provisioning (Avaya, Cisco, Poly, and Yealink) can be managed and enabled under **Device Management -> Zero Config -> Zero Config Settings -> Manage 3rd-Party Enterprise Phones**.

- Cisco IP Phones support line registration, remote Do Not Disturb (DND) synchronization, and conferencing features.
- Poly Edge B Series support multi-account template mapping across line keys.

Configuration Architecture for Endpoint Device

The end point device configuration in ZeroConfig is divided into the following three layers with priority from the lowest to the highest:

- Global

This is the lowest layer. Users can configure the most basic options that could apply to all SIP devices during provisioning via Zero config.

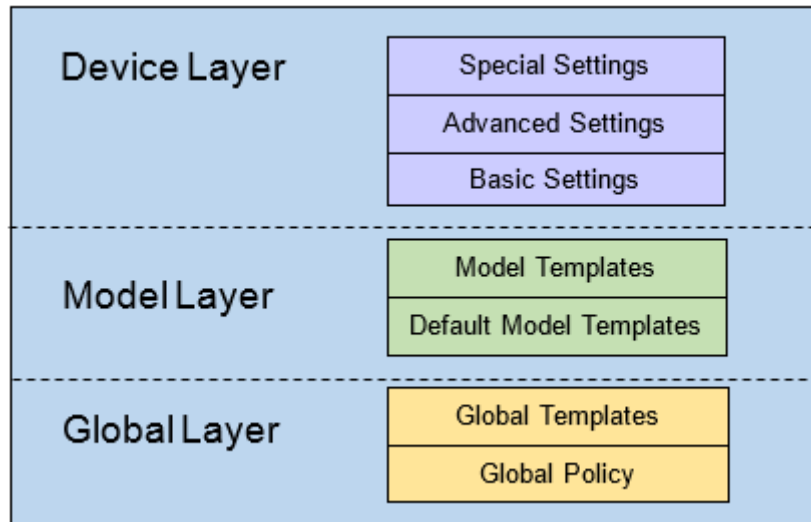
- Model

In this layer, users can define model-specific options for the configuration template.

- Device

This is the highest layer. Users can configure device-specific options for the configuration for the individual device here.

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



Zero Config Configuration Architecture for End Point Device

The configuration options available in the **Model** and **Device** layers fully include those defined in the **Global** layer. In other words, the Global layer options are a subset of the options available at both the Model and Device layers.

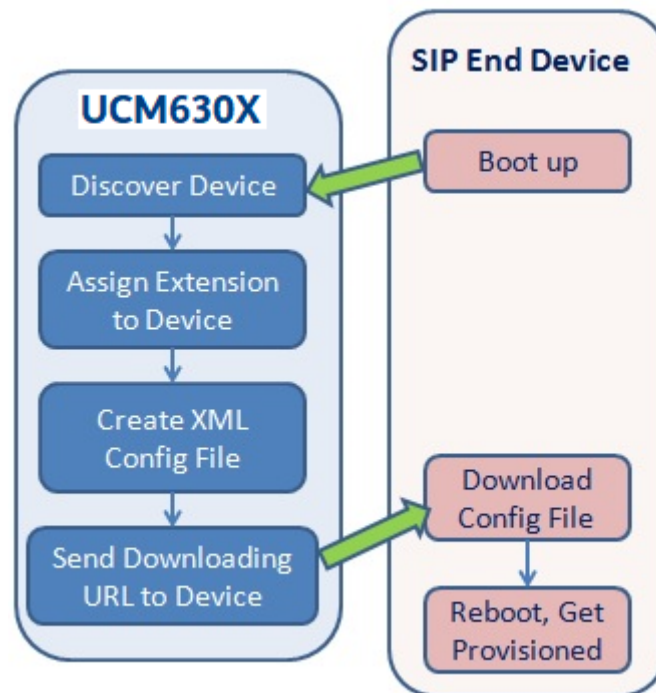
When the same option is configured in multiple layers with different values, the value from the higher-priority layer overrides those from lower-priority layers. Layer priority is as follows (from lowest to highest):

Global->Model->Device.

Example: if English is selected as the language in the Global Policy, and Spanish is selected in the Default Model Template, the device being provisioned will use Spanish, because the Model layer has higher priority than the Global layer.

Auto-Provisioning Settings

By default, the Zero Config feature is enabled on the UCM630xA for auto-provisioning. Three methods of auto-provisioning are used.



UCM630xA Zero Config

- 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.

- 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.

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

Zero Config
Global Policy
Global Templates
Model Templates
Model Update
Firmware
Zero Config Settings

Basic Settings

Enable Zero Config
☒

Automatically Distribute Configuration
☐

Manage 3rd Party Phones
☐

Auto Assign Extension

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 c

Auto Assign Extension
☐

Zero Config Extension Segment
5000 - 6299

Enable Pick Extension
☐

Pick Extension Segment
4000 - 4999

Pick Extension Period (hour)

Network Settings

Subnet Allowlist

Add

Zero Config Settings Page

The table below explains all the configurable parameters that can be found on the Zero Config Settings page:

Basic Settings	
Enable Zero Config	Enable or disable the zero-config feature on the PBX. The default setting is enabled.
Enable Automatic Configuration Assignment	By default, this is disabled. If disabled, when the SIP device boots up, the PBX will not send the SIP device the URL to download the config file, and therefore the SIP device will not be automatically provisioned by the PBX.
Manage 3rd Party Phones	This option controls whether third-party SIP phones can be provisioned using Zero Config. When enabled, port 69 (TFTP) and port 6970 (HTTP) are automatically opened on the UCM for non-encrypted provisioning communication. Only the phone models listed under the [Zero Config Supported Devices] section can be provisioned using this feature. To allow third-party SIP phones to be provisioned, configure the DHCP server in the phone's network with the following options:DHCP Option 66: UCM IP addressDHCP Option 160: http://<UCM-IP>:6970/zccgi Notes :All supported third-party enterprise phones share the same DHCP Option 66 and Option 160 configuration.DHCP Option 66 and Option 160 must be placed before any other identical DHCP options in the DHCP server configuration.HTTP provisioning traffic is not encrypted.Port 6970 is reserved for Zero Config provisioning and cannot be modified.
Auto Assign Extension	
Auto Assign Extension	If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in "Zero Config Extension Segment" to the device. The default setting is disabled.
Zero Config Extension Segment	Click on the link "Zero Config Extension Segment" to specify the extension range to be assigned if "Automatically Assign Extension" is enabled. The default range is 5000-6299. Zero Config Extension Segment-range can be defined in Web GUI->PBX Settings->General Settings->General page->Extension Preference section: "Auto Provision Extensions".

Enable Pick Extension	If enabled, the extension list will be sent out to the device after receiving the device's request. This feature is for the GXP series phones that support selecting extensions to be provisioned via the phone's LCD. The default setting is disabled.
Pick Extension Segment	Click on the link "Pick Extension Segment" to specify the extension list to be sent to the device. The default range is 4000 to 4999. Pick Extension Segment range can be defined in Web GUI->PBX Settings->General Settings->General page->Extension Preference section: "Pick Extensions".
Pick Extension Period (hour)	Specify the number of minutes to allow the phones being provisioned to pick extensions.
Network Settings	
Subnet Allowlist	This feature allows the UCM to provision devices in different subnets other than the UCM network. Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is <IP>/<CIDR>. Examples: 10.0.0.1/8, 192.168.6.0/24. Notes: Only private IP ranges (10.0.0.0 172.16.0.0 192.168.0.0) are supported. Up to 10 subnets can be configured in the allowlist.

Please make sure an extension is manually assigned to the phone or "Automatically Assign Extension" is enabled during provisioning. After the configuration on the 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

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

- PING
- ARP
- SIP Message (NOTIFY)

To start the discover process:

1. Click on "Auto Discover" under **Device Management->Zero Config->Zero Config**.
2. Choose the "Scan Method" and enter the "Scan IP". The IP address segment will be automatically filled in based on the network mask detected on the UCM630xA. If users need to scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address.
3. Click on "Save" to start discovering the devices within the same network. To successfully discover the devices, "Zero Config" needs to be enabled on the **Device Management->Zero Config->Auto Provisioning Settings**.

✕

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

Network Segment 192.168.6.0 - 192.168.6.255

Broadcast IP 192.168.6.255

Scan Method

Ping ▾

Subnet Allowlist

Local Subnet Only ▾

Scan IP

192

·

168

·

6

·

Scan all MACs ☐

MAC OUI Grandstream OUI

000B82	Grandstream	—
C074AD	Grandstream	—
EC74D7	Grandstream	—

Cancel

OK

Auto Discover

The following figure shows a list of discovered phones, displaying the MAC address, IP address, extension (if assigned), version, vendor, model, connection status, Create Config option, and available actions (Edit, Delete, Update, Reboot, and Access Device Web GUI).

Zero Config									
Zero Config Global Policy Global Templates Model Templates Model Update Firmware Zero Config Settings									
Total: 74 Registered: 0 Unregistered: 74 All All Model All Vendor Q: Model / Extension Number / MAC Address / IP Address									
Auto Discover Add Delete Edit Upgrade Update Config Reboot More ▾									
No.	Model	Extension	Vendor	MAC Address	IP Address	Version	Create Config	Options	
1	GRP2615	--	Grandstream	C074AD132F4C	192.168.6.153	1.0.13.59	--		
2	GRP2616	--	Grandstream	C074AD183280	192.168.6.113	1.0.13.59	2025-12-12 09:24:03		
3	GXV3350	--	Grandstream	C074AD1B200C	192.168.6.93	1.0.3.57	--		
4	GXV3350	--	Grandstream	C074AD1B51F0	192.168.6.56	1.0.3.57	--		
5	GDS3710	--	Grandstream	C074AD1CAFD0	192.168.1.168	1.0.13.15	--		

Zero Config Main Page

Firmware

In the Firmware tab, users can upload and manage endpoint firmware. Upgrades are performed per device, not per MAC address.

The uploaded files must use the .bin extension and must not exceed 1.5 GB in size

Zero Config

Zero ConfigGlobal PolicyGlobal TemplatesModel TemplatesModel UpdateFirmwareZero Config Settings

Firmware Storage Path

Local

CancelSave

Firmware List

UploadDelete

Q: Name / Firmware Version / Model

	Name	Status	Firmware Version	Model	Size	Date	Push status	Options
☐	grp2610fw.bin	Enable	1.0.13.59	GRP2616	108.12 MB	2025-11-19 11:21:41	--	  

Total 110 / pageGoto

Firmware Zero Config Page

After you click "Upload", a window appears displaying the configuration parameters below.

Upload New Firmware

✕

✱ Enable

☒

Choose File to Upload

Extension: .bin file, size cannot exceed 1.5G

Choose File to Upload

Model

Please enter Model

Firmware Version

Please enter Firmware Version

Remark

Cancel

Upload

Upload New Firmware Window

Option	Description
Enable	Toggles whether the UCM will provision this firmware to endpoints using the UCM as their firmware server. If disabled, the UCM rejects firmware requests for this file.
Choose File to Upload	Select the firmware file to upload from the user's PC. The file name must match the firmware file name requested by the endpoint.

Model	The device model for which this firmware is intended. For self-reference only; has no effect on provisioning.
Firmware	The firmware version of the file being uploaded. For self-reference only; has no effect on provisioning.
Remark	Add a comment about the uploaded firmware. For self-reference only; has no effect on provisioning.

Administrators can perform local firmware updates across one or multiple managed IP phones and gateways simultaneously via Zero Config.

To execute a local firmware upgrade:

1. Navigate to **Extension/Trunk -> Zero Config -> Zero Config**.
2. Select the target devices from the device list using the checkboxes.
3. Click the **Upgrade** button dropdown and select **Local**.
4. Choose the desired locally uploaded firmware file from the prompt to trigger the upgrade across all selected targets.

Zero Config Supports managing and deploying devices such as IP phones, gateways, access control devices, meeting devices, w

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

Manage 3rd-Party Enterprise Phones is not currently enabled, To configure, go to Zero Config Settings .

Total: 129 ● Registered: 0 ● Unregistered: 129

Auto Discover
Add
Delete
Edit
Upgrade
Push Config
Reboot

☐	No.	Model	Ext	GDMS	Vendor
☐	1	 GXW4232	--	Local	Grandstream
☐	2	 GXP2140	--		Grandstream
☐	3	 GXP2140	--		Grandstream
☒	4	 GXP2130	--		Grandstream
☒	5	 GXP2130	--		Grandstream
☐	6	 GXP2130	--		Grandstream

Batch Local Firmware Upgrade Selection

Uploading Devices List

Besides the built-in discovery method on the UCM, users could prepare a list of devices on a xlsx or csv file and upload it by clicking on the button **"Import"**, after which a success message prompt should be displayed.

Users need to make sure that the CSV file respects the format as shown on the following figure and that the entered information is correct (valid IP address, valid MAC address, device model, and an existing account), otherwise the UCM will reject the file and the operation will fail:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	===== Device Start =====													
2	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
3		Grandstream	1	192.168.5.172		https://192.168.5.147:80	#####	000B8249	1.0.7.10	0	GXW4248	no		5060
4														
5	===== Device Start =====													
6	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
7		Grandstream	1	192.168.5.114		https://192.168.5.147:80	#####	000B826B	1.0.3.227	0	GXV3240	no		5060
8														
9	===== Device Start =====													
10	config_name	vendor	state	ip	account_secre	file_url	url_paramete	last_access	mac	version	ad_state	model	hot_desking	port
11		Grandstream	1	192.168.5.201		https://192.168.5.147:80	#####	000B826F	1.0.1.106	0	--	no		5080

Device List CSV file Sample

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

Managing Discovered Devices

Users can manage the discovered devices in the Zero Config tab as follows:

- **Sorting:** Press or to sort per MAC Address, IP Address, Version, Vendor, Model or Create Config columns from lower to higher or higher to lower, respectively.
- **Filter:** Select a filter to display corresponding results. Users can filter by registration status, models, or vendors. The "All" filter displays all discovered devices.
- **Search:** Search in the list of discovered devices by model, extension number, MAC address, or IP address.
- **Add:** Use the "Add" button to add a new device to the Zero Config database using its MAC address.
- **Delete:** Use the "Delete" button delete selected devices from the Zero Config database.
- **Edit:** Modify selected devices by clicking the "Edit" button.
- **Upgrade:** Upgrade the software of the discovered devices to the latest version. Select the devices which you want to upgrade. If no devices are selected, all the discovered devices will be upgraded.
- **Update Config:** Batch update a list of devices, the UCM on this case will send SIP NOTIFY message to all selected devices to update them at once.
- **Reboot:** Use the "Reboot" option for selected devices (the selected devices should have provisioned extensions since the phone will authenticate the server sending the reboot command).
- **More:** Perform additional action like:
 - **Import:** Import a list of devices. Devices with duplicate MAC addresses can either be skipped, replaced or updated. The imported file should be in CSV or XLSX format.
 - **Export:** Export the list of the discovered devices in CSV or XLS format. Select the devices before exporting. If no devices are selected, all the discovered devices will be exported.
 - **Reset:** Reset the discovered devices. Select the devices to reset before clicking this button. If no devices are selected, all the discovered devices will be reset to their initial configuration.
 - **Copy:** Copy the configuration across devices.

Zero Config

Zero Config

Global Policy

Global Templates

Model Templates

Model Update

Firmware

Zero Config Settings

Total: 74

Registered: 0

Unregistered: 74

All

All Model

All Vendor

Q Model / Extension Number / MAC Address / IP Address

Auto Discover

Add

Delete

Edit

Upgrade

Update Config

Reboot

More

No.	Model	Extension	Vendor	Import	MAC Address	IP Address	Version	Create Config	Options
1	 GXV3470	--	Grandstream	Export	C074AD930CF8	192.168.6.175	1.0.5.14	--	    
2	 GXW4216V2 V1....	--	Grandstream	Reset	C074ADA3F1DC	192.168.6.33	1.0.33.3	--	    
3	 GXW4224V2 V1....	--	Grandstream	Copy	C074ADA8BCED	192.168.6.77	1.0.31.2	--	    

Managing Discovered Devices

Global Configuration

The global configuration will apply to all the connected SIP endpoint devices in the same LAN with the UCM630xA regardless of the device model. It is divided into two levels:

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

Global Templates configuration has higher priority to Global Policy configuration.

Global Policy

Global Policy can be accessed in **Device Management->Zero Config->Global Policy** page. On the top of the configuration table, users can select a category in the "Options" dropdown list to quickly navigate to the category or they can also complete the configuration by importing/exporting. The categories are:

- **Localization**: configure display language, data, and time.
- **Phone Settings**: configure the dial plan, call features, NAT, call progress tones, etc.
- **Contact List**: configure LDAP and XML phonebook download.
- **Maintenance**: configure upgrading, web access, Telnet/SSH access, and Syslog.
- **Network Settings**: configure the IP address, QoS, and STUN settings.
- **Customization**: customize LCD screen wallpaper for the supported models.
- **Communication Settings**: configure Email and FTP settings

Select the checkbox on the left of the parameter you would like to configure to activate the dropdown list for this parameter.

Zero Config

Zero Config **Global Policy** Global Templates Model Templates Model Update Firmware Zero Config Settings

The Global Policy configuration will be applied to all devices. Specific model configurations, if any, will be applied on top of the Global Policy

Import

Export ▾

▾ 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 Lumpur, Irkutsk) ▾



Enable Daylight Saving Time



Disabled ▾

> Phone Settings

> Contact List

> Maintenance

> Network Settings

> Customization

Global Policy Page

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

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

Global Policy Parameters - Localization

Default Call Settings	
Dial Plan	Configure the default dial plan rule. For syntax and examples, please refer to the user manual of the SIP devices to be provisioned for more details.
Enable Call Features	When enabled, "Do Not Disturb", "Call Forward" and other call features can be used via the local feature code on the phone. Otherwise, the ITSP feature code will be used.
Use # as Dial Key	If set to "Yes", pressing the number key "#" will immediately dial out the input digits.
Auto Answer by Call-info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info header sent from the server/proxy. The default setting is enabled.
NAT Traversal	Configure if NAT traversal mechanism is activated.
User Random Port	If set to "Yes", this parameter will force random generation of both the local SIP and RTP ports.
General Settings	
Call Progress Tones	Configure call progress tones including ring tone, dial tone, second dial tone, message waiting tone, ring back tone, call waiting tone, busy tone, and reorder tone using the following syntax: f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; Frequencies are in Hz and cadence on and off are in 10ms). "on" is the period (in ms) of ringing while "off" is the period of silence. Up to three cadences are supported. Please refer to the user manual of the SIP devices to be provisioned for more details
HEADSET Key Mode	Select "Default Mode" or "Toggle Headset/Speaker" for the Headset key. Please refer to the user manual of the SIP devices to be provisioned for more details.

Global Policy Parameters - Phone Settings

LDAP Phonebook	
Source	Select "Manual" or "PBX" as the LDAP configuration source. If "Manual" is selected, the LDAP configuration below will be applied to the SIP end device. If "PBX" is selected, the LDAP configuration built-in from UCM630X Web GUI→System Settings→LDAP Server will be applied.
Address	Configure the IP address or DNS name of the LDAP server.
Port	Configure the LDAP server port. The default value is 389.
Base DN	This is the location in the directory where the search is requested to begin. Example: dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com
Username	Configure the bind "Username" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Password	Configure the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Number Filter	Configure the filter used for number lookups. Please refer to the user manual for more details.
Name Filter	Configure the filter used for name lookups. Please refer to the user manual for more details.
Version	Select the protocol version for the phone to send the bind requests. The default value is 3.
Name Attribute	Specify the "name" attributes of each record that are returned in the LDAP search result. Example: gn cn sn description

Number Attribute	Specify the "number" attributes of each record that are returned in the LDAP search result. Example: telephoneNumber telephoneNumber Mobile
Display Name	Configure the entry information to be shown on the phone's LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber
Max Hits	Specify the maximum number of results to be returned by the LDAP server. The valid range is 1 to 3000. The default value is 50.
Search Timeout	Specify the interval (in seconds) for the server to process the request and the client waits for the server to return. The valid range is 0 to 180. The default value is 30.
Sort Results	Specify whether the searching result is sorted or not. The default setting is No.
Incoming Calls	Configure to enable LDAP number searching when receiving calls. The default setting is No.
Outgoing Calls	Configure to enable LDAP number searching when making calls. The default setting is No.
Lookup Display Name	Configures the display name when LDAP looks up the name for an incoming call or outgoing call. It must be a subset of the LDAP Name Attributes.
XML Phonebook	
Phonebook XML Server	Select the source of the phonebook XML server. Disable Disable phonebook XML downloading. Manual Once selected, users need to specify downloading protocol HTTP, HTTPS, or TFTP and the server path to download the phonebook XML file. The server path could be an IP address or URL, with up to 256 characters. Local UCM Server Once selected, click on the Server Path field to upload the phonebook XML file. Please note after uploading the phonebook XML file to the server, the original file name will be used as the directory name and the file will be renamed as phonebook.xml under that directory.
Phonebook Download Interval	Configure the phonebook download interval (in minutes). If set to 0, the automatic download will be disabled. The valid range is 5 to 720.
Remove manually edited entries on download	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed.

Global Policy Parameters - Contact List

Upgrade and Provision	
Firmware Source	Firmware source via ZeroConfig provisioning could be a URL for external server address, local UCM directory, or USB media if plugged into the UCM630X. Select a source to get the firmware file: URL If selected to use URL to upgrade, complete the configuration for the following four parameters: "Upgrade Via", "Server Path", "File Prefix" and "File Postfix". Local UCM Server Firmware can be uploaded to the UCM630X internal storage for firmware upgrade. If selected, click on the "Manage Storage" icon next to the "Directory" option, upload the firmware file, and select a directory for the end device to retrieve the firmware file. Local USB Media If selected, the USB storage device needs to be plugged into the UCM630X and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory. Local SD Card Media If selected, an SD card needs to be plugged into the UCM630X and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory.
Upgrade via	When URL is selected as firmware source, configure upgrade via TFTP, HTTP, or HTTPS.
Server Path	When URL is selected as firmware source, configure the firmware upgrading server path.
File Prefix	Configure the Config Server Path.
Config Server Path	When URL is selected as firmware source, configure the firmware file postfix. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.

Allow DHCP Option 43/66	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
Automatic Upgrade	If enabled, the end point device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week, or by minute. By week Once selected, specify the day of the week to check the HTTP/TFTP server for firmware upgrades or configuration files changes. By day Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes. By minute Once selected, specify the interval X that the SIP end device will request for new firmware every X minutes.
Firmware Upgrade Rule	Specify how firmware upgrading and provisioning requests are to be sent.
Zero Config	Select either to enable or disable Zero Config.
Web Access	
Admin Password	Configure the administrator password for admin-level login.
End-User Password	Configure the end-user password for the end-user level login.
Web Access Mode	Select HTTP or HTTPS as the web access protocol.
Web Server Port	Configure the port for web access. The valid range is 1 to 65535.
RTSP Port	Configure the RTSP Port.
Enable UPnP Discovery	Select either to enable or disable Enable UPnP Discovery
Login Settings	Configure the login settings.
User Login Timeout	Configure User Login Timeout.
Maximum Consecutive Failed Login Attempts	Configure Maximum Consecutive Failed Login Attempts.
Login Error Lock Time	Configure Login Error Lock Time.
Security	
Disable Telnet/SSH	Enable Telnet/SSH access for the SIP end device. If the SIP end device supports Telnet access, this option controls the Telnet access of the device; if the SIP end device supports SSH access, this option controls the SSH access of the device.
Syslog	
Syslog Server	Configure the URL/IP address for the Syslog server.
Syslog Level	Select the level of logging for Syslog.
Send SIP Log	Configure whether the SIP log will be included in the Syslog message.

Global Policy Parameters - Maintenance

Basic Settings	
IP Address	Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected. DHCP Once selected, users can specify the Host Name (option 12) of the SIP end device as DHCP client, and Vendor Class ID (option 60) used by the client and server to exchange vendor class ID information. PPPoE Once selected, users need to specify the Account ID, Password, and Service Name for PPPoE.
Host Name	Specify the name of the client. This field is optional but may be required by Internet Service Providers.
Vendor Class ID	Used by clients and servers to exchange vendor class ID.
Account ID	Enter the PPPoE account ID.
Password	Enter the PPPoE Password.

Service Name	Enter the PPPoE Service Name.
Advanced Setting	
Layer 3 QoS	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv, or MPLS. The valid range is 0-63.
Layer 3 QoS For RTP	Assign the priority value of the Layer 3 QoS for RTP packets. The valid range is 0 -63.
Layer 3 QoS For SIP	Assign the priority value of the Layer 3 QoS for SIP packets. The valid range is 0 -63.
Layer 2 QoS Tag	Assign the VLAN Tag of the Layer 2 QoS packets. The valid range is 0 -4095.
Layer 2 QoS Priority Value	Assign the priority value of the Layer 2 QoS packets. The valid range is 0-7.
STUN Server	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Keep-Alive	Select either to enable or disable Keep Alive.
Keep Alive Interval	Specify how often the phone will send a blank UDP packet to the SIP server to keep the "ping hole" on the NAT router open. The valid range is 10-160.
Register Expiration	Specify the Register Expiration.
Local SIP Port	Configure Local SIP Port.
Local RTP Port	Configure Local RTP Port.
Auto On-Hook Timer(s)	Configure Auto On-Hook Timer(s).
Ring Timeout	Configure Ring Timeout.
SIP Transport	Select either UDP, TCP, or TLS/TCP as SIP transport protocol.
Direct IP Call	Select either to disable or enable Direct IP Call support.
SIP Proxy Compatibility Mode	Select either to disable or enable SIP Proxy Compatibility Mode.
Unregister On Reboot	Select either to disable or enable Unregister On Reboot.
Whitelist	
Whitelist	Select either to enable or disable Whitelist
SIP Phone Number Whitelist	Configure the SIP Phone Number Whitelist.

Global Policy Parameters - Network Settings

Email Settings	
SMTP Settings	Check this option to configure the email settings that will be sent to the provisioned phones: Server The IP address of the SMTP server Port SMTP server port From E-Mail address Email address Sender Username Username of the sender Password Recovery Email Email where the recovered password will be sent Alarm receive Email 1 Email address where alarms notifications will be sent Alarm receive Email 1 Email address where alarms notifications will be sent Enable SSL Enable SSL protocol for SMTP
FTP	
FTP	Check this option to configure the FTP settings that will be sent to the provisioned phones: Storage Server Type Either FTP or Central Storage Server FTP server address Port FTP port to be used Username FTP username Path FTP Directory path

Global Policy Parameters - Customization

Wallpaper

Screen Resolution 1024 x 600	Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 800 x 400	Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 480 x 272	Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.
Screen Resolution 320 x 240	Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper. Source Configure the location where wallpapers are stored. File If "URL" is selected as the source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as the source, click to upload wallpaper file to the UCM630X.

Global Policy Parameters - Communication Settings

Global Templates

Global Templates can be accessed in **Device Management->Zero Config->Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates, or click on the "Import/Export" button to add multiple global templates.

When the user configures the device in the **Edit Device dialog->Advanced Settings**, they can select to use one of the global templates for the device. Please refer to section [\[Manage Devices\]](#) for more details on using the global templates.

When creating a Global Template, users can select the categories and specific parameters within each category to include in the template. Both the Global Policy and the selected Global Template are applied when generating the configuration file. However, for overlapping configuration options, the Global Template takes precedence over the Global Policy.

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

Zero Config > Create New Template

* Template Name	
Description	
Active	☒
Cancel Save	

Create New Global Template

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

- Zero Config > **Edit Global Templates: Test**

Global Template Configuration Settings

- The created global templates will show in the **Device Management->Zero Config->Global Templates** page. Users can delete one or multiple templates or click on "Toggle Selected Template Status" to toggle between enabled/disable status for the selected templates.

Model templates

The Model layer configuration allows users to apply model-specific settings to devices. Users can create, edit, or delete Model Templates through the Web GUI at **Device Management->Zero Config->Model Templates**.

If multiple Model Templates are created and enabled, users can select a specific template for a device in the **Edit Device** dialog under **Advanced Settings**. The selected Model Template is then applied to that device.

For each Model Template, users can designate it as the default template. When a Model Template is set as the default, its configuration values are applied to all devices of the corresponding model.

Only one default Model Template can be assigned at any given time on the UCM630xA.

Both the default Model Template and the selected Model Template are applied during configuration generation. For overlapping options, the selected Model Template takes precedence and overrides the default Model Template.

To configure a model template:

1. Click on "Add" to add a model template, and configure the following parameters:

Zero Config > Create New Template



Model

Template Name

Description

Default Model Template

Active

☐

☒

If the model is not found, please go to [\[Model Update > Model Template Package List\]](#) to install it first.

Cancel

Save

Create New Model Template

Model	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
Template Name	Create a name for the model template.
Description	Enter a description for the model template. This is optional.
Default Model Template	Select to assign this model template as the default model template. The value of the option in the default model template will be overridden if another selected model template has a different value for the same option.
Active	Check this option to enable the model template.

Create New Model Template

2. Click on the "Edit" icon to edit the model template. The editing window for a model template is shown in the following figure.



Model GRANDSTREAM GRP2614

Template Name GRP2614_Prod

Description

Default Model Template ☐

Active ☒

Options Maintenance

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.

[+ Add New Field](#)

Edit Model Template

- On the left side of each added option, click the "Trash" icon to delete this option from the template, or click on the "Reset" icon to reset the option value to the default value.
- In the "Options" field, enter the option name key word, the option that contains the keyword will be listed. The user could then select the option to be modified under the model template.

Options Maintenance

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.

[+ Add New Field](#)

Maintenance

- Upgrade and Provision
- Security
- Syslog
- Web Access
- Contact List
- Localization

Model Template Options

- Use "Add New Field" to add a P-value number and the value to the configuration. The following figure shows setting P-value "P1362" to "en", which means the display language on the LCD is set to English.

For P-value information of different models, please refer to the configuration template here <http://www.grandstream.com/support/tools>

Custom 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.

+ Add New Field

Custom Model Template Parameters

- Click on Save when done. The model template will be displayed on **Device Management->Zero Config->Model Templates** page.
- Click on the "Trash" icon to delete the model template or use the "Delete" button delete multiple selected templates at once.
- Click on "Toggle Selected Template Status" to toggle between enabled/disable status for the selected templates.
- Use the "Import/Export" buttons to upload/export the model template list in CSV or XLS format.

The filter option allows to search through the model templates. Please see the screenshot below:

Zero Config

Zero Config Global Policy Global Templates **Model Templates** Model Update Firmware Zero Config Settings

Add Delete Import Export v Toggle Selected Template Status Copy Template

☐	Model	Template Name	Description	Active
☐	GRP2614	Search All	--	Yes
☐	GRP2616	FwUpdate	--	Yes

Model Template Search Filter

Model Update

UCM630xA Zero Config feature supports provisioning all models of Grandstream SIP end devices including OEM device models, and supported third-party models.

OEM Models

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

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

X

OEM Models

i Use to reuse the exist model as an other name.

*** Source Model** *i*

*** Destination Model** *i*

*** Destination Vendor** *i*

Cancel

Save

Add OEM Models

Model Template Package List

Templates for most of the Grandstream models are built-in with the UCM630xA already. Templates for Wave, Grandstream surveillance products, and third-party devices require users to download and install under **Device Management->Zero Config->Model Update** first before they are available in the 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.

1. Click on the "Download" icon to download the template.
2. Click on "Upgrade" to upgrade an existing model template.

Model Template Package List

					All Vendor ▾	All Model ▾	Q Vendor / Model
Vendor	Model	Version (Remote/Local)			Size	Options	
Grandstream	GXV3370	1.9/-			58K	 	
Grandstream	GXV3380	1.7/-			62K	 	
Grandstream	GXV3450	1.5/1.5			85K	 	
Grandstream	GXV3470	1.6/-			76K	 	
Grandstream	GXV3480	1.5/-			69K	 	

Model Template Package List

Upload Model Template Package

By default, third-party model templates are not available on the UCM630xA and must be uploaded manually through the Web GUI.

In environments with restricted Internet connectivity, Grandstream model packages must also be uploaded manually.

Contact Grandstream customer support to obtain the required model template packages.

Upload Model Template Package

Choose Model Package to Upload ⓘ

Choose File to Upload



Upload Model Template Package

Device Configuration

On Web GUI, page **Device Management->Zero Config->Zero Config**, users could create a new device, delete existing device(s), make special configuration for a single device, or send NOTIFY to an existing device(s).

Create New Device

Users can directly create a new device and configure basic settings before the device is discovered by the 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.

Edit Device: C074AD112233

Cancel

Update

Save



* Model:	GRANDSTREAM GXV3350
* MAC Address:	c074ad112233
IP Address:	
Version:	

Basic Settings

Advanced Settings

| Accounts

☐	Account 1:	+123456789
☐	Account 2:	+123456789
☐	Account 3:	+123456789
☐	Account 4:	+123456789
☐	Account 5:	+123456789

Create New Device

Manage Device

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

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

Manage Devices

- Click on "Access Device Web UI" to access the Web GUI of the device.
- Click on the "Edit" icon to edit the device configuration.

A new dialog will be displayed for the users to configure "Basic" settings and "Advanced" settings. "Basic" settings have the same configurations as displayed when manually creating a new device, i.e., account, line key, and MPK settings; "Advanced" settings allow users to configure more details in a five-level structure.

Edit Device: 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

None

☐ 0 Selected

None

3 Default Model Template

Edit Device

A preview of the **Advanced Settings** is shown in the figure above. There are five configuration levels, as described in items (1) through (5) below, ordered from lowest to highest priority. All configuration levels are applied to the device.

If the same option is defined at multiple levels with different values, the value from the higher-priority level overrides the value from the lower-priority level.

1. Global Policy

This is the lowest level configuration. The global policy configured in **Device Management->Zero Config->Global Policy** will be applied here. Clicking on "Modify Global Policy" to redirect to page **Device Management->Zero Config->Global Policy**.

2. Global Templates

Select a Global Template and click the right arrow to add it to the device. Multiple Global Templates can be selected, and their priority can be adjusted using the up and down arrows. All selected templates take effect. If the same option is defined in multiple selected Global Templates, the value from the higher-priority template overrides that of the lower-priority template. Click the left arrow to remove a Global Template from the selected list.

3. Default Model Template

Default Model Template will be applied to the devices of this model. Default model template can be configured in the model template under **Device Management->Zero Config->Model Templates** page.

4. Model Templates

Select a Model Template to apply to the device and click the right arrow to add it. Multiple Model Templates can be selected, and their priority can be adjusted using the up and down arrows. All selected templates take effect.

If the same option is defined in multiple selected Model Templates, the value from the higher-priority template overrides that of the lower-priority template. Click the left arrow to remove a Model Template from the selected list.

5. Customize Device Settings

This is the highest-level configuration for the device. Click on "Modify Customize Device Settings" and the following dialog will show.

Edit Device: 000B82A95F94



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

Custom Fields

Custom Fields

Please use P-values for the Name fields.
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 device-specific options. To add options that are not included in the predefined list, click **Add New Field** and specify the P-value and its corresponding value.

In the example shown above, P-value **P1362** is set to **en**, which configures the LCD display language to English. The warning message on the right indicates that a predefined option matching this P-value already exists; clicking it navigates to the corresponding option.

For P-value information of different models, please refer to the configuration template here <http://www.grandstream.com/support/tools>

Select multiple devices that need to be modified and then click on "Update Config" to batch modify devices. If selected devices are of the same model, the configuration dialog is like the following figure. Configurations in five levels are all available for users to modify.

Modify Selected Devices Cancel Save



Model: GXV3275

MAC Address: 000B82000001 000B8227FB15

Basic Settings

Advanced Settings

Programmable MPK Settings

☐

MPK 1:

Speed Dial

Description

Value

☐

MPK 2:

Speed Dial

Description

Value

☐

MPK 3:

Speed Dial

Description

Value

☐

MPK 4:

Speed Dial

Description

Value

☐

MPK 5:

Speed Dial

Description

Value

☐

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 the arrows to view more devices of other models. Users are only allowed to make modifications to the Global Templates and Global Policy level.

Modify Selected Devices Cancel Save



Model: GXV3275

MAC Address: 000B8227FB15

Basic Settings

Advanced Settings

5 Custom Device Settings

Available only for single model

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 **Device Management->Zero Config->Zero Config** page. Users could then click on the "Update" icon to send NOTIFY to the SIP end point device and

trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.

On this web page, users can also click on "Reset All Extensions" to reset the extensions of all the devices.

Sample Application

Assuming in a small business office where there are 8 GXP2140 phones used by customer support and 1 GXV3275 phone used by customer support supervisor. 3 of the 8 customer support members speak Spanish and the rest speak English. We could deploy the following configurations to provision the office phones for the customer support team.

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

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:

Upgrade via:

Server Path:

File Prefix:

File Postfix:

URL

TFTP

fm.grandstream.com/gs

Zero Config Sample Global Policy

- 3. Go to **Device Management->Zero Config->Model Templates**, create a new model template "English Support Template" for GXP2170. Add option "Language" and set it to "English". Then select the option "Default Model Template" to make it the default model template.

4. Go to **Device Management->Zero Config ->Model Templates**, create another model template "Spanish Support Template" for GXP2170. Add option "Language" and set it to "Español".
5. After 9 devices are powered up and connected to the LAN network, use the "Auto Discover" function or "Create New Device" function to add the devices to the device list on **Device Management->Zero Config ->Zero Config**.
6. On Web GUI->**Device Management->Zero Config->Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on the "Edit" icon to edit the device settings.
7. For each of the 5 phones used by English-speaking customer support, in "Basic settings" select an available extension for account 1 and click on "Save". Then click on the "Advanced settings" tab to bring up the following dialog. Users will see the English support template is applied since this is the default model template. A preview of the device settings will be listed on the right side.

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:

Language:

NTP Server:

Self-Defined Time Zone:

Time Zone:

Date Format

Language

NTP Server

Self-Defined Time Zone

Time Zone

yyyy-mm-dd

English

MTZ+6MDT+5.M3.2.0.M11.1.0

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

12-hour Clock

Zero Config Sample Device Preview 1

8. For the 3 phones used by Spanish support, in "Basic settings" select an available extension for account 1 and click on "Save". Then click on the "Advanced settings" tab to bring up the following dialog.

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:

Language:

NTP Server:

Self-Defined Time Zone:

Time Zone:

Date Format

Language

NTP Server

Self-Defined Time Zone

Time Zone

yyyy-mm-dd

Español

MTZ+6MDT+5.M3.2.0.M11.1.0

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

12-hour Clock

Zero Config Sample Device Preview 2

9. Select "Spanish Support Template" in "Model Template". The preview of the device settings is displayed on the right side and we can see the language is set to "Español" since Model Template has the higher priority for the option "Language", which overrides the value configured in the default model template.
10. For the GXV3275 used by the customer support supervisor, select an available extension for account 1 on "Basic settings" and click on "Save". Users can see the preview of the device configuration in "Advanced settings". There is no model template configured for GXV3275.

5 Custom Device Settings

Modify Custom Settings

4 Model Templates

0 Item	Idle	0 Item	Selected
None		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

- Click on "Apply Changes" to apply saved changes.
- On the **Device Management->Zero Config->Zero Config** page, click on the "Update" icon to send NOTIFY to trigger the device to download the config file from 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 the LCD display since it is not specified in the global policy.

EXTENSIONS

Create New Extension

Create New SIP Extension

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

Extensions > Create New Extension

Basic Settings Media Call Policy Features Voicemail Custom Time AI Wave Client Follow Me Advanced Settings

Select Extension Type SIP Extension

Select Add Method Single

General

Extension 1006

Call Privileges Internal

AuthID

Disable This Extension

CallerID Number

SIP/IAX Password

Concurrent Registrations 3

User Settings

First Name

Last Name

Email Address

User/Wave Password

User Portal/Wave Privileges Default

Mobile Number +1

Add / Edit Privileges

Create a New SIP Extension

Extension options are divided into the following categories:

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

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

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user.Note:The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Call Privileges	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.Note: The password should contain at least 10 characters, with at least one lower-case letter, one upper-case letter, one numeral, and one special character.The password must not contain an ascending or descending consecutive numeric sequence, or a consecutive sequence of the same number/letter.
Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
Voicemail	Configure Voicemail. There are three valid options, and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user. Enable Remote Voicemail: Forward the notify message from the remote voicemail system for the user, and the local voicemail will be disabled. Note: Remote voicemail feature is used only for Infomatec (Brazil).
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Skip Voicemail Password Verification	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Send Voicemail Email Notification	Configures whether to send emails to the extension's email address to notify of a new voicemail.
Attach Voicemail to Email	Configures whether to attach a voicemail audio file to the voicemail notification emails.Note: When set to "Default", the global settings in Basic Call Features > Voicemail > Voicemail Email Settings will be used.
Keep Voicemail after Emailing	Whether to keep the local voicemail recording after sending them. If set to "Default", the global settings will be used.Note: When set to "Default", the global settings in Basic Call Features > Voicemail > Voicemail Email Settings will be used.

Enable Keep-alive	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".
Keep-alive Frequency	Configure the Keep-alive interval (in seconds) to check if the host is up. The default setting is 60 seconds.
Enable SCA	If enabled, (1) Call Forward, Call Waiting, and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Advanced Call Features > SCA page.
Emergency CID Name	CallerID name that will be used for emergency calls and callbacks.
Disable This Extension	If selected, this extension will be disabled on the PBX.Note: The disabled extension still exists on the PBX but cannot be used on the end device.
Sync Contact	If enabled, this extension number will be displayed in the Wave contact, otherwise, it will not be displayed, and it cannot be found in the chat, but the user can still dial this number.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User/Wave Password?	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.The password must respect the following criteria: At least one lower case letter At least one upper case letter At least one numeral At least one special character At least 10 total characters
User Portal/Wave Privileges	Change User Portal/Wave Privileges. Default: Setting this privilege will grant the standard Wave privileges. Wave Administrator: Setting this privilege will grant the user access to Management Portal on Wave.
Multi-Factor Authentication	When this option is enabled, the extension user will be prompted to configure multi-factor authentication on their account when they log in from the User Portal or Wave. The user can choose to use an OTP device or application, or they can use their email as a second factor of authentication.To ensure enabling Wave multi-factor authentication is successful, please refer to the minimum versions required below for Wave on each platform. Wave Web: 1.0.27.12 and later Wave Desktop: 1.27.10 and later Wave App for Android(TM): 1.0.27.18 and later Wave App for iOS(TM): 1.27.24 and later
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under PBX Settings > Voice Prompt > Language Settings. 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 PBX Settings > Voice Prompt > Language Settings.
Concurrent Registrations	The maximum endpoints which can be registered to this extension. For security concerns, the default value is 3.Note: The user can configure up to 10 registrations per extensions.
Mobile Phone Number	Configure the phone number for the extension, user can type the related star code for the phone number followed by the extension number to directly call this number.For example, the user can type *881000 to call the mobile number associated with extension 1000.
Department	Configure the user's department. The department can be configured in User Management > Address Book Management > Department Management. Job Title: The user's department position.
Contact Privileges	
Same as Department Contact Privileges	When enabled, The extension will inherit the same privilege attributed to the department it belongs to.

Contact View Privileges	Select the privileges regarding the contact view in SIP endpoints and Wave.
-------------------------	---

SIP Extension Configuration Parameters > Basic Settings

General	
NAT	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is a one-way audio issue, usually it is related to NAT configuration or the Firewall's support of SIP and RTP ports. The default setting is enabled.
Enable Direct Media	By default, the PBX will route the media streams from SIP endpoints through itself. If this option is enabled, the PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. Note: It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing.
DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is "RFC4733". If "Info" is selected, the SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, RFC4733 will be used if offered, otherwise "Inband" will be used. Note: The default DTMF mode selected is RFC4733.
TEL URI	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.
Alert-Info	When present in an INVITE request, the alert-Info header field specifies an alternative ring tone to the UAS.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
TURN Relay	Enable this option if the following are true: PBX is deployed on a private network. There are remote endpoints outside the PBX's network registering to it via its public IP address. The network's firewall is not configured for media port forwarding. Media NAT penetration is required. Once a TURN server is configured, media will be forwarded to it. This configuration does not affect endpoints that are registered via the PBX's RemoteConnect address.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.
QoS	
Jitter Buffer	Select the jitter buffer method. Disable: Jitter buffer will not be used. Fixed: Jitter buffer with a fixed size (equal to the value of "jitter buffer size"). Adaptive: Jitter buffer with an adaptive size (no more than the value of "max jitter buffer"). NetEQ: Dynamic jitter buffer via NetEQ.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission. NACK+NACK+RTX(SSRC-GROUP)OFF
Video FEC	Check to enable Forward Error Correction (FEC) for Video.
Audio FEC	Check to enable Forward Error Correction (FEC) for Audio.
Silence Suppression	If enabled, the PBX will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the PBX will send DTX packets instead.
FECC	Configure to enable Remote Camera Management.
RTP Encryption	
SRTP	Enable SRTP for the call. The default setting is disabled. Disabled Enabled and Enforced: SRTP will be necessary to transmit media traffic. If the IP phone of this extension has SRTP disabled, calls cannot be established. Optional: The PBX will negotiate whether to use SRTP or not. If the SIP endpoint has SRTP enabled, SRTP will be used. If it is disabled, SRTP will not be used.

SRTP Crypto Suite	SRTP encryption suite used by the PBX for outbound calls. Priority is based on order of configuration. The following encryption algorithms can be used to encrypt an RTP stream. AES_CM_128_HMAC_SHA1_80 (This is the default algorithm used) AES_256_CM_HMAC_SHA1_80 AEAD_AES_128_GCM AEAD_AES_256_GCM
ZRTP Encryption Mode	ZRTP, also known as Media Path Key Agreement for Secure RTP, is an encryption protocol which allows negotiating the encryption key for RTP traffic. ZRTP uses Diffie-Hellman exchange to establish an encrypted and secure connection between the PBX and the SIP endpoint. If the SIP endpoint has both SRTP and ZRTP enabled, ZRTP will always be prioritized.

SIP Extension Configuration Parameters > Media

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

Call Forward Busy	Configure the Call Forward Busy target number. Available options for target number are:"None": Call forward deactivated."Extension": Select an extension from the dropdown list as CFB target."Custom Number": Enter a customer number as a target. For example: *97"Voicemail": Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension."Ring Group": Select a ring group from the dropdown list as CFB target."Queues": Select a queue from the dropdown list as CFB target."Voicemail Group": Select a voicemail group from dropdown list as CFB target.Custom Prompt: The default setting is "None".
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions 'All', 'Office Time', 'Out of Office Time', 'Holiday', 'Out of Holiday', 'Out of Office Time or Holiday', 'Office Time and Out of Holiday', 'Specific Time', 'Out of Specific Time', 'Out of Specific Time or Holiday', 'Specific Time and Out of Holiday'.Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
Forwarding Exemption List	Calls from users in the forward exemption list will not be forwarded. Multiple numbers are supported and must be separated by new lines.Pattern matching is supported.Z match any digit from 1-9,N match any digit from 2-9,X match any digit from 0-9.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
DND Time Condition	Select time condition for Do Not Disturb. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes:"Specific" has higher priority to "Office Times" if there is a conflict in terms of time period.Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
DND Allowlist	If DND is enabled, calls from the allowlisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.Z match any digit from 1-9.N match any digit from 2-9.X match any digit from 0-9.
Call Number Handling Policy	Call Number Handling Policy determines the destination of the calls received. The user can configure the destination based on the a matching pattern of the callee number.Call Number Matching Mode: Support input extension numbers and pattern matching rules: [12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 are allowed. N ... Any digit from 2-9. Wildcard, matching one or more characters. ! ... Wildcard, matching zero or more characters immediately. X ... Any digit from 0-9. Z ... Any digit from 1-9. - ... Hyphens are used mainly to improve readability and are not involved in pattern matching. [] Contain special characters ([x], [n], [z]) represent letters x, n, z.Call Destination: Select the destination of the call. These are the destinations which can be set; Disconnect, Extensions, Voicemail, IVR, Hang up After Playing Background Sound, Call Accepted.

SIP Extension Configuration Parameters > Call Policy

CC Settings	
Enable CC	If enabled, the PBX will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.
CC Mode	Two modes for Call Completion are supported: Normal: This extension is used as an ordinary extension.For Trunk: This extension is registered from a PBX.The default setting is "Normal".
Call Settings	
Call Duration Limit	Block calls for the configured duration.
Maximum Call Duration (s)	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).

The Maximum Number of Call Lines	The maximum number of simultaneous calls that the extension can have. 0 indicates no limit.
Outgoing Call Frequency Limit	If enabled, if the number of outbound calls exceed the configured threshold within the specified period, further outbound will be not be allowed.
Period (m)	The time window for the configured outbound call frequency limit. Supported value range is 1 to 120 minutes. Default value is 1.
Max Number of Calls	The maximum allowed number of outbound calls within the specified period. Supported value range is 1 to 20. Default value is 5.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. '-' is the connection character that will be ignored. This field accepts only letters, numbers, and special characters + = * #.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension based on this time condition.
Use callee DOD on FWD or RS	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
Monitor Privilege Control	
Allowed to be Monitored	When disabled, this user's calls cannot be listened to by anyone. When enabled, this user's calls are allowed to be listened to through this extension or the opposite extension.
Call Monitoring Allowlist	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Allow Operator Panel Monitoring	Configure whether this extension can be monitored by the Operator Panel administrator.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the PBX can perform a seamless transfer. When using the Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform a seamless transfer to the edited extension.
PMS Remote Wakeup Whitelist	
Select the extensions that can set wakeup service for other extensions	Selected extensions can set a PMS wakeup service for this extension via feature code.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the PBX. The valid range is between 5 seconds and 600 seconds.Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under CDR > Recording Files.
Skip Trunk Auth	If set to "yes", users can skip entering the password when making outbound calls.If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition.If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering the password when making outbound calls.

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

SIP Extension Configuration Parameters > Features

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

SIP Extension Configuration Parameters > Custom Time

AI Call Transcription and Summary	
Automatic Transcribing And Summarizing	Enables or disables automatic transcription and summarization for all calls associated with this extension. When enabled, calls for this extension are automatically transcribed and summarized without user action.

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

SIP Extension Configuration Parameters > AI

General	
Enable Wave	Enable Wave for the specific extension.
Allow Concurrent Logins from the Same Client Type	Enables/disables the ability to login to Wave from different sessions on the same type of client Notes: Concurrent Registrations limit for the SIP extension will still apply. When this option is enabled, Concurrent Registrations cannot be configured as "1 (Allowed to Seize)" This option is disabled by default.
Multi-Factor Authentication	When this option is enabled, the extension user will be prompted to configure multi-factor authentication on their account when they log in using Wave. To ensure enabling multi-factor authentication successfully, please refer to the minimum version required below for Wave on each platform Wave Web: 1.0.27.12 and later Wave Desktop: 1.27.10 and later Wave App for Android(TM): 1.0.27.18 and later Wave App for iOS(TM): 1.27.24 and later
Wave Welcome Email	Wave Welcome Email template.
Wave Permission Settings	Clicking the path will direct you to Wave Permission configuration.
Wave	
Download Link?	https://fw.gdms.cloud/wave/download/

SIP Extension Configuration Parameters > Wave Client

Follow Me	
Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If the outbound calls need to check the password, we should enable this option or enable the option "Skip Trunk Auth" of the Extension. Otherwise this Follow Me cannot call out.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	If enabled, call will need to be confirmed after answering.
Enable Destination	Configure to enable destination
Default Destination	The call will be routed to this destination if no one in the Follow Me answers the call.

Use Callee DOD for Follow Me	Use the callee DOD number as CID if configured Follow Me numbers are external numbers.
Play Follow Me Prompt	If enabled, the Follow Me prompt tone will be played
New Follow Me Number	Add a new Follow Me number which could be a "Local Extension" or an "External Number". The selected dial plan should have permissions to dial the defined external number.
Dialing Order	This is the order in which the Follow Me destinations will be dialed to reach the user.

SIP Extension Configuration Parameters→*Follow Me*

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

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

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

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.

CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
DND Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Whitelist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
FWD Whitelist	Calls from users in the forward whitelist will not be forwarded.Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. '-' is the connection character that will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension based on this time condition.
Use callee DOD on FWD or RS	Use the callee's DOD number as CallerID on Outgoing Forwarding or Ring Simultaneously calls.
Monitor Privilege Control	
Call Monitoring Whitelist	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.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering the password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via the trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX lists.

Music On Hold	Configure the Music On Hold class to suggest to the bridged channel when putting them on hold.
Use MOH as IVR ringback tone	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
Call Duration Limit	Check to enable and set the call limit the duration.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
Email Missed Calls	Send a log of missed calls to the extension's email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are: Default: All missed calls will be sent in email notifications. Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications. Missed External Call: Only missed calls from trunks will be sent in email notifications.

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

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

Create New FXS Extension

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

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	
Extension	The extension number associated with the user.

Analog Station	Select the FXS port to be assigned for this extension.
Caller ID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Privilege	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls using this rule.
Voicemail	Configure Voicemail. There are three valid options, and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Skip Voicemail Password Verification	When a user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Send Voicemail Email Notification	Configures whether to send emails to the extension's email address to notify of a new voicemail.
Attach Voicemail to Email	Configures whether to attach a voicemail audio file to the voicemail notification emails.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
Emergency CID Name	CallerID name that will be used for emergency calls and callbacks.
Disable This Extension	If selected, this extension will be disabled on the UCM630X. Note: The disabled extension still exists on the PBX but cannot be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random password is automatically generated. It is recommended to use the randomly generated password for security purposes.
Mobile Phone Number	Configure the Mobile number of the user.
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under Web GUI→PBX Settings→Voice Prompt→Language Settings. The dropdown list shows all the currently available voice prompt languages on the UCM630X. To add more languages to the list, please download the voice prompt package by selecting "Check Prompt List" under Web GUI→PBX Settings→Voice Prompt→Language Settings.
Analog Settings	
Call Waiting	Configure to enable/disable call waiting feature. The default setting is "No".
User '#' as SEND	If configured, the # key can be used as SNED key after dialing the number on the analog phone. The default setting is "Yes".
RX Gain	Configure the RX gain for the receiving channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.

TX Gain	Configure the TX gain for the transmitting channel of the analog FXS port. The valid range is -30dB to +6dB. The default setting is 0.
Min RX Flash	Configure the minimum period of time (in milliseconds) that the hook flash must remain unpressed for the PBX to consider the event as a valid flash event. The valid range is 30ms to 1000ms. The default setting is 200ms.
Max RX Flash	Configure the maximum period of time (in milliseconds) that the hook flash must remain unpressed for the PBX to consider the event as a valid flash event. The minimum period of time is 256ms and it cannot be modified. The default setting is 1250ms.
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as Hangup on a polarity reversal. The default setting is "Yes".
Echo Cancellation	Specify "ON", "OFF" or a value (the power of 2) from 32 to 1024 as the number of taps of cancellation. Note: When configuring the number of taps, the number 256 is not translated into 256ms of echo cancellation. Instead, 256 taps mean $256/8 = 32$ ms. The default setting is "ON", which is 128 taps.
3-Way Calling	Configure to enable/disable the 3-way calling feature on the user. The default setting is enabled.
Send CallerID After	Configure the number of rings before sending CID. The default setting is 1.
Fax Mode	For the FXS extension, there are three options available in Fax Mode. The default setting is "None". None: Disable Fax. Fax Gateway: If selected, the UCM630X can support the conversation and processing of Fax data from T.30 to T.38 or T.38 to T.30. only for FXS ports. Fax Detection: During a call, the fax signal from the user/trunk will be detected, and the received fax will be sent to the email address configured for the user. If an email address has been configured for the user, the fax will be sent to the Default Email Address configured in Fax/T.38->Fax Settings.

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific". Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings->Time Settings->Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings->Time Settings->Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.

CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday", and "Specific".Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped.All call forward settings will be ignored.
DND Time Condition	The time condition of DND. The DND will take effect while the time condition is satisfied.
DND Whitelist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
FWD Whitelist	Calls from users in the forward whitelist will not be forwarded.Pattern matching is supported. Z match any digit from 1-9. N match any digit from 2-9. X match any digit from 0-9.
CC Settings	
Enable CC	If enabled, UCM630X will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as 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.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering a password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via the trunk.
Enable LDAP	If enabled, this extension will be added to the LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
Use MOH as IVR ringback tone	If enabled, when the call to the extension is made through the IVR, the caller will hear MOH as a ringback tone instead of the regular ringback tone.
Music On Hold	Select which Music On Hold class to suggest to the extension when putting the active call on hold.
Call Duration Limit	Check to enable and set the call limit the duration.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds
Email Missed Calls	Send a log of missed calls to the extension's email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are: Default: All missed calls will be sent in email notifications. Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications. Missed External Call: Only missed calls from trunks will be sent in email notifications.

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

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

Batch Add Extensions

Batch 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	
Create Number	Specify the number of extensions to be added. The default setting is 5.
Extension Incrementation	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,..... Note: Up to 3 characters.
Extension	Configure the starting extension number of the batch of extensions to be added.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". Note: Users need to have the same level as or higher level than an outbound rule's privilege to make outbound calls from this rule.
Voicemail	Configure Voicemail. There are three valid options and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user. Enable Remote Voicemail: Forward the notify message from remote voicemail system for the user, and the local voicemail will be disabled. Note: Remote voicemail feature is used only for Infomatec (Brazil).
SIP/IAX Password	Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions. User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Send Voicemail to Email	Send voicemail messages to the configured email address. If set to "Default", the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
CallerID Number	Configure CallerID Number when adding Batch Extensions. Use Extension as Number Users can choose to use the extension number as CallerID Use as Number Users can choose to set a specific number instead of using the extension number.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Enable Keep-alive	If enabled, the PBX will regularly send SIP OPTIONS to check if host device is online.
Keep-alive Frequency	Configure the keep-alive interval (in seconds) to check if the host is up.
Disable This Extension	Check this box to disable this extension.

Enable SCA	If enabled, (1) Call Forward, Call Waiting and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Advanced Call Features->SCA page.
Emergency Calls CID	CallerID number that will be used when calling out and receiving direct callbacks.
Enable Wave	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.
Sync Contact	If enabled, this extension number will be displayed in the Wave contact, otherwise it will not be displayed, and it cannot be found in the chat, but the user can still dial this number.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.
Media	
NAT	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it is related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.
Enable Direct Media	By default, the PBX will route the media 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".
DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is "RFC4733". If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, RFC4733 will be used if offered, otherwise "Inband" will be used.
Alert-info	When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS.
SRTP	Enable/disable SRTP for RTP stream encryption.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission. NACK NACK+RTX(SSRC-GROUP) OFF
Video FEC	Check to enable Forward Error Correction (FEC) for Video.
FECC	Configure to enable FECC
Audio FEC	Check to enable Forward Error Correction (FEC) for Audio.
ACL Policy	Access Control List manages the IP addresses that can register to this extension. Allow All: Any IP address can register to this extension. Local Network: Only IP addresses in the configured network segments can register to this extension. Press "Add Local Network Address" to add more IP segments.
Jitter Buffer	Select jitter buffer method. Disable: Jitter buffer will not be used. Fixed: Jitter buffer with a fixed size (equal to the value of "jitter buffer size") Adaptive: Jitter buffer with an adaptive size (no more than the value of "max jitter buffer"). NetEQ: Dynamic jitter buffer via NetEQ.
Codec Preference	Configure the codecs to be used.
Call Transfer	
Presence Status	Select which presence status to set for the extension and configure call forward conditions for each status. Six possible options are possible: "Available", "Away", "Chat", "Custom", "DND" and "Unavailable". More details at [PRESENCE].

Call Forward Unconditional	Enable and configure the Call Forward Unconditional target number. Available options for target number are: "None": Call forward deactivated. "Extension": Select an extension from dropdown list as CFU target. "Custom Number": Enter a customer number as target. For example: *97. "Voicemail": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. "Ring Group": Select a ring group from dropdown list as CFU target. "Queues": Select a queue from dropdown list as CFU target. "Voicemail Group": Select a voicemail group from dropdown list as CFU target. The default setting is "None".
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. Available options for target number are: "None": Call forward deactivated. "Extension": Select an extension from dropdown list as CFN target. "Custom Number": Enter a customer number as target. For example: *97. "Voicemail": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. "Ring Group": Select a ring group from dropdown list as CFN target. "Queues": Select a queue from dropdown list as CFN target. "Voicemail Group": Select a voicemail group from dropdown list as CFN target. The default setting is "None".
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. Available options for target number are: "None": Call forward deactivated. "Extension": Select an extension from dropdown list as CFB target. "Custom Number": Enter a customer number as target. For example: *97. "Voicemail": Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. "Ring Group": Select a ring group from dropdown list as CFB target. "Queues": Select a queue from dropdown list as CFB target. "Voicemail Group": Select a voicemail group from dropdown list as CFB target. The default setting is "None".
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
DND Time Condition	Select time condition for Do Not Disturb. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
DND Whitelist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9 N match any digit from 2-9 X match any digit from 0-9.

FWD Whitelist	Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported. Z match any digit from 1-9 N match any digit from 2-9 X match any digit from 0-9.
CC Settings	
Enable CC	If enabled, 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.
CC Mode	Two modes for Call Completion are supported: Normal: This extension is used as ordinary extension. For Trunk: This extension is registered from a PBX. The default setting is "Normal".
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel can make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored. This field accepts only letters, numbers, and special characters + = * #.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Use callee DOD on FWD or RS	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
Monitor privilege control	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform seamless transfer to the edited extension.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the 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. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under Web GUI→CDR→Recording Files.
Skip Trunk Auth	If set to "yes", users can skip entering the password when making outbound calls. If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.

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

Batch Add 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.

General	
Create Number	Specify the number of extensions to be added. The default setting is 5.
Extension Incrementation	Select how much to increment successive extensions. For example, if the value is 2, the extensions will be 1000,1002,1004,.....
Extension	The extension number associated with this particular user/phone.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". Note: Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls from this rule.
CallerID Number	Configure the Caller ID number displayed when dialing calls from this user. Note: The Caller ID usage might be limited by your VoIP provider. In Batch Add Method, "e" means to use the extension as the number.
Voicemail	Configure Voicemail. There are three valid options and the default option is "Enable Local Voicemail". Disable Voicemail: Disable Voicemail. Enable Local Voicemail: Enable voicemail for the user.
SIP/IAX Password	Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions. User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Send Voicemail to Email	Send voicemail messages to the configured email address. If set to "Default", the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.
Keep Voicemail after Emailing	Only applies if extension-level or global Send Voicemail to Email is enabled.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.

Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Disable This Extension	Check this box to disable this extension.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.
IAX Settings	
Max Number of Calls	Configure the maximum number of calls allowed for each remote IP address.
Require Call Token	Configure to enable/disable requiring call token. If set to "Auto", it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints. The default setting is "Yes".
SRTP	Enable/disable SRTP for RTP stream encryption.
ACL Policy	Access Control List manages the IP addresses that can register to this extension. Allow All: Any IP address can register to this extension. Local Network: Only IP addresses in the configured network segments can register to this extension.
Codec Preference	Configure the codecs to be used.
Call Transfer	
Call Forward Unconditional	Enable and configure the Call Forward Unconditional target number.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Note: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number.
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
DND Time Condition	Select time condition for Do Not Disturb. The available time conditions are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Notes: "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.

DND Whitelist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. Z match any digit from 1-9, N match any digit from 2-9, X match any digit from 0-9.
FWD Whitelist	Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported. Z match any digit from 1-9, N match any digit from 2-9, X match any digit from 0-9.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored. This field accepts only letters, numbers, and special characters + = * #.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Use callee DOD on FWD or RS	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
Monitor privilege control	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform seamless transfer to the edited extension.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the 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. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under Web GUI→CDR→Recording Files.
Skip Trunk Auth	If set to "yes", users can skip entering the password when making outbound calls. If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX list.
Music On Hold	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
Call Duration Limit	Check to enable and set the call limit the duration.
Maximum Call Duration (s)	The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds

Batch Extension Resetting Functionality

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

and confirm the reset functionality. Once done, all settings in Basic Settings page will be restored to default values with the exception of Concurrent Registrations. User voicemail password will be reset to Random Password. User voicemail prompts and recordings will be deleted. User Management settings will also be restored to default with the exception of usernames and custom privileges

Search and Edit Extension

All the 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"

, "Reboot"

and "Delete"

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

Extensions

+ Add

Edit

Delete

Edit All SIP

E-mail Notification

More

Q Extension Number or Name

Search

☐	STATUS	PRESENC...	EXTENSION	NAME	MESSAGE	TYPE	IP AND PORT	EXTENSION I...	OPTIONS
☐	● Unavailable Available		1000		0/0/0	SIP(WebRT...	--		
☐	● Idle	Available	1001		0/1/0	SIP(WebRT...	192.168.5.10...		
☐	● Unavailable Available		1002		0/0/0	SIP(WebRT...	--		
☐	● Unavailable Available		1003		0/0/0	SIP(WebRT...	--		
☐	● Unavailable Available		1004		0/0/0	SIP(WebRT...	--		

<

1

>

Total: 5

30 / page

Goto

1

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

Manage Extensions

- Status

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

Green: Idle

Blue: Ringing

Yellow: In Use

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

- **Edit single extension**

Click on

to start editing the extension parameters.

- **Reset single extension**

Click on

A close up of a logo Description generated with high confidence

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.

This is the expected behavior when you reset an extension:

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

- **Reboot the user**

Click on

to send NOTIFY reboot event to the device which has 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".

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

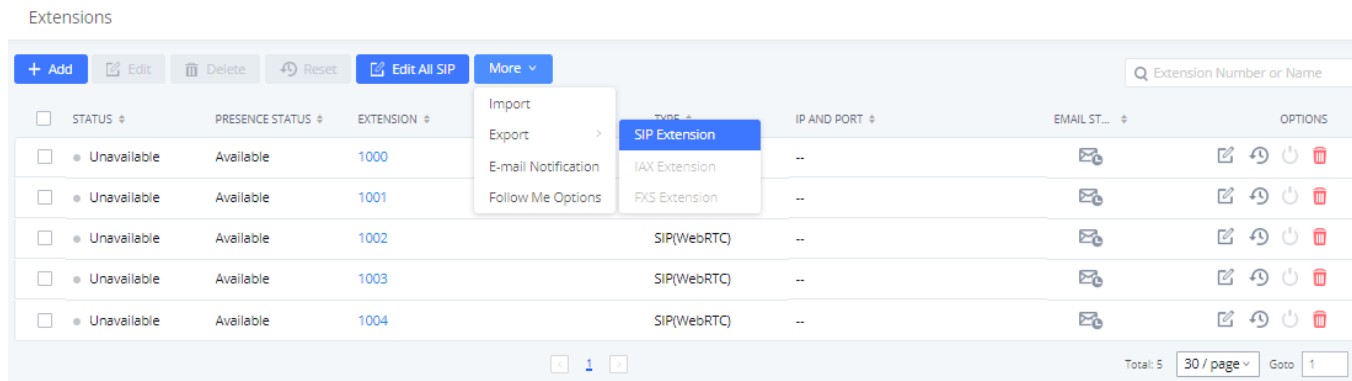
Select the checkbox for the extension(s). Then click on "Edit" to edit the extensions in a batch.

- 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.



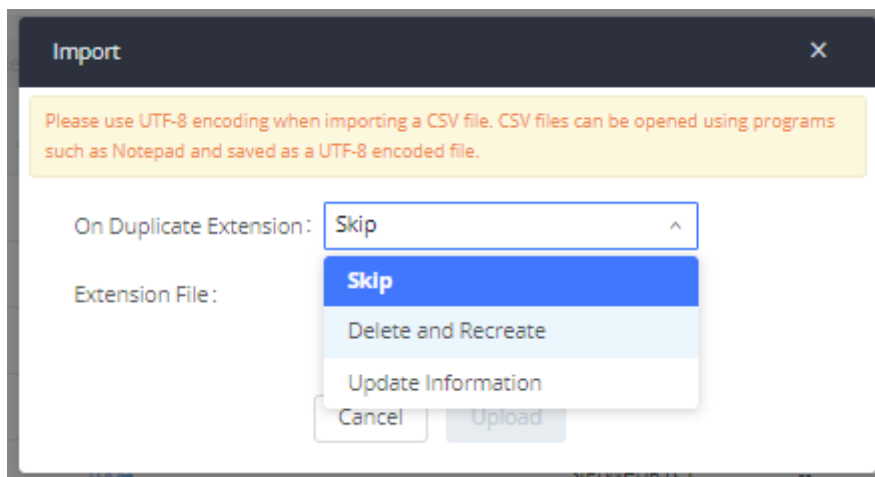
Export Extensions

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.

- **Skip:** Duplicate extensions in the csv file will be skipped. The PBX will keep the current extension information as previously configured without change.
 - **Delete and Recreate:** The current extension previously configured will be deleted and the duplicate extension in the csv file will be loaded to the PBX.
 - **Update Information:** The current extension previously configured in the PBX will be kept. However, if the duplicate extension in the csv file has different configuration for any options, it will override the configuration for those options in the extension.
5. Click on "Choose file to upload" to select csv file from local directory in the PC.
 6. Click on "Apply Changes" to apply the imported file on the 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
Extension	Digits
Technology	SIP/SIP(WebRTC)
Enable Voicemail	yes/no/remote
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask
Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime

Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,A DPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
NAT	yes/no
DTMF Mode	RFC4733/info/inband/auto
Insecure	Port
Enable Keep-alive	Yes/no
Keep-alive Frequency	Value from 1-3600
AuthID	Alphanumeric value without special characters
TEL URI	Disabled/user=phone/enabled
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Support Hot-Desking Mode	Yes/no
Dial Trunk Password	Digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Enable T.38 UDPTL	Yes/no
Max Contacts	Values from 1-10
Enable Wave	Yes/no
Alert-Info	None/Ring 1/Ring2/Ring3/Ring 4/Ring 5/Ring 6/Ring 7/ Ring 8/Ring 9/Ring 10/bellcore-dr1/bellcore-dr2/ bellcore-dr3/ bellcore-dr4/ bellcore-dr5/custom

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

SIP extensions Imported File Example

Field	Supported values
Extension	Digits
Technology	IAX
Enable Voicemail	yes/no
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask
Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,A DPCM,G.723,H.263,H.263p,vp8,opus

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

IAX extensions Imported File Example

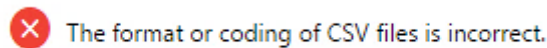
Field	Supported values
Extension	Digits
Technology	FXS
Analog Station	FXS1/FXS2
Enable Voicemail	yes/no

CallerID Number	Digits
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
Auto Record	yes/no
Fax Mode	None/Fax Gateway/Fax Detection
Skip Trunk Auth	Yes/no/bytime
Permission	Internal/Local/National/International
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Call Waiting	Yes/no
Use # as SEND	Yes/no
RX Gain	Values from -30→6
TX Gain	Values from -30→6
MIN RX Flash	Values from: 30 - 1000
MAX RX Flash	Values from: 40 - 2000
Enable Polarity Reversal	Yes/no
Echo Cancellation	On/Off/32/64/128/256/512/1024
3-Way Calling	Yes/no
Send CallerID After	1/2
Dial Trunk Password	digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time

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

FXS Extensions Imported File Example

The 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.



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.

