

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 TableAPI for integration with third-party platforms. By offering a high-end unified communications and collaboration solution packed with a suite of mobility, security, meeting and collaboration tools, the UCM6300A series provides a powerful platform for any organization.

Alert

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

Caution

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

Note

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

PRODUCT OVERVIEW

Technical Specifications

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

| Interfaces | |
|----------------------------|---|
| Analog Telephone FXS Ports | <ul style="list-style-type: none">● UCM6300A: 0 port● UCM6302A: 2 ports with lifeline support● UCM6304A: 4 ports with lifeline support● UCM6308A: 8 ports with lifeline support Each port supports 3 REN |
| PSTN Line FXO Ports | <ul style="list-style-type: none">● UCM6300A: 0 port● UCM6302A: 2 ports● UCM6304A: 4 ports● UCM6308A: 8 ports |

| | |
|--|--|
| | All ports have lifeline capability in case of power outage |
| Network Interfaces | Three self-adaptive Gigabit ports (switched, routed or dual card mode) with PoE+ |
| NAT Router | Yes (supports router mode and switch mode) |
| Peripheral Ports | <ul style="list-style-type: none"> ● UCM6300A: USB 3.0, and SD card interface ● UCM6302A: USB 2.0, USB 3.0, and SD card interface ● UCM6304A/6308A: 2x USB 3.0 and SD card interface |
| LED Indicators | <ul style="list-style-type: none"> ● UCM6300A/6302A/UCM6304A: None ● UCM6308A: Power 1/2, FXS, FXO, LAN, WAN, Heartbeat |
| LCD Display | <ul style="list-style-type: none"> ● 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 | <ul style="list-style-type: none"> - 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 | |
| DTMF Methods | Inband, RFC4733, and SIP INFO |
| Provisioning Protocol and Plug-and-Play | Mass provisioning using AES encrypted XML configuration file, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66 multicast SIP SUBSCRIBE mDNS), eventlist between local and remote trunk |
| Network Protocols | TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay (pending), IPv6, OpenVPN® |
| API | Full API available for third-party platform and application integration. |
| Disconnect Methods | Busy/Congestion/Howl Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect |
| Security | |

| | |
|------------------------------------|---|
| Media Encryption | SRTP, TLS1.2, HTTPS, SSH, 802.1x |
| Physical | |
| Universal Power Supply | <ul style="list-style-type: none"> ● UCM6300A/6302A/6304A: Input: 100 ~ 240VAC, 50/60Hz; Output: DC+12V, 1.5A ● UCM6308A: 2x DC 12V Power Jack Input: 100~240VAC,50/60Hz; Output: DC+12V, 2A |
| Dimensions | <ul style="list-style-type: none"> ● UCM6300A/6302A/6304A: 270mm(L) x 175mm(W) x 36mm(H) ● UCM6308A: 485mm(L) x 187.2mm(W) x 46.2mm(H) |
| Environmental | <ul style="list-style-type: none"> ● Operating: 32 - 113°F / 0 ~ 45°C, Humidity 10 - 90% (non-condensing) ● Storage: 14 - 140°F / -10 ~ 60°C, Humidity 10 - 90% (non-condensing) |
| Mounting | <ul style="list-style-type: none"> ● Wall mount (Unit will be fixed on the wall using screw) & Desktop for UCM6300A/6302A/6304A. ● Desktop & Rack mount for UCM6308A. |
| Weight | <ul style="list-style-type: none"> ● UCM6300A: Unit weight 705g, Package weight 1200g ● UCM6302A: Unit weight 725g, Package weight 1221g ● UCM6304A: Unit weight 775g, Package weight 1271g ● UCM6308A: Unit weight 2540g, Package weight 3465g |
| Additional Features | |
| Multi-language Support | <ul style="list-style-type: none"> ● Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech, Turkish ● Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Dutch, Polish, Portuguese, Russian, Swedish, Turkish, Hebrew, Arabic, Dutch ● 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: |

| | |
|---|---|
| | <ul style="list-style-type: none"> • Users: 250 • Concurrent calls (G.711): 50 • Max concurrent SRTP calls: 50 <p>UCM6302A:</p> <ul style="list-style-type: none"> • Users: 500 • Concurrent calls (G.711): 75 • Max concurrent SRTP calls: 75 <p>UCM6304A:</p> <ul style="list-style-type: none"> • Users: 1000 • Concurrent calls (G.711): 150 • Max concurrent SRTP calls: 120 <p>UCM6308A:</p> <ul style="list-style-type: none"> • Users: 1500 • Concurrent calls (G.711): 200 • Max concurrent SRTP calls: 150 |
| Maximum Attendees of Meeting Bridges | <ul style="list-style-type: none"> • 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 |
| Call Features | Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice meeting, eventlist, feature codes, busy camp-on/call completion, voice control |
| Wave Mobile App | Allows Android & iOS users to join UCM-hosted meetings & communicate with other users/solutions registered to the UCM630xA |
| Firmware Upgrade | Supported by Grandstream Device Management System (GDMS), a zero-touch cloud provisioning and management system, It provides a centralized interface to provision, manage, monitor, and troubleshoot Grandstream products |
| Compliance | <ul style="list-style-type: none"> • FCC: Part 15 (CFR 47) Class B, Part 68 • CE: EN 55032, EN 55035, EN61000-3-2, EN61000-3-3, EN 62368.1, ES 203 021, ITU K.21 • IC: ICES-003, CS-03 Part I Issue 9 • RCM: AS/NZS CISPR 32, AS/NZS 62368.1, AS/CA S002, AS/CA S003.1/2 • Power adapter: UL 60950-1 or UL 62368-1 |

Table 1: Technical Specifications

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 |

Table 2: UCM630xA Equipment Packaging

UCM6300A front and back view

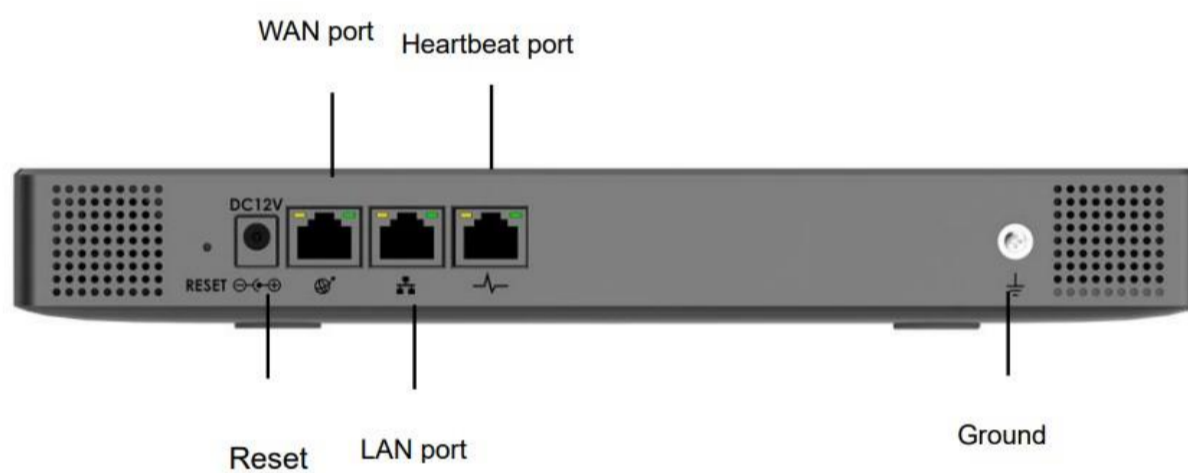


Figure 1: UCM6300A Back View



Figure 2: UCM6300A Front View

UCM6302A front and back view

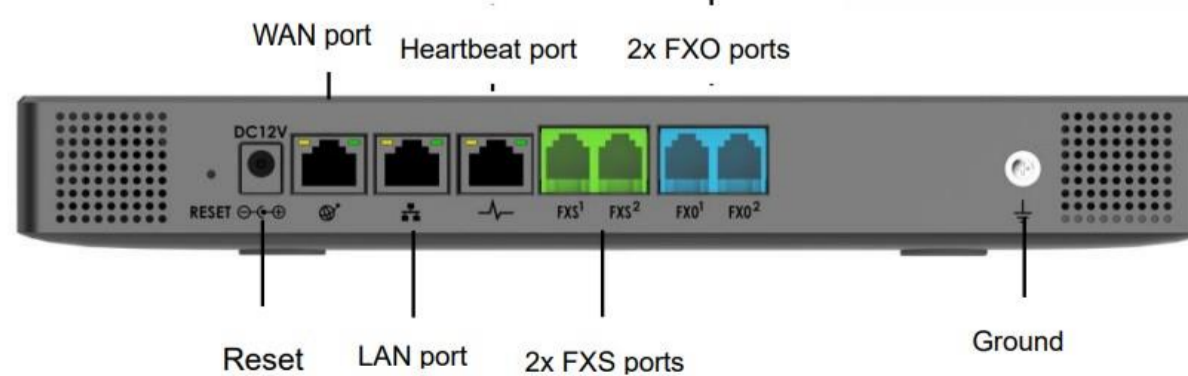


Figure 3: UCM6302A Back View



Figure 4: UCM6302A Front View

UCM6304A front and back view

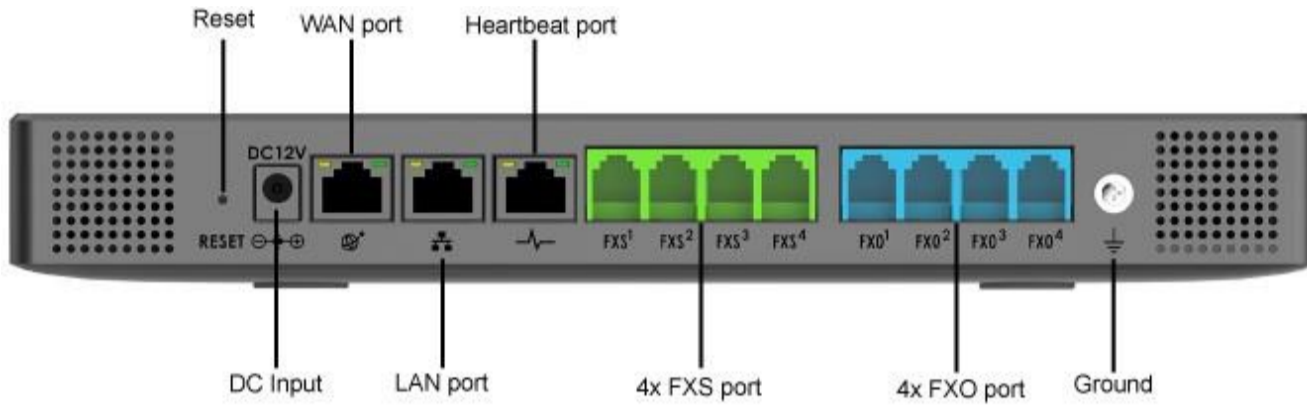


Figure 5: UCM6304A Front View



Figure 6: UCM6304A Back View

UCM6308A front and back view

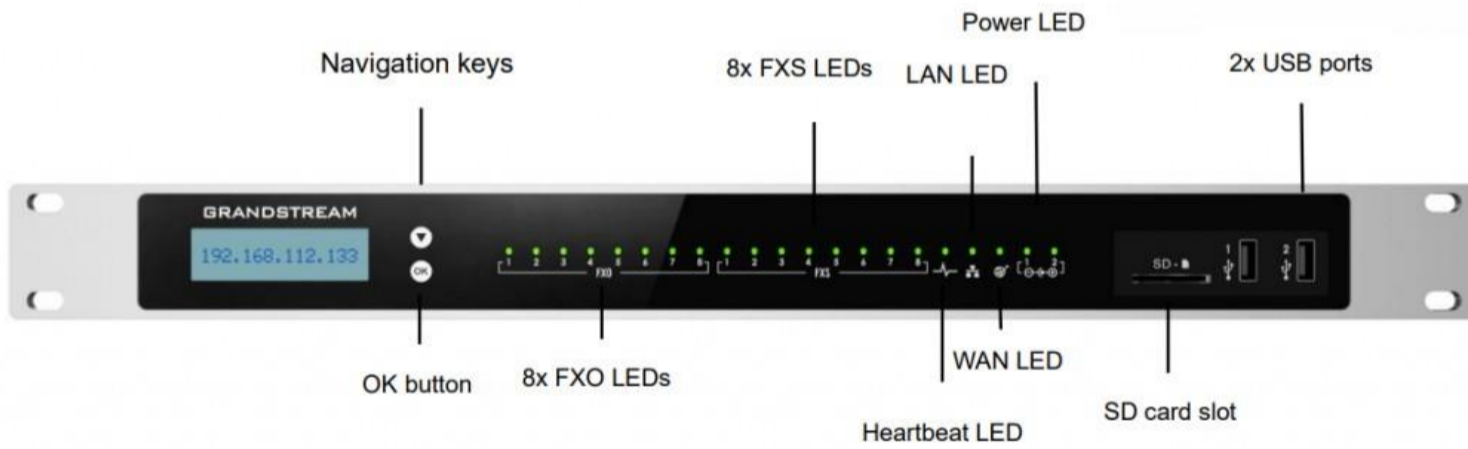


Figure 7: UCM6308A Front View

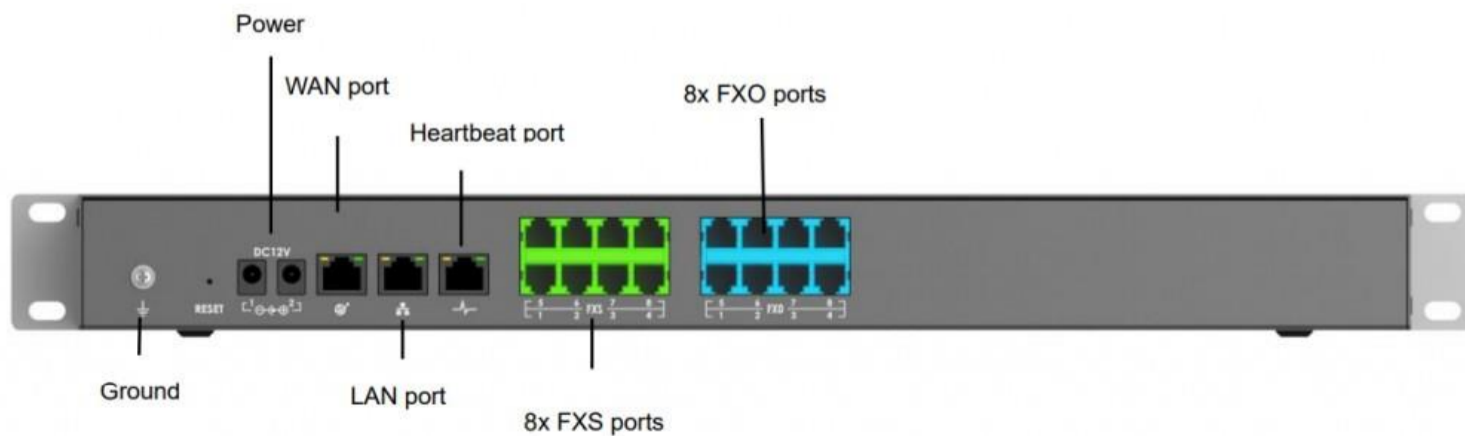


Figure 8: UCM6308A Back View

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.

i Warranty

If the UCM630xA series IP PBX was purchased from a reseller, please contact the company where the device was purchased for replacement, repair, or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.

! Warning

Use the power adapter provided with the UCM630xA series IP PBX. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.

GETTING STARTED

To get started with the UCM630xA setup process, use the following available interfaces: LCD display, and web portal.

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

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

Use the LCD Menu

◦ **Idle Screen**

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

◦ **Menu**

Pressing the Home button will show the main menu. All available menu options are found in *[Table 3: 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 | <ul style="list-style-type: none"> ◦ Critical Events ◦ Other Events |
| Device Info | <ul style="list-style-type: none"> ◦ 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 | <ul style="list-style-type: none"> ◦ WAN Mode: DHCP, Static IP, or PPPoE ◦ WAN IP: IP address ◦ WAN Subnet Mask ◦ LAN IP: IP address ◦ LAN Subnet Mask |
| Network Menu | <ul style="list-style-type: none"> ◦ WAN Mode: Select WAN mode as DHCP, Static IP or PPPoE ◦ Static Route Reset: Select this to reset static route settings. |

| | |
|----------------------------|--|
| <p>Factory Menu</p> | <ul style="list-style-type: none"> ◦ Reboot ◦ Factory Reset ◦ LCD Test Patterns <p>Press DOWN and OK buttons to scroll through and select different LCD patterns to test. Once a test is done, press the OK button to return to the previous menu.</p> <ul style="list-style-type: none"> ◦ Fan Mode <p>Select Auto or On.</p> <ul style="list-style-type: none"> ◦ LED Test Patterns <p>All On, All Off, and Blinking are the available options. Selecting Back in the menu will revert the LED indicators back to their actual status.</p> <ul style="list-style-type: none"> ◦ RTC Test Patterns <p>Select either 2022-02-22 22:22 or 2011-01-11 11:11 to start the RTC (Real-Time Clock) test pattern. Check the system time from either the LCD idle screen or in the web portal System Status→System Information→General page. To revert back to the correct time, manually reboot the device.</p> <ul style="list-style-type: none"> ◦ Hardware Testing <p>Select Test SVIP to verify hardware connections within the device. The result will display on the LCD when the test is complete.</p> |
| <p>Web Info</p> | <ul style="list-style-type: none"> ◦ Protocol: Web access protocol (HTTP/ HTTPS). HTTPS is used by default. ◦ Port: Web access port number, which is 8089 by default. |
| <p>SSH Switch</p> | <ul style="list-style-type: none"> ◦ Enable SSH ◦ Disable SSH <p>SSH access is disabled by default</p> |

Table 3: 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.

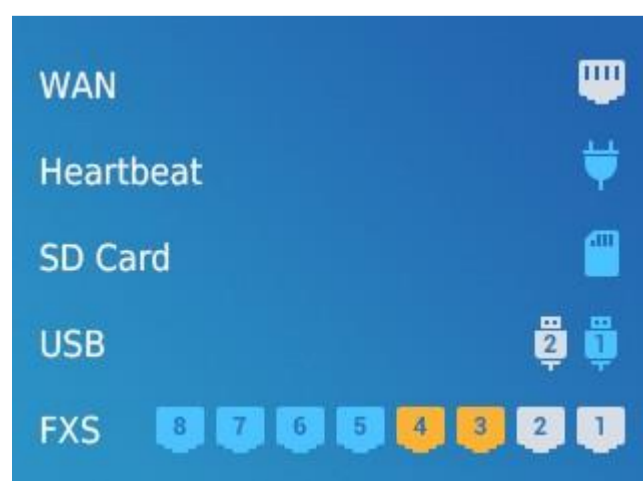


Figure 9: Ports Status

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

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

Table 4: 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:

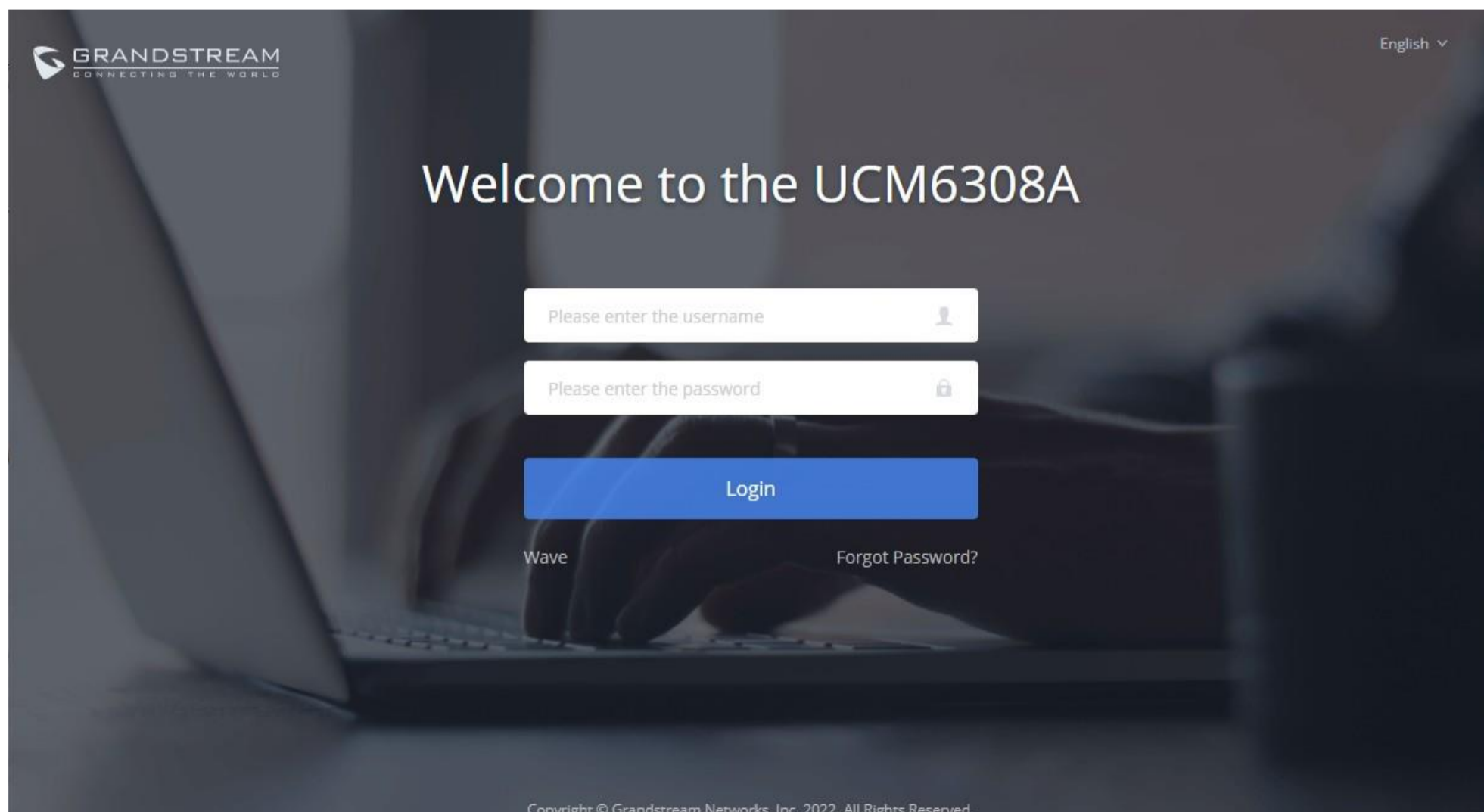


Figure 10: UCM630xA Web GUI Login Page

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

i By default, the UCM630xA has **Redirect From Port 80** enabled. As such, if users type in the UCM630xA IP address in the web browser, the web page will be automatically redirected to the page using HTTPS and port 8089. For example, if the LCD shows 192.168.40.167, and 192.168.40.167 is entered into the web browser, the web page will be redirected to: <https://192.168.40.167:8089>

The option **Redirect From Port 80** can be found under the UCM630xA Web GUI→System Settings→HTTP Server.