More

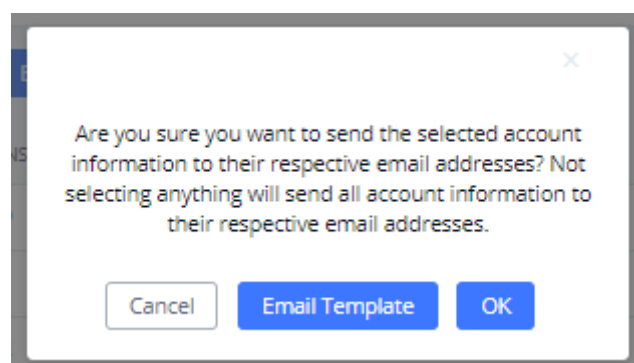
OPTIONS	VALUE
Extension	1000
Status	Unavailable
Presence Status	Available
Terminal Type	SIP(WebRTC)
CallerID Name	
Message	0/0/0
IP and Port	--
Email Status	To Be Sent
Ring Group	
Call Queue	
Call Queue(Dynamic)	

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

Account Registration Information

GSWave Settings

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

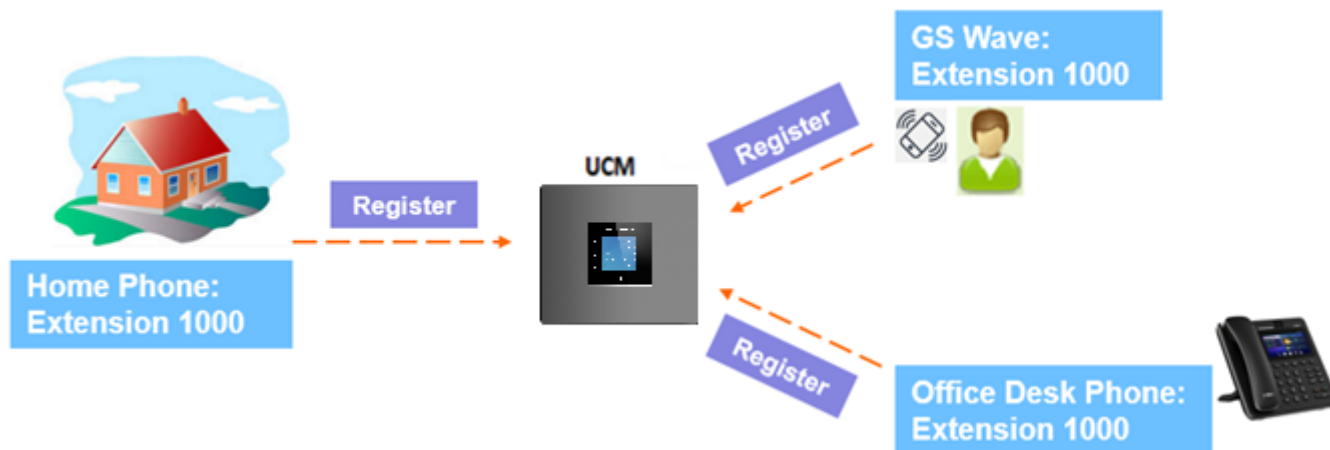


Use Web App to scan qr code and log in

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

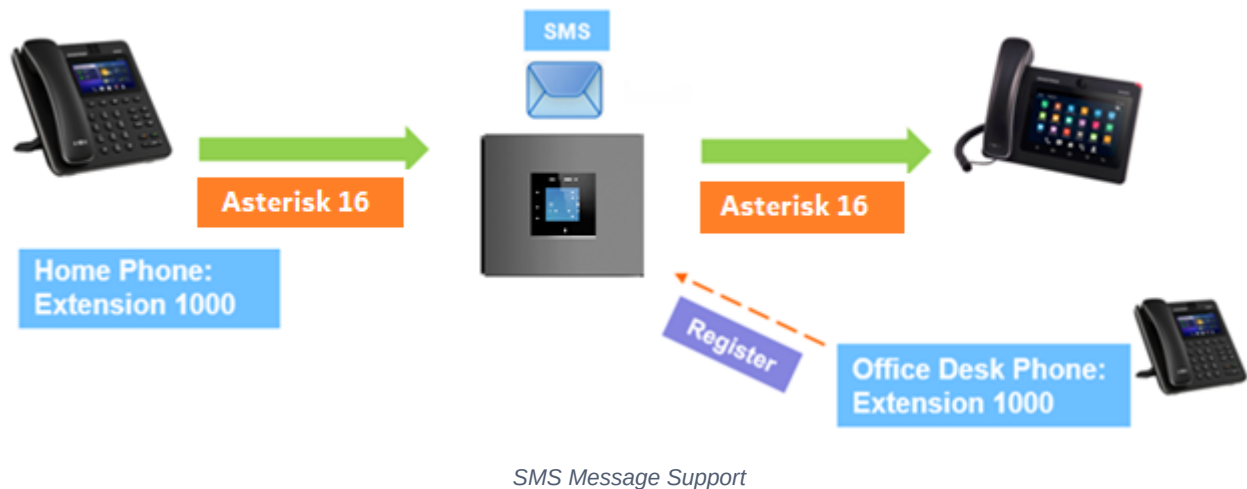
Basic Settings Media Features Specific Time Follow Me Cancel Save

General	
* Extension:	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:	☐
User Settings	
First Name:	
Email Address:	
* Language:	Default
Mobile Phone Number:	
Last Name:	
* User Password:	*****
* Concurrent Registrations:	3

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.



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.

Create New Extension Group

* Name:

Tech_Supprot_Team

Members:

☐ 0 item

Available

Search

Q

None

<

>

↑

^

↓

v

☐ 6 items

Selected

Search

Q

☐ 1000

☐ 4001

☐ 4002

☐ 4003

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:

test

Pattern:

_9x.

PIN Groups:

None

Password:

Disable This Route:

☐

Privilege Level:

Disable

PIN Groups with Privilege Level:

☐

Enable Filter on Source Caller ID

Enable Filter on Source Caller

☒

ID:

Custom Dynamic Route:

Outbound Route CID:

Available Extensions/Extension Groups:

Extension GroupGStest

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
FXO Port	Select the channel for the analog trunk. UCM6301: 1 channel UCM6302: 2 channels UCM6304: 4 channels UCM6308: 8 channels
Trunk Name	Specify a unique label to identify the trunk when listed in outbound rules, incoming rules, etc.
Advanced Options	
Disable This Trunk	If selected, the trunk will be disabled, and incoming/Outgoing calls via this trunk will not be possible.
SLA Mode	Enable this option to satisfy two primary use cases, which include emulating a simple key system and creating shared extensions on a PBX. Enable SLA Mode will disable polarity reversal.
Barge Allowed	The barge option specifies whether other stations can join a call in progress on this trunk. If enabled, the other stations can press the line button to join the call.The default setting is Yes.This option appears when SLA Mode is enabled.
Hold Access	The hold option specifies hold permissions for this trunk. If set to "Open", any station can place this trunk on hold and any other station is allowed to retrieve the call. If set to "Private", only the station that places the call on hold can retrieve the call.The default setting is Yes.

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

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

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

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.

Tone Settings

Busy Detection:

☒

Congestion Detection:

☒

* Tone Country:

United States of America (USA) ▼

* Congestion Tone Settings:

f1=480@-50,f2=620@-50,c=250/250

* Busy Tone Count:

2

* Congestion Count:

2

* Busy Tone:

f1=480@-50,f2=620@-50,c=500/500

PSTN Detection:

Detect

UCM630xA FXO Tone Settings

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

PSTN Detection [X]

Detect model: Auto Detect ▾

Source Channel (to be detected): 1 ▾

Destination Channel: 1 ▾

* Destination Number:

Dump Call Progress Tone ☐

File:

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.

Cancel Detect

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.

PSTN Detection [X]

Detect model: Auto Detect ▾

Source Channel (to be detected): 1 ▾

Destination Channel: 2 ▾

* Destination Number: 123654

Dump Call Progress Tone ☐

File:

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.

Cancel Detect

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

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.

- 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.
- Once done, the detected result will show. Users could save the detecting result as the current UCM630xA settings.

Detect Model	Select "Auto Detect" or "Semi-auto Detect" for PSTN detection. Auto Detect Please make sure two or more channels are connected to the 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. Semi-auto Detect 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. The default setting is "Auto Detect".
Source Channel	Select the channel to be detected.
Destination Channel	Select the channel to help detect when "Auto Detect" is used.
Destination Number	Configure the number to be called to help the detection.
Dump Call Progress Tone File	Choose whether to save the calling tone file, it is not checked by default.

- 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 on the UCM under **Web GUI->Extension/Trunk->VoIP Trunks**.

VoIP Trunks

VoIP Trunks Trunk Group

Add SIP Trunk Add IAX Trunk

Provider Name	Status	Active Calls	Endpoint Type	Type	Hostname/IP Address	Username	Total Time for Outbound Calls (m)	Options
Orange	Unreachable	0	SIP	peer	192.168.6.254		Unlimited	   
Route22	Unreachable	0	SIP	peer	192.168.6.208		Unlimited	   
Server	Unregistered	0	SIP	account		admin	Unlimited	   
UCM6308/A	Reachable	2	SIP	peer	192.168.6.75		Unlimited	   
UCM_B	Unreachable	0	SIP	peer	192.168.6.208		Unlimited	   

VoIP Trunks Overview Page

Once created, all VoIP trunks will appear in a list showing the following key information:

- **Provider Name:** A user-defined label to identify the trunk.
- **Status:** The current state of the trunk (Registered, Reachable, Unreachable, or Unmonitored).
- **Active Calls:** The number of calls currently using the trunk.
- **Endpoint Type:** The protocol used for the trunk (SIP or IAX).
- **Type:** The trunk type (register, peer, or account).
- **Hostname/IP Address:** The server address of the trunk.
- **Username:** The authentication username for register/account trunks.
- **Total Time for Outbound Calls (m):** The cumulative outbound call duration limit.
- **Options:** Quick access to management functions using the icons described below:
 - **Edit:** Opens the trunk configuration page (Basic + Advanced settings).
 - **DOD:** Opens Direct Outward Dialing settings for that trunk (maps extensions to outbound CallerID).
 - **Sync LDAP:** Starts LDAP phonebook synchronization (only for SIP peer trunks with Sync LDAP enabled).
 - **Delete:** Removes the trunk from the UCM system.

The following sections provide a detailed explanation of the available configuration parameters for each trunk type.

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.

Option	Description
Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send an UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
Type	Select the trunk type (e.g., Register SIP Trunk or Peer SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.
Auto Record	Enable automatic recording for calls using this trunk (SIP trunk only). The default setting is disabled. Recordings can be accessed under Web GUI -> CDR -> Recording Files.
Keep Original CID	Configures CID handling for forwarded outgoing calls. The default setting is "No". Yes: Keep the CID from the inbound call when dialing out. This setting overrides "Keep Trunk CID". Ensure the peer PBX supports matching user entries using the username field from the authentication line. No: Do not keep the original incoming CID. DOD: Checks if the originating extension has a DOD assigned. If assigned, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, set to "User=Phone" to attach a "User=Phone" parameter to the Request-Line and TO header in the SIP request. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. Default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when the "Register SIP Trunk" type is selected. Default setting is No.
Allow outgoing calls if registration fails	If enabled, outgoing calls can still go through even if registration to this trunk fails. Note: Unchecking "Need Registration" causes this option to be ignored.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
From User	Configure the actual username of the extension to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).

Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for the "Register SIP Trunk" type.
Verify Inbound Requests	If enabled, incoming SIP requests will be verified against authentication credentials or trunk parameters.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them.
Monitor Concurrent Calls	If enabled, the "Trunk Concurrent Calls" system event monitors the number of concurrent calls on this trunk and generates an alert if the threshold is exceeded. Turn on the alert for "Trunk Concurrent Calls" first.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	Enables setting a cumulative total outbound call duration limit for this SIP trunk across a specified time period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Advanced Settings	
Codec Preference	Select the audio codec for the VoIP trunk (PCMU, PCMA, GSM, G.726, G.729, iLBC, G.722, G.722.1, G.722.1C, G.723.1, H.263, H.263p, etc.).
Packet Loss Retransmission	Configure Packet Loss Retransmission: NACK NACK+RTX(SSRC-GROUP) OFF
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure Forward Error Correction (FEC) for video.
Media Traversal Method	Configures the media traversal method (e.g., None, STUN, TURN) used for NAT traversal.
FECC	Remote Camera Management.
Silence Suppression	Enables silence suppression to save bandwidth during periods of silence.
SRTP	Enable SRTP for the call (Default: Disabled): Disabled Enabled and Enforced: SRTP is required to transmit media traffic. Optional: Negotiates whether to use SRTP based on endpoint capability.
SRTP Crypto Suite	SRTP encryption suite priority order used by UCM for outbound calls: AES_CM_128_HMAC_SHA1_80 (Default) AES_256_CM_HMAC_SHA1_80 AEAD_AES_128_GCM AEAD_AES_256_GCM
ZRTP Encryption Mode	If disabled, ZRTP encryption is not supported. Otherwise, ZRTP will be supported and prioritized over SRTP if the endpoint supports both.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. May cause incompatibility when interconnecting with certain devices.

Send PPI Header	If enabled, outgoing SIP INVITE messages contain a PPI (P-Preferred-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.
Send PAI Header	If enabled, outgoing SIP INVITE messages contain a PAI (P-Asserted-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.
DOD as From Name	If enabled, uses the extension's assigned DOD name as the "From" display name in outgoing SIP headers.
DOD as Contact User	If enabled, uses the extension's assigned DOD number as the user portion of the SIP Contact header.
Passthrough PAI Header	If checked and "Send PAI Header" is disabled, the PAI header is passed through from one side to the other.
Send PANI Header	If checked, INVITE and REGISTER messages sent to the trunk contain the P-Access-Network-Info header.
Send Diversion Header	Configure whether to send a Diversion header on trunk calls to indicate call forwarding details.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). Not Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call.
Send Anonymous	If checked, the "From" header in outgoing INVITE messages is set to anonymous.
Outbound Proxy Support	Enables outbound proxy support for this trunk. Default setting is "No".
DID Mode	Configure whether to extract the incoming call destination ID from the SIP Request-line or To-header. Default is "Request-line".
GIN Registration	If enabled, the UCM sends a GIN REGISTER to generate implicit numbers.
DTMF Mode	Configures DTMF transmission mode: Default: Uses global ToS SIP settings. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO messages. Inband: Send DTMF using inband audio (requires PCMU or PCMA). Auto: Uses RFC4733 if offered; falls back to inband.
Enable Heartbeat Detection	If enabled, regularly sends SIP OPTIONS to monitor device availability. Default setting is "No".
Max Outgoing Calls	Configures maximum concurrent outgoing calls over the trunk (Default: 0 / unlimited).
Max Incoming Calls	Configures maximum concurrent incoming calls through the trunk (Default: 0 / unlimited).
Max Concurrent Calls	Configures maximum simultaneous incoming and outgoing calls going through the SIP trunk (Default: 0 / unlimited).
Response to Blocked Call	Configures the SIP response code returned when concurrent call limits are reached: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
STIR/SHAKEN	Configures STIR/SHAKEN authentication to prevent call spoofing, robocalls, and spam: Disabled Outgoing Attest: Authenticates outgoing caller IDs. Incoming Verify: Verifies incoming caller ID authentication. Both: Authenticates outgoing calls and verifies incoming calls.
CC Settings	
Enable CC	If enabled, automatically alerts the user when a previously busy or unavailable called party becomes available.

Register SIP Trunk

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

Option	Description
Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send an UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
Type	Select the trunk type (e.g., Register SIP Trunk or Peer SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.
Auto Record	Enable automatic recording for calls using this trunk (SIP trunk only). The default setting is disabled. Recordings can be accessed under Web GUI -> CDR -> Recording Files.
Keep Original CID	Configures CID handling for forwarded outgoing calls. The default setting is "No". Yes: Keep the CID from the inbound call when dialing out. This setting overrides "Keep Trunk CID". Ensure the peer PBX supports matching user entries using the username field from the authentication line. No: Do not keep the original incoming CID. DOD: Checks if the originating extension has a DOD assigned. If assigned, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, set to "User=Phone" to attach a "User=Phone" parameter to the Request-Line and TO header in the SIP request. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. Default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when the "Register SIP Trunk" type is selected. Default setting is No.
Allow outgoing calls if registration fails	If enabled, outgoing calls can still go through even if registration to this trunk fails. Note: Unchecking "Need Registration" causes this option to be ignored.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
From User	Configure the actual username of the extension to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk when "Register SIP Trunk" is selected.

Auth ID	Enter the Authentication ID for the "Register SIP Trunk" type.
Verify Inbound Requests	If enabled, incoming SIP requests will be verified against authentication credentials or trunk parameters.
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them.
Monitor Concurrent Calls	If enabled, the "Trunk Concurrent Calls" system event monitors the number of concurrent calls on this trunk and generates an alert if the threshold is exceeded. Turn on the alert for "Trunk Concurrent Calls" first.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	Enables setting a cumulative total outbound call duration limit for this SIP trunk across a specified time period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Advanced Settings	
Codec Preference	Select the audio codec for the VoIP trunk (PCMU, PCMA, GSM, G.726, G.729, iLBC, G.722, G.722.1, G.722.1C, G.723.1, H.263, H.263p, etc.).
Packet Loss Retransmission	Configure Packet Loss Retransmission: NACK NACK+RTX(SSRC-GROUP) OFF
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure Forward Error Correction (FEC) for video.
Media Traversal Method	Configures the media traversal method (e.g., None, STUN, TURN) used for NAT traversal.
FECC	Remote Camera Management.
Silence Suppression	Enables silence suppression to save bandwidth during periods of silence.
SRTP	Enable SRTP for the call (Default: Disabled): Disabled Enabled and Enforced: SRTP is required to transmit media traffic. Optional: Negotiates whether to use SRTP based on endpoint capability.
SRTP Crypto Suite	SRTP encryption suite priority order used by UCM for outbound calls: AES_CM_128_HMAC_SHA1_80 (Default) AES_256_CM_HMAC_SHA1_80 AEAD_AES_128_GCM AEAD_AES_256_GCM
ZRTP Encryption Mode	If disabled, ZRTP encryption is not supported. Otherwise, ZRTP will be supported and prioritized over SRTP if the endpoint supports both.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. May cause incompatibility when interconnecting with certain devices.
Send PPI Header	If enabled, outgoing SIP INVITE messages contain a PPI (P-Preferred-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.

Send PAI Header	If enabled, outgoing SIP INVITE messages contain a PAI (P-Asserted-Identity) header. Default setting is "No". Note: "Send PPI Header" and "Send PAI Header" cannot be enabled simultaneously.
DOD as From Name	If enabled, uses the extension's assigned DOD name as the "From" display name in outgoing SIP headers.
DOD as Contact User	If enabled, uses the extension's assigned DOD number as the user portion of the SIP Contact header.
Passthrough PAI Header	If checked and "Send PAI Header" is disabled, the PAI header is passed through from one side to the other.
Send PANI Header	If checked, INVITE and REGISTER messages sent to the trunk contain the P-Access-Network-Info header.
Send Diversion Header	Configure whether to send a Diversion header on trunk calls to indicate call forwarding details.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). Not Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call.
Send Anonymous	If checked, the "From" header in outgoing INVITE messages is set to anonymous.
Outbound Proxy Support	Enables outbound proxy support for this trunk. Default setting is "No".
DID Mode	Configure whether to extract the incoming call destination ID from the SIP Request-line or To-header. Default is "Request-line".
GIN Registration	If enabled, the UCM sends a GIN REGISTER to generate implicit numbers.
DTMF Mode	Configures DTMF transmission mode: Default: Uses global ToS SIP settings. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO messages. Inband: Send DTMF using inband audio (requires PCMU or PCMA). Auto: Uses RFC4733 if offered; falls back to inband.
Enable Heartbeat Detection	If enabled, regularly sends SIP OPTIONS to monitor device availability. Default setting is "No".
Max Outgoing Calls	Configures maximum concurrent outgoing calls over the trunk (Default: 0 / unlimited).
Max Incoming Calls	Configures maximum concurrent incoming calls through the trunk (Default: 0 / unlimited).
Max Concurrent Calls	Configures maximum simultaneous incoming and outgoing calls going through the SIP trunk (Default: 0 / unlimited).
Response to Blocked Call	Configures the SIP response code returned when concurrent call limits are reached: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
STIR/SHAKEN	Configures STIR/SHAKEN authentication to prevent call spoofing, robocalls, and spam: Disabled Outgoing Attest: Authenticates outgoing caller IDs. Incoming Verify: Verifies incoming caller ID authentication. Both: Authenticates outgoing calls and verifies incoming calls.
CC Settings	
Enable CC	If enabled, automatically alerts the user when a previously busy or unavailable called party becomes available.

Peer SIP Trunk

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

Option	Description
--------	-------------

Basic Settings	
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send an UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
Type	Select the trunk type (e.g., Peer SIP Trunk).
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". UDP TCP TLS
Minimize SIP Messages	If enabled, to minimize the size of SIP messages, this trunk will not support headers such as Remote-Party-ID, Session-Expires, and X-GS-Trunk; the SDP will only include audio media with PCMU/PCMA/G729 codecs and no special attributes.
Auto Record	Enable automatic recording for calls using this trunk (SIP trunk only). The default setting is disabled. Recordings can be accessed under Web GUI -> CDR -> Recording Files.
Keep Original CID	Configures CID handling for forwarded outgoing calls. The default setting is "No". Yes: Keep the CID from the inbound call when dialing out. This setting overrides "Keep Trunk CID". Ensure the peer PBX supports matching user entries using the username field from the authentication line. No: Do not keep the original incoming CID. DOD: Checks if the originating extension has a DOD assigned. If assigned, the system uses that extension's DOD for the outgoing forwarded call. If no DOD is assigned, it falls back to keeping the original caller's CID.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using a public IP and communicating with devices behind NAT. If there is a one-way audio issue, it is usually related to NAT configuration or SIP/RTP port configuration on the firewall.
TEL URI	If the trunk has an assigned PSTN telephone number, set to "User=Phone" to attach a "User=Phone" parameter to the Request-Line and TO header in the SIP request. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. Default setting is disabled.
CallerID Number	Configure the default Caller ID number sent when making calls through this trunk. Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: CID from inbound call (Keep Original CID Enabled) -> Trunk Username/CallerID (Keep Trunk CID Enabled) -> DOD -> Extension CallerID Number -> Trunk Username/CallerID (Keep Trunk CID Disabled) -> Global Outbound CID.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	Configure the actual domain name where the extension comes from to override the "From" Header (e.g., sip:1234567@trunk.UCM630X.provider.com).
Jitter Buffer	Configures the jitter buffer mechanism (e.g., NetEQ) for audio buffering and stabilization.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them. For Example: User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option "Direct Callback" is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.
RemoteConnect Mode	If enabled, RemoteConnect parameters are set synchronously. Ensure the trunk host is allocated by GDMS or supports TLS.

Monitor Concurrent Calls	If enabled, the "Trunk Concurrent Calls" system event monitors the number of concurrent calls on this trunk and generates an alert if the threshold is exceeded. Turn on the alert for "Trunk Concurrent Calls" first.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls through this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Total Time Limit For Outbound Calls	
Enable Total Time Limit For Outbound Calls	Enables setting a cumulative total outbound call duration limit for this SIP trunk across a specified time period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three calendar months.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Media	
Codec Preference	Select the audio codec for the VoIP trunk (PCMU, PCMA, GSM, G.726, G.729, iLBC, G.722, G.722.1, G.722.1C, G.723.1, H.263, H.263p, H.264, H.265, VP8, etc.).
Packet Loss Retransmission	Configure Packet Loss Retransmission.
Audio FEC	Configure to enable Forward Error Correction (FEC) for audio.
Video FEC	Configure Forward Error Correction (FEC) for video.
Media Traversal Method	Select the NAT traversal method for media packets: None: No NAT traversal mechanism will be used by the UCM. ICE Support: STUN will be used as a NAT traversal mechanism. TURN Relay: TURN relay will be used to relay the media packets.
FECC	Configure to enable Far-end Camera Control.
Silence Suppression	If enabled, the UCM will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint's OPUS codec supports the reception of DTX packets, the UCM will send DTX packets instead.
SRTP	Enable SRTP for the VoIP trunk. Default setting is "No".
SRTP Crypto Suite	SRTP encryption suite priority order used by UCM for outbound calls. Priority is based on order of configuration.
ZRTP Encryption Mode	If disabled, ZRTP encryption is not supported. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.
IPVT Mode	Configures the UCM to be used exclusively for IPVT. Warning: This will lock out certain UCM features.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. May cause incompatibility when interconnecting with certain devices.
Features	
Send PPI Header	If checked, the invite message sent to trunks will contain PPI (P-Preferred-Identity) Header.
Send PAI Header	If checked, the INVITE, 18x and 200 SIP messages sent to trunks will contain P-Asserted-Identity (PAI) header. It is not possible to send both PPI and PAI headers.
PAI Header	If "Send PAI Header" is enabled and "PAI Header" is configured, the PAI header in the SIP message sent from the UCM will contain the configured value. If empty, the PAI header will contain the original CID.

Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the UCM.
Send PANI Header	If checked, the INVITE sent to the trunk will contain P-Access-Network-Info header.
Access Network Info	Access network information carried in the P-Access-Network-Info header.
Send Diversion Header	Configure whether or not send Diversion header on the trunk call. Diversion header indicates that the call has been forwarded, it includes information about the call before the forwarding like the original callee and the type of forwarding: Yes: Include the Diversion header. No Deflection: Do not include Diversion header if the diversion reason is "deflection". No: Do not include the Diversion header.
Diversion Mode	Configures handling and filtering mode for Diversion headers: All: Include Diversion header for all forwarded calls. No Deflection: Do not include Diversion header if the diversion reason is "deflection" (e.g., Follow Me or inbound route rerouting). Not Passthrough: Strips/blocks any Diversion header received from the incoming caller's side while allowing the PBX to generate and attach its own local Diversion header for the forwarded call.
Send Anonymous	If checked, the "From" header in outgoing INVITE message will be set to anonymous.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	Configure the default DTMF mode when sending DTMF on this trunk: Default: Uses global ToS SIP settings. RFC4733: Send DTMF using RFC4733. Info: Send DTMF using SIP INFO message. Inband: Send DTMF using inband audio. Auto: Send DTMF using RFC4733 if offered; otherwise, inband is used.
Enable Heartbeat Detection	If enabled, the UCM630xA will regularly send SIP OPTIONS to the device to check if the device is still online. Default setting is "No".
Heartbeat Frequency (s)	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. Default setting is 60 seconds.
Max Outgoing Calls	The number of concurrent outgoing calls over the trunk at the same time. The default value 0 means no limit.
Max Incoming Calls	The max allowed number of concurrent incoming calls through the trunk.
Max Concurrent Calls	The maximum allowed number of concurrent incoming and outgoing calls going through the SIP trunk. Default value is 0 (no limit).
Response to Blocked Call	Set the response code to the caller when the concurrent calls has reached the upper limit: 480: Temporarily Unavailable 486: Busy Here 503: Service Unavailable
Sync LDAP Enable	Automatically sync local LDAP phonebooks to a remote peer (SIP peer trunk only). To ensure successful syncing, the remote peer must also enable this service and set the same password as the local UCM. Port 873 is used by default.
Sync LDAP Password	Password used for LDAP phonebook encryption and decryption. The password must be the same for both peers to ensure successful syncing.
LDAP Outbound Rule	Specify an outbound rule. The PBX system will automatically modify the remote contacts by adding prefix parsed from this rule.
LDAP Dialed Prefix	System will automatically modify the remote contacts by adding this prefix.
LDAP Sync Method	Specifies the sync method of the UCM. When an LDAP sync request is received, the UCM will send the phonebook data via the specified method.
LDAP Last Sync Date	Displays the timestamp of the last successful sync.

STIR/SHAKEN	Configure this feature to prevent call spoofing, robocalls and spam calls: Disabled Outgoing Attest: The UCM will only authenticate the caller ID. Incoming Verify: The UCM will only verify if the caller ID is authenticated. Both: The UCM will authenticate outgoing calls as well as verify if incoming calls are authenticated.
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. Minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. Minimum value is 1.

Create New IAX Trunk

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

- [IAX Peer Trunk](#)
- [IAX Register Trunk](#)

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules, etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by the extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.

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

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

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 TrunksTrunk 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.

Create New Trunk Group

CancelSave

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 Ni

/

Password

/

AuthID

Add Username

Line Selection Strategy:

Linear

AuthTrunk:

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

Trunk Group Configuration

Type	Register Trunk
------	----------------

Provider Name	Configure a unique label to identify the trunk when listed in outbound rules and incoming rules.
Host Name	Enter the IP address or hostname of the VoIP provider's server.
Transport	Configure the SIP Transport method. Using TCP requires local TCP support; using TLS requires local TLS support.
Keep Original CID	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.
Keep Trunk CID	Always use trunk CID if specified even if extension has DOD number or CID configured.
NAT	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.
Disable This Trunk	Check this box to disable this trunk
TEL URI	if "Enabled" option is selected, TEL URI and remove OBP from Route cannot be enabled at the same time. If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". A "User=Phone" parameter will 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.
Need Registration	Whether to register on the external server.
Allow outgoing calls if registration fails	Uncheck to block outgoing calls if registration fails. If "Need Registration" option is unchecked, this setting will be ignored.
CallerID Name	To display the caller ID name of the trunk, you must configure the caller ID number of the trunk.
Trunk Registration Number	The number used to register with the provider server, and the VoIP provider will authenticate the number based on the trunk registration number.
Line Selection Strategy	Linear: Select lines in list order and make Outbound calls. Round Robin: Rotary line selection with memory and making Outbound calls.
AuthTrunk	If enabled, the IPPBX will send a 401 response to the incoming call to authenticate the trunk.
Auto Record	If enabled, calls handled with this extension/trunk will automatically be recorded.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them.
RemoteConnect Mode	If enabled, RemoteConnect-related options will be automatically configured. Please confirm the trunk has a GDMS-assigned address or supports TLS.
Monitor Concurrent Calls	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
Concurrent Call Threshold	Threshold of all incoming and outgoing concurrent calls in this trunk.
Outgoing Concurrent Call Threshold	Threshold of all outgoing concurrent calls passing through this trunk.
Incoming Concurrent Call Threshold	Threshold of all incoming concurrent calls passing through this trunk.
Enable Total Time Limit For Outbound Calls	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 framework that enables audio and video communication directly through web browsers. The UCM63xx series supports creating WebRTC trunks to connect web applications with the PBX, allowing visitors or customers to initiate calls or join meetings directly from a website.

WebRTC Trunks

Add			
Trunk Name	Trunk Status	Inbound Link	Options
123	Available	https://gdmcloud.click2call?from_user=webrtc_trunk_10&to_user=se...	
Test123	Available	https://gdmcloud.click2call?from_user=webrtc_trunk_8&to_user=se...	
WebRTC_Live	Available	https://gdmcloud.click2call?from_user=webrtc_trunk_4&to_user=se...	

Total 310 / page

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

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

Embed the code snippet on your website

To add online call support to websites, users can

1. Embed the *Online Call Link Address* into the web page.

2. Embed the following JavaScript code snippet into the web page, which will create an online call button in the lower right corner of the page:

Download Code

Copy Code

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

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

Advanced Settings	
Packet Loss Retransmission	Configures packet loss recovery methods (e.g., NACK+RTX) to maintain call quality during network congestion.
Codec Preference	Specifies and prioritizes the supported audio and video codecs (e.g., PCMU, PCMA, Opus, G.722, H.264) used for WebRTC trunk calls.

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

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

Steps to configure DOD on the UCM630X:

1. To setup DOD go to UCM630xA Web GUI->**Extension/Trunk->VoIP Trunks** page.
2. Click on the "DOD" icon to access the DOD options for the selected SIP Trunk.
3. Click "Add DOD" to begin your DOD setup
4. Enter a SIP trunk DID number in the "DOD number" field. In this example, ABC company has a total of 4 DID numbers. Enter the phone number used by the CEO here.
5. When adding extensions, you can choose whether to "Enable Strip" according to your needs. If it is enabled, you can configure the number (0-64) that will be stripped from the extension number before being added to the DOD number. For example, if the entered digit is 2, and the DOD number for extension 4002 is 1122, then dialing out from 4002, 112202 will be used as the caller ID (DOD).
6. Select an extension from the "Available Extensions" list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO's extension. After making the selection, click on the button to move the extension(s) to the "Selected Extensions" list.

X

Create DOD

* DOD Number

DOD Name

Add Extension ⓘ ☒

Strip Extension ☐

* Strip ⓘ

☐ 126 Available

Search

- ☐ 1111
- ☐ 1200
- ☐ 1300
- ☐ 2222 "SDA 2222 SDA 2222"
- ☐ 3333 "SDA 3333 SDA 3333"
- ☐ 4001

<

>

☐ 0 Selected

Search

None

DOD Extension Selection

7. Click "Save" at the bottom.

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

VoIP Trunks > DOD: GSTR

ⓘ If DOD is configured on both outbound route and trunk, the outbound route DOD will take priority.

ⓘ 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.

☐	DOD	DOD Name	Extensions	Options
☐	0612345		1200 1300	
☐	0654321		4001 4444 5000	

Total: 2 1 10 / page Goto

Edit DOD

From this page users can:

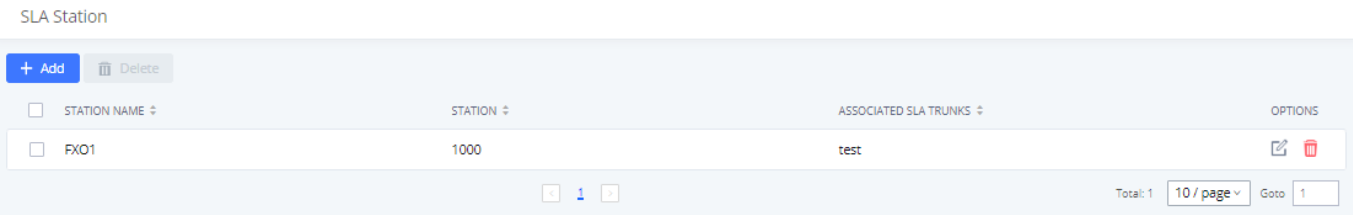
- Add Direct Outward Dialing (DOD) entries manually.
- Import DOD entries from CSV or XLSX files.
- Export DOD entries to CSV or XLSX files.
- Filter DOD entries by number or name.
- Select multiple DOD entries for bulk operations.
- Delete one or multiple selected DOD entries in batch.

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

- 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

Station Name	Configure a name to identify the SLA Station.
Station	Specify a SIP extension as a station that will be using SLA.
Available SLA Trunks	Existing Analog Trunks with SLA Mode enabled will be listed here.
Associated SLA Trunks	 Select a trunk for this SLA from the Available SLA Trunks list. Click on to arrange the order. If there are multiple trunks selected, when there are calls on those trunks at the same time, pressing the LINE key on the phone will pick up the call on the first trunk here.
SLA Station Options	
Ring Timeout	Configure the time (in seconds) to ring the station before the call is considered unanswered. No timeout is set by default. If set to 0, there will be no timeout.

Ring Delay	Configure the time (in seconds) for delay before ringing the station when a call first coming in on the shared line. No delay is set by default. If set to 0, there will be no delay.
Hold Access	This option defines the competence of the hold action for one particular trunk. If set to "open", any station could hold a call on that trunk or resume one held session; if set to "private", only the station that places the trunk call on hold could resume the session. The default setting is "open".

Sample Configuration

- 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:

test

Advanced Options

SLA Mode:

☒

Enable SLA Mode for Analog Trunk

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

Analog Trunks

Call Progress Tone File List

+ Add

TRUNKS	DISABLE	TRUNK MODE	ANALOG PORTS	OPTIONS
test	no	sla	1	 

1

Total: 110 / pageGoto1

Analog Trunk with SLA Mode Enabled

- 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
☐ FX01	1000	test	 

1

Total: 110 / pageGoto1

SLA Example SLA Station

- 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.
- 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_fx01	1005_fx01

SLA Example MPK Configuration

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

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

When the extension is in idle state, pressing the line key for this extension on the phone to off hook. Then dial the station's extension number, for example, dial 1002 on phone 1 (or dial 1005 on phone 2), to hear the dial tone. Then the users could dial external number for the outbound call.

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

When the extension is in idle state, pressing the MPK and users could dial external numbers directly.

- **Answering call using LINE key**

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

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

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

- **Hold/UnHold using BLF key**

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

CALL ROUTES

Outbound Routes

This section explains how to configure and manage outbound routes on the UCM630xA. Outbound routes control all external outgoing calls initiated by the UCM, regardless of trunk type (SIP, Analog, or Digital).

Configuring Outbound Routes

An outbound route in the UCM630xA links a dial pattern to a trunk, allowing different call types to use different trunks. For example:

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

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

To manage outbound routes:

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

</

Outbound Routes Overview Page

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

On the UCM630xA, route selection is determined by the Outgoing Routing Priority feature, which can prioritize routes by either list order or pattern accuracy. For detailed configuration, see the [Outgoing Routing Priority](#) section in this guide.

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

Option	Description
General	
Outbound Rule Name	Configure the name of the calling rule (e.g., local, long_distance, etc.). Letters, digits, _ and - are allowed.
Outbound Number Matching Pattern	All patterns are prefixed by the "_" character, but please do not enter more than one "_" at the beginning. All patterns can add comments, such as "_pattern /* comment */". In patterns, some characters have special meanings: [12345-9]: Any digit in the brackets (1,2,3,4,5,6,7,8,9 allowed). N: Any digit from 2-9. .: Wildcard, matching one or more characters. !: Wildcard, matching zero or more characters immediately. X: Any digit from 0-9. Z: Any digit from 1-9. -: Hyphen connects characters and is ignored. []: Containing special characters ([x], [n], [z]) represent letters x, n, z.
Auto Record	If enabled, calls using this route will automatically be recorded.
Local Country Code	If your local country code is affected by the outbound blacklist, enter it here to bypass the blacklist.
Outbound Route CID	Sets the Caller ID for this outbound route. Format must be "name<number>", "<number>", or "number". This CID is ignored if a DOD is configured. Note: This field does not apply to analog trunks.
Caller ID Manipulation	Enables Caller ID manipulation for this outbound rule. When enabled, the UCM applies the configured Strip/Prepend rules to calls using this route. The transformation is applied to both the SIP From header and the Remote-Party-ID (RPID) header. Example: A forwarded caller ID of 0123456789 with a strip of 1 and prepend of +972 results in +972123456789 in both From and RPID headers.
Caller ID Mode	Determines which Caller ID numbers the transformation applies to: Original CID: Transform only the forwarded caller's number. The UCM must have "Keep Original CID" enabled on the trunk for forwarded calls. All: Apply transformations to every outbound number on this route. Default: "Original CID".
Strip	Specifies the number of leading characters to remove from the Caller ID before sending the call out. Only numeric values (0-2) are allowed.
Prepend	Defines characters to add in front of the Caller ID after stripping. Supports 0-20 characters (Digits, Letters, + - * # only).

Diversion ID Manipulation	Enables transformation rules (strip and prepend) specifically applied to the SIP Diversion header number without altering the main Outbound Caller ID.
Strip	Specifies the number of leading characters to remove from the Diversion header number (0-2 characters, digits only).
Prepend	Defines characters to add in front of the Diversion header number after stripping (0-20 characters, allows digits, letters, and + - * #).
Don't Call Me Blocklist	If enabled, outgoing calls will first be checked against the "Don't Call Me" database. If the called number is in the database, the call will be blocked.
Disable This Route	Disables the outbound route. When disabled, the route will not take effect, but its settings remain stored in the UCM.
Outbound Permission	
Password Settings	Configures the authentication method for this outbound route: Password: The configured password will be used. PIN Groups: The PIN number related to the configured PIN Group will be used. Default: "Password".
Password	Configure the password for users to use this rule when making outbound calls.
PIN Groups	Select a PIN Group.
PIN Groups with Privilege Level	If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied.
Privilege Level	Select the privilege level for the outbound rule: Internal: The lowest level required. All users can use this rule. Local: Users with Local, National, or International levels can use this rule. National: Users with National or International levels can use this rule. International: The highest level required. Only users with the international level can use this rule. Disable: Default setting. Only the matched source caller ID will be allowed to use this outbound route. Note: Please be aware of potential security risks when using the "Internal" level.
Enable Source Caller ID Allowlist	When enabled, users can specify extensions allowed to use this outbound route. "Privilege Level" is automatically disabled if enabled. Select available extensions/extension groups from the list. Custom Dynamic Route: Define the pattern for the source caller ID (prefixed with "_", using pattern characters X, Z, N, ., !).
Call Duration Limit	Enable to configure the maximum duration for calls using this outbound route.
Per-Call Duration Limit	Enable to configure the maximum duration of each individual call using this outbound route. Once reached, the call is terminated.
Maximum Call Duration (s)	Configure the maximum duration of the call (in seconds). Default is 0 (no limit).
Warning Time (s)	Configure the warning time before call termination. A warning tone is played when x seconds remain.
Warning Repeat Interval (s)	Configure the repeat interval for the warning tone after the first warning.
Total Call Duration Limit	Enables setting a maximum cumulative call duration for this outbound route within a specified period.
Period	Configures the cumulative period for total outgoing call duration: Monthly: Cycle is one calendar month. Quarterly: Cycle is three months. Default: "Monthly".
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period (in minutes).
Main Trunk	
Trunk	Select the main trunk for this outbound rule.
Strip	Specify the number of digits to strip from the beginning of the dialed string before placing the call.

Prepend	Specify digits to prepend to the dialed number after stripping.
Failover Trunk	
Failover Trunk	Configures alternate trunks (up to 10) to route calls when the primary trunk is busy or down.
Strip	Specify the number of digits to strip from the dialed string for the failover trunk.
Prepend	Specify digits to prepend before placing the call via the failover trunk.
Time Condition	
Time Condition Mode	Selects the trunk routing behavior during time conditions: Use Main Trunk or Failover Trunk: Use the main trunk during configured time conditions; fall back to failover trunk if unavailable. Use Specific Trunks: Use specific trunks during configured time conditions using main trunk strip/prepend rules.

Failover Trunk Toggles

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

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

CancelSave

No-Failover Response Codes

6 itemsAvailable

Search

☐ 403

☐ 404

☐ 408

☐ 480

☐ 503

☐ 603

<

>

↑

↓

1 itemSelected

Search

☐ 486

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

No Failover Response Codes

If a call receives the selected response 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. A failover trunk can be set up to be used when the primary trunk fails. Note: This panel only manages individual outgoing calling rules.

AddDeleteScheduled SyncOutbound BlocklistPIN GroupsFailover Trunk TogglesCarrierImportExport

All LevelsQ Name/Outbound Number Matc...

Priority	Name	Outbound Number Matching Pattern	Privilege Level	Total Time for Outbound Calls (m)	Options
1	OUT_LCR	_06xxxxxxxx	Internal	Unlimited	     
2	OUT_MTEL_Code	_333#06xxxxxxxx	Internal	Unlimited	     
3	OUT_UCMB	_1x.	Internal	Unlimited	     

Total: 3<1>10 / pageGoto

Outbound Routes Page

Outbound Routes > DOD: OUT_LCR

Item is saved successfully. Please click Apply Changes to take effect.

If DOD is configured on both outbound route and trunk, the outbound route DOD will take priority.

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 DODDeleteImportExportFilter

DOD	DOD Name	Extensions	Options
DOD1	1234	1000 1001 1002	 

Total: 1<1>10 / pageGoto

DOD for First Outbound Route

Outbound Routes > DOD: OUT_UCMB

If DOD is configured on both outbound route and trunk, the outbound route DOD will take priority.

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 DODDeleteImportExportFilter

DOD	DOD Name	Extensions	Options
DOD2	5678	1004 1111 1200	 

Total: 1<1>10 / pageGoto

DOD for Second 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.

The blacklist (based on CalleeID) 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

Q Please enter blacklist number or

☐	CONTINENT	COUNTRY	BLACKLIST RULE	OPTIONS
No Data				

Country Codes

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

Import

Blacklist File:

Choose File to Upload

Cancel

Upload

Blacklist ImportExport

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**.

Outbound Routes > Outbound Blacklist

Blacklist Manage

Integrate Don't Call Me Blacklist

Integrate Don't Call Me Blacklist

☒

* Authorization Token

This field is required

* Query Timeout Time (s)

This field is required

Query Timeout Handling

Allow Dialing

Test Connection

Start

Cancel

Save

Don't Call Me Database Integration

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

Scheduled Sync

The 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

Scheduled Sync	Enable the Scheduled Sync feature
Server Address	Enter the TFTP server address. For example, "192.168.1.2:69".
File Name	Specify the file name
Sync Time	Enter the sync time (24hr format). Valid range is 0-23.

Sync Frequency	Create new sync every x day(s). The valid range is 1 to 30.
----------------	---

PIN Groups

The 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**.

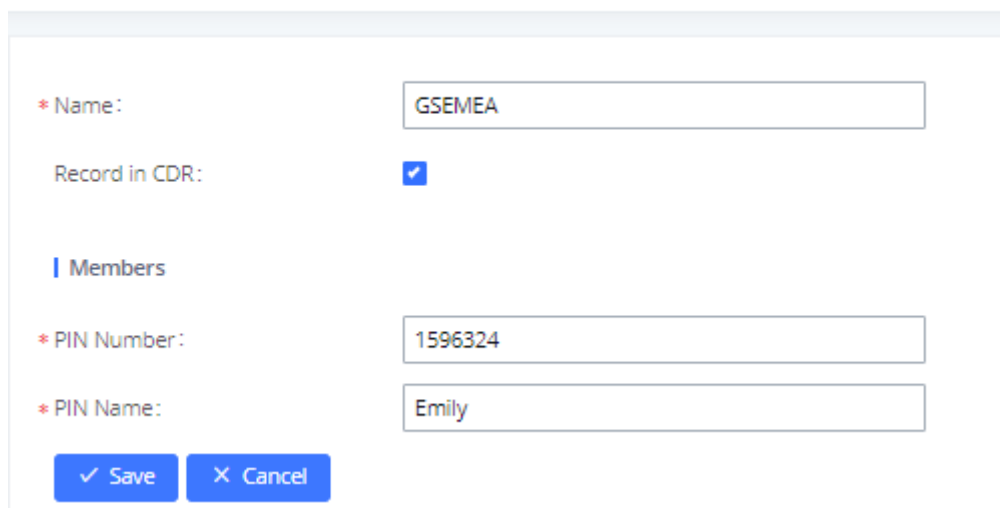
Outbound Routes/PIN Group

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

Once user click on

the following figure shows to configure the new PIN.

Create New PIN Group



* Name:

Record in CDR: ☒

Members

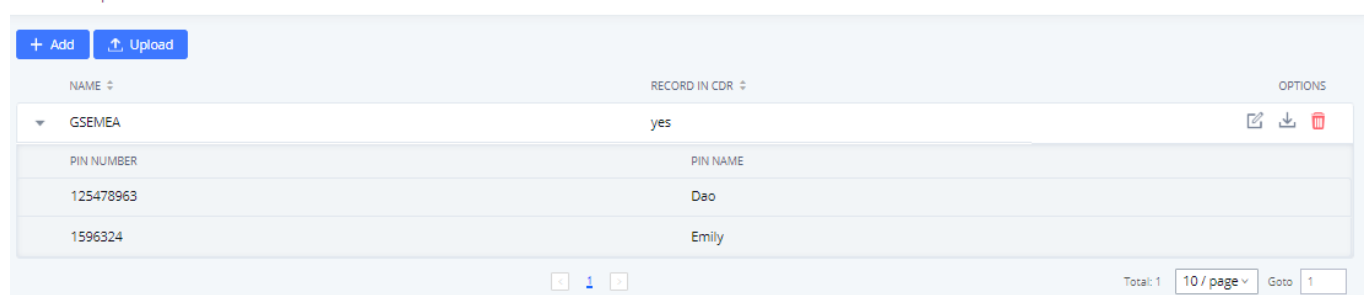
* PIN Number:

* PIN Name:

Create New PIN Group

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

< PIN Groups



NAME	RECORD IN CDR	OPTIONS
GSEMEA	yes	
PIN NUMBER	PIN NAME	
125478963	Deo	
1596324	Emily	

Total: 1 10 / page Goto 1

PIN Members

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:

GStest

Pattern:

_9.

PIN Groups:

GSEMEA

Password:

Disable This Route:

Privilege Level:

Disable

PIN Groups with Privilege Level:

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

-

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

- 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

1

Total: 1

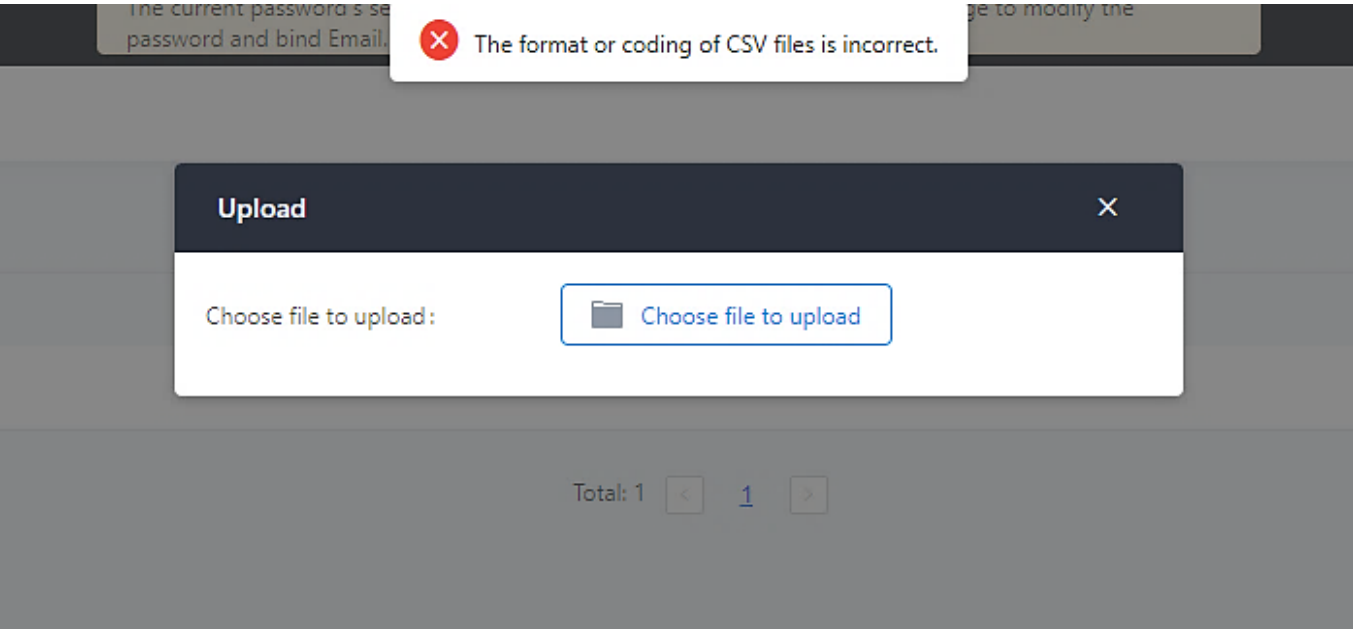
10 / page

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

Clipboard Font Alignment Number				
A1 ALPHA				
	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

Carrier

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

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

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. 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 Blocklist

PIN Groups

Failover Trunk Toggles

Carrier

Import

Export

All Levels

Q Name/Outbound Numbe...

ID	Name	Outbound Number Matching Pattern	Privilege Level	Options
1	Rule_1	_+212xxxxxxxx _+213xxxxxxxx _X.	Internal	

Total: 1

< 1 >

10 / page

Goto

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

Outbound Routes > Carrier

If "Least Cost Routing" is selected as an outbound route main trunk, the destination number for the outgoing call will be matched according to the table below to find the carrier, trunk, and rate rules that are available and identify the trunk with the lowest cost. If rates are the same, use the preferred carrier.

Add

Global Billing Unit

All

Q Carrier

Priority	LCR	Carrier	Number of Trunks	Options
1	Supported	CarrierA	1	
2	Supported	CarrierABC	1	

Total: 2

< 1 >

10 / page

Goto

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

Carrier

Please select a provider

2 - 64 characters, characters " ' = # & \$ | , ; \ > < are not allowed.

Trunk

0

Available

Search

Q

None

0

Selected

Search

Q

None

<

>

⌵

⌴

⌶

⌷

LCR supported

☒

Carrier Rates

Add

Delete

Import

Export

Match Prefix/Rate

Q

☐ Match Prefix

Rate

Expiration Date

Options

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

Add Rate

×

Match Prefix

1 - 12 characters, Only numbers and special characters + can be entered

Rate

1 - 12 characters, Please enter a digit or a decimal.

Expiration Date

Start Time

-

End Time

Cancel

Save

Add Call Rate

Parameter Name	Description
Match Prefix	If the prefix entered is matched, this rate will apply to this call.
Rate	Enter the rate of the call.

Outgoing routing priority policy



Priority Strategy

Accuracy First

List Sorting Priority

Matches outgoing routes from top to bottom by list priority.
For example: For calls that start with 137, because the priority of _1 is above _137, the outgoing call is routed through the route _1.

Priority	Name	Outbound Number Matching Pattern	Privilege Level
1	...	_1	...
2	...	_137	...

Accuracy First

The outgoing route with more specific number matching is preferred. For example: For calls starting with 137, _137 is preferred because it is more specific than _1.

ID	Name	Outbound Number Matching Pattern	Privilege Level
1	...	_1	...
2	...	_137	...

Cancel

OK

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

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

Inbound Routes

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

Configuring Inbound Routes

To manage inbound routes:

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

Inbound Routes									
Add Delete Blocklist Set Global Inbound Mode 3rd Party Database Search Import Export Filter SIP Trunks -- Route22									
Inbound Route Name	Inbound Number Matching Pattern	Source Caller ID Pattern	Inbound Mode	Inbound Mode Feature Code	Time Condition	Time	Destination	Options	
☐ IN22	_06xxxxxxxx	No Limit	Default Mode		--	Default	Default Mode trip 6	By DID -- S	
Total: 1 1 10 / page Goto									

Inbound Routes Overview Page

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

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

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

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

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

Inbound Route: Prepend 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

Default Mode

Mode 1

* Default Destination :

By DID

Strip :

8

Prepend :

2

Inbound Route feature Prepend

Inbound Route: Multiple Mode

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

Inbound 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, calls coming into the inbound routes will be routed to the default destination.

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

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

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

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

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

Default Mode

BLF Subscription Number

777

Inbound Mode

Toggle Feature Code

Name

Prompt

Default Mode

*61

Mode 1

*62

Name

None

Add Audio

Mode 2

*63

Name

None

Add Audio

Mode 3

*64

Name

None

Add Audio

Mode 4

*69

Name

None

Add Audio

Mode 5

*70

Name

None

Add Audio

Cancel

Save

Add

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

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

Inbound Route: Custom Inbound Mode

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

Inbound 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

- 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

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

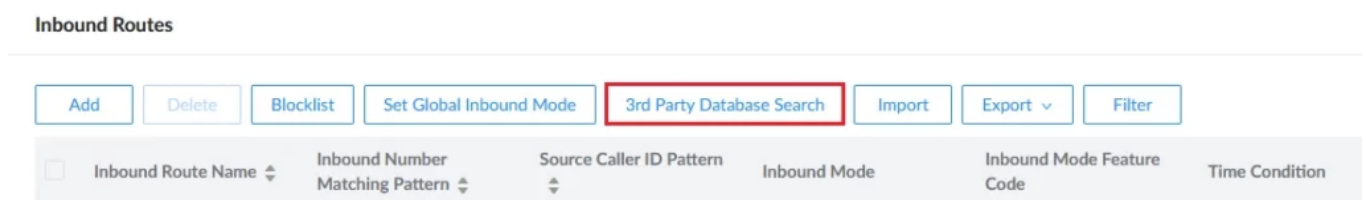


Inbound Mode Mode 1

Inbound Routes: 3rd Party Database Search

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

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



Inbound Routes Page

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

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

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



3rd Party Database Search Feature for Inbound Routes

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

Field	Description
-------	-------------

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

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

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

The inbound caller number is dynamically substituted at call time.

Inbound Route: Import/Export Inbound Route

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

Inbound Routes								
+ Add Blacklist Set Global Inbound Mode Import Export Filter								
INBOUND ROUTE NAME	PATTERN	CALLERID PATTERN	INBOUND MODE	INBOUND MODE SUFFIX	TIME CONDITION	TIME	TYPE	DESTINATION
No Data								

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.

Blacklist

CancelSave

The blacklist (by CallerID) is used for all inbound routes.

Warning: Too many blacklist entries will lower overall system performance.

Blacklist Enable: ☒

Blacklist Manage

* Add Blacklist Number:

Scope Of Action:

All ×

Add

Blacklist list

ClearDeleteImportExport

Please enter blacklist number

☐	NUMBER ↕	INBOUND ROUTE INDEX	OPTIONS
☐	Anonymous	All	

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.

Paste		Format Painter		B I U		Font	
Clipboard							
F8		X		✓		fx	
	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**.

WHATSAPP TRUNK

The WhatsApp Trunk feature allows the UCM Series to integrate directly with Meta WhatsApp Business accounts as a specialized SIP trunk. Once configured, businesses can handle incoming voice calls initiated by customers from WhatsApp, as well as make outbound WhatsApp voice calls directly to authorized clients through Wave applications or registered endpoints.

WhatsApp Trunk			
Add			
Trunk Name	Trunk Status	Phone Number	Options
whatsapp_123	Available	15556720635	
Total: 1			10 / page

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

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

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

WhatsApp Trunk > Create New WhatsApp Trunk

*Trunk Name

Whatsapp_Account

2-64 letters, numbers, and Chinese characters. Special characters ' ' * \ = & \$ | < > , ; are not supported.

Disable This Trunk

☐

Auto Record

☐

*Phone Number

1234568456

1 - 64 characters, supports letters, numbers, and special characters + * # - _ . \$ %

*Phone Number ID

12255551002000

Supports 1-64 numbers and special characters +

*Token

.....

1 - 256 characters, supports letters, numbers, and special characters - + _ . * #

Learn more about WhatsApp Trunk Configuration with the [WhatsApp Trunk Configuration Guide](#)

Cancel

Save

Configure the parameters as described in the table below:

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

Inbound and Outbound Whatsapp Routing

Inbound Routing (Manual)

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

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

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

Outbound Routing (Automatic Provisioning)

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

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

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

FAX SERVER

The UCM6300A series supports T.30/T.38Fax and Fax Pass-through. It can convert the received Fax to PDF format and send it to the configured Email address. Fax/T.38 settings can be accessed via Web **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:

14400

▼

• Minimum Transfer Rate:

2400

▼

• Max Concurrent Sending Fax:

Single

▼

• Fax Queue Length:

6

▼

User Information in Fax Header:

☐

Fax Header Information:

Default Email Address:

Email Template

Send PDF Files Only:

☐

Enable Fax Resend:

☐

Max Resend Attempts:

5

Fax Resend Frequency:

50

Fax Settings

FAX/T.38Settings

Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is "Yes".
Maximum Transfer Rate	Configure the maximum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14400. The default setting is 14400.
Minimum Transfer Rate	Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14000. The default setting is 2400.
Max Concurrent Sending Fax	Configure the concurrent fax that can be sent by UCM6300A. Two modes "Only" and "More" are supported. Only Under this mode, the UCM6300A allows only single user to send fax at a time. More Under this mode, the UCM6300A supports multiple concurrent fax sending by the users. By default, this option is set to "only".
Fax Queue Length	Configure the maximum length of Fax Queue from 6 to 10. The default setting is 6.

User Information in Fax Header	If enabled this this will give users the option to send a special header in SIP fax messages.
Fax Header Information	Adds fax header into the fax file.
Default Email Address	Configure the Email address to send the received Fax to if user's Email address cannot be found. Note: The extension's Email address or the Fax's default Email address needs to be configured in order to receive Fax from Email. If neither of them is configured, Fax will not be received from Email.
Template Variables	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users. The template variables are: \${CALLERIDNUM} : Caller ID Number \${CALLERIDNAME} : Caller ID Name \${RECEIVEEXTEN} : The extension to receive the Fax \${FAXPAGES} : Number of pages in the Fax \${VM_DATE} : The date and time when the Fax is received
Send PDF Files Only	If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.
Enable Fax Resend	Enables the fax resend option which allow the UCM to keep attempting to send faxes up to a specified amount of times. Additionally, if a fax still fails to send, a Resend button will appear in the File Send Progress list in OtherFeatures→Fax Sending to allow manual resending.
Max Resend Attempts	Configures the maximum attempts number to resend the fax. Default value is set to 5.
Fax Resend Frequency	Configures the Fax Resend Frequency. Default value is set to 50.

Receiving Fax

Example Configuration to Receive Fax from PSTN Line

The following instructions describe how to use the 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".

* FXO Port: ☒ 1 ☐ 2

* Trunk Name: FAX

Advanced Options

SLA Mode: ☐Enable Polarity Reversal: ☐Current Disconnect
Threshold (ms): ☒ 200

* Ring Timeout: 8000

* 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

Analog Station: FXS 1

CallerID Number:

* Privilege: Internal

Voicemail: Local Voicemail

* Voicemail Password: 96902350

Skip Voicemail Password Verification: ☐

Send Voicemail Email Notification: Default

Attach Voicemail to Email: Default

Keep Voicemail after Emailing: Default

Disable This Extension: ☐

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: ☐

Use "*" as SEND: ☒

* RX Gain: 0dB

* TX Gain: 0dB

* MIN RX Flash (ms): 200

* MAX RX Flash: 1250

Enable Polarity Reversal: ☒

* Echo Cancellation: ON

3-way Calling: ☒

* Send CallerID After: 1

* Fax Mode: Fax Gateway

Fax to Email: Yes

None
Fax Detection
Fax Gateway

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

Inbound Route Name:

* Pattern: S

CallerID Pattern:

Disable This Route: ☐

Seamless Transfer

Whitelist:

Alert-info: None

Ringback Tone: None

Fax Detection: ☐

Auto Record: ☐

Prepend Trunk Name: ☐

Set CallerID Info: ☐

Enable Route-Level

Inbound Mode:

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 New Fax Extension

* Extension:

7200

* Name:

Fax

* Email Address:

fax@domain.local

[Add Email Address](#)

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.

Create New Inbound Rule

CancelSave

* 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:

Fax

Fax

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.

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	
☐	VFAX-7200-20210125-112246-1611570166.49.pdf	2021-01-25 11:22:46 UTC+01:00	1.49 KB		
☐	VFAX-7200-20210125-112246-1611570166.49.tiff	2021-01-25 11:22:46 UTC+01:00	5.69 KB		

List of Fax Files

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:	0123456789
Fax File:	test.pdf
Send	

File Send Progress					
Delete		Clear		External Fax Number	

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:	Choose File to Upload
Send	

File Send Progress						
Delete		Clear		External Fax Number		
☐	NAME	DATE	SENDER	EXTERNAL FAX NUMBER	CURRENT PROGRESS	OPTIONS
☐	test.pdf	2021-01-25 11:29:19 UTC+01:00	admin	0123456789	Sending... 5%	

Fax Send Progress

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**→**Multimedia 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

Extension	The number to dial to reach the meeting room.
Meeting Name	The name of the meeting room.
Privilege	Select the permission level for outgoing calls.
Allow User Invite	If enabled, participants can invite other users to the meeting.
Allowed to Override Host Mute	If enabled, participants will be able to unmute themselves if they have been muted by the host.
Auto Record	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.Note: When this option has been enabled the meeting host cannot stop the recording of the meeting.
Room Password	If meeting room password is configured, meeting participants will need to enter a password to enter the room. Scheduling meetings will not be supported for this room.

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

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

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.

The Meeting Schedule Parameters are described below:

General	
Meeting Subject	Configure the name of the scheduled meeting. Letters, digits, some special characters are also supported. The characters ` % # ? < > @ \$ ^ ~ are not allowed.

Public Meeting Room	Choose which room to have this scheduled meeting.
Time	Configure the meeting date and time.
Time Zone	Select the meeting time zone.
Repeat	Choose when to repeat a scheduled meeting. No Repeat Every Day Weekly Monthly Custom: it specifies how often the meeting is repeated per days/weeks. E.g., every 3 days/weeks.
End Repeat	This option appears when a reccurent schedule is configured.Configure the date when the recurrence stops.
Password	Configure the meeting's login password.
Meeting Agenda	The description of this scheduled meeting.
Attendee	
Host	Configure Host.
Host Password	Configure the Host Password.Note: It is randomly generated when first creating a new meeting Schedule.
Invitees	Local extensions, remote extensions, and special extensions are supported.
Allow User Invite	If enabled, participants will be able to invite others to the meeting by pressing 1 on their keypad or by clicking the Participants->Invite option.
Advanced	
Email Reminder (m)	Check to enable scheduled meeting email reminder. Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-120. 60 is the default value.Note: After editing the time of a single recurrence of a scheduled meeting, a cancellation email will be sent out followed by a meeting update email.
Call Participant	If enabled, the invited participants will be called upon meeting start time.
Allowed to Override Host Mute	If enabled, participants will be able to unmute themselves if they have been muted by the host.
Play Joining/Leaving Meeting Announcement	Configure whether the join/leave meeting prompt is played when participants join or leave.
Auto Record	Meeting audio can be automatically recorded. These recordings can be found under the Meeting Recordings page. None: The meeting audio will not be automatically recorded. Record Audio: Record only the meeting audio. Note: Please note that UCM63XX Audio Series doesn't support Screen Sharing, Whiteboard, or PDF file sharing.
Sync Google Calendar	Select this option to sync scheduled meeting with Google Calendar.Note: Google Service Setting OAuth2.0 must be configured on the IPPBX. Please refer to section [Google Service Settings Support].
Support AI transcription	Choose whether to support AI transcription for the scheduled meeting. This parameter cannot be controlled if the AI meeting transcription and summary is disabled in the general AI Settings.
Language	Specifies the language recognition behavior used for AI transcription. The options are: Automatic Recognition: Automatically detects the spoken language during the meeting. This is recommended when multiple languages are expected, though recognition accuracy may vary. Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy. Note: This setting controls only the transcription language for this scheduled meeting. It does not apply to the general AI Conference Transcription and Summary feature.
Automatic AI Transcription	Once enabled, meeting audio will be automatically transcribed in real time once the meeting starts. A summary will also be generated after the meeting.

Allow Participants to View Summary	When enabled, meeting summaries generated by AI are made accessible to all attendees via meeting reports, rather than restricting access exclusively to the host or organizer.
------------------------------------	--

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

Meeting

Room
Meeting
Google Service Settings
Meeting Recordings

Pending MeetingMeeting History

Schedule Meeting

Meeting Su...
Search

MEETING SUBJECT	MEETING ROOM	MEETING OWNER	START TIME	MEETING DURATION	REPEAT	OPTIONS
No Data						

Meeting Schedule

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

Unstarted MeetingHistorical Meeting

Schedule Meeting

CONFERENCE SUBJECT	CONFERENCE ROOM	CONFERENCE OWNER	START TIME	MEETING DURATION	REPEAT	OPTIONS
test Ongoing	6301	lili	Today 15:50 Etc/GMT-1	00:15:00	No Repeat	

<1>

Total: 110 / 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	

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

Meeting

Room

Meeting

Google Service Settings

Meeting Recordings

Download

Download All

Delete

Clear

Local

2022-05

	NAME	ROOM	DATE	SIZE	OPTIONS
No Data					

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.

Onsite Meeting

Scheduled Meetings Room Management Equipment Address Management

Scheduled Meetings Pending Meeting Meeting History

Time: 2022-11-15 Office Building: All Equipment: All Participant Capacity: All Status: All

Meeting_Room_1 Idle 5, Main Office projector

< 1 > Total: 1 10 / page Goto 1

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

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 Starting soon	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.



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-33f96e39-8ff4-4bf5-9821-8bf1ba35bbbba.ics [Download](#)

Onsite Meeting Email Invitation

IVR

Basic Settings

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.

IVR > Create New IVR

[Basic Settings](#)[Key Pressing Events](#)

General

* Name

* Extension

Auto Record ☐

Prompt Language

* Prompt [Upload Audio File](#)

[Add Prompt](#) 

IVR Webhook

IVR Webhook ☐

Dialed Number

Dial Other Extensions ☐ All ☒ Extension

☐ External Number

☐ Multimedia Meeting

☐ Call Queue ☐ Ring Group

☐ Paging/Intercom Groups

☐ Voicemail Groups

[Cancel](#)[Save](#)[Create New IVR](#)

IVR Configuration Parameters

General	
Name	Configure the name of the IVR. Letters, digits, _ and - are allowed.
Extension	Enter the extension number for users to access the IVR.
Auto Record	If enabled, calls to this IVR will automatically be recorded.
Prompt Language	Select voice prompt language for this extension. If set to "Default", the global setting for Voice Prompt will be used.?This configuration only applies to the system prompt, and does not affect the language of custom prompt.
Prompt	Initial tone that plays when the user enters the IVR.
IVR Webhook	

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

Alert Info	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.
Timeout	When exceeding the number of defined answer timeout, IVR will enter the configured event when timeout. If not configured, then it will Hangup.
Invalid	Configure the destination when the Invalid Repeat Loop is done.
Time Condition	Configure the time condition for each key press event, so that it goes to the corresponding destination within a specified time.

Key Pressing Events

Standard Key Event

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

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

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

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

Option	Description
Key Event Type	Select Standard to configure single-key DTMF events (0-9, *, #). This mode supports time-based routing per key.
Key (0-9, *, #)	Each section corresponds to a specific DTMF key. Configuration under a key defines how calls are routed when that key is pressed.
Destination	Select the destination type and target for the key event. Supported destinations include: Extension Meeting Voicemail Voicemail Group IVR (Maximum 64 nested IVRs) Ring Group Queues Paging/Intercom Group Fax Custom Prompt Hang-up DISA Dial By Name External Number Callback Announcement SMS (Sends a pre-configured automated SMS template to the caller) Time Condition Routing

Time Condition	Assign a time condition to each destination entry. The IVR evaluates time conditions in order and routes the call to the first matching rule. Common options include All Time, Office Time, Out of Office Time, Holiday, and Specific Time. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for the same key, or the (-) icon to remove an existing rule.
Timeout	Configures the destination when the Timeout Repeat Loop is done. Note: Multiple destination entries with different time conditions (up to five) can be configured for this option.
Invalid	Configures the destination when the Invalid Repeat Loop is done. Note: Multiple destination entries with different time conditions (up to five) can be configured for this option.
End Key	Configures whether the caller can press a designated End Key to complete their DTMF input immediately and be directed to the target destination. Options: Press the "#" key to end Press the "*" key to end Note: The configured End Key value must not conflict with key values defined in key pressing events to avoid recognition failure.

Custom Key Event

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

IVR > Create New IVR

Basic Settings **Key Pressing Events**

Key Event Type ☐ Standard ☒ Custom

Key Events

[Add](#) [Delete](#) [Clear](#)

☐ Key 123

☒ Destination Multimedia Meeting 6300 Time Condition All Time

Other Settings

Timeout Destination Custom Prompt goodbye Time Condition All Time

Invalid Destination Custom Prompt goodbye Time Condition All Time

Option

End Key ☒ ☐ Press the "*" key to end ☐ Press the "#" key to end

[Cancel](#) [Save](#)

This feature supports the following:

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

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

The following options are available for Custom Key Pressing Events:

Option	Description
Key Event Type	Select Custom to configure multi-digit DTMF key combinations. This mode supports time-based routing and advanced IVR logic.

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

VOICE PROMPTS

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.

Voice Prompt

Language Settings

Custom Prompt

Username Prompt

Add Voice Prompt Package

Upload

Voice Prompt Package List

LANGUAGE	OPTIONS
☒ English : en	
☐ 中文 : zh	

Cancel

Save

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.