Setup Wizard

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

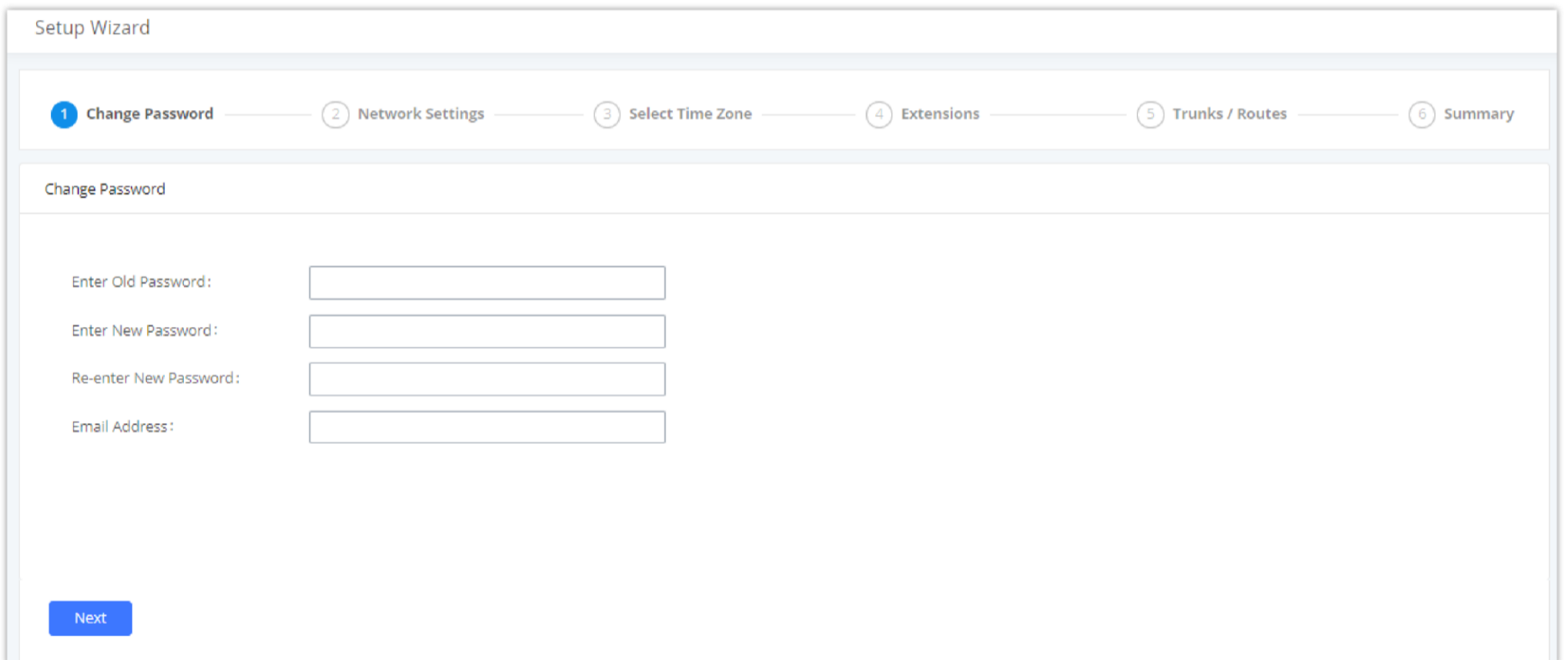


Figure 11: UCM630xA Setup Wizard

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.

Main Settings

There are 8 main sections in the web portal to manage various features of the UCM.

- **System Status:** Displays the dashboard, system information, current active calls, and network status.
- **Extensions/Trunks:** Manages extensions, trunks, and routing rules.
- **Call Features:** Manages various features of the UCM such as the IVR and voicemail.
- **PBX Settings:** Manages the settings related to PBX functionality such as SIP settings and interface settings.
- **System Settings:** Manages the settings related to the UCM system itself such as network and security settings.
- **CDR:** Contains the call detail records, statistics, and audio recordings of calls processed by the UCM.

- **Other Features:** Manages the settings of features unrelated to core PBX functionality such as Zero Config provisioning and CRM/PMS integrations.
- **Maintenance:** Manages settings and logs related to system management and maintenance such as user management, activity logs, backup settings, upgrade settings and troubleshooting tools.

Web GUI Languages

Currently the 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.

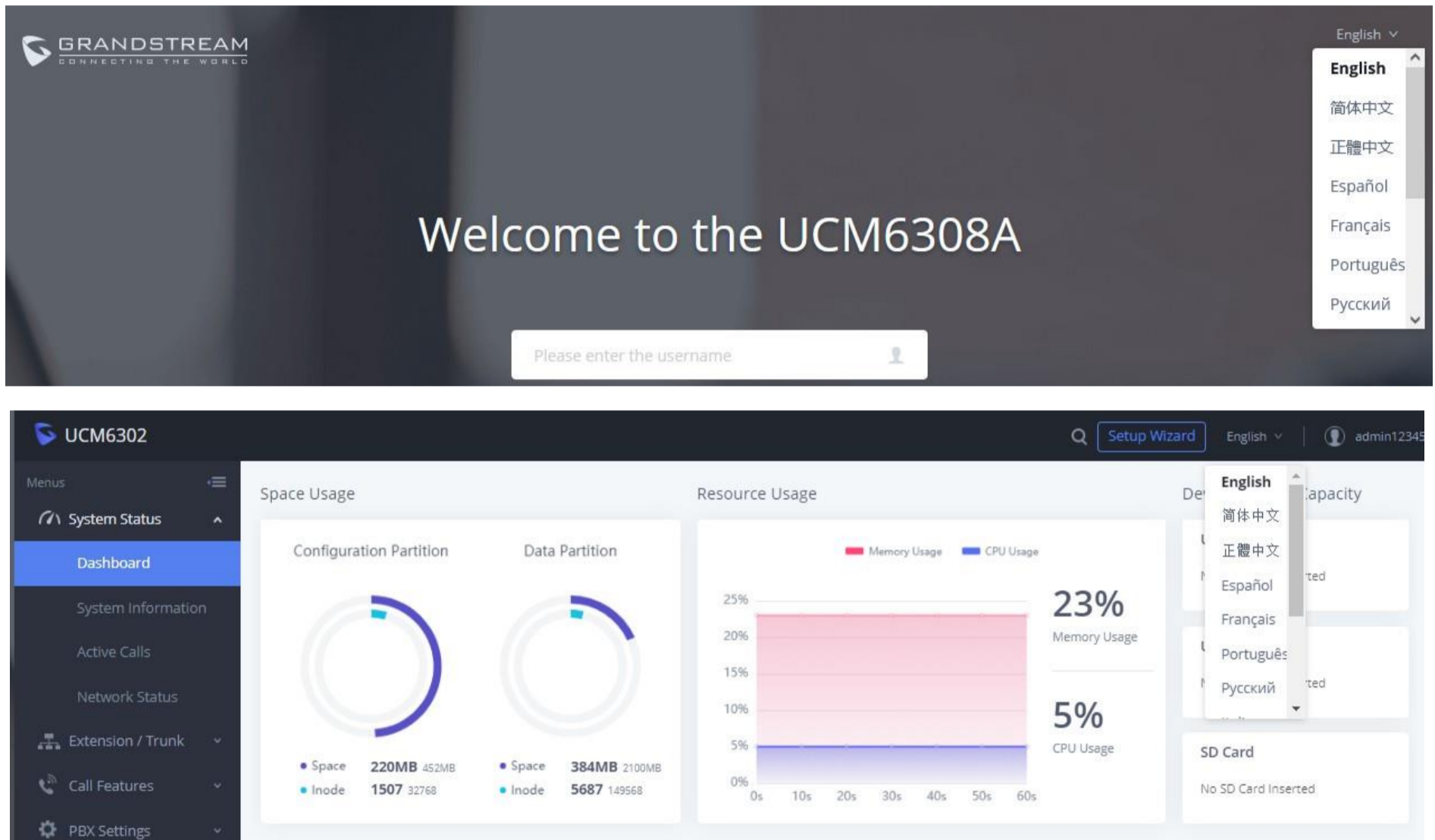


Figure 12: UCM630xA Web GUI Language

Web GUI Search Bar

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

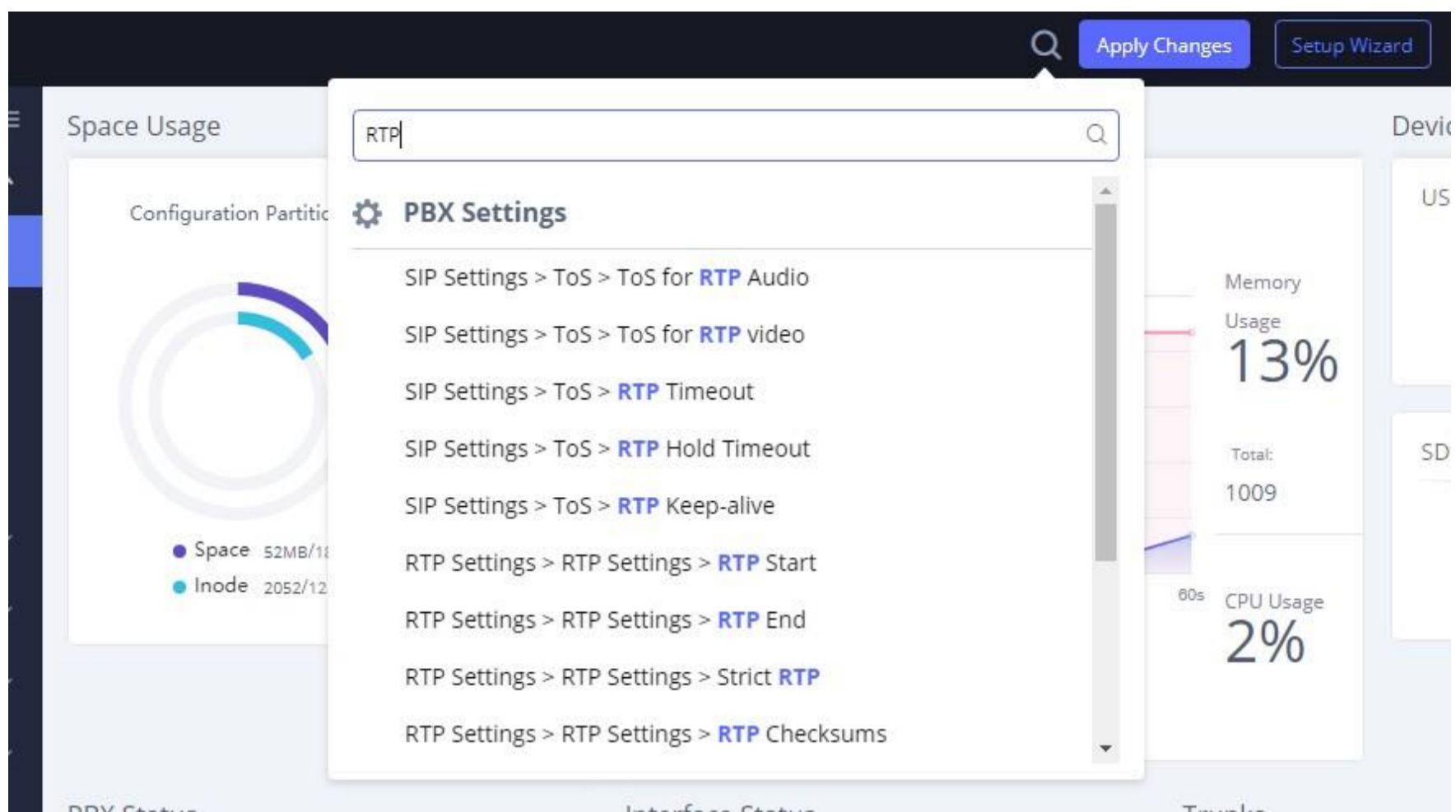


Figure 13: Web GUI Search Bar

Saving and Applying Changes

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

Setting Up an Extension

Power on the UCM630xA and your SIP endpoint. Connect both devices to the same network and follow the steps below to set up an extension.

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

SYSTEM SETTINGS

This section will explain the available system-wide parameters and configuration options on the UCM630xA series. This includes settings for the following items: General Settings, HTTP server, network Settings, OpenVPN, DDNS Settings, Security Settings, LDAP server, Time settings, Email settings and TR-069.

General Settings

System administrators can prevent the UCM from making calls and/or writing to the data partition (e.g., CDR, recordings, etc.) once the system reaches a specified threshold of storage usage and CPU usage respectively. These options are located in the System Settings → General Settings page.

The screenshot shows the 'General Settings' interface. It contains the following fields and values:

- Device Name: [Empty text input field]
- Enable CPU Flow Control:
- CPU Flow Control Threshold: 90% (dropdown menu)
- Data Partition Write Threshold: 90% (dropdown menu)

Figure 14: 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% . |

Table 5: General Settings Parameters

IM Settings

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.

Figure 15: Cloud IM

| Cloud IM Service | |
|--------------------------------|--|
| Enable Cloud IM | If you have purchased the UCM 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 UCM 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. |
| Company Name | Company Name |
| Trusted User | The trusted user of the cloud IM. Only letters, numbers, and special characters are allowed. |
| Prepend | 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

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

IM Server

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

IM Server

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

Close IM Server Mode

Bound Device Information

| DEPARTMENT | MAC ADDRESS | DIAL PREFIX |
|------------|-------------|-------------|
| No Data | | |

Figure 16: 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 |
|-------------|------------------|

Table 7: IM Server parameters

HTTP Server

The UCM630xA'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". |
| Port | Specifies the port number used to access the UCM HTTP server. Default is "8089". |
| Enable IP Address Whitelist | If enabled, only the server addresses in the whitelist will be able to access the UCM's web portal. It is highly recommended to add the IP address currently used to access the UCM web page before enabling this option. Default is "Disabled". |
| Permitted IP(s) | List of addresses that can access the UCM web portal.Ex: 192.168.6.233 / 255.255.255.255 |
| External Host | Configure a URL and port (optional) used to access the UCM web portal or a public link to the conference room if the UCM is behind NAT. |
| Wave Settings | |
| External Host | Configure a URL and port (optional) used to access the UCM web portal or a public link to the conference room if the UCM is behind NAT. |
| Port | The port to access Wave Web and Wave Mobile. If behind NAT, please make sure to map the external port to this port. |
| Certificate Settings | |
| 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 Private Key | Uploads the private key for the HTTP server. Note: Key file must be under 2MB in file size and *.pem format. The file name will automatically be changed to "private.pem". |
| TLS Cert | Uploads the certificate for the HTTP server. Note: Certificate must be under 2MB in file size and *.pem format. This will be used for TLS connections and contains a private key for the client and a signed certificate for the server. |
| Domain | Enter the domain to request the certificate for and click on "Request Certificate" button. |

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 | <p>Select "Route", "Switch" or "Dual" mode on the network interface of UCM630X Audio Series. The default setting is "Switch".</p> <ul style="list-style-type: none"> • 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. The default value is 0. |
| Layer 2 QoS 802.1p Priority Value | Assign the priority value of the layer 2 QoS packets for the WAN port. The default value is 0. |
| 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 default value is 0. |
| 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. |
| 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 Audio Series WAN port) or LAN 2 (mapped to UCM6302 Audio Series 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 default value is 0. |
| 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. |
| 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. <ul style="list-style-type: none"> ● 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 Audio Series WAN port) or LAN 2 (mapped to UCM630X Audio Series 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 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 . |
| 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 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 . |
| 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 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 . |
| 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.

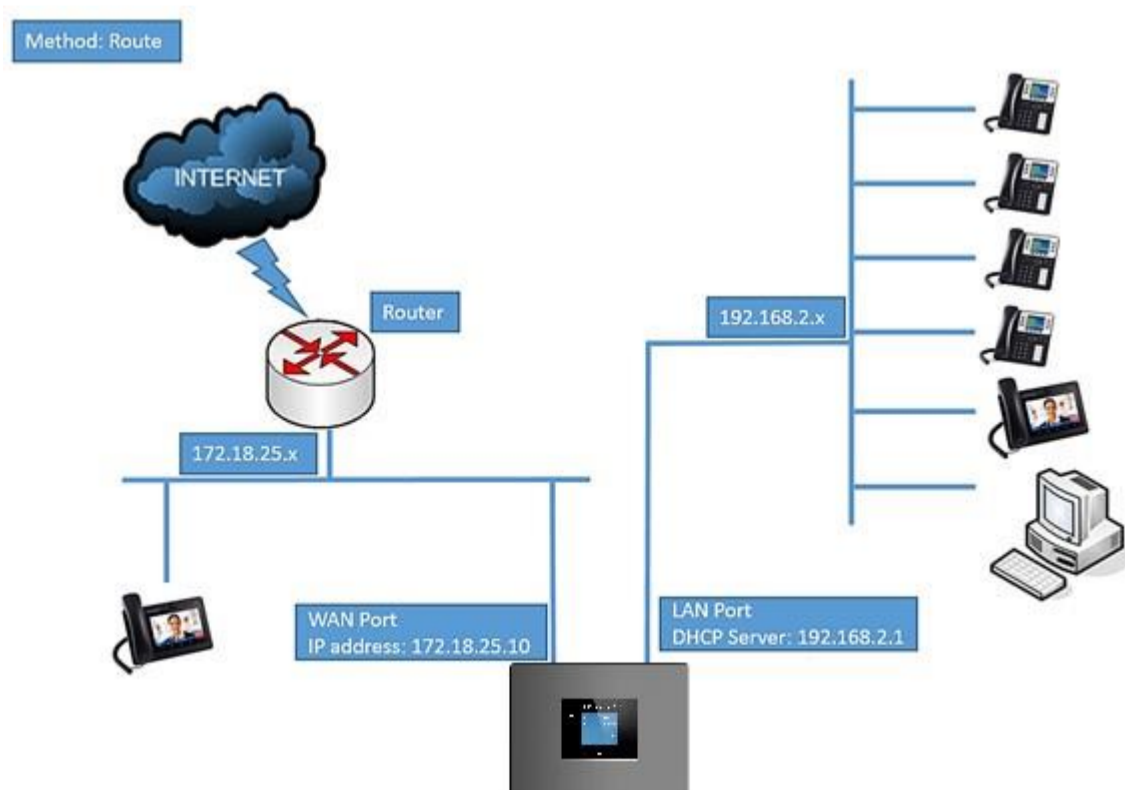


Figure 17: UCM6302A Network Interface Method: Route

◦ **Method: Switch**

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

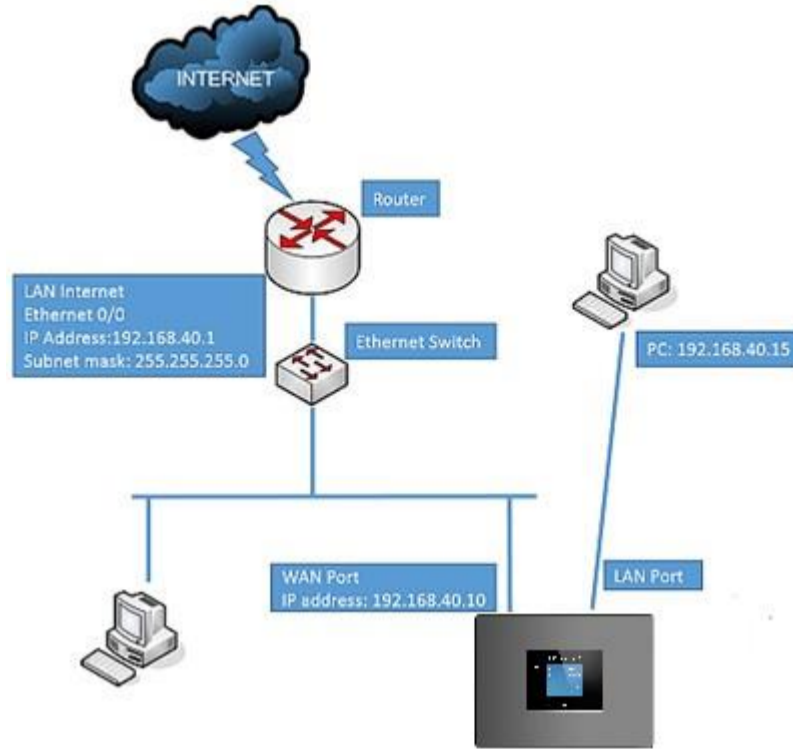


Figure 18: UCM6302A Network Interface Method: Switch

o **Method: Dual**

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

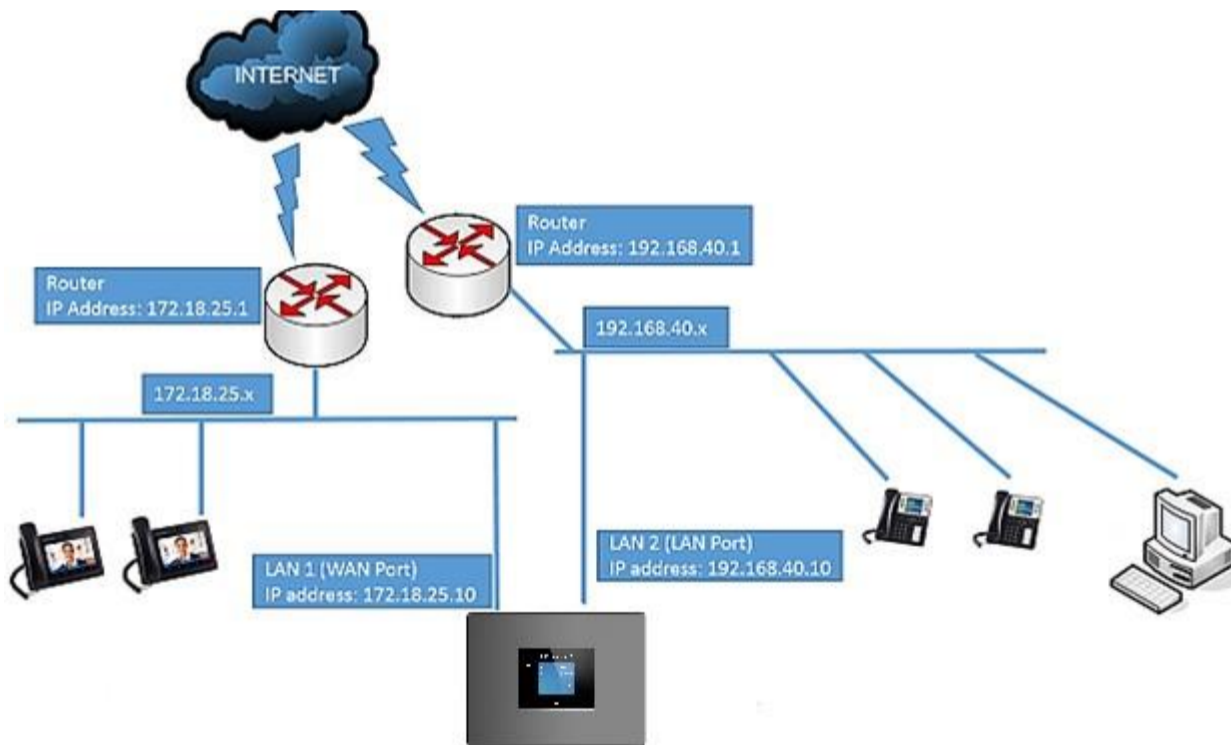


Figure 19: UCM6302A Network Interface Method: Dual

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.

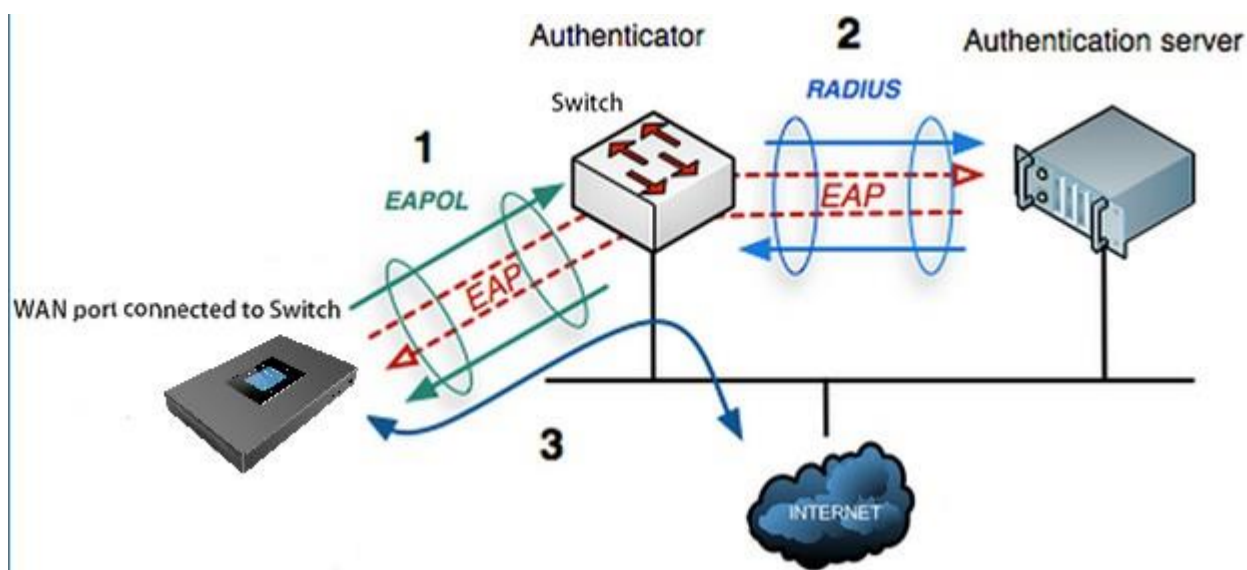


Figure 20: UCM630xA Using 802.1X as Client

Network Settings

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

802.1X Mode:

* Identity:

* MD5 Password:

Figure 21: UCM630xA Using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on UCM630xA. Identity and MD5 password are required for authentication, which should be provided by the network administrator obtained from the RADIUS server. If “EAP-TLS” or “EAP-PEAPv0/MSCHAPv2” is used, users will also need to upload 802.1X CA Certificate and 802.1X Client Certificate, which should be also generated from the RADIUS server.

| | |
|----------------------------------|--|
| 802.1X Mode | Select 802.1X mode. The default setting is “Disable”. The supported 802.1X mode are: <ul style="list-style-type: none"> ◦ 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. |

Table 10: 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



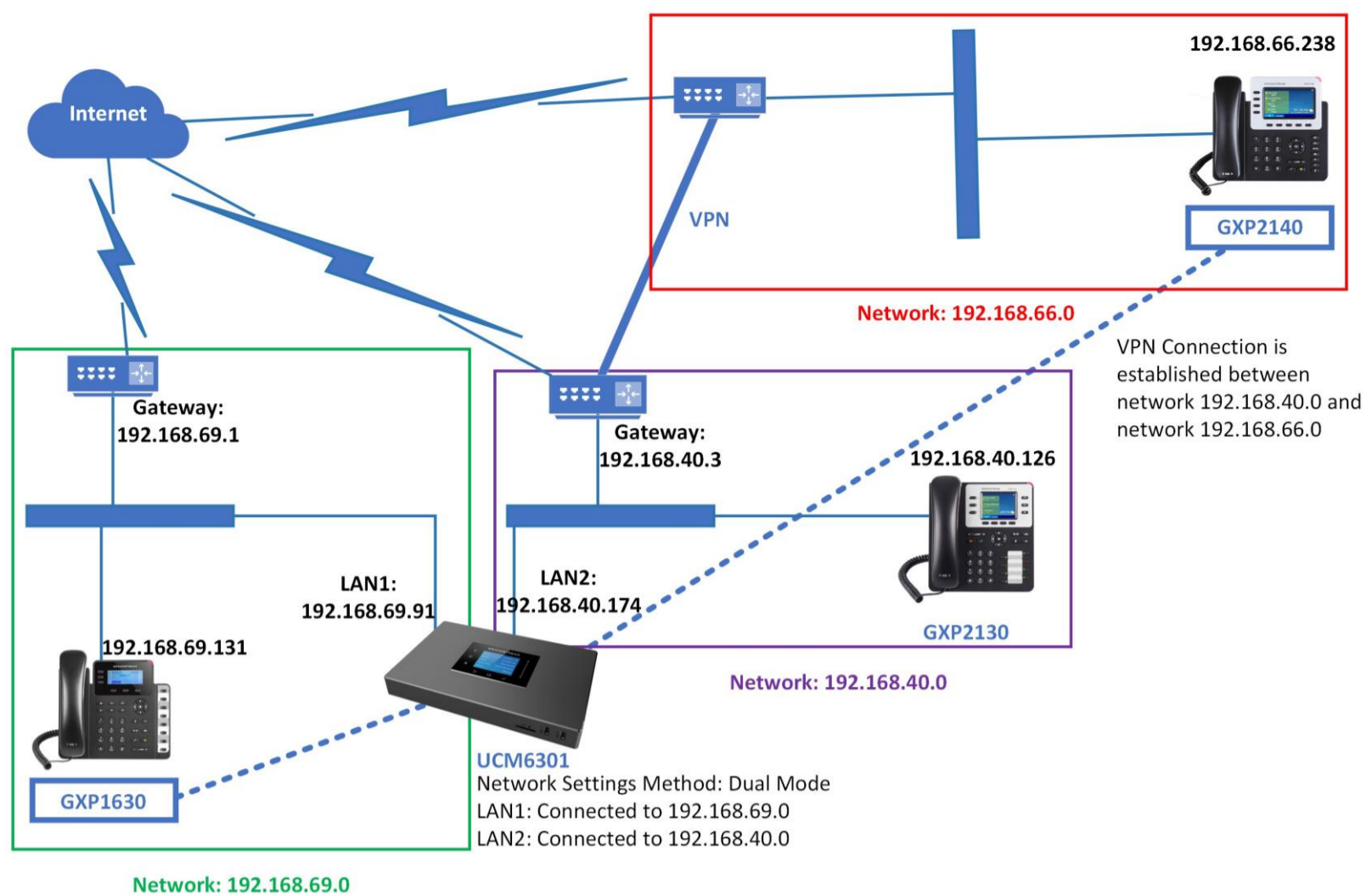
to delete the static route.

| | |
|---------------------------|---|
| <p>Destination</p> | <p>Configure the destination IPv4 address or the destination IPv6 subnet for the UCM630xA to reach using the static route.</p> <p>Example:</p> <p>IPv4 address – <i>192.168.66.4</i></p> <p>IPv6 subnet – <i>2001:740:D::1/64</i></p> |
| <p>Subnet Mask</p> | <p>Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255.</p> <p>Example:</p> <p><i>255.255.255.0</i></p> |
| <p>Gateway</p> | <p>Configure the IPv4 or IPv6 gateway address so that the UCM630xA can reach the destination via this gateway. Gateway address is optional.</p> <p>Example:</p> <p><i>192.168.40.5 or 2001:740:D::1</i></p> |
| <p>Interface</p> | <p>Specify the network interface on the UCM630xA to reach the destination using the static route.</p> <p>LAN interface is eth0; WAN interface is eth1.</p> |

Table 11: UCM630xA Network Settings→Static Routes

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

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



--- GXP1630 and GXP2140 call each other

Figure 22: 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 |

Figure 23: 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”. |

Table 12: 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: | <input type="text" value="8088"/> |
| * LAN IP: | <input type="text" value="192.168.2.100"/> |
| * LAN Port: | <input type="text" value="8088"/> |
| * Protocol Type: | <input type="text" value="UDP Only"/> |

Figure 24: 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 | | | | |

Figure 25: UCM630xA Port Forwarding Configuration

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

1.1.1.1:8088/#page:status_network

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

GRANDSTREAM
CONNECTING THE WORLD STATUS ACCOUNTS SETTINGS NETWORK MAINTENANCE PHONEBOOK

Version 1.0.5.23

Status

- 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 |

Figure 26: 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. |

Table 13: ARP Settings

OpenVPN®

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

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

OpenVPN® Enable:

Configuration Method:

* OpenVPN® Server Address:

OpenVPN® Server Protocol:

OpenVPN® Device Mode:

OpenVPN® Use Compression:

Allow Weak SSL Ciphers:

OpenVPN® Encryption Algorithm:

* OpenVPN® CA Cert:

* OpenVPN® Client Cert:

* OpenVPN® Client Key:

User Authentication:

* Username:

* Password:

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

Figure 27: OpenVPN® Feature on the UCM630xA

| | |
|-----------------------------|---|
| OpenVPN® Enable | Enable / Disable the OpenVPN® feature. |
| Configuration Method | Select the OpenVPN® configuration method. Manual Configuration: Allows to configure OpenVPN® settings manually. |

| | |
|--------------------------------------|--|
| | Upload Configuration File: Allows to upload .ovpn and .conf files to the UCM and to automatically configure OpenVPN® settings. |
| OpenVPN® Server Address | Configures the hostname/IP and port of the server. For example 192.168.1.2:22 |
| OpenVPN® Server Protocol | Specify the protocol user, user should use the same settings as used on the server |
| OpenVPN® Device mode | Use the same setting as used on the server. <ul style="list-style-type: none"> • Dev TUN: Create a routed IP tunnel. • Dev TAP: Create an Ethernet tunnel. |
| OpenVPN® Use Compression | Compress tunnel packets using the LZO algorithm on the VPN link. Do not enable this unless it is also enabled in the server config file. |
| Enable Weak SSL Ciphers | Either to enable the Weak SSL ciphers or not. |
| OpenVPN® Encryption Algorithm | Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server. |
| OpenVPN® CA Cert | Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically. |
| OpenVPN® Client Cert | Upload a client certificate. This file will be renamed as 'client.crt' automatically. |
| OpenVPN® 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: | <input checked="" type="radio"/> DNS Host (A) <input type="radio"/> DNS Host (Round Robin) <input type="radio"/> DNS Alias (CNAME) <input type="radio"/> Port 80 Redirect <input type="radio"/> Web Redirect | ✔ |
| IP Address: | <input type="text" value="1.2.3.4"/> Last Update: 2015-01-07 17:29:20 PST | ✔ |
| Assign to Group: | <input type="text" value="- No Group -"/> <input type="button" value="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. | ✔ |

Figure 28: Register Domain Name on noip.com

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

UCM6302

DDNS Settings

DDNS Server: no-ip.com

Enable DDNS:

* Username: user_no_ip

* Password:

* Host Name: MyGSPBX.ddns.net

Figure 29: UCM630xA DDNS Setting

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

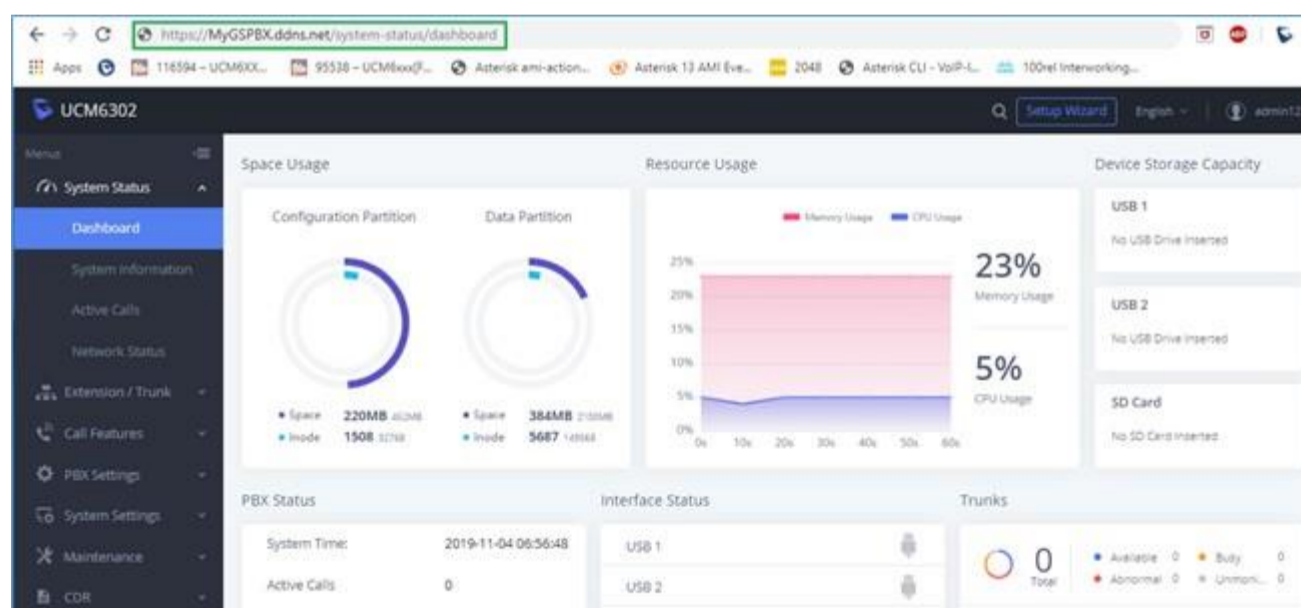


Figure 30: Using Domain Name to Connect to UCM630xA

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 | SIP |
| 38563 | Asterisk | udp/ipv4 | SIP |
| 10000 | gs_avs | udp/ipv4 | gs_avs |
| 10001 | gs_avs | udp/ipv4 | gs_avs |
| 10002 | gs_avs | udp/ipv4 | gs_avs |
| 10003 | gs_avs | udp/ipv4 | gs_avs |
| 10004 | gs_avs | udp/ipv4 | gs_avs |
| 10005 | gs_avs | udp/ipv4 | gs_avs |
| 10006 | gs_avs | udp/ipv4 | gs_avs |
| 10007 | gs_avs | udp/ipv4 | gs_avs |
| 10010 | gs_avs | udp/ipv4 | gs_avs |
| 10012 | gs_avs | udp/ipv4 | gs_avs |
| 10013 | gs_avs | udp/ipv4 | gs_avs |
| 10014 | gs_avs | udp/ipv4 | gs_avs |
| 10015 | gs_avs | udp/ipv4 | gs_avs |
| 10018 | gs_avs | udp/ipv4 | gs_avs |
| 10019 | gs_avs | udp/ipv4 | gs_avs |
| 10020 | gs_avs | udp/ipv4 | gs_avs |

| Port | Process | Type | Protocol or Service |
|-------|----------|----------|---------------------|
| 6066 | Python | udp/ipv4 | python |
| 3306 | Mysqld | tcp/ipv4 | mysqld |
| 45678 | Python | udp/ipv4 | python |
| 8439 | Lighttpd | tcp/ipv4 | HTTP |
| 8088 | asterisk | tcp/ipv4 | SIP |
| 8888 | Pbxmid | tcp/ipv4 | pbxmid |
| 25 | Master | tcp/ipv4 | master |
| 636 | Slapd | tcp/ipv4 | SLDAP |
| 4569 | asterisk | udp/ipv6 | SIP |
| 42050 | asterisk | udp/ipv6 | SIP |
| 7681 | Pbxmid | tcp/ipv4 | pbxmid |

Table 15: 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 | <p>Allows the UCM630xA to handle excessive amounts of SYN packets from one source and keep the web portal accessible. There are two options available and only one of these options may be enabled at one time.</p> <ul style="list-style-type: none"> ◦ 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. <p>SYN Flood Defense will limit the amount of SYN packets accepted by the UCM from one source to 10 packets per second. Any excess packets from that source will be discarded.</p> |
| 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. |

Table 16: Typical Firewall Settings

Under “Custom Firewall Settings”, users could create new rules to accept, reject or drop certain traffic going through the UCM630xA. To create new rule, click on “Create New Rule” button and a new window will pop up for users to specify rule options.

Right next to “Create New Rule” button, there is a checkbox for option “Reject Rules”. If it is checked, all the rules will be rejected except the firewall rules listed below. In the firewall rules, only when there is a rule that meets all the following requirements, the option “Reject Rules” will be allowed to check:

- Action: “Accept”
- Type “In”
- Destination port is set to the system login port (e.g., by default 8089)
- Protocol is not UDP

Create New Firewall Rule

* Rule Name:

* Action:

* Type:

* Interface:

* Service:



Figure 31: Create New Firewall Rule

| | |
|-----------------------------------|--|
| Rule Name | Specify the Firewall rule name to identify the firewall rule. |
| Action | <p>Select the action for the Firewall to perform.</p> <ul style="list-style-type: none"> ◦ ACCEPT ◦ REJECT ◦ DROP |
| Type | <p>Select the traffic type.</p> <ul style="list-style-type: none"> ◦ IN <p>If selected, users will need specify the network interface “LAN” or “WAN” (for UCM630xA) for the incoming traffic.</p> <ul style="list-style-type: none"> ◦ OUT |
| Interface | Select the interface to use the Firewall rule. |
| Service | <p>Select the service type.</p> <ul style="list-style-type: none"> ◦ FTP ◦ SSH ◦ Telnet ◦ HTTP ◦ LDAP ◦ Custom <p>If “Custom” is selected, users will need specify Source (IP and port), Destination (IP and port) and Protocol (TCP, UDP or Both) for the service. Please note if the source or the destination field is left blank, it will be used as “Anywhere”.</p> |
| 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. |

Table 17: 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: <i>192.168.2.100-192.168.2.105, 1000:9999</i> |

Table 18: UCM630xA Firewall Dynamic Defense

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:
(s):

* Connection Threshold:

Dynamic Defense Whitelist:

Figure 32: Configure Dynamic Defense

Fail2ban

Fail2Ban feature on the UCM630xA provides intrusion detection and prevention for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. Once the entry is detected within “Max Retry Duration”, the UCM630xA will act to forbid the host for certain period as defined in “Banned Duration”. This feature helps prevent SIP brute force attacks to the PBX system.

Security Settings

Static Defense Dynamic Defense **Fail2Ban** SSH Access

Global Settings

Enable Fail2Ban:

Banned Duration (s):

Max Retry Duration (s):

Fail2ban Whitelist: / +

[Add Fail2ban Whitelist](#) +

Local Settings

Asterisk Service:

Login Attack Defense:

Customer Service System Call Defense:

Figure 33: Fail2ban Settings

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

| | |
|---|--|
| Max Retry Duration | Within this duration (in seconds), if a host exceeds the max times of retry as defined in "MaxRetry", the host will be banned. The default setting is 600. |
| MaxRetry | Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5. |
| Fail2Ban Whitelist | Configure IP address, CIDR mask, or DNS host in the whitelist. Fail2Ban will not ban the host with a matching address in this list. Up to 20 addresses can be added to the list descriptions/comments can be added for each whitelist entry for admin to log what's the whitelist IP address is for. |
| Local Settings | |
| Asterisk Service | Enable Asterisk service for Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on to use Fail2Ban for SIP authentication on the UCM630X. |
| Listening Port Number | Configure the listening port number for the service. By default, port 5060 will be used for UDP and TCP, and port 5061 will be used for TCP. |
| MaxRetry | Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5. Please make sure this option is properly configured as it will override the "MaxRetry" value under "Global Settings". |
| Login Attack Defense | Enables defense against excessive login attacks to the UCM's web GUI. The default setting is disabled. |
| Listening Port Number | This is the Web GUI listening port number which is configured under System Settings → HTTP Server → Port. The default is 8089. |
| MaxRetry | When the number of failed login attempts from an IP address exceeds the MaxRetry number, that IP address will be banned from accessing the Web GUI. |
| Customer Service System Call Defense | Enable call defense in the customer service system. Off by default. |
| Listening Port Number | The current service listening port. Default UDP port: 5060, TCP port: 5060, 5061, WebSocket communication port: 8088. |
| MaxRetry | Set the maximum number of calls allowed in the "time span". The local matching threshold has a higher priority than the global matching threshold. The default setting is 5. |
| Blacklist | |
| Blacklist | Users will be able to view the IPs that have been blocked by UCM. |

SSH Access

SSH switch now is available via Web GUI and LCD. User can enable or disable SSH access directly from Web GUI or LCD screen. For web SSH access, please log in 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.

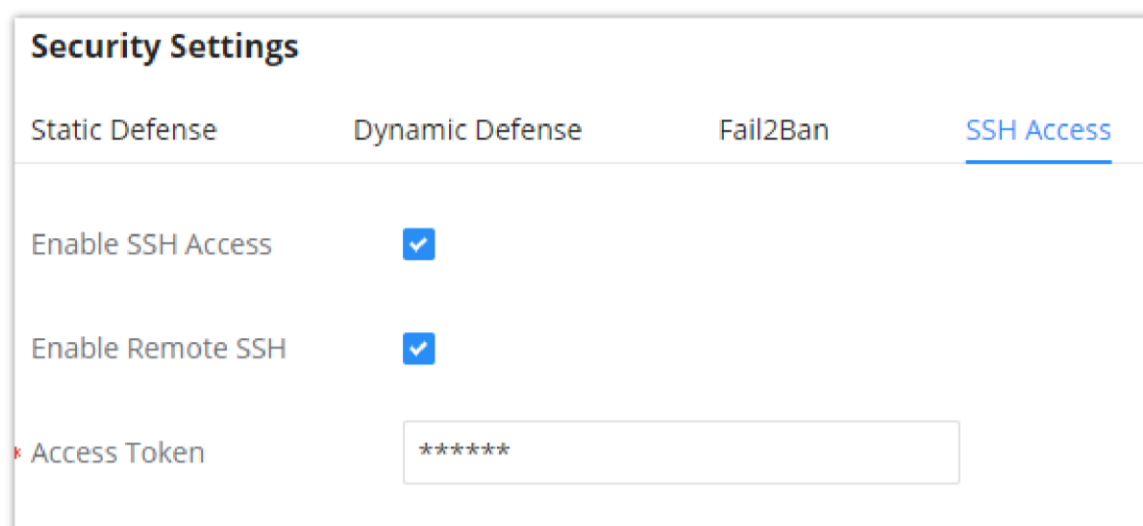


Figure 34: SSH Access

| | |
|--------------------------|---|
| Enable SSH Access | This option is used for system debugging. Once enabled, UCM will allow SSH access. The SSH connection requires super administrator's username and password. The default setting is "No". It is recommended to set it to "No" if there is no need for debugging. |
| Enable Remote SSH | If this option is enabled, remote SSH access will be allowed through the Feedback platform. It is strongly recommended to keep this disabled unless remote troubleshooting is necessary. |
| Access Token | Please enter the token to request SSH data. |

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

* Base DN:

PBX DN: ,dc=pbx,dc=com

Root DN: ,dc=pbx,dc=com

* Root Password:

* Confirm Root Password:

LDAP Cert:

LDAP Private Key:

LDAP CA Cert:

Figure 35: LDAP Server Configurations

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

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



for the first phonebook under LDAP Phonebook.