Details



Voice Prompt Package List	Version (Remote/Local)	Size	Options
British English	1.10/-	4.3M	
Deutsch	1.12/-	4.66M	
English	1.16/1.16	6.4M	
Español	1.15/-	4.92M	
Español(Català)	1.9/-	3.2M	
Español(Español)	1.12/-	4.54M	
Ελληνικά	1.15/-	4.85M	
Français	1.15/-	4.51M	
Italiano	1.15/-	4.44M	
Nederlands	1.10/-	3.73M	
Polski	1.9/-	5.1M	

Voice Prompt Package List

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

Voice Prompt

[Language Settings](#)

[Custom Prompt](#)

[Username Prompt](#)

[Add Voice Prompt Package](#)

[Upload](#)

Voice Prompt Package List

LANGUAGE	OPTIONS
☐ English : en	
☐ 中文 : zh	
☒ British English : en_GB	

[Cancel](#)

[Save](#)

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.

Custom Prompt

Record New Custom Prompt

In the UCM630xA **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

WAV ▾

* Extension

1000 ▾

Cancel

Record

Record New Custom Prompt

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

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

Voice Prompt

Language Settings Custom Prompt Username Prompt

Uploaded prompt files cannot have the same name even if the file format is different.

Record Upload Download All Delete Clear

Name	Type	Format	Play	Options
☐ notification-beep-229154.wav	Audio	wav	🔊	📄 ⬇️ 🗑️

Total: 1 1 / page Goto:

Custom Prompt Page

Upload Custom Prompt

If the user has a pre-recorded IVR prompt file, click on "Upload" in Web GUI→PBX Settings→**Voice Prompt**→**Custom Prompt** page to upload the file to the 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 5MB.

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

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

Prompt successfully uploaded.

The uploaded file is an mp3 file. The system will convert it to a wav file.

☐ Keep Copy of MP3

Using MP3 files will result in better audio quality when using the paging/intercom feature with Grandstream GSC speakers.

OK

Tick "Keep Copy of MP3" to keep an mp3 copy of the file which can be diffused with certain GSC speakers. Diffusing the MP3 files result in a highr quality sound played by GCS speakers.

Download All Custom Prompt

On the 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

* File Name

prompt_20250203_150441

Cancel

Download

Download All Custom Prompt

The downloaded file will have a .tar extension.

Username Prompt

There are two ways to customize/set new username prompt:

Upload Username Prompt File from Web GUI

1. First, Users should have a pre-recorded file respecting the following format:
 - PCM encoded / 16 bits / 8000Hz mono.
 - In .tar/.tar.gz/.tgz format
 - File size under 30M.
 - Filename must be set as the extension number with 18 characters max. For example, the recorded file name 1000.wav will be used for extension 1000.
2. Go under web GUI **PBX Settings → Voice Prompt → Username Prompt** and click on **"Upload"** button.
3. Select the recorded file to upload it and press Save and Apply Settings.
 - Click on  to record again the username prompt.
 - Click on  to play recorded username prompt.
 - Select username prompts and press  to delete specific file or select multiple files for deletion using the button **"Delete"** .

Record Username via Voicemail Menu

The second option to record username is using voicemail menu, please follow below steps:

- Dial *98 to access the voicemail
- After entering the desired extension and voicemail password, dial "0" to enter the recordings menu and then "3" to record a name.

Another option is that each user can record their own name by following below steps:

- The user dials *97 to access his/her voicemail
- After entering the voicemail password, the user can press "0" to enter the recordings menu and then "3" to record his name.

Call Prompt Tones

SIP Trunk Prompt Tone

Prompt Tone Settings tab on the UCM helps users choose which prompt will be played by the UCM during call failure, the voice message responses can be set to be played for 4XX, 5XX, and 6XX call failures.

The following **default prompt names** and their associated messages are supported:

Prompt Name	Message Played
sip-trunk-out-busy	"All circuits are busy now. Please try again later."
sip-trunk-out-rejected	"The call was rejected by the server. Please try again later."
sip-trunk-out-server-error	"Server error. Please check your device."
sip-trunk-out-wrong-number	"Your call can't be completed as dialed. Please check the number and dial again."

general-failed	"Your call cannot be completed as dialed."
no-answer	"The number you dialed is not answering. Please try again later."
no-permission	"You are not allowed to dial this number."
user-busy	"The number you have dialed is busy. Please try again later."
wrong-number	"The number you dialed is incorrect. Please check the number and dial again."

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

Call Prompt Tones

[SIP Trunk Prompt Tone](#)

General Call Prompt Tones

Specify the tones to play for various SIP trunk call failure scenarios.

Reset All

Default All

400	sip-trunk-out-busy	401	sip-trunk-out-busy
402	sip-trunk-out-busy	403	sip-trunk-out-rejected
404	sip-trunk-out-wrong-nu...	405	sip-trunk-out-busy
406	sip-trunk-out-busy	407	sip-trunk-out-busy
408	sip-trunk-out-busy	410	sip-trunk-out-busy
413	sip-trunk-out-busy	414	sip-trunk-out-busy
415	sip-trunk-out-busy	416	sip-trunk-out-busy
420	sip-trunk-out-busy	421	sip-trunk-out-busy
423	sip-trunk-out-busy	480	sip-trunk-out-busy
481	sip-trunk-out-busy	482	sip-trunk-out-busy
483	sip-trunk-out-busy	484	sip-trunk-out-busy

Cancel

Save

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 Prompt Tones > General Call Prompt Tones** page as shown on the following figure:

Call Prompt Tones

SIP Trunk Prompt ToneGeneral Call Prompt Tones

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

Blocklist Outgoing Failure

no-remote

General Failed

general-failed

Call Waiting

Default Ringback Tone

Cancel

Save

General Call Propt Tones

Alert-info Prompt

The user can change upload the ringtone files which can be used with Alert-info to play various ringtones depending on the configured behaviour. In this setting, the user can view all the ringtones uploaded, play them, download them, or delete them. If the user wishes to upload new ringtones, he/she can click on "Upload" and choose the ringtone files to upload.

Alert-info Prompt

Uploaded greeting files cannot have the same name even if the file format is different.

Upload

Download All

Delete

☐	Name ↕	Type ↕	Format ↕	Options
☐	Ring-IVR.wav	Audio	wav	
☐	Ring-External.wav	Audio	wav	
☐	Ring-Queue.wav	Audio	wav	
☐	Ring-Extension.wav	Audio	wav	

Total: 4

<

1

>

10 / page

Goto

Alert info Prompt Ringtones

VOICEMAIL

Configure Voicemail

If voicemail is enabled for UCM630xA extensions, global voicemail configurations can be managed under **Basic Call Features -> Voicemail -> Voicemail**.

Voicemail

Voicemail

Voicemail Email Settings

Voicemail Groups

*Max Greeting Time (s) ⓘ	60
Dial "0" for Operator ⓘ	☐
Operator Type	Extension
Operator Extension ⓘ	None
*Max Messages Per Folder ⓘ	50
Max Message Length (m) ⓘ	15 minutes
Min Message Length (s) ⓘ	3 seconds
Announce Message Caller-ID ⓘ	☐
Announce Message Duration ⓘ	☐
Play Envelope ⓘ	☒
Play Most Recent First ⓘ	☐
Allow User Review ⓘ	☐
Voicemail Remote Access	☐

The table below describes the global voicemail configuration parameters:

Option	Description
Max Greeting Time (s)	Configure the maximum duration (in seconds) for voicemail greetings (range: 60-600, default: 60).
Dial '0' For Operator	If enabled, callers pressing 0 during voicemail exit the application to connect to the designated operator destination.
Operator Type	Select the operator destination type (Extension or Ring Group).
Operator Extension	Select the operator extension or ring group called when callers dial 0.
Max Messages Per Folder	Configures the maximum allowed messages per voicemail folder (range: 10-1000, default: 50).
Max Message Length (m)	Select the maximum recording duration for a voicemail message (1, 2, 5, 15, 30 minutes, or Unlimited; default: 15 minutes). Note: Silence and noise duration are excluded from message time.
Min Message Length (s)	Configures the minimum recording length required to save a message (No Minimum, 1, 2, 3, 4, 5 seconds). Messages shorter than this value are discarded. Note: Silence and noise duration are excluded from message length.
Announce Message Caller-ID	If enabled, announces the caller ID of the sender at the start of message playback (Default: No).
Announce Message Duration	If enabled, announces the message duration before playback (Default: No).
Play Envelope	If enabled, plays timestamp and sender information before message playback.
Play Most Recent First	If enabled, plays the newest voicemail messages first.
Allow User Review	If enabled, callers can review and re-record their message before submitting.

Voicemail Remote Access	If enabled, external callers arriving via DID are prompted with two choices: Press 1: Leave a message for the called extension. Press 2: Access the remote voicemail management system (requires extension number and PIN). Note: Applies strictly to inbound DID calls (Default: Disabled).
Forward Voicemail to Peered UCMs	Enables forwarding voicemail messages to remote extensions on peered UCM trunks (Default: Disabled).
Voicemail Password	Sets the default voicemail PIN used when extensions are reset. Numeric digits only (minimum 4 digits). Sequential or repetitive numbers (e.g., 1234, 1111) are rejected.
Audio Encoding Format	Selects the audio encoding codec used for voicemail file storage: GSM: Encodes audio using the GSM codec, producing compressed .WAV (uppercase) files to save disk space. PCM: Encodes audio using uncompressed PCM codec, producing high-quality .wav (lowercase) files (uses significantly more storage space).
Username Prompt	Configure or upload a custom username prompt file.

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

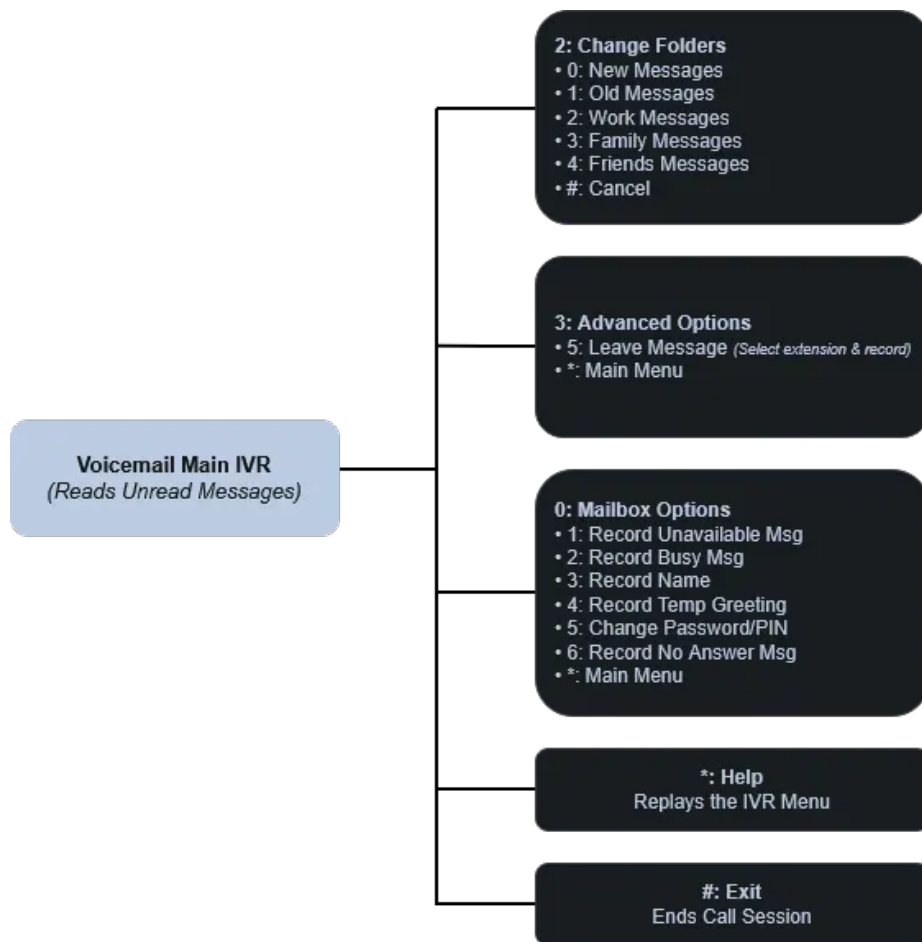
Access Voicemail

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

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

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

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



Leaving Voicemail

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

In case if the caller is calling from an internal extension, they will be directly forwarded to the extension's voicemail box. But if the caller is calling from outside the system and the incoming call is routed by DID to the destination extension, then the caller will be prompted with the choice to either 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.

Send Voicemail to Email	If enabled, voicemail will be sent to the user's email address. Note: SMTP server must be configured to use this option.
Keep Voicemail after Emailing	Enable this option if you want to keep recording files after the Email is sent. The default setting is Enable.

Email Template	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending to the user. The template variables are: \t: TAB \${VM_NAME}: Recipient's first name and last name \${VM_DUR}: The duration of the voicemail message \${VM_MAILBOX}: The recipient's extension \${VM_CALLERID}: The caller ID of the person who has left the message \${VM_MSGNUM}: The number of messages in the mailbox \${VM_DATE}: The date and time when the message is left
----------------	---

Voicemail Email Settings

Voicemail Email Settings

Send Voicemail to Email:

☒

Keep Voicemail after

☒

Emailing:

Email Template:

Email Template

Voicemail Email Settings

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

Configure Voicemail Group

The UCM630xA supports voicemail groups, allowing all member extensions assigned to a group to receive voicemail messages left for the group extension. Voicemail groups can be configured under **Basic Call Features -> Voicemail -> Voicemail Group**. Click on **Add** to configure a new group.

Voicemail > Create New Voicemail Groups

* Extension

* Name

* Method ☒ Forwarded ☐ Shared

Voicemail Password

Email Address

Shared Voicemail Status ☐

Members

☐ 498 Available

- ☐ 1000 " "
- ☐ 1003 "Johnny Doe"
- ☐ 1004 "John Marston"
- ☐ 1005 "Abigail Roberts"
- ☐ 1006 "Mary-Beth Gaskill"
- ☐ 1007 "Hosea Matthews"

☐ 0 Selected

None

Voicemail prompt will be played when user enters voicemail. Priority: Temporary Prompt > Unavailable Prompt > Name Prompt
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.

Name Prompt

Temporary Prompt

Unavailable Prompt

Voicemail Group

When creating or editing a Voicemail Group, administrators can configure the parameters detailed in the table below:

Parameter	Description
Extension	Configure a unique extension number for the voicemail group.
Name	Configure a label to identify the voicemail group.
Method	Select the distribution method for incoming voicemails: Forwarded: Copies of voicemails left for the group extension are distributed to each member extension's individual mailbox. Shared: Voicemails are saved in a single shared mailbox accessible by all group members.
Voicemail Password	Configure the password required to access the voicemail group mailbox.
Email Address	Configure the email address to receive voicemail notification emails and audio attachments when a message is left.
Shared Voicemail Status	Enable this option to sync message read/unread status across all members in shared voicemail mode.
Members	Select extensions from the Available list and move them to the Selected list to add them as group members. Up to 150 extensions can be added to a single voicemail group.
Name Prompt	Upload or select the audio prompt for the voicemail group name. Click Add Audio to choose an existing file, upload a local audio file, or generate audio using Text-to-Speech (TTS). Note: Audio priority is Temporary Prompt > Unavailable Prompt > Name Prompt. Files must be under 30 MB (.mp3, .wav, .ulaw, .alaw, .gsm; WAV files must be 16-bit mono 8000Hz PCM).
Temporary Prompt	Upload or select a temporary audio greeting prompt (e.g., holiday or temporary absence messages) that overrides other prompts when configured.

Unavailable Prompt	Upload or select the default unavailable audio greeting prompt played to callers when leaving a voicemail.
Allow Members to Modify Voice Prompts	Check this box to allow assigned member extensions to record, update, and manage the voicemail group's custom voice prompts directly via DTMF menus when calling the Voicemail Group Access Code (*99).

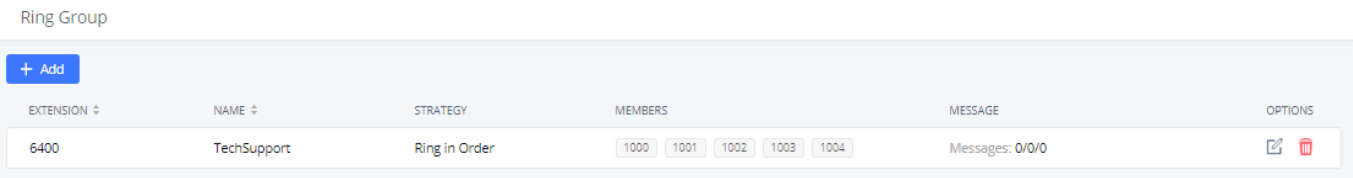
The administrator can add up to 150 extensions to a single voicemail group.

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.



Ring Group

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

Ring Group Name	Configure ring group name to identify the ring group. Letters, digits, _ and - are allowed.
Extension	Configure the ring group extension.
Members	Select available users from the left side to the ring group member list on the right side. Click on ? ? to arrange the order.
LDAP Phonebook	Select available remote users from the left side to the ring group member list on the right side. Click on ? ? to arrange the order. Note: LDAP Sync must be enabled first.
Ring Strategy	Select the ring strategy. The default setting is "Ring in order". Ring Simultaneously: Ring all the members at the same time when there is incoming call to the ring group extension. If any of the member answers the call, it will stop ringing. Ring in Order: Ring the members with the order configured in ring group list. If the first member does not answer the call, it will stop ringing the first member and start ringing the second member.
Music On Hold	Select the "Music On Hold" Class of this Ring Group, "Music On Hold" can be managed from the "Music On Hold" panel on the left.

Custom Prompt	This option is to set a custom prompt for a ring group to announce to caller. Click on 'Prompt', it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings?? Voice Prompt?? Custom Prompt, where they could record new prompt or upload prompt files.
Ring Timeout on Each Member	Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 60 seconds.Note: The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.
Auto Record	If enabled, calls on this ring group will be automatically recorded. The default setting is No. The recording files can be accessed from WebGUI?? CDR?? Recording Files.
Endpoint Call Forwarding Support	This allows the UCM to work with endpoint-configured call forwarding settings to redirect calls to ring group. For example, if a member wants to receive calls to the ring group on his mobile phone, he will have to set his endpoint's call forwarding settings to his mobile number. By default, it is disabled.However, this feature has the following limitations: This feature will work only when call forwarding is configured on endpoints, not on the UCM. If the forwarded call goes through an analog trunk, and polarity reversal is disabled, the other ring group members will no longer receive the call after it is forwarded. If the forwarded call goes through a VoIP trunk, and the outbound route for it is PIN-protected and requires authentication, the other ring group members will no longer receive the call after it is forwarded. If the forwarded call hits voicemail, the other ring group members will no longer receive the call.
Replace Display Name	If enabled, the UCM will replace the caller display name with the Ring Group name the caller know whether the call is incoming from a direct extension or a Ring Group.
Skip Busy Agent	If enabled, skip busy agents regardless of call waiting settings.
Enable Destination	If enabled, users could select extension, voicemail, ring group, IVR, call queue, voicemail group as the destination if the call to the ring group has no answer. Secret and Email address are required if voicemail is selected as the destination.
Default Destination	The call would be routed to this destination if no one in this ring group answers the call.Note: Users can now set the voicemail of ring groups as routing destinations and IVR key press event destinations and to do so ring group must have their Default Destination set to Voicemail with Ring Group Extensions.
Voicemail	Whether to enable the voicemail for the ring group or not.
Voicemail Password	Configure the voicemail password (only numbers).
Email Address	Fill in the user's Email address (s), the voice message will be sent to this address (s).
Busy Prompt	This voicemail prompt will be played when the callee is in another call or is in DND mode. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet PromptSound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Greet Prompt	This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
Temporary Prompt	This voicemail prompt well be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.

Unavailable Prompt

This voicemail prompt will only be played when the callee's extension is unregistered. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.

Create New Ring Groups

* Ring Group Name:

test

* Extension:

6400

Members:

27 items

Available

Search

1000

1001

1005

1006

1007

3 items

Selected

Search

1002

1003

1004

LDAP Phonebook:

0 item

Available

Search

None

0 item

Selected

Search

None

| Ring Group Options

Ring Strategy:

Ring in Order

Music On Hold:

None

Custom Prompt:

None

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:

☐ 106 Available Extensions

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 0 Selected Extensions

☐ 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)

☐ 0 Selected LDAP

Ring Group Remote Extension

RESTRICT CALLS

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

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

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

Name

RestrictRule

Restrict Calls between Extension

☒

Members

25

Available

Search

☐ 1021
☐ 1022
☐ 1023
☐ 1024
☐ 2000 "Jean Doe"
☐ 2001 "Manager Extension"

2

Selected

Search

☐ 1001
☐ 1004

Allowed List

26

Available

Search

☐ 1007
☐ 1020
☐ 1021
☐ 1022
☐ 1023
☐ 1024

1

Selected

Search

☐ 1003 "name"

Restrict Calls

Configure Restrict Calls

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

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

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

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

2-way Intercom

▼

* Extension

Private Intercom

☐

Auto Record

☐

Replace Display Name

☐

* Maximum Call Duration (s)

Custom Prompt

None

▼

Upload Audio File

Play Prompt to Caller

☐

* Members

☐ 5 items

Available

Search

Q

☐ 1000

☐ 1001

☐ 1002

<

>

☐ 0 item

Selected

Search

Q

None

Cancel

Save

2 way Intercom

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

LDAP Members	Select a number from the LDAP phonebook. If LDAP contacts were synchronized through the SIP trunk, the IPPBX will use that same trunk to send the call. Other trunks will not be used.
Paging/Intercom Allowlist	Select the extensions which are allowed to initiate the paging/intercom. Selected: Only selected extension will be allowed to initiate paging/intercom. All: Allow all extensions and configured services to initiate paging/intercom.
Custom Prompt	This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on 'Upload Audio File', it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings > Voice Prompt > Custom Prompt, where they could record new prompt or upload prompt files.
Play Prompt to Caller	Play the prompt to the caller.

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

2-Way_Intercom

* Strategy

2-way Intercom

* Extension

Extension

Private Intercom

☒

Auto Record

☐

Replace Display Name

☐

* Maximum Call Duration (s)

0

Custom Prompt

None

Play Prompt to Caller

☐

* Members

☐ 5 items

Available

Search

☐ 0 item

Search

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

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

1-way Paging

Paging/Intercom > Create New Paging/Intercom Group

Disable

☐

* Name

Page_1

* Strategy

1-way Paging

* Extension

Extension

Video Broadcast

☐

Auto Record

☐

Replace Display Name

☐

Delayed Paging

☐

* Maximum Call Duration (s)

0

Announcement File

None

Upload Audio File

Play Prompt to Caller

☐

* Members

5 items

Available

Search

0 item

Search

1 way Paging

Parameter	Description
Name	Configure paging/intercom group name.
Strategy	Select "1-way Paging".
Extension	Configure the paging/intercom group extension.

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

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 (.)

Multicast Paging

Paging/Intercom > Create New Paging/Intercom Group

Disable
☐

* Name

* Strategy

Multicast Paging

* Extension

Delayed Paging
☐

* Maximum Call Duration (s)

Custom Prompt

None

Upload Audio File

Play Prompt to Caller
☐

* Prompt Playback Count

* Multicast Address/Port

Multicast IP Address

Port

Add Multicast IP Address

Paging/Intercom Allowlist

Selected

All

0 item

Available

Search

5 items

Selected

Search

1000

Cancel

Save

Multicast Paging

Paging/Intercom	Select existing paging/intercom groups and multicast communities.
Name	Enter the name of the scheduled Intercom/Paging.
Caller	Once a caller is selected, and the specified start time is reached, the system will contact the caller. If this call is rejected, the page/intercom will be cancelled. If caller is set to None, the system will call all group members and play the configured prompt.
Start Date	Select the date of the start of the paging/intercom.
Start Time	Select the start time of the paging/intercom.
Repeat	Select the repeat interval of the paging/intercom. No Repeat: The intercom/paging will play once on the scheduled date and time. Everyday: The intercom/paging will play daily starting from the scheduled day and on the time scheduled every day. Weekly: The intercom/paging will play weekly on the selected day(s) of the week. Monthly: The intercom/paging will play monthly on the selected date of the month.
Include Holidays	When Every day, Weekly, or Monthly is selected. This option will appear. If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.
Sync to Google Calendar	This feature cannot be used if Google Services have not been authorized. Please resolve this in the Integrations > Google Services page.

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

Name

* Extension

Extension

Delayed Paging

☐

* Maximum Call Duration (s)

0

Custom Prompt

None ▾

Upload Audio File

Play Prompt to Caller

☐

* Prompt Playback Count

1

* Multicast Paging Group

☐ 0 Available

Search

🔍

None

<

>

☐ 0 Selected

Search

🔍

None

Paging/Intercom

☐ Selected ☒ All

Cancel

Save

Multicast Community Parameters

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

Include Holidays	When Every day, Weekly, or Monthly is selected. This option will appear. If enabled, scheduled pages/intercoms will run during holidays. Otherwise, scheduled pages/intercoms displayed on the calendar will not actually be run.
Sync to Google Calendar	This feature cannot be used if Google Services have not been authorized. Please resolve this in the Integrations > Google Services page.

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

2024-03-07

* Start Time

Select time

Add Start Time

Repeat

No Repeat

Sync to Google Calendar

Google Services

Cancel

Save

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

Sync to Google Calendar

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

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

Pending Paging/Intercom

Paging/Intercom Schedule

+ Add

Name

Time:

Start Time

 to

End Time

Search

Reset

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	

Total: 3

<1>

10 / page

Goto

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 GroupsMulticast CommunityScheduled 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

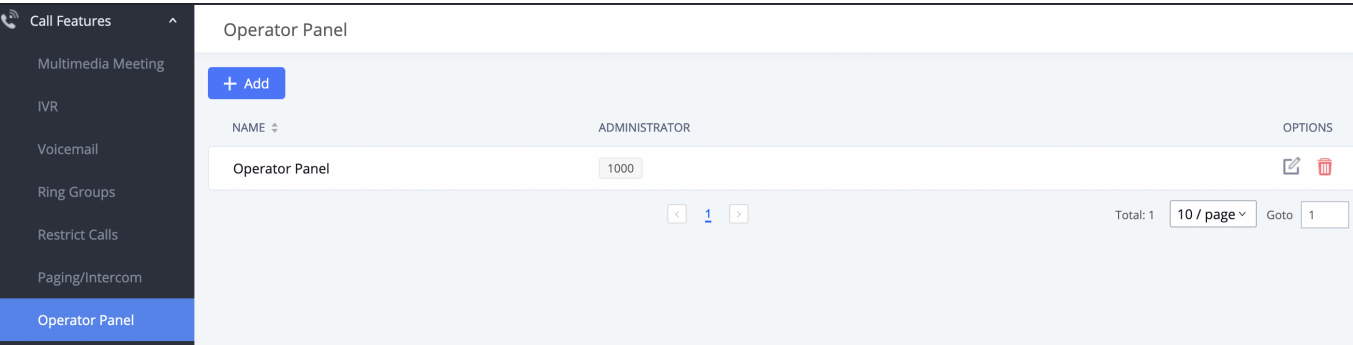
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	1	2
3	4	5	6	7 03:00 Multicast_G 06:00 Paging	8	9
10	11	12	13	14	15	16
17	18	19	20 11:00 Multicast_G	21	22	23
24	25	26 11:00 Multicast_G	27	28	29	30
31	1	2 11:00 Multicast_G	3	4	5	6

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.

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

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→**Basic Call Features**→**Call Queue**.

Add Call Queue

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

Call Queue						
Call Queue Queue Recordings Queue Switchboard Call Queue Statistics						
Add Global Queue Settings						
Extension ↕	Name ↕	Strategy ↕	Queue Chairman	Members		
6500	Help_Desk	Ring All	1005	1000	1001	1002
6501	Sales	Ring All	1005	1003	1004	1005
6502	Marketing	Ring All	4005	4000	4001	4002
6503	Support	Ring All	5009	5001	5002	5003
Total: 4 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.

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

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

Parameter	Description
Basic Settings	
General	
Extension	Configure the call queue extension number.
Name	Configure the call queue name to identify the call queue.
Proficiency Routing	If enabled, incoming calls will be routed to the agents with the highest available proficiency level (lower number = higher proficiency). If multiple agents have the same level, the Ring Strategy for Same Proficiency Level will be used to route calls among those agents. Please make sure to assign proficiency levels to the agents under the Agents tab. Note: This option applies to both static and dynamic agents.
Strategy	Select the strategy for the call queue: Ring All: Ring all available Agents simultaneously until one answers. Linear: Ring agents in the specified order. Least Recent: Ring the agent who has been called the least recently. Fewest Calls: Ring the agent with the fewest completed calls. Random: Ring a random agent. Round Robin: Ring the agents in Round Robin scheduling with memory. The default setting is "Ring All".

Ring Strategy for Same Proficiency Level	Select the strategy for the call queue: Ring All: Ring all available Agents simultaneously until one answers. Linear: Ring agents in the specified order. Least Recent: Ring the agent who has been called the least recently. Fewest Calls: Ring the agent with the fewest completed calls. Random: Ring a random agent. Round Robin: Ring the agents in Round Robin scheduling with memory. The default setting is "Ring All".
Music On Hold	Select the Music On Hold class for the call queue. Note: Music On Hold classes can be managed from Web GUI > PBX Settings > Music On Hold.
Max Queue Length	Configure the maximum number of calls to be queued at once. This number does not include calls connected with agents, only calls still in queue. When exceeded, callers hear a busy tone and are forwarded to the configured failover destination. Default is 0 (unlimited).
Agent Rest Time (s)	Configure the amount of time in seconds after ending a call where the agent will not receive additional calls. Default is 10 seconds.
Retry Time (s)	Configure the number of seconds to wait before ringing the next agent. Minimum is 1, default is 5 seconds.
Agent Ring Time	Configure the number of seconds to ring an agent. Minimum is 5, default is 30 seconds.
Auto Record	If enabled, calls on the queue will be automatically recorded. Choose to record internal calls, external calls, or all calls. Default is disabled.
Prompt Language	Choose the language of the prompt played to callers. Selecting "default" uses the language defined under PBX Settings > Voice Prompt > Language Settings.
Welcome Prompt	
Enable	Enable the welcome prompt.
Custom Prompt	Choose the initial tone that plays when the user dials the queue number. Note: Custom prompts can be uploaded directly in .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, or .ulaw formats.
Play Full Welcome Prompt	If enabled, queue agents will not be rung until after the welcome prompt finishes playing. Otherwise, agents are rung while the prompt plays.
Satisfaction Survey Prompt	
Custom Prompt	After an agent hangs up, a prompt plays asking the caller to rate satisfaction on a scale of 1 to 5. Survey results can be reviewed under Call Queue Statistics > Overview > Agent Satisfaction Statistics / Queue Satisfaction Statistics.
Max Wait Time	
Max Wait Time	Configures the amount of time (in seconds) a caller is kept in queue before automatic routing to the Max Wait Time Destination. Default is 60 seconds.
Destination	The destination where calls are routed if no agent answers before max wait time expires.
Transfer Call Based on Time Conditions	
Enable	Toggles time-based routing rules for holidays and non-working hours.
Destination During Holidays	Set the destination type and target destination during official holidays.
Destination During Non-working Hours	Set the destination type and target destination outside defined office time.
Priority Destination	Select whether holiday routing or non-working hours routing takes priority when overlapping.
Play Holiday Prompt During Holiday	Toggles playing the designated holiday voice prompt before transfer. The holiday prompt can be configured in Time Settings -> Holiday.
Reset Agent Call Counter	
Enable	Specifies the frequency at which the agent call counter is reset. Affects ring strategy counters and switchboard data.

Repeat	Set repeat frequency to One-time, Daily, Weekly, or Monthly.
Date/Time	Set the reset date and time.
Destination Prompt Cycle	
Enable	If enabled, callers hear a custom prompt at set intervals while waiting. Pressing "1" routes them immediately to a predefined failover destination.
Destination Prompt Cycle	Configure the voice prompt cycle interval (in seconds).
Custom Prompt	Select or upload the voice prompt file played during the cycle.
Destination	Select the failover destination when callers press "1".
Advanced Settings	
Virtual Queue	
Enable Virtual Queue	If enabled, activates a virtual queue allowing users to request an automated callback while retaining their position in line.
Virtual Queue Mode	Select the triggering mode for virtual queue: DTMF mode (Press 2): Callers can manually request a virtual queue callback at any time while waiting in line by pressing key 2 on their telephone keypad. The system will then play a prompt asking the caller to manually enter their preferred callback number. Timeout mode: The system automatically offers the virtual queue callback once the caller's wait time reaches the threshold configured in Virtual Queue Period (s). Callers will hear a prompt allowing them to choose a callback number, or if Auto-fill Callback Number is enabled, the field automatically populates using their detected Caller ID. The default mode is Timeout mode.
Virtual Queue Period (s)	The amount of time in seconds that must pass before virtual queue is offered in Timeout or Auto mode.
Auto-fill Callback Number	When enabled, automatically populates the callback field with the caller's Caller ID. Note: This option can only be enabled when Virtual Queue Mode is set strictly to Timeout mode.
Virtual Queue Outbound Prefix	System adds this prefix to dialed numbers when performing virtual queue callbacks.
Enable Virtual Queue Position Announcement	Informs waiting callers of their exact position in line.
Enable Virtual Queue Wait Time Announcement	Periodically announces estimated wait times to callers.
Enable Virtual Queue Callback Timeout	Sets a maximum time limit for agents to answer a virtual queue callback.
Write Timeout	The amount of time in seconds agents have to answer a callback.
Virtual Queue Welcome Prompt	Upload the welcome prompt file for the virtual queue.
Queue Announcement	
Enable Position Announcement	Inform callers waiting in queue of their line position.
Enable Wait Time Announcement	Periodically announce estimated wait times (announced if greater than one minute).
Announcement Interval	Configure announcement frequency (20 to 600 seconds, default 20).
Agent ID Announcement	Plays the agent ID prompt to the caller upon connection.
Premium Code	Callers can enter a premium code and # to increase queue priority.
Premium Code Prompt	Shares the announcement cycle with position announcements.
Custom Announcement	
Custom Prompt	Periodically play custom audio announcements to queued callers.
Announcement Interval (s)	Interval between custom announcements (20 to 600 seconds, default 60).
Empty Queue	

Leave When Empty	Configure whether callers disconnect if no agents remain in queue (Yes, No, or Strict). Default is Strict.
Dial in Empty Queue	Configure whether callers can dial into an empty queue (Yes, No, or Strict). Default is No.
Failover Destination	Choose failover destination (Play Sound, Extension, Voicemail, Queue, Ring Group, Voicemail Group, IVR, External Number) when queue is empty or unstaffed.
CTI	
Allow Static Agent Login/Logout	Enabling static agent login restricts dynamic agent access.
Queue Chairman	Assign extensions permitted to operate and monitor the queue via Web UI.
Priority Queue	
Enable Priority Queue	Activates weighted call routing for agents who belong to multiple queues simultaneously. When enabled, the UCM prioritizes calls from queues with a higher overall weight.
Weight	Configures the base priority level for the call queue (Range: 1 to 99). Higher weight values take precedence when routing calls to multi-queue agents.
Enable Accelerated Weighting	Prevents excessive waiting times for callers in lower-weight queues. When enabled, the queue weight automatically increments by 1 after callers wait for a specified duration.
Accelerated Weighting Duration (seconds)	Configures the waiting time interval in seconds (Range: 10 to 1800) required for the queue's overall weight to increase by 1.
Service Level Agreement (SLA)	
Enable SLA	Toggles SLA measurement to track call response times against threshold goals.
SLA Time (s)	Maximum target time in seconds for agents to answer calls (1 to 180s, default 20).
SLA Alert Email Notification	Enable SLA breach email notifications.
Alert Threshold (%)	Minimum acceptable SLA answer percentage before triggering alerts (default 80%).
SLA Alert Interval (m)	Minimum time between breach email alerts (1 to 120 minutes, default 120).
SLA Alert Email Template	Select email template used for SLA breach notifications.
Alert Email Recipients	Designate email recipients for SLA breach alerts.
Other Settings	
Report Hold Time	If enabled, reports caller hold duration to the agent upon call connection.
Replace Display Name	Replaces caller display name with the Call Queue name on agent devices.
Enable Feature Codes	Enable feature code operations (e.g., *83 for Agent Pause) for this queue.
Autofill	Distributes waiting calls automatically to agents as soon as they become free.
Dynamic Login Password	Requires dynamic agents to enter a PIN when logging in.
Alert-info	Specifies custom Alert-Info SIP header for alternative ringtones.
Call Memory	Prioritizes connecting returning callers to the agent they last spoke with.
Memory Retention Time (Days)	Retention window for Call Memory matching (1 to 30 days, default 7).
Enable RPID Header	Toggles sending Remote-Party-ID SIP header to caller.

Skip Busy Agent	Configures whether the queue will ring agents who are currently on an active call. When enabled, busy agents are skipped during call distribution.
Agents	
Dynamic Agents	Assign users authorized to dynamically sign into or out of the queue via feature codes. When Proficiency Routing is enabled, individual skill levels can be configured here.
Static Agents	Assign static agents manually and configure their ringing order within the call queue. When Proficiency Routing is enabled, individual skill levels can be configured here.
Queue Permissions	
Queue Chairman Permissions	
Queue Board	Grants access to view the Queue Board (Wallboard) metrics, real-time status charts, and agent statistics for this queue.
Queue Operation Panel	Enables access to the interactive Queue Operation Panel interface for this queue.
Change the status of the agent position	Allows the chairman to modify agent login states (Log In, Logout, Pause/Resume) directly from the Queue Operation Panel.
Call Assignment Management	Allows the chairman to assign waiting calls to agents, including manual drag-and-drop call dispatching from the queued list.
Allows for answering or hanging up calls on the agent's line	Grants remote control capabilities to answer or disconnect active calls on assigned agent lines.
Call monitoring operation	Enables live call supervision capabilities (Listen, Whisper, and Barge-In) for calls handled within this queue.
Call hold operation	Allows the chairman to remotely place active queue calls on hold or resume held calls.
View the CDR of this queue	Grants permission to view and review Call Detail Records (CDR) specifically filtered for this call queue.
Queue Agent Permissions	
Queue Board	Grants access to view the Queue Board wallboard for monitoring queue metrics and performance.
Queue Operation Panel	Enables access to the Queue Operation Panel for the agent.
Call Assignment Management	Allows the agent to manage call assignments and answer or retrieve queued calls from the waiting list.
Allows for answering or hanging up calls on the agent's line	Allows the agent to answer or hang up calls directly through the panel interface.
Call hold operation	Allows the agent to place calls on hold or resume held calls via the panel interface.
View the CDR of this queue	Grants permission to view and review Call Detail Records (CDR) specific to this call queue.

Static and Dynamic Agents

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:

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

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.

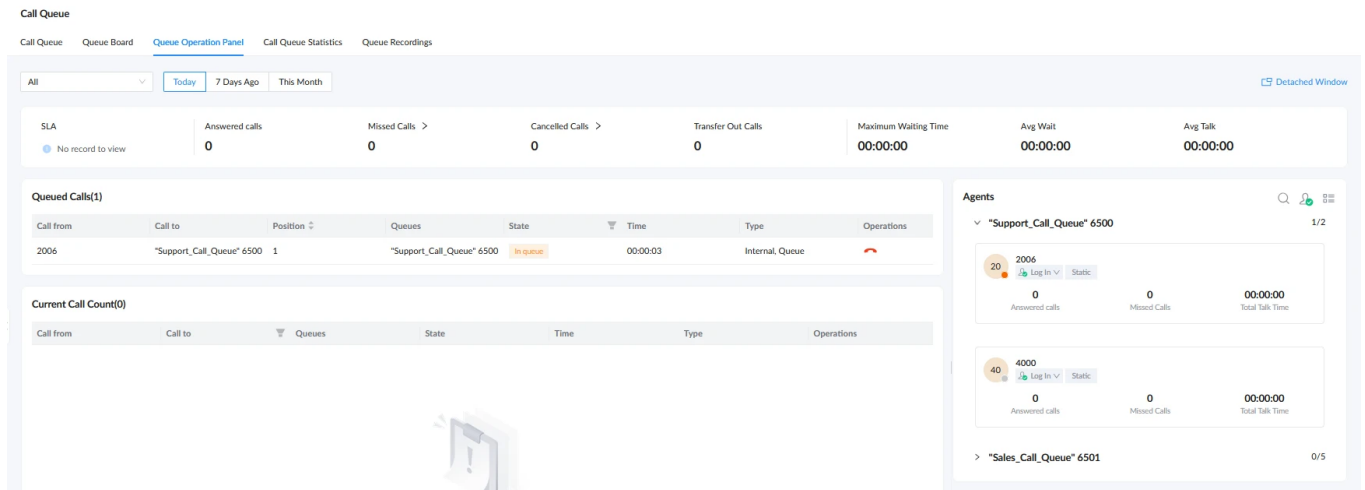
Users can configure up to 10 pause reason when the Agent Pause Reason Settings are set to "Custom".

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 logout from all queues.

Queue Operation Panel

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



The main workspace is divided into three functional areas:

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

Queue Permissions

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

Queue Chairman

☒ Queue Board

☒ Queue Operation Panel

☒ Change the status of the agent position ⓘ
☒ Call Assignment Management ⓘ
☒ Allows for answering or hanging up calls on the agent's line
☒ Call monitoring operation
☒ Call hold operation

☒ View the CDR of this queue ⓘ

Queue Agent

☒ Queue Board

☒ Queue Operation Panel

☐ Call Assignment Management ⓘ
☐ Allows for answering or hanging up calls on the agent's line
☐ Call hold operation

☒ View the CDR of this queue ⓘ

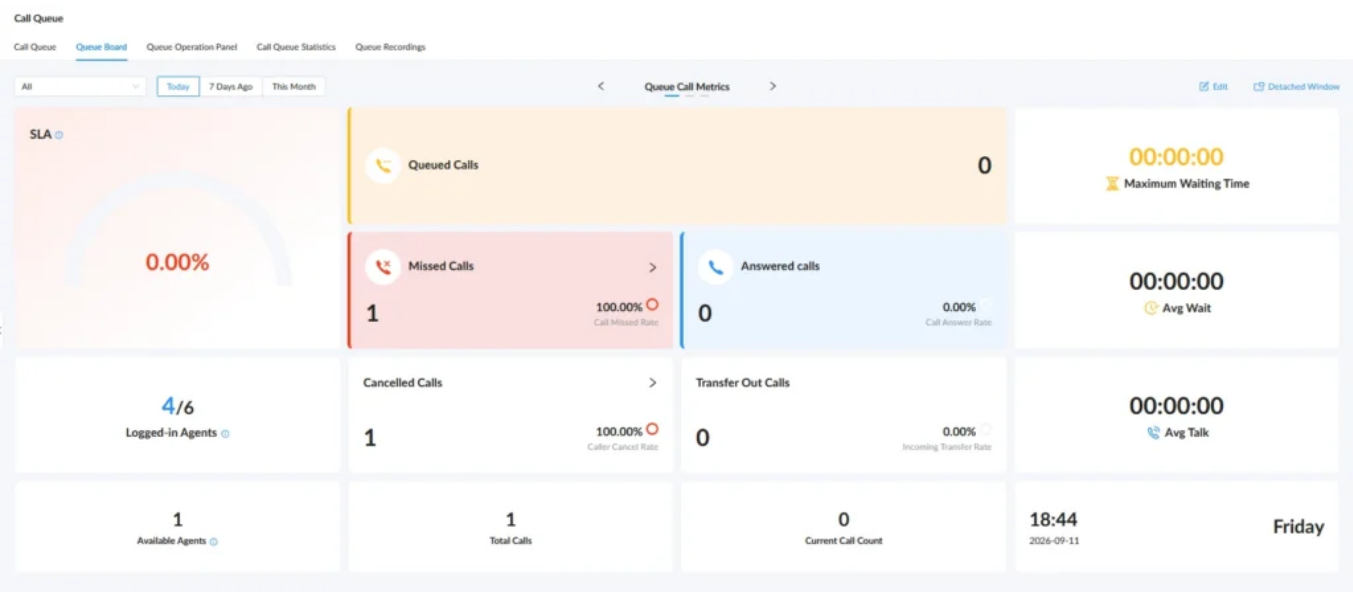
The table below describes the configurable permission options available for each role:

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

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

Queue Board

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



The Wallboard features three analytical views:

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

/heading

Queue Recordings

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

Call Queue

Call Queue

Queue Recordings

Queue Switchboard

Call Queue Statistics

Recording files are currently stored in **GDMS**. Change the storage location? This will modify the storage paths of basic call recordings, queue recordings, meeting recordings, SCA recordings, emergency call recordings, and paging/intercom recordings.

Download

Download All

Delete

Clear

Local

2024-10

☐	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 or by downloading all files through the button.

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.

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

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 button. They can also set up automatic email deliveries of these statistics at regular intervals by clicking on

Additionally, users can clear the statistics using the 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

By Week



Mon



23



Email

james@company.com

[Email Template](#)

Cancel

Save

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 shows the following information:

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

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

Abandoned Call Calculation

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

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

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

Details



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

Total Calls

Answered Calls

Abandoned Calls

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

Queue Statistics Details

Agent Details 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.

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

Search

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.

Call QueueQueue RecordingsQueue SwitchboardCall Queue Statistics

DownloadReset StatisticsAutomatic Download

2024-10-01to2024-10-24

Filter

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

Search

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

Total: 3

<1>

10 / page

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...)

Call Queue

Call QueueQueue RecordingsQueue SwitchboardCall Queue Statistics

DownloadReset StatisticsAutomatic Download

2024-10-01to2024-10-24Filter

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

Search

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

Total: 410 / page

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.

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 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

Default

CancelSave

Global Queue Settings

Dynamic Agent Login Settings	
Agent Login Code Suffix	Configure the code to dial after the queue extension to log into the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log in.

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

CALL FLOW DESIGN

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

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

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

Call Flow System Specifications & Limits

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

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

Call Flow Management

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

System Status

Extension/Trunk

Basic Call Features

Advanced Call Featu...

Call Flow Design

Pickup Groups

Dial By Name

DISA

Call Flow Design

During calls, the terminating key will be 'X'.

Add

Delete

Export

CL Name/Number

Name	Enable	Number	Remark	Operations
Flow_Test		8300		
Flow_Test-copy				

Total 2

1

10 / page

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

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

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

Creating a Call Flow

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

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

Create New Call Flow

×

*

Name

2 - 64 characters, Alphanumeric characters, Chinese characters, and special characters _ - are supported

Remark

*

Add Method

Based on Existing Template

▼

*

Manual

Based on Existing Template

Based on Existing Flow

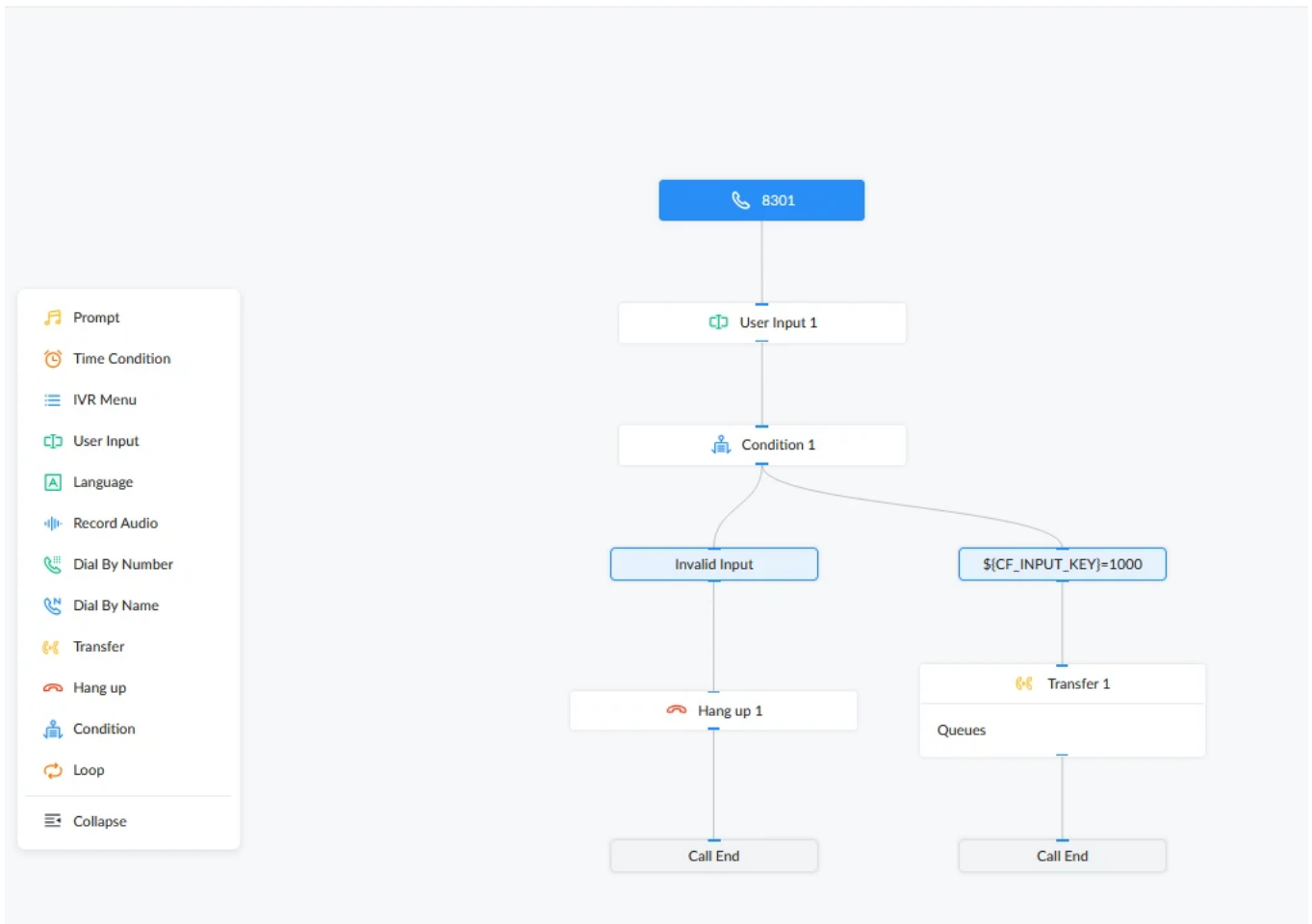
Import Call Flow File

Cancel

Next

Call Flow Configuration Options

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



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

Call Flow Node	Description
Initial Action(Start Component)	The mandatory entry point for every flow. Configures the assigned extension number, initial welcome audio prompt, and loop settings.
Prompt	Plays selected audio files or AI-generated Text-to-Speech (TTS) announcements to the caller. Users can also play the prompt on loop 3 times.
Time Condition	Evaluates system time conditions (Office Hours, Custom Time, or Custom Time Groups) and branches the routing path accordingly.
IVR Menu	Presents multiple DTMF menu options, stores keystroke entries into variables, and branches calls based on valid inputs, timeouts, or invalid entries.
User Input	The User Input component is used to play an instructional prompt and capture DTMF key sequences (such as PINs or account IDs) entered by the caller and passes the call to the next connected node (typically a Condition node) for expression evaluation.
Language	Overrides the system default voice prompt language for all subsequent components in the call flow path.
Record Audio	Dynamically enables or disables call recording at a specific stage in the flow, with options to play pre-recording notification prompts.
Dial by Number	Directs callers to manually enter numbers to reach allowed extension ranges, predefined internal destinations (IVR, Ring Group, Queue, Conference, Call Flow), or external numbers using a defined pattern or LDAP directory contacts.

Dial by Name	Allows callers to search for and connect to a target user by spelling the letters of the user's name with their phone keypad. The search directory can be configured using local extensions, LDAP phonebooks, or both.
Transfer	Directs the caller out of the Call Flow to a final internal or external destination (Extension, Voicemail, Ring Group, Queue, IVR, or another Call Flow).
Hang Up	Terminates the active call session.
Condition	Evaluates logical expressions configured under custom branches. Branches evaluate variables (such as \${CF_INPUT_KEY}, \${CALLERID(number)}, or \${CALLFLOW_LANGUAGE}), constants, or built-in functions to determine subsequent call routing. Note: Please refer to the Call Flow Design Configuration Guide for a list the supported expressions.
Loop	Repeats execution of its child components either for a fixed count (Range: 1-99) or until a custom logical condition expression.

PICKUP GROUPS

The 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.

Pickup Groups

* Name:

Members:

☐ 2 Available

☐ 1005

☐ Extension Group--AccountingDep...

☐ 3 Selected

☐ 1000 "John DOE"

☐ 1001

☐ 1002

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

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:

Default



Record

Delete

Upload

☐	DISABLED/ENABLED	SOUND FILE	OPTIONS
☐	ON 	macroform-cold_day.wav	  
☐	ON 	macroform-robot_dity.wav	  
☐	ON 	macroform-the_simplicity.wav	  
☐	ON 	manolo_camp-morning_coffee.wav	  
☐	ON 	reno_project-system.wav	  

< 1 >

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.

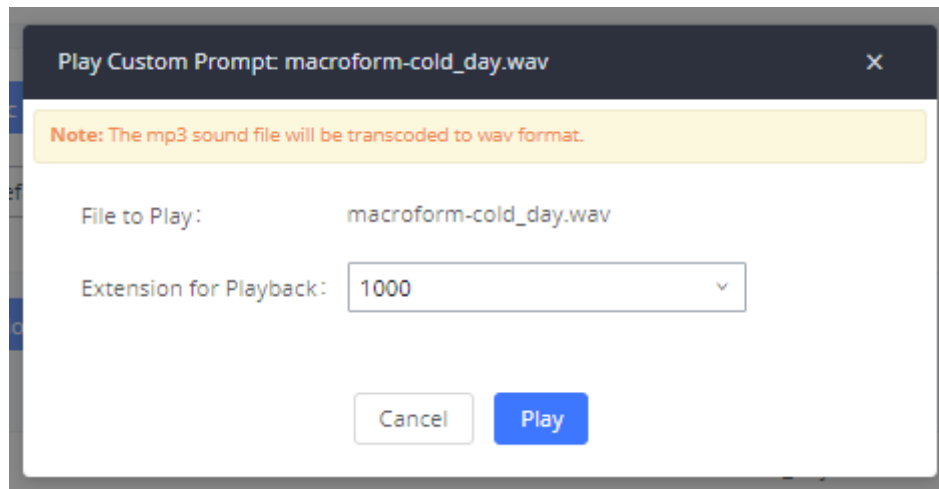
The UCM630xA allows Users to select the Music On Hold file from Web GUI to play it. The UCM630xA will

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



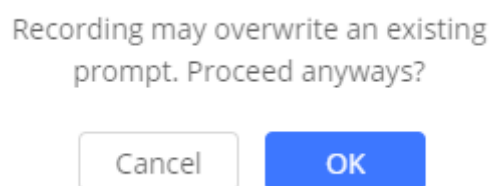
Play Custom Prompt

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

The screenshot shows a web-based interface for editing a custom prompt. The title bar reads "Edit Custom Prompt: macroform-robot_dity.wav". Below the title bar is a yellow note box that says "Note: The mp3 sound file will be transcoded to wav format." The main area contains three labels: "File to Play:" with the value "macroform-robot_dity.wav", "Extension for" with a dropdown menu showing "1000", and "Recording:". At the bottom are two buttons: "Cancel" and "Record".

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.

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:

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.

Call Transfer

Presence Status: Available

Available

Away

Chat

Custom Presence Status

Unavailable

Call Forward Unconditional: None

Call Forward No Answer: None

Call Forward Busy: None

CFU Time Condition: All Time

CFN Time Condition: All Time

CFB Time Condition: All Time

Do Not Disturb: ☐

* DND Time Condition: All Time

FWD Whitelist:

Add FWD Whitelist

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:

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

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, one the user dials the feature code (default is *48), a prompt will be played to select which status they want to put themselves in, by pressing the corresponding key.

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

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

SIP Presence Feature Code

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

CDR Display Filter

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

Recording files are currently stored in USB Disk . Do you want to change the location? This will change the file storage location for basic call, conference, queue, SCA, and emergency call recordings.

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
	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:

Default

Confirm When Answering: ☒

Use Callee DOD for Follow Me: ☐

Enable Destination: ☐

Default Destination:

Voicemail

Follow Me Numbers

New Follow Me Number: ☒ Dial Local Extension ☐ Dial External Number

for

30

 (seconds)

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

Add

EXTENSION	OPTIONS
1002 for 30 (seconds)	

Edit Follow Me

1. Click on

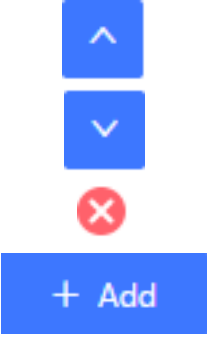
to add local extensions or external numbers to be called after ringing the extension selected in the first step.

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:

Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If external number is added in the Follow Me, please make sure this option is enabled or the "Skip Trunk Auth" option of the extension is enabled, otherwise the external Follow Me number cannot be reached.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking users
Confirm When Answering	By default, it is enabled, and user will be asked to press 1 to accept the call or to press 2 to reject the call after answering a Follow Me call. If it is disabled, the Follow Me call will be established once after the user answers.
Enable Destination	When enabled, the call will be routed to the default destination if no one in the Follow Me extensions answers the call.
Default Destination	Configure the destination if no one in the Follow Me extensions answers the call. The available options are: Extension Voicemail Queues Ring Group Voicemail Group IVR External Number

Follow Me Numbers	 The added numbers are listed here. Click on to arrange the order. Click on to delete the number. Click on to add new numbers.
New Follow Me Number	Add a new Follow Me number which could be a 'Local Extension' or 'External Number'. The selected dial plan should have permissions to dial the defined external number.
Dialing Order	Select the order in which the Follow Me destinations will be dialed to reach the user: ring all at once or ring one after the other.

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.

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

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.

Speed Dial > Create New Speed Dial

Enable Speed Dial



* Speed Dial Extension

Speed Dial Name

Default Destination

Extension



1000



Cancel

Save

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.
- **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 v Goto 1

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.

Speed Dial

+ Add 📄 Import 📄 Export				
SPEED DIAL EXTENSION ↕	SPEED DIAL	DEFAULT DESTINATION	DEFAULT DESTINATION	OPTIONS
123	Enable	Extension	1000	✎ 🗑
999	Enable	Voicemail		✎ 🗑
< 1 > Total: 2				10 / page v Goto 1

Import Speed Dial List

Then select the csv file of the speed dial entries and click

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.

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.

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.

Speed Dial

+ Add

↶ Import

↶ Export

SPEED DIAL EXTENSION ⚙	SPEED DIAL	DEFAULT DESTINATION	DEFAULT DESTINATION	OPTIONS
123	Enable	Extension	1000	 
999	Enable	Voicemail		 

< 1 >

Total: 2

10 / page ▾

Goto 1

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**.

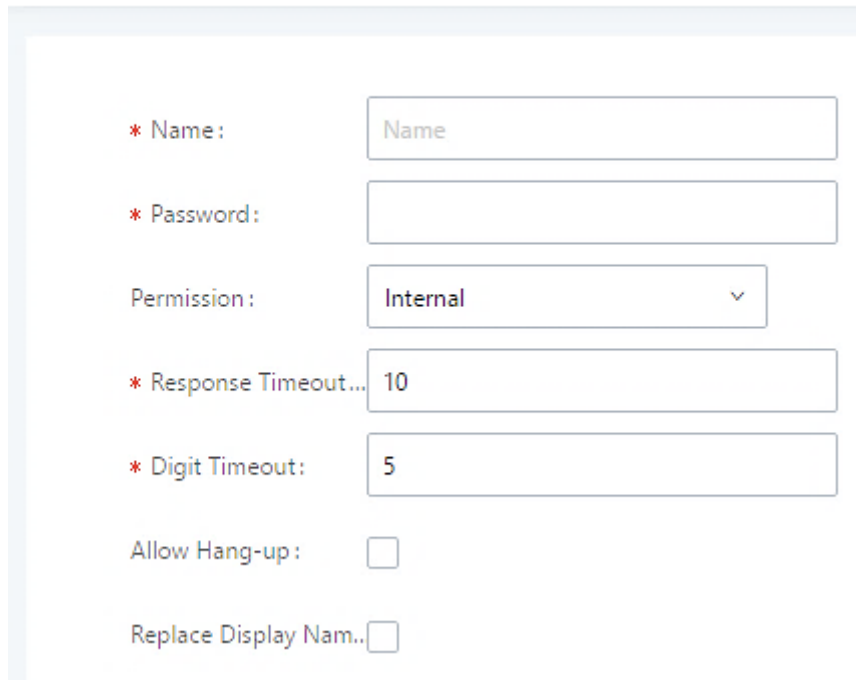
- Click on

to add a new DISA.
- Click on

to edit the DISA configuration.
- Click on

to delete the DISA.

Create New DISA



* Name:

* Password:

Permission:

* Response Timeout:

* Digit Timeout:

Allow Hang-up: ☐

Replace Display Name: ☐

Create New DISA

The following table details the parameters to set and configure DISA feature on UCM630xA PBX.

Name	Configure DISA name to identify the DISA.
Password	Configure the password (digit only) required for the user to enter before using DISA to dial out. Note: The password must be at least 4 digits.
Permission	Configure the permission level for DISA. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the DISA, the UCM630xA will compare the DISA's permission level with the outbound route's privilege level. If the DISA's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Response Timeout	Configure the maximum amount of time the UCM630xA will wait before hanging up if the user dials an incomplete or invalid number. The default setting is 10 seconds.
Digit Timeout	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
Allow Hangup	If enabled, during an active call, users can enter the 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".
Replace Display Name	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:

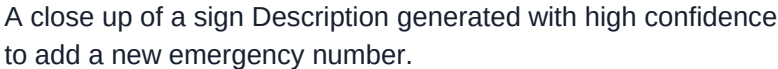
<https://www.fcc.gov/general/9-1-1-and-e9-1-1-services>

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 A close up of a sign Description generated with high confidence to add a new emergency number.
3. Configure the required fields "Name, Emergency Number and Trunk(s) to be used to reach the number".
4. Save and apply the configuration.

Create New Emergency Call

* Name:

* Emergency Number:

Emergency Level:

1 - Not Urgent

▼

Disable Hunt on Busy:

☐

Custom Prompt:

None

▼

Prompt

* Use Trunks:

* Members Notified:

☐ 11 items Available

☐ 1001 "John Doe"
 ☐ 1002
 ☐ 1003
 ☐ 1004

☐ 1 item Selected

☐ 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.

Name	Configure the name of the emergency call. For example, "emergency911", "emergency211" and etc.
Emergency Number	Config the emergency service number. For example, "911", "211" and etc.
Emergency Level	Select the emergency level of the number. Level "3" means the most urgent.
Disable Hunt on Busy	If this option is not enabled, when the lines of trunks which the coming emergency call routes by are completely occupied, the line-grabbing function will automatically cut off a line from all busy lines so that the coming emergency call can seize it for dialing out. This option is not enabled by default.
Custom Prompt	This option sets a custom prompt to be used as an announcement to the person receiving an emergency call. The file can be uploaded from the page "Custom Prompt". Click "Prompt" to add additional record.
Use Trunks	Select the trunks for the emergency call. Select one trunk at least and select five trunks at most.
Members Notified	Select the members who will be notified when an emergency call occurs.
Strip	Specify the number of digits that will be Stripped from the beginning of the dialed number before the call is placed via the selected trunk.

Prepend	Specify the digits to be Prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Auto Record	When enabled, emergency call will be automatically recorded.
Send Recording File	When enabled recording files will be sent to the configured email address.
Email Address	The email address to where the recording files will be sent.

Emergency Numbers Parameters

Emergency Calls

Emergency CallsEmergency RecordingsEmergency Location Mapping

+ Add

NAME ↕	EMERGENCY NUMBER ↕	EMERGENCY LEVEL ↕	DISABLE HUNT ON BUSY ↕	OPTIONS
911	911	1	No	 

< 1 >

Total: 1 10 / page Goto 1

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 Calls

Emergency CallsEmergency RecordingsEmergency Location Mapping

 Download

 Download All

 Delete

 Clear

Local 2022-06 

☐ NAME ↕	EMERGENCY CALLS ↕	CALLER NUMBER ↕	DATE ↕	SIZE ↕	OPTIONS
No Data					

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

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 Calls > Create New Emergency Location Mapping

* ELIN

Geolocation Routing

Send PAI Header ☐

Type

Location Mapping

Add

Delete

☐ Subnet	Location	Options
 No data		

Cancel

Save

Emergency Location Mapping

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

Parameter	Description
ELIN	The emergency location identification number registered with the E911 provider. This number will be sent out as the emergency call's caller ID (CID) number.
Carry Geolocation Routing	If enabled, the UCM sends Geolocation-Routing and Geolocation headers in SIP messages, allowing downstream service providers and vendors to make location-based routing policy decisions for emergency calls.
Geolocation Routing	Toggles whether to include the Geolocation header in the emergency call SIP INVITE message. The Location field value will be used as the Geolocation header value.
Send PAI Header	PAI stands for P-Asserted-Identity. Once enabled, the ELIN number will be sent via the PAI header field to ensure accurate location tracking for emergency services. This PAI header field takes precedence over the PAI header field configured on the trunks.
Type	Selects the mapping method used to identify the caller's location: Network Method: Click Add to map specific IP subnets to location descriptions. Extension Method: Click Add to map specific extension numbers to location descriptions.

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

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

. Configuration parameters are listed in the following table.

Callback Configuration Parameters

Name	Configure a name to identify the Callback. (Enter at least two characters)
CallerID Pattern	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the CallerID match this pattern so that the caller can get callback after hanging up the call. Note: If leaving as blank, all numbers are allowed to use this callback.
Outbound Prepend	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.
Delay Before Callback	Configure the number of seconds to be delayed before calling back the user.
Destination	Configure the destination which the callback will direct the caller to. Two destinations are available: IVR DISA The caller can then enter the desired number to dial out via UCM630xA trunk.

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.

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.

URI	Configure the name of this event list (for example, office_event_list). Please note the URI name cannot be the same as the extension name on the UCM630xA. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions/Extension Groups listed on the local UCM630xA to be monitored in the event list.
Remote Extensions	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.
Special Extensions	Manually enter the remote extensions in the peer/register trunk to be monitored in the event list. Valid format: 5000,5001,9000

Event List Settings

Create New Event List

* URI:	test	
Event Type:	Dialog	
Local Extensions:	☐ 9 items Available Search here ☐ 1003 "Betty" ☐ 1004 ☐ 1005 "Will" ☐ 1006 "Iala" ☐ 1007 "Kiki" < > ↑ ↓ ↶ ↷	

☐ 3 items Selected

☐ 1000 "Mia"

☐ 1001 "John"

☒ 1002 "Chris"

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.

- 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**.

* Name :

Name

* Extension :

7101

Custom Prompt :

None

Upload Audio File

Members :

30 items Available

Search

< >

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

0 item Selected

Search

None

LDAP Phonebook :

1 item Available

Search

< >

☐ ou=GStest,dc=pbx,dc=com

0 item Selected

Search

None

Options

* Prompt Wait Time :

5

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:	John	Last Name:	DOE
Email Address:		* User Password:	*****
* Language:	Default	* Concurrent Registration...	1
Mobile Phone Number:			

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.

Edit IVR: Test

Basic Settings

Key Pressing Events

Press 0:	Dial By Name ▾	DialByNameG... ▾
Press 1:	Select an Opti... ▾	
Press 2:	Select an Opti... ▾	

Dial By Name Group In IVR Key Pressing Events

* Pattern:	.	CallerID Pattern:	<input _\""="" type="text" value="Separate patterns by commas, such as \"/>
Disable This Route:	☐	Prepend Trunk Name:	☐
Prepend User Defined Nam...	☐	Inbound Multiple Mode:	☐
Alert-info:	None	Dial Trunk:	☐
Privilege Level:	Internal	DID Destination:	
Allowed to seamless transfe...			
Default Mode			
* Default Destination:	Dial By Name	DialByNameGP1	

Dial By Name Group In Inbound Rule

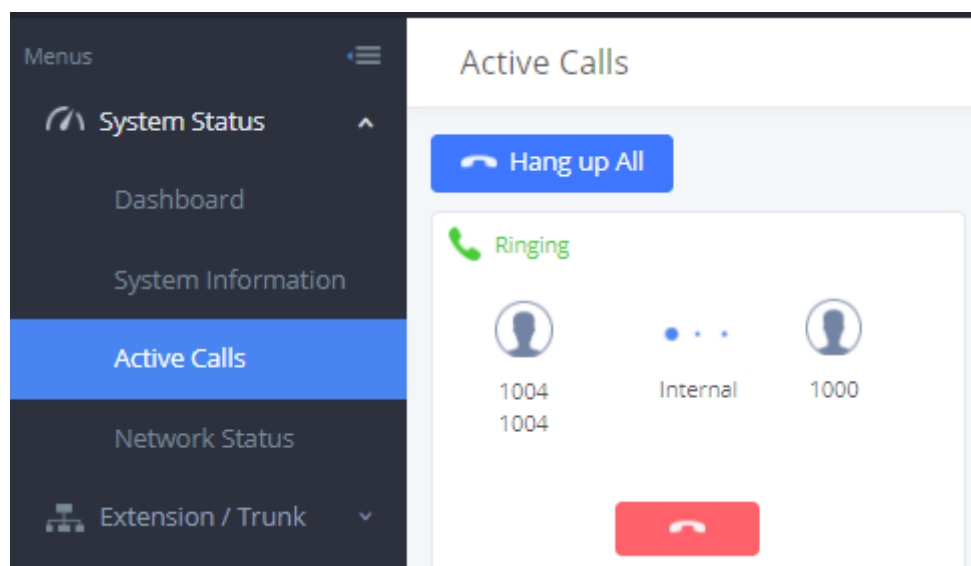
Please refer to [Username Prompt Customization] for User Name Prompt Customization.

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.

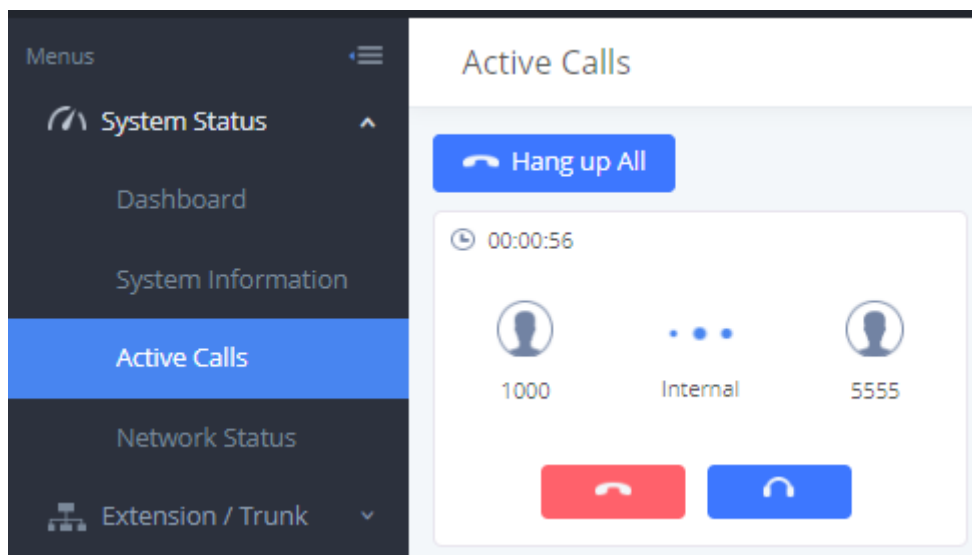
Active Calls Status

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.