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

+ 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

Figure 36: Default LDAP Phonebook DN

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

Figure 37: Default LDAP Phonebook Attributes

LDAP Phonebook

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

| PHONEBOOK DN | OPTIONS |
|--|---------|
| <input type="checkbox"/> ou=pbx,dc=pbx,dc=com 30 | |

Figure 38: LDAP Server→LDAP Phonebook

◦ Add new phonebook

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

Add Phonebook [X]

* Phonebook Prefix:

Phonebook DN:

Cancel Save

Figure 39: 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

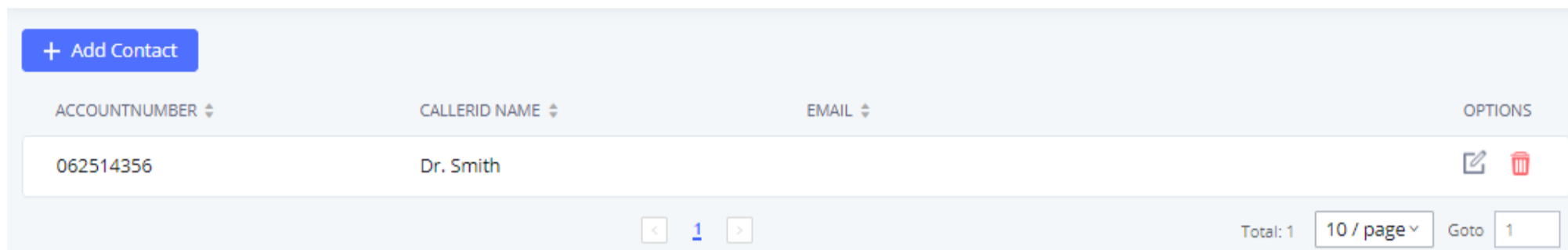


Figure 40: Edit LDAP Phonebook

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

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

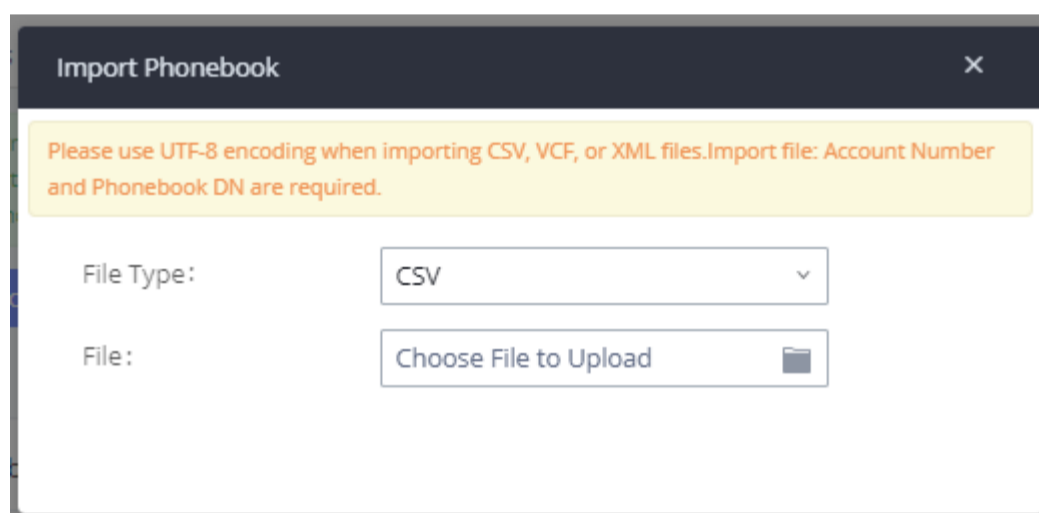


Figure 41: Import Phonebook

The file to be imported must be a CSV, VCF or XML file with UTF-8 encoding. Users can open the file with Notepad and save it with UTF-8 encoding.

Here is how a sample file looks like. Please note “Account Number” and “Phonebook DN” fields are required. Users could export a phonebook file from the UCM630xA LDAP phonebook section first and use it as a sample to start with.

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

Figure 42: 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.

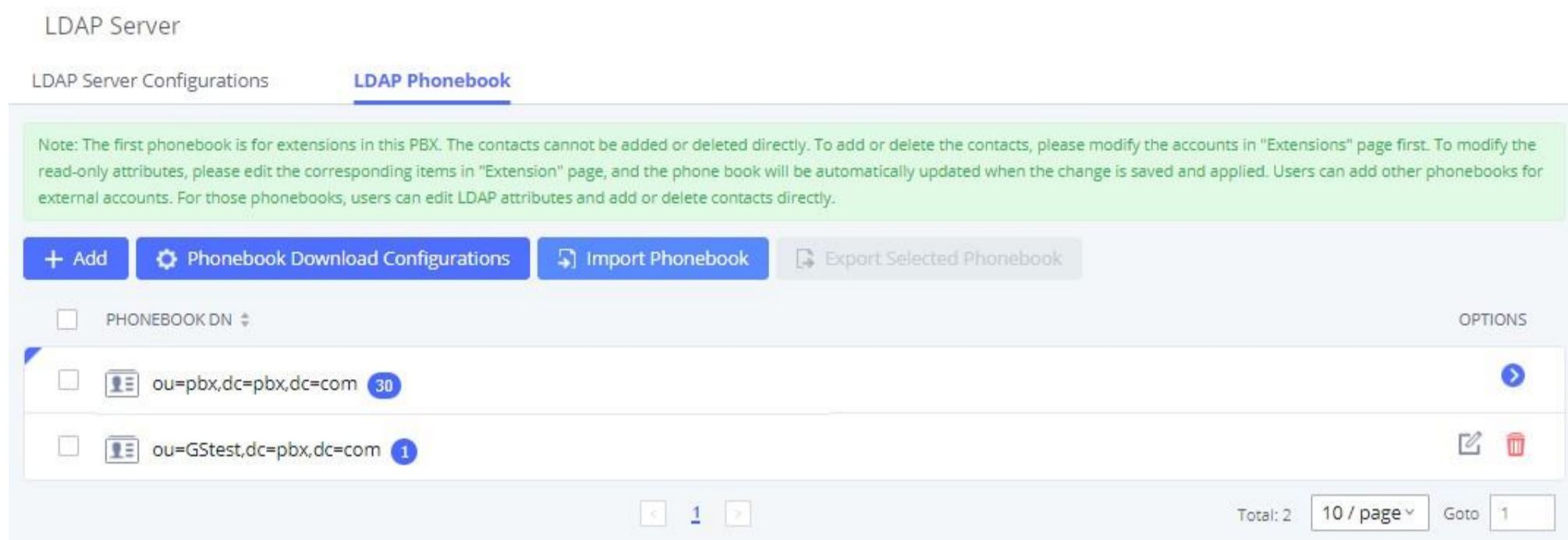


Figure 43: LDAP Phonebook After Import

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

- **Export phonebook to your computer from 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.

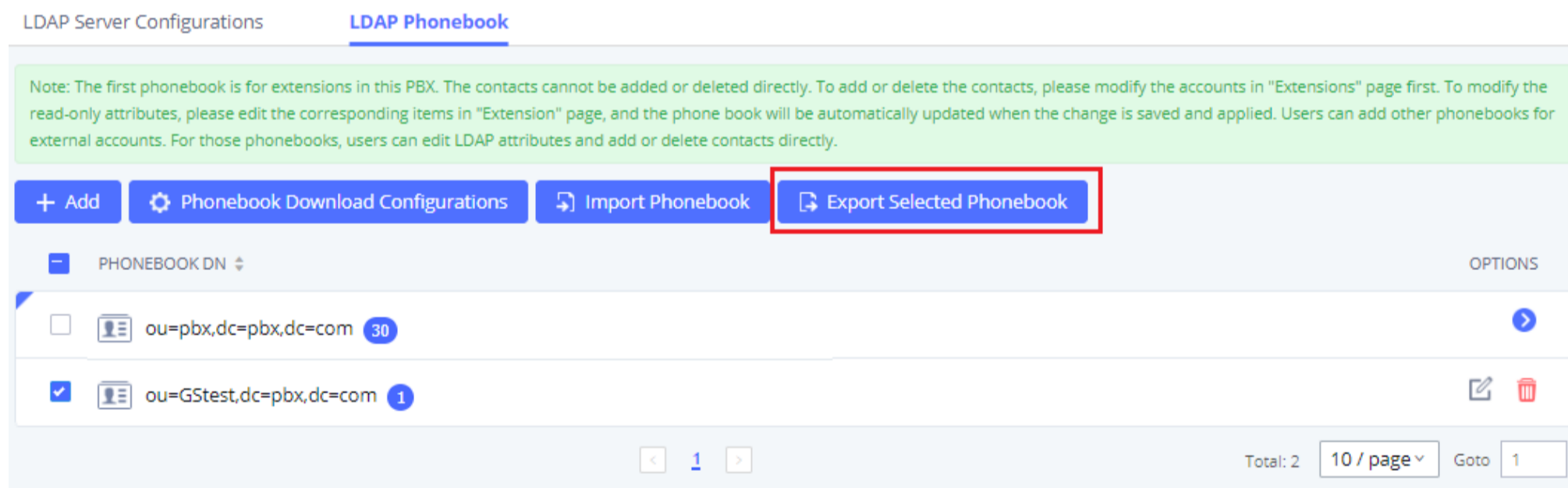


Figure 44: Export Selected LDAP Phonebook

LDAP Settings

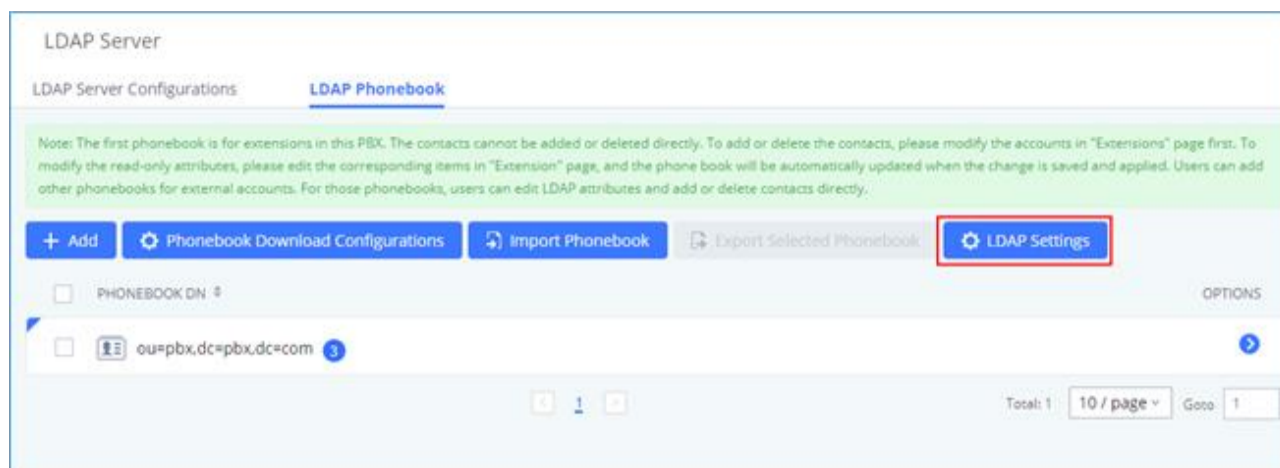
Prerequisites to support contacts sync-up to IP Phones, UCM needs to support the following:

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

4. If Cloud IM is disabled, the contacts sent from UCM to end device should only contain contacts on the UCM.

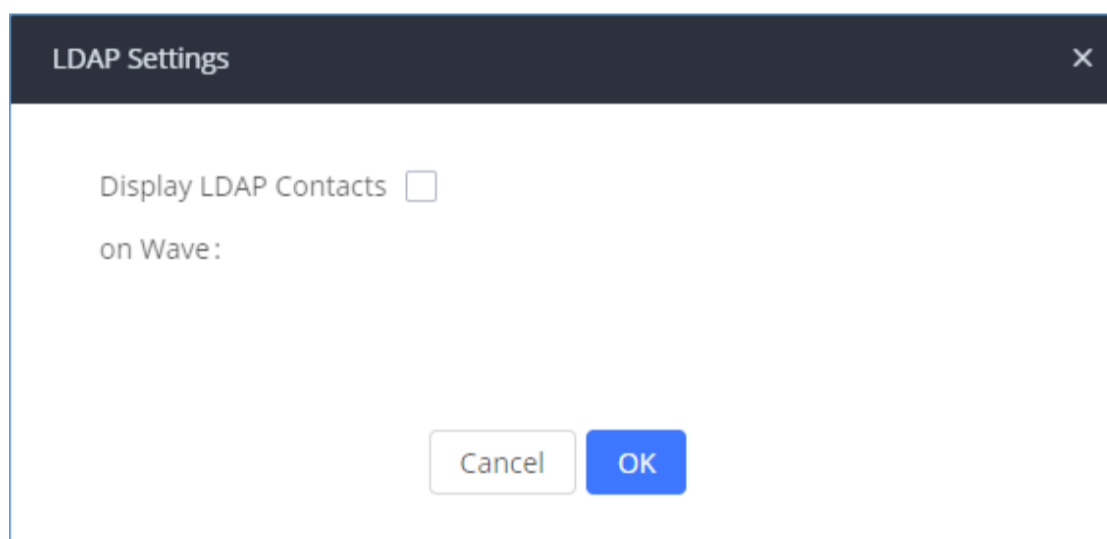
To support contacts sync-up to Wave, it allows Wave to obtain enterprise contacts from Cloud IM or LDAP. On UCM SIP peer trunk, if LDAP sync is enabled, end point can obtain remote UCM extensions' info via LDAP. Also, it will allow configuring whether to sync up LDAP contacts on Wave so that Wave doesn't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

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



LDAP Settings

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



Display LDAP Contacts on Wave

LDAP Client Configurations

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

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

| | |
|-----------------------|--|
| 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.

Figure 45: 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 35: 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 | <input type="radio"/> Version 2 <input checked="" type="radio"/> Version 3 |
| LDAP Name Attributes | CallerIDName |
| LDAP Number Attributes | AccountNumber |
| LDAP Display Name | AccountNumber CallerIDName |
| Max. Hits | 50 |
| Search Timeout | 30 |
| Sort Results | <input checked="" type="radio"/> No <input type="radio"/> Yes |
| LDAP Lookup | <input checked="" type="checkbox"/> Incoming Calls <input checked="" type="checkbox"/> Outgoing Calls |
| Lookup Display Name | |
| | <input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Reset"/> |

Figure 46: 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.

| | |
|------------------------------|--|
| Remote NTP Server | Specify the URL or IP address of the NTP server for the UCM630xA to synchronize the date and time. The default NTP server is pool.ntp.org. |
| Enable DHCP Option 2 | If set to “Yes”, the UCM630xA can get provisioned for Time Zone from DHCP Option 2 in the local server automatically. The default setting is “Yes”. |
| Enable DHCP Option 42 | If set to “Yes”, the UCM630xA can get provisioned for NTP Server from DHCP Option 42 in the local server automatically. This will override the manually configured NTP Server. The default setting is “Yes”. |
| Time Zone | Select the proper time zone option so the UCM630xA can display correct time accordingly. |

Table 21: Time Auto Updating

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:

Figure 47: Set Time Manually

i Manually setup time will take effect immediately after saving and applying change in the Web GUI. If users would like to reboot the UCM630xA and keep the manually setup time setting, please make sure “Remote NTP Server”, “Enable DHCP Option 2” and “Enable DHCP Option 42” options under Web GUI→Settings→Time Settings→Auto Time Updating page are unchecked or set to empty. Otherwise, time auto updating settings in this page will take effect after reboot.

NTP Server

The UCM630xA can be used as an NTP server for the NTP clients to synchronize their time with. To configure the UCM630xA as the NTP server, set “Enable NTP server” to “Yes” under Web GUI→System Settings→Time Settings→NTP Server. On the client side, point the NTP server address to the UCM630xA IP address or host name to use the UCM630xA as the NTP server.

Office Time

On the UCM630xA, the system administrator can define “office time”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure office time, go to Web GUI→System Settings→Time Settings→Office Time. Click on “Add” to create an office time.

Figure 48: 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. |

Table 22: 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





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

Figure 49: Settings→Time Settings→Office Time

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

Holiday

On the UCM630xA, the system administrator can define “holiday”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure holiday, go to Web GUI→**System Settings**→**Time Settings**→**Holiday**. Click on “**Add**” to create holiday time.

Create New Holiday

* Name :

Holiday Memo :

Year :

Month :

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

Day :

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

Show Advanced

Options :

Week :

| | | | |
|-----|-----|-----|-----|
| Sun | Mon | Tue | Wed |
| Thu | Fri | Sat | |

Time :

Figure 50: Create New Holiday

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

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

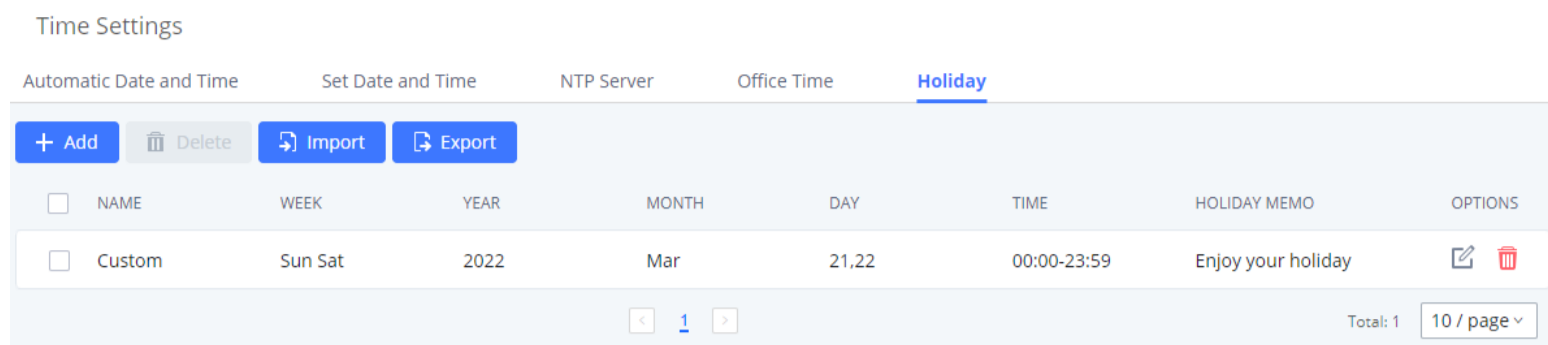




Figure 51: Settings→Time Settings→Holiday

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

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 Web GUI→System Settings→Email Settings→Email Settings.

| | |
|-----------------------------------|--|
| TLS Enable | Enable or disable TLS during transferring/submitted your Email to another SMTP server. The default setting is “Yes”. |
| Type | <p>Select Email type.</p> <ul style="list-style-type: none"> ◦ MTA: Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it or no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. ◦ Client: Submit Emails to the SMTP server. A SMTP server is required, and users need login with correct credentials. |
| Domain | Specify the domain name to be used in the Email when using type “MTA”. |
| SMTP Server | Specify the SMTP server when using type “Client”. |
| Enable SASL Authentication | Enable SASL Authentication. When disabled, UCM will not try to use the username and password for mail client login authentication. Most of the mail server requires login authentication while some others private mail servers allow anonymous login which requires disabling this option to send Email as normal. For Exchange Server, please disable this option. |
| Username | Username is required when using type “Client”. Normally it is the Email address. |
| Password | Password to login for the above Username (Email address) is required when using type “Client”. |
| Enable Email-to-Fax | Monitors the inbox of the configured email address for the specified subject. If enabled, the UCM will get a copy of the attachment from the email and send it to the XXX extension by fax. The attachment must be in PDF/TIF/TIFF format. |

| | |
|---|---|
| Email-to-Fax Blacklist/Whitelist | The user can enable the Email-to-Fax Blacklist or Email-to-Fax Whitelist. |
| Email-to-Fax Subject Format | Select the email subject format to use for emails to fax. XXX refers to the extension that the fax will be sent to. This extension can only contain numbers. |
| Internal Black/Whitelist | Email address blacklist/whitelist for local extensions. |
| External Blacklist/Whitelist | Email address blacklist/whitelist for non-local contacts. Separate multiple addresses with semicolon (;) (i.e. "xxx;yyy"). |
| Fax Sending Success/Failure Confirmation | If enabled, the UCM will send an email notification to the sender about the fax sending result. |
| POP/POP3 Server Address | Configure the POP/POP3 server address for the configured username Example: pop.gmail.com |
| POP/POP3 Server Port | Configure the POP/POP3 server port for the configured username Example: 995 |
| Display Name | Specify the display name in the FROM header in the Email. |
| Sender | Specify the sender's Email address. For example: pbx@example.mycompany.com. |

Table 24: Email Settings

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 Template
Email footer hyperlink
Email Send Log

TLS Enable:

Type:

Email Template Sending Format:

* SMTP Server:

* Enable SASL Authentication:

* Username:

* Password:

Enable Email-to-Fax:

POP/POP3 Server Address:

POP/POP3 Server Port:

* Display Name:

* Sender:

Figure 52: UCM630xA Email Settings

Once the configuration is finished, click on “Test”. In the prompt, fill in a valid Email address to send a test Email to verify the Email settings on the UCM630xA.

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

Email Templates

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

- Click on



icon to edit the template.

| Email Settings | | | | |
|-----------------------------|-----------------------------------|------------------------|-------------------------------|---------|
| 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 | |

Figure 53: Email Template

Note

The “Multimedia Meeting Schedule” template is improved. Click on “Edit” for this template to view the improved default template.

- Added “Edge” and “Safari” as supported browser.
- Added “Download Wave” button for user to download Wave app from: <https://fw.gdms.cloud/wave/download/>
- Improved descriptions

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.

Figure 54: 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.

Figure 55: Email Send Log

| Field | Description |
|-------------------|---|
| Start Time | Enter the start time for filter |
| End Time | Enter the end time for filter |
| Receivers | Enter the email recipient, while searching for multiple recipients, please separate them with comma and no spaces. |
| Send Result | Enter the status of the send result to filter with |
| Return Code | Enter the email code to filter with |
| Email Send Module | Select the email module to filter with from the drop-down list, which contains: <ul style="list-style-type: none"> ◊ All Modules ◊ Extension ◊ Voicemail ◊ Meeting Schedule ◊ User Password ◊ Alert Events ◊ CDR ◊ Test |

Table 25: 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 | (i) |
| 2020-12-21 18:00:04 | Video Conference Schedule | m.g@gmail.com | 12-21 18:00:06 | m.g@gmail.com | sent | 250 | (i) |
| 2020-12-20 18:00:04 | Video Conference Schedule | m.g@gmail.com | 12-20 18:00:07 | m.g@gmail.com | sent | 250 | (i) |
| 2020-12-19 18:00:03 | Video Conference Schedule | m.g@gmail.com | 12-19 18:00:06 | m.g@gmail.com | sent | 250 | (i) |
| 2020-12-18 18:00:03 | Video Conference Schedule | m.g@gmail.com | 12-18 18:00:06 | m.g@gmail.com | sent | 250 | (i) |
| 2020-12-17 18:00:03 | Video Conference Schedule | m.g@gmail.com | 12-17 18:00:06 | m.g@gmail.com | sent | 250 | (i) |

Total: 32 10 / page Goto 1

Figure 56: 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 | <p>Possible reasons:</p> <ol style="list-style-type: none"> 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 | <p>Indicates that there is no return code.</p> <p>If the sending result is “deferred”, the general reason is that the mail service area is configured incorrectly. Please check whether the server configuration is correct.</p> <p>If the sending result is “bounced”, the general reason is that the receiving email address domain name is wrong, please check whether the email recipient is the correct email address. If it is in MTA mode, please check whether the “domain” is configured to be in the same domain name as the “recipient”.</p> |

Table 26: Email Codes

SMS Settings

SMS Configuration

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

SMS Settings > SMS Settings

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

Enable SMS

* SMS Carrier

Region

* Account ID

* Secret

* From

| | |
|--------------------|---|
| Enable SMS | Tick this box to enable SMS service. |
| SMS Carrier | Choose the SMS carrier: <ul style="list-style-type: none">• Amazon• Twilio |
| Region | Choose the region. |
| Account ID | Enter the ID of the account created at the carrier. |
| Secret | Enter the secret code. |
| From | Enter the number phone allocated for the UCM. |

SMS Template

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

SMS Settings > SMS Settings

SMS Settings

SMS Template

SMS Delivery Log

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

| TYPE | TEMPLATE CONTENT | OPTIONS |
|--------------------|---|---------|
| Verification Code | [UCM] Your verification code is <code>\$(code)</code> . It will expire in 10 minutes. | |
| Alarm Notification | [UCM] <code>\$(hostName)\$(macAddr)</code> system event: <code>\$(content)</code> | |

© 2023 Grandstream Networks, Inc.

SMS Template

SMS Delivery Log

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

SMS Settings

SMS Settings

SMS Template

SMS Delivery Log

Show All Logs

Clear

Delete Search Result(s)

Display Filter

SEND RESULT

RECIPIENT

SMS CATEGORY

SEND TIME

No data

© 2023 Grandstream Networks, Inc.

SMS Delivery Log

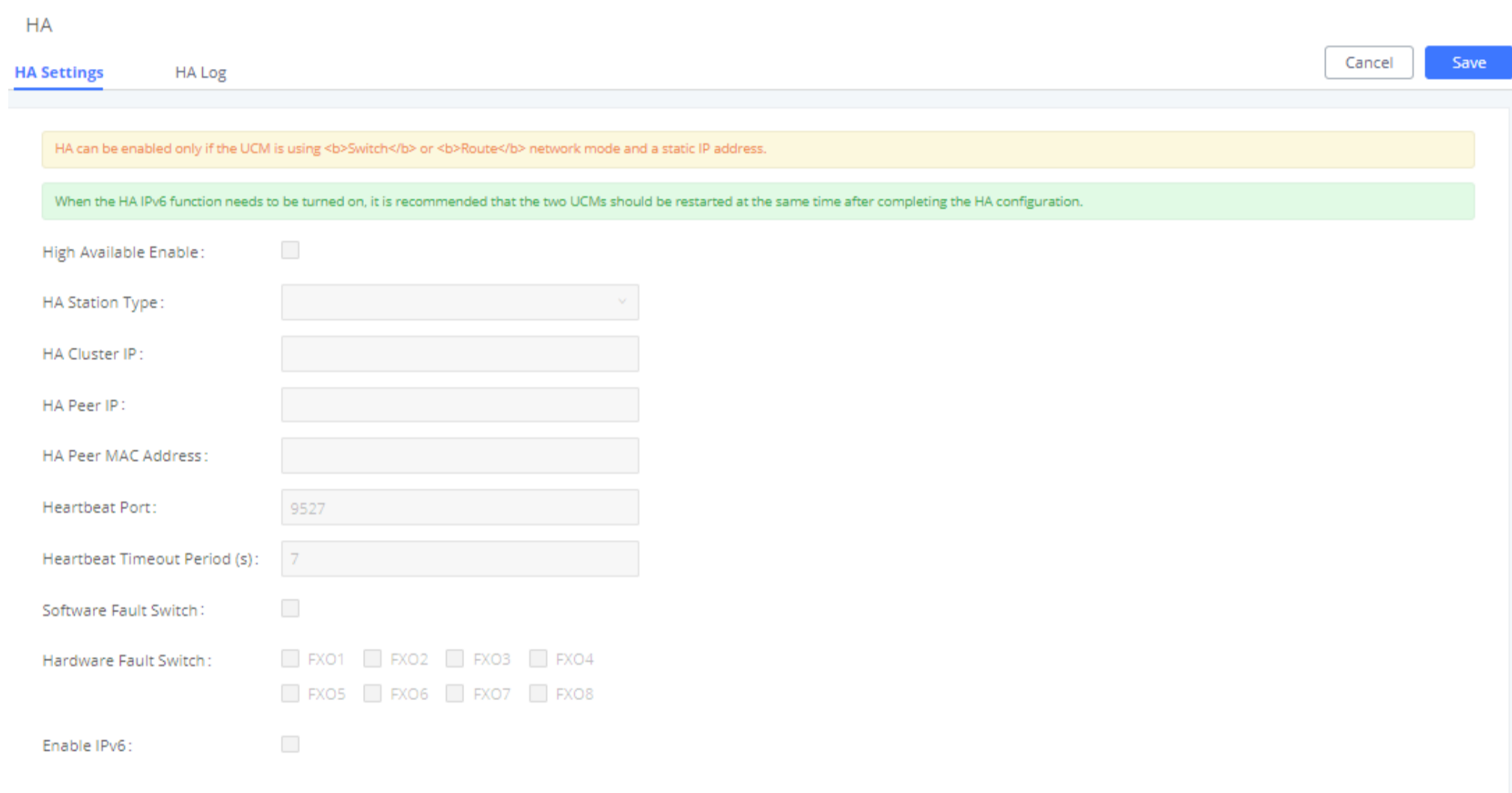
HA

Dual-system hot standby provides a highly reliable and fault-tolerant solution for enterprises using 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 monitors the running status of the host at all times. 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.

Before forming a paired HA dual-system hot backup, two UCM devices need to complete their respective network settings. The network mode can only be switching or routing, and the IP type can only be static.

HA settings

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



HA

HA Settings HA Log Cancel Save

HA can be enabled only if the UCM is using **Switch** or **Route** network mode and a static IP address.

When the HA IPv6 function needs to be turned on, it is recommended that the two UCMs should be restarted at the same time after completing the HA configuration.

High Available Enable:

HA Station Type:

HA Cluster IP:

HA Peer IP:

HA Peer MAC Address:

Heartbeat Port:

Heartbeat Timeout Period (s):

Software Fault Switch:

Hardware Fault Switch: FX01 FX02 FX03 FX04
 FX05 FX06 FX07 FX08

Enable IPv6:

Figure 57: HA Settings

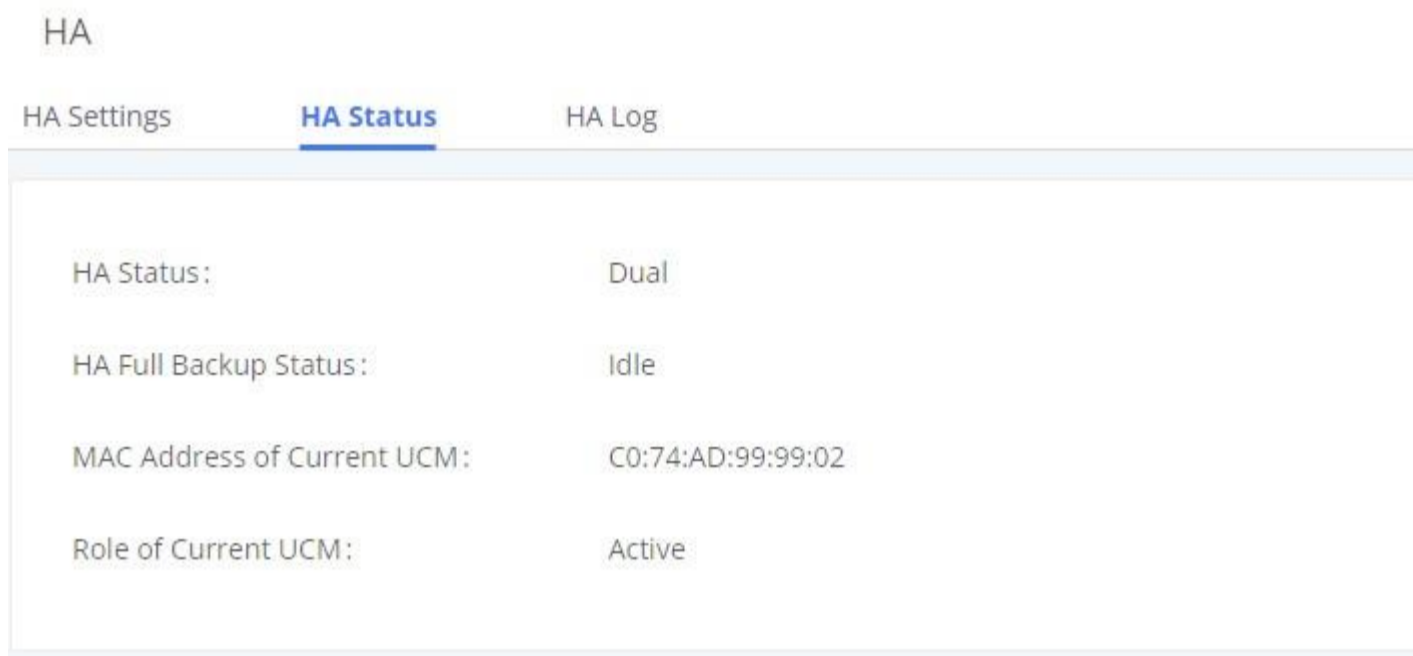
| Parameter | Description |
|-------------------------------------|--|
| High Available Enable | Enables/disables the HA functionality. By default, is Disabled. |
| Force switch | After clicking the button, the active/standby switch will be enforced. |
| HA Station Type | The master and slave static configuration of the device, The real active / standby is decided dynamically by the active / standby. |
| HA Virtual IP | To carry the service, the main and standby computers should be set the same, and the intranet terminal should register and use the IP address. |
| HA Peer IP | Local IP address of HA peer device. |
| HA Peer MAC Address | Need to specify this peer MAC address while using the UCM RemoteConnect service. |
| Heartbeat Port | The number of the heartbeat port should be consistent with the peer heartbeat port. |
| Heartbeat Timeout Period (s) | If timeout occurs, services will be transferred over to the Slave UCM. |

| Parameter | Description |
|------------------------------|---|
| Software Fault Switch | Enable Software Fault Switch |
| Hardware Fault Switch | If issues are detected with the selected connection interfaces, the backup UCM6510 will take over services after the master/slave handover. If not checked, UCM will send only a fault alarm. |
| Enable IPv6 | If enabled, HA on UCM can be used with IPv6 while compatible with IPv4. |

Table 27: HA Settings parameters

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 Status: | Dual |
| HA Full Backup Status: | Idle |
| MAC Address of Current UCM: | C0:74:AD:99:99:02 |
| Role of Current UCM: | Active |

Figure 58: 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.

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:

Figure 59: 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 Cancel Save

* Name:

* Access Level:

Figure 60: 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

Cancel Save

* Name:

* IP Address:

* Port:

* Community: ▼

* Type: ▼

Figure 61: 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: <ul style="list-style-type: none"> • 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

* Authentication Password:

* Privacy Protocol: DES

* Privacy Password:

* Group Level: Read Only

Figure 62: SNMP v3

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

SNMP Trap Proxy

Create New SNMP Trap Proxy

Cancel

Save

* Name:

* IP Address:

* Port:

Figure 63: 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

* Radius Shared Secret 🔒

* Maximum Number of Retransmission

* Radius Timeout (s)

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 server Default 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. |
| Periodic Inform Enable | Enables periodic inform. If set to 'Yes', device will send inform packets to the ACS. |
| Periodic Inform Interval | Periodic time when UCM630xA will send inform packets to TR-069 ACS server. This option is specified in seconds. |
| ACS Connection Request Username | The username for the ACS to connect to UCM. |
| ACS Connection Request Password | The password for the ACS to connect to UCM. |
| Connection Request Port | Port for incoming connection requests. The default value is 7547 . |
| CPE Cert File | The Cert file for UCM to connect to the ACS via SSL. |
| CPE Cert Key | The Cert key for UCM to connect to the ACS via SSL. |

PROVISIONING

Overview

Grandstream SIP Devices can be configured via Web interface as well as via configuration file through TFTP/HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file and XML format configuration file. The UCM630xA provides a Plug and Play mechanism to auto-provision the Grandstream SIP devices in a zero-configuration manner by generating XML config file and having the phone to download it within LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

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

Configuration Architecture for End Point Device

Started from firmware version 1.0.7.10, the end point device configuration in zero config is divided into the following three layers with priority from the lowest to the highest:

- **Global**

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

- **Model**

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

- **Device**

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

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

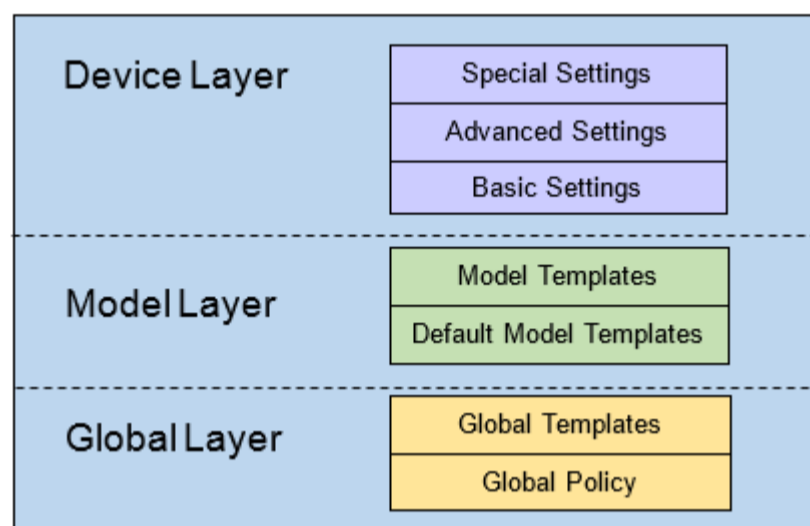


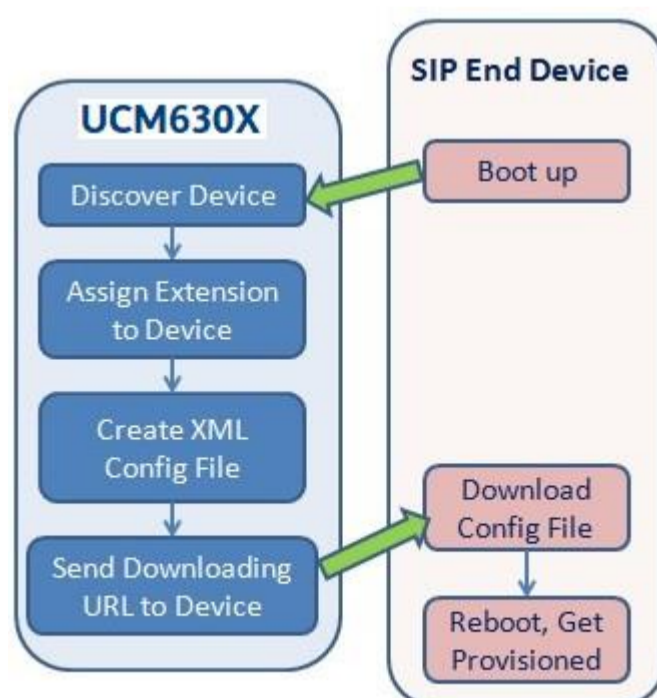
Figure 64: Zero Config Configuration Architecture for End Point Device

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

After understanding the zero-config configuration architecture, users could configure the available options for end point devices to be provisioned by the UCM630xA by going through the three layers. This configuration architecture allows users to set up and manage the Grandstream end point devices in the same LAN area in a centralized way.

Auto Provisioning Settings

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



◦ **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.

◦ **mDNS**

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

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

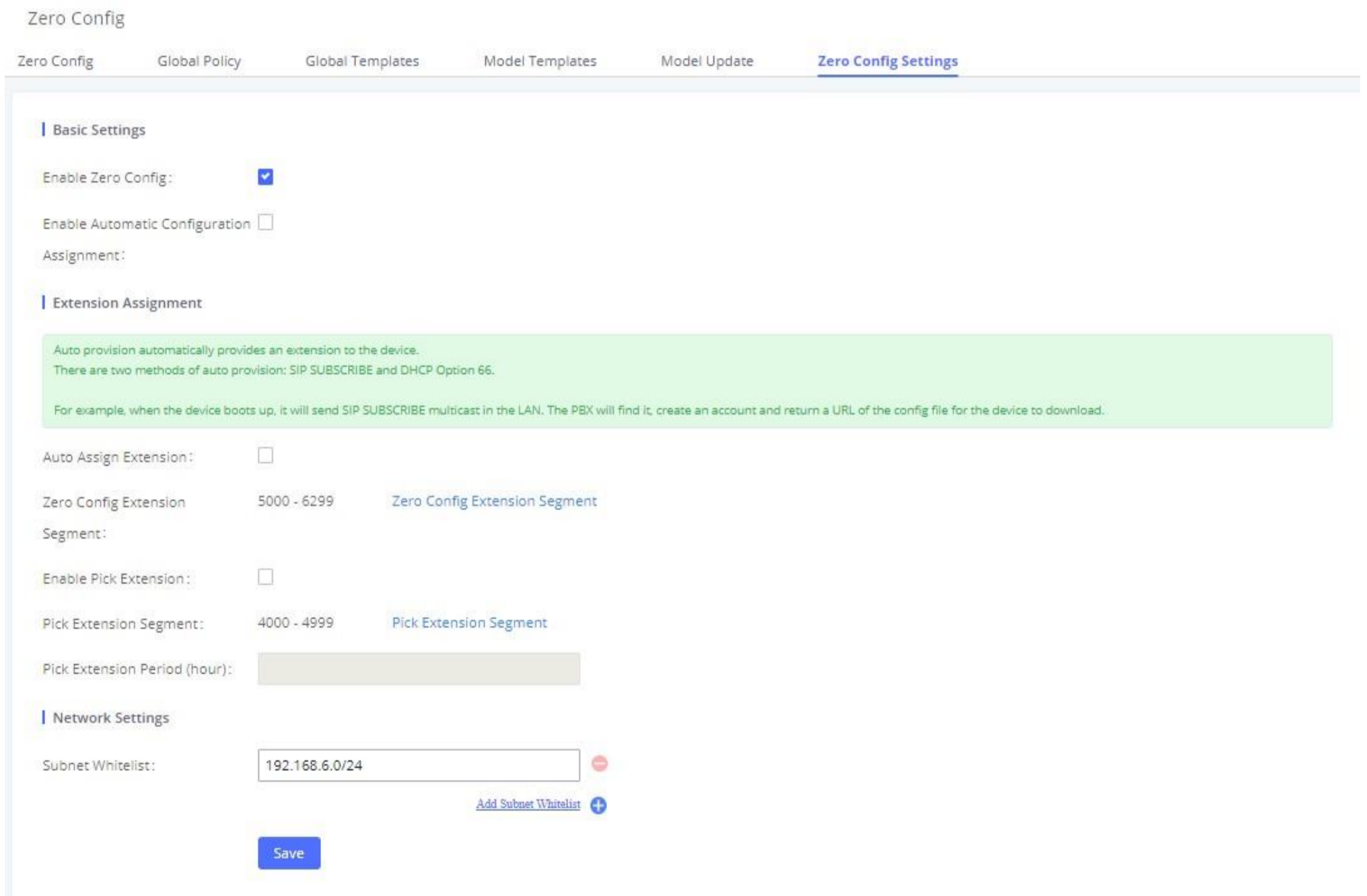


Figure 66: Auto Provision Settings

| | |
|---------------------------|---|
| Enable Zero Config | Enable or disable the zero-config feature on the PBX. The default setting is enabled. |
|---------------------------|---|

| | |
|--|---|
| Enable Automatic Configuration Assignment | <p>By default, this is disabled. If disabled, when SIP device boots up, the UCM630xA will not send the SIP device the URL to download the config file and therefore the SIP device will not be automatically provisioned by the UCM630xA.</p> <p>Note: When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the UCM630xA which will include the XML config file URL for the SIP device to download.</p> |
| Auto Assign Extension | If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in “Zero Config Extension Segment” to the device. The default setting is disabled. |
| Zero Config Extension Segment | Click on the link “Zero Config Extension Segment” to specify the extension range to be assigned if “Automatically Assign Extension” is enabled. The default range is 5000-6299. Zero Config Extension Segment range can be defined in Web GUI→ PBX Settings → General Settings → General page→Extension Preference section: “Auto Provision Extensions”. |
| Enable Pick Extension | If enabled, the extension list will be sent out to the device after receiving the device’s request. This feature is for the GXP series phones that support selecting extension to be provisioned via phone’s LCD. The default setting is disabled. |
| Pick Extension Segment | Click on the link “Pick Extension Segment” to specify the extension list to be sent to the device. The default range is 4000 to 4999. Pick Extension Segment range can be defined in Web GUI → PBX Settings → General Settings → General page → Extension Preference section: “Pick Extensions”. |
| Pick Extension Period (hour) | Specify the number of minutes to allow the phones being provisioned to pick extensions. |
| Subnet Whitelist | <p>This feature allows the UCM to provision devices in different subnets other than UCM network.</p> <p>Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is <IP>/<CIDR>.</p> <p>Examples:</p> <p>10.0.0.1/8</p> <p>192.168.6.0/24</p> <p>Note: Only private IP ranges (10.0.0.0 172.16.0.0 192.168.0.0) are supported.</p> |

Table 28: Auto Provision Settings

Please make sure an extension is manually assigned to the phone or “Automatically Assign Extension” is enabled during provisioning. After the configuration on the UCM630xA Web GUI, click on “Save” and “Apply Changes”. Once the phone boots up and picks up the config file from the UCM630xA, it will take the configuration right away.