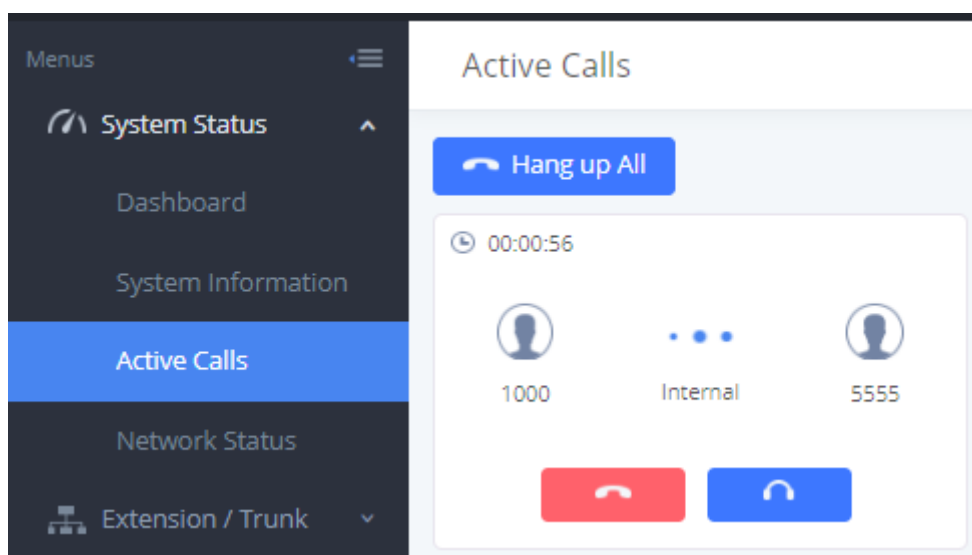
Active Calls Call Ringing

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



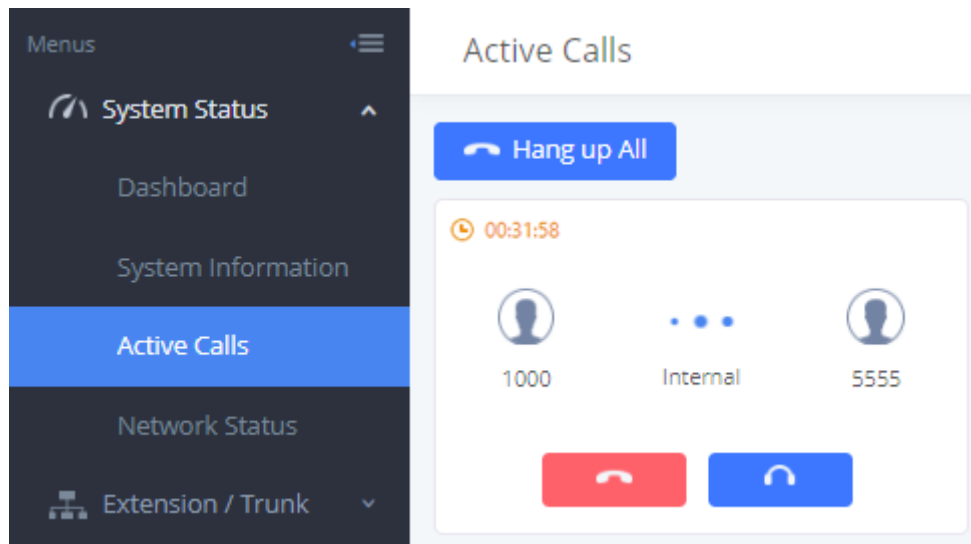
Active Calls Call Established

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.



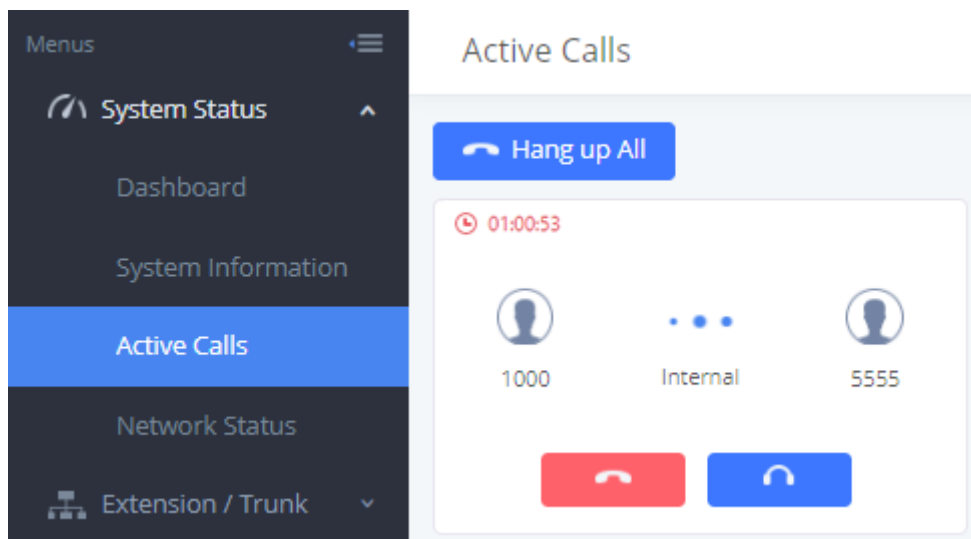
Call Duration Less than 30 Minutes

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 [X]

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 FEATURE

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**.

- 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.
Attended Transfer	- Default code: *2 - Enter the code during active call. After hearing "Transfer", you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. In case of the called party does not answer, users could press *0 to cancel the call and retrieve the first call leg. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Transfer Dialing Timeout Period (s)	Configures the dial timeout period of blind and attended transfers.
 Seamless Transfer	Default code: *44 (Disabled by default). Seamless Transfer allows user to perform blind transfer using PBX feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple. During an active call use the feature code (*44 by default) followed by the number you want to transfer to in order to perform the seamless transfer. (This feature code cannot be nested by other feature codes)
 Start/Stop AI Call Transcription	Allows authorized extension users to manually start or stop AI call transcription dynamically during an active call session. The default feature code for this option is *6(This feature code cannot be nested by other feature codes)
Disconnect	- Default code: *0 - Enter the code during active call. It will disconnect the call. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Call Park	- Default code: #72- Enter the code during active call to park the call. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Feature Code Input Timeout (ms)	Configure the maximum interval (ms) between digits for feature code activation.

Start/Stop Call Recording	-Default code: *3 - Enter the code followed by # or SEND to start recording the audio call and the PBX will mix the streams natively on the fly as the call is in progress. - Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Enable Recording Whitelist	Enable the Recording Whitelist feature
Recording Operation Whitelist	Select extension in the whitelist that can use the *3 recording function.
Feature Code Digits Timeout	Set the maximum interval (ms) between digits for feature code activation
DND/Call Forward	
Call Forward Setting Type	Basic Advanced If Advanced is selected, call forwarding can be set for all calls, internal calls and external calls. To do this, users can dial one of the feature codes below and then dial 0, 1 or 2. The feature code modifiers are as follow: → 0 corresponds to "All calls". → 1 refers to "Internal calls". (calls that came within the PBX) → 2 is used for "External calls". (calls from outside the PBX)
Do Not Disturb (DND) Activate	Default code: *77Activate DND feature to ignore any incoming calls.
Do Not Disturb (DND) Deactivate	Default code: *78Deactivate DND Feature.
 Call Forward Busy Enable	Default Code: *90 Enables Call Forward Busy (CFB) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced.(This feature code cannot be nested by other feature codes)
Call Forward Busy Disable	Default Code: *91Disables Call Forward Busy (CFB) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
 Call Forward No Answer Enable	Default Code: *92 Enables Call Forward No Answer (CFNA) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced.(This feature code cannot be nested by other feature codes)
Call Forward No Answer Disable	Default Code: *93Disables Call Forward No Answer (CFNA) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
 Call Forward Always Enable	Default Code: *72Enables Call Forward Always (CFA) for the dialing extension.Assuming feature code is xxx, the following call forward setting methods are available :Method 1: Dial xxx and follow the system prompts.Method 2: Dial xxx + target extension (e.g., xxx6000).Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000).Methods 1 and 2 are supported in Basic.Methods 1 and 3 are supported in Advanced. (This feature code cannot be nested by other feature codes)
Call Forward Always Disable	Default Code: *73Disables Call Forward Always (CFA) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
Remote Call Forward Enable	Enable this option and configure the Remote Call Forward Whitelist below to allow specific extensions to dial the remote call forwarding feature codes to set call forwarding for any extension.
Remote DND / Call Forward Settings	
Enable	Enable this option and configure the Whitelist below to allow specific extensions to dial feature codes to set DND or call forwarding for any extension.

Remote Call Forward Busy Enable	Default code: *65 Configures and enables CFB for any extension.
Remote Call Forward No Answer Enable	Default code: *66 Configures and enables CFNA for any extension.
Remote Call Forward Always Enable	Default code: *67 Configures and enables CFU for any extension.
Remote DND Enable	Default code: *68 Enables Do Not Disturb for any extension.
Remote Call Forward Busy Disable	Default code: *651 Disables CFB for any extension.
Remote Call Forward No Answer Disable	Default code: *661 Disables CFNA for any extension.
Remote Call Forward Always Disable	Default code: *671 Disables CFU for any extension.
Remote DND Disable	Default code: *681 Disables Do Not Disturb for any extension.
Whitelist	Extensions in this whitelist can configure DND or call forwarding for any extension via feature codes.
Feature Codes	
Voicemail	
 Voicemail Access Code	- Default code: *98 - Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box. (This feature code cannot be nested by other feature codes)
My Voicemail	- Default code: *97 - Press *97 to access the voicemail box.
Voicemail Group Access Code	Default code: *99 Dial this code to access group voicemail. If password is required, enter password followed by the pound (#) key. If Allow Members to Modify Voice Prompts is enabled under Voicemail Group settings, group members dialing *99 can also record, update, or customize voice prompts and greetings for the Voicemail Group via DTMF audio menus.
Direct Dial Voicemail Prefix	Prefix used to dial directly to voicemail.
Call Queue	
 Agent Pause	Default code: *83 Pause the agent in all call queues. (This feature code cannot be nested by other feature codes)
Agent Unpause	Default code: *84 Unpause the agent in all call queues.
Dynamic Agent Logout	Default code: *85 Log the dynamic agent out of all queues.
Call Pickup	
 Pickup on Ringing Prefix	Picks up a ringing call for another extension. Example: If the prefix is **, and there is a call ringing ext 1008, dial **1008 from a different extension to pick up the call to 1008. (This feature code cannot be nested by other feature codes)
Pickup In-call Prefix	Picks up an ongoing call for another extension. Example: If the feature code is *45, and ext 1008 is in a call, dialing *45 and then 1008 following the prompt will take that call. Note: The feature code user must be in the extension's Allowed to seamless transfer list to pick up calls for it.
Pickup Extension	This is the feature code to pick up incoming calls for other extensions in the same pickup group. The default setting is *8.
Call Barging	
Enable Spy	Check this box to enable spy feature codes.

Listen Spy		This is the feature code to listen in on a call to monitor performance. Your line will be muted, and neither party will hear you. The default setting is *54.(This feature code cannot be nested by other feature codes)
Barge Spy		This is the feature code to join in on the call to assist both parties. The default setting is *56.(This feature code cannot be nested by other feature codes)
Whisper Spy		This is the feature code to speak to only one party in the call. For example, you could whisper to employees to help them handle a call. Only an employee on your account will be able to hear you. The default setting is *55.(This feature code cannot be nested by other feature codes)
PMS		
PMS Wakeup Service		Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service.
PMS Remote Wakeup Service		Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions.
Update PMS Room Status		2 methods are available:1. Dial the room status feature code + housekeeper code, listen to the prompt and then the dial the appropriate key for the desired room status. Example: The housekeeper with housekeeper code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available.2. Dial room status feature code*housekeeper code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: Housekeeper with Housekeeper code 0001 dials *23*0001*1 to change room status Available.(This feature code cannot be nested by other feature codes)
Misc		
Paging Prefix		Configure the paging prefix for paging. For example, if the Paging Prefix is set to *81, dial *816000 to initiate a paging call to extension 6000.(This feature code cannot be nested by other feature codes)
Intercom Prefix		Configure the intercom prefix for intercom calls. For example, if the Intercom Prefix is set to *80, dial *806000 to initiate an intercom call to extension 6000.(This feature code cannot be nested by other feature codes)
Blacklist Add		Follow the voice prompt to add a caller ID to blacklist.
Blacklist Last Caller		Add the last inbound caller ID number to blacklist.
Blacklist Remove		Follow the voice prompt to remove a caller ID from blacklist.
Direct Dial Mobile Phone Prefix		If calling mobile phone numbers is permitted, use this prefix plus the extension number to dial the mobile phone number of this extension directly.(This feature code cannot be nested by other feature codes)
Call Completion Request		If the caller wants to use CC to complete a call, he/she can dial this code. After the CC has been registered successfully, the system will start to monitor the status of the callee. The system will call back the caller when the callee's extension is available.

Call Completion Cancel	If the caller has requested CC successfully, and he/she doesn't need to call back anymore, he/she can dial this code to cancel the request.
Presence Status	Dial this feature code to set the presence status of the extension.
Call Flip	- Default code: *46- Dial this code to move the call of this extension from another device to the current device.
Wakeup Service	Dial this feature code to access PBX Wakeup Service. You can add, update, activate or deactivate PBX Wakeup Service.
Remote Extension Privilege Update	Whitelisted extensions will be able to use the Remote Extension Privilege Update feature code to remotely change any extension's outgoing call privilege. Note: After this function has been enabled, the extension in the whitelist can set the privilege for outgoing calls of any extension by dialing the feature code.
Remote Extension Privilege Update Whitelist	Remote Extension Privilege Update Whitelist Procedure: Dial *26 on the whitelisted extension, hear the prompt "Change extension's outgoing permission level, please enter the phone number, then enter # key." After the process, voice will prompt "Press 1 to set to internal, press 2 to set to local, press 3 to set to national, press 4 to set to international." After selecting, it will prompt "Change extension XXXX outgoing permission to XXX", and hang up.
Privileged Call	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.
Privileged Call Whitelist	The extensions in this white list can use the feature code of the privileged call.
 Priority Call	Makes a high priority call to a specified extension by dialing the feature + extension number. If the specified extension is an ongoing call, it will be forcibly hung up to allow the caller to ring the extension. (This feature code cannot be nested by other feature codes)
Priority Call Whitelist	Extension in the whitelist will be allowed to use this feature code to make priority calls.

The UCM630xA also allows user to one click enable / disable specific feature code as shown below:

Feature Codes

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

Cancel Save

Default All

Voicemail

* Voicemail Access Code: *98 ☒

* Voicemail Group Access Code: *99 ☒

* My Voicemail: *97 ☒

* Direct Dial Voicemail Prefix: * ☒

Call Queue

* Agent Pause: *83 ☒

* Dynamic Agent Logout: *85 ☒

* Agent Unpause: *84 ☒

Call Pickup

* Pickup on Ringing Prefix: ** ☒

* Pickup In-call Prefix: *45 ☐

* Pickup Extension: *8 ☒

Call Barging

Enable Spy: ☐

* Listen Spy: *54

* Barge Spy: *56

* Whisper Spy: *55

PMS

* PMS Wakeup Service: *35 ☒

* PMS Remote Wakeup: *37 ☒

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

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

Parking Lot Settings Parking Lot Status

+ Add

EXTENSION ↕	NAME ↕	SLOTS ↕	OPTIONS
700	DefaultLot	701-720	
7000	Dales	7001-7022	

◀

1

▶

Total: 2 10 / page Goto 1

Parking Lot

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

Create New Parking Lot

Cancel
Save

* Parking Lot Extension:

* Parking Slots:

* Parking Timeout (s):

Fallover Destination:

Forward to Destination on Timeout:

☐

* Parking Lot Name:

Use parklot as extension:

☐

Music on Hold Playlists:

Default

Ring-All Callback on Timeout:

☐

New Parking Lot

Parking Lot

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

Call Park

The 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.

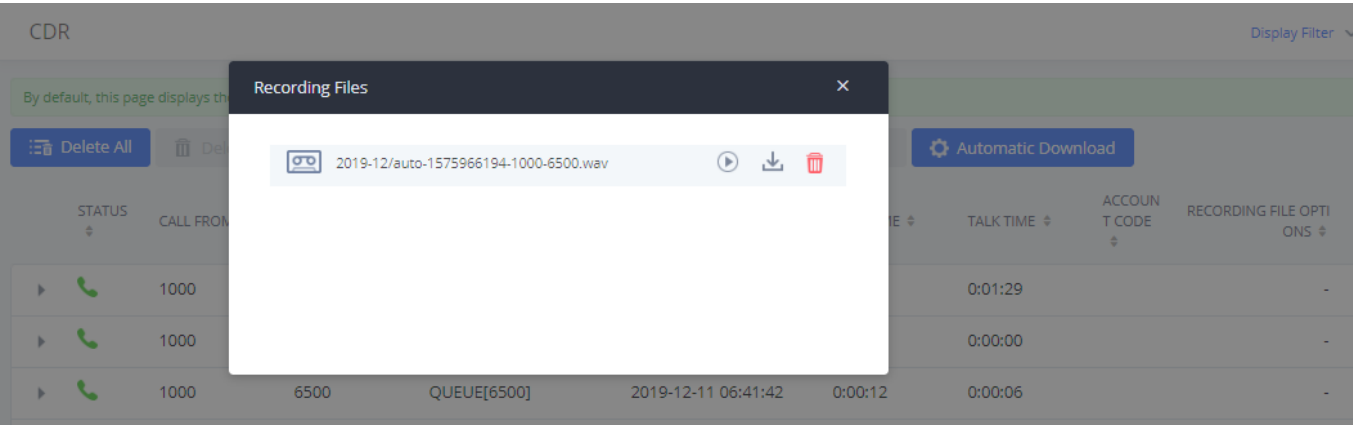
Call Recording

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

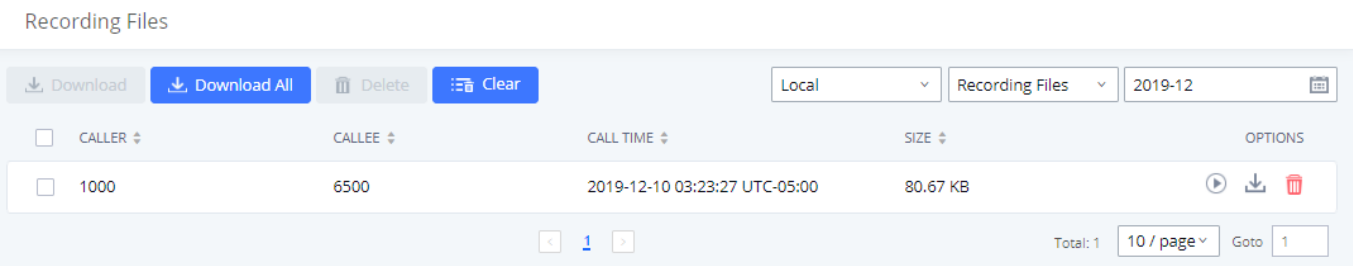
to show and play the recording or click on

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.



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.

"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.

Edit Extension: 1000

Basic Settings Media Features Specific Time Follow Me Cancel Save

General

* Extension:	1000	CallerID Number:	1000
* Permission:	Internal	* SIP/IAX Password:	*****
AuthID:		VoiceMail:	Local VoiceMail
* VoiceMail Password:	*****	Skip VoiceMail Password	☐
Send VoiceMail to Email:	Default	Verification:	
Enable Keep-alive:	☐	Keep VoiceMail after Emailing:	Default
Disable This Extension:	☐	* Keep-alive Frequency:	60
Emergency Calls CID:		Enable SCA:	☒

Enabling SCA option under Extensions 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	+ -

Total: 1 10 / page Goto: 1

3. Configure the private number as desired.

Add Private Number ×

* Private Number:

Related Shared Line:

1000

Enable This Number:

☒

Allow Origination from This Number:

☒

Allow Termination to This Number:

☒

Cancel

Save

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.

Edit SCA Number Group:

* Shared Line Number:

1000

Allow Call Retrieve from

☒

Another Location:

Alert All Appearances for

☐

Group Paging Calls:

Multiple Call Arrangement:

☐

Allow Bridging between

☐

Locations:

Bridge Warning Tone:

Barge-In only

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

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

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

Editing the SCA Number

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

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

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) allows users to set an unskippable audio prompt to play to callers before automatically routing them to a configured destination. Announcements can be assigned as a destination in the Inbound Routes page.

To configure an Announcement, follow the steps below:

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

4. Save and apply the configuration.

Announcement > Edit Announcement: Ave_Maria_Announcement

* Name

Ave_Maria_Announcement

* Prompt ⓘ

English_IVR_Prompt.wav

Add Audio ▾

Default Destination

External Number ▾

* Call Privileges ⓘ

Local ▾

Cancel

Save

Announcement settings

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

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

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

Option	Description
General Preference	

Global Outbound CID Number	Global-level CID Number used for all outgoing calls if no other CID numbers have been configured for the calling party.
Global Outbound CID Name	Global-level CID Name used for all outgoing calls if no other CID names have been configured for the calling party.
Ring Timeout (s)	Number of seconds to ring the extension before forwarding the call to voicemail. Default setting is 60 seconds. If Extensions > Features > Ring Timeout is not configured, this global setting is used.
Call Duration Limit	Block calls for the configured duration. If Extensions > Features > Call Duration Limit and Outbound Routes > Call Duration Limit are not configured, this value is used. Disabled by default.
International Call Prefix	Digits users dial before a country code to place an international call (e.g., 00 or 011). The PBX uses this prefix to detect and classify a dialed number as international for routing, permissions, and PMS billing/records. Input: digits only.
Domestic Long Distance Call Prefix	Digits users dial to reach a national (out-of-area) number within the same country (commonly 0 or 1 in NANP countries). Leave blank if not used.
Local Area Code	The area/city code of the PBX's location, used to normalize local dialing. Input the area/city code without the domestic long-distance prefix.
Station ID	Configures a unique device station identifier for the UCM. Note: This Station ID can be prepended as a prefix to randomly created meeting room numbers (configured under Basic Call Features > Meeting > Meeting Settings), enabling cross-PBX routing so remote extension nodes can dial into random conference rooms via outbound routes.
Enterprise Contact Number	Configures contact phone numbers for the enterprise, which can be selected for inclusion in automated meeting invitations and notifications. Click Add to configure additional numbers.
Recording Settings	
Record Prompt	If enabled, the system will play the voice prompt "This call will be recorded" before recording starts. Disabled by default.
Allow External Numbers to Cancel Recording	If enabled, external calling parties will be given the option to decline call recording.
Merge Same Call Recordings	If enabled, the system merges all recordings created during a call regardless of how many times recording is started and stopped.
Stereo Recording	If enabled, caller and callee audio streams are split into separate audio channels during call recording. Applicable for two-party calls.
Calling Channel	Configures the audio channel assignment for caller and callee when Stereo Recording is enabled (e.g., Right Channel).
Start/Stop Recording Feature Codes	Provides a quick navigation link (Go to Page) to configure in-call recording feature codes under Feature Codes settings.
Extension Preference	
Enable Strong Password	If enabled, enforces a strong password policy for extension registration/user passwords.
Enable Random Password	If enabled, newly created extensions are automatically assigned a randomly generated password.
Send Extension Update Emails	If enabled, an email notification is automatically sent to an extension's configured email address upon creation or modification.
Enable Extension Range	Toggles whether extension ranges are strictly enforced across the IPPBX. Enabled by default. Note: Extension ranges allocate number pools for specific call features and do not dictate the maximum capacity of those features.
User Extensions	Defines the allocated range for user extensions (Default: 1000-6299).
Meeting Extensions	Defines the allocated range for meeting rooms (Default: 6300-6399).
Ring Group Extensions	Defines the allocated range for ring groups (Default: 6400-6499).

Queue Extensions	Defines the allocated range for call queues (Default: 6500-6599).
Voicemail Group Extension	Defines the allocated range for voicemail groups (Default: 6600-6699).
IVR Extensions	Defines the allocated range for IVR menus (Default: 7000-7100).
Dial By Name Extensions	Defines the allocated range for Dial By Name directory services (Default: 7101-7199).
Fax Extension	Defines the allocated range for T.38 Fax extensions (Default: 7200-8200).
Call Flow Number	Defines the allocated range for Call Flow Control numbers (Default: 8300-8499).
Zero Config Extension	
Pick Extensions	Defines the range of extensions (Default: 4000-4999) that can be manually selected from end devices during provisioning via Zero Config.
Auto Provision Extensions	Defines the range of extensions (Default: 5000-6299) automatically assigned to provisioned end devices during Zero Config discovery.
Default Extension Segment	Resets all allocated extension ranges back to factory default values.

PBX Settings/RTP Settings

RTP Settings

Internal Options/RTP Settings

RTP Start	Configure the RTP port starting number. The default setting is 10000.
RTP End	Configure the RTP port ending address. The default setting is 20000.
Strict RTP	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is "Disable".
RTP Checksums	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".
ICE Support	Configure whether to support ICE. The default setting is enabled. ICE is the integrated use of STUN and TURN structure to provide reliable VoIP or video calls and media transmission, via a SIP request/response model or multiple candidate endpoints exchanging IP addresses and ports, such as private addresses and TURN server address.
STUN Server	Configure STUN server address. STUN protocol is a Client/Server and also a Request/Response protocol. It is used to check the connectivity between the two terminals, such as maintaining a NAT binding entries keep-alive agreement. The default STUN Server is stun.ipvideotalk.com. Valid format: [(hostname IP-address) [':' port]] The default port number is 3478 if not specified.
BFCP UDP Start	Configure BFCP UDP port starting number. The default setting is 50000.
BFCP UDP End	Configure BFCP UDP port ending number. The default setting is 52999.
BFCP TCP Start	Configure BFCP TCP port starting number. The default setting is 53000.
BFCP TCP End	Configure BFCP TCP port ending number. The default setting is 55999.
TURN Server	Configure TURN server address. TURN is an enhanced version of the STUN protocol and is dedicated to the processing of symmetric NAT problems.

TURN Server Name	Configure turn server account name
TURN Server Password	Configure turn server account password.
Connection Protocol	Protocol used to connect to the TURN server.
Number of ICE Candidates	This configures the number of pre-collected ICE candidates to gather and send to remote peers. The higher the number, the greater the network traffic consumption.

Payload

The UCM630xA payload type for audio codecs and video codes can be configured here.

Internal Options/Payload

AAL2-G.726	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112.
DTMF	Configured payload type for DTMF. The default setting is 101.
G.721 Compatible	Configure to enable/disable G.721 compatible. The default setting is Yes.
G.726	Configure the payload type for G.726 if "G.721 Compatible" is disabled. The default setting is 111.
iLBC	Configure the payload type for iLBC. The default setting is 97.
OPUS	Configure the payload type for OPUS. The default setting is 123.
Audio FEC Payload Type	Configure the Audio FEC Payload Type. The default setting is 127
Audio RED Payload Type	Configure the Audio RED Payload Type. Default setting is 122
H.264	Configure the payload type for H.264. The default setting is 99.
H.263P	Configure the payload type for H.263+. The default setting is 100 103.
VP8	Configure the payload type for VP8. The default setting is 108.
Main Video FEC	Configure the Main Video FEC
RTP FECC	Configure the RTP FECC
RTX	Configure the RTX
G.722.1	G.722.1:Low-complexity coder, 24kbps.
G.722.1C	G.722.1C:Low-complexity coder, 48kbps.

PBX Settings/Voice Prompt Customization

Record New Custom Prompt

In the 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 :

GSM

▼

Extension :

1000 "Mia"

▼

Cancel

Record

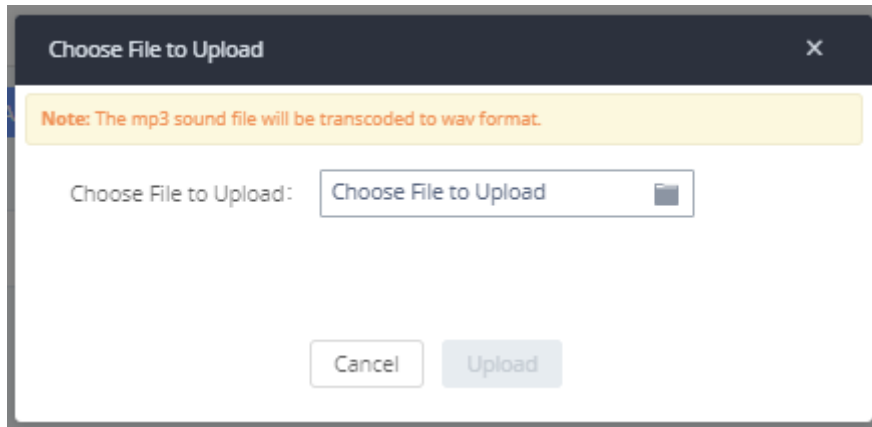
Record New Custom Prompt

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:

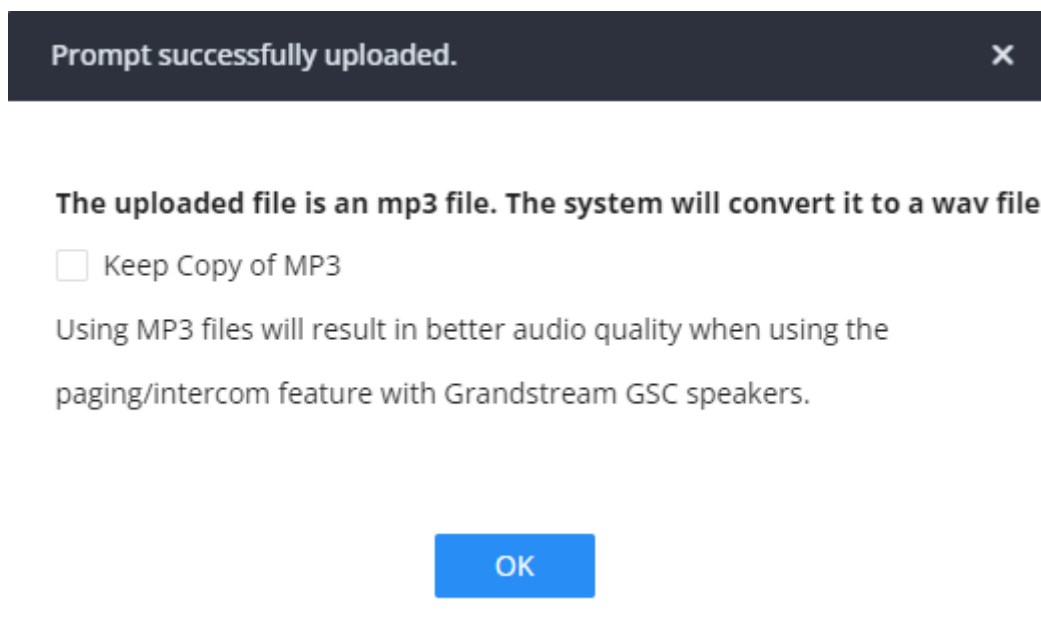
- PCM encoded.
- 16 bits.
- 8000Hz mono.
- In .mp3 or .wav format; or raw/ulaw/alaw/gsm file with .ulaw or .alaw suffix.
- File size under 5M.



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

X

* File Name :

prompt_20170505_091512

Cancel

Download

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 on the UCM helps users choose which prompt will be played by the UCM during call failure, the voice message responses can be set to be played for 4XX, 5XX, and 6XX call failures.

The following **default prompt names** and their associated messages are supported:

Prompt Name	Message Played
sip-trunk-out-busy	"All circuits are busy now. Please try again later."
sip-trunk-out-rejected	"The call was rejected by the server. Please try again later."
sip-trunk-out-server-error	"Server error. Please check your device."
sip-trunk-out-wrong-number	"Your call can't be completed as dialed. Please check the number and dial again."
general-failed	"Your call cannot be completed as dialed."
no-answer	"The number you dialed is not answering. Please try again later."
no-permission	"You are not allowed to dial this number."
user-busy	"The number you have dialed is busy. Please try again later."
wrong-number	"The number you dialed is incorrect. Please check the number and dial again."

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

Call Prompt Tones

[SIP Trunk Prompt Tone](#)

General Call Prompt Tones

Specify the tones to play for various SIP trunk call failure scenarios.

Reset All

Default All

400	sip-trunk-out-busy	401	sip-trunk-out-busy
402	sip-trunk-out-busy	403	sip-trunk-out-rejected
404	sip-trunk-out-wrong-nu...	405	sip-trunk-out-busy
406	sip-trunk-out-busy	407	sip-trunk-out-busy
408	sip-trunk-out-busy	410	sip-trunk-out-busy
413	sip-trunk-out-busy	414	sip-trunk-out-busy
415	sip-trunk-out-busy	416	sip-trunk-out-busy
420	sip-trunk-out-busy	421	sip-trunk-out-busy
423	sip-trunk-out-busy	480	sip-trunk-out-busy
481	sip-trunk-out-busy	482	sip-trunk-out-busy
483	sip-trunk-out-busy	484	sip-trunk-out-busy

Cancel

Save

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

User Busy: user-busy

No Answer: no-answer

Do Not Disturb: user-busy

Call Waiting: Default Ringback Tone

Out Of Service: out-of-service

Trunk Busy: trunk-busy

No Permission: no-permission

General Failed: general-failed

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

General call Failure Prompts

File Manager

The File Manager section defines the storage location and automatic storage switching behavior for files generated by the UCM630x Audio system. Storage is configured separately for each file category. This section determines where new files are written and how the system behaves when multiple storage targets are available.

The following file types are supported:

- **Recording Files**
- **IM Files**

File Manager

① EXT4 is the recommended file system for external storage devices.

Recording Files

Enable Auto Change ☒

Storage Path Priority GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > USB1 (Unavailable) > USB2 (Unavailable) > SD Card (Unavailable) > Local (In Use) Custom

IM Files

Enable Auto Change ☒

Storage Path Priority GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > USB1 (Unavailable) > USB2 (Unavailable) > SD Card (Unavailable) > Local (In Use) Custom

Save

File Manager

Each file category allows the administrator to define the storage path used for newly generated files. Available options depend on system configuration and detected storage devices (e.g., Local storage, GDMS Cloud Storage, USB, NAS).

When Enable Auto Change is enabled, the system stores files according to the defined **Storage Path Priority**. If the active storage device becomes unavailable or reaches capacity, the system automatically

switches to the next available device in the priority list.

After configuring storage paths, administrators should configure external disk usage alerts under **Maintenance->System Events->Alert Events List** to ensure sufficient storage capacity.

Custom Storage Path Priority

×

Change Path Priority

Drag to change the path priority. Files will be automatically stored in order from top to bottom.

GDMS Cloud Storage

NAS

USB1

USB2

SD Card

Local

Cancel

Save

Custom Storage Path Priority

When the storage path for Recording Files is changed from **Local** to an external storage device (such as USB or NAS, if available), the Migrate Local Recordings option becomes available. This option allows existing recordings stored in internal memory to be copied to the newly selected external storage device. The administrator can select specific recording categories to migrate as shown below.

- This option does not appear when switching from Local to GDMS Cloud Storage.
- The function copies existing recordings to the selected storage device and does not delete the original files from local storage.

File Manager

① EXT4 is the recommended file system for external storage devices.
After configuring the storage path, please navigate to the *Maintenance->System Events->Alert Events List* page to enable the *External Disk Usage* alert notifications to ensure that storage space is sufficient.

Recording Files

Enable Auto Change [?](#) ☐

Current Path ☒ USB1 ☐ Local ☐ GDMS Cloud Storage [!](#)

Migrate Local Recordings ☐ All ☒ Basic Call Recordings ☒ Record Meeting ☐ Queue Recordings ☒ SCA Recordings ☐ Emergency Recordings ☐ Paging/Intercom Recordings

IM Files

Enable Auto Change [?](#) ☒

Storage Path Priority [?](#) GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > **USB1 (In Use)** > USB2 (Unavailable) > SD Card (Unavailable) > Local [Custom](#)

Migrate Local Recordings Option

Storage Device Management

NAS

The UCM supports adding and backing up recordings to a network-attached storage (NAS) server.

Storage Device Management

NAS

SFTP

USB Disk/SD Card File Management

Amazon S3

① Please make sure that the NAS is connected and writeable if using it as storage for recordings.

① NOTE: NAS will not be available if the local disk usage exceeds the set threshold.

Enable [?](#)



*Host [?](#)

192.168.6.55

*Folder Path [?](#)

UCM/test

Example: folder1/subfolder2

Username [?](#)

storageuser

Password [?](#)

••••••••



Security Mode [?](#)

None



SMB Protocol Version

3.0



Status

Unavailable

Cancel

Save

The following table describes the configurable NAS settings:

Option	Description
Enable	Check the box to enable Network Attached Storage (NAS) support on the UCM.

Host	Enter the IP address or hostname of the NAS server (e.g., 192.168.6.55).
Folder Path	Configure the directory path on the NAS storage where files will be saved (e.g., folder1/subfolder2).
Username	Enter the username required for authenticating with the NAS storage server.
Password	Enter the password required for authenticating with the NAS storage server.
Security Mode	Select the security authentication mode required by the NAS server (e.g., None, NTLM, NTLMv2).
SMB Protocol Version	Select the Server Message Block (SMB) protocol version used to communicate with the network storage server. Supported Options: 1.0: SMB version 2.0 protocol. 2.0: SMB version 3.0 protocol. 3.0: SMB version 3.0.2 protocol.
Status	Displays the real-time connection status between the UCM and the NAS server (e.g., Available, Unavailable).

If Network Storage Device has 1GB of storage space left, it will be considered unavailable the UCM will trigger the external disk usage alert.

SFTP

SFTP integration offers synchronizing files between from the UCM to the SFTP server. SFTP is used to synchronize the following data: CDR Records, Recording Files, Voicemail, and Fax.

Storage Device Management

NAS

SFTP

USB Disk/SD Card File Management

Please enter the SFTP server information. The SFTP server can be used for regular backups, data sync, packet capture storage, PMS and other data syncing services.

Enable

☒

* Account

SFTP_User

Password

* Server Address

192.168.6.12

Test Connection

Start

Cancel

Save

SFTP Integration

Enable	Tick this box to enable SFTP integration.
Account	Enter the account of the SFTP server.
Password	Enter the password of the account of the SFTP server.
Server Address	Enter the address of the SFTP server.

USB Disk/SD Card File Management

USB Disk/SD Card File Management is a feature which allows to manages the files stored on the USB flash drive attached to the UCM device, or an SD card attached to the system.

Storage Device Management

NAS

SFTP

USB Disk/SD Card File Management

EXT4 is the recommended file system for external storage devices.

No SD card

No USB Device Connected

Delete

☐	Name ▾	Type ▾	Date ▾	Size ▾	Options
No data					

USB Disk/SD Card File Management

Amazon S3

The Storage Device Management module allows you to integrate your UCM63xxA with external cloud storage services. This page provides the option to configure a connection to a third-party Amazon S3 bucket to archive a copy of your critical data, specifically backup files.

This feature is designed for organizations that require an additional, independent copy of their configuration and data for long-term retention, compliance, or disaster recovery purposes, separate from the primary Grandstream cloud storage.

This integration is used for storing backup files to your own S3 bucket. All other system data, such as call recordings and voicemails, will continue to be stored in your primary storage space.

Storage Device Management

NAS

SFTP

USB Disk/SD Card File Management

Amazon S3

Enable



* Region ⓘ

US East (N. Virginia) us-east-2

Please go to [AWS Documentation](#) to search the region



If there is no option, enter the **AWS Region code**, for example, enter "us-east-2" for the eastern part of the United States (Ohio).

* Bucket ⓘ

my-storage-bucket-01

3 - 63 characters, Supports lowercase letters, numbers and special characters.-

* Key ID ⓘ

.....

* Secret Key ⓘ

.....

Test Connection

Start



It is recommended that you perform a connection test during the initial configuration and when modifying the configuration to ensure that it is configured correctly.

Cancel

Save

Amazon S3 Storage Settings

The table below describes the parameters that can be found on the Amazon S3 configuration tab:

Enable	Enables or disables Amazon S3 integration. When enabled, the configuration fields below become editable.
Region	Manually enter, or select from the drop-down list the AWS region where the bucket is located.
Bucket	Enter the name of the S3 bucket. Must be 3-63 characters, lowercase letters, numbers, and hyphens only.
Key ID	Enter the AWS Access Key ID generated after creating an account on the AWS platform. This value is encrypted and cannot be viewed after saving.
Secret Key	Enter the AWS Secret Access Key generated after creating an account. This value is encrypted and cannot be viewed after saving.
Test Connection	Click on this button to Test the connection to AWS S3 with the current settings. Note: It is recommended to perform a connection test during the initial configuration to ensure your UCM can successfully communicate with the Amazon S3 bucket.

SIP SETTINGS

The UCM630xA SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

SIP Settings/General

SIP Settings/General

Realm For Digest Authentication	Configure the host name or domain name for the UCM630xA. Realms MUST be globally unique according to RFC3261. The default setting is Grandstream.
---------------------------------	---

Bind UDP Port	Configure the UDP port used for SIP. The default setting is 5060.
Bind IPv4 Address	Configure the IPv4 address to bind to. The default setting is 0.0.0.0, which means binding to all addresses.
Bind IPv6 Address	Configure the IPv6 address to bind to. The default is : "[::]" and it means to bind to all IP addresses.
Allow Guest Calls	If enabled, the UCM630xA allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is "No". Warning: Please be aware of the potential security risk when enabling "Allow Guest Calls" as this will allow any user with the UCM630xA address to dial into the UCM630xA.
Allow Transfer	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".
MWI From	When sending MWI NOTIFY requests, this value will be used in the "From:" header as the "name" field. If no "From User" is configured, the "user" field of the URI in the "From:" header will be filled with this value.
Enable Diversion Header	If disabled, the UCM will not forward the diversion header.
Block Collect Calls	If enabled, collect calls will be blocked. Note: Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call".

SIP Settings/MISC

Parameter	Description
Outbound SIP Registrations	
Register Timeout	Configure the register retry timeout (in seconds). The default setting is 20.
Register Attempts	Configure the number of registration attempts before the UCM630X gives up. The default setting is 0, which means the UCM630X will keep trying until the server side accepts the registration request.
Initial REGISTER Delay Interval (s)	Configures the time window within which to send initial trunk registration requests. Instead of sending out all initial trunk registration requests at once, requests will be randomly sent out within this period. The default setting is 10.
Video	
Support SIP Video	Select to enable video support in SIP calls. The default setting is "Yes".
Security	
Reject Non-Matching INVITE	If enabled, when rejecting an incoming INVITE or REGISTER request, the UCM630X will always reject with "401 Unauthorized" instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. Default setting is "No".
SDP Attribute Passthrough	
Enable Attribute Passthrough	If enabled, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passed through.
Early Media	
Enable Use Final SDP	If enabled, call negotiation will use final response SDP.
Ignore 180 Response	If enabled, ringing indication after 183 response will be ignored.
Transfer	
Allow Transfer	If checked, all transfers initiated by endpoints will be enabled.

Allow callback when blind transfer fails	If enabled, the UCM will call back to the transferrer when blind transfer fails (reason of failure includes busy and no answer). Note: This feature takes effect only on internal calls.
Blind transfer timeout	Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s.
Allow Early Blind Transfer	Enabling this allows callers to perform transfers while the original callee's phone is still ringing during attended transfer. Note: Requires compatible endpoints such as Grandstream GRP261x on firmware 1.0.15.8 or higher.
Hold	
Forward HOLD Requests	Configure the UCM to forward HOLD requests instead of processing holds internally. This serves to meet the standards set by some providers that require HOLD requests to be passed along from endpoint to endpoint. This option is disabled by default. Note: Enabling this option may cause hold retrieval issues and MOH to not be heard.

Transparent Call-info Header

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

```

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

```

SIP Settings/Session Timer

SIP Settings/Session Timer

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

SIP Settings/TCP and TLS

SIP Settings

<

General

Session Timer

TCP/TLS

NAT

ToS

STIR/SHAKEN

>

Cancel

Save

TCP Enable

☒

TCP Bind IPv4 Address

0.0.0.0:5060

TCP Bind IPv6 Address

:::5060

TLS Enable

☒

TLS Bind IPv4 Address

0.0.0.0:5061

TLS Bind IPv6 Address

:::5061

TLS Do Not Verify

☒

TLS Self-signed CA

TLS.ca

Reset Certificates

Private Certificate and Key

TLS Cert

TLS.crt

TLS Key

TLS.key

Reset Certificates

Cipher Suite

Cipher Blacklist

☐

© 2023 Grandstream Networks, Inc.

TCPTLS

SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the PBX. The default setting is "No".
TCP Bind IPv4 Address	Configure the IP address for the TCP server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 5060. For example, 192.168.1.1:5062.
TCP Bind IPv6 Address	Configure the IPv6 address for the TCP server to bind to. ":::" means bind to all interfaces. The port number is optional with the default being 5060. For example, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5060.
TLS Enable	Configure to allow incoming TLS connections with the PBX. The default setting is "Yes".
TLS Bind IPv4 Address	Configure the IPv4 address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 5061. For example, 192.168.1.1:5063. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.
TLS Bind IPv6 Address	Configure the IPv6 address for TLS server to bind to. ":::" means bind to all interfaces. The port number is optional with default being 5061. For example, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5061. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.

TLS Do Not Verify	If enabled, the TLS server's certificate will not be verified when acting as a client. The default setting is "Yes".
TLS Self-Signed CA	This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server's public key. This file will be renamed as "TLS.ca" automatically. Notes: Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca. DER-formatted certificates are supported and will automatically be converted to PEM format upon upload. The size of the uploaded certificate file must be under 2MB.
Reset Certificates	Clicking on this button will reset the certificates.
Private Certificate and Key	
TLS Cert	Upload the certificate file used for TLS connections. It must contain the client's private key and the server's signed certificate. Uploaded files will automatically be saved as "TLS.crt". Notes: Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca. DER-formatted certificates are supported and will automatically be converted to PEM format upon upload. The size of the uploaded certificate file must be under 2MB.
TLS Key	This file must be named with the CA subject name hash value. It contains CA's (Certificate Authority) public key, which is used to verify the accessed servers. This file will be renamed as "TLS.key" automatically. Notes: Supported file extensions include .crt, .cer, .der, .pem, .key, and .ca. DER-formatted certificates are supported and will automatically be converted to PEM format upon upload. The size of the uploaded certificate file must be under 2MB.
Reset Certificates	Clicking on this button will reset the certificates.
Cipher Suite	
Restrict Cipher List	By default, all SIP TLS encryption suites are in effect on the system, and when turned on, you can configure the encryption suites allowed to be used.
Cipher Suite	Select the encryption suites that are allowed to be used for SIP TLS connections, in the order of priority as configured.

SIP Settings/NAT

SIP Settings/NAT

External Host	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.
Use IP address in SDP	If enabled, the SDP connection will use the IP address resolved from the external host.
External UDP Port	Configure externally mapped UDP port when the PBX is behind a static NAT or PAT.
External TCP Port	Configure the externally mapped TCP port when the UCM630xA is behind a static NAT or PAT.
External TLS Port	Configures the externally mapped TLS port when UCM630xA is behind a static NAT or PAT.
Local Network Address	Specify a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly. A sample configuration could be as follows: 192.168.0.0/16

SIP Settings/ToS

SIP Settings/ToS

ToS for SIP	Configure the Type of Service for SIP packets. The default setting is None.
ToS for RTP Audio	Configure the Type of Service for RTP audio packets. The default setting is None.
ToS for RTP Video	Configure the Type of Service for RTP video packets. The default setting is None.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120.
Max Registration/Subscription Time	Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the UCM630xA. The default setting is 3600.
Min Registration/Subscription Time	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM630xA. The default setting is 60.
Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".
DTMF Mode	Select DTMF mode to send DTMF. The default setting is RFC4733. If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, a-law or u-law are required. When "Auto" is selected, "RFC4733" will be used if offered, otherwise "Inband" will be used. The default setting is "RFC4733".
RTP Timeout	During an active call, if there is no RTP activity within the timeout (in seconds), the call will be terminated. The default setting is no timeout. Note: This setting does not apply to calls on hold.
RTP Hold Timeout	When the call is on hold, if there is no RTP activity within the timeout (in seconds), the call will be terminated. This value of RTP Hold Timeout should be larger than RTP Timeout. The default setting is no timeout.
RTP Keep-alive	This feature can be used to avoid abnormal call drop when the remote provider requires RTP traffic during proceeding. For example, when the call goes into voicemail and there is no RTP traffic sent out from UCM, configuring this option can avoid voicemail drop. When configured, RTP keep-alive packet will be sent to remote party at the configured interval. If set to 0, RTP keep-alive is disabled.
100rel	Configure the 100rel setting on UCM630xA. The default setting is "Yes".
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted. The default setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
Generate In-Band Ringing	Configure whether the UCM630xA should generate Inband ringing or not. The default setting is "Never". Yes: The UCM630xA will send 180 Ringing followed by 183 Session Progress and in-band audio. No: 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. Never: 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.
Server User Agent	Configure the user agent string for the UCM630xA.
Send Compact SIP Headers	If enabled, compact SIP headers will be sent. The default setting is "No".
Passthrough PAI Header	Passthrough PAI Header

SIP Settings/STIR/SHAKEN

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

SIP Settings

General
Session Timer
TCP/TLS
NAT
ToS
STIR/SHAKEN
Misc

+ Add
Delete
Certificate Settings

Q Authentication Number

☐ AUTHENTICATION NUMBER
DEVICE NAME
CREDITABILITY
OPTIONS

No Data

STIRSHAKEN

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

Add Authentication Number

* Authentication Number:

* Device Name:

Grandstream

* Creditability:

Cancel

Save

Add Authentication Number

SIP Settings/STIR/SHAKEN - Add Authentication Number Settings

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

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

Certificate Settings

×

* Certificate Download

2

Time (s):

* Signature Valid Time (s):

15

* Private Key:

private.key

* Public Key:

public.crt

Cancel

Save

Certificate Settings

SIP Settings/STIR/SHAKEN - Certificate Settings

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

Transparent Call-Info header

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

```
[-] 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

Bind Port	Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569.
Bind IPv4 Address	Force IAX2 to bind to a specific address instead of all addresses.
Bind IPv6 address	Configure the IPv6 address to bind to. "[::]" means to bind to all IP addresses.
IAX1 Compatibility	Select to configure IAX1 compatibility. The default setting is "No".
No Checksums	If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this feature. The default setting is "No".
Delay Reject	If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is "No".
ADSI	Select to enable ADSI phone compatibility. The default setting is "No".
Music On Hold Interpret	Specify which Music On Hold class this channel would like to listen to when being put on hold. This music class is only effective if this channel has no music class configured and the bridged channel putting the call on hold has no "Music On Hold Suggest" setting.
Music On Hold Suggest	Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold.
Bandwidth	Configure the bandwidth for IAX settings. The default setting is "Low".

IAX Settings/Registration

IAX Settings/Registration

IAX Registration Options

Min Reg Expire	Configure the minimum period (in seconds) of registration. Default setting is 60.
Max Reg Expire	Configure the maximum period (in seconds) of registration. Default setting is 3600.
IAX Thread Count	Configure the number of IAX helper threads. The default setting is 10.
IAX Max Thread Count	Configure the maximum number of IAX threads allowed. The default is 100.
Auto Kill	If enabled and no ACK is received for new messages after the specified wait time, the connection will be terminated.
Authentication Debugging	If enabled, authentication traffic in debugging will not show. The default is "No".
Codec Priority	Configure codec negotiation priority. The default setting is "Reonly". Caller Consider the callers preferred order ahead of the host's. Host Consider the host's preferred order ahead of the caller's. Disabled Disable the consideration of codec preference all together. Reonly This is the same as "Disabled", except when the requested format is not available. The call will only be accepted if the requested format is available.
Type of Service	Configure ToS bit for preferred IP routing.
IAX Trunk Options	
Trunk Frequency	Configure the frequency of trunk frames (in milliseconds). The default is 20.
Trunk Time Stamps	If enabled, time stamps will be attached to trunk frames. The default is "No".

IAX Settings/Security

IAX Settings/Static Defense

Call Token Optional	Enter a single IP address (e.g., 1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) for which call token validation is not required.
Max Call Numbers	Configure the maximum number of calls allowed for a single IP address.
Max Unvalidated Call Numbers	Configure the maximum number of Unvalidated calls for all IP addresses.
Max Call Numbers	Configure to limit the number of calls for a give IP address of IP range.
IP or IP Range	Enter the IP address (1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) to be considered for call number limits.

INTERFACE SETTINGS

Analog Hardware

The analog hardware (FXS port and FXO port) on the 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

Tone Region	Select country to set the default tones for dial tone, busy tone, ring tone and etc. to be sent from the FXS port. The default setting is "United States of America (USA)".
Advanced Settings	
FXO Opermode	Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)".
FXS Opermode	Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)".
FXS TISS Override	Configure to enable or disable override Two-Wire Impedance Synthesis (TISS). The default setting is No. If enabled, users can select the impedance value for Two-Wire Impedance Synthesis (TISS) override. The default setting is 600 Ω .

PCMA Override	Select the codec to be used for analog lines. North American users should choose PCMU. All other countries, unless already known, should be assumed to be PCMA. The default setting is PCMU. Note: This option requires system reboot to take effect.
Boost Ringer	Configure whether normal ringing voltage (40V) or maximum ringing voltage (89V) for analog phones attached to the FXS port is required. The default setting is "Normal".
Fast Ringer	Configure to increase the ringing speed to 25HZ. This option can be used with "Low Power" option. The default setting is "Normal".
Low Power	Configure the peak voltage up to 50V during "Fast Ringer" operation. This option is used with "Fast Ringer". The default setting is "Normal".
Ring Detect	If set to "Full Wave", false ring detection will be prevented for lines where Caller ID is sent before the first ring and proceeded by a polarity reversal, as in UK. The default setting is "Standard".
FXS MWI Mode	Configure the type of Message Waiting Indicator on FXS lines. The default setting is "FSK". FSK: Frequency Shift Key Indicator NEON: Light Neon Bulb Indicator.
FXO Frequency Tolerance	Allows users to adjust the tolerance of the FXO ringing frequency. 63Hz is considered the standard value and is selected by default.

DAHDI Settings

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

Interface Settings

Analog Hardware **DAHDI Settings**

* Analog Buffers: 32,half

* Fax Buffers Policy: 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.

"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.

Contact Management

Extension Contacts

External Contacts

Change Department

Contact Privilege Settings

Delete

Q Extension Number or Name

Search

☐	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)	 

<

1

2

>

Total: 11

10 / page

Goto

1

Extension Contacts

"Delete" extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

Click Edit icon to configure name, department, email address and etc for each extension contact.

* 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

Extension	Displays extension number.
First Name	Configure first name for the extension contact.
Last Name	Configure last name for the extension contact.
Department	Select department for the extension contact. Department can be created in "Department Management" page.
Department Title	Configure the job title for the extension contact.
Email Address	Configure email address for the extension contact.
Mobile Phone Number	Configure mobile phone number for the extension contact.
Home Number	Configure home number for the extension contact
Fax	Configure Fax for the extension contact.
Same as Department Contact Privileges	When this option is enabled, the contact extension will inherit the same privilege as the department it belongs to.
Contact View Privileges	This option allows configuring privileges for the contact extension. Note: This option will be disabled if "Same as Department Contact Privileges" has been enabled.

- External contacts

On external contacts page, the admin can create single external contact, import contacts in batch, edit contacts, delete contacts and export contacts.

Contact Management

Extension Contacts External Contacts

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

Phone Number or Name
 [Search](#)

☐	MOBILE PHONE NUMBER	NAME	DEPARTMENT	EMAIL ADDRESSES	REMARK	OPTIONS
☐	55555555	Sadie Adler	Sales	adler.s@mycompany.com		Edit Delete

[<](#)
[1](#)
[>](#)
 Total: 1
 / page
 [Goto](#)

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:

- **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.

Contacts

Contact Manage

Extension Conta

[+ Add](#)

☐ MOBILE

☐ 555555

Import [×](#)

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.

On Duplicate External

Contacts:

Extension File:

[Cancel](#)
[Upload](#)

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

+ Add	
--- (9)	
Quality Control	
Finance	
Marketing	
Technical Support	
Sales (1)	
Human Resources	
IT	
Logistics	

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

×

* Department Name :

Marketing

Upper Level

▼

Department :

* Contact View Privileges :

Department & Sub-Department... ▼

Add / Edit Privileges

Privileges Applied To

☐

Sub-Level

Departments :

Cancel

OK

Edit Department

Department Name	Enter the name of the department.
Upper Level Department	Select the upper level department if the department being created is a nested department.
Contact View Privileges	All Contacts?: The extensions in this department will be able to see all the contacts. Department & Sub-department Contacts: The extensions in this department will only be able to see the contacts which are in the same department or in sub-departments.
Set as Shared Department	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.
Share to Following Sites	Pick the sites to which you want to share this specific department.

The user can create up to 100 departments with up to 4 levels of nested departments.

To be able to use shared department, the UCM devices will have to be subscribed to a RemoteConnect plan that offers Cloud IM service. For more information please refer to: <https://ucmrc.gdms.cloud/plans>

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

+ Add		
NAME	PRIVILEGE STATUS	OPTIONS
All Contacts	In Use	
Department & Sub-Department Contacts	Not Applied	

<

1

>

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

Support

Show Agent's Real Name

Cancel

Save

Live Chat Configuration

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

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

Enterprise Administrator

* Message Content

* Recipients

Search

Company Contact

☐ All

☐ Technical Support

☐ Quality Control

☐ Sales

☐ IT

☐ Marketing

☐ Human Resources

☐ Finance

☐ 1000 " "

Selected(0)

Cancel

Send

Message Broadcast Configuration

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

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

+ Add

Edit Allowed Members

Delete

Import

Export

☐	STATUS ▾	DEVICE NUMBER ▾	DEVICE NAME ▾	URL ▾	OPTIONS
☐	● Unmonitored	4001	GSC3620	rtsp://192.168.5.74:554	

< 1 >

Total: 1

10 / page ▾

Goto 1

IP Camera Devices

Edit the IPC device settings in the table below.

IPC Devices Settings

Device Number	The number that allowed members can dial to access the IP camera.
Device Name	Enter the name that you want to allocate for the device.
Protocol	The media control protocol used. RTSP
IP Address	Enter the IP address of the IP camera.
Port	Enter the port of the IP camera. The default is 554
Channel Path	If you want to view the stream of the specified channel, please configure the path of this stream.
Username	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Password	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Transmission Protocol	Transport protocol of the IP camera. Default is UDP.
Heartbeat Detection	If enabled, the PBX will regularly send RTSP OPTIONS to check of the device is still online.
Allowed Members	Extensions, Extension Groups, and Departments can be selected to access this IP camera by dialling the configured Device Number.

Create New IP Camera Devices

Cancel
Save

General

* Device Number:

* Device Name:

* Protocol: RTSP

* IP Address:

* Port: 554

Channel Path:

Username:

Password:

* Transmission Protocol: UDP

Heartbeat Detection: ☐

User Settings

* Allowed Members:

Selected(0)

Company Contact

☐ All
 ☐ 1005
 ☐ 2004
 ☐ 2003

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

IP Camera Device Configuration

REMOTECONNECT

An integrated and essential component of Grandstream's GDMS cloud-based device management service, UCM RemoteConnect runs on Amazon Web Services (AWS) and provides high-availability remote communication and collaboration services.

UCM RemoteConnect enables work from home and mobile users to securely access UCM services using Grandstream Wave softphones, with license-free WebRTC-based communication, automatic NAT traversal, and centralized cloud-based management. In addition, RemoteConnect provides GDMS cloud storage, Cloud IM, AI Services, and other collaboration and management features.

The RemoteConnect service can be configured from the UCM Web GUI under the **RemoteConnect** tab.

For more information about the UCM RemoteConnect services, please refer to the UCM RemoteConnect - User Guide.

Plan

This section provides an overview of the RemoteConnect service associated with the UCM, including service description, current subscription status, and configurable plan options.

Service Description

After the UCM is added to GDMS, RemoteConnect enables automated SIP extension synchronization, Media NAT Traversal, and basic statistics without requiring manual configuration. These services allow remote users and devices to connect reliably through the cloud.

This tab provides an overview of the UCMRC services and displays the current subscription plan, as well as related links and learning resources for the services supported by RemoteConnect.

RemoteConnect

[Plan](#)[AI Services](#)[Beta](#)[Integrated Customer Service](#)[Enterprise UI Customization](#)[Statistics](#)[GDMS Cloud Storage Space](#)

[Service Description](#)[My Plan](#)[Plan Settings](#)

Current Plan: Enterprise with Add-on (Active)[Renewal/Upgrade](#)[Learn about UCMRC](#)[UCMRC User Guide](#)

Grandstream has launched the UCM RemoteConnect service, a remote communications solution that offers TURN penetration capabilities to meet the needs of those working in home offices or out on business trips. Additionally, it offers cloud storage space, Cloud IM, add-in integrations and other collaboration features.

Remote Communication

[How to configure and use](#)[How to configure endpoints](#)[Notify Employees to Use](#)

Use Wave to make/receive calls, schedule and start up meetings with colleagues remotely and easily invite outside parties to join in on meetings for cost-effective communication.

Remote Management of UCMs and Endpoints

[Learn more](#)[How to Manage Remotely](#)[Log into GDMS](#)

Use GDMS to deploy, provision, monitor, and diagnose UCM6300 series devices and registered endpoints. The GDMS mobile app is also available to allow users to manage their devices right from their mobile device.

Wave – Communicate & Collaborate From Anywhere

[Learn more](#)[How to Use Wave](#)[Notify Employees to Use](#)

Available on desktop, web, Android and iOS, Wave gives your team the power to communicate and collaborate from anywhere and anytime on any device. Whether they're in the office, traveling or working from home, Wave provides easy access to voice and video calling, meetings, instant messaging and more.

Wave Integration

[Learn About Wave SDK](#)[Learn About Wave Add-ins](#)

Wave can be integrated with a wide variety of services and applications, including popular CRM platforms, WebRTC, SIP trunks, WhatsApp, Office365 and more. Wave also provides an SDK that allows it to be integrated with your apps and services.

Expand UCM Storage

[How to configure and use](#)

Cloud IM Server

[Learn more](#)[User Manual](#)

RemoteConnect Service Description Tab

My Plan

This page displays detailed information about the currently active RemoteConnect subscription, including plan name, expiration date, concurrent session limits, remote registration limits, call time limits, allocated GDMS cloud storage space, Wave RemoteConnect addresses, and support status for Wave add-ins, Cloud IM Server, and AI features.

RemoteConnect

[Plan](#)[AI Services](#) [Beta](#)[Integrated Customer Service](#)[Enterprise UI Customization](#)[Statistics](#)[GDMS Cloud Storage Space](#)[Service Description](#)[My Plan](#)[Plan Settings](#)

Plan Name	Enterprise with Add-on (Active) 
	AI Transcript × 2
Plan Expiration Date	Until 2030-12-14
Max Remote Concurrent Sessions 	64
Max Remote Registrations 	400
Max Remote Call Time	
Per Call 	Unlimited
Per Day 	Unlimited
Per Month 	Unlimited
GDMS Cloud Storage	10 GB
STUN Address	161.189.44.114
Wave RemoteConnect Address 	 
IP Endpoint/Trunk RemoteConnect Address 	 
Wave 3rd Party Add-ins 	Supported
Cloud IM Server	Supported
AI Features	Supported

RemoteConnect My Plan Tab

Plan Settings

This tab allows administrators to configure how the UCM interacts with UCMRC services, including SIP synchronization, NAT traversal, cloud storage, backups, and remote access behavior. All settings on this page take effect immediately after saving and directly impact how the UCM integrates with GDMS and cloud services.

RemoteConnect
Plan
AI Services
Beta
Integrated Customer Service
Enterprise UI Customization
Statistics
GDMS Cloud Storage Space

Service Description
My Plan
Plan Settings

Bound Enterprise: cl
Service Site: US
Organization: Default

Subscription

Subscription Package Status ⓘ

General

SIP Extension Sync ⓘ

Media NAT Traversal Service ⓘ

Automatically Update the External Host Address for Wave ⓘ

Alert Events Sync ⓘ

Remote Login Settings ⓘ

Storage & Backup

GDMS Cloud Storage ⓘ

CDR Stored in GDMS Cloud ⓘ

Back up to GDMS

RemoteConnect Plan Settings Tab

The table below describes the configurable parameters on this page.

Subscription	
Subscription Package Status	Once enabled, the configured email address will receive notifications about the UCMRC package status such as expiration or low balance.
Email	The email entered in this field will receive updates regarding subscription status.
General	
SIP Extension Sync	Enables synchronization of SIP extensions between the UCM and GDMS. When enabled, all SIP extensions on the UCM are automatically exported to GDMS.
Media NAT Traversal Service	Enables automatic TURN based NAT traversal for remote users and devices. When enabled, any defined NAT traversal or TURN settings configured locally on the UCM are overridden.
Automatically Update the External Host Address for Wave	Controls whether the Wave external host address is automatically synchronized from UCMRC. Disable this option to retain a user defined Wave domain or external address.
Alert Events Sync	Synchronizes alarm and event information generated on the UCM to the GDMS platform.
Remote Login Settings	Opens the configuration page for managing passwordless remote access to the UCM.
Storage & Backup	
GDMS Cloud Storage	Enables cloud storage services provided by GDMS. This option must be enabled to use cloud-based storage features. Notes:Even if this option is disabled, users will still be able to retrieve data/files stored on GDMS.The UCM will automatically turn on the GDMS Cloud Storage alert event option if this feature is enabled.
CDR Stored in GDMS Cloud	If enabled, UCM CDR data will be synced to the GDMS server at 2 AM on the 1st of each month based on the UCM's system time.

Back up to GDMS	Opens the backup configuration page, allowing UCM configuration backups to be stored in GDMS cloud storage.
Recordings Stored in GDMS Cloud	Opens the file manager configuration page, where administrators can control if call recordings are stored in GDMS cloud storage.
Chat Data Cloud Storage	Opens the file manager configuration page, where administrators can control the chat data storage, allowing instant messaging data to be stored in GDMS cloud storage.
Passwordless Remote Access	
Enable Passwordless Remote Access	Allows authorized GDMS users to access the UCM without entering the local UCM account password.

When "SIP Extension Sync" is enabled, the accounts synchronized to GDMS platform can be viewed on the **GDMS->VoIP Account->SIP Account** page. As shown in the figure below:

GDMS Unified Communications

Plans & Services

EU Region

Dashboard

Organization

HA TEST

Overview

Extension

SIP Account

SIP Server

UCMRC

CloudUCM

VoIP Device

Call Quality

Device Template

Site

Task

Diagnostics

System

Resources

SIP Account

How to batch edit accounts?

+ Add Account

Import Account

Export Account

There are currently 1 PBX devices that have not synced extensions. Fix Now

Delete

Modify SIP Server

From All

All Statuses

All SIP Servers

Site

Q User ID/Account/Name/Device Name/MAC

☐	User ID	Account Name	Display Name	Extension Email	SIP Server	Status	Last Updated	Options
☐	1002	1002	—	—	local_20241227110435_1...	Unassigned	2024/12/27 11:04	
☐	1003 PBX	1003	—	—	192.168.6.67:5060,c074a...	Unassigned	2025/01/06 18:51	
☐	1002 PBX	1002	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	1001 PBX	1001	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	1000 PBX	1000	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	3004 PBX	3004	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	3003 PBX	3003	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	3002 PBX	3002	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	3001 PBX	3001	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	
☐	3000 PBX	3000	—	—	192.168.6.67:5060	Unassigned	2025/01/06 18:51	

Total 30110/page123456...31>

© 2025 Grandstream Networks, Inc. Cookies

UCM SIP Extensions synchronized to GDMS

- Deleting an account on GDMS only removes the association between the account and the device, and does not delete the SIP account information on UCM.
- Any creation, deletion or modification of the SIP account on UCM will be automatically synchronized to the GDMS cloud platform.

AI Services

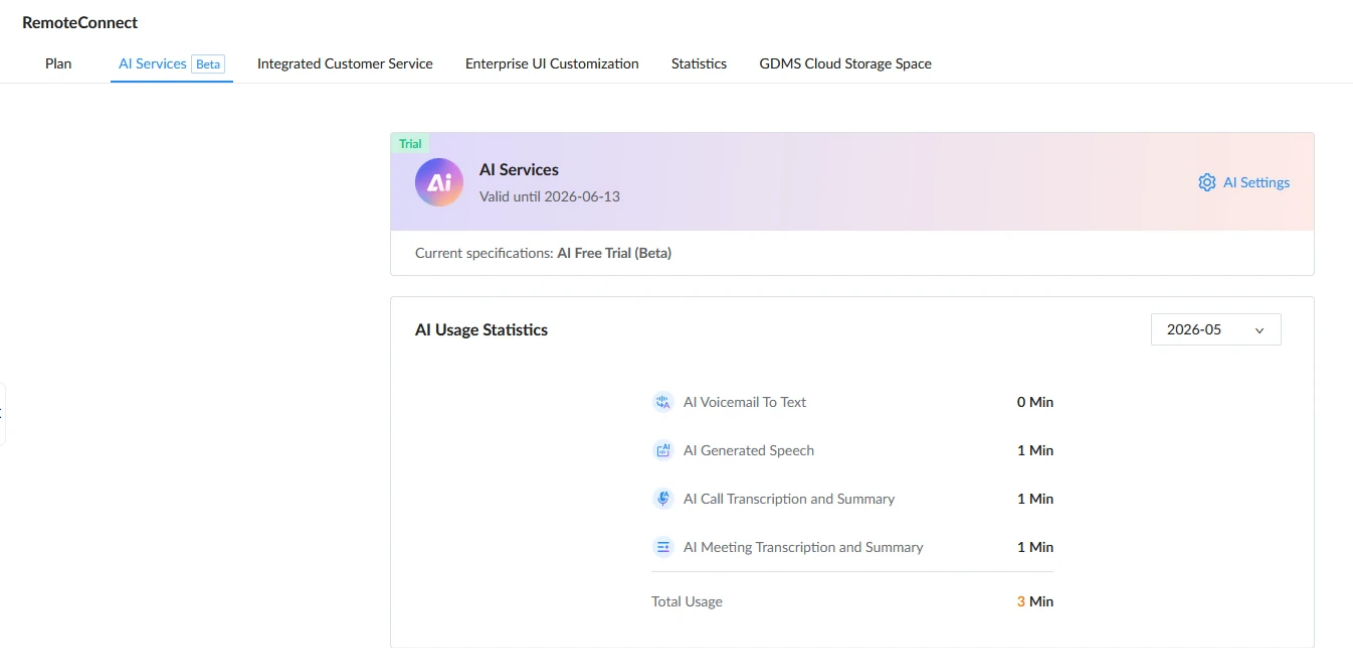
This section displays AI related service status and usage information for the UCM. It provides visibility into the active AI plan, its validity period, and detailed usage statistics. Users can also jump to configure AI Settings from this page.

Supported AI features include:

- AI Voice Message to Text
- AI Generated Speech (Text-to-Speech)
- AI Call Transcription and Summary

- AI Conference Transcription and Summary

Usage statistics show monthly consumption per feature and total usage versus the available quota, helping administrators monitor AI resource usage.



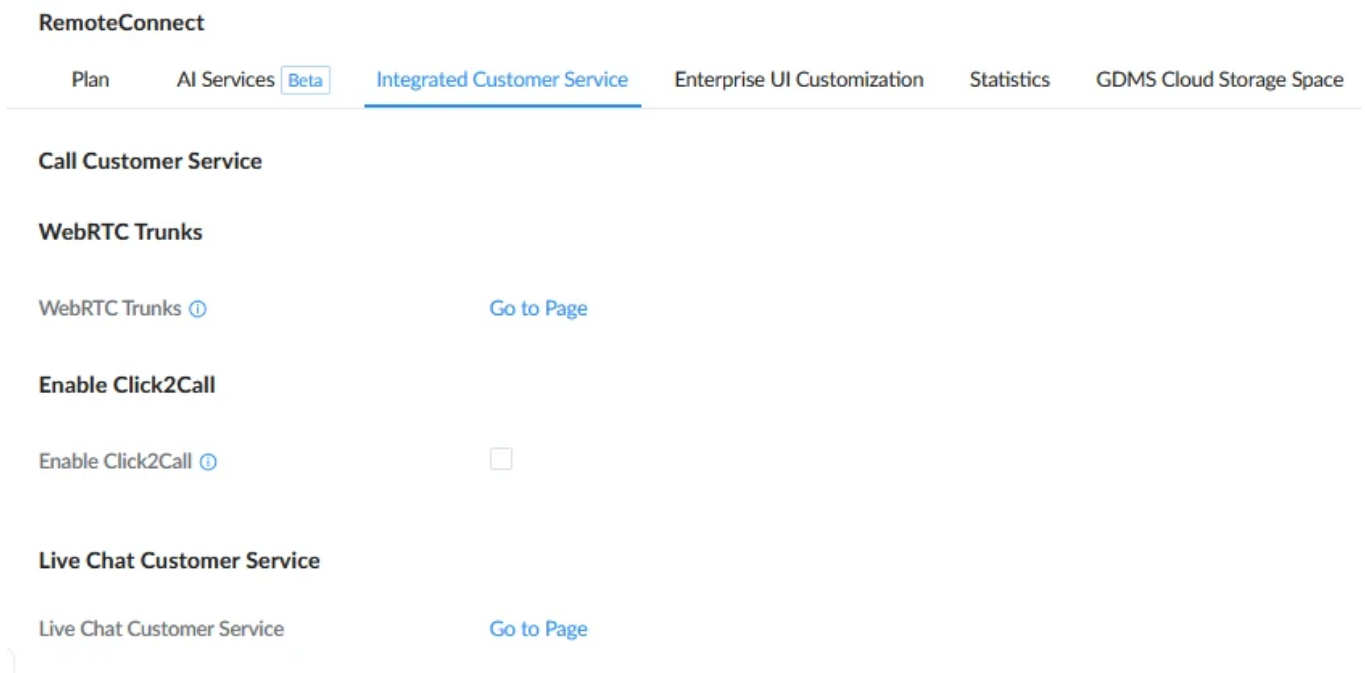
RemoteConnect AI Services Page

Integrated Customer Service

This section allows administrators to configure web-based customer service features that integrate communication tools into websites. Under the **Integrated Customer Service** tab, administrators can access options for WebRTC Trunks, Enable Click2Call, and Live Chat Customer Service.

Through this section, administrators can navigate directly to the configuration pages for WebRTC Trunks and Live Chat Customer Service to manage web-based customer interactions.

The Click2Call feature has been retired for new setups. However, users who had Click2Call enabled prior to this update will still see the configuration options in the Web GUI to ensure existing configurations remain functional without interruption.



RemoteConnect Integrated Customer Service Page

Enterprise UI Customization

With a RemoteConnect plan, the Enterprise UI Customization page allows administrators to apply customized branding across the UCM and Wave interfaces. From this page, the company name can be configured and multiple logo images can be uploaded to replace the default branding in supported system interfaces.

The system supports different logo sizes and formats to ensure proper rendering in various locations as described below

- **Logo 1 (80x80px):** Replaces the Grandstream logo on the top left corner of the Wave Web interface and UCM management interface. The recommended format is PNG, and the maximum file size is 2 MB.
- **Logo 2 (256x64px):** Replaces the Grandstream banner on the top left corner of the login page and emails. The recommended format is PNG, and the maximum file size is 2 MB.
- **Logo 3 (64x64px):** Replaces Browser tab icon. The recommended format is .ico, and the maximum file size is 2 MB.

A built-in preview panel is provided on the right side of the page, allowing administrators to review how the configured company name and logos will appear in different interfaces.

To ensure optimal visibility and contrast with the system UI, it is recommended not to use blue, black, or white as the primary logo color.

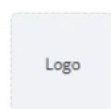
Company Name

Logo1 Preview: UCM

Logo

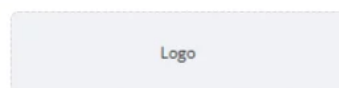
It is recommended to not use blue, black, and white for the logo color.

Logo 1 80×80px



Upload

Logo 2 256x64px

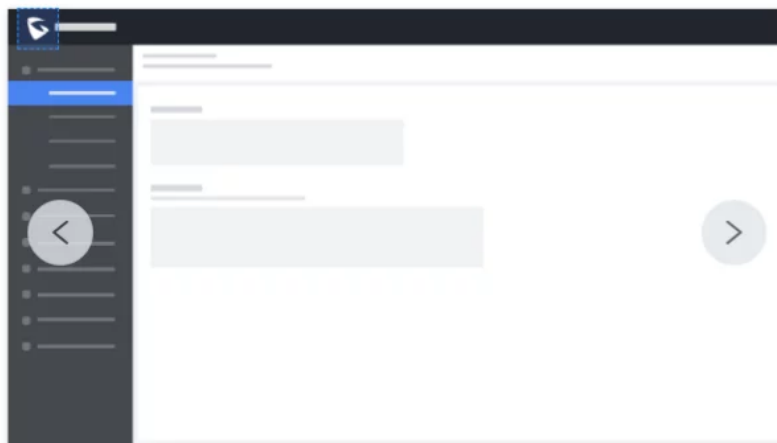


Upload

Logo 3 64x64px (.ico)



Upload



Cancel

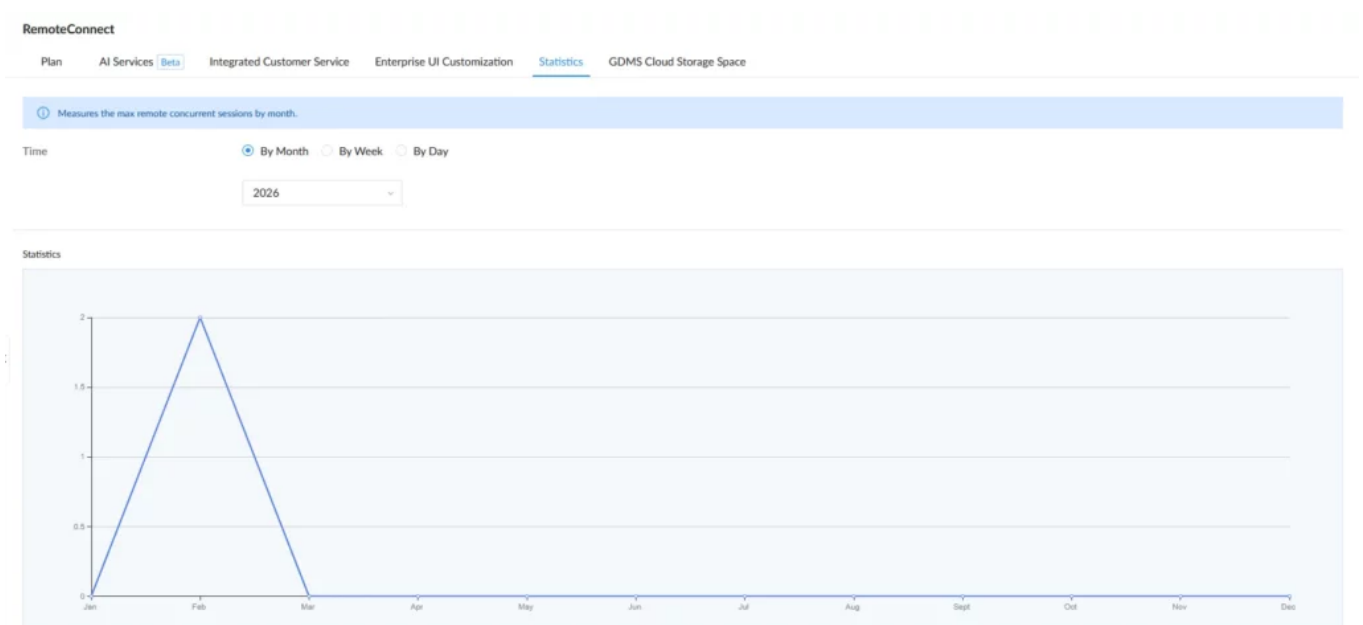
Save

RemoteConnect Enterprise UI Customization Page

Statistics

The Statistics page provides an overview of RemoteConnect usage by displaying historical data on maximum concurrent remote sessions. This information helps administrators monitor RemoteConnect capacity usage and understand how remote access services are consumed over time.

Usage statistics can be viewed by month, week, or day. When viewing data by month, the system displays the highest number of concurrent remote sessions recorded during each month of the selected year.



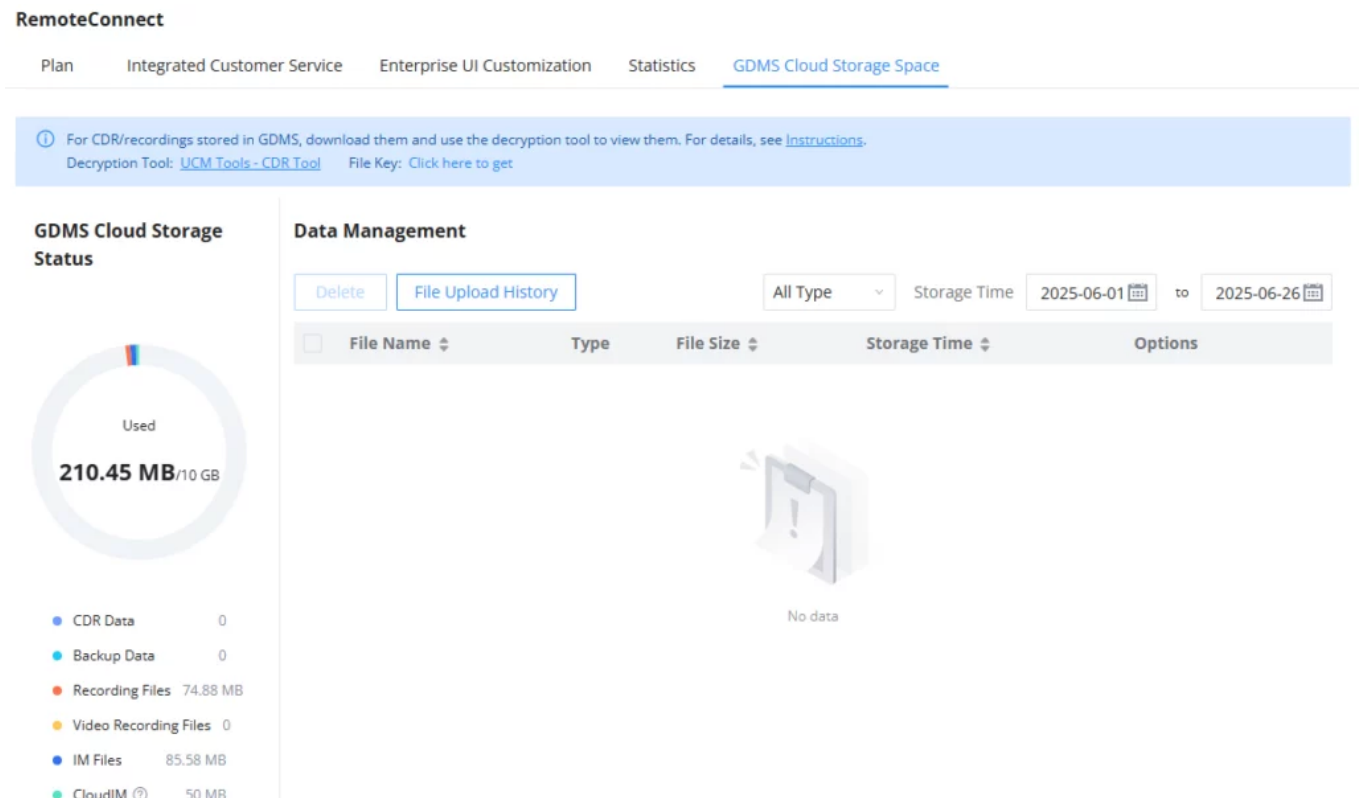
RemoteConnect Statistics Page

For more information, please visit the following website: <https://ucmrc.gdms.cloud/home> and check the UCM63XX RemoteConnect Guides.

GDMS Cloud Storage Space

When the correspondent RemoteConnect plan is active, the user can access to a GDMS Cloud Storage Space to get an overview about how the storage space is being used. The data is represented in four categories of file types: CDR Data, Backup Data, Recording Files, and IM Files.

The user is also able to see the names of all the files stored in the GDMS Cloud Storage Space.



RemoteConnect GDMS Cloud Storage Space Page

On this page the user can obtain the file key by clicking on the following hyperlink.

 For CDR/recordings stored in GDMS, download them and use the decryption tool to view them. For details, see [Instructions](#).
Decryption Tool: [UCM Tools - CDR Tool](#) **File Key: [Click here to get](#)**

To decrypt the files, please refer to the following guide: UCM6300/A Series IP PBX - CDR Tool Guide.

AI SETTINGS (BETA)

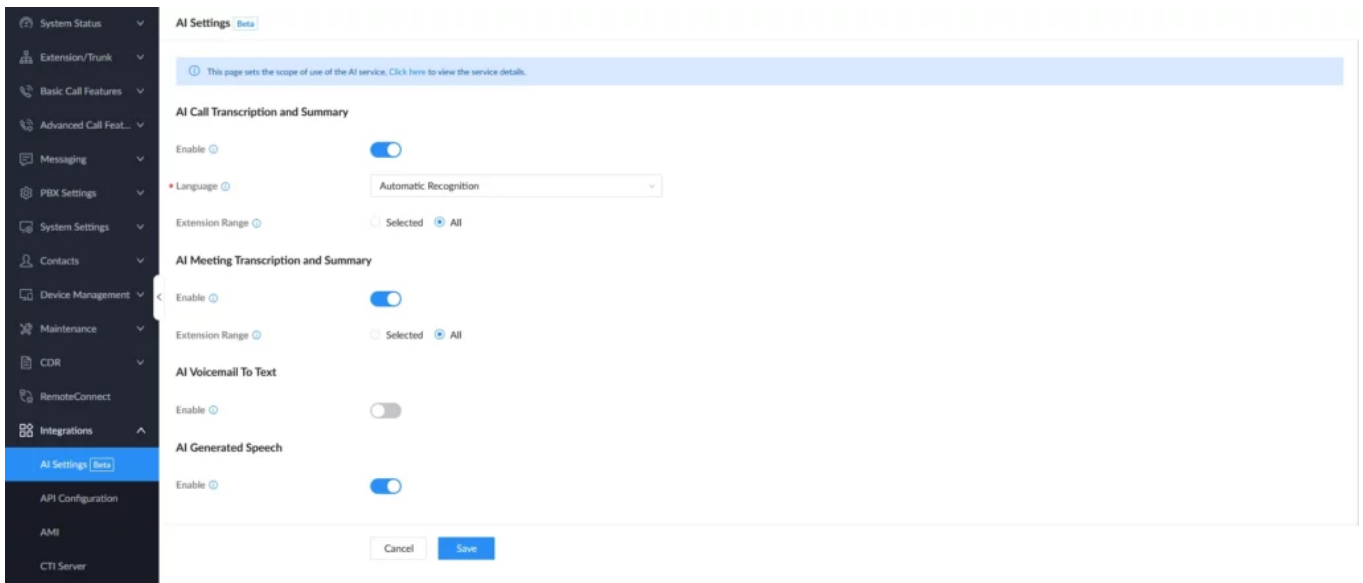
The AI Settings page allows administrators to configure the usage of AI services provided through the RemoteConnect AI service. These features enable automatic speech recognition, transcription, summarization, and text-to-speech processing for calls, conferences, and voice messages.

AI services are a purchaseable add-on and subject to usage limits defined by the active RemoteConnect plan. The administrator can enable each AI feature independently and define whether it applies to all extensions or only selected extensions.

For more information, please refer to the RemoteConnect pricing page: <https://cloud.grandstream.com/plans>

The following AI capabilities are supported on the UCM:

- **AI Call Transcription and Summary**
- **AI Conference Transcription and Summary**
- **AI Voice Message to Text**
- **AI Generated Speech**



AI Settings Page

RemoteConnect

Plan

AI ServicesBeta

Integrated Customer Service

Enterprise UI Customization

Statistics

GDMS Cloud Storage Space

Trial

AI

AI Services

Valid until 2026-06-13

AI Settings

Current specifications: AI Free Trial (Beta)

AI Usage Statistics

2026-05

AI Voicemail To Text

0 Min

AI Generated Speech

1 Min

AI Call Transcription and Summary

1 Min

AI Meeting Transcription and Summary

1 Min

Total Usage

3 Min

Voice Transcription

The **Voice Transcription** tab consolidates configuration for all speech-to-text features, including calls, meetings, media recording files, and voicemails.

AI Call Transcription and Summary

This feature enables AI-based transcription and summarization for one-to-one calls. When enabled globally, the administrator defines whether the feature applies to all extensions or only selected extensions. Only extensions included in this scope are eligible for call transcription and summarization.

AI Call Transcription and Summary

Enable

Language

Automatic Recognition

Extension Range

Selected

All

Search

Company Contact

1007

1011

2000

2003

2004

2005

2006

3000

3012

Selected(4)

1011

2000

2003

2004

AI Call Transcription and Summary General Setting

At the extension level, the Automatic Transcribing and Summarizing option determines whether calls for that extension are processed automatically. When enabled, all calls made or received by the extension are automatically transcribed and summarized.

The recognition language can be configured globally under **AI Settings (Beta)->AI Call Transcription and Summary** and followed by the extension, or explicitly set per extension.

Extensions > Edit Extension: 1000

Basic SettingsMediaCall PolicyFeaturesVoicemailCustom TimeAIWave ClientFollow MeAdvanced Settings

AI Call Transcription and Summary

Automatic Transcription and Summary ☒

Language Follow Global Settings

AI Voicemail To Text

Automatic Transcription ☐

Language Follow Global Settings

Cancel

Save

Extension Automatic Call Transcription

Generated transcripts and summaries can be viewed by users through the **Wave client**, as shown below.

A call between 18099876761 and the hotel receptionist

DownloadCopyShare

2025-12-24 09:04 - 09:10 (UTC+08:00)

BookingRoom TypeFacilitiesConfirmationPaid

Summary

A customer named John Smith made a reservation for a deluxe room at the hotel from December 25th to December 30th. The hotel receptionist provided information about the room's amenities and confirmed the reservation upon receiving payment details.

Notes

Room Amenities (09:06:22 - 09:06:57)

- King-size bed
- Free Wi-Fi
- Mini-bar
- Access to gym and pool

Reservation Details(09:08:32 - 09:08:57)

- Customer Name: John Smith
- Stay Dates: December 25th to December 30th
- Room Type: Deluxe room

Follow-up Actions

1. The receptionist will send a confirmation email to John Smith.

2. Ensure the deluxe room is ready for the customer's arrival on December 25th.

Voice Transcript

1818099876761 09:04:22

PEHello, I would like to make a reservation for a room.

180904:57

PEHotel Receptionist 09:04:57

PESure! Can you please tell me the dates of your stay?

180905:22

1818099876761 09:05:22

18I plan to stay from December 25th to December 30th.

180905:57

PEHotel Receptionist 09:05:57

PEGreat! Let me check the availability for those dates. We have a standard room and a deluxe room available. Which one would you prefer?

180906:22

1818099876761 09:06:22

18I'll go with the deluxe room. What are the amenities included?

180906:57

PEHotel Receptionist 09:06:57

PEThe deluxe room includes a king-size bed, free Wi-Fi, a mini-bar, and access to the gym and pool.

180907:22

1818099876761 09:07:22

18That sounds good. Can I confirm the reservation now?

180907:57

PEHotel Receptionist 09:07:57

PEAbsolutely! I just need your name and payment details to finalize the booking.

180908:32

1818099876761 09:08:32

18My name is John Smith, and I'd like to pay by credit card.

180908:57

PEHotel Receptionist 09:08:57

PEThank you, Mr. Smith. Your reservation is confirmed for a deluxe room from December 25th to December 30th. You will receive a confirmation email shortly.

180909:42

1818099876761 09:09:42

18Thank you for your help!

180910:07

PEHotel Receptionist 09:10:07

PEYou're welcome! If you have any other questions, feel free to ask. Have a great day!

Call Transcript on Wave

AI Meeting Transcription and Summary

This feature enables AI-based transcription and summarization for conference calls and meetings. When enabled, meeting audio is processed by the AI service and a transcript and summary are generated after the meeting ends. The administrator can define whether the feature applies to all extensions or only selected extensions participating in conferences.

AI Meeting Transcription and Summary

Enable ⓘ



• Extension Range ⓘ

☒ Selected ☐ All

Search Company Contact ☒ All ☐ Sales ☐ Quality Control ☐ Finance ☒ Marketing ☐ Technical Support ☐ IT ☐ Human Resources ☐ Logistics	Selected(1) Marketing x
--	---

AI Meeting Transcription and Summary Setting

When scheduling a meeting, the meeting organizer can explicitly choose whether the conference will be transcribed or not. This selection applies only to the scheduled meeting and does not affect global or extension-level AI settings.

System Status

Extension/Trunk

Basic Call Features

Multimedia Meeting

IVR

Voicemail

Ring Groups

Paging/Intercom

Call Queue

Speed Dial

Event List

Feature Codes

Parking Lot

Advanced Call Feat...

Messaging

Multimedia Meeting > Schedule Meeting

resource-intensive codec.
[Batch Add](#)

Allow User Invite ⓘ ☒

Advanced

Email Reminder (m) ⓘ ☒ 60 Range 5 - 120

Call Participants ⓘ ☒

Allowed to Override Host Mute ⓘ ☐

Play Joining/Leaving Meeting Announcement ⓘ ☒

Auto Record ⓘ

None

Sync to Google Calendar ⓘ ☐ [Google Services](#)

Support AI transcription ☒

Language ⓘ

Automatic Recognition

Automatic AI Transcription ⓘ ☐

AI Transcription Support for Scheduled Meeting

Meeting transcripts and summaries can be accessed by participants through supported Wave clients and user portals.

Hotel Weekly Meeting

2025-12-24 10:04 - 10:24 (UTC+08:00)

Participants: Jianhua Zhao, Peter, Kevin, Lucy, Daniel, James

Hotel Operations

Occupancy Rate

Guest Satisfaction

F&B Services

Maintenance

Revenue Growth

Upcoming Events

Sustainability

Download

Copy

Share

Voice Transcript

Summary

The meeting focused on reviewing last week's operational performance, discussing guest feedback, operational issues, and strategies for the upcoming peak season. Each department provided updates on their progress and outlined plans for future work.

Notes

🔊 Operations Management (Front Office & Facilities)(10:04:22 - 10:08:32)

- Front Office Operations: 85% occupancy rate last week; 40% of guests used the online check-in feature, significantly reducing front desk wait times.
- Facility Maintenance: Resolved Sunday's key card encoder glitch and inconsistent HVAC temperatures on floors 5-7; pending investigation of slow-draining showers in some rooms. Cleaning Progress: Completed deep cleaning of floors 1-4 (next floors scheduled for next week).

🍽️ Food & Beverage Services(10:08:52 - 10:24:37)

- Performance & Feedback: 10% growth in dinner revenue, with the new seafood platter and vegetarian risotto receiving positive reviews. Long-stay guests noted repetitive breakfast buffets, prompting plans for a rotating menu.
- Cost & Planning: Food costs remained within budget, while beverage costs exceeded projections slightly due to a special event.

Follow-up Actions

- Coordinate a dedicated check-in area for the "Global Innovators" group.
- Collaborate with James on the banquet menu for the corporate client.
- Test A/V equipment in all conference rooms and ensure HVAC systems are monitored.

JH

Jianhua Zhao 10:04:22

Let's start with a quick overview of last week's performance, then we'll dive into guest feedback, operational issues, and the upcoming peak season strategy.

PE

Peter 10:06:57

Morning, Jianhua. Last week was fairly busy. We saw a steady 85% occupancy rate. The new online check-in feature has been a huge success, with about 40% of guests using it. We've seen a corresponding decrease in wait times at the front desk. The main issue was a small technical glitch with the key card encoder on Sunday afternoon, which Kevin's team resolved quickly.

KE

Kevin 10:10:07

Yes, Peter. It was a software-related issue. We've updated the driver and it should be stable now. We'll be doing a full diagnostic on all the key card machines this week to prevent a recurrence.

JH

Jianhua Zhao 10:12:12

Good, Kevin, what's the status of the HVAC system on floors 5 through 7? We had a few complaints about inconsistent temperatures.

KE

Kevin 10:15:27

We've replaced the main thermostat controllers for that entire section. The new units are more precise and energy-efficient. We'll be monitoring them closely over the next few days. We're also starting the preventative maintenance schedule on all guest room AC units this week.

LU

Lucy 10:16:02

Speaking of that, Kevin, my team reported a couple of rooms with slow-draining showers. Could you have your maintenance crew take a look?

KE

Kevin 10:19:55

Lucy, yes, of course. I've already got two on the list. I'll have a team up there this afternoon.

Meeting Transcript on Wave

AI Recording Transcription and Summary

This feature allows audio recording files stored on the UCM to be transcribed and summarized using AI. When enabled globally, the administrator specifies whether the scope applies to all extensions or selected extensions.

 This page sets the scope of use of the AI service, [Click here](#) to view the service details.

[Voice Transcription](#)[AI Translation](#)[Voice Generation](#)[Voice Assistant](#)**AI Call Transcription and Summary**Enable **AI Meeting Transcription and Summary**Enable **AI Recording Transcription and Summary**Enable 

 Transcription for stereo recordings is not supported. You can go to [General Settings](#) to adjust the recording settings.

Extension Range ☐ Selected ☒ All **AI Voicemail-to-Text**Enable [Cancel](#)[Save](#)

Transcription for stereo recordings is not currently supported. Administrators can adjust recording audio channel modes under PBX Settings->General Settings.

Once transcribed, users can review recording transcripts with interactive synchronization. Clicking a text segment automatically seeks media playback progress to that timestamp, and active media playback dynamically highlights the corresponding transcript text.

AI Voicemail to Text

This feature converts voice messages (voicemail) into text using AI speech recognition. When enabled globally, voice messages left for eligible extensions can be transcribed.

AI Voicemail To Text

Enable ⓘ



* Language ⓘ

Automatic Recognition

* Extension Range ⓘ

☒ Selected ☐ All

Company Contact

☒ All

☐ Sales

☐ Quality Control

☐ Finance

☐ Marketing

☒ Technical Support

☐ IT

☐ Human Resources

☐ Logistics

Selected(1)

Technical Support x

At the extension level, the Automatic Transcription option determines whether voice messages for that extension are automatically converted into text.

The recognition language can follow the global configuration or be explicitly specified for the extension.

Extensions > Edit Extension: 1000

Basic Settings

Media

Call Policy

Features

Voicemail

Custom Time

AI

Wave Client

Follow Me

Advanced Settings

AI Call Transcription and Summary

Automatic Transcription and Summary ⓘ



Language ⓘ

Follow Global Settings

AI Voicemail To Text

Automatic Transcription



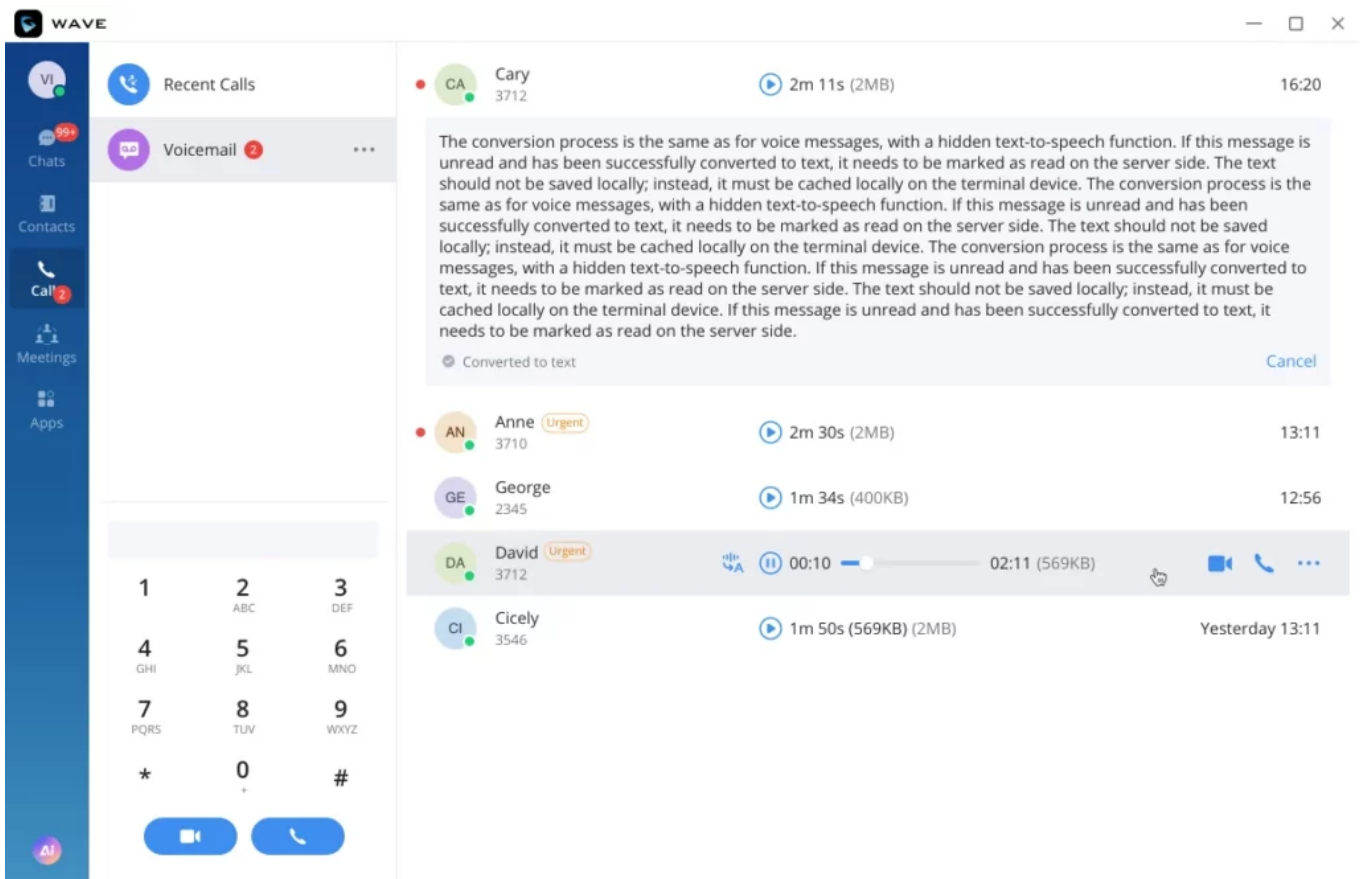
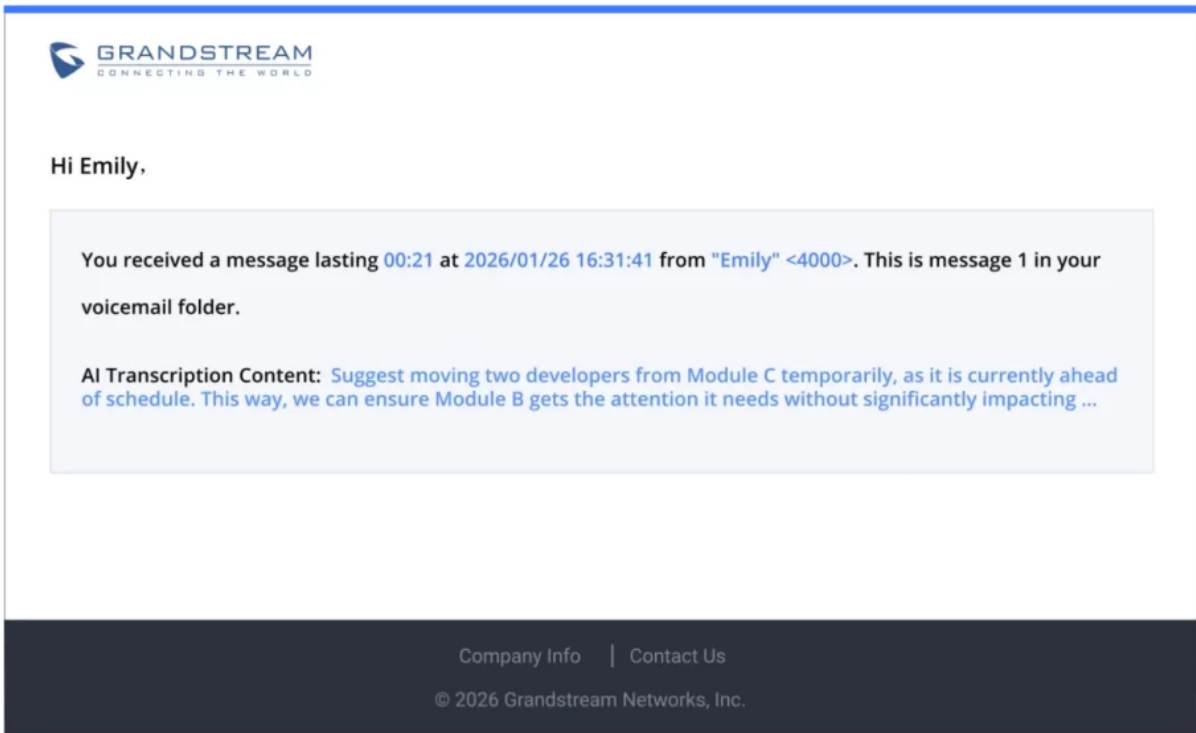
Language ⓘ

Follow Global Settings

Cancel

Save

Transcribed voicemail content can be viewed in supported Wave clients, through the User Portal (where accessing or playing the voicemail marks it as read), and may also be included in voicemail email notifications depending on system configuration.



AI Voice Message to Text

This feature converts voice messages (voicemail) into text using AI speech recognition. When enabled globally, voice messages left for eligible extensions can be transcribed.

AI Voicemail To Text

Enable ⓘ



* Language ⓘ

Automatic Recognition

* Extension Range ⓘ

☒ Selected ☐ All

Company Contact

☒ All

☐ Sales

☐ Quality Control

☐ Finance

☐ Marketing

☒ Technical Support

☐ IT

☐ Human Resources

☐ Logistics

Selected(1)

Technical Support x

AI Voice Message to Text General Setting

At the extension level, the Automatic Transcription option determines whether voice messages for that extension are automatically converted into text.

The recognition language can follow the global configuration or be explicitly specified for the extension.

Extensions > Edit Extension: 1000

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

AI Call Transcription and Summary

Automatic Transcription and Summary ⓘ



Language ⓘ

Follow Global Settings

AI Voicemail To Text

Automatic Transcription



Language ⓘ

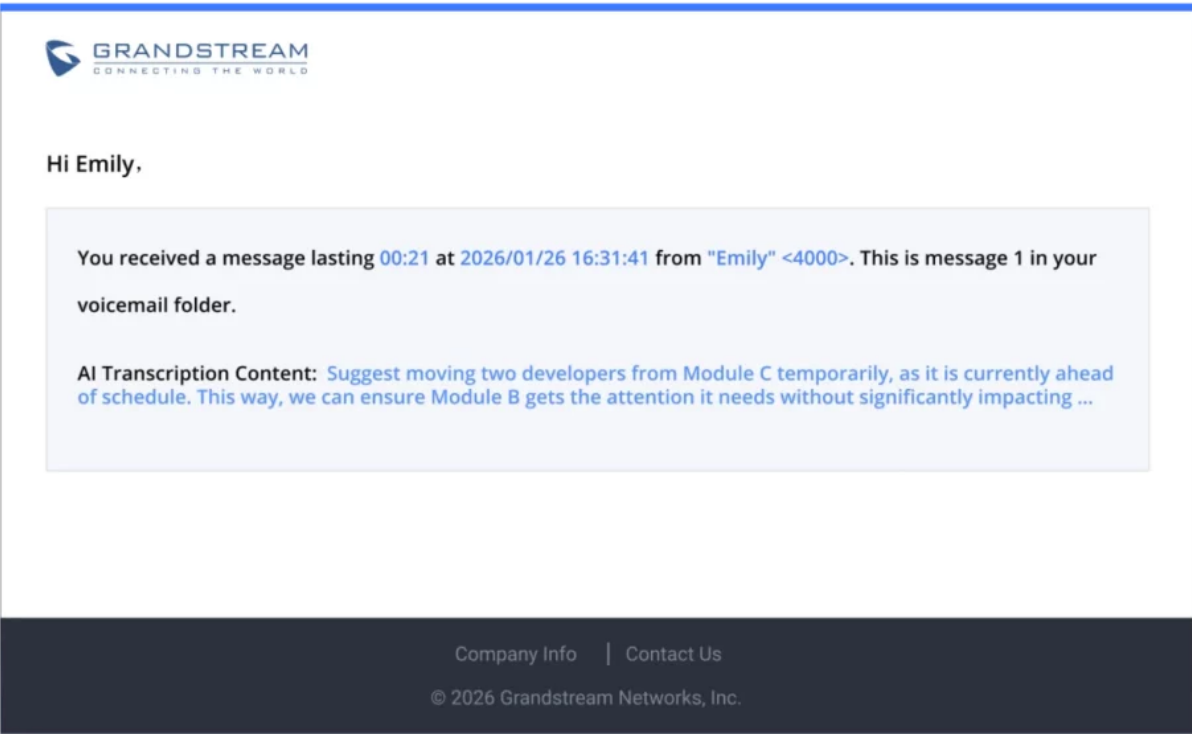
Follow Global Settings

Cancel

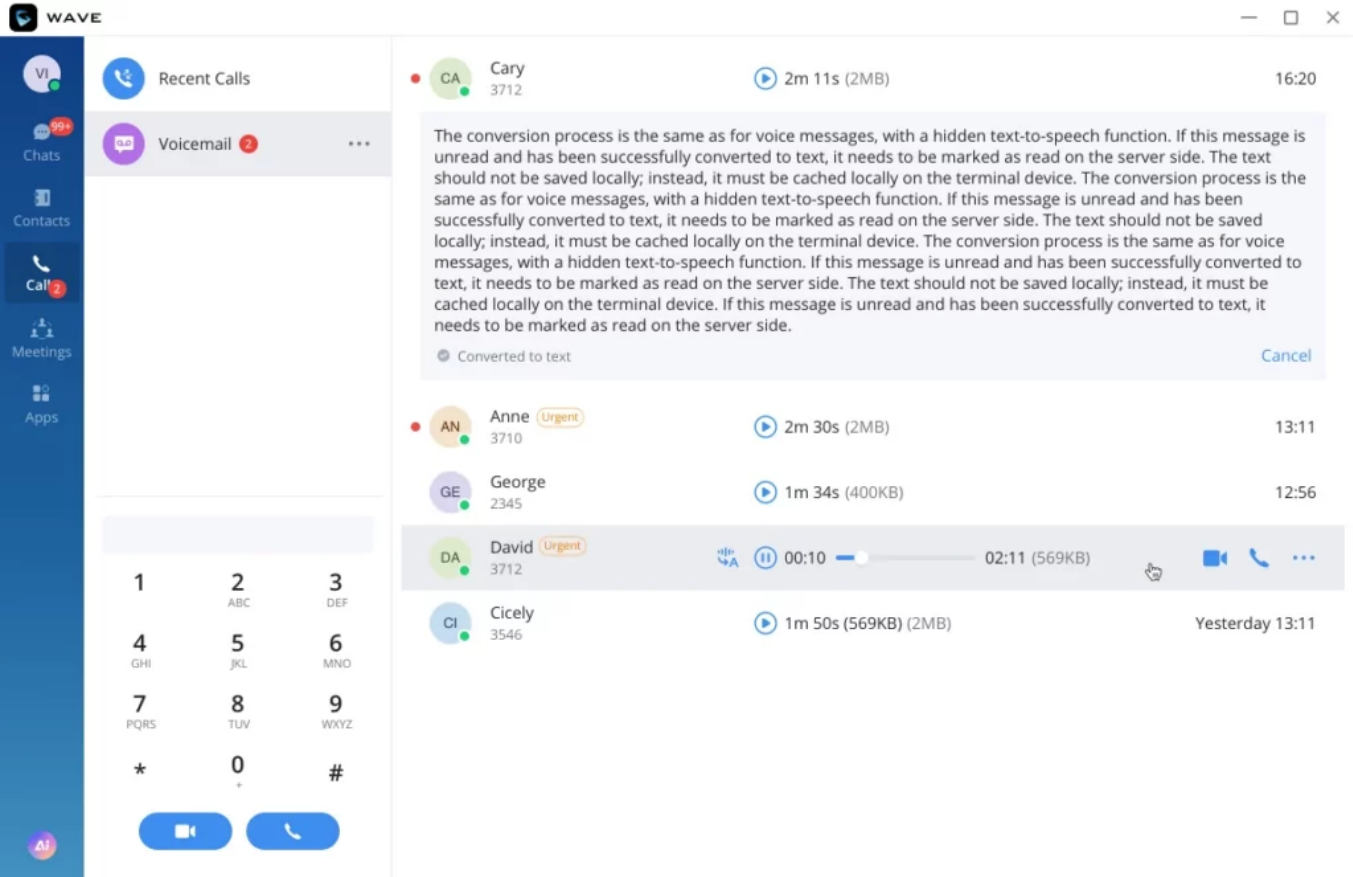
Save

Extension Automatic Voicemail Transcription

Transcribed voicemail content can be viewed in supported Wave clients and may also be included in voicemail notifications, depending on system configuration.



Voicemail Transcript Email



Voicemail Transcript on Wave

AI Translation

The **AI Translation** feature provides real-time translation capabilities for call transcripts, conference transcripts, and chat messages across Wave endpoints. When enabled globally, the administrator defines the

extension scope (All Extensions or Selected Extensions) authorized to use AI Translation.

AI Settings Beta

This page sets the scope of use of the AI service. [Click here](#) to view the service details.

Voice Transcription

AI Translation

Voice Generation

Voice Assistant

AI Translation

Enable ⓘ

Extension Range ⓘ

Selected

•

All ⓘ

Cancel

Save

Once granted permission, users can translate live speech-to-text transcripts during active calls/meetings or translate instant chat messages on-demand.

AI Voice Generation

The **Voice Generation** tab manages AI Generated Speech capabilities. This feature provides text-to-speech (TTS) processing powered by the AI service, allowing administrators to generate voice prompt audio directly from text. This feature is primarily used for IVR prompts, queue announcements, and other system voice prompts, eliminating the need to manually record or upload audio files.

Before using this feature, AI Generated Speech must be enabled on the **Voice Generation** tab under **AI Settings**. Once enabled, administrators can generate AI-based voice prompts from multiple entry points in the system.

AI Settings Beta

This page sets the scope of use of the AI service. [Click here](#) to view the service details.

Voice Transcription

AI Translation

Voice Generation

Voice Assistant

AI Generated Speech

Enable ⓘ

Cancel

Save

The feature can be accessed from **PBX Settings->Voice Prompt->Custom Prompt** by clicking the AI Generated Speech button, which opens the AI generation window.

Voice Prompt

Language Settings Custom Prompt Username Prompt

Uploaded prompt files cannot have the same name even if the file format is different.

Record Upload **AI Generated Speech** Download All Delete Clear

☐	Name ↕	Type ↕	Format ↕	Play	Options
☐	en-hourly-break.wav	Audio	wav		
☐	en-hourly-break.mp3	Audio	mp3		
☐	en-lunch.wav	Audio	wav		
☐	en-lunch.mp3	Audio	mp3		
☐	en-backoffice.mp3	Audio	mp3		

AI Generated Speech Option in Custom Prompt

It is also accessible while configuring features that require voice prompts (such as call queues). In those cases, selecting AI Generated Speech from the prompt selection dropdown redirects the user to the same AI generation window used in the Voice Prompt page.

System Status **Extension/Trunk** **Basic Call Features** **Multimedia Meeting** **IVR** **Voicemail** **Ring Groups** **Paging/Intercom** **Call Queue** **Speed Dial** **Event List** **Feature Codes** **Parking Lot** **Advanced Call Feat...** **Messaging**

Call Queue > Edit Queue: 6500

Basic Settings Advanced Settings Agents

Welcome Prompt

Enable ☒

Custom Prompt ⓘ None Add Audio

Play Full Welcome Prompt ⓘ ☒

Upload Audio File

AI Generated Speech

Satisfaction Survey Prompt

Custom Prompt ⓘ None Add Audio

Max Wait Time

Max Wait Time ⓘ 60

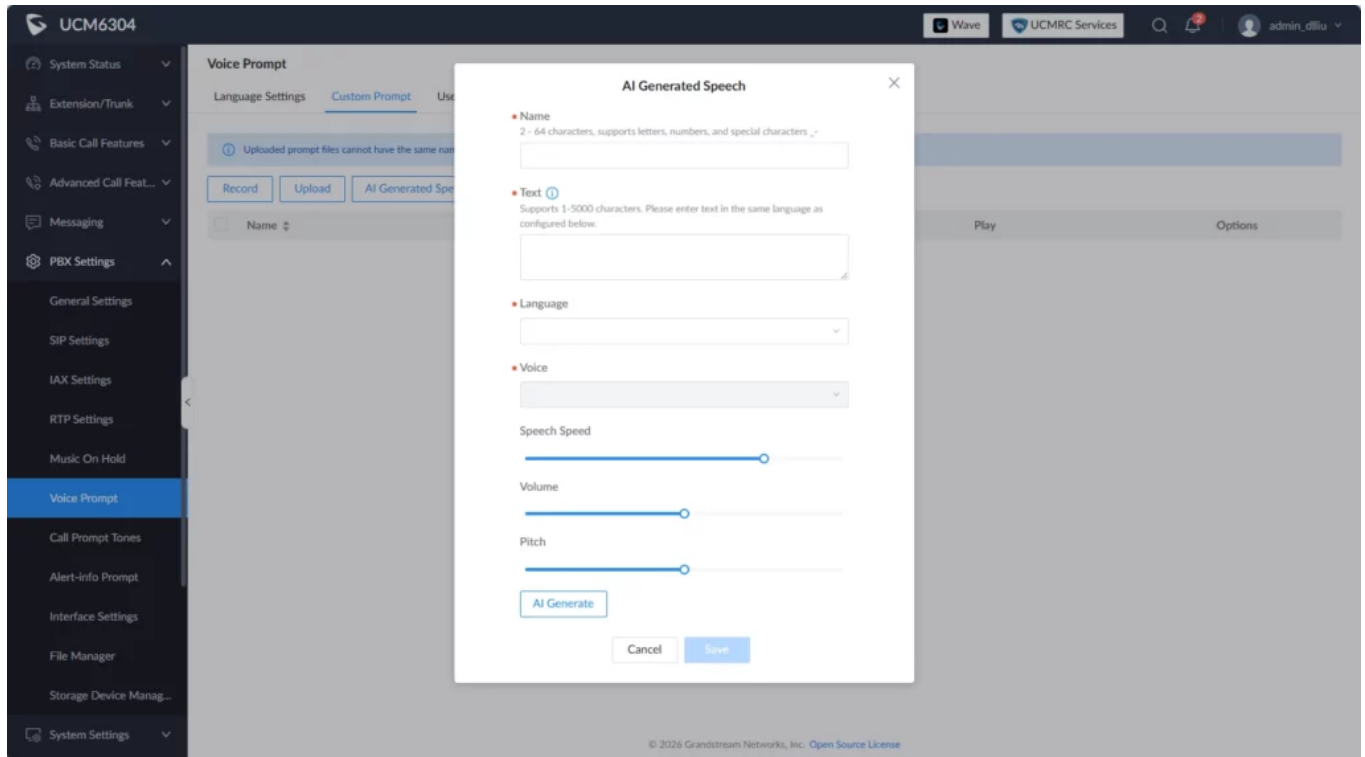
Destination ⓘ Hang up

Reset Agent Call Counter

Enable ⓘ ☐

Call Queue AI Generated Prompt Option

When creating an AI-generated voice prompt, the following settings are available:



AI Generated Speech Configuration Options

Name	Defines the name of the generated voice prompt. This name is used to identify the prompt in the system and must be unique. The field supports 2-64 characters, including letters, numbers, and special characters.
Text	Specifies the text content that will be converted into speech. The text length supports up to 5,000 characters.
Language	Specifies the language used for text-to-speech processing.
Voice	Selects the voice profile used to generate the speech. Different voice options may be available depending on the selected language. A preview option is provided, allowing administrators to listen to the voice style before generating the prompt.
Speech Speed	Controls the playback speed of the generated speech. The speed can be adjusted from slower to faster relative to normal speaking speed.
Volume	Adjusts the output volume level of the generated audio. The value can be set from 0 to 100 to accommodate different playback environments.
Pitch	Controls the pitch of the generated voice. Higher values produce a higher-frequency voice, while lower values produce a deeper tone. The pitch range can be set from 0 to 100.

After configuring the parameters, clicking AI Generate produces the audio preview. Once satisfied, the generated prompt can be saved and reused like any other system voice prompt.

AI Voice Assistant

The **Voice Assistant** tab allows administrators to configure natural voice command controls for endpoints. When enabled globally, extension users within the configured scope can issue spoken commands to perform actions such as making calls, transferring calls, initiating meetings, or sending messages.

 This page sets the scope of use of the AI service. [Click here](#) to view the service details.

Voice Transcription

AI Translation

Voice Generation

Voice Assistant**AI Voice Assistant**Enable Extension Range ☐ Selected ☒ All AI Contacts ☐ Selected ☒ All Contact Name Language 

Cancel

Save

Administrators can configure the following settings under **AI Settings->Voice Assistant**.

- **Enable:** Toggles the AI Voice Assistant service on or off.
- **Extension Range:** Controls which extensions are permitted to speak commands to the AI Voice Assistant (e.g., Only allow Extensions 1000-1005 to use the Voice Assistant feature).
- **AI Contacts:** Controls which contacts/directory entries the AI can look up when executing a voice command (e.g., Allow to search the entire contacts when an extension user asks "Call John").
- **Contact Name Language:** Defines the language rules used to recognize and match spoken names in the directory.

API CONFIGURATION

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

Permitted IP (s)	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)	
Basic Settings	
Enable	Enable/Disable API. The default setting is disabled.
TLS Bind Address	Configure the IP address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional, and the default port number is 8443. The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses. The default setting is 0.0.0.0:8443.
Username	Configure the username for TLS authentication.
Password	Configure the password for TLS authentication.
Permitted IP(s)	Specify a list of IP addresses permitted to use the API. This creates an API-specific access control list. Multiple entries are allowed. For example, "192.168.40.3/255.255.255.255" denies access from all IP addresses except 192.168.40.3. By default, this is blank, which indicates that no IP addresses are allowed to use this API.
Other Settings	
TLS Private Key	Upload TLS private key. The size of the key file must be under 2MB. This file will be renamed as 'private.pem' automatically.
TLS Cert	Upload TLS cert. The size of the certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection. This file will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.
API Module	
CDR API	Enable/disable CDR API module.
REC API	Enable/disable REC API module.
PMS API	Enable/disable PMS API module.

For more details on CDR API (Access to Call Detail Records), REC API (Access to Call Recording Files) and PMS API, please refer the document in the link here:

- <https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>
- <https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>
- PMS API

API Queries Supported

The new API supports the queries listed below which will accomplish certain requests and get data about different modules on UCM630xA.

The table below describes the new API Supported Queries.

getSystemStatus	addInboundRoute	listPaginggroup
getSystemGeneralStatus	getInboundRoute	addPaginggroup
listAccount	updateInboundRoute	getPaginggroup
getSIPAccount	deleteInboundRoute	updatePaginggroup
updateSIPAccount	playPromptByOrg	deletePaginggroup

listVoIPTrunk	listBridgedChannels	MulticastPaging
addSIPTrunk	listUnBridgedChannels	MulticastPagingHangup
getSIPTrunk	Hangup	listIVR
updateSIPTrunk	Callbarge	addIVR
deleteSIPTrunk	listQueue	getIVR
listOutboundRoute	getQueue	updateIVR
addOutboundRoute	updateQueue	deleteIVR
getOutboundRoute	addQueue	cdrapi
updateOutboundRoute	deleteQueue	recapi
deleteOutboundRoute	loginLogoffQueueAgent	pmsapi
listInboundRoute	pauseUnpauseQueueAgent	queueapi
mute	Unmute	hold
unhold	dialExtension	dialOutbound
callTransfer	transferNumberInbound	transferNumberOutbound
dialIVR	dialIVROutbound	dialQueue
dialRinggroup	dialOutboundTwo	listUser
getUser	updateUser	listExtensionGroup
listPinSets	refuseCall	acceptCall
applyChanges	addAnalogTrunk	getAnalogTrunk
listAnalogTrunk	updateAnalogTrunk	deleteAnalogTrunk
addSLATrunk	updateSLATrunk	deleteDigitalTrunk
addDigitalTrunk	getDigitalTrunk	listDigitalTrunk
updateDigitalTrunk	listDepartment	addContact
updateContact	deleteContact	

API Configuration Parameters

CDR Real-time Output Settings	
Enable	Enables real-time CDR output module. This module connects to selected IP addresses and ports and posts CDR strings as soon as it is available.
Server Address	CDR server IP address
Port	CDR server IP port
Upload Prompts User Configuration	
Username	Username used to upload prompts.
Password	Password used to upload prompts.

Upload Voice Prompt via API

Customers now can use the "Upload Prompts User Configuration" to upload/replace voice prompt files as an alternative method to the manual upload method on UCM **PBX Settings→Voice Prompt→Custom Prompt**.

The workflow of the prompt file upload goes as:

An HTTP/HTTPS request is sent to the UCM to upload/replace a voice prompt file, the request should include authentication details to the UCM and the name of the file to be uploaded. Then the UCM will contact an FTP server that should be hosted on the same IP address of the HTTP/HTTPS requester and download the prompt file from the FTP server.

The steps and conditions to upload the voice prompt via API are listed below:

1. Configure the prompt User under **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
```

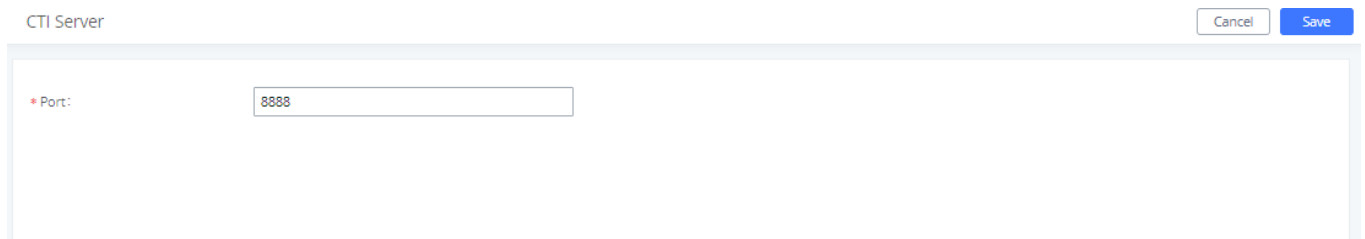
If the File name on the HTTP/HTTPS request exists already on the UCM's Custom voice prompts list the existing file will be overwritten by the new file downloaded from the FTP server.

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 Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link:

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:

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

Customer Relationship Management (CRM) refers to practices, strategies, and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers.

The UCM630X supports seamless integration with various CRM systems, allowing users to look up contact information in the Contacts, Leads, and Accounts tables, display contact records directly in the CRM web interface during incoming calls, perform one-click outbound calling, and automatically synchronize call history into the contact's activity history.

To accommodate different business environments, the UCM630X provides two flexible integration approaches:

- **Default Built-in Integration Templates:** Pre-configured, out-of-the-box integration solutions for widely used CRM platforms, including SugarCRM, VtigerCRM, Bitrix24CRM, Zoho Telephony, Salesforce, ACT! CRM, and ODOO CRM.
- **Custom CRM Templates:** Designed for proprietary or third-party CRM platforms not included in the default list. Administrators can create, import, export, or edit custom CRM templates.

For step-by-step instructions on creating, importing, exporting, and managing custom CRM integration templates, please refer to the UCM630X Custom CRM Integration Guide.

The main **CRM** page serves as the central hub for selecting and managing integrated CRM platforms. Here, administrators can view all available default and custom CRM modules, activate or switch the active CRM instance.

CRM

[Template Management](#)[Integration Manual](#)

Supports deep integration solutions with CRM, seamlessly integrating enterprise communication flow and business flow through core functions such as incoming call pop-ups, one-click outbound calling via CRM web interface, CRM contact lookup, and automatic contact creation for unknown numbers.



SugarCRM



VtigerCRM



Bitrix24CRM



Zoho Telephony



Salesforce



ACT! CRM



ODOO CRM



CRM_Integrati...





One Click Call
Install the Wave add-on or interface directly through the PBX. Linked users can use click-to-dial on the CRM interface to quickly call contacts.



Contact Lookups
Automatically display the names of contacts saved on the CRM when receiving calls, personalizing customer call experience and improving internal communication efficiency.



Call Log Sync
After the extension ends the call with the CRM contact, the call history will be automatically synced to the CRM, ensuring customer communication history is complete and traceable for easy management and analysis.



Incoming Call Pop-up Screen
Bring up CRM contact information on your browser straight from the incoming call pop-up.



Add Unknown Number
Automatically create contacts from calls with new numbers not found in the CRM database. This feature converts calls into sales leads, ensures that customer information is not missed, and builds a complete customer data pool.

CRM Integration Main Page

Navigating to **Template Management -> Default Template** displays the list of pre-configured CRM templates built into the system. From this page, administrators can inspect the structure of default templates or download them as JSON configuration files to serve as reference models when building custom integrations.

CRM > Template Management

[Default Template](#)[Custom Template](#)

Name	Operations
default_sugarCRM	 
default_ODOOCRM	 
default_Zoho	 
default_Bitrix24CRM	 
default_Bitrix24CRM_OAuth2	 

Default CRM Templates Management

Clicking the **View Template** icon on any default template opens a pop-up window displaying its underlying JSON schema. This view reveals the exact REST API endpoints, request methods, authentication structure, token refresh URLs, and parameter definitions used by the platform.

View template - default_sugarCRM



```
{
  "crm_name" : "default_sugarCRM"
  "crm_remark" : "Use 'Follow-up Request' to get the Session_ID."
  "custom_sync_contacts_enable" : 1
  "custom_auth_info" : {
    "auth_info" : {
      "auth_type" : 0
      "auth_url" : NULL
      "scope" : NULL
      "additional_query" : NULL
      "token_url" : NULL
      "auth_url_path" : NULL
      "base64_encoded" : NULL
      "request_content_type" : "application/json"
      "token_path" : NULL
      "request_method" : "get"
      "request_body" : NULL
      "token_refresh_method" : NULL
      "token_refresh_time" : 0
      "token_refresh_url" : NULL
      "token_refresh_content_type" : NULL
      "token_refresh_body" : NULL
      "refresh token path" : NULL
    }
  }
}
```

OK

View Default CRM Template Details

The **Template Management -> Custom Template** page allows administrators to manage user-defined CRM templates. From this tab, administrators can create new templates manually by clicking **Add**, batch-upload existing JSON template files, export custom templates for deployment across other UCM systems.

CRM > Template Management

Default Template Custom Template

[Add](#) [Upload](#) [Delete](#) [Download](#)

☐	Name	Last Modified Time	Remark	Operations
☐	CRM_Integration In Use	2026-09-11 15:21:53	This is a testing CRM	Edit Delete Download

Custom CRM Templates List

When creating or editing a custom CRM template, the **Edit Custom Template** interface provides sections to upload a custom CRM logo, set general metadata (Name and Remarks), and configure detailed REST API request parameters.

This includes selecting authentication protocols (Basic, Bearer Token, OAuth 2.0), providing certificates or tokens, and defining custom fields that prompt users for required credentials during initial CRM pairing

① When configuring, please first obtain the REST API document of the target CRM system as a reference and obtain the necessary verification information according to the authentication requirements of the CRM system.

Basic Settings

Logo



Upload Logo

Please select files in png (recommended), jpg, or jpeg format. Size must not exceed 2M

* CRM Name

CRM_Integration

2 - 64 digits, supports numbers, letters, special characters _-, and Chinese characters

Remark ①

This is a testing CRM

0 - 1024 characters

Request Configuration

Authentication

* Authentication Method

Basic

Base64 Encoded Certificate ①

dGVzdDp0ZXN0

0 - 256 characters

Custom Parameters

① These fields will be displayed as input boxes on the docking page, requiring the user to provide the necessary information. During the docking authentication process, the values entered by the user can be used as variable values in the template.

Edit Custom CRM Template Configuration

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.

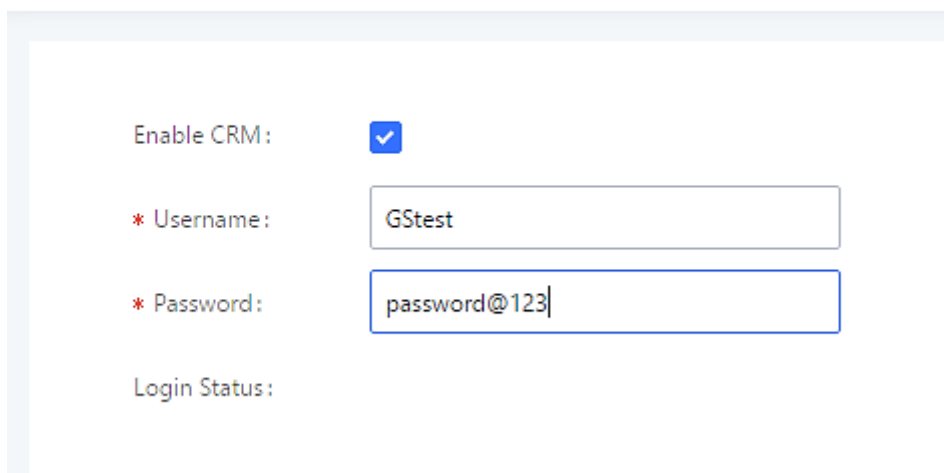
Sugar CRM Settings

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	  Select from the "Available" list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Once settings on admin access are configured:

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 :

VtigerCRM

* CRM Server Address :

http://vtiger.mydomain.com

* Add Unknown Number :

Organizations

Contact Lookups :

☐ 0 item Available

None

☐ 3 items Selected

Look up in Organizatio...

Look up in Leads table

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

CRM System	Select a CRM system from the dropdown menu, four CRM systems are available: Sugar CRM, Vtiger CRM, Zoho CRM (v2), Salesforce and ACT! CRM.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	  Select from the "Available" list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.

Once settings on admin access are configured:

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

Bitrix24 CRM

The UCM6300 Series supports integration with Bitrix24 CRM, allowing the system to query CRM records during calls, display contact information, and automatically create CRM records for unknown numbers based on configuration.

For detailed step-by-step instructions on preparing the Bitrix24 account, generating webhooks, and completing the integration, refer to the Bitrix24 CRM Configuration Guide.

CRM

CRM System

Bitrix24CRM

* CRM Server Region ⓘ

* Add Unknown Number ⓘ

Contact Lookups

☐ 3 Available

Search

Q

☐ Look up in Contacts table

☐ Look up in Leads table

☐ Look up in Organizations table

<

>

☐ 0 Selected

Search

Q

None

⌵

⌶

⌷

✱

Bitrix24 CRM Settings

The table below describes the configurable parameters for this integration.

CRM System	Select "Bitrix24CRM" from the CRM System dropdown menu to enable Bitrix24 integration.
------------	--

CRM Server Region	Specify the Bitrix24 server region or domain associated with the Bitrix24 account. This value must match the region or URL used when configuring the Bitrix24 webhook.
Add Unknown Number	Specifies how the UCM handles incoming or outgoing calls from phone numbers that do not exist in Bitrix24 CRM. None: No CRM record is created when an unknown number is detected. Contacts: Automatically creates a new Contact record in Bitrix24 when the number is not found in existing CRM records. Leads: Automatically creates a new Lead record in Bitrix24 when the number is not found. Accounts: Automatically creates a new Account record in Bitrix24 when the number is not found.
Contact Lookups	Select from the "Available" list and move items to the "Selected" list to define where the UCM performs contact lookups in Bitrix24. Supported lookup tables include Contacts, Leads, and Organizations. When multiple tables are selected, the lookup order determines the priority of the search.

Once the Bitrix24 CRM settings on the admin interface are configured:

1. Click Save and Apply Changes.
2. Log out from the admin account.
3. Log in to the UCM as a user and navigate to **User Portal->Other Features->CRM User Settings**.
4. Enable CRM and enter the Bitrix24 account credentials information as required.
5. Click Save to complete the login process.

After successful login, the CRM status will change from Logged Out to Logged In, and the user can start using Bitrix24 CRM features during calls.

Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI **Integrations → CRM**.

CRM

CRM System:

Salesforce

* Add Unknown Number:

Contacts

Contact Lookups:

☐ 1 item Available

☐ Look up in Leads table

☐ 2 items Selected

☐ Look up in Contacts table

☐ 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:

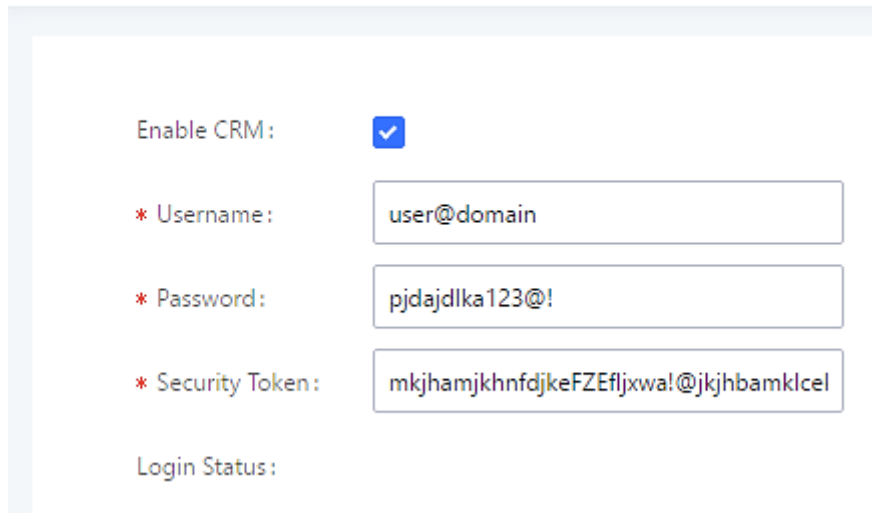
2. Click on and .

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:

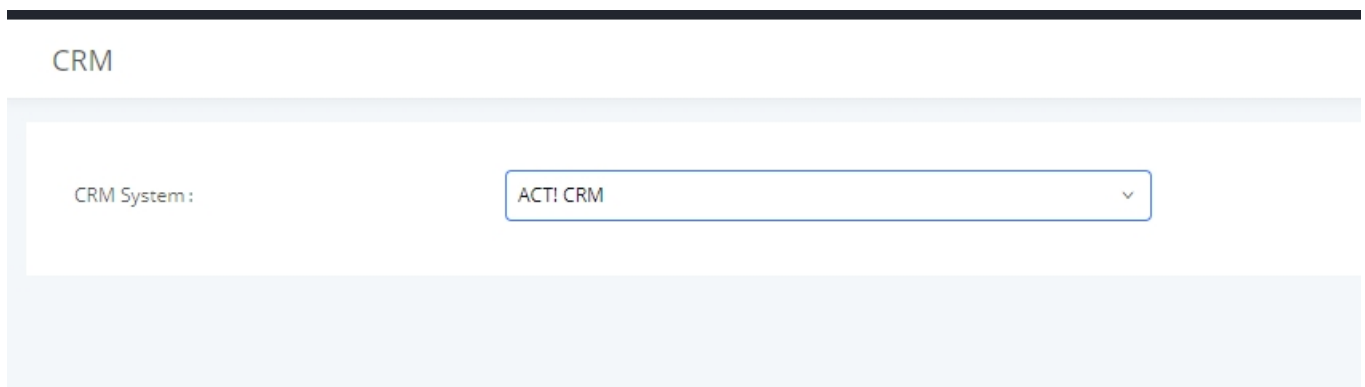
Salesforce User Settings

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.



CRM

CRM System:

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/>

CRM User Settings

Enable CRM:

☐

Username:

Password:

Login Status:

Enabling CRM on the User Portal

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**.

CRM

CRM System

ODOO CRM



* Add Unknown Number



Cancel

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

Cancel

Save

CRM User Settings

PMS INTEGRATION

UCM630xA supports Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI->**Integrations**->**PMS**.

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

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

Feature	Mitel	char pmslink	HSC	IDS	Oracle OPERA
Check-In	Yes	Yes	No	Yes	Yes
Check-out	Yes	Yes	No	Yes	Yes
Wake-up Call	Yes	Yes	No	Yes	Yes
Name Change	Yes	No	No	No	Yes
Update	No	Yes	No	Yes	Yes
Set Credit	Yes	No	No	No	No
Set Station Restriction	Yes	No	No	No	No
Room Status	No	Yes	No	Yes	Yes
Room Move	No	Yes	No	Yes	Yes
Do Not Disturb	No	Yes	Yes	No	Yes
Mini Bar	No	Yes	No	Yes	Yes

MSG	No	Yes	No	No	No
MWI	No	No	Yes	No	No
Unconditional Call Forward	No	No	Yes	No	No

Char pmslink

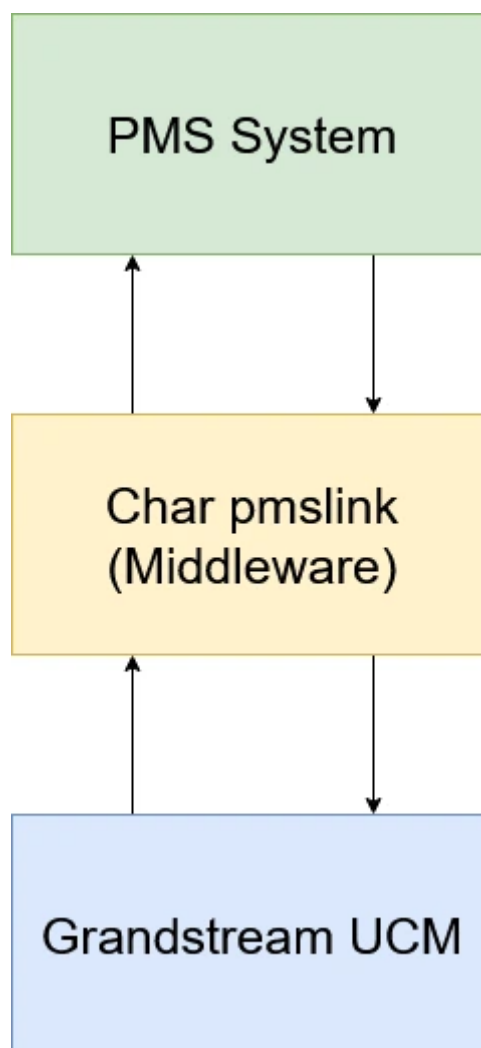
In this mode, the system leverages the **char pmslink** cloud middleware to integrate the UCM with a wide variety of Property Management System (PMS) software.