Discovery

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

- PING
- ARP
- SIP Message (NOTIFY)

Click on “Auto Discover” under Web GUI→Other Features→Zero Config→Zero Config, fill in the “Scan Method” and “Scan IP”. The IP address segment will be automatically filled in based on the network mask detected on the UCM630xA. If users need scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address. Then click on “Save” to start discovering the devices within the same network. To successfully discover the devices, “Zero Config” needs to be enabled on the UCM630xA Web GUI→Other Features→Zero Config→Auto Provisioning Settings.

Auto Discover [X]

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

PBX LAN/LAN1: 192.168.5.147

Address:

Network Segment: 192.168.5.0 - 192.168.5.255

Broadcast IP: 192.168.5.255

Scan Method: SIP-Message

Subnet Whitelist: Local Subnet Only

Scan IP: 192 . 168 . 5 . 137

Cancel OK

Figure 67: Auto Discover

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

| <input type="checkbox"/> | MAC ADDRESS | IP ADDRESS | EXTENSION | VERSION | VENDOR | MODEL | CREATE CONFIG | OPTIONS |
|--------------------------|--------------|-------------------------------|-----------|-------------|-------------|---------|---------------|--|
| <input type="checkbox"/> | 000B82000001 | 192.168.2.111 | 1000 | unknown | GRANDSTREAM | GXV3275 | -- | [Edit] [Delete] [Update] [Reboot] [Access] |
| <input type="checkbox"/> | 000B8227FB15 | 192.168.2.108 | -- | 1.0.3.208 | GRANDSTREAM | GXV3275 | -- | [Edit] [Delete] [Update] [Reboot] [Access] |
| <input type="checkbox"/> | 000B82A46ACE | 192.168.2.106 | -- | 1.0.0.36 | GRANDSTREAM | -- | -- | [Edit] [Delete] [Update] [Reboot] [Access] |
| <input type="checkbox"/> | 000B82D33AC4 | 192.168.2.105 | -- | 20.19.10.30 | GRANDSTREAM | -- | -- | [Edit] [Delete] [Update] [Reboot] [Access] |
| <input type="checkbox"/> | 000B82F66470 | 192.168.2.107 | -- | 10.19.9.26 | GRANDSTREAM | -- | -- | [Edit] [Delete] [Update] [Reboot] [Access] |

Figure 68: Discovered Devices

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

Auto Discover

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

Interface: LAN 1

PBX Network Interface IP Address :

Network Segment: 192.168.50.0 - 192.168.50.255

Auto Discover LAN1/LAN2

Firmware

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

Firmware Storage Path : Local

Firmware List

[Upload](#)

| NAME | MODEL | FIRMWARE VERSION | DATE | SIZE | STATUS | OPTIONS |
|------|-------|------------------|------|------|--------|---------|
|------|-------|------------------|------|------|--------|---------|

No Data

Upload New Firmware



* Enable:



Model:

Firmware Version:

Remark:

Choose File to Upload

:

Cancel

Upload

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

Uploading Devices List

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

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

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

Figure 69: Device List – CSV file Sample

Managing Discovered Devices

- Sorting: Press or to sort per MAC Address, IP Address, Version, Vendor, Model or Create Config columns from lower to higher or higher to lower, respectively.

- Filter: Select a filter

Filter:

to display corresponding results.

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

Zero Config

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

Auto Discover | + Add | Delete | Edit | Update Config | Reboot | More

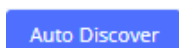
Filter: All

| | MAC ADDRESS | IP ADDRESS | EXTENSION | VERSION | VENDOR | MODEL | CREATE CO... | OPTIONS |
|-------------------------------------|--------------|-------------------------------|-----------|-----------|-------------|---------|----------------|---------|
| <input checked="" type="checkbox"/> | 000B825C59CB | 192.168.5.183 | -- | 1.0.9.148 | GRANDSTR | 2140 | -- | |
| <input type="checkbox"/> | 000B8262583D | 192.168.5.179 | -- | 1.0.9.25 | GRANDSTREAM | GXP2130 | -- | |
| <input type="checkbox"/> | 000B826B1A63 | 192.168.5.160 | -- | 1.0.3.225 | GRANDSTREAM | GXV3240 | 2021-01-18 ... | |
| <input type="checkbox"/> | 000B826F91E3 | 192.168.5.113 | -- | 1.0.1.106 | GRANDSTREAM | -- | -- | |
| <input type="checkbox"/> | 000B827119B5 | 192.168.5.37 | -- | 1.0.3.23 | GRANDSTREAM | -- | -- | |

Figure 70: Managing Discovered Devices

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

- Click on



in order to access to the discovery menu as shown on [Discovery] section.

- Click on

Add

to add a new device to zero config database using its MAC address.

- Click on

Delete

to delete selected devices from the zero-config database.

- Click on

Edit

to modify selected devices.

- Click on

Update Config

to batch update a list of devices, the UCM on this case will send SIP NOTIFY message to all selected devices in order to update them at once.

- Click on

Reboot

to reboot selected devices (the selected devices, should have been provisioned with extensions since the phone will authenticate the server which is trying to send it reboot command).

- Click on

Reset

to clear all devices configurations.

- Click on

Import

to upload CSV file containing list of devices.

- Click on

Export

to export CSV file containing list of devices. This file can be imported to another UCM to quickly set it up with the original UCM's devices.

- Click on

Copy


to copy configuration from one device to another. This can be useful for easily replace devices and note that this feature works only between devices of same model.

All these operations will be detailed on the next sections.

Global Configuration

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

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

 Global Templates configuration has higher priority to Global Policy configuration.

Global Policy

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

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

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



Figure 71: Global Policy Categories

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

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

Table 29: Global Policy Parameters – Localization

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

| | |
|---------------------------------|---|
| Enable Call Features | When enabled, “Do Not Disturb”, “Call Forward” and other call features can be used via the local feature code on the phone. Otherwise, the ITSP feature code will be used. |
| Use # as Dial Key | If set to “Yes”, pressing the number key “#” will immediately dial out the input digits. |
| Auto Answer by Call-info | If set to “Yes”, the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info header sent from the server/proxy. The default setting is enabled. |
| NAT Traversal | Configure if NAT traversal mechanism is activated. |
| User Random Port | If set to “Yes”, this parameter will force random generation of both the local SIP and RTP ports. |
| General Settings | |
| Call Progress Tones | Configure call progress tones including ring tone, dial tone, second dial tone, message waiting tone, ring back tone, call waiting tone, busy tone and reorder tone using the following syntax: f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; <ul style="list-style-type: none"> ◦ Frequencies are in Hz and cadence on and off are in 10ms). ◦ “on” is the period (in ms) of ringing while “off” is the period of silence. Up to three cadences are supported. ◦ Please refer to user manual of the SIP devices to be provisioned for more details |
| HEADSET Key Mode | Select “Default Mode” or “Toggle Headset/Speaker” for the Headset key. Please refer to user manual of the SIP devices to be provisioned for more details. |

Table 30: Global Policy Parameters – Phone Settings

| | |
|-----------------------|--|
| LDAP Phonebook | |
| Source | Select “Manual” or “PBX” as the LDAP configuration source. <ul style="list-style-type: none"> ◦ 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 UCM630xA 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: <ul style="list-style-type: none"> ◦ dc=grandstream, dc=com ◦ ou=Boston, dc=grandstream, dc=com |

| | |
|----------------------------|---|
| Username | Configure the bind “Username” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds. |
| Password | Configure the bind “Password” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds. |
| Number Filter | Configure the filter used for number lookups. Please refer to user manual for more details. |
| Name Filter | Configure the filter used for name lookups. Please refer to user manual for more details. |
| Version | Select the protocol version for the phone to send the bind requests. The default value is 3. |
| Name Attribute | Specify the “name” attributes of each record which are returned in the LDAP search result. Example: gn cn sn description |
| Number Attribute | Specify the “number” attributes of each record which are returned in the LDAP search result. Example: telephoneNumber telephoneNumber Mobile |
| Display Name | Configure the entry information to be shown on phone’s LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber |
| Max Hits | Specify the maximum number of results to be returned by the LDAP server. Valid range is 1 to 3000. The default value is 50. |
| Search Timeout | Specify the interval (in seconds) for the server to process the request and client waits for server to return. Valid range is 0 to 180. Default value is 30. |
| Sort Results | Specify whether the searching result is sorted or not. Default setting is No. |
| Incoming Calls | Configure to enable LDAP number searching when receiving calls. The default setting is No. |
| Outgoing Calls | Configure to enable LDAP number searching when making calls. The default setting is No. |
| Lookup Display Name | Configures the display name when LDAP looks up the name for incoming call or outgoing call. It must be a subset of the LDAP Name Attributes. |
| XML Phonebook | |

| | |
|---|--|
| Phonebook XML Server | <p>Select the source of the phonebook XML server.</p> <ul style="list-style-type: none"> ◦ Disable <p>Disable phonebook XML downloading.</p> <ul style="list-style-type: none"> ◦ Manual <p>Once selected, users need specify downloading protocol HTTP, HTTPS or TFTP and the server path to download the phonebook XML file. The server path could be IP address or URL, with up to 256 characters.</p> <ul style="list-style-type: none"> ◦ Local UCM Server <p>Once selected, click on the Server Path field to upload the phonebook XML file. Please note after uploading the phonebook XML file to the server, the original file name will be used as the directory name and the file will be renamed as phonebook.xml under that directory.</p> |
| Phonebook Download Interval | <p>Configure the phonebook download interval (in Minute). If set to 0, automatic download will be disabled. Valid range is 5 to 720.</p> |
| Remove manually edited entries on download | <p>If set to “Yes”, when XML phonebook is downloaded, the entries added manually will be automatically removed.</p> |

Table 31: Global Policy Parameters – Contact List

| | |
|------------------------------|---|
| Upgrade and Provision | |
| Firmware Source | <p>Firmware source via ZeroConfig provisioning could a URL for external server address, local UCM directory or USB media if plugged in to the UCM630xA. Select a source to get the firmware file:</p> <ul style="list-style-type: none"> ◦ URL <p>If select to use URL to upgrade, complete the configuration for the following four parameters: “Upgrade Via”, “Server Path”, “File Prefix” and “File Postfix”.</p> <ul style="list-style-type: none"> ◦ Local UCM Server <p>Firmware can be uploaded to the UCM630xA internal storage for firmware upgrade. If selected, click on “Manage Storage” icon next to “Directory” option, upload firmware file and select directory for the end device to retrieve the firmware file.</p> <ul style="list-style-type: none"> ◦ Local USB Media <p>If selected, the USB storage device needs to be plugged into the UCM630xA and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory.</p> <ul style="list-style-type: none"> ◦ Local SD Card Media <p>If selected, an SD card needs to be plugged into the UCM630xA and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory.</p> |

| | |
|--|--|
| 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 | <p>If enabled, the end point device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week or by minute.</p> <ul style="list-style-type: none"> ◦ By week <p>Once selected, specify the day of the week to check HTTP/TFTP server for firmware upgrades or configuration files changes.</p> <ul style="list-style-type: none"> ◦ By day <p>Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes.</p> <ul style="list-style-type: none"> ◦ By minute <p>Once selected, specify the interval X that the SIP end device will request for new firmware every X minutes.</p> |
| Firmware Upgrade Rule | Specify how firmware upgrading and provisioning request to be sent. |
| Zero Config | Select either to enable or disable zero config. |
| Web Access | |
| Admin Password | Configure the administrator password for admin level login. |
| End-User Password | Configure the end-user password for the end user level login. |
| Web Access Mode | Select HTTP or HTTPS as the web access protocol. |
| Web Server Port | <p>Configure the port for web access.</p> <p>The valid range is 1 to 65535.</p> |
| RTSP Port | Configure the RTSP Port. |
| Enable UPnP Discovery | Select either to enable or disable Enable UPnP Discovery |
| Login Settings | Configure the login settings. |
| User Login Timeout | Configure User Login Timeout. |
| Maximum Consecutive Failed Login Attempts | Configure Maximum Consecutive Failed Login Attempts. |
| Login Error Lock Time | Configure Login Error Lock Time. |
| Security | |

| | |
|---------------------------|--|
| Disable Telnet/SSH | Enable Telnet/SSH access for the SIP end device. If the SIP end device supports Telnet access, this option controls the Telnet access of the device; if the SIP end device supports SSH access, this option controls the SSH access of the device. |
| Syslog | |
| Syslog Server | Configure the URL/IP address for the syslog server. |
| Syslog Level | Select the level of logging for syslog. |
| Send SIP Log | Configure whether the SIP log will be included in the syslog message. |

Table 32: Global Policy Parameters – Maintenance

| | |
|----------------------------|---|
| Basic Settings | |
| IP Address | <p>Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected.</p> <ul style="list-style-type: none"> ◦ DHCP <p>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.</p> <ul style="list-style-type: none"> ◦ PPPoE <p>Once selected, users need specify the Account ID, Password and Service Name for PPPoE.</p> |
| Host Name | Specifies the name of the client. This field is optional but may be required by Internet Service Providers. |
| Vendor Class ID | Used by clients and servers to exchange vendor class ID. |
| Account ID | Enter the PPPoE account ID. |
| Password | Enter the PPPoE Password. |
| Service Name | Enter the PPPoE Service Name. |
| Advanced Setting | |
| Layer 3 QoS | Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0-63. |
| Layer 3 QoS For RTP | <p>Assign the priority value of the Layer 3 QoS for RTP packets.</p> <p>Valid range is 0 -63.</p> |
| Layer 3 QoS For SIP | <p>Assign the priority value of the Layer 3 QoS for SIP packets.</p> <p>Valid range is 0 -63.</p> |
| Layer 2 QoS Tag | <p>Assign the VLAN Tag of the Layer 2 QoS packets.</p> <p>Valid range is 0 -4095.</p> |

| | |
|-------------------------------------|---|
| Layer 2 QoS Priority Value | Assign the priority value of the Layer 2 QoS packets. Valid range is 0-7. |
| STUN Server | Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN. |
| Keep Alive | Select either to enable or disable Keep Alive. |
| Keep Alive Interval | Specify how often the phone will send a blank UDP packet to the SIP server in order to keep the “ping hole” on the NAT router to open. Valid range is 10-160. |
| Register Expiration | Specify the Register Expiration. |
| Local SIP Port | Configure Local SIP Port. |
| Local RTP Port | Configure Local RTP Port. |
| Auto On-Hook Timer(s) | Configure Auto On-Hook Timer(s). |
| Ring Timeout | Configure Ring Timeout. |
| SIP Transport | Select either UDP, TCP or TLS/TCP as SIP transport protocol. |
| Direct IP Call | Select either to disable or enable Direct IP Call support. |
| SIP Proxy Compatibility Mode | Select either to disable or enable SIP Proxy Compatibility Mode. |
| Unregister On Reboot | Select either to disable or enable Unregister On Reboot. |
| Whitelist | |
| Whitelist | Select either to enable or disable Whitelist |
| SIP Phone Number Whitelist | Configure the SIP Phone Number Whitelist. |

Table 33: Global Policy Parameters – Network Settings

| | |
|-------------------------------------|--|
| Wallpaper | |
| Screen Resolution 1024 x 600 | <p>Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> ◦ Source <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> ◦ File <p>If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM630xA.</p> |

| | |
|---|---|
| <p>Screen Resolution 800 x 400</p> | <p>Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> ◦ Source <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> ◦ File <p>If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM630xA.</p> |
| <p>Screen Resolution 480 x 272</p> | <p>Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> ◦ Source <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> ◦ File <p>If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM630xA.</p> |
| <p>Screen Resolution 320 x 240</p> | <p>Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> ◦ Source <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"> ◦ File <p>If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM630xA.</p> |

Table 34: Global Policy Parameters – Customization

| |
|------------------------------|
| <p>Email Settings</p> |
|------------------------------|

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

| | |
|---|--|
| FTP | Check this option to configure the FTP settings that will be sent to the provisioned phones: |
| | <ul style="list-style-type: none"> ◦ Storage Server Type |
| | Either FTP or Central Storage |
| | <ul style="list-style-type: none"> ◦ Server |
| | FTP server address |
| | <ul style="list-style-type: none"> ◦ Port |
| | FTP port to be used |
| <ul style="list-style-type: none"> ◦ Username | |
| FTP username | |
| <ul style="list-style-type: none"> ◦ Path | |
| FTP Directory path | |

Table 35: Global Policy Parameters – Communication Settings

Global Templates

Global Templates can be accessed in Web GUI→**Other Features**→**Zero Config**→**Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates. Later on, when the user configures the device in Edit Device dialog→Advanced Settings, the user can select to use one of the global templates for the device. Please refer to section *[Manage Devices]* for more details on using the global templates.

When creating global template, users can select the categories and the parameters under each category to be used in the template. The global policy and the selected global template will both take effect when generating the config file. However, the selected global template has higher priority to the global policy when it comes to the same setting option/field. If the same option/field has different value configured in the global policy and the selected global template, the value for this option/field in the selected global template will override the value in global policy.

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

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

Table 36: Create New Template

- Click on



to edit the global template.

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

Edit Global Templates: test

* Template Name:









Description:

Active:

Options:

Phone Settings

Default Call Settings

| | | | |
|---|-----------------------|---|--|
|  | Dial Plan: |  | <input type="text" value="{ x+ *x+ *xx*x+ }"/> |
|  | Enable Call Features: |  | <input type="text" value="Yes"/> |
|  | Use # as Dial Key: |  | <input type="text" value="Yes"/> |
|  | Auto Answer by Call- |  | <input type="text" value="No"/> |

Info:

Figure 72: Edit Global Template

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



to delete this option from the template. On the right side of each option, users can click on



to reset the option value to the default value.

Click on “Save” to save this global template.

- The created global templates will show in the Web GUI→Other Features→Zero Config→Global Templates page. Users can click on



to delete the global template or delete multiple selected templates at once.

- Click on “Toggle Selected Template(s)” to toggle the status between enabled/disabled for the selected templates.

Model configuration

Model templates

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

For each created model template, users can assign it as default model template. If assigned as default model template, the values in this model template will be applied to all the devices of this model. There is always only one default model template that can be assigned at one time on the UCM630xA.

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

- Click on “Add” to add a model template.

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

Table 37: Create New Model Template

- Click on



to edit the model template.

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

Once added, the option will be shown in the list below. On the left side of each option, users can click on



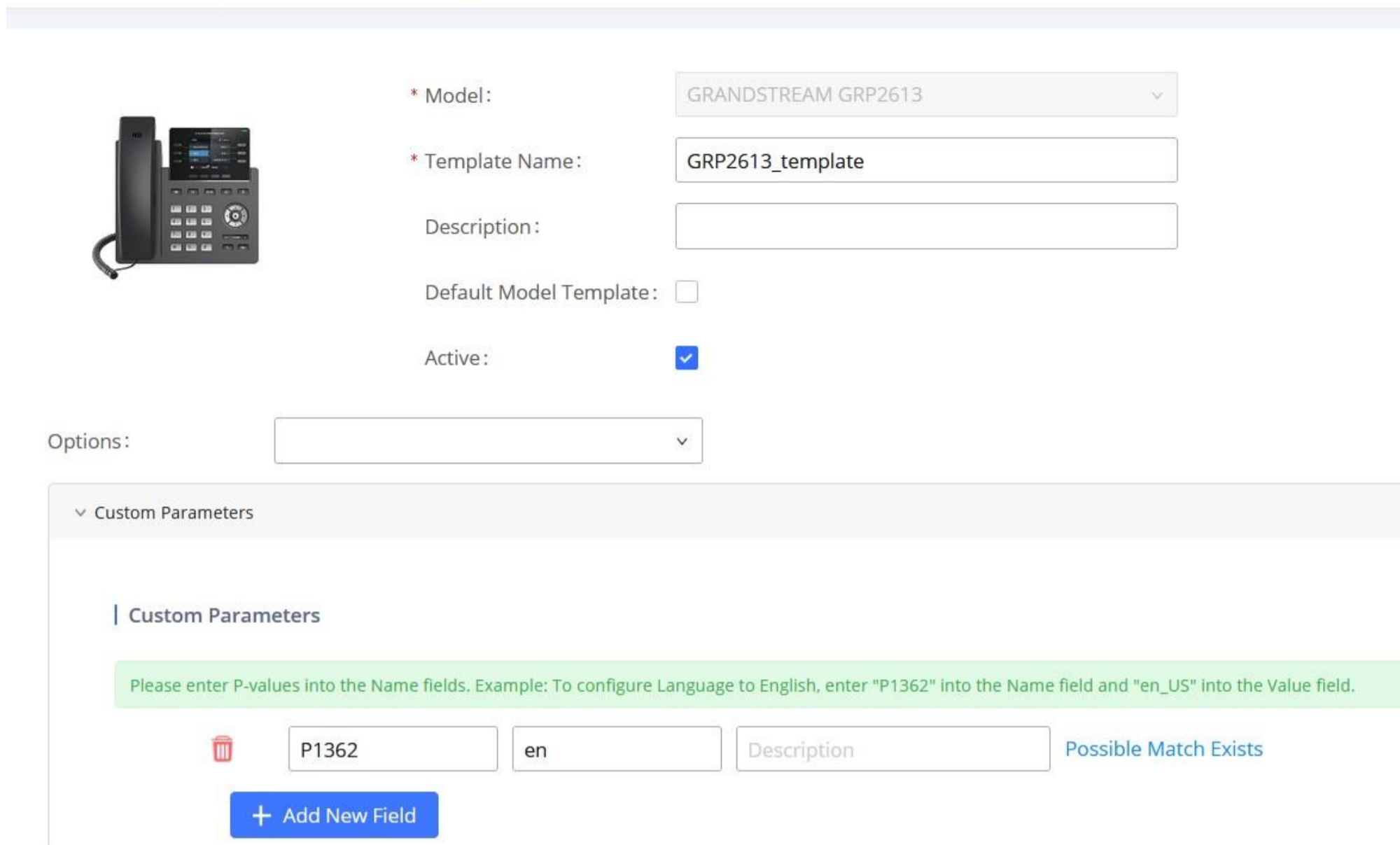
to remove this option from the model template. On the right side of each option, users can click on



to reset the option to the default value.

User could also click on “Add New Field” to add a P value number and the value to the configuration. The following figure shows setting P value “P1362” to “en”, which means the display language on the LCD is set to English. For P value information of different models, please refer to configuration template here <https://www.grandstream.com/support/tools>

Edit Model Templates: GRP2613_template



* Model: GRANDSTREAM GRP2613

* Template Name: GRP2613_template

Description:

Default Model Template:


Active:

Options:

Custom Parameters


Custom Parameters

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

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

+ Add New Field

Figure 73: Edit Model Template

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


Model Update

UCM630xA zero config feature supports provisioning all models of Grandstream SIP end devices including OEM device models.

OEM Models

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

- Click on



button.

- In the *Source Model* field, select the Grandstream device that the OEM model is based on from the dropdown list.
- For the *Destination Model* and *Destination Vendor* field, enter the custom OEM model name and vendor name.

- The newly added OEM model should now be selectable as an option in *Model* fields.

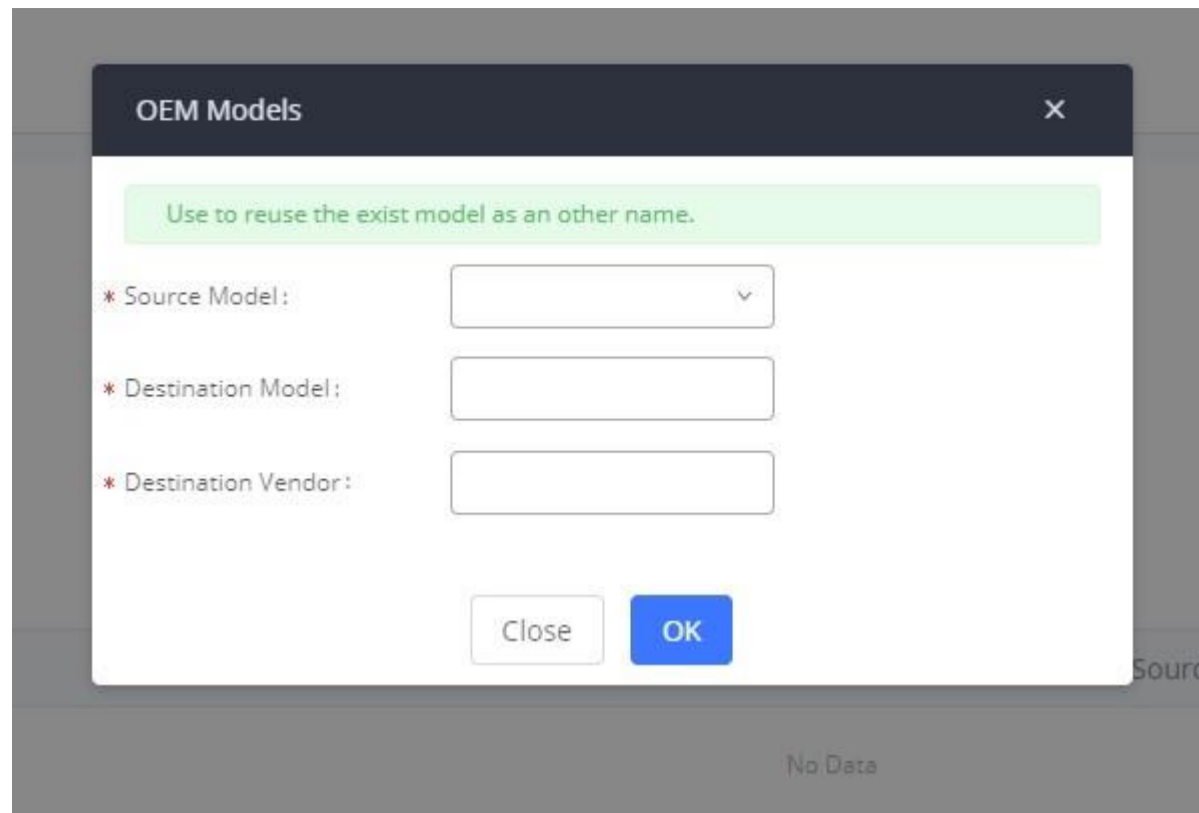


Figure 74: OEM Models

Model Template Package List

Templates for most of the Grandstream models are built in with the UCM630xA already. Templates for Grandstream Wave and Grandstream surveillance products require users to download and install under Web GUI→**Other Features**→**Zero Config**→**Model Update** first before they are available in the UCM630xA for selection. After downloading and installing the model template to the UCM630xA, it will show in the dropdown list for “Model” selection when editing the model template.

- Click on



to download the template.

- Click on



to upgrade the model template. Users will see this icon available if the device model has template updated in the UCM630xA.

Model Template Package List

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

Figure 75: Template Management

Upload Model Template Package

In case the UCM630xA is placed in the private network and Internet access is restricted, users will not be able to get packages by downloading and installing from the remote server. Model template package can be manually uploaded from local device through Web GUI. Please contact Grandstream customer support if the model package is needed for manual uploading.

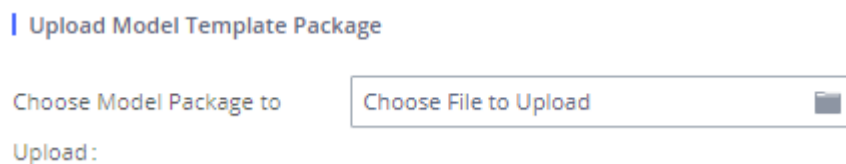


Figure 76: Upload Model Template Manually

Device Configuration

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

Create New Device

Besides configuring the device after the device is discovered, users could also directly create a new device and configure basic settings before the device is discovered by the 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.

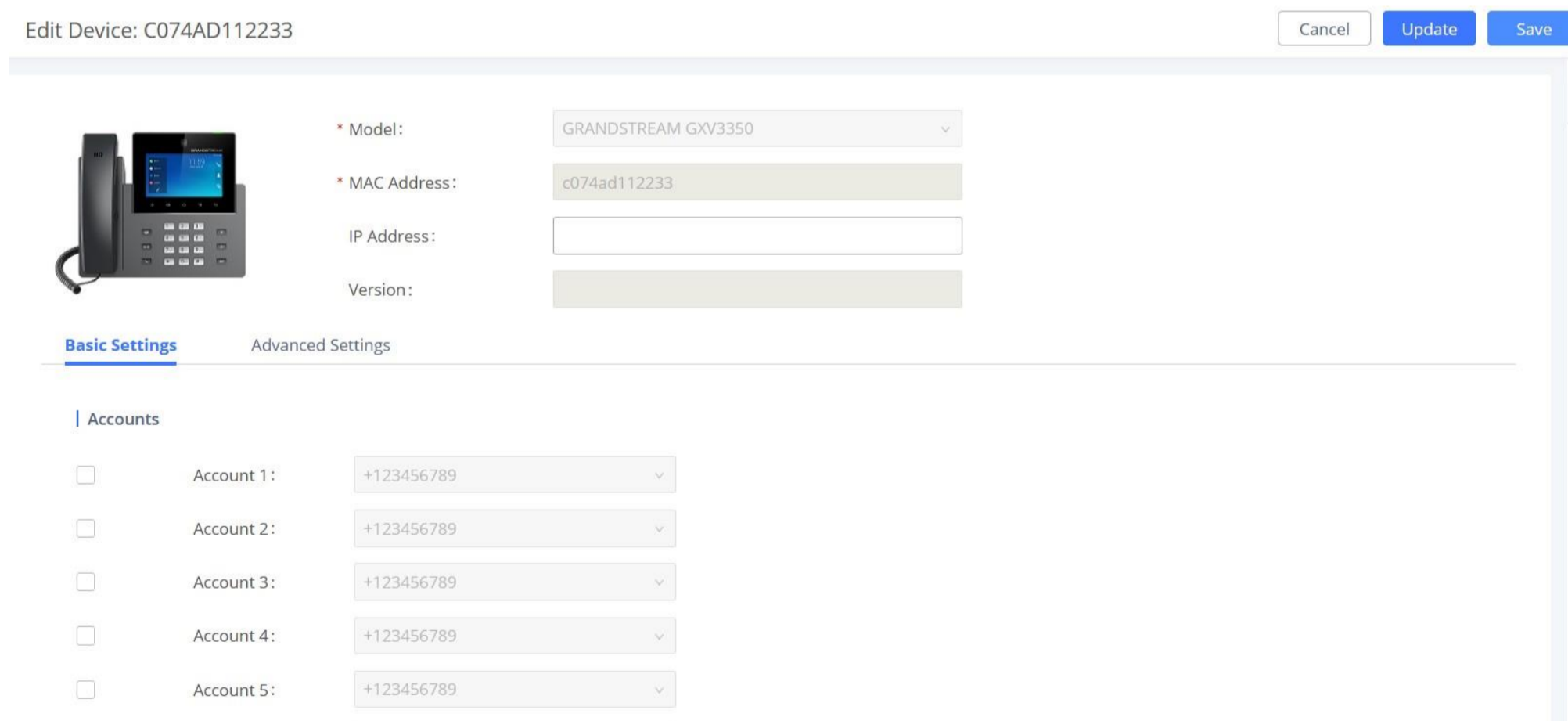


Figure 77: Create New Device

Manage Devices

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







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

Figure 78: Manage Devices

- Click on



to access the Web GUI of the phone.


- Click on



to edit the device configuration.

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

Edit Device: 000B8273C559



* Model:

* MAC Address:

IP Address:

Version:

Basic Settings
Advanced Settings

5 Custom Device Settings

[Modify Custom Settings](#)

4 Model Templates

0 item Idle
None

<
>
↑
^
↓
v

0 Selected
None

3 Default Model Template

Preview

Figure 79: Edit Device

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

1. Global Policy

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

2. Global Templates

Select a global template to be used for the device and click on



to add. Multiple global templates can be selected, and users can arrange the priority by adjusting orders via



and



. All the selected global templates will take effect. If the same option exists on multiple selected global templates, the value in the template with higher priority will override the one in the template with lower priority. Click on



to remove the global template from the selected list.

3. Default Model Template

Default Model Template will be applied to the devices of this model. Default model template can be configured in model template under Web GUI→**Other Features**→**Zero Config**→**Model Templates** page. Please see default model template option in *[Table 37: Create New Model Template]*.

4. Model Templates

Select a model template to be used for the device and click on



to add. Multiple model templates can be selected, and users can arrange the priority by adjusting orders via



and



. All the selected model templates will take effect. If the same option exists on multiple selected model templates, the value in the template with higher priority will override the one in the template with lower priority. Click on



to remove the model template from the selected list.

5. Customize Device Settings

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



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

Custom Fields

Custom Fields

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

Possible Match Exists

Figure 80: Edit Customize Device Settings

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


https://content.grandstream.com/hubfs/Grandstream_Feb_2021/Zip%20File/config-template.zip?hsLang=en

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

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

Modify Selected Devices Cancel Save

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

 * Model: GXV3275
 MAC Address: 000B82000001 x 000B8227FB15 x

Basic Settings | Advanced Settings

Programmable MPK Settings

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

Figure 81: Modify Selected Devices – Same Model

If selected devices are of different models, the configuration dialog is like the following figure. Click on



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

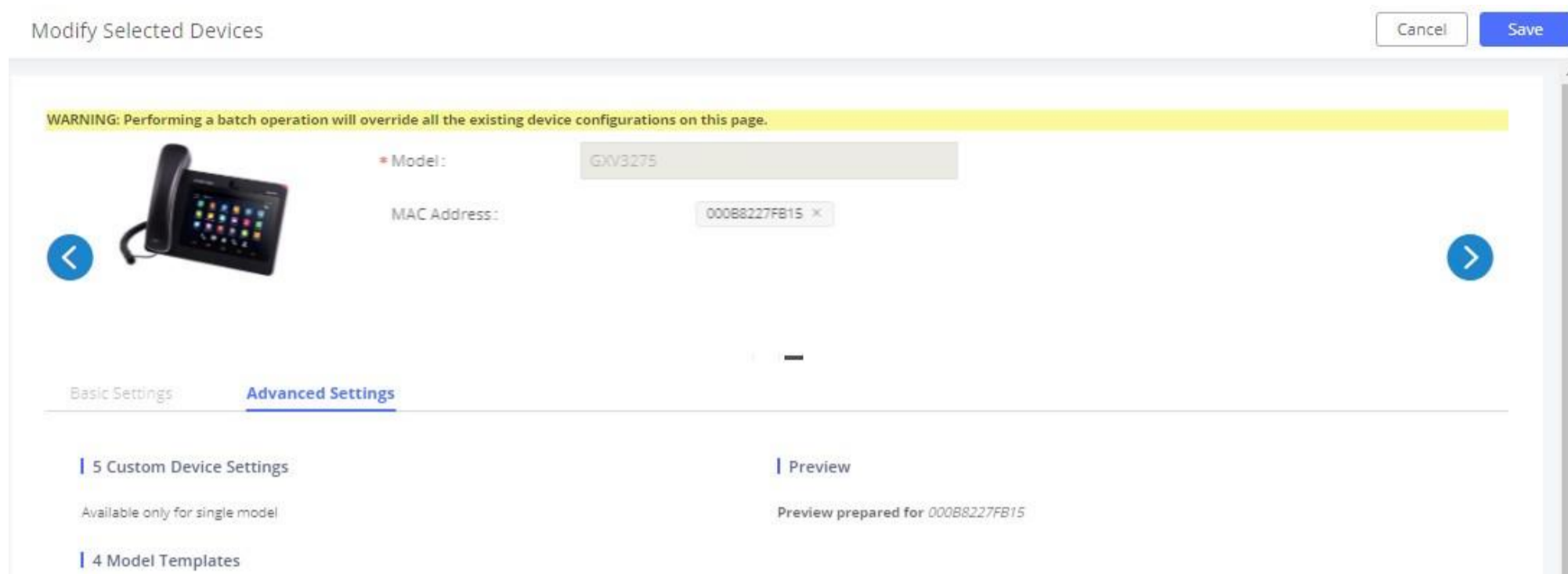


Figure 82: Modify Selected Devices – Different Models

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

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



to send NOTIFY to the SIP end point device and trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.

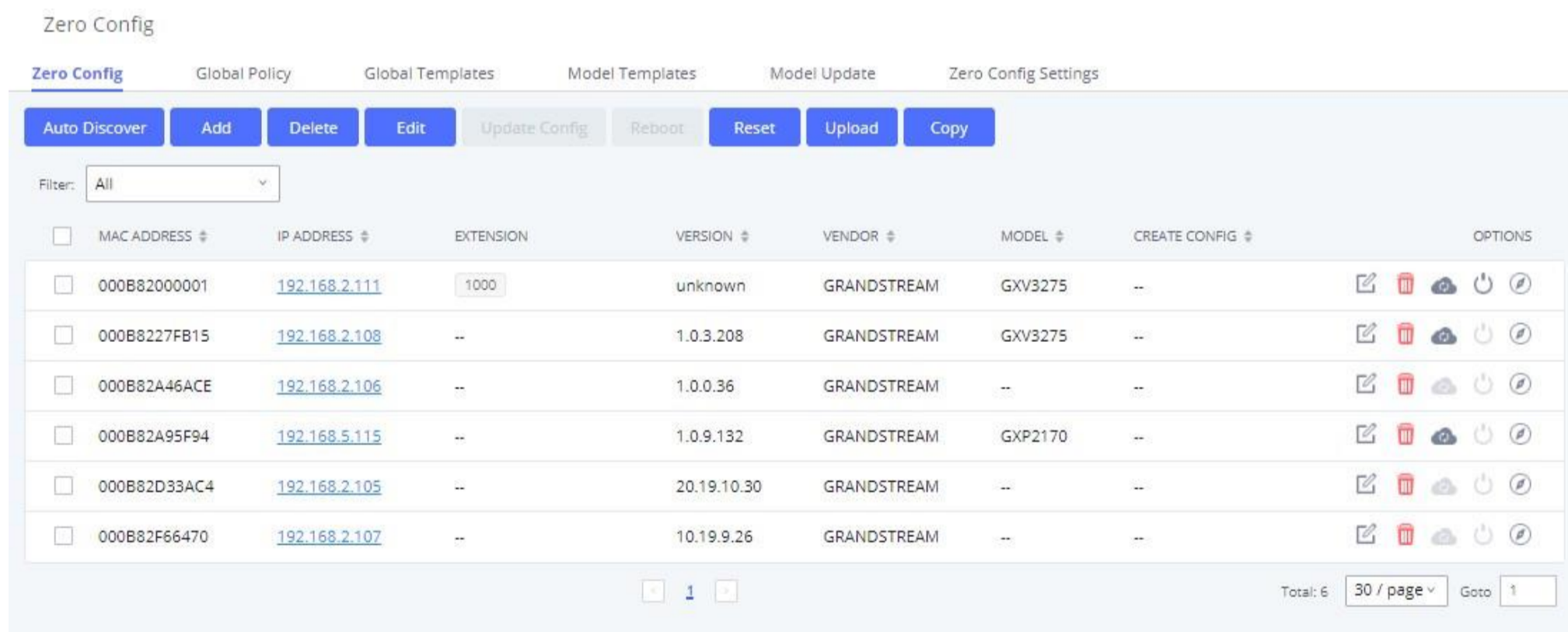


Figure 83: Device List in Zero Config

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

Sample Application

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

1. Go to Web GUI→Other Features→Zero Config→Zero Config Settings, select “Enable Zero Config”.

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

Localization

Language Settings

* Language: English

Date and Time

Date Format: yyyy-mm-dd

Time Format: 12-hour Clock

Enable NTP: Disabled

NTP Server:

NTP Update Interval: 1440

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

Enable Daylight Saving Time: Disabled

Phone Settings

Contact List

Maintenance

Upgrade and Provision

Firmware Source:

Source: URL


Upgrade via: TFTP

Server Path: fm.grandstream.com/gs

File Prefix:

File Postfix:

Figure 84: Zero Config Sample – Global Policy

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

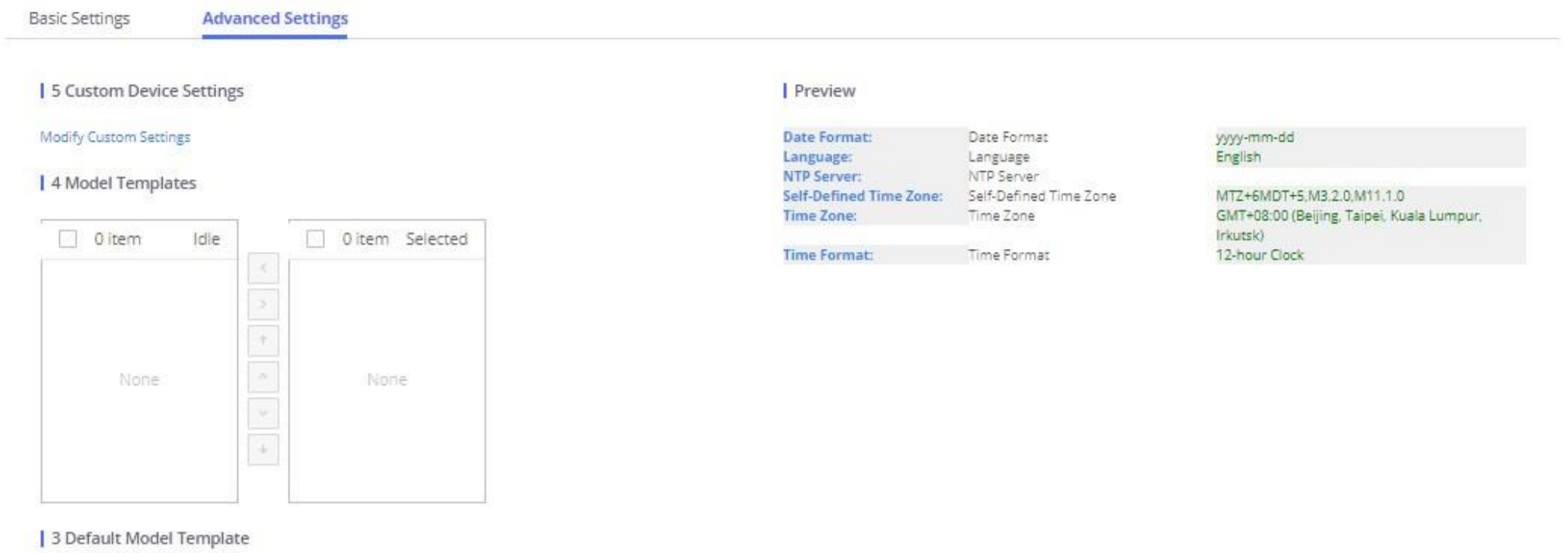


Figure 85: Zero Config Sample – Device Preview 1

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

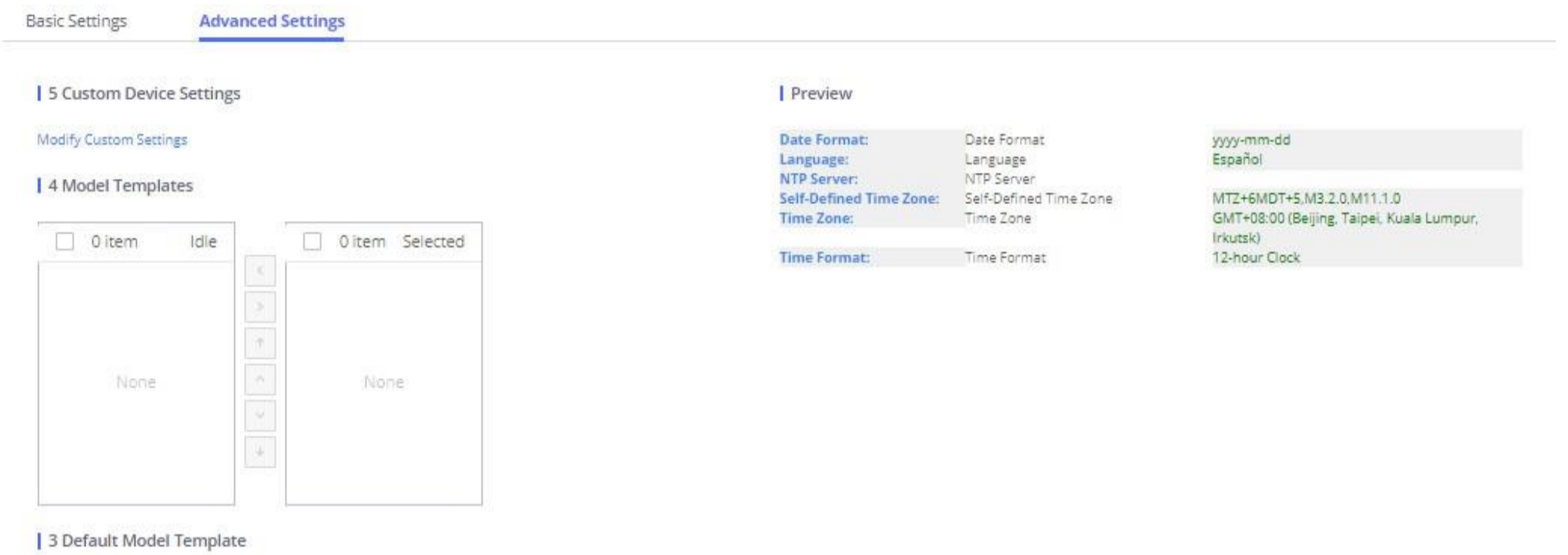


Figure 86: Zero Config Sample – Device Preview 2

Select “Spanish Support Template” in “Model Template”. The preview of the device settings is displayed on the right side and we can see the language is set to “Español” since Model Template has the higher priority for the option “Language”, which overrides the value configured in default model template.

9. For the GXV3275 used by the customer support supervisor, select an available extension for account 1 on “Basic settings” and click on “Save”. Users can see the preview of the device configuration in “Advanced settings”. There is no model template configured for GXV3275.