The communication flow is divided into three parts:

- **PMS (Property Management System):** Your hotel's management software.
- **charpmslink (Middleware):** Acts as the universal interface, translating messages between the PMS and the PBX.
- **PBX (UCM630xA):** The Grandstream UCM, which receives commands from the PMS via charpmslink to execute hospitality features.

This integration enables a large variety of hotel features such as: Check-in, Check-out, set Room Status, Wake-up call, and more.

The following figure illustrates the communication flow between the UCM and PMS software, which is done through a middleware system (char pmslink) acting as an interface between both parties.



UCM Char pmslink interaction

HSC PMS

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

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series has integrated HSC PMS providing the following features:

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

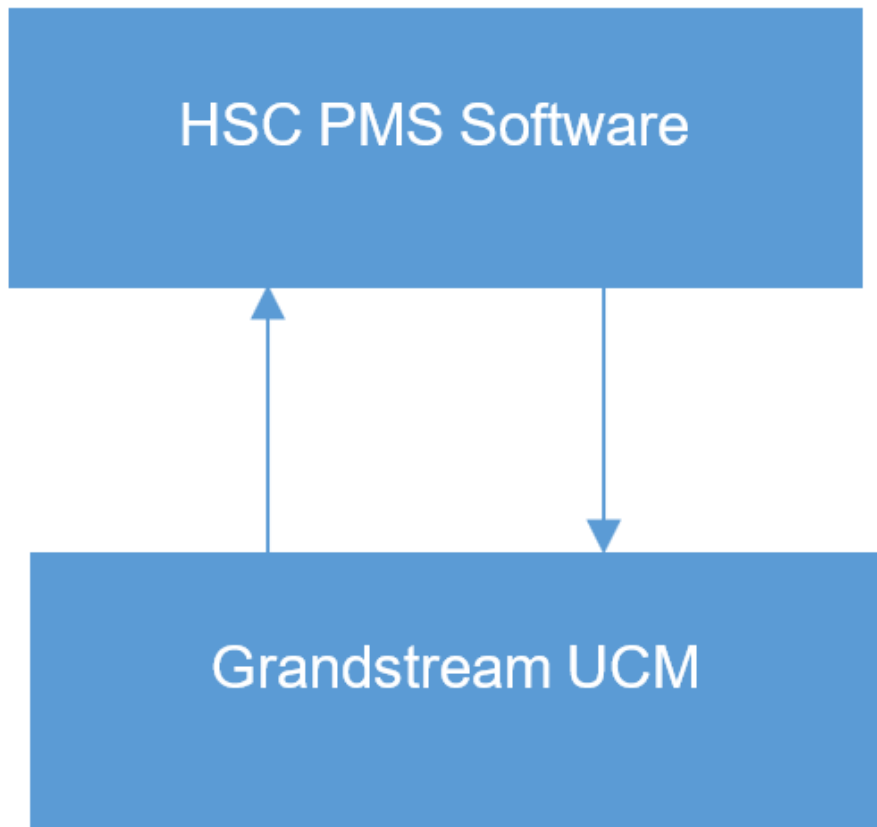
Notes:

1. Added support for receiving HTTP GET keep-alive messages from HSC PMS. This will allow the PMS to be aware of its connection to the UCM and take the appropriate actions such as raising alarms, sending notifications, etc.
2. Added support for HTTP GET requests from HSC PMS to retrieve UCM extension information. UCM can provide the following information:
 - extension - UCM extension number
 - name - extension display name / CID name
 - mwi - MWI state
 - permission - permission level of the extension
 - cfw - 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 UCM630xA Series) and PMS software (HSC). The communication between both parties is direct with no middleware.



UCM HSC PMS interaction

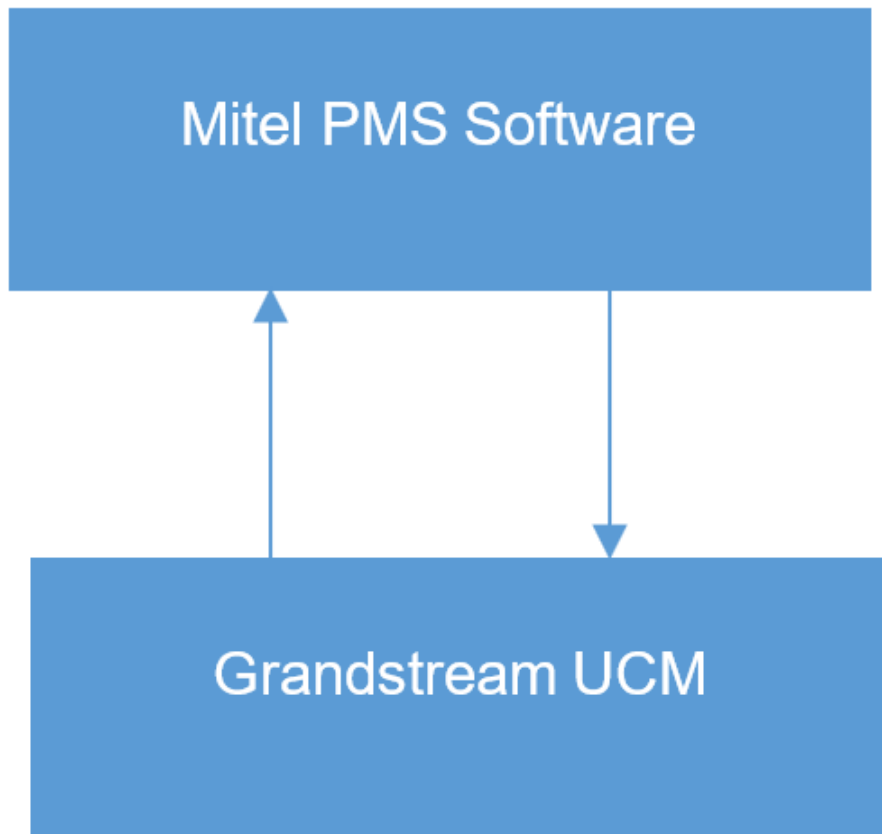
Mitel PMS

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

- PMS (Property Management System)
- PBX

Grandstream UCM630xA series has integrated Mitel PMS providing the following hospitality features: Check-in, Check-out, set Room Status, Wake-up call, and more.

The following figure illustrates the communication flow between the PBX (Grandstream UCM630xA Series) and PMS software (Mitel). The communication between both parties is direct with no middleware.



UCM Mitel PMS interaction

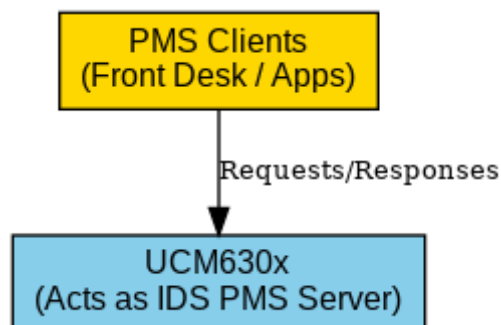
IDS PMS

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

- **PMS Clients** - These are the hotel management applications such as the front desk system, reservation software, or any client that normally communicates with a PMS server.
- **UCM PBX** - Instead of acting as a client or middleware, the UCM directly emulates an IDS PMS server.

With this setup, PMS clients connect directly to the UCM through its PMS port. The UCM listens for incoming requests and responds as if it were the IDS PMS server. This allows hotel staff to perform operations such as setting room status (clean, occupied, available), posting Mini Bar charges, scheduling and managing wake-up calls, or enabling and disabling dialing permissions.

By integrating IDS PMS in this way, the UCM simplifies deployment since no external IDS PMS server or additional middleware is required-the PBX itself provides the PMS server functionality.



UCM IDS PMS interaction

PMS AP

The PMS API allows users to use their middleware to work with PMS systems instead of currently supported integrations.

Additionally, this API allows access to read and modify certain UCM parameters that current supported PMS integrations cannot. To use this, users must first enable and configure the HTTPS API settings.

For more details, please refer to the online

<https://documentation.grandstream.com/knowledge-base/https-api/>, Pmsapi section.

Oracle Hospitality OPERA

The UM603xA series integrates directly with Oracle Hospitality OPERA PMS to manage room statuses and extensions from within the OPERA interface. This connection is established using the IFC_PBX interfacing protocol.

To configure the integration, first select the pre-built interface, "Oracle Hospitality OPERA TMS Interface for UCM Series PBX by Grandstream Networks," within the OPERA software. Once enabled, you can complete the setup from the CloudUCM admin portal.

Data exchange between the UCM and the OPERA server is handled by the Fidelio Interface Application Specification (FIAS) protocol. FIAS uses specific attributes to define the data being transmitted. For example:

- **"RN"** represents the Room Number.
- **"RS"** represents the Room Status.
- **"RU"** is used as an update indicator to initiate a room status change.

A typical FIAS message to update a room's status would be formatted as follows: **RU|RN211|RS3**

In this example, room 211 is updated to status code 3.

In addition, The UCM630xA supports Oracle OPERA's Youth Hostel Mode. This feature allows a single room to be partitioned into multiple independent units, enabling management of separate groups with distinct extensions and individual billing records within the same physical room.

PMS

- Basic Settings
- Room Management
- Room Status
- Wakeup Service
- Mini Bar
- Housekeeper

General

PMS Module

Oracle Hospitality OPERA

PMS URL

192.168.5.91

PMS Port

50001

Protocol Type

tcp

Prompt

Wakeup Prompt

Wake Call

Upload Audio File

Room Status Update Prompt

Default Room Status Update Pr...

Upload Audio File

Automatically Clear/Reset

Automatically Clear Phone Call History

Check Out

Automatically Clear Wakeup Calls

None

Automatically Clear Wave Chat History

None

Automatically Reset User/Wave Password

☐

Billing

Oracle Hospitality OPERA

General	
PMS Module	Select "Oracle Hospitality OPERA"
PMS URL	Enter the URL of the Oracle Hospitality Opera server.
PMS Port	Enter the PMS server port.Note: The allowed range 1 - 65535.
Protocol Type	Select the transport protocol to use.TCP: The connection is established using only TCP handshake.Simple SSL: Authentication is required to establish the connection. The identity is verified only on the Oracle OPERA Hospitality server.Mutual SSL: Authentication is required to establish the connection. The identity of both parties is verified by having both parties exchanging their certificates. This reinforces the security by ensuring that only the authorized parties are allowed to contact the server.
Prompt	
Wakeup Prompt	Upload the prompt to play when a wakeup call is answered, or used the default prompt.The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate.Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size.File name can only contain alphanumeric characters and special characters -_Mp3 and WAV formats are supported. If the user uploads an mp3 recording, it will be converted to WAV.

Room Status Update Prompt	Select the prompt to play when the room status is updated, or use the default prompt. The audio file must be less than 30 MB in file size with a file extension of .mp3/.wav/.ulaw/.alaw/.gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate. Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size. File name can only contain alphanumeric characters and special characters - _
Automatically Clear/Reset	
Automatically Clear Phone Call History	Select when to clear phone call history. None: The phone call history will not be cleared. Check Out: The phone call history of the guest will be cleared upon checking-in. Check In: The phone call history will be cleared when checking-in a new guest.
Automatically Clear Wake Up Calls	Select when to clear scheduled Wakeup calls. None: The wake-up call configuration will not be cleared. Check In/Out: The wake-up call configuration will be cleared upon either checking-in or checking-out. Check Out: The wake-up call configuration will be cleared upon checking-out. Check In: The wake-up call configuration will be cleared upon checking-in.
Automatically Clear Wave Chat History	Select when to clear Wave chat history. None: Wave chat history will not be cleared. Check Out: Wave chat history will be cleared upon checking-out. Check In: Wave chat history will be cleared when checking-in a new guest.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
Billing	
Type of Call Billing	Select the type of billing the call fees for the guests. Send to Oracle PMS: The call details will be sent and calculated on Oracle Opera. PBX Direct Billing: The billing will be calculated by the UCM and synchronized with Oracle Opera.
Mini Bar Billing Type	Select the type of billing the mini bar. Send to Oracle PMS: The consumed mini bar goods will be pushed to Oracle Opera where they will be processed for the billing. PBX Direct Billing: The consumed mini bar goods will be processed for billing on the UCM, and the bill will be synchronized with Oracle Opera.
Other	
Back Up Voicemail Recordings	Back up voicemail recordings to external storage after check-out. When this option is enabled, the user can select the storage location option, SD Card, USB 1, USB 2, NAS, or SFTP Server. The user can also specify an email address to send voicemail recordings for archiving purpose.
Sync Guest Name to Phone	Provisions the name of checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisionable by Zero Config.

Local PMS

The UCM6300 series includes an integrated on-premise Property Management System (PMS), providing essential hospitality management capabilities directly from the Web GUI under **Integrations -> PMS** without requiring external software licenses.

The local PMS solution manages core hotel operations including Room Management, Reservation and Check-in/Check-out management, Hourly Room rentals, Minibar consumption tracking, Wake-up Services, and more.

Key highlights and features supported by the Local PMS include:

- **Custom Hotel Branding:** Configure hotel logos, contact phone numbers, website, and a QR code to customize printed bills and automated self-check-in/check-out emails.
- **Self Check-in and Check-out:** Guests can check in and check out using emails automatically sent by the UCM for reservations.

- **Room & Calendar Management:** Real-time Room Availability Calendar, itemized bill printing (breakdowns for taxes, room charges, and minibar items), and hourly room options.
- **Guest List:** Stored database of guests which helps with future bookings and retains guest information for quick reference.

For detailed step-by-step configuration guides and operational workflows, refer to the Local PMS Guide.

<https://documentation.grandstream.com/knowledge-base/ucm63xx-local-pms-guide>

PMS
Basic Settings
Room Management
Check-in Management
Wakeup Service
Mini Bar
Housekeeper

General
PMS Module
Hotel Name
Address
Hotel Phone Number
Hotel Email
Hotel Website
Logo
QR Code
Prompt
Wakeup Prompt
Room Status Update Prompt
Automatically Clear/Reset
Automatically Clear Phone Call History

Local PMS
Hotel
123456
987654
email@test.com
test.com

Supports JPEG, JPG, and PNG images up to 5 MB in file size.

Supports JPEG, JPG, and PNG images up to 5 MB in file size.
Wake Call
Add Audio
Default Room Status Update Prompt
Add Audio
None

The configuration parameters available under Local PMS Basic Settings are explained in the table below:

Parameter	Description
General	
PMS Module	Selects the Local PMS module functionality.
Hotel Name	Configures the official hotel name to be displayed on guest bills, and emails.
Address	Configures the hotel physical address displayed on bills and emails.
Hotel Phone Number	Configures the contact phone number printed on bills and emails.
Hotel Email	Configures the official hotel email address used for bills and emails.
Hotel Website	Configures the hotel website URL printed on guest bills and emails.
Logo	Uploads a custom hotel logo for printed bills and automated emails. Supports JPEG, JPG, and PNG formats up to 5 MB.
QR Code	Uploads a custom QR code (e.g., for online hotel guides) displayed on printed bills and automated emails. Supports JPEG, JPG, and PNG formats up to 5 MB.
Prompt	
Wakeup Prompt	A customized prompts that can be played when the wakeup call is answered. To customize it please navigate to PBX Settings->Voice Prompt->Custom Prompt.

Room Status Update Prompt	Choose a previously uploaded prompt or upload the prompt which will be played when the room status is changed. If the room status codes have been change, please update the Room Status accordingly.
Automatically Clear/Reset	
Automatically Clear Phone Call History	Configures whether or not the call history of phones will be automatically cleared upon check-in or check-out. Currently only supported on Grandstream phones. None: Call history will not be deleted after checking-in or checking-out. Check Out: Call history will be delete when the guest checks-out. Check In: Call history will be delete when a new guest checks-in.
Automatically Clear Wakeup Calls	Scheduled wakeup calls for rooms can be cleared upon checking in or checking out. None: The wakeup calls won't be automatically cleared. Check out: The wake up calls assigned to the guest will be cleared when they check out. Check In: The wake up calls assigned to a guest will be cleared when a new client checks in.
Automatically Clear Wave Chat History	If enabled, room Wave chat history will be automatically cleared upon check-in or check-out.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
Self-service Settings	
Self-Check-In Via Email	Enables the system to automatically send a self check-in email with a link prior to the guest's arrival.
Check-in Email Template	Selects the email template used for sending automated self check-in notifications.
Send in Advance (hrs)	Defines how many hours before the scheduled check-in time the self check-in email will be sent. (Range: 0 - 6 hours).
Self-Check-Out Via Email	Allows the system to automatically send a self check-out email with a link prior to departure.
Check-out Email Template	Selects the email template used for sending automated self check-out notifications.
Send in Advance (hrs)	Defines how many hours before the scheduled check-out time the email will be delivered. (Range: 0 - 6 hours).
Allow Check-out with Unsettled Bill	Controls whether guests are allowed to complete self check-out even if their bill is not fully paid. Enabled: The guest may check out before completing the payment. Disabled: Payment must be settled before self-check-out is allowed. This option is disabled by default.
Other	
Back Up Voicemail Recordings	Configures automatic backup of voicemail recordings to external storage after check-out. When this feature is enabled, users can specify the storage destination.
Storage Location	Select the storage location for voicemail recordings. The available options are: SFTP Server NAS USB SD Card Note: To configure storage devices, go to PBX Settings->Storage Device Management.
Email Address	Enter the destination email address where the system will deliver backup files.
Sync Guest Name to Phone	Provisions the name of the checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisionable by Zero Config.
Review Bill at Check-Out	If enabled, a pop-up window with all the charges will appear during guest check-out for reviewing purposes.
Call Billing	
Call Rate	Configures call charge rates for outbound calls made from guest room extensions.

Currency Unit	The currency unit for the call rate. These are the supported options which you can choose from: American Dollar Euro Sterling Pound Yen Won Hong Kong Dollar Australian Dollar Canadian Dollar Baht Singapore Dollar Swiss Franc Swedish Krona Danish Krone Norwegian Krone New Zealand Dollar South African Rand Brazilian Rial Indian Rupee Russian Ruble Vietnamese Dong Polish Zloty Czech Koruna Turkish Lira Custom: Enter the currency unit.
Periodically Send Records to Email	If enabled, new recordings will be automatically sent to the specified email inbox periodically at the specified intervals.
Type	Configures the type of recordings that should be sent periodically: Wakeup Service Check-in/Check-out History CDR Records
Period	Specifies the automatic download period. The default option is "By Day". At the specific time of each day, week or month, the last cycle of new records will be sent to the user. By Day By Week By Month
Email	Specifies the automatic download period. The default option is "By Day". At the specific time of each day, week or month, the last cycle of new records will be sent to the user.
Guest Email	
Customer Email	Enables the system to send automated emails to guests. This includes reservation updates and billing information. Note: Email notifications will not be sent if the customer's email address is missing.
Reservation Notification	When enabled, the guest will automatically receive an email whenever a reservation is created, modified, or cancelled.
Billing Notification	If enabled, billing-related emails will be sent automatically to the guest.
Email Template	Selects or edits custom email templates used for reservation and billing notifications.

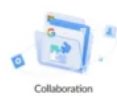
INTEGRATION OF COLLABORATION PLATFORMS

The UCM6300/A Series supports integration with enterprise collaboration and identity platforms to centralize user management, authentication, and directory synchronization. These integrations allow administrators to synchronize user identity information from external platforms into the UCM, associate users with extensions or system accounts, and enable Single Sign-On for simplified and secure access to the UCM web interface.

Supported platforms include:

- **Microsoft Entra ID (Azure AD)**
- **Windows Active Directory**
- **Google Workspace**

Deep integration with mainstream identity providers (such as Microsoft Entra ID, Windows AD, and Google Workspace) enables centralized user account management and automated extension provisioning. Employees can use enterprise Single Sign-On (SSO) to log into UCM/Wave clients, significantly improving security and operational efficiency.



Collaboration



User Synchronization



Single Sign-on (SSO)



Contacts Sync

Supported Platform



Microsoft Entra ID (Azure AD)
Connected

[Configuration Manual](#)[Integration](#)

Windows AD
Connected

[Configuration Manual](#)[Integration](#)

Google Workspace
Connected

[Configuration Manual](#)[Integration](#)*Integration of Collaboration Platforms Page*

Each integration provides configurable options for user synchronization scope, user linking behavior, LDAP directory integration, and authentication methods. The following sections describe the configuration and usage of each platform.

Microsoft Entra ID (Azure AD)

Microsoft Entra (formerly Azure Active Directory) is a cloud platform which provides access management and identity provision. When integrated with the UCM6300 Series, it allows synchronizing the identity information with the UCM which can be used to log into the UCM's user interface.

For step-by-step configuration guide for Microsoft Entra, please refer to the following link:

<https://documentation.grandstream.com/knowledge-base/microsoft-entra-id-azure-ad-configuration-guide/>

The Microsoft Entra ID configuration page consists of the following tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-On (SSO)**

Each tab is described below.

Basic Settings

This tab defines the connection between the UCM and Microsoft Entra ID.

Microsoft Entra ID (Azure AD)

Basic Settings User Settings Single Sign-on (SSO)

✔

Authorized Account:
Connected

Authorization

Microsoft Entra ID Authorization

ⓘ

Copy the application information that has been created in Microsoft Azure and fill it in below.

* Redirect URIs

* Application (Client) ID

* Client Password

.....

* Tenant ID

For more information about Microsoft Entra ID (Azure AD), see [Microsoft Entra ID \(Azure AD\) Configuration Manual](#).

Cancel

Save and Authorize

Microsoft Entra ID Basic Settings

Parameter	Description
Microsoft Entra ID Authorization	Enable Microsoft Entra ID
Redirect URIs	Enter a URI to return Microsoft tokens.
Application (Client) ID	Enter the application ID
Client Password	Enter the client password. If the client's password expires, this will interrupt Microsoft user synchronization. Ensure that the password is updated in a timely manner.
Tenant ID	Enter the tenant ID provided by Microsoft. This can be found in the admin center of Microsoft Entra ID.

User Settings

This tab controls how Microsoft users are synchronized to the UCM.

Microsoft User

Get Microsoft User



When enabled, Microsoft users can be associated one-to-one with system users/extensions in UCM.

User Range ⓘ

Specify Type User

* User Type

Guest ×

Add User to LDAP ⓘ



Linked User Settings

Linked UCM



If enabled, the linked UCM user's information (first name, last name, email, mobile number, job title) will be overwritten by the Microsoft user's information.

Linking Method ⓘ

☒ Automatic Link ☐ Manual Link

Linked User Range

Specify Type User

* Linked User Type

Members ×

Link Policy ⓘ

Read Attribute Value

Attribute Name

BusinessPhones

Cancel

Save

The table below describes the parameters available on this tab

Get Microsoft User	
Get Microsoft User	Enable to retrieve users from Microsoft Entra ID. When enabled, Microsoft users can be associated with UCM users/extensions. When disabled, synchronization is stopped.
User Range	Defines the scope of Microsoft users to retrieve. Options include retrieving all users or specifying user types.
User Type	Available when "Specify Type User" is selected. Defines which Entra user types (e.g., Members, Guest) will be retrieved. Only selected types are synchronized.
Add User to LDAP	When enabled, synchronized Microsoft users are added to the UCM LDAP directory, allowing them to appear in LDAP searches and dialing features.
Linked User Settings	
Linked UCM	Enable to associate Microsoft Entra users with existing UCM users/extensions. When enabled, the linked UCM user's information will be overwritten by the Microsoft user's information.
Linking Method	Defines how Microsoft users are linked to UCM users. Automatic Link: The system automatically matches Microsoft users to UCM users based on defined matching rules. Manual Link: Administrator must manually associate users.
Linked User Range	Specifies which UCM users are eligible for linking. Options include linking all users or only selected user types.
Linked User Type	Available when "Specify Type User" is selected. Defines the Entra user categories (e.g., Members) that are eligible for linking.
Link Policy	Defines how the extension number is assigned during automatic linking. Available options are: Automatic Allocation: assigns extensions sequentially, starting from a specified number. Read Attribute Value: The extension number is taken from a specified Microsoft Entra user attribute.

Additionally, enabling Single Sign-On (SSO) allows AD users to log in to the UCM web interface using their domain credentials, enhancing security and simplifying password management.

For step-by-step configuration guide for Windows AD, please refer to the following link:
<https://documentation.grandstream.com/knowledge-base/windows-ad-configuration-guide/>

Windows AD

Basic Settings

Unconnected

Windows AD

* Server Address

192.168.1.1

IPv4 Address

* Domain

* Port

389

Range 1 - 65535

* Username

1 - 64 characters

* Password

At least 4 bits

* Filter

(objectClass=*)

* Base DN

dc=pbx,dc=com

1 - 128 characters, supports numbers, letters, chinese characters, and special characters _

* Phone Book Name

LdapClient

* AD properties

☐ All

☒ telephoneNumber

☐ mail

☐ displayName

☐ givenName

☐ sn

☐ mobile

☐ homePhone

☐ facsimileTelephoneNumber

☒ userPrincipalName

☐ department

☐ title

Cancel

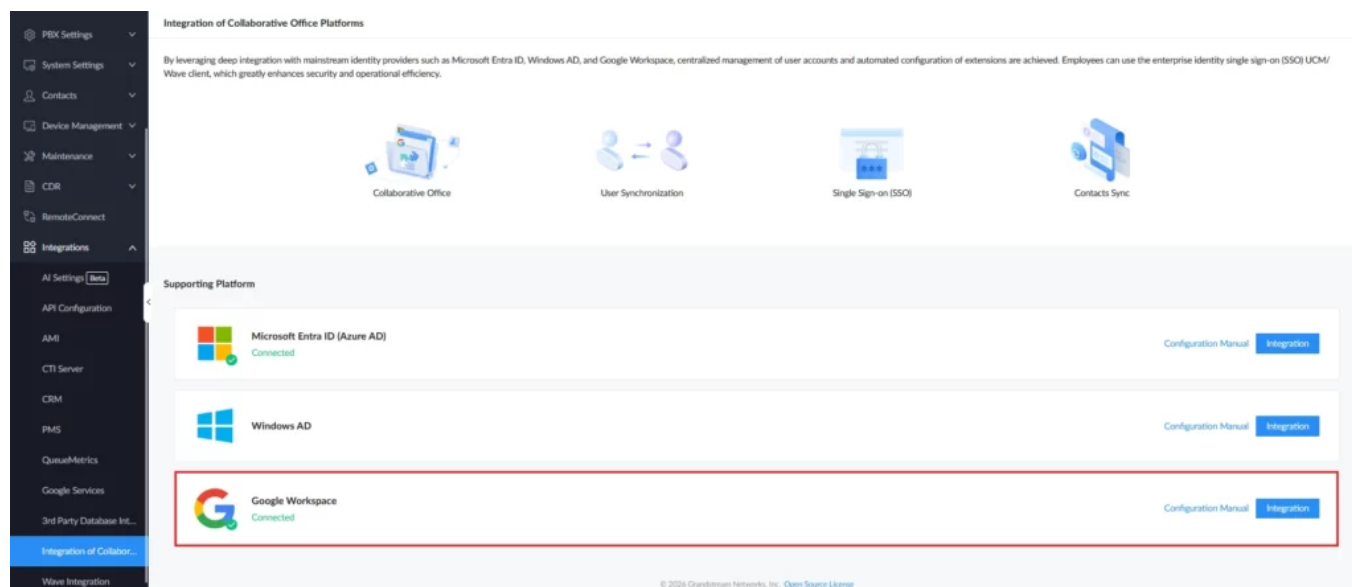
Save and Connect

Parameter	Description
Windows AD	Toggle on/off the Windows AD integration
Server Address	Enter the AD server address.
Domain	Enter the domain
Port	Enter the port to use. The port number must be within the range 1 - 65535
Username	Enter the username.
Password	Enter the password.
Filter	Enter the filter which can be an object class.
Base DN	Information about the AD node to be pulled, for example,dc=pbx,dc=com.
Phonebook Name	Enter the phonebook name.
AD Properties	Select the AD properties which can be used by the UCM.

Google Workspace Integration

The Google Workspace Integration allows the UCM Series to connect with a Google Workspace domain in order to synchronize user identity information and enable Single Sign-On (SSO). When enabled, Google users can be associated with UCM system users or extensions, optionally synchronized into the UCM LDAP directory, and used for authentication when accessing the UCM web interface.

This feature is configured under **Integrations->Integration of Collaborative Office Platforms->Google Workspace**.



Integration of Collaborative Office Platforms Page

The Google Workspace integration module consists of three tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-on (SSO)**
- **Google Calendar**

For detailed configuration procedures refer to the **Google Workspace Integration Guide**.

Basic Settings

The Basic Settings tab is used to configure OAuth authorization between the UCM and Google Workspace. This step is mandatory before any user synchronization or SSO functionality can be enabled.



Connected

For more information about Google Workspace, see [Google Workspace Configuration Manual](#).

Google Workspace Authorization



Enter your Google Workspace app details below.

* Redirect URIs

* Application (Client) ID

* Client Password

Google Workspace Basic Settings Tab

The table below describes the parameters of this page:

Parameter	Description
Google Workspace Authorization	Enables or disables Google Workspace integration on the UCM.
Redirect URIs	OAuth redirect URI used to receive authorization tokens from Google. This value must exactly match the redirect URI configured in the Google Cloud Console application.
Application (Client) ID	OAuth Client ID generated in Google Cloud Console for the Workspace application.
Client Password	OAuth Client Secret associated with the Client ID. If the client secret expires or is regenerated, it must be updated here to avoid authorization failure.

User Settings

The User Settings tab controls how Google Workspace users are retrieved, synchronized, and linked to UCM users or extensions. The settings on this page are grouped into three categories:

1. **Google User**
2. **Linked User Settings**
3. **Google User Management**

The sections below describe each of the Google Workspace user settings tab categories.

Integration of Collaborative Office Platforms > Google Workspace

Basic Settings User Settings Single Sign-on (SSO)

Google User

Get Google User

☒

When enabled, Google users can be associated one-to-one with system users/ extensions in UCM.

User Range

Users within the designated group

* Groups

Tech Support

Add User to LDAP

☒

Linked User Settings

Linked UCM

☒

If enabled, the linked UCM user's information (first name, last name, email, mobile number, job title) will be overwritten by the Google user's information.

Linking Method

☐ Automatic Link
 ☒ Manual Link

☒ After saving, edit the link on the right side of the Google users table below.

Cancel

Save

Google User

Sync Now

Search Link

Sync Settings

Mobile Number / Link UCM User

☐	User	First Name	Last Name	Mobile Number	Job Title	Link UCM User	Options
☐	antonio.brock@gptest.com	Antonio	Brock				Link
☐	glenn.horton@gptest.com	Glenn	Horton				Link
☐	roberta.sullivan@example.com	Robert	Sullivan	67000		67000	Link

Google Workspace User Settings Tab

Google User

This section defines how Google Workspace users are retrieved from the domain and whether they are synchronized into the UCM system.

Google User

Get Google User

☒

When enabled, Google users can be associated one-to-one with system users/extensions in UCM.

User Range

Users within the designated group

* Groups

Tech Support

Add User to LDAP

☒

User Settings Google User

Parameter	Description
Get Google User	Enables/disables retrieval of users from the connected Google Workspace domain. When enabled, Google users can be listed and managed on the UCM.
User Range	Specifies the scope of Google Workspace users to retrieve. The available options are: All Users: Retrieves all users from the Google Workspace domain. Users within the designated organizational unit: Retrieves users from a specific Google Workspace organizational unit. Users within the designated group: Retrieves only users who belong to one or more specified Google Workspace groups.
Organizational Unit	Specify the Google Workspace Organizational Units whose users will be retrieved.
Groups	Specify the Google Workspace Groups whose users will be retrieved.

and user linking.

Google User

Sync NowBatch LinkSync Settings

Q Mobile Number / Link UCM User

☐	User	First Name	Last Name	Mobile Number	Job Title	Link UCM User	Options
☐	antonio.brock@gsdevtest.com	Antonio	Brock				
☐	glenn.horton@gsdevtest.com	Glenn	Horton				
☐	angela.wright@gsdevtest.com	Angela	Wright	5000		5000	

Total 3110 / pageGoto

User Settings Google User List

Parameter	Description
Sync Now	Immediately retrieves the latest user information from Google Workspace based on the current User Settings configuration.
Sync Settings	Opens the Google Workspace Sync Settings page, which allows configuration of automatic extension deletion policies (for deleted, paused, or unlinked Google users), scheduled synchronization, and provides visibility into synchronization history.
Batch Link	Available when Manual Link is selected. Allows multiple Google users to be linked to UCM users or extensions in a single operation.
Google User List Table Columns	User (email address) First Name Last Name Mobile Number Job Title Linked UCM User Note: For manually linked users, the Options column provides controls to link, modify, or remove the association with a UCM user or extension.

The **Sync Settings** page is used to define how Google Workspace user data is synchronized with the UCM and how linked extensions are handled during synchronization events. This page is accessed by clicking Sync Settings from the Google User List section.

Integration of Collaborative Office Platforms > Google Workspace > Sync Settings

Extensions

Automatically Delete Extensions of

☐ Deleted Google Workspace users
☐ Paused Google Workspace users
☐ Unlinked Users

Google User Data Sync

1

Data synchronization includes obtaining the latest Google users and updating the association between Google users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours.

Scheduled Sync

Cancel

Save

Sync History

Sync Time	Sync Mode	Results	Options
2026-02-09 14:10:04	Manual sync	Success	
2026-02-09 14:09:56	Manual sync	Success	
2026-02-05 16:59:40	Manual sync	Success	
2026-02-05 15:11:11	Manual sync	Success	

Google Workspace Sync Settings

The **Extensions** section controls automatic cleanup behavior for UCM extensions based on Google Workspace user status:

- **Deleted Google Workspace users:** Automatically deletes the linked UCM extension when the corresponding Google Workspace user is deleted.
- **Paused Google Workspace users:** Automatically deletes the linked UCM extension when the corresponding Google Workspace user is suspended or paused.
- **Unlinked Users:** Automatically deletes UCM extensions that are no longer linked to any Google Workspace

user.

Extensions

Automatically Delete Extensions of ⓘ

☐ Deleted Google Workspace users

☐ Paused Google Workspace users

☐ Unlinked Users

Extensions Sync Settings

The **Google User Data Sync** section controls how and when Google Workspace user data is synchronized. When **Scheduled Sync** is enabled, the UCM automatically retrieves the latest Google Workspace users and updates the association between Google users and UCM users or extensions according to the current configuration.

Data synchronization may temporarily impact system performance. It is recommended to perform synchronization during non-office hours.

Google User Data Sync

ⓘ Data synchronization includes obtaining the latest Google users and updating the association between Google users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours.

Scheduled Sync

☒

Sync Time

By Day ▾

04:00 ▾

Cancel

Save

Google User Data Sync Settings

The **Sync History** section displays historical records of Google Workspace synchronization activities. The following information is shown for each synchronization event:

- **Sync Time:** Date and time when the synchronization was executed.
- **Sync Mode:** Indicates whether the sync was triggered manually or by schedule.
- **Results:** Displays the synchronization result (Success, Partial Success, or Failed).
- **Options:** Provides access to detailed synchronization logs for troubleshooting purposes.

Sync History

Sync Time	Sync Mode	Results	Options
2026-02-09 14:10:04	Manual sync	Success	ⓘ
2026-02-09 14:09:56	Manual sync	Success	ⓘ
2026-02-05 16:59:40	Manual sync	Success	ⓘ
2026-02-05 15:11:11	Manual sync	Success	ⓘ
2026-02-05 15:10:46	Manual sync	Partial Success	ⓘ
2026-02-05 15:10:34	Manual sync	Success	ⓘ
2026-02-05 15:10:30	Manual sync	Failed	ⓘ
2026-02-05 15:08:56	Manual sync	Failed	ⓘ

Google Workspace Sync History

Single Sign-On (SSO)

The Single Sign-On (SSO) tab controls Google-based authentication for accessing the UCM web interface. This page is used to enable or disable Google Workspace SSO and define how Google-authenticated users are mapped to UCM system users.

- For Google Workspace SSO to function, **at least one Google Workspace** user must be successfully linked to a UCM system user. SSO authentication will fail if no linked user exists.
- Google Workspace SSO requires the UCM to be accessed using a **valid domain name (FQDN)**. Accessing the UCM via a private IP address is not supported and will trigger a warning during OAuth authorization.

Integration of Collaborative Office Platforms > Google Workspace

Basic Settings User Settings Single Sign-on (SSO)

Single Sign-on (SSO)

☒

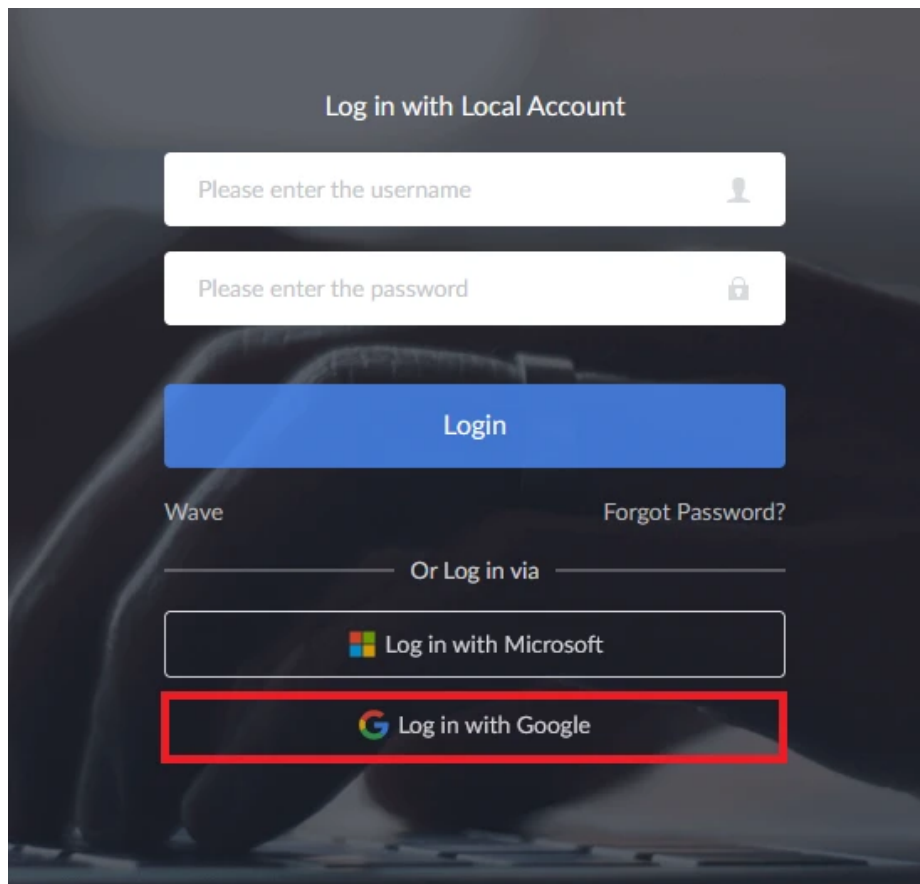
If enabled, users will be able to log into the webUI and Wave with their linked Google account.

Cancel

Save

Google Workspace Single Sign on SSO Tab

If SSO is enabled, the Sign in with Google option will appear on the UCM login page.



Log in with Google Option for UCM

Detailed configuration flows, and OAuth authorization steps for Google Workspace SSO are covered in the **Google Workspace Integration Guide**.

Google Calendar

The Google Calendar tab allows administrators to synchronize Google Calendar schedules with PBX extension presence statuses, enabling automated call routing policies based on a user's calendar availability.

- Please complete the relevant configurations in Google Workspace before setting up this page. For more information, see the Google Calendar Usage Guide.
- If extension presence status sync is behaving abnormally, please re-authorize Google Workspace before enabling Google Calendar to ensure the feature works properly

① Please complete the relevant configurations in Google Workspace before setting up this page. For more information, see [Google Calendar Usage Guide](#).
If extension presence status sync is behaving abnormally, please re-authorize Google Workspace before enabling Google Calendar to ensure the feature works properly.

Google Calendar Sync



① If enabled, the schedules of associated users can be retrieved and synced to the PBX extension's presence status to configure different call policies.

* Key File

google_workspace_service_account_key.json

Scheduled Sync

Every Day

10:00

Real-time Update via Webhook



* WebHook URL ①

https://[redacted].b.gdms.cloud/calendar-webhook

[Auto Obtain](#)

① Using the Webhook URL requires the domain to be verified by Google.

Enable Calendar Sync for Extensions

▼ 0 item

Available

No data

▼ 0 item

Selected

No data

Cancel

Save

The table below describes the parameters available on the Google Calendar tab:

Parameter	Description
Google Calendar Sync	Enables or disables Google Calendar synchronization. When enabled, the schedules of associated users are retrieved and synced to PBX extensions' presence status to apply dynamic call policies.
Key File	Upload or select the service account JSON key file generated in Google Cloud Console for API authentication.
Scheduled Sync	Configures the periodic sync schedule (e.g., Every Day at a specified time) to fetch calendar updates.
Real-time Update via Webhook	Enables real-time event updates via Google push notifications using a Webhook URL.
WebHook URL	Specifies the Webhook URL used to receive real-time calendar updates. Clicking the Auto Obtain button automatically populates it with the UCMRC domain URL. Note: Using the Webhook URL requires domain verification in Google Console.
Enable Calendar Sync for Extensions	Select extensions from the Available list and move them to the Selected list to enable calendar-based presence sync for specific extensions.

Using the Real-time Update via Webhook feature requires domain verification in Google Search Console:

- **Custom Domain:** If using your own domain, follow the Google Search console instructions to complete verification.

- **UCMRC Subdomain:** If using UCMRC domain, please contact Technical Support to assist with the verification.

When a scheduled event occurs on a linked user's Google Calendar, the UCM automatically updates the extension's SIP presence status to Do Not Disturb (DND) for the duration of the event window. Any call routing rules or forwarding policies configured for the DND status will apply automatically during the event.

SAML SSO

SAML Single Sign-On (SSO) is an enterprise-grade identity authentication solution that allows the UCM6300 series to integrate with external Identity Providers (IdP) such as Microsoft Entra ID, Okta, OneLogin, or AD FS. Once configured, users can authenticate via their organization's centralized identity provider to access the UCM Web UI without managing separate local credentials.

This feature is configured under **Integrations -> Integration of Collaborative Office Platforms -> SAML SSO**.

For step-by-step instructions on configuring external Identity Providers (Entra ID, AD FS, etc.) to pair with the UCM, please refer to the SAML SSO Configuration Guide.

SAML SSO Configuration

To enable SAML SSO, configure the Identity Provider credentials, Service Provider details, and user mapping rules under the SAML SSO tab.

Collaborative Office Integration

Enterprise Platform **SAML SSO**

SAML SSO

IdP Entity ID 1 - 128 characters

X.509 Cert SHA1 Fingerprint 0 - 512 characters

SSO Login URL 1 - 256 characters

User Mapping Attribute Name 1 - 256 characters

Reply URL [Click to copy](#)
Before using SSO, please fill this URL into the SAML Service Provider configuration.

Identifier ID [Click to copy](#)

[Learn more about SAML SSO with the SAML SSO Configuration Guide](#)

[Cancel](#) [Save](#)

UCM/IdP User Association

[Add](#) [Delete](#) [Batch Link](#) [Refresh](#)

UCM User	IdP User	Options
☐ John	John@emeags.onmicrosoft.com	Link Delete

Total: 1 [1](#) 10 / page

The table below describes the parameters available on the SAML SSO page:

Parameter	Description
SAML SSO	Enables or disables SAML Single Sign-On integration on the UCM.
IdP Entity ID	Enter the unique entity identifier (Issuer URL) provided by your Identity Provider. Used as a mechanism to validate SAML responses.
X.509 Cert SHA1 Fingerprint	Enter the SHA1 fingerprint of the IdP's X.509 signing certificate for response validation.

SSO Login URL	Enter the Single Sign-On service endpoint URL provided by your IdP where UCM will redirect authentication requests.
User Mapping Attribute Name	Specifies the attribute name on the IdP side used for user mapping. The value of this attribute for the IdP user must have a one-to-one correspondence with the UCM user/extension (it is recommended that the value be unique on the IdP side). Example: userName, email.
Reply URL	Use Click to copy to copy the Assertion Consumer Service (ACS) URL of the UCM and paste it into the SAML Service Provider configuration on the IdP side.
Identifier ID	Use Click to copy to copy the SP Entity ID of the UCM and paste it into the SAML Service Provider configuration on the IdP side.

Account Linking

Before users can log in via SAML SSO, their enterprise IdP attribute value must be mapped to a corresponding UCM user account.

To associate accounts:

1. Click **Add** to open the Account Linking dialog.
2. Select the target **UCM User** from the drop-down menu.
3. In the **IdP User** field, enter the exact attribute value (e.g., user email address or username) corresponding to the configured User Mapping Attribute Name.
4. Click **OK** to save the association.

Account Linking [X]

UCM User: 1012 [v] → IdP User: sarah@emeags.onmicrosoft.com [trash]

[+ Add]

[Cancel] [Save]

Logging in with SAML SSO

Once SAML SSO is enabled and user accounts are linked, a **Log in with SAML** option will appear on the UCM Web UI login page. Clicking this option redirects the user to the configured Identity Provider login page. Upon successful authentication, the user is redirected back to the UCM Web UI and logged in automatically.

Welcome to the UCM6302

Log in with Local Account

Please enter the username



Please enter the password



Login

Wave

Forgot Password?

Or Log in via

Log in with Radius

Log in with SAML

Log in with SAML

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:

GS_Wakeup

Prompt:

wakeup-call

Prompt

Custom Date:

☐

* Date:

2017-08-11

* Time:

14:00

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.

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

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

Max Wakeup Members

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

and

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.

* Listen Spy:

*54

* Barge Spy:

*56

* PMS Wakeup Servi...

*35

✓

* Presence Status:

*48

✓

* Whisper Spy:

*55

* Wakeup Service:

*36

✓

* Update PMS Room...

*23

✓

Feature Codes

- 1. Click

and

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.

Announcement Center

+ Add Announcement Center

Code	Name	Options
123	Test_1	 

Total: 1 < 1 > 10 / page ▼ Goto

+ Add Group

Number	Name	Members	Options
1	Test	500050015002	 

Total: 1 < 1 > 10 / page ▼ Goto

Announcements Center

Announcement Center Settings

Announcement Center > Create New Announcement Center

* Name

* Code

* Custom Prompt

 Upload Audio File

* Ring Timeout (s)

* Auto Answer

* Call Privileges

Announce Message
Caller-ID

☐

Cancel

Save

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

Group Settings

Group Settings

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

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

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.

Create New Group

* Name :

GStest

* Number :

666

Members :

☐ 27 items

Available

Search

☐ 1003

☐ 1004

☐ 1005

☐ 1006

☐ 1007

<

>

☐ 3 items

Selected

Search

☐ 1000

☐ 1001

☐ 1002

Announcement Center Group Configuration

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

1. Click

to create a new Announcement Center.

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

Create New Announcement Center

* Name :	GStest
* Code :	55
* Custom Prompt :	Lee_Rosevere_-_12_-_Were_Almost_There-... Upload Audio File
* Ring Timeout :	30
* Auto Answer :	No

Announcements Center Code Configuration

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

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the 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.

Announcement Center

+ Add Announcement Center

CODE	NAME	OPTIONS
55	GStest	 

< 1 >

Total: 1 10 / page Goto 1

+ Add Group

NUMBER	NAME	MEMBERS	OPTIONS
666	GStest	1000 1001 1002	 

< 1 >

Total: 1 10 / page Goto 1

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.

QueueMetrics

Enable QueueMetrics Integration



* QueueMetrics URL

* Username

webqloader

* Webqloader Password

.....

Partition

Outbound Call Tracking



Cancel

Save

QueueMetrics

Parameter	Description?
Enable QueueMetrics Integration	Tick this box to enable QueueMetrics integration module.

QueueMetrics URL	Enter the URL of the QueueMetrics on-premise server you have installed. (i.e. http://xxx.xxx.xxx.xxx:8080/queuemetrics.).
Username	Please enter the username used to interface with QueueMetrics. This is typically the QueueMetrics webqloader user. Please confirm that the user is enabled to avoid connection failure.
Webqloader Password	Please enter the webqloader password.
Partition	Enter the data storage partition identifier
Outbound Call Tracking	If enabled, QueueMetrics will track the outgoing calls of all extensions. Note: Outbound Call Tracking is available only on the PBX.

Queue Metrics configuration parameters

3RD PARTY DATABASE INTEGRATION

The Third-Party Database Integration feature allows the UCM to connect to external databases (such as MySQL) to query contact information when calls are received. When a matching record is found, the caller name is displayed. Optionally, contacts can be synchronized into the UCM LDAP phonebook for centralized management.

For comprehensive details on this integration, its workflows, and configuration steps, please refer to the following guide.

[Third-Party SQL Database Integration Guide](#)

LDAP phonebooks synced from third-party databases support up to 500,000 contacts.

This feature is configured under **Integrations->3rd Party Database Integration**.

3rd Party Database Integration

Connection success

Basic Settings

Contacts Sync

3rd Party Database Integration
☒

Database Type

MySQL

* Server Address

192.168.6.36

IPv4 Address

* Port

3306

Range 1 - 65535

* Database Name

phonebook

* Connection Timeout (s)

5

* Username

phonebook_user

1 - 64 characters

* Password

Phonebook123!

At least 4 characters

* Character Set ⓘ

UTF8MB4

Test Connection

Start

Cancel

Save

3rd Party Database Integration Basic Settings

The Basic Settings tab is used to configure and enable the database connection. The table below describes the parameters on this page:

3rd Party Database Integration	Enable or disable 3rd party database integration. When enabled, the UCM queries the configured database for contact information.
Database Type	Select the database engine: SQL Server MySQL
Server Address	Enter the IPv4 address of the database server.
Port	Enter the port used by the database service. Valid range: 1-65535
Database Name	Enter the name of the database used for establishing the connection.
Connection Timeout (s)	Set the time (in seconds) to wait before a connection attempt times out. Please enter a value between 1 and 300. The default value is 5.
Username	Enter the username used to connect to the database.
Password	Enter the password for the specified username.
Character Set	Specifies the character set for MySQL connections. ASCII UTF-8 GBK GB2312 UTF8MB4
Test Connection	Click to test connectivity and authentication to the configured database.

After the database connection is successfully established, an additional Contact Synchronization tab becomes available, which enables synchronization of database contacts into the UCM LDAP phonebook.

3rd Party Database Integration

Basic Settings

Contacts Sync

Sync successful

Contacts Sync ⓘ

*Table

contacts

*Phonebook Name ⓘ

PhonebookSQL

1 - 32 characters, supports alphanumeric characters, chinese characters, and underscore (.)

Attribute Mapping ⓘ

display_name

→

CallerIDName

⊖

phone

→

AccountNumber

⊖

email

→

Email

⊖

Add

⊕

Scheduled Sync

By Day

⌵

00:00

⌵

Cancel

Save and Sync

3rd Party Database Integration Contacts Sync

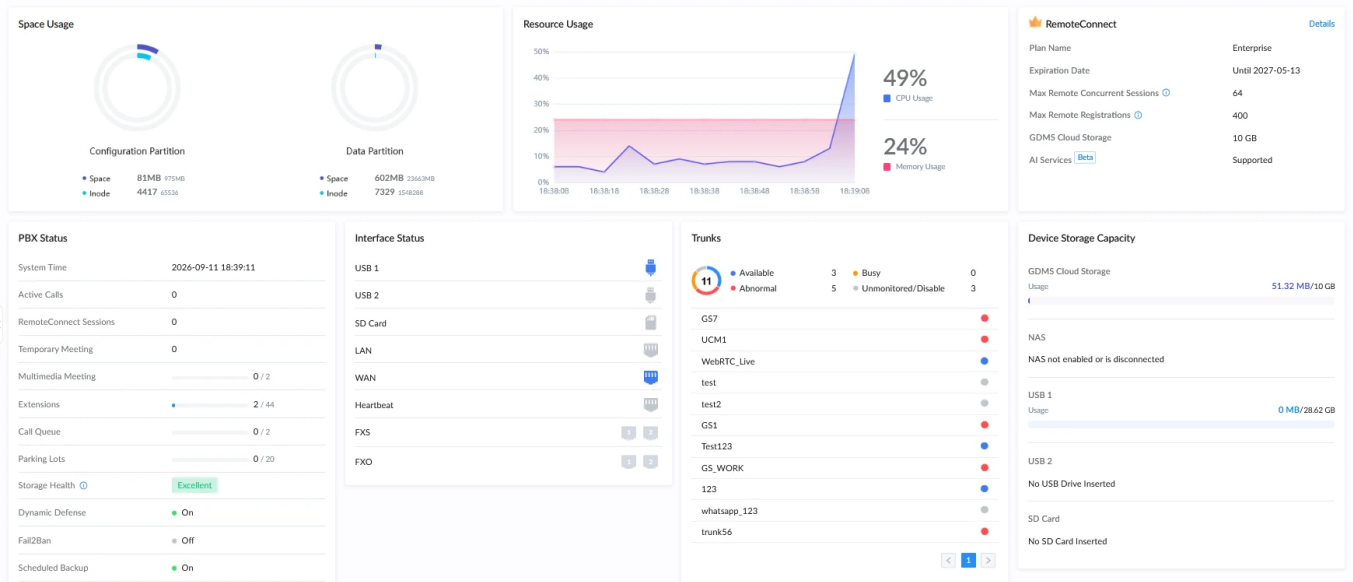
The configurable parameters on this page are described in the table below:

Contacts Sync	Enables synchronization of database contacts into the UCM LDAP phone book. When disabled, real-time caller lookup remains available, but contacts are not synchronized.
Table	Enter the database table containing contact records.
Phonebook Name	Choose the display name of the LDAP phone book created on UCM.
Attribute Mapping	Maps the 3rd party database fields to UCM LDAP attributes (max 10).
Scheduled Sync	Defines automatic synchronization schedule.

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

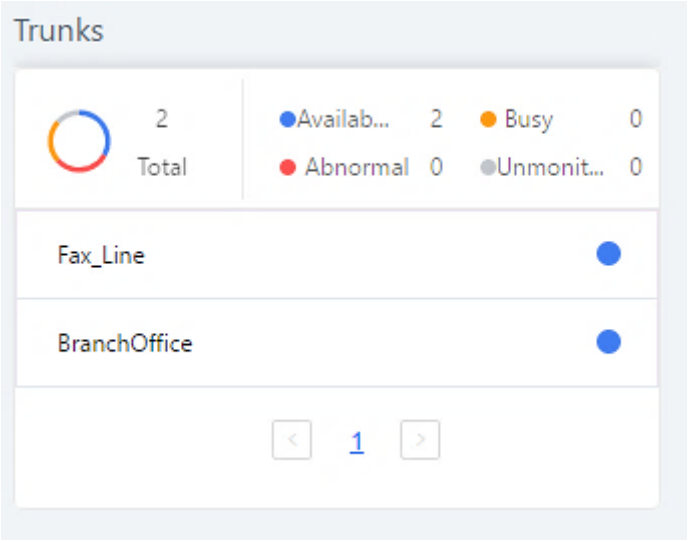
The administrator can also use the dashboard to view information about the different services. Such as the number of meetings, the number of extensions (registered and unregistered), Storage Health status, active security modules (Dynamic Defense, Fail2Ban), scheduled system tasks, etc...

PBX Status

System Time	2026-09-30 15:55:50
Active Calls	0
RemoteConnect Sessions	0
Temporary Meeting	0
Meeting	0 / 0
Extensions	0 / 5
Call Queue	0 / 0
Parking Lots	0 / 20
Storage Health ①	Excellent
Dynamic Defense	Off
Fail2Ban	On
Scheduled Backup	Off
Auto Sync	Off
Automatic Cleaning	On

Trunks

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



Trunk Status

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

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
☐	● Ringing	Available	1000		SIP(WebRTC)	192.168.5.199:5070		
☐	● Unavailable	Available	1001		SIP(WebRTC)	--		
☐	● In Use	Available	5555		SIP(WebRTC)	192.168.5.199:63827		

Extension Status

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

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.

Interface Status	
USB 1	
USB 2	
SD Card	
LAN	
Heartbeat	
FXS	1 2
FXO	1 2

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.

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

Base	Base version.
Program	Program version. This is the main software release version.
Recovery	Recovery version.
Lang	Lang version
Wave	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.

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

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.

Menus

System Status
Dashboard
System Information
Active Calls
Network Status
Extension/Trunk
Call Features
PBX Settings

System Information
General
Network
Remark

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.

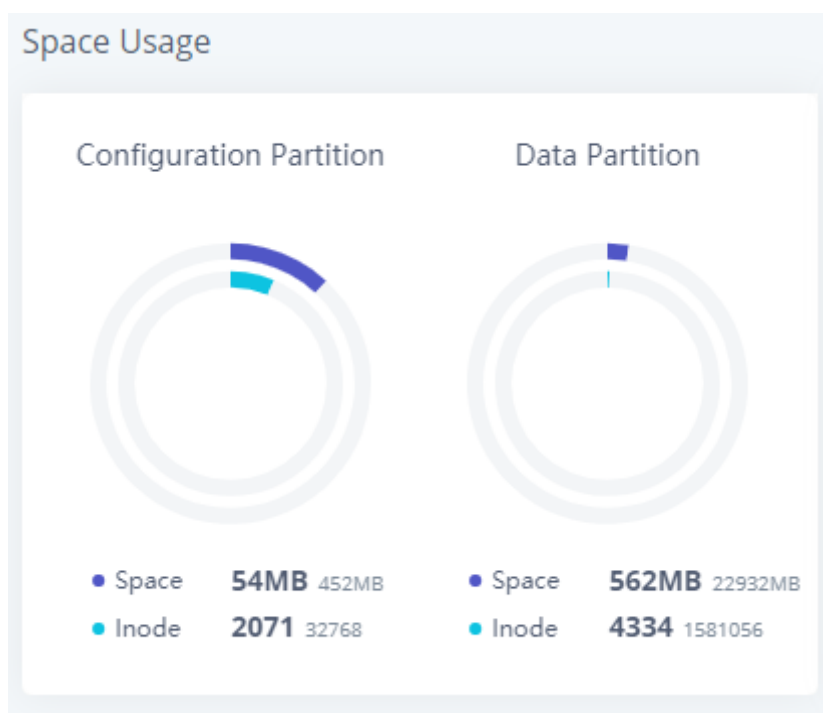
Inode Usage includes:

- **Configuration partition**

- **Data partition**

Note:

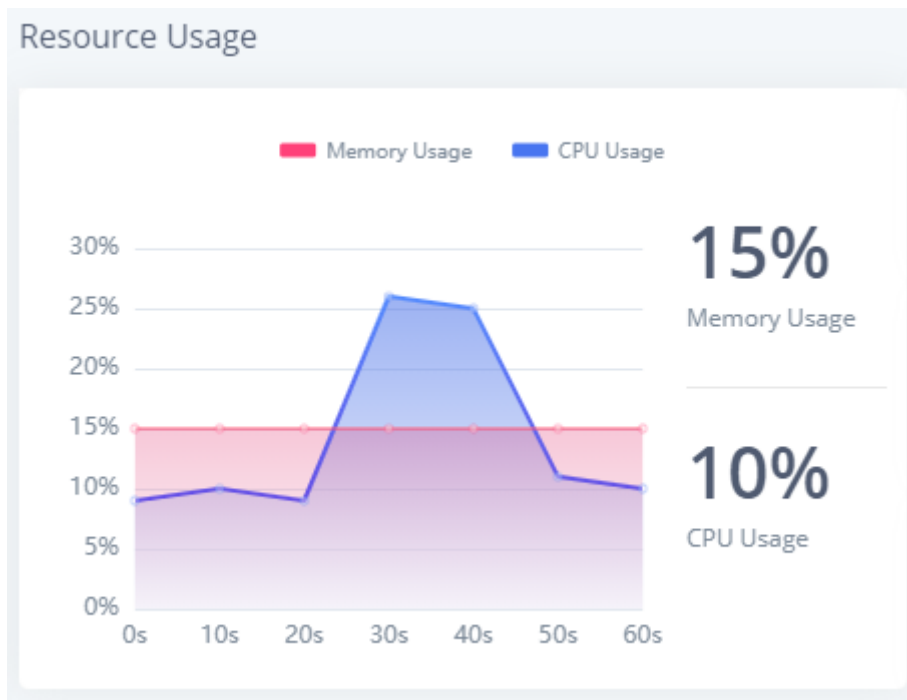
Inode is the pointer used for file reference in the system. The system usually has limited resources of pointers



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 **Maintenance -> System Events -> Alert Events List**. The UCM630X supports various system event types that generate alerts and/or email notifications when triggered.

System Events

Alert Log [Alert Events List](#) Alert Contact

Some alerts will display the following icons when toggled on.  indicates that the alert is associated with other settings that must be configured;  indicates that the alert is active for the enabled settings, and other related settings can be enabled.

☐	Event Name	Alert	Alert Contact				Options
Security							
☐	Fail2ban Blocking	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	Flood Attacks	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	Network Traffic Storm	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	User Login Banned	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	Remote Login	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	User Login Success	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	User Login Failed	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	Modify Super Admin Password	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
System							
☐	System Crash	☒ ON	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	System Update	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		
☐	System Reboot	☐ OFF	Email ☐ OFF	SMS ☐ OFF	HTTP ☐ OFF		

Alert Event List

For users who have purchased a GDMS package, once the option **Alert Events Sync** is enabled under RemoteConnect, triggered system alert events will be pushed automatically to their GDMS platform.

Click on the **Edit** icon next to any event entry to configure its notification parameters. The table below describes the available configuration options for alert events.

Event	Description
Security	
Fail2ban Blocking	If the system Fail2ban is blocking, the event will be recorded in the alert log.
Flood Attacks	An alert will be generated in case a DDoS attack attempt is detected by the UCM. The event will be registered in the alert log and pushed to GDMS.
Network Traffic Storm	An alert will be generated in case there is an excessive amount of packets on the LAN that consumes network resources and saturates bandwidth. Recorded in alert log and pushed to GDMS.
User Login Banned	If user login is blocked, the event will be recorded in the alert log.
Remote Login	An alert will be generated upon a remote login.
User Login Success	Successful user login events will be recorded in the alert log.
User Login Failed	User login failure events will be recorded in the alert log.
Modify Super Admin Password	An alert will be generated when the super admin password is changed.

System	
System Crash	The UCM will detect system crash events based on a specified cycle time.
System Update	Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
System Reboot	UCM detects system restarts and sends alerts containing MAC address, reboot reason, and initiator. Detects both: Manual restart: Reboot via Web GUI, LCD, or GDMS. Automatic restart: Reboot due to firmware upgrade, HA switchover, factory reset, power failure, or setting changes.
CPU Usage Call Control	Triggered when CPU usage exceeds the threshold configured under System Settings > General Settings (default 90%). Logs the event and prohibits new calls.
Memory Usage	Generates an alert if system memory usage exceeds the configured percentage threshold.
TLS Cert Expiration	Sends daily notifications starting 7 days before HTTP Server TLS certificate expiration, upon expiration, and after uploading a new valid certificate.
Cloud IM Abnormal	An alert message will be generated if Cloud IM encounters issues or exhibits abnormal behavior.
Data Sync Backup	If system data synchronization and backup abnormalities occur, the event will be recorded in the alert log.
Restore Config	Once system configuration is restored, the event is recorded in the alert log.
HA	
HA Failure	Generates an alert when a software or hardware fault occurs in HA dual-system hot backup deployment.
HA Switch	Sends an alert event once a switchover between primary and secondary UCM devices is detected.
HA Data Sync Failure	Generates an alert event in case of Data Sync failure in HA deployment.
Storage	
Local Disk Usage	Performs local disk detection periodically. Generates an alert if usage exceeds the configured percentage threshold. Note: If threshold is exceeded, disk operations (uploads, IM writing, recording, CDR) will be rejected.
External Disk Usage	Generates an alert if external disk usage exceeds the configured threshold percentage.
External Disk Status	Records connection and disconnection events of external disk storage in the alarm log.
Switching File Storage Path	Sends an alert once the file storage path on the UCM device is changed.
GDMS Cloud Storage	Triggered if cloud backup to GDMS fails.
Call Features	
Emergency Calls	If an emergency call is generated by the system, the event is recorded in the alert log.
SIP Outgoing Call through Trunk Failure	If an outgoing call via a SIP trunk fails, the event will be recorded in the alert log.
SIP Internal Call Failure	If an internal extension call fails within the system, the event will be recorded in the alert log.
Remote Concurrent Calls	If a remote concurrent call fails, the event will be recorded in the alert log.
Excessive Outbound Calls	Logged in the alert log and notification pushed when an extension initiates calls frequently.

Outbound Route Per-Call Duration	Triggers an alert notification when single outbound call duration thresholds are exceeded on configured outbound routes.
Outbound Call Duration	Triggered if a call reaches the cumulative duration limit set on an outbound rule.
Trunk Outbound Call Duration Usage	Triggered if a call reaches the duration limit set on a specific trunk.
Trunk Concurrent Calls	Triggered if the maximum allowed concurrent calls threshold is reached on a specific trunk.
Extension/Trunk Status	
Register SIP trunk failed	Detects failure of SIP trunk registration at configured intervals.
SIP Peer Trunk Status	If SIP peer trunk status becomes abnormal, the event will be recorded in the alert log.
Register SIP failed	Configures the notification cycle for SIP registration failures. Immediately alerts on first failure per IP/account, then counts subsequent failures until cycle expiration. Immediate mode if set to 0.
SIP Lost Registration	Records system SIP extension registration loss in the alert log. Note: Clicking the edit button allows enabling or disabling Ignore Wave App Registration Loss.

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

[Alert Log](#)[Alert Events List](#)[Alert Contact](#)

Delete Search ResultsClear

Display Filter

Time	Event Name	Type	Content
2024-10-14 08:20:23	System Reboot	Generate Alert	MAC: C0:74:AD - 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 - 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/192.168.1.100:5060, account ID is: 4001

Total: 131210 / pageGoto

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:
- Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.
 - 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 :

2020-11-03

00:00

End Time :

2020-11-10

14:31

Event Name :

All

Type :

All

Reset

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.

Super Admin Email	Configure the email addresses to send alert notifications to. Up to 10 email addresses can be added.
Admin Email	Configure the email addresses to send alert notifications to. Up to 10 email addresses can be added.
Email Template	Please refer to section Email Templates
Protocol	Protocol used to communicate with the server. HTTP or HTTPS. Default one is HTTP.
HTTP Server	The IP address or FQDN of the HTTP/HTTPS server.
HTTP Server Port	HTTP/HTTPS port
Warning Template	Customize the template used for system warnings. By default: { "action": "\${ACTION}", "mac": "\${MAC}", "content": "\${WARNING_MSG}" }
Notification Template	Customize the notification template to receive relevant alert information. By default: { "action": "\${ACTION}", "cpu": "\${CPU_USED}", "memory": "\${MEM_USED}", "disk": "\${DISK_USED}", "external_disk": "\${EXTERNAL_DISK_USED}" } Note: The notification message with "action:0" will be sent periodically if Notification Interval is set.
Notification Interval	Modifies the frequency at which notifications are sent in seconds. No notifications will be sent if the value is "0". Default value: 20
Template Variables	 \${MAC} : MAC Address \${WARNING_MSG} : Warning message \${TIME} : Current System Time \${CPU_USED} : CPU Usage \${MEM_USED} : Memory Usage \${ACTION} : Message Type. Refer to [Alert Events] \${DISK_USED} : Disk Usage \${EXTERNAL_DISK_USED} : Disk Usage

Alert Contact

Task Management

The Task Management feature allows users to schedule various tasks to be performed at a configured date and time. Each task can be set to run either once or repeatedly, depending on user requirements.

The tasks that can be scheduled include:

- **Paging/Intercom:** Schedule automated paging or intercom announcements at specific times.
- **Backup:** Schedule automatic backups of system data to USB, SD card, SFTP server, NAS, or Amazon S3. Users can configure multiple backup tasks, each with its own schedule and storage location.
- **Data Sync:** Schedule synchronization of system data with remote servers to ensure data consistency.
- **Cleaner:** Schedule cleaning tasks for system data, such as CDR records, reports, IM messages, and other files, to maintain storage efficiency.
- **Detect New Firmware:** Schedule automatic checks for new firmware versions.
- **Update Country/Region:** Schedule updates for system country/region settings, which are used for Geo-IP Access Control.
- **Update Time Zone:** Schedule updates for the system time zone configuration.

Task List

In the Task List, users can schedule tasks to be performed either once or repeatedly all of the above task types can be scheduled with specific parameters.

To schedule a task, please follow the steps below:

1. Navigate to **Maintenance->Task Management->Task List->Pending Task**
2. Click on the "Add" button.

Task Management

[Task List](#) [Task Schedule](#)

[Pending Task](#) [Historical Task](#)

[Add](#)

Name

Name	Type	Start Time
------	------	------------

Add Task

3. Select the type of task from the drop-down menu.
4. Click Next and configure the required parameters for the task, such as date, time, frequency, and additional options specific to the task type.

Create New Task



* Type

Scheduled Paging/Intercom

Cancel

Next

Create New Task

The Pending Tasks section displays all tasks that have been scheduled but not yet executed. Users can review, edit, or delete tasks from this list before execution.

Task Management

Task List

Task Schedule

Pending Task

Task History

Add

Name

Time:

Start Time

to

End Time

Search

Reset

Name

Type

Start Time

Repeat

Options

Schedule Cleaning

Scheduled Cleaner (IM Data)

2024-10-10 00:00

Per 30 Days
00:00

Edit

Delete

Total: 1

<

1

>

10 / page

Goto

Pending Tasks

The Task History section logs all tasks that have been performed, including execution time, task type, and status. Users can use this log to verify completed tasks and troubleshoot any issues.

Task Management

Task List Task Schedule

Pending Task Task History

Clear

Name

Time: 2024-09-01 to 2024-09-10

Search

Reset

Name	Type	Action Status	Start Time	Repeat	Options
No data					

Task History

Scheduled Paging/Intercom

The user can configure a paging or intercom to be initiated automatically according to a schedule. Refer the configuration explained in the table below to be able to configure this feature successfully.

Task Management > Create New Scheduled Paging/Intercom

* Paging/Intercom

7777 -- Test_background

* Name

Test_background

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

* Caller

* Start Date

2025-07-24

* Start Time

Select time

Add Start Time

Repeat

No Repeat

Sync to Google Calendar

Google Services

Cancel

Save

Create New Scheduled Paging

Paging/Intercom	Select pre-existing paging/intercom groups and multicast communities.
Name	Specify the name of the Paging/Intercom schedule.
Caller	When the scheduled time arrives, the system will call this extension. If the call is answered, the paging/intercom will be initiated, if rejected, the paging/intercom will be cancelled.If no caller is specified, the paging/intercom will be directly initiated.
Start Date	Select the start date.
Start Time	Select the start time
Repeat	Select the repeating frequency.No RepeatEvery DayWeeklyMonthly
Sync to Google Calendar	Enabling this option will automatically synchronize the paging/intercom event to the administrator Google Calendar.Note: This requires that the Google Service integration is configured in this specific UCM.

Scheduled Backup

Scheduled backup task management allows the user to schedule regular backups with a specific interval. This provides an efficient and reliable archiving process which can prevent any accidental loss of data.

Task Management > Create New Scheduled Backup

① Backups may take some time if backing up large amounts of data. It is recommended to use external storage devices such as SD cards, USB flash drives, etc. EXT4 is the recommended file system for external storage devices.

① SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

*

Name

Schedule Backup

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

*

Choose Storage Location

*

Backup Time

00:00

*

Backup Frequency

1

Choose Backup Files

☐ All
☐ Config File
☐ IM Message
☐ IM Files
☐ CDR Records
☐ Recording Files
☐ Fax Files
☐ Voicemail
☐ Voice Prompt Files
☐ Queue Statistics Report
☐ ZeroConfig Storage
☐ Meeting Report

①

Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

Cancel

Save

Create New Scheduled Backup

Parameter	Description
Name	Enter the name of the scheduled task.
Choose Storage Location	Choose storage location.NASSFTP ServerUSB DiskSD CardAmazon S3
Date	Specifies the calendar date when the backup task should be executed. Users can select a single date for a one-time backup or a start date for recurring backups.

Scheduled Cleaner

Scheduled Cleaner allows the user to automate the process of cleaning the files stored in the UCM as well as the attached storage of the UCM.

The following is the list of the types of the cleaner which can be configured for scheduling.

- Scheduled Cleaner (CDR)
- Scheduled Cleaner (Report)
- Scheduled Cleaner (IM Data)
- Scheduled Cleaner (File)

CDR Cleaner

Parameter	Description
Name	Enter the name of the data sync scheduling.
Choose Data Sync Files	Choose the type of data to synchronize.CDR RecordsRecording FilesVoicemailFax
Account	Enter the username of the account created on the SFTP server.
Password	Enter the password of the account created on the SFTP server.
Server Address	Enter the server address. The port number is not mandatory.
Destination Directory	Enter the directory name on which the data will be store for this specific IPPBX.
Sync Time	Select the time when the synchronization is triggered. We recommend that the synchronization is required outside of the production hours.

Report Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (Report) is selected.
Data Type	Select the type of the report to clean automatically.Queue Statistics ReportMeeting Call Statistics ReportMeeting History
Clean Time	Select the time when the cleaning is triggered.
Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the reports which are within this period of time.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

IM Data Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (IM Data) is selected.
Data Type	Select the type of the data to clean automatically.IM FilesIM Message
Clean Time	Select the time when the cleaning is triggered.

Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the files within this period of time.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

File Cleaner

Parameter	Description
Name	Configure the name of the scheduled task.
Cleaner Type	If Scheduled Cleaner (File) is selected.
Clean Files In External Storage	If enabled, files in the external storage currently being used will be cleaned as configured.
Choose Cleaner Files	Select the file systems for the cleaning.Basic Call RecordingsMeeting RecordingsPaging/Intercom RecordingsQueue RecordingsVoicemail FilesEmergency RecordingsFaxSCA RecordingsBackup Files
Clean Time	Select the time when the cleaning is triggered.
Cleaning Conditions	Select the factor of triggering the cleaning.By Schedule: If the value is set to 3, the cleaning will performed every three days, and will delete all the CDR entries which were generated in the 3 days prior.Keep Last X Records: This option sets a threshold of the number of entries to keep stored. E.g., if set to 50000 entries and the CDR reaches that threshold, the UCM will start deleting the older records.Keep Last X Days: Keep the files which are within the period range.
Corresponding Parameter to "Cleaning Conditions"	When By Schedule is selected as cleaning condition, enter the Clean Interval as number of days.When Keep Last X Records is selected, enter the number of records as a threshold.When Keep Last X Days records is selected, the user can configure how long before the cleaner deletes all the files.

Scheduled Detect New Firmware

Task scheduling for detecting new firmware allows the user to automate the process of verifying the availability of a new firmware update. Using this feature can ensure that the administrator is notified as soon as there is a new update of the UCM6300 Series software.

Task Management > Create New Scheduled Detect New Firmware

*

Name

Schedule Detect New Firmware

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

Upgrade Method

Notify When New Firmware is Ava... ▾

*

Date

2025-07-25



*

Time

Select time



Repeat

No Repeat ▾

Cancel

Save

Create New Scheduled Detect New Firmware

Parameter	Description
Name	Configure the name of the scheduled task.
Upgrade Method	Select the action when a new firmware is detected.Notify When a New Firmware is AvailableAuto Download and Upgrade Firmware
Email Reminder Before Upgrade (m)	This option appears when you select Auto Download and Upgrade Firmware.
Date	Select the date when the firmware detection first starts.
Time	Select the time when the firmware is detected.
Repeat	Select the frequency of the detection.No RepeatEvery DayWeeklyMonthly

Scheduled Update of Country/Region List

Scheduling a regular update of the Country/Region List ensures keeping the list for Geo-IP Access Control up to date with any emergence of new countries or name-change of existing countries. This also allows receiving the update without having to wait for a new firmware release.

Task Management > Create New Scheduled Update Country/Region

*

Name

Schedule Detect Country Region

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

*

Date

2025-07-25



*

Time

Select time



Repeat

No Repeat

▼

Cancel

Save

Create New Scheduled Update CountryRegion

Schedule Update Time Zone

Scheduling update for timezones ensures that the list can be updated regularly and without the need to wait for a new firmware release.

Task Management > Create New Scheduled Update Time Zone

*

Name

Schedule Update Time Zone

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

*

Date

2025-07-25



*

Time

Select time



Repeat

No Repeat

▼

Cancel

Save

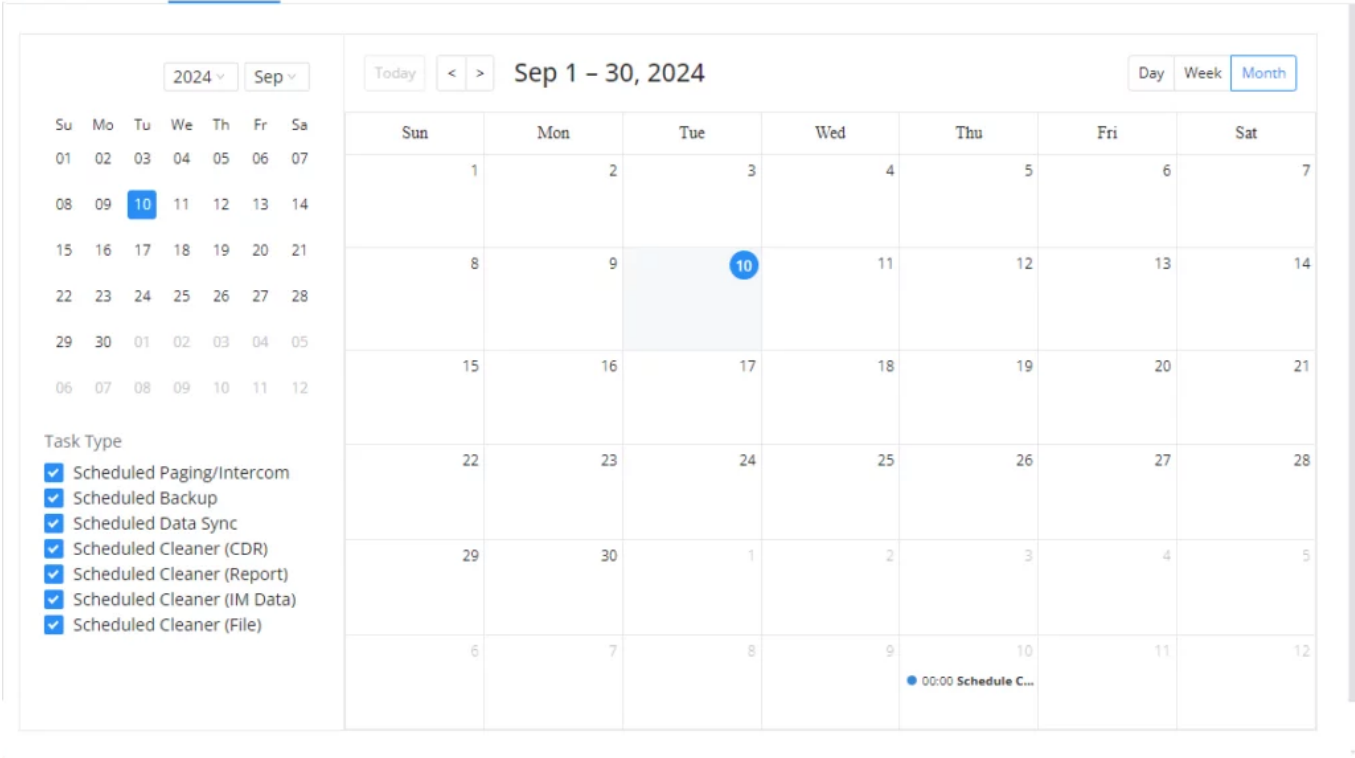
Create New Scheduled Update Time Zone

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 Management

Task ListTask 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.

CDR										Display Filter
By default, this page displays the CDR entries from the current month. Use the "Display Filter" button to specify a time range.										
Recording files are currently stored in GDMs Cloud Storage . Click here to modify. The recording files contain basic call recordings, queue recordings, meeting recordings, SCA recordings, emergency call recordings, and paging/intercom recordings.										
Delete AllDelete Search Result(s)Download All RecordsDownload Search Result(s)Automatic DownloadCDR SettingsCDR in GDMs Cloud										
Status	Call from	Call to	Action Type	Start Time	Call Time	Talk Time	Call/Meeting AI Trans...	Call Note	Options	
▶	2006	*98	DIAL	2026-09-11 15:24:48	0:00:09	0:00:09	Not Transcribed		☑	
▶	"Alice" 1002	1003	DIAL	2026-09-11 14:22:58	0:00:28	0:00:24	Not Transcribed		☑	
▶	"Jane Don" 1000	"Keith More" 1006	DIAL	2026-09-11 11:58:05	0:01:52	0:01:47	Transcribed		☑	
▶	"James Smith" 1007	"Jane Don" 1000	DIAL	2026-09-11 10:18:49	0:00:41	0:00:38	Not Transcribed		☑	
▶	"James Smith" 1007	"Jean Doe" 2000	VM	2026-09-11 09:49:55	0:00:00	0:00:00	Not Transcribed		☑	
▶	"James Smith" 1007	1003	VM	2026-09-11 09:49:42	0:00:01	0:00:01	Not Transcribed		☑	
▶	"James Smith" 1007	"Alex Doe" 1005	DIAL	2026-09-11 09:48:22	0:00:03	0:00:00	Not Transcribed		☑	
▶	"John" +2126... NAT	+15556724562	WHATSAPP[155567206...	2026-09-10 22:11:33	0:00:13	0:00:00	Not Transcribed		☑	
▶	"Jane Don" 1000	1001	DIAL	2026-09-10 18:08:49	0:00:15	0:00:12	Not Transcribed		☑	
▶	"Jane Don" 1000	1001	DIAL	2026-09-10 16:42:56	0:03:18	0:03:14	Not Transcribed		☑	
Total: 409 < 1 2 3 4 5 ... 41 > 10 / page Go to Page										

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.

CDR

Hide Filter

Start Time:

Select date

Select time

End Time:

Select date

Select time

Caller Number:

Caller Name:

Callee Number:

Account Code:

Source Trunk Name:

Destination Trunk Name:

Action Type:

Export File Data:

Extension Group:

Call Type:

☐ Inbound Calls
 ☐ Outbound Calls
 ☐ Internal Calls
 ☐ External Calls

Status:

☐ Answered
 ☐ No Answer
 ☐ Busy
 ☐ Failed

Filter

Reset

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

CDR Filter

Option / Field	Description
Status	Indicates the final status of the call (Answered, Busy, No Answer, or Failed).
Call From	Displays the caller's name and extension number or external CID (e.g., "Jane Doe" 1005).
Call To	Displays the recipient's name and extension number or external dialed number (e.g., "Robert More" 1006).
Action Type	Displays the mechanism/destination type used for the call (e.g., DIAL, IVR, WAKEUP, MEETING).
Start Time	Timestamp when the call was initiated (Format: YYYY-MM-DD HH:MM:SS). Clicking the column header sorts the list by start time.
Call Time	Total duration of the call from initiation to hang-up (Format: HH:MM:SS).
Talk Time	Connected duration between parties (Format: HH:MM:SS).
Call/Meeting AI Transcription	Displays the status of AI recording transcription (e.g., Transcribed or Not Transcribed).
Call Note	Displays assigned labels or custom comments attached to the call record. Click the Edit Call Note (pencil) icon under the Options column to modify the label or add comments.
Recordings Management	If the call has an associated audio recording, a tape/cassette icon appears in the Options column. Clicking this icon opens the Recordings pop-up dialog to play, download, transcribe, or delete the recording.
Download Search Result(s)	Exports currently filtered CDR records into a .csv file.
Download All Records	Exports all stored system CDR records into a .csv file.
Delete All	Removes all CDR call history entries from the system.
Delete Search Result(s)	Removes only the CDR entries matching the current filter criteria. A secondary prompt asks whether to simultaneously delete associated call recording files.
Automatic Download	Configures scheduled exports of CDR CSV files to email destinations or synced cloud platforms (such as Google Docs).
CDR Settings	Opens global CDR management parameters.

Administrators and authorized users can categorize call records by attaching pre-configured labels or adding custom comments by clicking the Edit icon under **Options** to open the **Edit Call Note** window.

CDR

Display Filter

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

Recording files are currently stored in GDMS Cloud Storage. Click here to modify. The recording files contain basic call recordings, queue recordings, meeting recordings, SCA recordings, emergency call recordings, and paging/intercom recordings.

Delete All
Delete Search Result(s)
Download All Records
Download Search Result(s)
Automatic Download
CDR Settings
CDR in GDMS Cloud

Status	Call from	Call to	Action Type	Start Time	Call Time	Talk Time	Call/Meeting AI Trans...	Call Note	Options
▶	2006	*98	DIAL	2026-09-11 15:24:48	0:00:09	0:00:09	Not Transcribed		
▶	"Alice" 1002	1003	DIAL	2026-09-11 14:22:58	0:00:28	0:00:24	Not Transcribed		
▶	"Jane Don" 1000	"Keith More" 1006	DIAL	2026-09-11 11:58:05	0:01:52	0:01:47	Transcribed		

CDR Entries

The dialog allows selecting a pre-configured tag from the drop-down menu (configured under **CDR -> Call Note**) or entering a custom note regarding the call (up to 512 characters; special characters \$ & | : > ` are restricted).

Edit Call Note

Label

Comment

0 - 512 characters, characters \$&|:>` are not allowed.

Cancel

Save

Edit Call Note

Clicking the recording icon on a CDR entry opens the **Recordings** pop-up modal, allowing users to preview, manage, or transcribe call recording files. The pop-up dialog provides interactive operations including:

- **Playback** (using the built-in audio player controls to play, pause, or seek)
- **Download** (saving the recording file in .wav format to the local computer)
- **AI Recording Transcription** (initiating AI speech-to-text transcription after selecting the desired language)
- **Delete** (deleting the recording file without removing the CDR call entry).

Download Search Result(s)
Automatic Download
CDR Settings
CDR in GDMS Cloud

Call to	Action Type	Start Time	Call Time	Talk Time	Call/Meeting AI Trans...	Call Note	Options
"Robert James" 1008	DIAL	2026-09-09 09:06:51	0:03:22	0:03:20	Not Transcribed		
"Robert James" 1007	DIAL	2026-09-09 09:06:51	0:03:22	0:03:20	Transcribed		
"Robert James" 1007	DIAL	2026-09-09 09:06:51	0:03:22	0:03:20	Transcribed		
"Robert James" 1007	DIAL	2026-09-09 09:06:51	0:03:22	0:03:20	Transcribed		
"Jane Don" 1000	DIAL	2026-09-11 11:58:05	0:01:52	0:01:47	Not Transcribed		
"Robert James" 1008	DIAL	2026-09-09 09:06:51	0:03:22	0:03:20	Transcribed		

Recordings

Name

Recording AI Transcription

Play

Options

2026-09/

auto-1788875732-1007-1

Not Transcribed

00:00









006.wav

Transferred calls are represented in the CDR log as consolidated entries. Accessing CDR entries under Web GUI -> **CDR -> CDR** allows administrators to review full details for individual call sessions.

Click the **Option** icon next to a specific call record entry to view detailed call flow information, including

primary caller IDs, call transfer steps, and timing details.

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

CDR Report Page

	"abllili lolo" 1000...	9985632	DIAL	2019-12-10 03:23:14	0:00:13	0:00:07		1	
STATUS	PREMIER CALLER	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT T CODE	RECORDING FILE OPTIONS
	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 Log View

CDR Automatic Download

The UCM630x Audio series can be configured to automatically export and transmit CDR records at scheduled intervals. Administrators can deliver CDR files via email or automatically sync them to Google Sheets by navigating to **CDR -> CDR** and clicking on **Automatic Download Settings**.

Automatic Download

Auto Download CDR

*Download Destination

☐ Email
 ☒ Google Docs

Automatic Download Period

By Day

10

☒ Delete Downloaded CDR

Cancel

OK

The table below describes the parameters available in the Automatic Download configuration dialog:

Parameter	Description
Auto Download CDR	Enables or disables the scheduled automatic downloading and exporting of CDR logs.
Download Destination	Select the delivery method for auto-downloaded CDR records: Email: Transmits exported CDR files as email attachments to designated recipient email addresses. Google Docs: Automatically uploads exported CDR CSV files to Google Drive/Sheets. Note: The Email destination requires configured Email Settings (under System Settings -> Email Settings), while the Google Docs destination requires an active Google Workspace Integration (under Integrations -> Collaborative Office Integration).
Email Address	Displayed when Email is selected as a destination. Enter the email addresses that will receive the CDR records. Multiple email addresses should be separated by commas.

Automatic Download Period	Defines the recurrence schedule and exact hour of the day for automatic CDR exports: By Day: When the configured download hour arrives, the system exports CDR records of the entire previous day. By Week: Select a specific day of the week and hour. When triggered, the system exports records covering the previous 7 days. By Month: Select a specific day of the month and hour. When triggered, the system exports records spanning from the previous month.
Delete Downloaded CDR	When enabled, CDR records that have been successfully generated and sent to the configured destination (Email or Google Docs) will be automatically deleted from local UCM storage to conserve disk space.

-

Downloaded CDR File

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

- Context

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.

ext-did-XXXXX: inbound calls. It starts with "ext-did", and "XXXXX" content varies case by case, which also relate to the order when the trunk is created.

ext-local: internal calls between local extensions.

- Source Channel, Dest Channel

Sample 1:

caller number	callee number	context	calerid	source channel	dest channel	disposition
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	ANSWERED

Downloaded CDR File Sample Source Channel and Dest Channel 1

- DAHDI means it is an analog call, FXO or FXS.
- For UCM6302A, DAHDI/(1-2) are FXO ports, and DAHDI(3-4) are FXS ports.
- For UCM6304A, DAHDI/(1-4) are FXO ports, and DAHDI(5-6) are FXS ports.
- 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

- "SIP" means it is a SIP call. There are three format:
- (a) **PJSIP/NUM-XXXXXX**, where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.
- (c) **PJSIP/trunk_X/NUM**, where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.
- (c) **PJSIP/trunk_X-XXXXXX**, where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

There are some other values, but these values are the application name which are used by the dialplan.

IAX2/NUM-XXXXXXX: it means this is an IAX call.

Local/@from-internal-XXXXX: it is used internally to do some special feature procedure. We can simply ignore it.

Hangup: the call is hung up from the dialplan. This indicates there are some errors or it has run into abnormal cases.

Playback: play some prompts to you, such as 183 response or run into an IVR.

ReadExten: collect numbers from user. It may occur when you input PIN codes or run into DISA

Note: The language of column titles in exported CDR reports and statistics reports will be based on the UCM's display language

CDR Export Customization

Users can select the data they want to see in exported CDR reports by first clicking on the Filter button on the CDR page under **CDR→CDR** and selecting the desired information in the Export File Data field.

The screenshot displays the CDR Export Customization interface. It includes several input fields for filtering: End Time (with a date picker), Caller Name, Account Code, Destination Trunk Name, and Export File Data. Below these fields are checkboxes for Outbound Calls, Internal Calls, No Answer, and Busy. A green banner提示用户使用“Filter”按钮指定时间范围。 At the bottom, there are buttons for All Records and Download Search Result (s). A dropdown menu is open for the Export File Data field, showing a list of selectable data fields: ACCOUNT CODE, SESSION, ACTION OWNER, ACTION TYPE, SOURCE TRUNK NAME, DEST TRUNK NAME, CALLER NUMBER, and CALLERID. The bottom of the interface shows a table header with columns: type, Start Time, Call Time, Talk Time, Account Code, and 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 Cancel

Delete

☐	NAME	DATE	SIZE	OPTIONS
No Data				

CDR in GDMS Cloud

Call Note

Under **CDR -> Call Note**, administrators can enable the Call Note feature and define customized call labels (tags) that users can attach to call detail records and call logs across the User Portal and Wave application.

Extension user access permissions for modifying call notes can be configured under Maintenance -> User Management -> User Portal/Wave Privileges.

Call Note

Call Note

If enabled, adding tags and notes to call logs will be supported. Extension user permissions can be configured at User Portal/Wave Privileges.

Cancel

Save

Label

Add

Label	Description	Options
Cancelled		
Processed		
CallBack		

Total 3 < 1 > 10 / page

The table below describes the parameters available on the Call Note configuration page:

Option	Description
Call Note	Toggles the Call Note feature on or off. When enabled, users can add tags, labels, and text comments to call logs and CDR entries.
Label Table	Displays all created call labels along with their descriptions and management options (edit or delete).

To create a new call label tag, click the **Add** button to open the **Add Call Label** window.

Edit Call Note

×

Label ⓘ

▼

Comment

0 - 512 characters, characters \$&|;>` are not allowed.

Cancel

Save

Configure the following fields in the **Add Call Label** dialog:

- **Label:** Enter a unique name for the call tag (1-128 characters; supports numbers, letters, special characters _ -, and Chinese characters).
- **Description:** Enter an optional summary or explanation for the label (0-128 characters; special characters \$ & | : > ` are restricted).

Call Rate

In Call Rate, the user can set call billing for outbound calls. The user can choose to include the call rate configured in **Least Call Rates** or configure rates for calls which are identified through a prefix.

Call Rate

LCR Carrier Call Rates

Using LCR Carrier Call Rates ☒ LCR Operator

When enabled, if the user uses LCR to go out, the call rate will be calculated according to the rate corresponding to the actual outgoing carrier. In other cases, call rates are calculated based on a list of other call rates.

Cancel Save

Name	Match Prefix	Starting Cost	Starting Time (seconds)	Rate	Billing Unit (sec)	Valid Time	Options
LCR-123Cloud-5	5			5	60	2025-05-14 12:55:02~2099-12-31 23:59:59	

Total: 1 < 1 > 10 / page Goto

Other Call Rates

The system matches rates based on the prefix of the caller's number, and after matching, the rates in the table below are used to calculate the cost of the call. When more than one rate can be matched, the rate with the highest priority is used.

Add Rate Delete Selected Rate Import Export

Q Name/Match Prefix/Rate

☐	Priority	Status	Name	Match Prefix	Starting Cost	Starting Time (seconds)	Rate	Billing Unit (sec)	Valid Time	Options
--------------------------	----------	--------	------	--------------	---------------	-------------------------	------	--------------------	------------	---------



No data

Call Rate

To add specific rates, click on "Add Rate".

Call Rate > Add Other Call Rates

Call Charge = Starting Cost + Rate x Number of Billing Units Exceeding Start Time

* Name

Match Prefix

Starting Cost

Starting Time (seconds)

* Rate

* Billing Unit (sec)

60

Start Time

Date

Time

End Time

Date

Time

Disable the rate

☐

Cancel Save

Parameter	Description
Name	Enter the name of the call rate.
Match Prefix	Enter the matching prefix of the outgoing number dialed to match the corresponding rate. The prefix entered must match the outgoing mode of the outgoing route. Leave this field blank if you want to calculate every call using this rate. The matching will be done before any digit stripping or prepending is done.
Starting Cost	Configure the starting flat fee to charge for calls. If the length of the external call does not exceed the start time, only this fee will be charged.
Starting Time (seconds)	Sets the starting time period for call billing. If the length of an external call does not exceed the starting time, only the starting cost amount will be charged. Example 1: If the starting cost is set to 0.2, and the starting time is set to 60, the first 60 seconds of a call will be charged a flat amount of 0.20 dollars (or other currency). If the starting cost is set to 0 instead, the first 60 seconds will be free. Example 2: If the starting cost is set to 0.2 and the starting time is set to 0, the call billing will start upon dialing with an initial cost of 0.2 currency unit. Example 3: If the starting cost is set to 0 and the billing time is set to 0, the billing will start upon dialing with no initial cost.
Rate	Sets the billing rate of a call after the starting time period has ended. This is used with Billing Unit (sec) to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time).
Billing Unit (sec)	Sets the billing unit used after the starting time period has ended. This is used with Rate to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time). Partial units are rounded up (e.g., If the billing unit is set to 60 seconds, and the call lasted 90 seconds (1.5 units), the guest will be billed for 120 seconds (2 units)).
Start Time	Define the starting time. After this time, this rate will be applied.
End Time	Define the end time. After this time, this rate will not be applied.
Disable the rate	Ticking this box will disable this rate. Unticking this box means that this rate will apply.

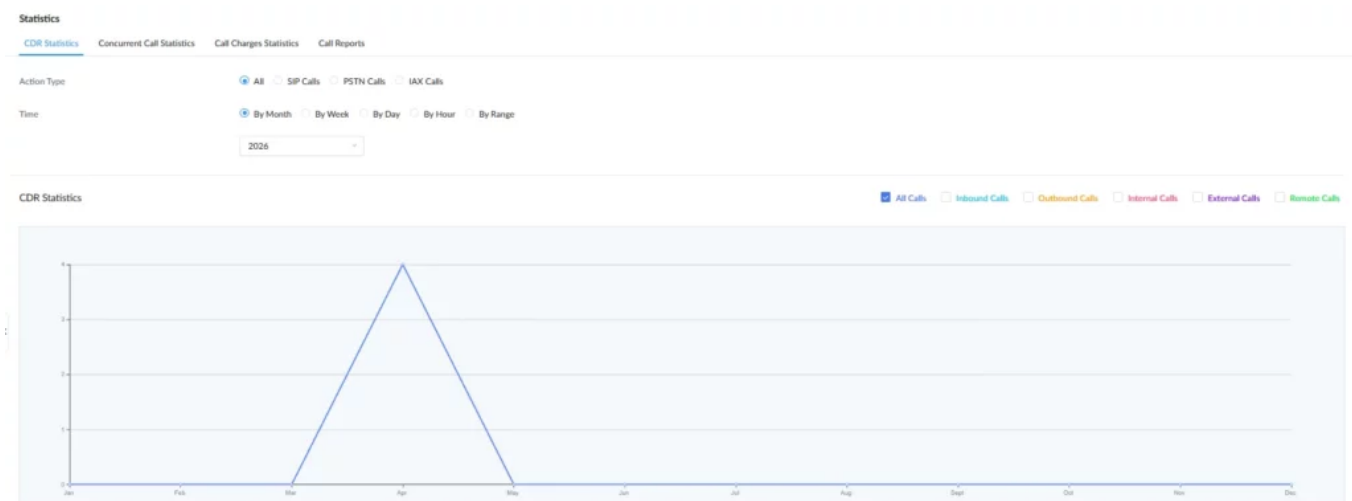
For more information on the UCM6300 Audio series built-in billing feature, please refer to the Grandstream Billing System Guide.

Statistics

The UCM provides a comprehensive CDR analytics framework for monitoring, analyzing, and reporting voice traffic across the system. This module is designed to give administrators operational visibility into call patterns, resource utilization, user behavior, and cost distribution.

CDR Statistics

UCM supports the function of concurrent call statistics. This function provides users with statistics on the number of concurrent calls of all VoIP trunks (SIP trunks and IAX trunks). Users can set search criteria to generate custom charts. Select the trunk and time to view the chart of the maximum number of concurrent calls corresponding to the trunk in a certain day or month.

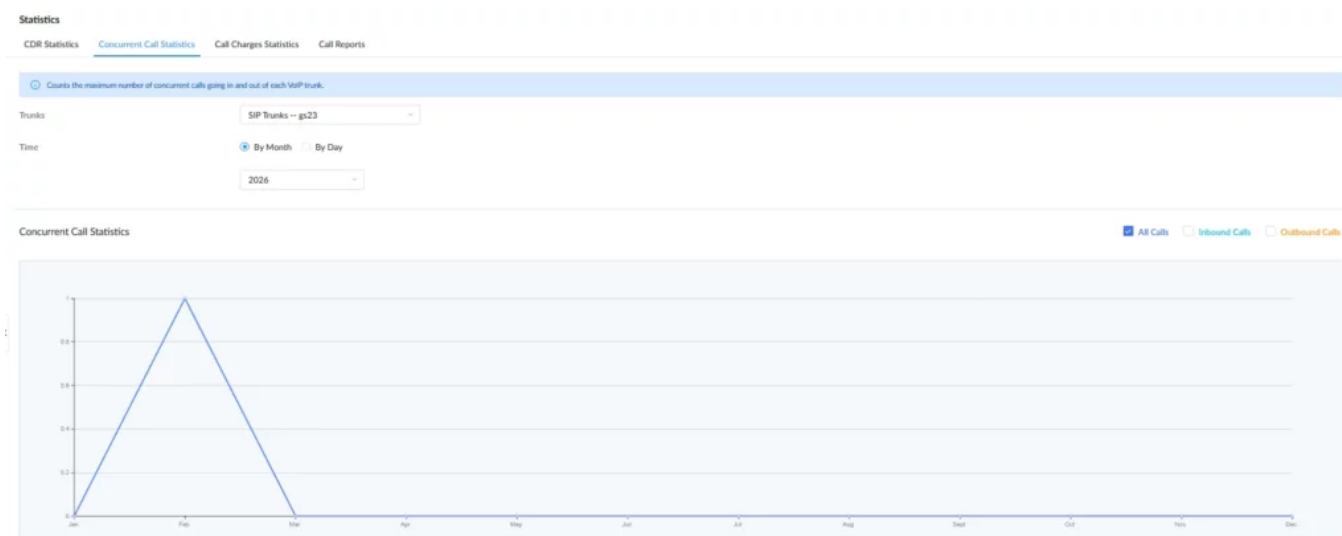


CDR Statistics Tab

Action Type	Select one of the following trunk type All SIP Calls PSTN Calls
Time Range	Select the time period to use for filtering By month (of the selected year) By week (of the selected year) By day (of the specified month for the year) By hour (of the specified date) By range. Example: 2016-01 to 2016-03
Call Type	Select one or more in the following checkboxes. All Calls Inbound Calls Outbound Calls Internal Calls External Calls Remote Calls

Concurrent Call Statistics

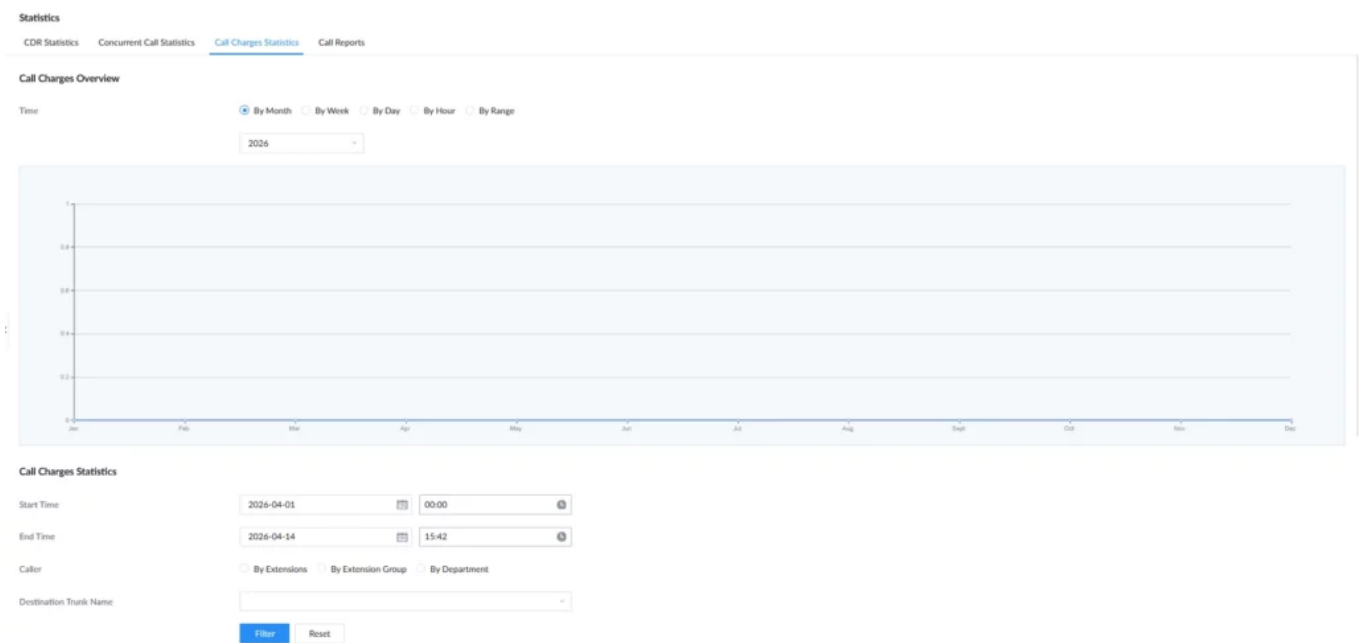
In this tab, the administrator can view the statistics regarding the concurrent calls. The administrator can choose to view the statistics per day, month, and year. The user can also view all calls, inbound calls, or outbound calls; or a combination of all of them together.



Concurrent Call Statistics Tab

Call Charges Statistics

In call Charges Statistics tab, the administrator can view the charges applied to the calls represented in a graph. The administrator can search by time interval, they can also filter per extension, extension group, by department. Once the administrator sets the intended parameters in the filter, they can display and download the filtered statistics.



Call Charges Statistics Tab

Call Reports

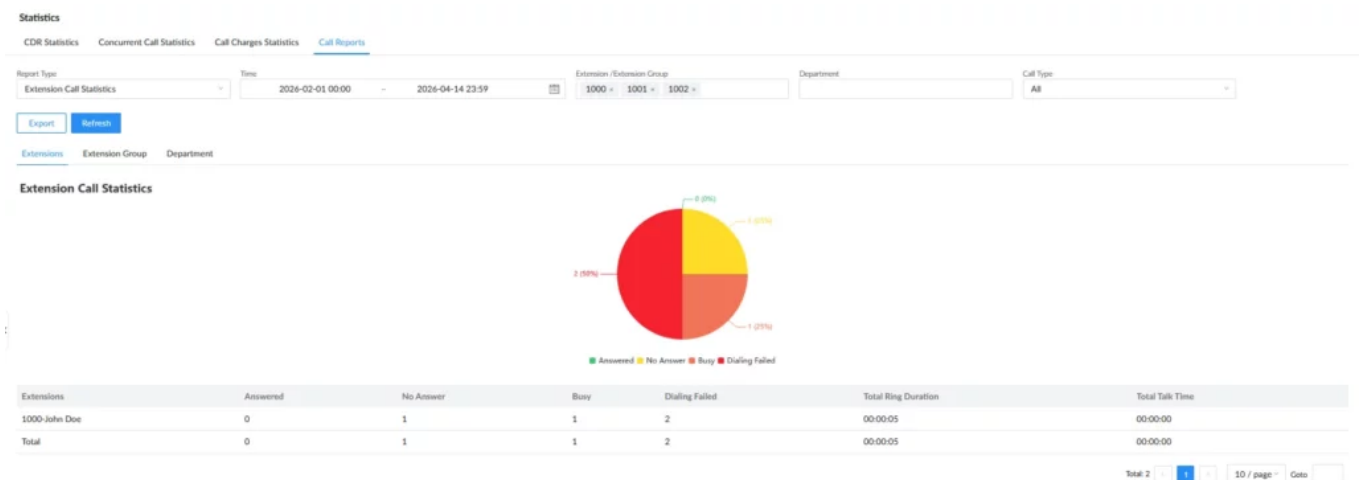
The Call Reports section provides analytics based on different operations within the PBX. These reports allow administrators to analyze how calls are distributed, handled, and processed across extensions, trunks, and system components.

Extension Call Statistics

This report displays insights into call volume associated with selected:

- Extensions
- Extension groups
- Departments

Administrators can filter by time period and call type (inbound, outbound, internal, etc.) to analyze how traffic is distributed across users or organizational units.

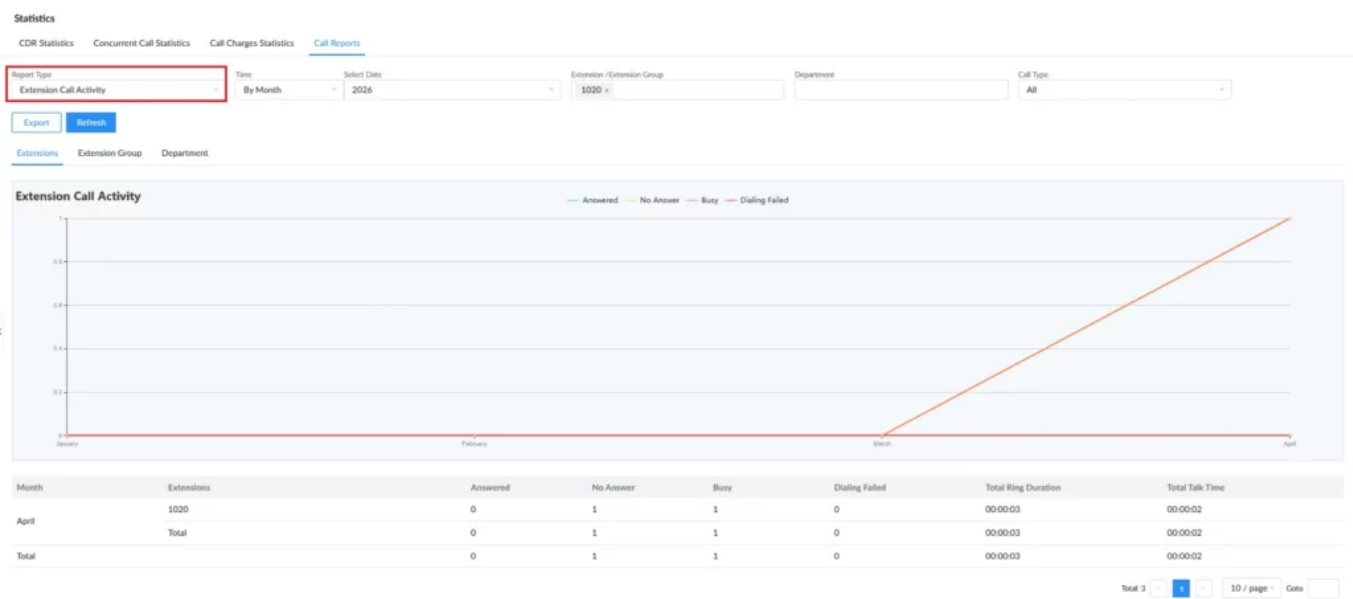


Extension Call Statistics

Extension Call Activity

This report focuses on how calls and selected call types were handled by the specified extensions/extension

groups/departments over the specified time periods.

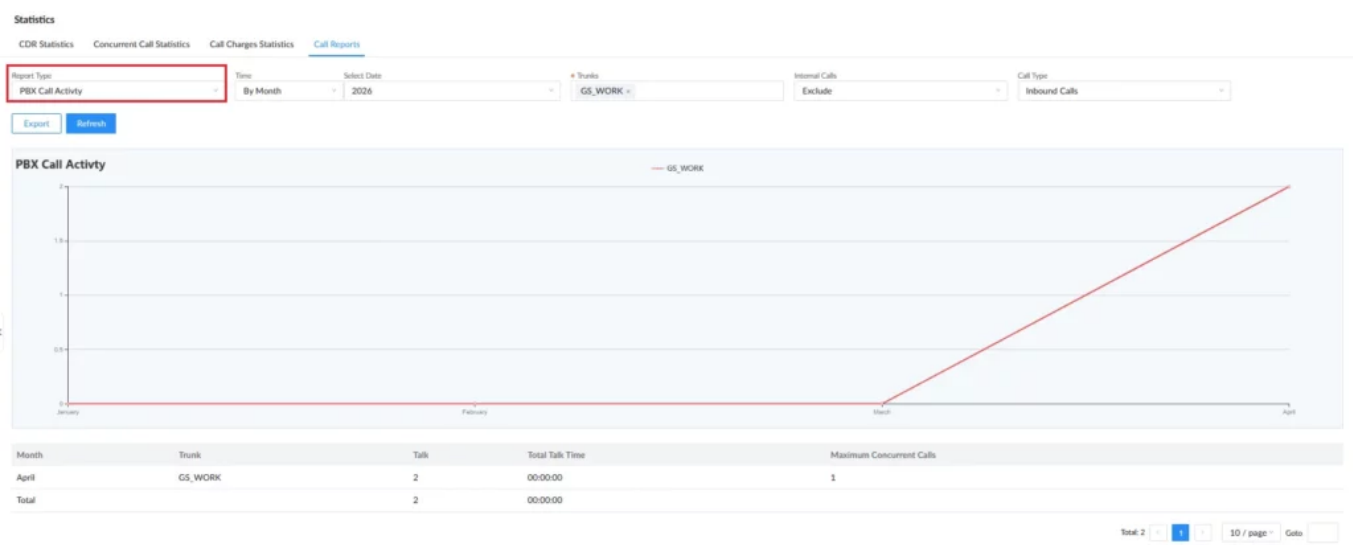


Extension Call Activity

PBX Call Activity

This report provides a system-wide view of call activity across selected trunks, which include or exclude internal calls (extension-to-extension) and can be filtered by call direction.

This enables comparison between internal PBX traffic and external trunk usage, helping identify overall system load distribution and trunk utilization patterns.



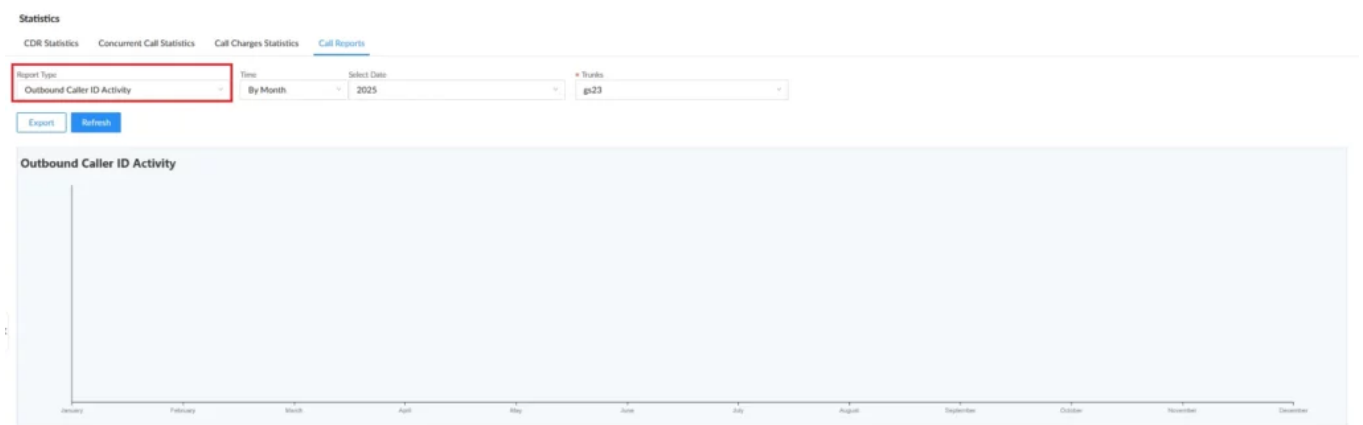
PBX Call Activity

Outbound Caller ID Activity

This report provides visibility into outbound call usage based on the selected trunk and caller ID configuration.

It displays how outbound calls are distributed across:

- Trunks
- Caller IDs



Outbound Caller ID Activity

IVR Report

This option provides analysis of IVR interactions over a selected time period and supports two reporting modes:

- **Standard Mode:** Captures key press events (0-9, *, #), including invalid inputs and timeout events, providing detailed per-key interaction statistics.
- **Custom Mode:** Supports multi-digit or combined key inputs. Reports aggregate IVR activity, including total call entries, invalid inputs, and timeouts.

Statistics

CDR Statistics Concurrent Call Statistics Call Charges Statistics **Call Reports**

Report Type: IVR Report Time: 2026-03-01 00... ~2026-05-08 23... Type: Standard IVR: 7000-70001

Export Refresh

IVR	Press 0	Press 1	Press 2	Press 3	Press 4	Press 5	Press 6	Press 7	Press 8	Press 9	Press #	Press *	Response Timeout	Invalid Input Destination	Details
7000	1	3	1	9	1	1	1	1	1	2	0	1	1095	6	i

Total: 1 [<](#) [1](#) [>](#) 10 / page Goto

Standard IVR Report

Statistics

CDR Statistics Concurrent Call Statistics Call Charges Statistics **Call Reports**

Report Type: IVR Report Time: 2026-03-01 00... ~2026-05-08 23... Type: Custom IVR: 7000-70001

Export Refresh

Key	Count	Details
Overall IVR	1115	i
Response Timeout	1095	i
Invalid Input Destination	6	i
1	1	i
3	6	i
9	1	i
911	3	i
9911	3	i

Total: 8 [<](#) [1](#) [>](#) 10 / page Goto

The report can be exported in two formats:

- **Basic List:** Lists all IVRs and the trigger counts of their key press events.
- **Detailed List:** Includes the caller information, triggered key press events, the time of the events, and how long the callers were in the IVRs. In addition to the information in the Basic report

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Report Type

Time

IVR Report

2026-04-14 00:00 ~ 2026-04-14 23:59

Export

Refresh

Export (Basic List)

Export (Detailed List)

Press 1

Press 2

Press 3

Press 4

Press 5

Press 6

P

IVR Report Export Types

Ring Group Statistics

This report provides performance metrics for ring groups, including total calls received, answered calls, and answer rate.

It enables evaluation of call distribution efficiency and group responsiveness across configured ring groups.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Report Type

Time

Ring Groups

Ring Group Statistics

2026-04-14 00:00 ~ 2026-04-14 23:59

6400-RG1 ~ 6401-Sales_Ring_Group

Export

Refresh

Ring Groups	Answered	Received	Answered Rate
6400	0	1	0.00%
6401	1	1	100.00%
Total	1	2	50.00%

Total: 3

1

10 / page

Go to

Ring Group Statistics

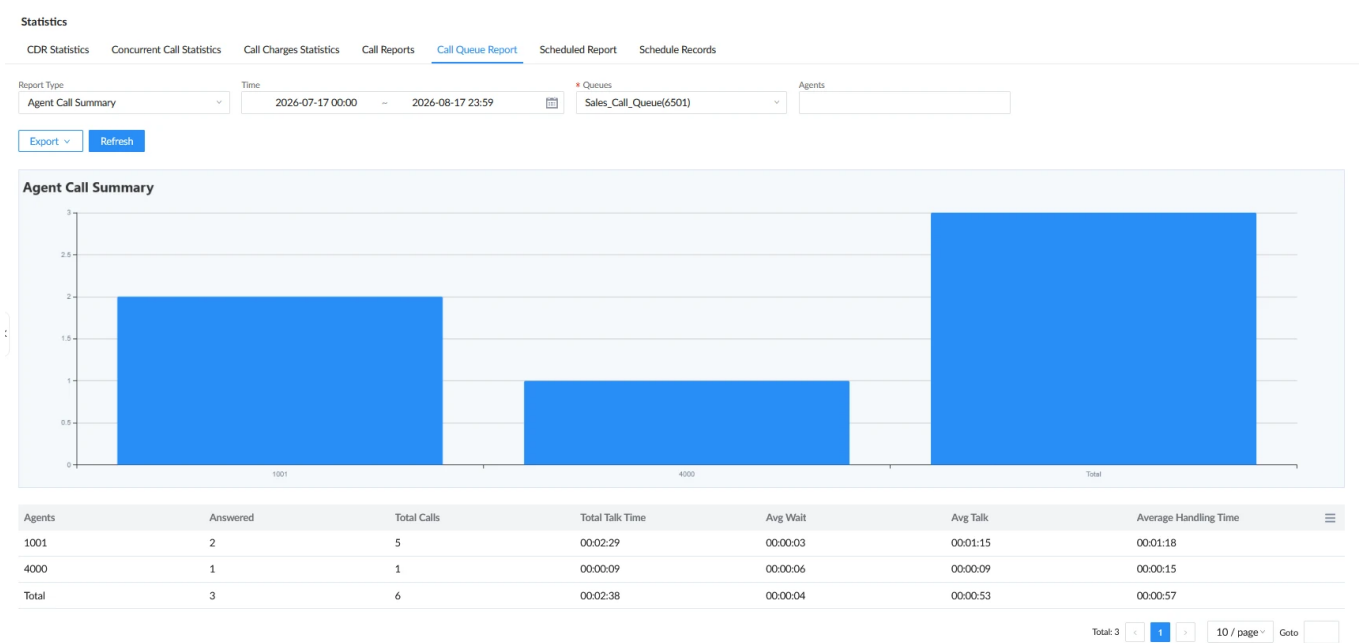
Call Queue Reports

The Call Queue Reports section provides comprehensive, dedicated analytics for call queue performance, agent activities, and queue response metrics across the UCM. Administrators can use these reports to analyze call flow efficiency, monitor agent productivity, and track queue responsiveness over selected time periods.

To access these reports, please navigate to **CDR -> Statistics -> Call Queue Report** and select a report type from the drop-down menu to view its detailed metrics.

Agent Call Summary

Measures individual agent call statistics throughout a specified date range and queue. It displays total calls handled, answered volume, total talk time, average wait time, average talk time, and average handling time per agent.



Agent Login Report

Lists individual agent login activity throughout a selected date range for a specific call queue, allowing administrators to track attendance, active duration, and login/logout timestamps.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Agent Login Report

Time

2026-07-17 00:00 – 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

Refresh

Agents	Queues	Login Time	Logout Time	Login Duration
1000	6501	2026-05-21 18:13:51	2026-08-17 15:49:18	2109:35:27
Total				2109:35:27
1001	6501	2026-05-21 18:13:53	2026-08-17 15:49:22	2109:35:29
Total				2109:35:29
4000	6501	2026-07-17 14:46:53	2026-08-17 15:49:27	745:02:34
Total				745:02:34

Total: 6110 / pageGoto

Agent Unanswered Report

Displays individual agent unanswered calls throughout a date range. It provides visibility into the number of missed calls, attempts, and caller number.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Agent Unanswered Report

Time

2026-07-17 00:00 – 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

Refresh

Agents	Time	Total Wait Duration	Caller Number	Queues	Queue Status	Call Attempts	Count
1001	2026-08-17 14:53:08	00:00:14	4001	6501	Unanswered	1	1
1001	2026-08-17 15:01:05	00:00:54	4002	6501	Unanswered	2	1
Total		00:01:08				3	2

Total: 3110 / pageGoto

Agent Pause Report

Lists individual agent pausing activity throughout a date range, tracking pause durations, reasons, and total offline time during operational hours.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Call Queue Report

Scheduled Report

Schedule Records

Report Type

Agent Pause Report

Time

2026-07-17 00:00

2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

Refresh

Agents	Pause Time	Pause Reason	Resume Time	Pause Duration	Count
1001	2026-08-17 15:54:54	Backoffice		00:00:00	1
Total				00:00:00	1
1002-Marketing Department	2026-08-17 15:51:48	Lunch	2026-08-17 15:53:07	00:01:19	1
Total				00:01:19	1

Total: 4

<

1

>

10 / page

Goto

Agent Performance

Measures individual agent performance listed and grouped directly under their respective queues throughout a date range, enabling direct performance comparisons within specific teams.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Call Queue Report

Scheduled Report

Schedule Records

Report Type

Agent Performance

Time

2026-07-17 00:00

2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

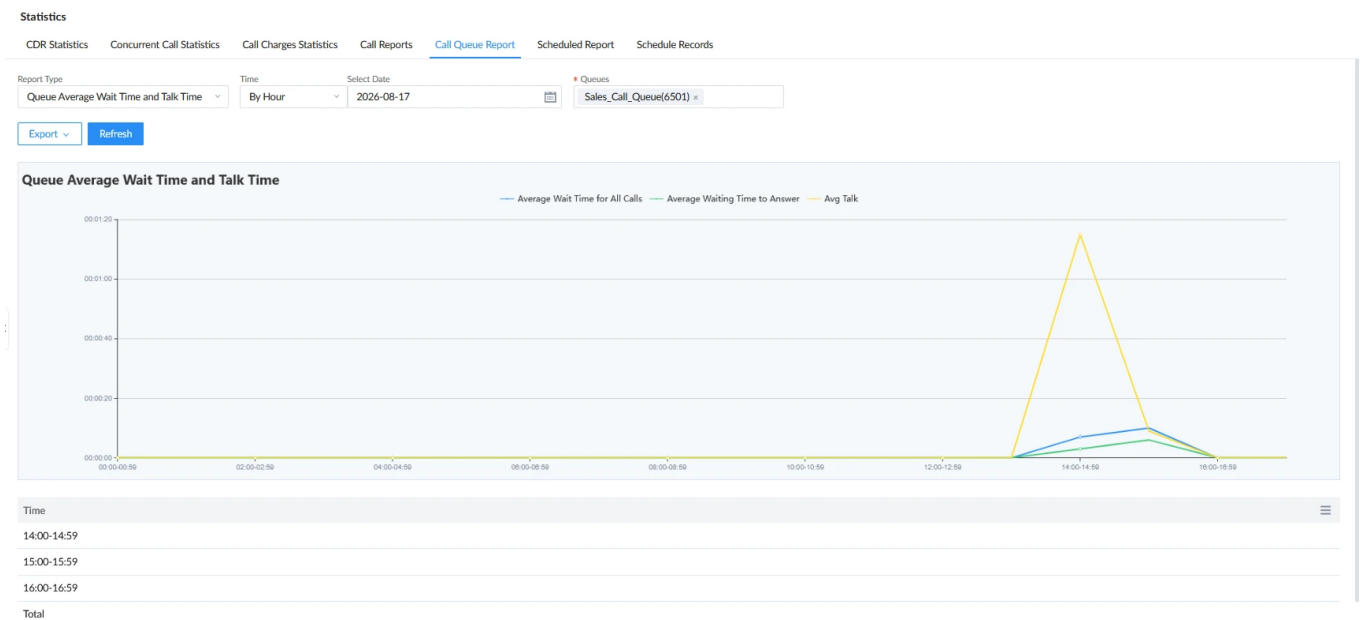
Refresh

Queues	Total Calls	Answered	Unanswered	Total Wait Duration	Maximum Waiting Time	Total Talk Time	Call Answer Rate
6501	13	3	10	00:00:12	00:00:06	00:02:38	23.08%

Agents	Total Calls	Answered	Total Wait Duration	Maximum Waiting Time	Total Talk Time	Call Answer Rate	Options
1001	5	2	00:00:06	00:00:04	00:02:29	40.00%	ⓘ
4000	1	1	00:00:06	00:00:06	00:00:09	100.00%	ⓘ

Queue Average Wait Time & Talk Time

Displays a graph showing caller wait time and talk time hourly, daily, or monthly for selected queues, averaging the data across the chosen time frame to help optimize queue staffing levels.



Queue Callback Report

Lists individual queue callback activity throughout a date range and specified queue, detailing requested callbacks, execution timestamps, and call results.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Queue Callback Report

Time

2026-07-17 00:00 - 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Export

Refresh

Queues	Callback Time	Callback Number	Total Wait Duration	Callback Result
Total			00:00:00	

Total: 1

1

10 / page

Goto

Queue Callback Summary

Displays a graphical representation of queue callback statistics over a specified date range. It provides visual insights into overall callback performance, comparing successful connections against failed callback attempts across the selected queues.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Queue Callback Summary

Time

2026-07-17 00:00 - 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Export

Refresh

Queue Callback Summary

Callback Success

Callback Failure

Queues	Callback Failure	Callback Success	Callback Requests	Total Calls
6501	0	0	0	13
Total	0	0	0	13

Queue Performance

Measures individual queue performance throughout a date range, focusing on total wait duration, average handling time, and overall service levels per queue.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Queue Performance

Time

2026-07-17 00:00 - 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Export

Refresh

Queues	Total Calls	Answered	Unanswered	Total Wait Duration	Maximum Waiting T...	Avg Wait	Average Handling TI...	Total Talk Time	Avg Talk	Call Answer Rate	SLA
6501	13	3	10	00:00:12	00:00:06	00:00:04	00:00:57	00:02:38	00:00:53	23.08%	0.00%
Total	13	3	10								

Total: 2

1

10 / page

Goto

Queue Performance Activity

Provides a time-based breakdown (hourly, daily, or monthly) of call queue activity. Administrators can use this report to evaluate traffic distribution, monitor answer rates and average wait times, and track SLA performance over a selected period.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Queue Performance Activity

Time

By Hour

Select Date

2026-08-17

Queues

Sales_Call_Queue(6501)

Export

Refresh

Time	Total Calls	Answered	Unanswered	Maximum Waiting Time	Avg Wait	Avg Talk	Call Answer Rate	SLA
14:00-14:59	4	2	2	00:00:04	00:00:03	00:01:15	50.00%	0.00%
15:00-15:59	6	1	5	00:00:06	00:00:06	00:00:09	16.67%	0.00%
16:00-16:59	3	0	3	00:00:00	00:00:00	00:00:00	0.00%	0.00%
Total	13	3	10	00:00:06	00:00:04	00:00:53	23.08%	0.00%

Total: 4

<1>

10 / page

Goto

Agent Activity Report

Provides a comprehensive performance breakdown for each agent across selected queues over a specified date range. It details total call volume, answer rates, unanswered calls, wait times, talk duration, and average handling times per agent.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Agent Activity Report

Time

2026-07-17 00:00 – 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

Refresh

Agents	Queues	Total Calls	Answered	Call Answer Rate	Avg Wait	Avg Talk	Average Handling TL...	Unanswered	Total Wait Duration	Maximum Waiting T...	Total Talk Time
1001	6501	5	2	40.00%	00:00:03	00:01:15	00:01:18	3	00:00:06	00:00:04	00:02:29
4000	6501	1	1	100.00%	00:00:06	00:00:09	00:00:15	0	00:00:06	00:00:06	00:00:09
Total		6	3					3			

Total: 3

<1>

10 / page

Goto

Queue Record Report

Lists every individual call made to the selected queues throughout a specified date range. It details the caller number, queue status, number of call attempts, answering agent, call timestamp, total wait duration, and total talk time.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall ReportsCall Queue ReportScheduled ReportSchedule Records

Report Type

Queue Record Report

Time

2026-07-17 00:00 – 2026-08-17 23:59

Queues

Sales_Call_Queue(6501)

Export

Refresh

Queues	Caller Number	Total Talk Time	Queue Status	Call Attempts	Answered Agent	Time	Total Wait Duration
6501	4002	00:00:09	Answered	1	4000	2026-08-17 15:14:51	00:00:06
6501	4002	00:00:00	Unanswered	2		2026-08-17 15:01:05	00:00:54
6501	4001	00:02:14	Answered	1	1001	2026-08-17 14:55:52	00:00:02
6501	4001	00:00:00	Unanswered	1		2026-08-17 14:53:08	00:00:14
6501	4001	00:00:15	Answered	1	1001	2026-08-17 14:52:32	00:00:04

Total: 5

<1>

10 / page

Goto

Agent Inbound Queue Record Report

Displays a granular call log for each agent within selected queues over a date range, tracking individual interactions, ring duration, talk time, wait time, and whether the agent answered or missed the call.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Call Queue Report

Scheduled Report

Schedule Records

Report Type

Agent Inbound Queue Record Report

Time

2026-07-18 00:00

2026-08-18 23:59

Queues

Support_Call_Queue(6500)

Sales_Call_Queue(6501)

Agents

Export

Refresh

Agents	Agent Last Call Status	Queues	Caller Number	Call Attempts	Queue Status	Total Ring Duration	Total Talk Time	Queue Wait Time	Time
4000	Answered	6501	4002	1	Answered	00:00:06	00:00:09	00:00:06	2026-08-17 15:14:51
1001	Unanswered	6501	4002	2	Unanswered	00:00:49	00:00:00	00:00:04	2026-08-17 15:01:05
1001	Answered	6501	4001	1	Answered	00:00:02	00:02:14	00:00:02	2026-08-17 14:55:52
1001	Unanswered	6501	4001	1	Unanswered	00:00:14	00:00:00	00:00:14	2026-08-17 14:53:08
1001	Answered	6501	4001	1	Answered	00:00:04	00:00:15	00:00:04	2026-08-17 14:52:32

Total: 5

1

10 / page

Goto

Queue Analysis Report

Sorts and measures call statistics on an hourly, daily, or monthly basis, displaying a dedicated row for each individual queue during every time interval. This provides per-queue trends, unlike Queue Performance Activity, which summarizes total system traffic.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Call Queue Report

Scheduled Report

Schedule Records

Report Type

Queue Analysis Report

Time

By Month

Select Date

2026

Queues

Sales_Call_Queue(6501)

Export

Refresh

Month	Queues	Total Calls	Answered	Unanswered	Maximum Waiting TL...	Call Answer Rate	Avg Wait	Avg Talk	SLA
August	6501	13	3	10	00:00:06	23.08%	00:00:04	00:00:53	0.00%
Total		13	3	10	00:00:06	23.08%	00:00:04	00:00:53	0.00%

Total: 2

1

10 / page

Goto

Queue Statistics Report

Generates a satisfaction breakdown for selected queues within a date range, categorizing caller rating scores into levels 1 to 5 alongside counts for non-surveyed calls.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Call Queue Report

Scheduled Report

Schedule Records

Report Type

Satisfaction Report

Time

2026-07-18 00:00

2026-08-18 23:59

Queues

Sales_Call_Queue(6501)

Agents

Export

Refresh

Queues	Not Surveyed	Not Evaluated	Level 1	Level 2	Level 3	Level 4	Level 5
6501	3	0	0	0	0	0	0

Agents	Not Surveyed	Not Evaluated	Level 1	Level 2	Level 3	Level 4	Level 5
1001	2	0	0	0	0	0	0
4000	1	0	0	0	0	0	0

Scheduled Report

The Scheduled Report tab allows administrators to create automated report delivery schedules and have reports sent via email at regular intervals.

This feature is limited to call queue reports.

In order to receive the scheduled reports, administrators must correctly configure Email Settings.

To configure an automated report schedule:

- Navigate to **CDR -> Statistics -> Scheduled Report**.

2. Click **Add** to open the creation window (or click **Email Template** to customize the notification layout).

Statistics

CDR Statistics Concurrent Call Statistics Call Charges Statistics Call Reports Call Queue Report Scheduled Report Schedule Records

Add Email Template

Display Filter

Name	Report Type	Schedule Time	Repeat	Options
Report1	Agent Call Summary	2026-08-17 11:41:58	Every Day, 12:00	

Total: 1 < 1 > 10 / page Goto

3. Under **Report Data**, select the Report Type, Time frame, target Queues, Agents, and customize the List Fields to include in the output.

Statistics > Create New Scheduled Report

Report Data

* Report Type

Agent Activity Report

Time

This Month

* Queues

Sales_Call_Queue(6501) x

* Agents

1001 x

* Select List Fields 1

3/12 Available

Search

☒ Agents

☐ Queues

☐ Total Calls

☐ Answered

☒ Call Answer Rate

☒ Avg Wait

< >

0 Selected

Search

None

4. Under **Schedule Information**, enter the schedule Name, recipient Email, preferred Export Type (XLSX, CSV, PDF), and execution recurrence pattern (Repeat interval and time).

Schedule Information

* Name

Agent_Report

* Email

john.doe@grandstream.com

Export Type

PDF

Repeat

By Day

10:00

Cancel

Save

Once configured, all active schedules are listed on this page for quick editing or management.

Statistics

CDR Statistics Concurrent Call Statistics Call Charges Statistics Call Reports Call Queue Report Scheduled Report Schedule Records

AddEmail Template

Display Filter

Name	Report Type	Schedule Time	Repeat	Options
Report1	Agent Call Summary	2026-08-17 11:41:58	Every Day, 12:00	  
Agent_Report	Agent Activity Report	2026-08-18 09:03:12	Every Day, 10:00	  

Total: 2

<1>

10 / page

Goto

Schedule Records

The **Schedule Records** tab provides full historical tracking and audit logging for all automated email report transmissions. On this page users can:

- Review historical entries including the schedule **Name**, transmission **Send Status** (e.g., Sent successfully), and exact **Send Time**.
- Click the **Info icon (i)** under the Options column to preview the sent report in a different tab.
- Select individual or multiple log entries to delete historical records as needed.

Statistics

CDR Statistics Concurrent Call Statistics Call Charges Statistics Call Reports Call Queue Report Scheduled Report Schedule Records

Delete

Display Filter

☐	Name	Send Status	Send Time	Options
☐	Report1	Sent successfully	2026-08-17 12:00:17	 

Total: 1

<1>

10 / page

Goto

Recordings

This page lists all the recording files recorded by "Auto Record" per extension/ring group/call queue/trunk, or via feature code "Audio Mix Record". If external storage device is plugged in, for example, SD card or USB drive, the files are stored on the external storage. Otherwise, internal storage will be used on the UCM630xA.

Recording Files

DownloadDownload AllDeleteClearScan

LocalBasic Call Recordings2022-08

Display Filter

☐	CALLER	CALLEE	CALL TIME	SIZE	OPTIONS
No Data					

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

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.

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 ...).

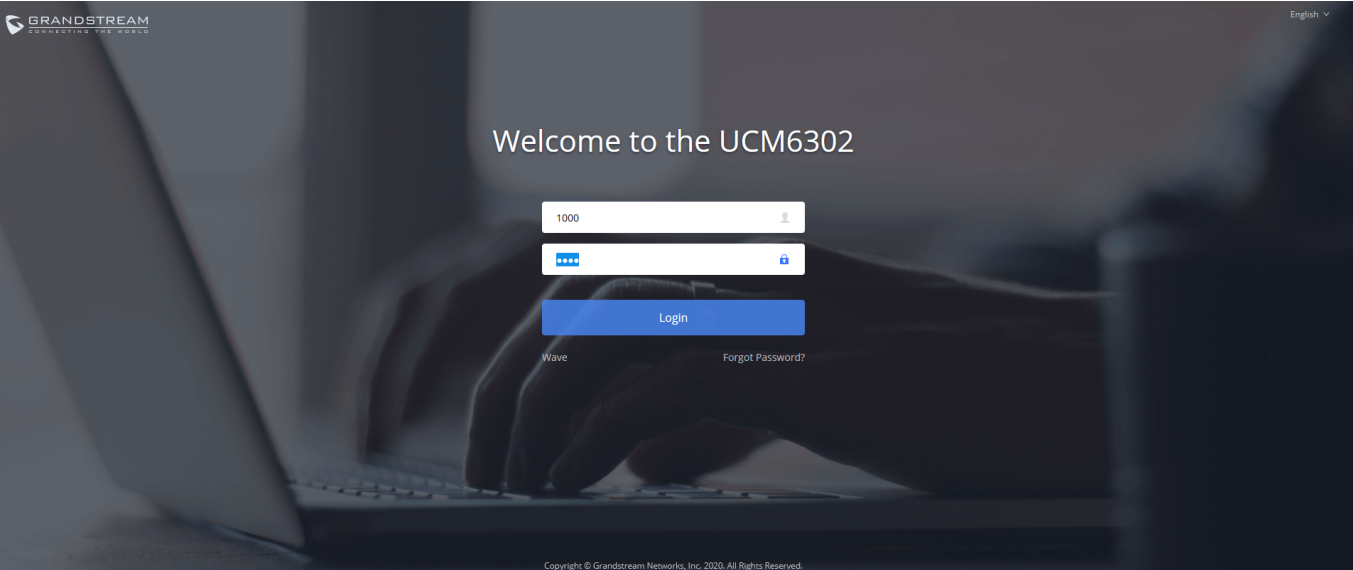
The login credentials are configured by Super Admin. The following figure shows the dialog of editing the account information by Super Admin. The Username must be the extension number and it is not configurable, and the password is set on "User Password" field and it should not be confused with the SIP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

Edit User Information: 1000

* User Name :	1000	* User Password :	mYpassWord!
Privilege :	Consumer ▼	Department :	Support
Fax :		Email Address :	user1000@domain.local
First Name :	John	Last Name :	DOE
Home Number :		Mobile Phone Numb...	

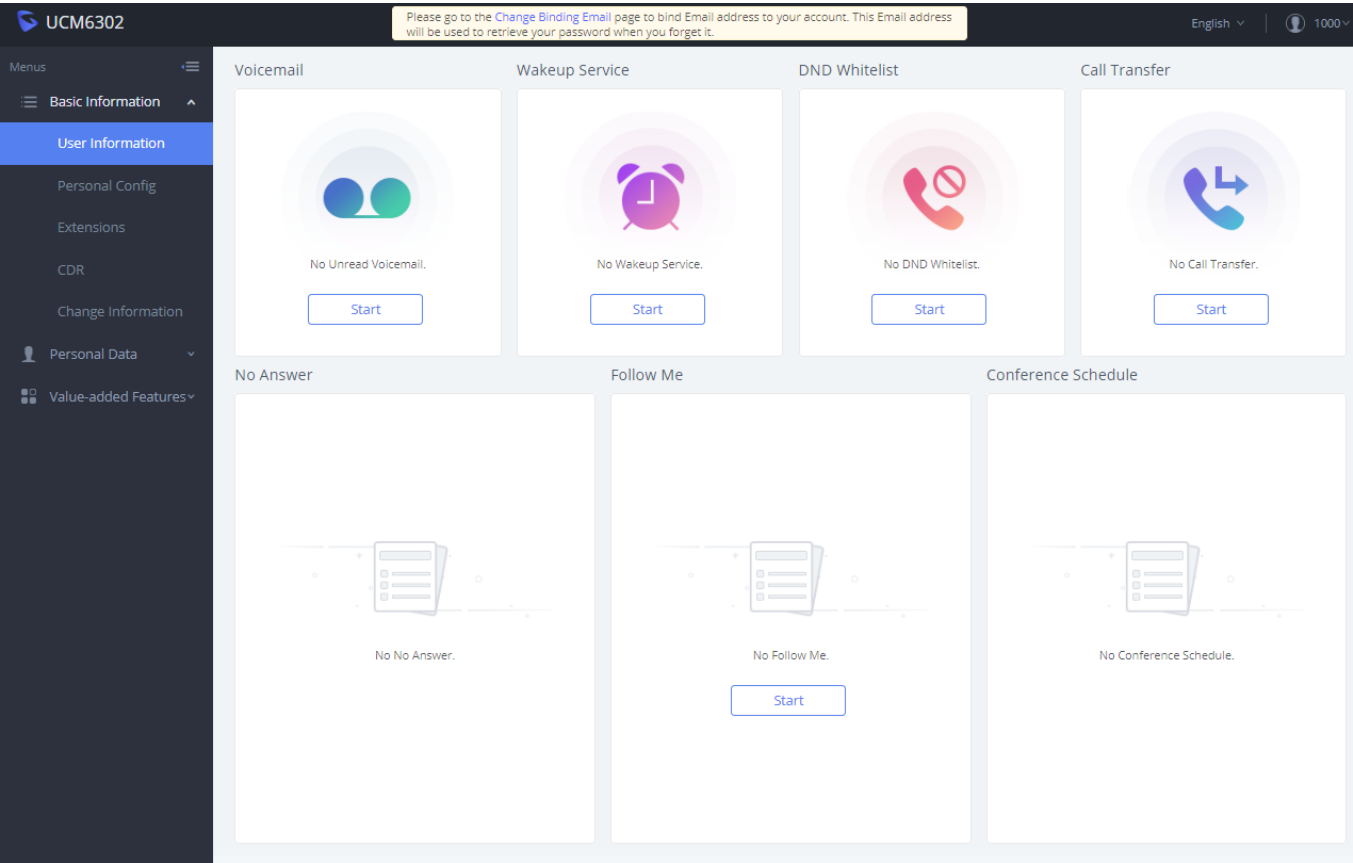
Edit User Information by Super Admin

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.

User Management

User Information

Custom Privilege

+ Add

USERNAME	PRIVILEGE	LAST OPERATION TIME	OPTIONS
admin	Super Administrator	2021-11-05 13:02:11	 

1

10 / page

User Management Page Display

User Information

When logged in as Super Admin, click on "Add" to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.

Create New User

CancelSave

Username:

John

Privilege:

Administrator

User Password:

Admin123@

Multi-Factor Authentication:

☐ Email Settings

Email Address:

Create a New User

Username	Configure a username to identify the user which will be required in Web GUI login. Letters, digits, and underscore are allowed in the username.
User Password	Configure a password for this user which will be required in Web GUI login. English input is allowed without space, ' and ".
Privilege	This is the role of the Web GUI user. When super admin creates new user, "Administrator" or customized privilege can be selected.
Multi-Factor Authentication	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.
Email Address	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

User Management

User InformationCustom Privilege

+ Add

USERNAME	PRIVILEGE	LAST OPERATION TIME	OPTIONS
admin	Super Administrator	2021-11-05 13:08:50	
John	Administrator	--	

< 1 >

10 / page

User Management New Users

Multi-Factor Authentication

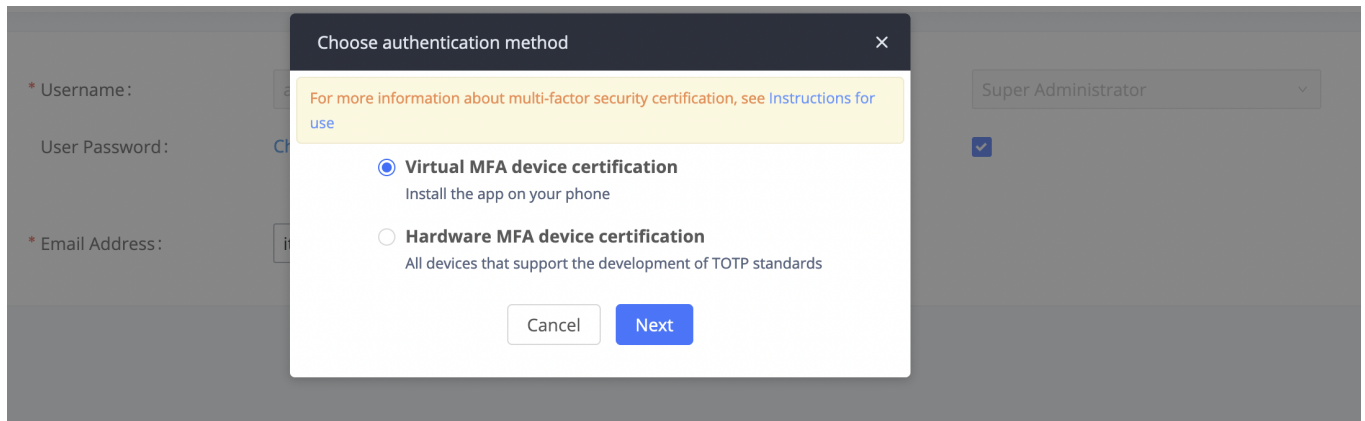
To enhance the security for UCM, super admin and admin can select to use multi-factor authentication method for login to protect the login information. Virtual MFA and hardware MFA are supported and can be selected. Once enabled, the user must use MFA code to verify before login.

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**:

System Status
Extension/Trunk
Basic Call Features
Advanced Call Features
Messaging
PBX Settings
System Settings
Contacts
Device Management
Maintenance
User Management
Login Settings

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	
Admin	Administrator	
Wave_Admin	Wave Administrator	

Super Administrator

- This is the highest privilege. Super Admin can access all pages on UCM630xA Web GUI, change configuration for all options and execute all the operations.
- Super Admin can create, edit, and delete one or more users with the "Admin" privilege
- Super Admin can edit and delete one or more users with the "Consumer" privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account "admin" is configured with the "Super Admin" privilege and it is the only user with the "Super Admin" privilege. The Username and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on **Maintenance->Login Settings** page.
- Super Admin could view operations done by all the users in **Maintenance->User Management->Operation Log**
- The Super Admin can allow administrators to view SFTP, NAS and Email Account passwords.

* Privilege Name 2 - 64 characters, alphanumeric characters, chinese characters, and special characters _ - are supported

Password Visibility Toggle ⓘ ☒ SFTP Password ☒ NAS Password ☒ Email Account Password

* Custom Privilege ⓘ

▼ ☒ All

☒ Basic Privileges ☐ Backup ☐ Upgrade ☐ RemoteConnect

Password Visibility Toggle

Administrator

- Users with "Admin" privilege can only be created by "Super Admin" user.
- "Admin" privilege users cannot create new users for login.
- "Admin" privilege users are by default not allowed to access the following pages:

Maintenance → Backup

Maintenance → Upgrade

RemoteConnect

Settings→User Management→Operation Log

Note: By default, administrator accounts are not allowed to access backup menu, but this can be assigned to them by editing the option "**Maintenance->User Management->Custom Privilege**" then press the "Edit" icon to edit the "Admin" account and include backup operation permission for these types of users.

* Privilege Name 2 - 64 characters, alphanumeric characters, chinese characters, and special characters _ - are supported

Password Visibility Toggle ⓘ ☒ SFTP Password ☒ NAS Password ☒ Email Account Password

* Custom Privilege ⓘ

▼ ☒ All

☒ Basic Privileges ☐ Backup ☐ Upgrade ☐ RemoteConnect

Assigning Permissions to Admin Users

Wave Administrator

- This permission type does not support editing or deletion.
- This includes management of Wave-related function settings only and does not involve access to the UCM module.
- Users can set the Wave Admin privilege for specific extension under **Extension/Trunk->Extensions->Edit Extension**.

For more information, please refer to the Wave Administrator Guide guide.

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	☒		

Add Custom Privilege

User Management

Add		
Privilege Name	Privilege Type	Options
Super_Admin	Super Administrator	 
Admin	Administrator	 
Wave_Admin	Wave Administrator	 

To create a custom privilege role, click **Add** and select the accessible modules from the table below:

Module	Custom Privileges
System Status	System Status
Extension/Trunk	Extensions, Extension Groups, Outbound Routes, Inbound Routes
Basic Call Features	Meeting, IVR, Voicemail, Ring Groups, Paging/Intercom, Call Queue, Queue Recordings, Queue Statistics, Queue Board, Queue Operation Panel, Speed Dial, Event List, Feature Codes, Parking Lot
Advanced Call Features	Pickup Groups, Dial By Name, DISA, Callback, Scheduled Call, Fax Sending, Fax/T.38, Announcement, SCA, Emergency Calls, Restrict Calls
PBX Settings	Music on Hold, Voice Prompt
System Settings	Time Settings, LDAP Server
Contacts	Contacts
Device Management	Zero Config
Maintenance	System Events, Backup
CDR	CDR Recordings, CDR Records, Call Note, CDR Statistics, Call Rate
RemoteConnect	UCM RemoteConnect

User Portal/Wave Privileges

The administrator can create customized privileges related to an extension's User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.

After the creation of the privilege, the administrator can assign the privilege to a specific extensions by navigating to **Extension/Trunk > Extensions > Basic Settings > User Portal/Wave Privileges**.

User Settings

First Name ⓘ

Email Address ⓘ

* User Portal/Wave Privileges

Default



[Add / Edit Privileges](#)

Department ⓘ

Enterprise Root Directory



User Portal/Wave Configuration

Wave Permissions

Under Wave Permissions category, the user can configure the various permissions for the basic features of Wave such as using the chat, making audio/video calls, meeting, use application store, etc...

User Management > Edit User Portal/Wave Privileges: Default

Privilege Name

Default

Wave Permissions ⓘ User Portal/Wave Privileges ⓘ Administrator Privileges ⓘ

Chat ⓘ

Delete Chat Session ⓘ

Delete Message ⓘ

Send File ⓘ

Download Chat Logs ⓘ

End-to-End Encrypted Chat ⓘ

Wave App Screenshot and Screen Recording ⓘ

Video Call ⓘ

Meeting ⓘ

Online Status ⓘ

Login Settings

Multi-client Login Settings ⓘ

Remote Logout ⓘ

Wave Permissions Tab

- **Chat:** Toggles ability to use the Wave Chat feature.
 - **Delete Chat Session:** Toggles support for Wave to delete chats and chat history. This data will only be deleted on the Wave client side.
 - **Delete Message:** Controls whether Wave users will be allowed to delete messages that have been sent.

Deleted messages will not be visible to anyone.

- **Send File:** Toggles file/image sending support in Wave chat. If disabled, users will still be able to download, view and forward chat files.
- **Download Chat Logs:** If enabled, chat logs will be downloadable from the Wave client, including chat logs from Wave/WhatsApp/Telegram/LiveChatsessions.
- **End-to-End Encrypted Chat*:** Toggles ability to use the Wave End-to-End Encrypted Chat feature.
- **Wave App Screenshot and Screen Recording:** Controls whether users are allowed to take screenshots and perform screen recordings in the Wave mobile app.
- **Meeting:** Toggles ability to use the Wave Meeting feature.
- **Online Status:** Toggles ability to set Wave online status such as "Busy", "Appear Away", "Do Not Disturb", "Appear Offline", etc. If unchecked, the status will be displayed as only either "Online" or "Idle".
- **Login Settings**
 - **Multi-client Login Settings:** If enabled, users will be allowed to enable or disable the option "Allow Simultaneous Logins from the Same Client Type".
- **Remote Logout:** If enabled, Wave users will be able to log out of their accounts from other logged-in devices.
- **Recording Status:** Controls whether the recording status is displayed in all calls/conferences of the extensions. **Note:** If the call recording prompt is enabled, it will be played as this setting affects the indicator that shows that a call is being recorded on Wave.
- **Clear Recent Call History:** Toggles ability to delete recent call history entries and entire recent call history on Wave.
- **Application:** Toggles ability to access the "Applications" page under Wave Desktop and Wave Web.
- **Smart Devices:** Toggling off privileges will hide the corresponding pages and options in Wave.
- **Door System**
- **Monitor**
- **Call Device (CTI)**
- **3rd Party Applications**
- **App Store:** Toggles ability to install applications from Wave application store. If unchecked, the application store will be hidden, but installed apps can still be used.

User Portal/Wave Privileges

Under User Portal/Wave Privileges, the administrator can configure access privileges to specific settings and features, such as adjusting account settings, changing SIP/IAX passwords and AuthIDs, setting DND, or managing personal data (e.g., CDRs, Follow Me, Voicemail, recordings, etc.).

* Privilege Name

Wave Permissions [?](#) **User Portal/Wave Privileges** [?](#) Administrator Privileges [?](#)

- ▼ ☒ Account Settings [?](#)
 - ☒ Change Email Address [?](#)
- ▼ ☐ Extension Settings [?](#)
 - ☒ Do Not Disturb [?](#)
 - ☒ SIP/IAX Password & AuthID [?](#)
 - ☐ Configuration Voicemail
- ▼ ☐ Manage Recordings [?](#)
 - ☐ Delete Recordings [?](#)
- ▼ ☒ Personal Data Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
 - ▼ ☒ CDR
 - ☒ Create or Edit Call Notes [?](#)
 - ☒ Follow Me
 - ☒ Voicemail
 - ☒ Recording 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
 - ☒ Scheduled Call

The table below describes the privilege options available under the User Portal/Wave Privileges tab:

Privilege Option	Description
Account Settings	If unchecked, hides the User Portal -> Basic Information -> Account Settings page and the Wave -> Sidebar -> User -> Account Settings option. Change Email Address: Toggles whether users assigned to this privilege role are allowed to modify their extension email address. If unchecked, the email modification field will be restricted.
Extension Settings	If unchecked, hides the extension's User Portal -> Basic Information -> Extensions page and the Wave -> Sidebar -> User -> Call Settings option. Do Not Disturb: Toggles the ability to configure Do Not Disturb (DND) status through the User Portal or Wave. SIP/IAX Password & AuthID: Toggles access to view or edit the SIP/IAX Password and AuthID settings under the User Portal -> Basic Information -> Extensions -> Basic Settings page. Configuration Voicemail: Toggles the ability to configure voicemail preferences directly.
Manage Recordings	Toggles the ability to view recordings through the User Portal and Wave, including call log recordings, meeting details, and Wave application recordings. Delete Recordings: Toggles the ability to delete recordings through the User Portal and Wave. For Wave, this includes deleting call logs, meeting details, and recording files.
Personal Data	Toggling off parent or sub-privileges hides the corresponding pages and options in the User Portal and Wave: CDR: Toggles access to Call Detail Records. Create or Edit Call Notes: Toggles permission to create, edit, or view notes/tags attached to call records. Follow Me: Toggles access to Follow Me forwarding rules. Voicemail: Toggles access to personal voicemail messages. Recording Files: Toggles access to dedicated recording files. Fax Files: Toggles access to received/sent fax files. SCA: Toggles access to Shared Call Appearance features.

Other Features	Toggling off parent or sub-privileges hides the corresponding pages and options in the User Portal and Wave: Fax Sending: Toggles permission to send faxes. Call Queue: Toggles access to call queue management/wallboard interfaces. Scheduled Call: Toggles permission to create or manage scheduled calls.
----------------	---

*: Features which are marked by an asterisk are a part of RemoteConnect plans.

Administration Privileges

Under Administrator Privileges, the administrator can configure enabling certain extensions to view a designated team's CDR.

User Management > Edit User Portal/Wave Privileges: Default

Privilege Name

Wave Permissions ⓘ User Portal/Wave Privileges ⓘ Administrator Privileges ⓘ

☐ View Team CDRs And Recordings ⓘ Team

☐ Download Team Recording Files

Cancel Save

Administrator Privileges

- **View Team CDRs and Recordings:** Define whether certain extensions can view each other's CDR. Click on "Team" to designate the extensions.
- **Download Team Recording:** When this option is enabled, the extensions selected in the team will be allowed to access each other's CDR and call recording files.

Pre-installed Plugins

The administrator can set the plug-ins which will be installed when the user logs into Wave Desktop. To configure the pre-installed plugins, follow the steps below.

1. Navigate to **Maintenance > User Management > User Portal/Wave Privileges** then click "Pre-installed Plug-ins".

User Management

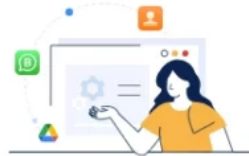
System User Information User Portal/Wave Privileges Extension Login Management User Endpoint Access History

Add **Pre-installed plugins**

Privilege Name ⓘ	Options
Default	

Total: 1 < 1 > 10 / page ▾ Goto

2. Click on "Add Add-in" button.



Pre-install the Wave add-in for extension users. After users sign in to Wave, the assigned add-ins will be automatically installed.

[Add Add-in](#)

Pre installed Plug ins

[< Add](#)

*Add-in

Configure Parameters

Only json format is supported. Please refer to the user manual for rules

[User Manual](#)

*Users

☒ All Users ☐ Specific Users

Add Pre installed Plug ins

Parameter	Description
Add-in	Select an add-in.Act! CRMBitrix24Capsule CRMDynamics 365FreshdeskGoogle DriveHubspotIPVideoTalkLess Annoying CRMMonday Sales CRMODOO CRMOffice365OfficeRnD Hybrid WorkOracle NetSuiteSalesforceSugarCRMTelegramVtiger CRMWhatsapp BusinessZendeskZoho CRMZoho Desk
Configure Parameters	Enter the configuration parameters. The configuration parameters consist of authentication information, database name, webhook url etc....Note: Please note that only JSON format is supported.Example: Whatsapp Business{"config": [{"name":"xxxxx","accessToken":"xxxxx","payloadKey":"xxxxx","webhookUrl":"xxx","phoneNumIDList": ["xxxxx","xxxxx"] } }
Users	Select which extension(s) to apply this rule to.All UsersSpecific Users

For the complete steps and information about pre-installing plug-ins, please refer to the following guide:

Extension Login Management

Extension Login Management allows the administrator to review the logged-in sessions of SIP devices and Wave.

User Management

User Information

Custom Privilege

User Portal/Wave Privileges

Extension Login Management

User Endpoint Access History

Updated based on SIP registration status.

Extension Number or Name

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	

Total: 4

<

1

>

10 / page

Goto

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	2022-11-11 10:18:22	192.168.5.119
			Android/iOS	2022-11-14 16:10:37	192.168.5.76
			User portal	2022-08-10 09:26:40	192.168.5.111
1002	Bonnie MacFarlan	SIP(WebRTC)	Wave Web/Desktop	2022-11-11 10:18:22	192.168.5.93
			Android/iOS	2022-11-14 16:53:03	192.168.5.79
			User portal	2022-08-23 15:49:30	192.168.5.111
1003	Catherine Braitwaite	SIP(WebRTC)	Wave Web/Desktop	2022-10-18 14:14:12	192.168.5.111
			Android/iOS	2022-11-14 20:34:59	192.168.5.76
			User portal	2022-11-17 09:19:44	192.168.5.168
1004	John Marston	SIP(WebRTC)	Wave Web/Desktop	2022-08-16 15:32:37	192.168.5.111
			Android/iOS	2022-11-16 11:26:44	192.168.5.91
1005	Abigail Roberts	SIP(WebRTC)	Wave Web/Desktop	2022-11-16 17:42:47	
			Android/iOS	2022-11-16 18:11:34	192.168.5.79
1006	Mary-Beth Gaskill	SIP(WebRTC)	Wave Web/Desktop	2022-11-16 16:21:14	192.168.5.165
			Android/iOS	2022-11-16 17:37:50	192.168.5.79
1007	Hosea Matthews	SIP(WebRTC)	Wave Web/Desktop	2022-11-16 17:50:35	192.168.5.63

< 1 >

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 :

814088094@qq.com

[Email Template](#)

Enter Old Password	Enter the Old Password for UCM630xA
Change Password	Enable Change Password
Enter New Password	Enter the New Password for UCM630xA
Re-enter New Password	Retype the New Password for UCM630xA
Change Username	Enable Change Username
Please enter the username	Enter the Username
Email Address	The Email address is the User Email Address. It is used for receiving password information if the user forgets his password.

Change Password

Change Username

UCM630xA allows users now to change Super Administrator username.

Change Username

Change Username :



* Please enter the username :

GSadmin

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:

814088094@qq.com

Email Template

Change Binding Email

Email Address	Email Address is used to retrieve password when password is lost
---------------	--

Change Binding Email option

Login Security

After the user logs in the UCM630X Web GUI, the user will be automatically logged out after certain timeout, or he/she can be banned for a specific period if the login timeout is exceeded. Those values can be specified under UCM630X 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 0 indicates no automatic logout.

SMS OTP Login ☐

Login Security Policy

Enable Login Security ☒

Max Login Attempts (IP) 50

Maximum number of login attempts 5

Ban Period (m) 5 0 indicates a permanent ban after exceeding the max number of failed login attempts.

Login Banned IP/User List

Banned

Ban History

Q

Please enter ip address / userna...

Q

IP Address	Username	Banned Time	Estimated Ban Lift Time	Options
No data				

Login Allowlist

Cancel Save

Login Timeout Settings

Login Settings	
Login Timeout (m)	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. If set to 0, the user will not be logged out automatically. Valid range is 0 to 60 and default value is 0.
SMS OTP Login	If enabled, users will be able to log in and reset password via SMS verification code. Mobile phone numbers will need to be configured for administrators and extensions.
Login Security Policy	
Enable Login Security	Enable login security measure to prevent authentication attacks.
Max Login Attempts (per IP address)	The max allowed number of consecutive failed login attempts from an IP address. Once exceeded, no users will be able to log in from that IP address.Note: The valid range is between 5 to 100 attempts.
Maximum number of login attempts (per user)	The maximum number of consecutive failed login attempts. When exceeded, the user will not be able to log in for the amount of time specified in "User ban period".Note: The valid range is between 1 to 100 attempts.
Ban Period (m)	The amount of minutes that a user will be banned for after exceeding the maximum allowed number of consecutive failed login attempts. Note: The valid range is between 0 and 10000 minutes, with 0 indicating a permanent ban.
Login Banned User List	List of IP addresses which are banned from making any further login attempts.

Login Whitelist	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.

Login Settings

[Change Password / Email](#)

[Login Security](#)

[Remote Login](#)

+ Add Trusted Login Location

LOGIN LOCATION	OPTIONS
▶ Trusted Login Locations (1/5) When the UCM is logged into from a location other than the trusted login locations, a remote login alert will be generated if enabled. Note: Additional logins from that location will not trigger remote login alerts.	
▶ Other Login Locations Users can create a list of trusted login locations on the UCM.	

< 1 >

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

Remote Login

To add a trusted login location, the user must click on

Add Trusted Login Location

If a public IP address is entered as the trusted login location, the UCM will automatically detect the location of the IP address.

IP Address:
Check Location

Format: xxx.xxx.xxx.xxx

Close OK

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"**.

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".

Operation Log Display Filter

Delete Search Result(s) Clear Download Search Result(s) Download All Log

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.	Click to modify notes
2022-08-04 15:47:53	admin	192.168.5.111	Wrong account or password!	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 15:47:43	admin	192.168.5.111	Wrong account or password!	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 15:17:52	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 14:44:19	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 14:26:53	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 14:14:39	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 12:26:36	admin	192.168.5.111	This trusted login location already exists.	addCommonLoginAddr	Details	Click to modify notes
2022-08-04 12:26:26	admin	192.168.5.111	This trusted login location already exists.	addCommonLoginAddr	Details	Click to modify notes
2022-08-04 12:15:54	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes

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

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

Date	The date and time when the operation is executed.
Username	The username of the user who performed the operation
IP Address	The IP address and geographical location from which the operation has been made.
Results	The result of the operation.

Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
Specific Operation	Click on the hyperlinked operation detail to reveal more details.
Remark	Allows users to add notes and remarks to each operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on "Display Filter".

Operation Log

Hide Filter ^

Start Time:2019-12-1000:00

End Time:2019-12-1100:00

IPv4/IPv6 Address:

User Name:admin

FilterReset

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.

Upgrade

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 Series, please access the web UI of the UCM, then navigate to **Maintenance > Upgrade**

Upgrade Firmware

① It is recommended to back up your current configuration and data before upgrading. [Click here to back up](#)

① After downgrading, please factory reset the device to minimize risk of potential issues. It is highly recommended to create and keep backups of earlier firmware versions to restore in these scenarios.

UCM Upgrade

Current Firmware Version V 1.0.29.1

Detect New Firmware

Scheduled Detect [Scheduled Task](#)

Last Detect: No update record

Find New Version: -

System Firmware (.bin)

Wave Upgrade

Wave Web Firmware (.tgz)

Upgrade Firmware

On this page, the user can view the firmware version which is installed on the UCM. Clicking "Detect" will initiate firmware version verification, if there is a newer version, a prompt will appear to confirm downloading and installing the firmware.

The user can also schedule detection of the firmware version by clicking on "Schedule Task". For more information regarding scheduling tasks, please refer to [\[Task Management\]](#) section.

1. Click on "Choose File to Upload" field in front of "System Firmware (.bin)"
2. 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

Click on the "Upload" 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.

The **Scheduled Backup** feature enables UCM to automatically back up selected data according to defined schedules. Users can configure multiple backup tasks, each with its own schedule and storage destination, while ensuring that no two backups run simultaneously. Supported storage options include USB, SD card, SFTP server, NAS, and Amazon S3 storage.

To configure a scheduled backup, please refer to the steps below:

1. Access the Schedule Backup feature either by clicking the "Schedule Backup" button on the **Maintenance->Backup** page or by creating a new task in the **Maintenance->Task Management** page.

Backup

[Backup/Restore](#)

[Data Sync](#)

 Backup files must be .tar or .tgz, named with alphanumeric characters, dashes (-) and underscores (_).

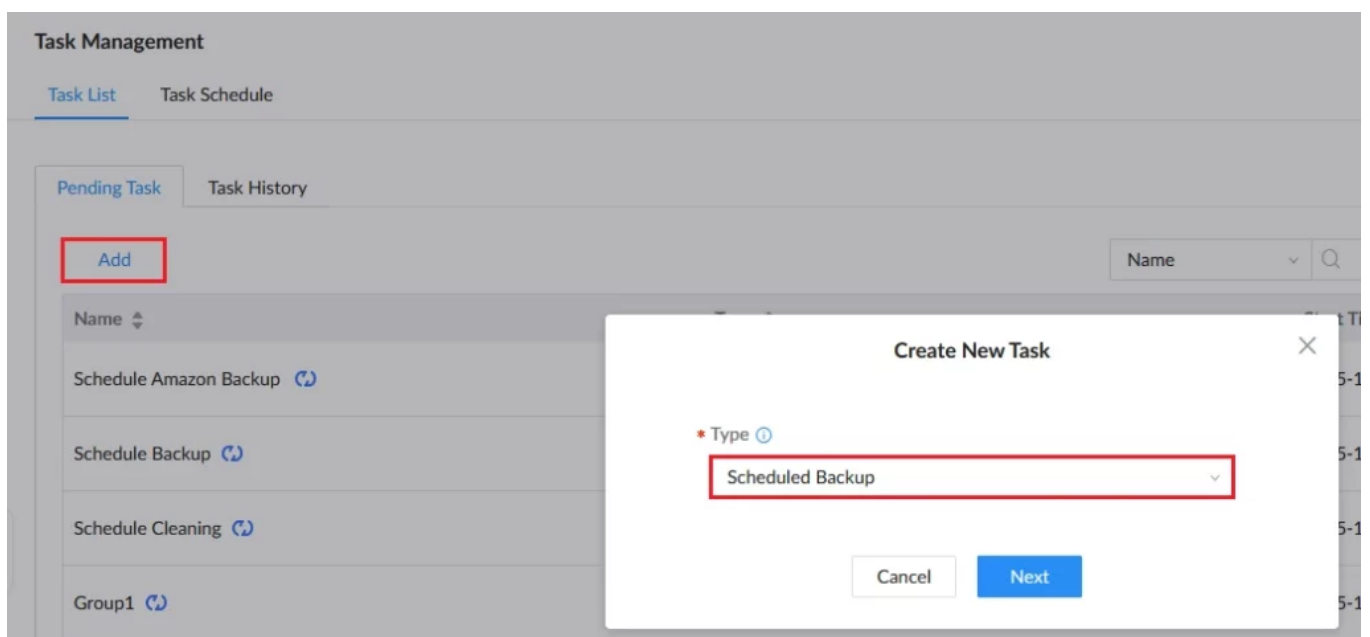
Backup

Schedule Backup

Upload

Scheduled Backup Task List

Delete



2. Check the Schedule Backup option checkbox to activate backup scheduling.
3. Enter a name for the task (should be between 2 and 64 characters. Names can include alphanumeric characters, Chinese characters, spaces, and the special characters _ and -).
4. Select the desired storage destination, such as USB, SD card, SFTP server, NAS, or Amazon S3. The same location can be used for multiple tasks as long as each task is scheduled at a different time.
5. Specify the date and time for the backup. Scheduled backup times must be at least one hour apart.

① Backups may take some time if backing up large amounts of data. It is recommended to use external storage devices such as SD cards, USB flash drives, etc. EXT4 is the recommended file system for external storage devices.

① SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

① Configuring multiple scheduled backups at the same time may affect performance. Try to set them during non working hours or set certain intervals for different backup tasks.

Schedule Backup



* Name ⓘ

Schedule Backup

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

* Choose Storage Location

* Date

2025-12-02



* Time

00:00

* Repeat

Choose Backup Files

☐ All ☐ Config File ☐ IM Message ☐ IM Files ☐ CDR Records ☐ Recording Files ☐ Fax Files ☐ Voicemail ☐ Voice Prompt Files
☐ Queue Statistics Report ☐ ZeroConfig Storage ☐ Meeting Report ☐ GDS Manager Data

① Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

The system does not allow two backup tasks to be scheduled at the same time. If users attempt to create overlapping tasks, the configuration will be blocked because simultaneous backups can affect system performance.

Task Management > Create New Schedule Backup



A backup task already exists at the selected time.

① Backups may take some time if backing up large amounts of data. It is recommended to use external storage devices such as SD cards, USB flash drives, etc. EXT4 is the recommended file system for external storage devices.

① SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

① Configuring multiple scheduled backups at the same time may affect performance. Try to set them during non working hours or set certain intervals for different backup tasks.

* Name ⓘ

Schedule Amazon Backup

2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

* Choose Storage Location

Amazon S3

Amazon S3

* Date

2025-12-02



* Time

18:00

* Repeat

Every Day

Choose Backup Files

☐ All ☒ Config File ☒ IM Message ☒ IM Files ☐ CDR Records ☐ Recording Files ☐ Fax Files ☐ Voicemail ☒ Voice Prompt Files
☐ Queue Statistics Report ☒ ZeroConfig Storage ☐ Meeting Report ☐ GDS Manager Data

① Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

6. Choose how often the backup should occur: Every Day, Weekly, Monthly, or Custom.
7. **Incremental Backup (Optional):** When a supported target storage device (USB, SD Card, or NAS) is selected, users can enable the Incremental Backup option. When enabled, the system automatically backs up data added or modified during the previous cycle (specifically CDR Records, Recording Files and Queue Statistics Reports) rather than creating a full system copy.
 - Example: For a monthly incremental backup task running on the 28th, the backup data range will cover from the 28th of the previous month (00:00:00) to the 27th of the current month (23:59:59). If a scheduled day (e.g., 29th, 30th, or 31st) does not exist in a given month, the task automatically executes on the last day of that month.

① SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

Schedule Backup ☒

• Name 2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

• Choose Storage Location

• Date

• Time

Incremental Backup ☒

• Repeat

Choose Backup Files

☐ All ☐ Config File ☐ IM Message ☐ IM Files ☒ CDR Records ☒ Recording Files ☐ Fax Files ☐ Voicemail ☐ Voice Prompt Files ☒ Queue Statistics Report ☐ ZeroConfig Storage

☐ Meeting Report

① Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

8. Choose which data to include in the backup. Options include: All, Config File, IM Message, IM Files, CDR Records, Recording Files, Fax Files, Voicemail, Voice Prompt Files, Queue Statistics Report, ZeroConfig Storage, Meeting Report, and GDS Manager Data.
9. Users can view both scheduled backup tasks and completed backup tasks in the **Maintenance->Task Management** page. Within this page, the **Task List** displays all the pending and completed tasks, while the **Task Schedule** shows the timing and recurrence of upcoming backups.

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

Enable Data Sync	Enable the auto data sync function. The default setting is "No".
Account	Enter the Account name on the SFTP backup server.
Password	Enter the Password associate with the Account on the SFTP backup server.
Server Address	Enter the SFTP server address.
Destination Directory	Specify the directory in SFTP server to keep the backup file. Format: 'xxx/xxx/xxx', If this directory does not exist, UCM will create this directory automatically.
Sync Time	Enter 0-23 to specify the backup hour of the day.

Before saving the configuration, users could click on

. The 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

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.

Backup

Backup/Restore Data Sync

Backup file must be in .tar format and less than 30MB in size. Filename supports alphanumeric characters, dashes (-), and underscores (_).

Backup

Schedule Backup

Upload

Local Backups

Delete

☐	NAME	DATE	SIZE	OPTIONS
No Data				

Backups in GDMS Cloud Storage

Delete

☐	NAME	DATE	SIZE	OPTIONS
☐	backup_2020717_124754.tar	2020-07-17 12:49:04	14.61MB	  

< 1 >

Total: 1 10 / page Goto 1

Restore UCM630xA from Backup File

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 30MB.

System Cleanup/Reset

Reset and Reboot

Users could perform reset and reboot under Web GUI→**Maintenance→System Cleanup/Reset→Reset and Reboot**.

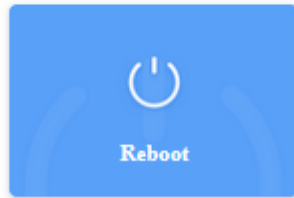
- To reboot the device, click on reboot icon.
- To factory reset the device, click on reset icon, then all the configurations and data will be reset to factory default.

System Cleanup/Reset

Reset & Reboot

Cleaner

USB Disk/SD Card File Management



Reset and Reboot

- User can also verify UCM certificate under the same path.

Cleaner

Users can configure the system to clean Call Detail Records (CDRs), voice recordings, voicemails, reports, chat data, meeting history, fax files, backup files, and other stored data either manually or automatically. The Cleaner feature is available under **Maintenance->System Cleanup/Reset->Cleaner**.

UCM provides the ability to manually clean a variety of data types, including CDRs, report data, chat messages and shared files, recording files, meeting history records, voicemails, fax files, and backup files.

The following screenshot illustrates the settings and parameters available for configuring the Manual Cleaning feature on UCM630xA.

AI Transcripts and Summaries are automatically or manually cleared according to their source:

- **AI Recording Transcripts:** Follow the Recordings cleanup rules.
- **Call & Meeting Transcripts:** Tied directly to CDR records and are cleared whenever CDR records are cleared.
- **Voicemail Transcriptions:** Follow the Voicemail cleanup rules.

System Cleanup/Reset

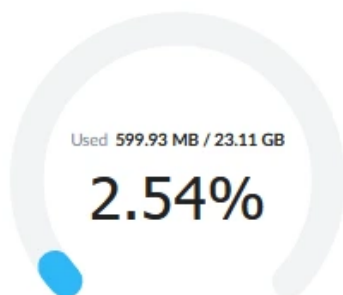
Reset & Reboot

Cleaner

Manual Cleaning

Automatic Cleaning

Storage Usage



- | | | | |
|---|--|--|--|
| ☐ All (2.54%) | ☐ Recordings (0.00%) | ☐ Fax Files (0.00%) | ☐ Voicemail (0.01%) |
| ☐ Music On Hold (0.01%) | ☐ Voice Prompts (0.07%) | ☐ CDR (0.01%) | ☐ Zero Config Files (0.46%) |
| ☐ Operation Log (0.01%) | ☐ Backups (0.07%) | ☐ Coredumps (0.00%) | ☐ Troubleshooting (0.01%) |
| ☐ Queue Statistics Reports (0.01%) | ☐ Meeting Reports (0.01%) | ☐ IM Files (0.21%) | ☐ IM Message (0.02%) |
| ☐ System Data (1.67%) | | | |

Clear Chat Data from Endpoint

Clear Chat Data from Endpoint ☐

Clean

Manual Cleaning Tab

Automatic cleanup is not enabled by default. When configured, automatic cleanup supports scheduled deletion of file data based on parameters such as cleanup time, cleanup conditions, and cleanup intervals.

Users can configure Automatic Cleaning by navigating to **Maintenance->System Cleanup/Reset->Cleaner->Automatic Cleaning**, or by creating an automated cleaning task under **Maintenance->Task Management**.

The following screenshot shows some available parameters for configuring automatic cleanup on UCM630xA.

System Cleanup/Reset
Reset & Reboot
Cleaner

Manual Cleaning
Automatic Cleaning

CDR Cleaner

Enable Cleaner
☒

* Clean Time
18:00

Cleaning Conditions
By Schedule

* Clean Interval (d)
1

Report Cleaner

Enable Cleaner
☒

* Data Type
☐ Queue Statistics Report
☐ Meeting Call Statistics Report
☒ Multimedia Meeting History

* Clean Time
06:00

Cleaning Conditions
By Schedule

* Clean Interval (d)
1

IM Data Cleaner

Enable Cleaner
☒

Clear Chat Data from Endpoint
☐

* Data Type
☒ IM Files
☐ IM Message

Automatic Cleaning Tab

The table below describes all the configurable options that can be configured for automatic cleaning:

CDR Cleaner	
Enable Cleaner	Enable the CDR Cleaner function.Note: All call and meeting transcript files are removed alongside cleared CDR records
Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated in the past 3 days.Keep Last X Records: If the max number of CDR has been reached, CDR will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval (d)	Enter 1-30 to specify the day of the month to clean up CDR when By Schedule is selected as Cleaning Conditions.
Max Entries	Set the maximum number of CDR entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
Report Cleaner	
Enable Cleaner	Enable scheduled queue log cleaning.
Data Type	Select a type of data to clean. Queue Statistics ReportMeeting Call Statistics ReportMeeting HistoryIVR Statistics Report
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.

Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.Keep Last X Records: If the max number of Queue Statistics Report entries has been reached, Queue Statistics Report entries will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.
Max Entries	Set the maximum number of Queue Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of Queue Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
IM Data Cleaner	
Enable Cleaner	Enable IM data cleaner
Clear Chat Data from Endpoint	This option allows users to clean endpoint chat data and is only available when the selected data type includes IM messages. It is disabled by default.
Data Type	Select a type of file to clean.IM Files IM Messages
Clean time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.Keep Last X Records: If the max number of Conference Call Statistics Report has been reached, Conference Call Statistics Report will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.
Max Entries	Set the maximum number of CDR Conference Call Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions.Default is 50000. Valid range: 10000 - 100000.
Keep Last X Days	Enter the number of days of Conference Call Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions.Default is 30. Valid range: 1 - 730.
File Cleaner	
Enable Cleaner	Enabling files cleaning.
Clean Files in External Device	If enabled the files in external device will be automatically cleaned up as configured.
Choose Cleaner File	Select the files for system automatic clean.Basic Call Recording FilesMeeting Recording FilesPaging/Intercom Recordings Queue Recording FilesVoicemail FilesEmergency RecordingsFax Backup Files SCA Recording FilesNote: The AI recording transcript files are deleted alongside their associated audio recording files.
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to delete all files.By Threshold: Check at the configured cleaning time every day to see if the storage threshold has been exceeded and perform cleaning of all files if it has.Keep Last X Days: Delete all files older than X days.
File Clean Interval	Enter 1-30 to specify the day of the month to clean up the files.
File Clean Threshold	Enter the internal storage disk usage threshold (in percent). Once this threshold is exceeded, the file cleanup will proceed as scheduled. Valid range is 0-99.

Keep Last X Days	Automatically delete all recordings older than this x days when the threshold is reached. If not set, all data is cleared. Valid range: 1 - 730.
Record History	
Name	Shows the identifier for the cleanup task.
Type	Specifies the category of cleanup the task performs
Task Status	Shows the final state of the cleanup task.
Start Time	The exact date and time when the cleanup task was triggered.
Repeat	Indicates the schedule for automatic repetition (if enabled).
Options	Provides the available actions for each task, such as Info and Delete. The Delete action removes the task from the record history, while the Info action displays details about the cleaned files.

When automatic cleaning tasks run, the system logs the cleaning results, allowing users to review each task results, including the total size cleaned and number of items removed, by checking either the **Cleaner** page or the **Task Management** sections (**Task History**).

Reset & Reboot

Cleaner

Clean Files in External Storage

Choose Cleaner Files

Basic Call Recordings

Meeting Video Recordings

Paging/Intercom Video Recordings

Voicemail Files

Fax

SCA Recordings

Record Meeting

Paging/Intercom Recordings

Queue Recordings

Emergency Recordings

Backup Files

Clean Time

16:00

Cleaning Conditions

By Schedule

File Clean Interval (d)

1

Record History

Name	Type	Task Status	Start Time	Repeat	Options
Schedule Cleaning	CDR	Cleaned	2025-12-03 18:00	Every Day 18:00	 
Schedule Cleaning	File	Cleaned	2025-12-03 16:00	Every Day 16:00	 
Schedule Cleaning	CDR	Cleaned	2025-12-02 18:00	Every Day 18:00	 
Schedule Cleaning	File	Cleaned	2025-12-02 16:00	Every Day 16:00	 

Checking Cleaning Records from the Cleaner Page

Task Management

Task List

Task Schedule

Pending Task

Task History

Clear

TypeScheduled Cleaner (File)Time2025-12-012025-12-04

Name	Type	Task Status	Start Time	Repeat	Options
Schedule Cleaning	File	Cleaned	2025-12-03 16:00	Every Day 16:00	 
Schedule Cleaning	File	Cleaned	2025-12-02 16:00	Every Day 16:00	 

Total 210 / pageGo

Checking Cleaning Records from Task History

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 Disk -- sda1

PBX_Queue_000B826704AF

PBX_SCA_000B826704AF

PBX_Emergency_000B826704AF

PBX_Conferences_000B826704AF

PBX_Recordings_000B826704AF

System Volume Information

No SD card

Delete

☐	NAME ↕	TYPE ↕	DATE ↕	SIZE ↕	OPTIONS
☐	Backup.tar	File	2019-11-05 17:06:46 UTC+02:00	18.68 MB	
☐	PBX_Queue_000B826704AF	Directory	2019-11-05 16:08:30 UTC+02:00	4.00 KB	
☐	PBX_SCA_000B826704AF	Directory	2019-11-05 16:08:30 UTC+02:00	4.00 KB	
☐	PBX_Emergency_000B826704AF	Directory	2019-11-05 16:08:30 UTC+02:00	4.00 KB	
☐	PBX_Conferences_000B826704AF	Directory	2019-11-05 16:08:30 UTC+02:00	4.00 KB	
☐	PBX_Recordings_000B826704AF	Directory	2019-11-05 16:08:30 UTC+02:00	4.00 KB	

USBSD Card Files Cleanup

USB/SD Card Files Cleanup

Current Path	Displays the current path.
Directory	Select the directory user want to clean.
Delete Selected File	Select multiple entries to delete from USB or SD card.

System Recovery

In some cases (for example after wrong upgrading procedure where the user doesn't follow the correct steps to perform an upgrade) the system may go into some hardware/software issues where the web UI access is lost as well as SSH, in this case the only solution would be to perform a full system recovery in order to reset or update the software version of the device in order to use it again.

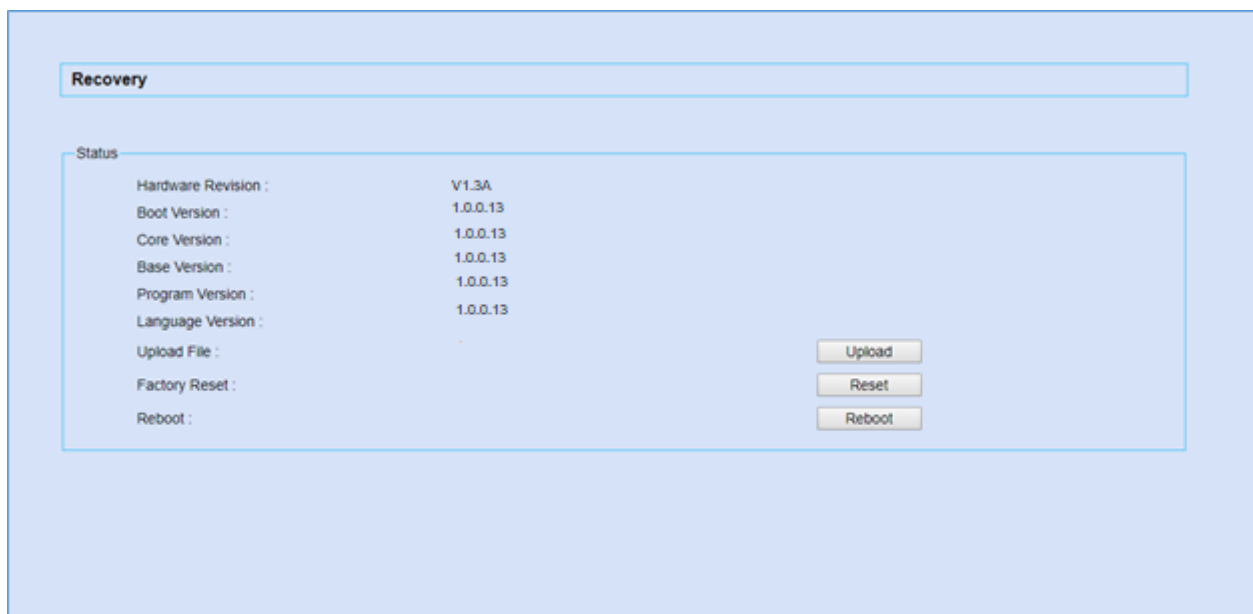
1. To access recovery mode on UCM, please follow below steps:
2. Remove the power from the unit and keep the network cable connected.
3. Press using a PIN the reset button and keep holding.
4. Plug back the power supply while maintaining the reset button pressed.
5. Wait for couple of seconds until you hear a click sound.
6. Release the reset button, and the system should display on the LCD a message "Recovery Mode" along with an IP address.

Once at this stage, the administrator can access the recovery mode web portal by typing in either the IP0 address (typically WAN) or IP1 address (typically LAN) into a browser address bar. The following page should appear:



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).

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.</p>

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	Ethernet Capture
Interface Type	LAN
Capture Filter	
Storage Location	Local
TLS Key	☐ Download
Start Download	

Output Result

The file has been deleted or does not exist.

S RTP Debugging

Enable S RTP Debugging	☐ Download
------------------------	--

Ethernet Capture

The capture packets can be stored locally and downloaded for analysis. However, if the user is diagnosing a randomly-occurring issue, he/she can run a continuous packet capture which can be limited by the size of the packet capture and the number of packet capture instances

When the maximum packet capture file size is reached, a new packet capture file will be created. When the maximum number of capture files number is reached, then the UCM will delete the oldest file created file and replace it with the new one.

Parameter	Description
Capture Type	Ethernet Capture: Gets a packet capture of all network traffic going through the device.WebSocket Capture: Gets a packet capture of WebSocket protocol. Mainly used for troubleshooting Wave Web calling and conferencing issues.
Interface Type	Select the network interface to monitor.
Capture Filter	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto...).
Storage Location	Local: Store the captured packets in the local storage. SFTP Server: Save the capture trace to a SFTP server. Please make sure that SFTP is correctly configured under PBX Settings -> Online Storage -> SFTP Server External Storage: Save the capture trace in a usb flash drive or an SD card. This requires that a USB flash drive or SD card to be plugged into the PBX. File formats supported are FAT32 and ExFat.

Save to External Storage	When or more external storage units are connected to the PBX, the user will be able to pick which one to use.? Note: This option is available only when you choose "External Storage" as the storage destination of the capture trace.
Destination Directory	When SFTP is selected, this option will appear. Please enter the directory path in which you would like to store the captured packets.
Packet Capture Size	This option appears only when "External Storage" or "SFTP" options are selected. Define the packet capture size, the option available are: 50MB, 100MB, and 200MB.
Number of Packet Capture	Define the maximum number of the packets captured. The available options are 5, 10, and 20 packets.
TLS Key	SSL/TLS packets can be decrypted through Wireshark. The packet capture must contain the TLS handshake process.
Start	Start capturing network traffic.
Stop	Stop capturing network traffic.
Download	Download the captured packets. This option can only be used when the captured packets are stored locally.
Enable SRTP Debugging	Check this box to troubleshoot calls encrypted with TLS/SRTP.

The output result is in .pcap format. Therefore, users could specify the capture filter as used in general network traffic capture tool (host, src, dst, net, protocol, port, port range) before starting to capture the trace.

Capture files saved on external devices will now have "capture" prepended to file names.

IP Ping

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.

Network Troubleshooting

Ethernet Capture
IP Ping
Traceroute
Record Meeting for Diagnosis

* Target Host:

 Start

Output Result

Dignostic run

PING 192.168.5.220 (192.168.5.220) 56(84) bytes of data.

64 bytes from 192.168.5.220: icmp_seq=1 ttl=128 time=0.780 ms

64 bytes from 192.168.5.220: icmp_seq=2 ttl=128 time=0.995 ms

Done

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.

Network Troubleshooting

Ethernet CaptureIP PingTracerouteRecord Meeting for Diagnosis

* Target Host:

192.168.5.220

▶ Start

Output Result

Dignostic run

traceroute to 192.168.5.220 (192.168.5.220), 30 hops max, 46 byte packets

1 *

Done

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.

Network Troubleshooting

Ethernet CaptureIP PingTracerouteRecord Meeting for Diagnosis

* Target Meeting:

▶ Start

Download

Delete

Output Result

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.

Signaling Troubleshooting

☒ Analog Record Trace ☐ Key dial-up FXO

* Record Ports:

FXO Ports: ☐ All ☒ 1 ☐ 2

FXS Ports: ☐ All ☐ 1 ☐ 2

☐ Stop

☐ Download

☐ Delete

Output Result

Capturing...

Troubleshooting Analog Trunks

- A key Dial-up FXO

Users can directly set a PSTN number on the "**External Extension**" text box to troubleshoot issues related to the analog trunk easily, the following steps shows how to use this feature:

1. Configure analog trunk on UCM, including outbound route.
2. Enter a reachable external number in "**External Extension**".
3. Press "**Start**" button. The call will be initiated to the external number.
4. Answer and finish the call before pressing "Stop" button.

The trace will be available for analysis to download after output result shows "Done! Click on Download to download the captured packets".

Signaling Troubleshooting

☐ Analog Record Trace ☒ Key dial-up FXO

* External Number :

99235467

■ Stop

⬇ Download

🗑 Delete

Output Result

Capturing...

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

Enable Server Check :

☒

* Check Cycle :

60

* Check times :

3

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.

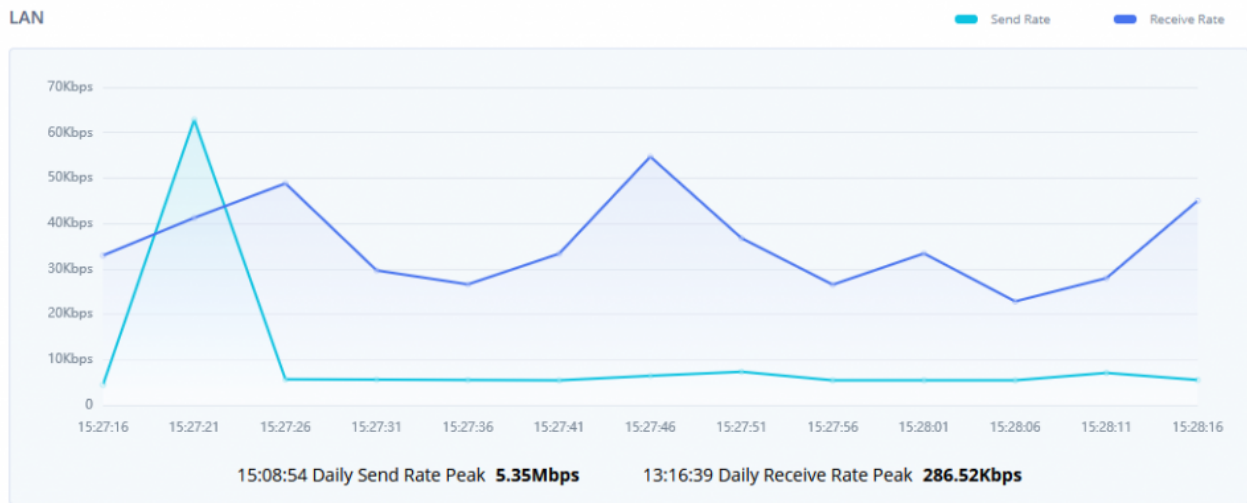
Network Status

Network Port Real-time Traffic

Active Connections

Active Unix Domain Sockets

LAN



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

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 1.0.35.8

- **Call Flow Design**
 - Added Visual Call Flow Design (Call Flow Design) to build complex call routing using drag-and-drop components. [[Call Flow Design](#)]
- **WhatsApp Trunk**
 - Added support for WhatsApp SIP Trunk integration and Wave WhatsApp calling support. [[WhatsApp Trunk](#)]
- **AI Features**
 - Added AI Translation feature for real-time translation of call/meeting transcripts and chat messages. [[AI Translation](#)]
 - Added AI Voice Assistant (Beta) support for controlling endpoints via voice commands. [[AI Voice Assistant](#)]
 - Added option to allow meeting summaries to be shared with all participants. [[Schedule Meeting](#)]
 - Added AI Recordings Transcription and Summary support for audio recording files. [[AI Recording Transcription and Summary](#)]
 - Added interactive synchronization between recording playback progress and AI transcript text. [[AI Recording Transcription and Summary](#)]
 - Added automated and manual cleanup options as well as backup and restore support for AI transcript files. [[Cleaner](#)][[Backup/Restore](#)]
 - Added feature code to start or stop AI call transcription during an active call. [[Feature Codes](#)]
 - Added User Portal support for playing and accessing AI transcriptions of voicemails. [[AI Voicemail to Text](#)]
- **Collaborative Office Integration**

- Added support for automatically syncing CDR CSV files to Google Docs via Google Workspace integration. [[Google User](#)][[CDR Automatic Download](#)]
- Added support for SAML SSO authentication. [[SAML SSO](#)]
- Added Google Workspace Calendar integration to dynamically map user calendar events to extension status. [[Google Calendar](#)]
- **Messaging**
 - Added support for Voxtelesys SMS provider integration. [[SMS Configuration](#)]
 - Added support for VoiceMeUp SMS provider integration. [[SMS Configuration](#)]
 - Added Smart Call SMS Link Service to trigger automatic SMS messages with links via IVR key presses. [[SMS Template](#)]
 - Added Message Edit/Delete Period option to the IM settings page. [[IM Settings](#)]
- **Call Queue**
 - Added Wallboard feature to display real-time call queue metrics and agent status. [[Queue Board](#)]
 - Added Queue Panel for interactive call management, agent status changes, and real-time monitoring. [[Queue Operation Panel](#)]
 - Added dedicated Queue Permissions configuration to restrict control operations for chairmen and agents. [[Queue Permissions](#)]
 - Added Queue CDR management with support for viewing, calling back, and tracking missed call processing status. [[Queue Permissions](#)]
 - Added Priority Queue feature to dynamically assign call weights and route high-priority calls first. [[Call Queue](#)]
 - Added time-based condition routing for call queues during out-of-office hours or holidays. [[Call Queue](#)]
 - Optimized virtual queue timeout triggering logic and updated user interface. [[Call Queue](#)]
 - Added "Skip Busy Agents" option to allow or prevent ringing call queue agents who are currently in a call. [[Call Queue](#)]
 - Removed Queue Switchboard to be replaced with Queue Operation Panel. [[Queue Operation Panel](#)]
 - Added custom user permissions for Queue Wallboard and Queue Operation Panel. [[Add Custom Privilege](#)]
- **PMS**
 - Added Local PMS unique order ID generation for reservation tracking across lists and invoices. [[Local PMS](#)]
 - Added Local PMS read-only historical reservation views to prevent accidental data changes. [[Local PMS](#)]
 - Added Local PMS overdue reservation filtering to identify guests who failed to check in on time. [[Local PMS](#)]
 - Added global Local PMS reservation time settings to configure default daily check-in/check-out times and set allowed thresholds for earliest check-in and latest check-out. [[Local PMS](#)]
 - Updated Local PMS multi-room reservations to preserve checked-in room rates when reservation prices are modified. [[Local PMS](#)]
 - Added a dedicated refresh button to the Local PMS Room Availability Calendar for real-time updates. [

[Local PMS](#)

- Added tax-inclusive rate displays for active bookings on the Local PMS Room Availability Calendar. [[Local PMS](#)]
- Added Local PMS hour-room management rules restricting room changes after check-in. [[Local PMS](#)]
- Added mandatory base price requirement when enabling Local PMS hourly rental option. [[Local PMS](#)]
- Added customizable hotel branding logo, phone numbers, and websites to Local PMS bill printing. [[Local PMS](#)]
- Added Local PMS auto-assign room button for automated room selection during reservation creation. [[Local PMS](#)]
- Added itemized tax, room charge, and minibar breakdowns to Local PMS bill printing. [[Local PMS](#)]
- Added Local PMS support for custom hotel branding (logo, phone number, website, and QR code) in self-check-in and self-check-out emails. [[Local PMS](#)]
- Added custom permission controls for PMS Basic Settings and Minibar management. [[Add Custom Privilege](#)]
- **Zero Config**
 - Added support for batch local firmware upgrades via Zero Config. [[Firmware](#)]
 - Added Zero Config support for Avaya IP phones. [[Zero Config Supported Devices](#)]
 - Added Zero Config multi-account configuration support for Poly Edge B Series IP phones. [[Zero Config Supported Devices](#)]
 - Added Zero Config support for Grandstream HT and GXW gateways. [[Zero Config Supported Devices](#)]
 - Added support for Cisco phone DND and Conference features. [[Zero Config Supported Devices](#)]
 - Added support for Cisco CP-6921 and CP-3905 IP phones. [[Zero Config Supported Devices](#)]
- **CRM**
 - Added Custom CRM Integration interface, custom templates, OAuth2/Bearer Token options, and import/export capabilities. [[CRM](#)]
- **VoIP Trunk**
 - Added option to select whether to use DOD numbers when "Keep Original CID" is enabled on SIP trunks. [[VoIP Trunks](#)]
 - Added "Not Passthrough" option and refined configuration for Diversion headers on SIP trunks. [[VoIP Trunks](#)]
- **Inbound Routes**
 - Added support for custom Inbound Mode names and audio prompts for mode switching. [[Inbound Route: Multiple Mode](#)]
- **Outbound Routes**
 - Added Diversion ID Manipulation settings (strip and prepend) for outbound routes. [[Configuring Outbound Routes](#)]
- **User Management**

- Added global configuration option to restrict users from modifying their extension email addresses. [[User Portal/Wave Privileges](#)]
- Added Multi-Factor Authentication (MFA) login support for User Portal. [[Create New SIP Extension](#)]
- **Upgrade**
- Added interactive feature highlights guide on new system updates for administrators. [[New Feature Guide](#)]
- **Backup**
- Added support for incremental backup tasks for CDR, queue statistics, and recording files. [[Backup/Restore](#)]
- **Storage Device Management**
- Added support for SMB 3.0 protocol for network disk storage. [[NAS](#)]
- **System Cleanup/Reset**
- Increased maximum automatic cleanup retention period to 730 days. [[Cleaner](#)]
- **System Events**
- Added alert notifications when outbound call duration thresholds are exceeded on outbound routes. [[Alert Events List](#)]
- **Voicemail**
- Optimized voicemail audio encoding format terminology in the web interface. [[Configure Voicemail](#)]
- **Fax/T.38**
- Added support for configuring a unified administrator email address for failed Email-to-Fax notifications. [[Email Settings](#)]
- **Meeting**
- Added support for including UCM Station IDs in random meeting room numbers for cross-PBX routing. [[General Settings](#)][[Meeting Settings](#)]
- **CDR**
- Added Call Notes and Labels feature for tagging and adding comments to call records. [[CDR](#)][[Call Note](#)]
- **IVR**

- Added support for configurable IVR end keys (including #). [[Key Pressing Events](#)]
- **Emergency Calls**
 - Added option to configure whether Geolocation-Routing headers are included in emergency call location mapping. [[Emergency Location Mapping](#)]
- **Voicemail**
 - Added support for feature code *99 to record and modify Voicemail Group prompts. [[Feature Codes](#)][[Configure Voicemail Group](#)]
- **Announcement**
 - Added call permission configuration for Announcements when the destination is set to an external number. [[Announcement](#)]
- **Time Settings**
 - Added custom prompt support for holiday events in Time Settings. [[Holiday](#)]
- **SIP Settings**
 - Added option to enable blind transfers while the callee's phone is still ringing. [[Misc](#)]
- **WebRTC Trunk**
 - Added WebRTC Trunk one-click dialing mode and script-based integration code. [[WebRTC Trunks](#)]
- **Dashboard**
 - Added Storage Health display to dashboard. [[PBX Status](#)]
- **RemoteConnect**
 - Retired Click2Call option while preserving existing configurations for legacy setups. [[Integrated Customer Service](#)]
- **PBX Settings**
 - Moved Enterprise Contact Number field to PBX Settings->General Settings. [[General Settings](#)]

Firmware Version 1.0.33.42

- Added support for call queue reports. [[Call Queue Reports](#)]
- Added support for scheduling call queue reports. [[Scheduled Report](#)]

Firmware Version 1.0.33.32

- No major changes.

Firmware Version 1.0.33.30

- Added AI configuration tab to SIP extensions, allowing per-extension control of Automatic AI Transcription. [[Create a New SIP Extension](#)]
- Added scheduled meeting configuration with AI transcription option, allowing organizers to enable or disable AI transcription per meeting. [[Schedule Meeting](#)]
- Added AI Settings (Beta) page to centrally manage AI services. [[AI Settings \(Beta\)](#)]
- Added RemoteConnect AI Services page to display AI service status, plan validity, and detailed usage statistics [[AI Services](#)]
- Added support for AI Call Transcription & Summary. [[AI Call Transcription and Summary](#)]
- Added support for AI Conference Transcription & Summary. [[AI Meeting Transcription and Summary](#)]
- Added support for AI Voice Message to Text. [[AI Voice Message to Text](#)]
- Added AI Generated Speech (TTS) feature for creating voice prompts directly from text. [AI Generated Speech]

Firmware Version 1.0.33.22

- No major changes.

Firmware Version 1.0.33.21 (BETA Only)

- Added several new call report types for various call scenarios [[Call Reports](#)]
- Added support for Cisco CP69xx/78xx/88xx endpoints DND. [[Extensions](#)]

Firmware Version 1.0.33.7 (BETA Only)

- Added Strict Defend Mode option to Geo-IP Access Control [[Geo-IP Access Control](#)]
- Added unified Integration tab for collaboration and identity platforms. [[Integration of Collaboration Platforms](#)]
- Added support for Google Workspace integration to synchronize user identity information between Google Workspace and the UCM Series. [[Google Workspace Integration](#)]
- Added Google Workspace Single Sign-On (SSO) support for UCM web interface authentication. [[Google Workspace Integration](#)]
- Added support for configuring Microsoft Entra ID user synchronization scope. [[Microsoft Entra ID \(Azure AD\)](#)]
- Added support for configuring holidays by date or by week. [[Holiday](#)]
- Increased the maximum size limit for backup files uploaded to the UCM via the Web GUI. [[Restore Configuration from Backup File](#)]
- Added Zero Config support for Yealink IP phones. [[Zero Config Supported Devices](#)]
- Updated the Local PMS wake-up service prompt to dynamically use the language configured during room check-in. [[Local PMS](#)]
- Optimized Local PMS check-in and check-out actions to take effect immediately without requiring "Apply Changes". [[Local PMS](#)]
- Added option to control Wave app Screenshot and Screen Recording permission. [[Wave Permissions](#)]
- Added support for configuring whether the Wave external host address is automatically synchronized from UCMRC. [[Plan Settings](#)][[HTTP Server](#)]
- Added support for Bitrix24 CRM integration. [[Bitrix24 CRM](#)]
- Added support for network abnormality HA switchover. [[HA Settings](#)]

Firmware Version 1.0.31.7

- Added support for third-party SQL database integration for phonebook lookup and synchronization. [[3rd Party Database Integration](#)]
- Updated the Inbound Routes->3rd Party Database Search page to align with the new third-party SQL database integration feature. [[Inbound Routes: 3rd Party Database Search](#)]

- Added support for enabling local HA while operating in Dual network mode. [[HA Settings](#)]
- Added third-party SIP Phone support (Cisco/Poly). [[Zero Config Supported Devices](#)]
- Added vendor and model search capability when downloading model templates. [[Model Update](#)]
- Increased maximum Zero Config firmware upload size to support larger GXV series firmware packages. [[Firmware](#)]
- Added configurable room types with support for day-based pricing, holiday pricing, tax rates, and hourly pricing. [[Local PMS](#)]
- Added reservation management. [[Local PMS](#)]
- Added a guest list for centralized customer profile management, including search, import/export. [[Local PMS](#)]
- Added email templates for reservation notifications, cancellation notices, and billing emails. [[Email Template](#)]
- Added multiple check-in workflows, supporting check-in from reservation list, from room list (immediate check-in), and hourly or full-day room selection. [[Local PMS](#)]
- Added room change (house switch) functionality to move checked-in guests to another available room while preserving guest and billing data. [[Local PMS](#)]
- Added a room availability calendar with visual status indicators, booking and check-in actions, hover-based detail display. [[Local PMS](#)]
- Added bill printing with detailed room charges, minibar costs, call charges, tax breakdowns, and prepayment deductions. [[Local PMS](#)]
- Added wake-up service management with support for room group based scheduling. [[Local PMS](#)]
- Added support for self-service check-in and check-out via email for guests with valid reservations. [[Local PMS](#)]
- Added configurable email delivery timing for self-service check-in and check-out messages relative to arrival and departure times. [[Local PMS](#)]
- Added tracking of check-in and check-out methods, distinguishing between front-desk and self-service operations in history records. [[Local PMS](#)]
- Added automatic room assignment during self-service check-in when reservations are not pre-assigned to specific rooms. [[Local PMS](#)]
- Added support for DOD numbers batch deletion. [[Direct Outward Dialing \(DOD\)](#)][[Outbound Routes DOD](#)]
- Added support for inbound and outbound routes batch deletion. [[Configuring Inbound Routes](#)][[Configuring Outbound Routes](#)]
- Added outbound route total call duration limit setting. [[Configuring Outbound Routes](#)]
- Added display of trunk status and current call count display on the VoIP Trunk page [[VoIP Trunks](#)]
- Added Caller ID Transform feature on outbound routes [[Configuring Outbound Routes](#)]
- Added support for data backup and archiving to third-party cloud storage (Amazon S3). [[Amazon S3](#)]
- Add the ability to play/hear the uploaded Prompts directly from the WebGUI. [[Custom Prompt](#)]
- Added support for manual addition of Fail2Ban blocklist entries. [[Fail2Ban](#)]
- Added Cleaner Record and Details [[Cleaner](#)]
- Added the ability to have multiple Scheduled Backup tasks on different storage locations. [[Scheduled Backup](#)][[Backup/Restore](#)]
- Added ability to modify LDAP phonebooks through API. [[API Queries Supported](#)]
- Added support for adding LDAP contacts as members of paging/intercom groups to 2-way intercom and 1 way paging. [[LDAP Members](#)]
- Added support for proficiency-based routing as a routing strategy in the call queue. [[Proficiency Routing](#)]
- Added selecting the dynamic agents which can be added to a specific call queue. [[Dynamic Agents](#)]
- Added recording file and CDR access permission. [[View Team CDRs and Recordings](#)]

- Added Wave recording indicator appearance permission. [[Recording Status](#)]
- Added support for configuring the pre-installed Wave add-ins. [Pre-installed Plugins]
- Added support for multifactor authentication using email for Wave. [[Multifactor Authentication](#)]

Firmware Version 1.0.29.21

- Some general call failure prompt tones (e.g., no-answer, user-busy, no-permission, wrong-number, general-failed) can now be used for SIP trunk call failure messages. [[SIP Trunk Prompt Tone](#)]

Firmware Version 1.0.29.11

- Added Least Cost Routing policy to Outbound Routes [Carrier]
- Added support for call billing [[Call Rate](#)]
- The administrator can choose to prioritize call pattern matching or outbound route priority order as the criteria for call routing [[Outgoing Routing Priority](#)]
- Added a configuration field to enter maximum concurrent calls allowed by a SIP trunk. [[VoIP Trunk Configuration](#)]
- Added ability to select the error message to display when the number of maximum current calls is achieved. [[VoIP Trunk Configuration](#)]
- Added support for enabling/disabling sending the diversion header on a particular trunk. [[VoIP Trunk Configuration](#)]
- Added support for Microsoft Entra ID integration, this allows synchronizing SIP accounts from LDAP or Active Directory for single sign-on. There is potential synchronization of additional information other than authentication information. [[Microsoft Entra ID \(Azure AD\)](#)]
- Added support for Active Directory to synchronize SIP accounts (user portal and Wave login only) and admin accounts. [[Windows AD](#)]
- Strong password requirements have changed, now administrator password and user portal password requires at least 10 characters, with at least one upper letter and one lower letter, one number, and one special character.
- Added support for detecting new firmware directly from the web UI, regular firmware version checking can be scheduled on the webUI. [[Upgrade](#)]
- Added country-specific restriction in ACL [Country/Region IP Defense]
- Added support for automatic update of the timezone list [[Automatic Date and Time](#)]
- Now some of the services can have their ports modified, while this was not possible before []
- Added a link to the Open Source Software License Agreement
- Administrator password, user password, and SIP password now require at least 10 characters [[Create New SIP Extension](#)][[User Management](#)]
- Added TLS compression for LDAP server [[LDAP Server Configurations](#)]
- Backup allows now excluding instant messages [[Backup](#)]
- The dashboard now displays the physical port name [[PBX Status](#)]
- Added Call Policy [[Create New SIP Extension](#)]
- Added name configuration in Speed Dial [[Speed Dial](#)]
- Added "First Answer Termination" in Paging configuration [[Paging/Intercom Groups](#)]
- Added Call Privilege to Announcement Center [[Announcement Center](#)]
- Increased voicemail group members number to 150
- CDR now displays the name of the callee
- Added prompt language configuration in Call Queue [[Add Call Queue](#)]
- Call Queue Chairman can now view the CDR
- Queue Chairman codes can now be configured

- Added option to disable RPID in the Call Queue
- ELIN field in Emergency calls now can be configured with more character, letters and numbers [[Emergency Location Mapping](#)]
- Add the ability to support Emergency Location Mapping based on a single Extension approach for the Emergency calls feature [[Emergency Location Mapping](#)]
- Added default emergency callID field for Extension's autopopulate [[Emergency Location Mapping](#)]
- Added ability to customize PAI for Emergency Calls in multi-site environment [[Emergency Location Mapping](#)]
- Added Oracle Hospitality OPERA PMS integration [PMS]
- PMS parameters have been added to list of privileges for admins [[Custom Privilege](#)]
- Added ability to use key pressing events when receiving a wake up call. [Wakeup Service]
- Improved "Move" function in PMS, now more information are transferred along with the guest
- Added support for configuring the allowed API modules when adding a user [[API Configuration Parameters](#)]
- The administrator can now configure up to 10 subnets on Zero Config whitelist [[Zero Config Settings](#)]
- Administrator can now use MAC OUI to filter search results when searching for devices on Zero Config [[Discovery](#)]
- Updated email template for "new messages to inactive user notification" [[Email Template](#)]
- Added "Delete message" Wave permission. [[User Portal/Wave Privileges](#)]
- Added "Allow Simultaneous Logins from the Same Client Type" Wave permission [[User Portal/Wave Privileges](#)]
- Added "Play Joining/Leaving Meeting Announcement" which enables/disables the sound played when a user joins/leave [Schedule Meeting]
- Add permission for the meeting host to play, delete, and download meeting recordings
- Added end time for scheduled meetings [[Schedule Meeting](#)]
- Meeting will now end when a GDS or GSC extensions are the only ones left in the meeting
- Added event alert in case synchronizing files to cloud storage fails [[Alert Events List](#)]
- GDMS cloud storage security key can now be obtained [[GDMS Cloud Storage Space](#)]
- Added compatibility for GDMS configuration template for the UCM6300 Series
- Import and export functions now support ".xlsx" files.
- Backup packages now use .tgz format by default instead of .tar
- Added support for triggering webhooks via an IVR [Configure IVR]
- Added Background Sound to Multicast Community [[Multicast Community](#)]
- Added Linked ID to CDR AMI event reporting for improved call tracking and management
- Added Premium Code and and Premium Code Prompt option to Advanced Settings page. The user can use the premium code to increase their priority in the queue. [[Add Call Queue](#)]

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 Meetings page and moved several meeting-related options to it. [[Meeting](#)]
- Regular meeting participants can now invite other members to join the meeting by dialing 1 if "Allow User

Invite" is enabled. [\[Meeting\]](#)

- 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. [\[Meeting\]](#)
- 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.