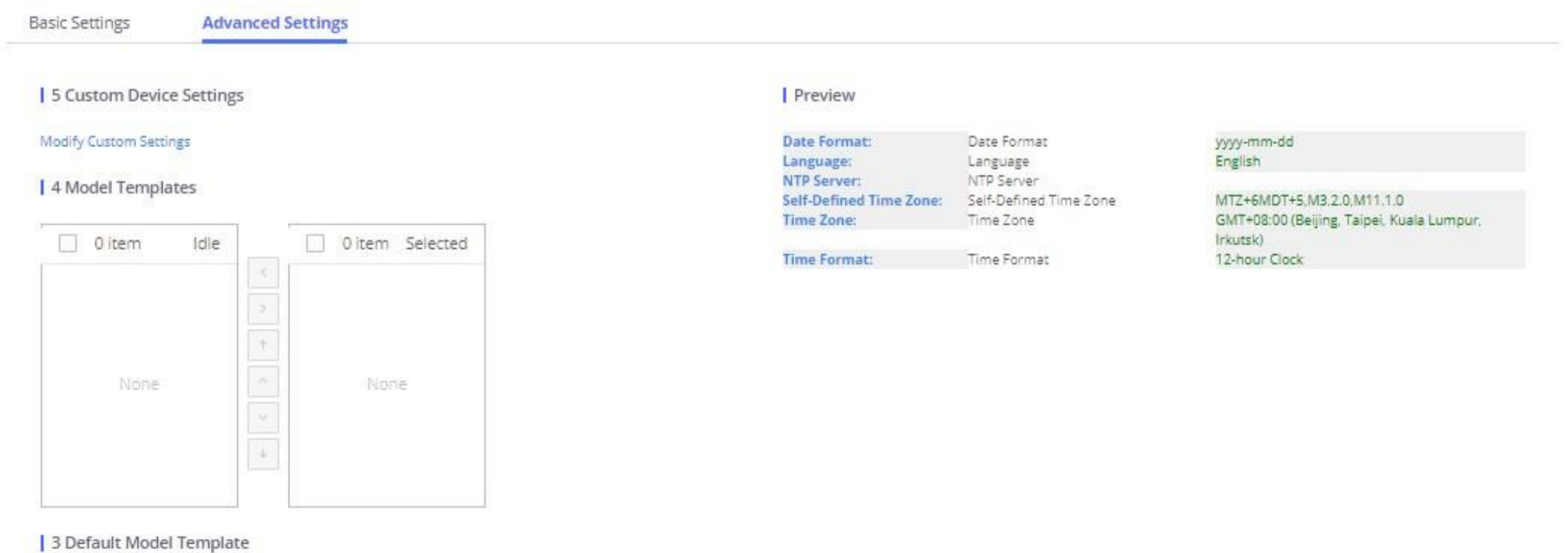


Figure 87: Zero Config Sample – Device Preview 3

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

11. On the Web GUI→Other Features→Zero Config→Zero Config page, click on



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

Now all the 9 phones in the network will be provisioned with a unique extension registered on the UCM630xA. 3 of the phones will be provisioned to display Spanish on LCD and the other 5 will be provisioned to display English on LCD. The GXV3275 used by the supervisor will be provisioned to use the default language on LCD display since it is not specified in the global policy.

EXTENSIONS

Create New User

Create New SIP Extension

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

Create New Extension

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

Cancel Save

* Select Extension Type: SIP Extension

Select Add Method: Single

General

* Extension: 1005

* Privilege: Internal

AuthID:

* Voicemail Password: 1161554273

Send Voicemail Email Notification: Default

Enable Keep-alive:

Disable This Extension:

Emergency CID:

CallerID Number:

* SIP/IAX Password: %27JbN@r8

Voicemail: Local Voicemail

Skip Voicemail Password Verification:

Attach Voicemail to Email: Default

Keep Voicemail after Emailing: Default

* Keep-alive Frequency: 60

Enable SCA:

Enable Wave:

Sync Contact:

User Settings

First Name:

Last Name:

Figure 88: Create New Device

Extension options are divided into four categories:

- Basic Settings
- Media
- Features

- Specific Time
- Follow me

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

| General | |
|---|--|
| 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. |
| 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". <ul style="list-style-type: none"> ● 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 Call Features → Voicemail → Voicemail Email Settings will be used. |
| Keep Voicemail after Emailing | Whether to keep the local voicemail recording after sending them. If set to "Default", the global settings will be used. Note: When set to "Default", the global settings in Call Features → Voicemail → Voicemail Email Settings will be used. |

| | |
|---------------------------------|--|
| Enable Keep-alive | If enabled, 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 Call Features→SCA page. |
| Emergency CID Name | CallerID name that will be used for emergency calls and callbacks. |
| Disable This Extension | If selected, this extension will be disabled on the UCM630X. Note: The disabled extension still exists on the PBX but cannot be used on the end device. |
| 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 Password | Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security 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 . |
| Concurrent Registrations | The maximum endpoints which can be registered into this extension. For security concerns, the default value is 1. |
| Mobile Phone Number | Configure the phone number for the extension, user can type the related star code for 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 | When enabled, The extension will inherit the same privilege attributed to the department it belongs to. |

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

| | |
|-----------------------------------|---|
| SIP Settings | |
| NAT | Use NAT when the UCM630X is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is 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 UCM630X 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 UCM630X to negotiate endpoint-to-endpoint media routing. The default setting is "No". |
| DTMF Mode | Select DTMF mode for the user to send DTMF. The default setting is "RFC4733". If "Info" is selected, 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. |
| 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. |
| SRTP | Enable SRTP for the call. The default setting is disabled. |
| Jitter Buffer | Select the jitter buffer method. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● 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 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. |
| FECC | Configure to enable Remote Camera Management. |
| ACL Policy | <p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> ● 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. |
| SRTP Crypto Suite | <p>The following encryption protocols can be used to encrypt an RTP stream.</p> <ul style="list-style-type: none"> ● AES_CM_128_HMAC_SHA1_80 (This is the default used protocol) ● AES_256_CM_HMAC_SHA1_80 ● AEAD_AES_128_GCM ● AEAD_AES_256_GCM |
| 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 | |
| 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]. |
| Internal Calls & External Calls | |
| Call Forward Unconditional | <p>Enable and configure the Call Forward Unconditional target number. Available options for target number are:</p> <ul style="list-style-type: none"> ● “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. <p>The default setting is “None”.</p> |
| CFU Time Condition | <p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● “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. |

| | |
|--------------------------------------|--|
| <p>Call Forward No Answer</p> | <p>Configure the Call Forward No Answer target number. Available options for target number are:</p> <ul style="list-style-type: none"> ● “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. <p>The default setting is “None”.</p> |
| <p>CFN Time Condition</p> | <p>Select time condition for Call Forward No Answer. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● “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. |
| <p>Call Forward Busy</p> | <p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"> ● “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: <p>The default setting is “None”.</p> |
| <p>CFB Time Condition</p> | <p>Select time condition for Call Forward Busy. The available time conditions ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● “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. |
| <p>Do Not Disturb</p> | <p>If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.</p> |
| <p>DND Time Condition</p> | <p>Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> |

| | |
|---|--|
| | <ul style="list-style-type: none"> • “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. <p>Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</p> |
| DND Whitelist | <p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"> • Z match any digit from 1-9. • N match any digit from 2-9. • X match any digit from 0-9. |
| FWD Whitelist | <p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> • 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 | <p>If enabled, UCM630X will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.</p> |
| CC Mode | <p>Two modes for Call Completion are supported:</p> <ul style="list-style-type: none"> • Normal: This extension is used as an ordinary extension. • For Trunk: This extension is registered from a PBX. <p>The default setting is “Normal”.</p> |
| CC Max Agents | <p>Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel can make.</p> <p>The minimum value is 1.</p> |
| CC Max Monitors | <p>Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time.</p> <p>The minimum value is 1.</p> |
| Ring Simultaneously | |
| Ring Simultaneously | <p>Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.</p> |
| External Number | <p>Set the external number to ring simultaneously. ‘-’ is the connection character that will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p> |
| Time Condition for Ring Simultaneously | <p>Ring the external number simultaneously along with the extension based on this time condition.</p> |

| | |
|---|---|
| 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 | |
| Call Monitoring Whitelist | 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 UCM 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 UCM630X. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device. |
| Auto Record | Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under Web GUI→CDR→Recording Files . |
| Skip Trunk Auth | <ul style="list-style-type: none"> • 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. |
| Call Duration Limit | Check to enable and set the call limit the duration. |
| Maximum Call Duration (s) | The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds |
| The Maximum Number of Call Lines | The maximum number of simultaneous calls that the extension can have. 0 indicates no limit. |
| Outgoing Call Frequency Limit | If enabled, if the number of outbound calls exceed the configured threshold within the specified period, further outbound calls will be not be allowed. |
| Send PCPID Header | If enabled, this extension's SIP INVITE messages will contain the P-Called-Party-ID (PCPID) header if the callee is a SIP device. |
| Period (m) | The period of outgoing call frequency limit. The valid range is from 1 to 120. The default value is 1. |
| 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: <ul style="list-style-type: none"> ● 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 specific time for this extension. |

Table 41: SIP Extension Configuration Parameters→Specific Time

Table 42:

| 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. |

Table 42: 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 | <p>Configure Voicemail.</p> <p>There are three valid options, and the default option is “Enable Local Voicemail”.</p> <ul style="list-style-type: none"> • 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 | <p>If selected, this extension will be disabled on the UCM630X.</p> <p>Note: The disabled extension still exists on the PBX but cannot be used on the end device.</p> |
| User Settings | |
| First Name | Configure the first name of the user. The first name can contain characters, letters, digits, and _. |
| Last Name | Configure the last name of the user. The last name can contain characters, letters, digits, and _. |
| Email Address | Fill in the Email address for the user. Voicemail will be sent to this Email address. |
| User Password | Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security 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 | <p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> • 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 | <p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Note:</p> <ul style="list-style-type: none"> • “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 | <p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “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 | <p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “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 | <p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"> • Z match any digit from 1-9. • N match any digit from 2-9. • X match any digit from 0-9. |
| FWD Whitelist | <p>Calls from users in the forward whitelist will not be forwarded.</p> <p>Pattern matching is supported.</p> <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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 | <p>If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are:</p> <ul style="list-style-type: none"> • 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.

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. |

| | |
|---|---|
| | <p>There are three valid options, and the default option is “Enable Local Voicemail”.</p> <ul style="list-style-type: none"> • 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 | <p>If selected, this extension will be disabled on the UCM630X.</p> <p>Note: The disabled extension still exists on the PBX but cannot be used on the end device.</p> |
| User Settings | |
| First Name | Configure the first name of the user. The first name can contain characters, letters, digits, and _. |
| Last Name | Configure the last name of the user. The last name can contain characters, letters, digits, and _. |
| Email Address | Fill in the Email address for the user. Voicemail will be sent to this Email address. |
| User Password | Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes. |
| Mobile Phone Number | Configure the Mobile number of the user. |

| | |
|-----------------|--|
| Language | <p>Select the voice prompt language to be used for this extension.</p> <p>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.</p> |
|-----------------|--|

| 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 | <p>For the FXS extension, there are three options available in Fax Mode. The default setting is “None”.</p> <ul style="list-style-type: 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 | <p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Note:</p> <ul style="list-style-type: none"> • “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 | <p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “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 | <p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “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 | <p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p> |
| DND Time Condition | The time condition of DND. The DND will take effect while the time condition is satisfied. |
| DND Whitelist | <p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"> • Z match any digit from 1-9. |

| | |
|---|---|
| | <ul style="list-style-type: none"> • N match any digit from 2-9. • X match any digit from 0-9. |
| FWD Whitelist | <p>Calls from users in the forward whitelist will not be forwarded.</p> <p>Pattern matching is supported.</p> <ul style="list-style-type: none"> • 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 | <p>Configure the Hotline Type:</p> <ul style="list-style-type: none"> • 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 | <p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM630X, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→Voice Prompt→Custom Prompt: General Preference.</p> <p>The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the endpoint also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p> |
| Auto Record | <p>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.</p> |
| Skip Trunk Auth | <ul style="list-style-type: none"> • 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 | <p>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.</p> |
| Dial Trunk Password | <p>Configure personal password when making outbound calls via the trunk.</p> |
| Enable LDAP | <p>If enabled, this extension will be added to the LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.</p> |
| Use MOH as IVR ringback tone | <p>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.</p> |
| Music On Hold | <p>Select which Music On Hold class to suggest to the extension when putting the active call on hold.</p> |
| Call Duration Limit | <p>Check to enable and set the call limit the duration.</p> |
| Maximum Call Duration (s) | <p>The maximum call duration (in seconds). The default value 0 means no limit. Max value is 86400 seconds</p> |
| Email Missed Calls | <p>Send a log of missed calls to the extension’s email address.</p> |
| Missed Call Type | <p>If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are:</p> <ul style="list-style-type: none"> • 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 | <p>Click to add Time Condition to configure a specific time for this extension.</p> |

| | |
|------------------|--|
| Follow Me | |
| Enable | <p>Configure to enable or disable Follow Me for this user.</p> |

| | |
|-------------------------------------|--|
| 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 | <p>Configure Voicemail.</p> <p>There are three valid options and the default option is “Enable Local Voicemail”.</p> <ul style="list-style-type: none"> ◦ 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 | <p>Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"> ◦ User Random Password. <p>A random secure password will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> ◦ Use Extension as Password. ◦ Enter a password to be used on all the extensions in the batch. |
| Voicemail Password | <p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"> ◦ User Random Password. <p>A random password in digits will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> ◦ Use Extension as Password. <p>Enter a password to be used on all the extensions in the batch.</p> |
| Send Voicemail to Email | <p>Send voicemail messages to the configured email address. If set to “Default”, the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.</p> |
| Keep Voicemail after Emailing | <p>Only applies if extension-level or global Send Voicemail to Email is enabled.</p> |
| CallerID Number | <p>Configure CallerID Number when adding Batch Extensions.</p> <ul style="list-style-type: none"> ◦ 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 | <p>When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.</p> |
| Enable Keep-alive | <p>If enabled, the PBX will regularly send SIP OPTIONS to check if host device is online.</p> |
| Keep-alive Frequency | <p>Configure the keep-alive interval (in seconds) to check if the host is up.</p> |

| | |
|-----------------------------------|--|
| Disable This Extension | Check this box to disable this extension. |
| Enable SCA | If enabled, (1) Call Forward, Call Waiting and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Call Features->SCA page. |
| Emergency Calls CID | CallerID number that will be used when calling out and receiving direct callbacks. |
| 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. <ul style="list-style-type: none"> ◦ 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. <ul style="list-style-type: none"> ◦ 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 | <p>Select jitter buffer method.</p> <ul style="list-style-type: none"> ◦ 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 | <p>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].</p> |
| Call Forward Unconditional | <p>Enable and configure the Call Forward Unconditional target number. Available options for target number are:</p> <ul style="list-style-type: none"> ◦ “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. <p>The default setting is “None”.</p> |
| CFU Time Condition | <p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ “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. |

| | |
|--------------------------------------|--|
| <p>Call Forward No Answer</p> | <p>Configure the Call Forward No Answer target number. Available options for target number are:</p> <ul style="list-style-type: none"> ○ “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. <p>The default setting is “None”.</p> |
| <p>CFN Time Condition</p> | <p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ○ “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. |
| <p>Call Forward Busy</p> | <p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"> ○ “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. <p>The default setting is “None”.</p> |

| | |
|---------------------------|--|
| CFB Time Condition | <p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ “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 | <p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p> |
| DND Time Condition | <p>Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ “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. <p>Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</p> |
| DND Whitelist | <p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"> ◦ Z match any digit from 1-9 ◦ N match any digit from 2-9 ◦ X match any digit from 0-9. |
| FWD Whitelist | <p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> ◦ 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 | <p>If enabled, UCM630xA will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.</p> |

| | |
|---|---|
| CC Mode | <p>Two modes for Call Completion are supported:</p> <ul style="list-style-type: none"> ◦ Normal: This extension is used as ordinary extension. ◦ For Trunk: This extension is registered from a PBX. <p>The default setting is “Normal”.</p> |
| 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 | <p>Set the external number to be rang simultaneously. ‘-’ is the connection character which will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p> |
| 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 | <p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM630xA, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→Voice Prompt→Custom Prompt: General Preference. The valid range is between 3 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p> |

| | |
|---|--|
| 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 | <ul style="list-style-type: none"> ◦ 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 | <p>If disabled, UCM will not invite the extension when it is already in a call and will do the same work as the user is busy.</p> <p>Note: the option only works when the caller dials the extension directly.</p> |

Table 53: 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 | <p>Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”.</p> <p>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.</p> |
| 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 | <p>Configure Voicemail. There are three valid options and the default option is “Enable Local Voicemail”.</p> <p>Disable Voicemail: Disable Voicemail.</p> <p>Enable Local Voicemail: Enable voicemail for the user.</p> |
| SIP/IAX Password | <p>Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"> ◦ User Random Password. <p>A random secure password will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> ◦ Use Extension as Password. ◦ Enter a password to be used on all the extensions in the batch. |
| Voicemail Password | <p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"> ◦ User Random Password. <p>A random password in digits will be automatically generated. It is recommended to use this password for security purpose.</p> <ul style="list-style-type: none"> ◦ Use Extension as Password. ◦ Enter a password to be used on all the extensions in the batch. |
| Send Voicemail to Email | <p>Send voicemail messages to the configured email address. If set to “Default”, the global setting will be used. Global settings can be found in Voicemail->Voicemail Email Settings.</p> |
| Keep Voicemail after Emailing | <p>Only applies if extension-level or global Send Voicemail to Email is enabled.</p> |
| Auto Record | <p>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.</p> |
| Skip Voicemail Password Verification | <p>When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.</p> |
| Disable This Extension | <p>Check this box to disable this extension.</p> |
| Language | <p>Select voice prompt language for this extension. If set to “Default”, the global setting for voice prompt language will be used.</p> |
| IAX Settings | |
| Max Number of Calls | <p>Configure the maximum number of calls allowed for each remote IP address.</p> |
| Require Call Token | <p>Configure to enable/disable requiring call token. If set to “Auto”, it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints.</p> <p>The default setting is “Yes”.</p> |
| SRTP | <p>Enable/disable SRTP for RTP stream encryption.</p> |

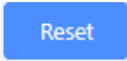
| | |
|-----------------------------------|---|
| ACL Policy | <p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"> ◦ Allow All: Any IP address can register to this extension. ◦ Local Network: Only IP addresses in the configured network 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 | <p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ “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 | <p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ “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 | <p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ “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 | <p>If Do Not Disturb is enabled, all incoming calls will be dropped.</p> <p>All call forward settings will be ignored.</p> |
| DND Time Condition | <p>Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ “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 | <p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"> ◦ Z match any digit from 1-9, ◦ N match any digit from 2-9, ◦ X match any digit from 0-9. |
| FWD Whitelist | <p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"> ◦ 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 | <p>Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.</p> |

| | |
|---|---|
| External Number | <p>Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p> |
| 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 | <p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM630xA, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→Voice Prompt→Custom Prompt: General Preference. The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p> |
| 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 | <ul style="list-style-type: none"> ◦ 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.

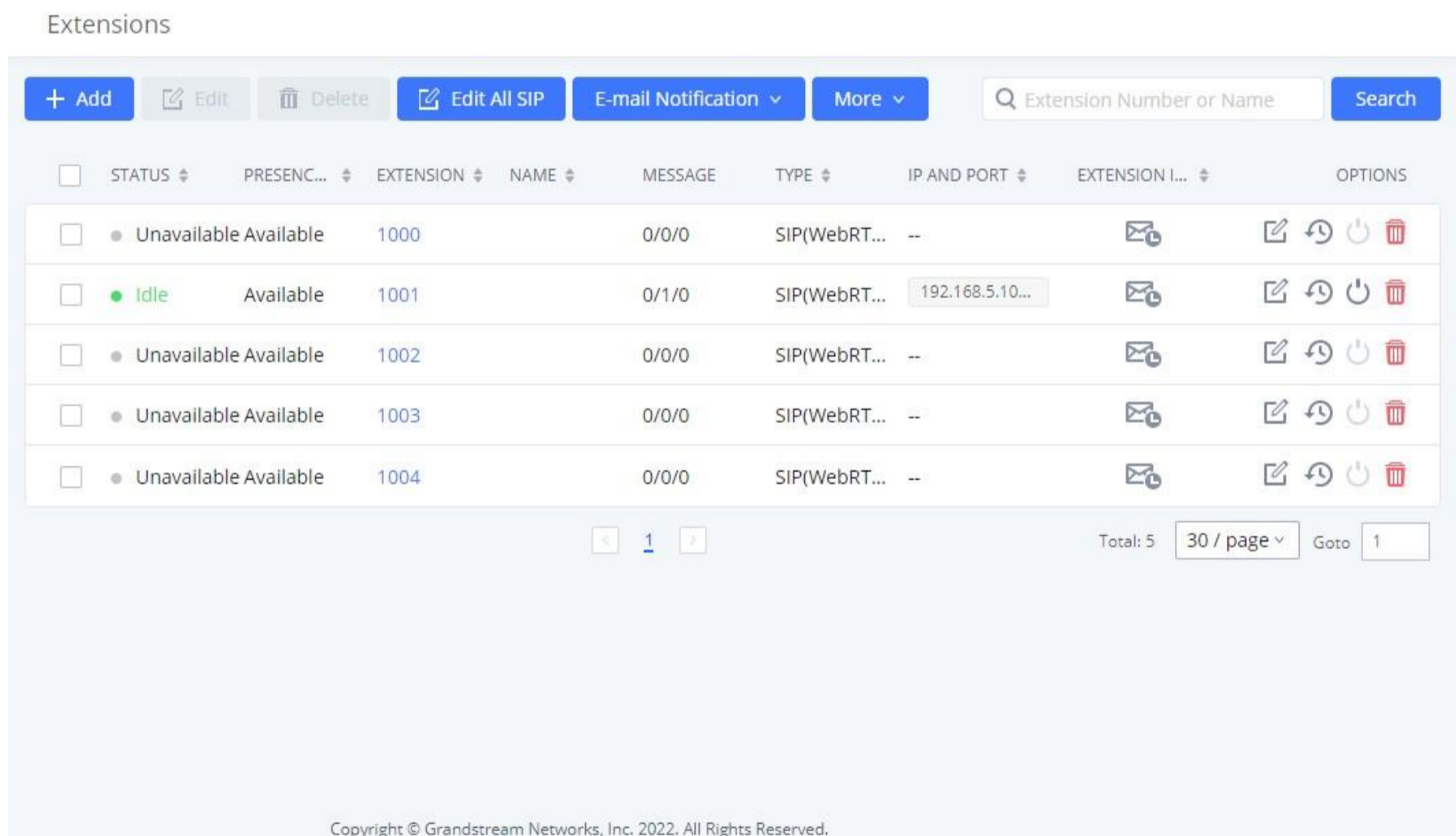


Figure 84: Manage Extensions

o Status

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



Green: Idle



Blue: Ringing

Yellow: In Use

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

- **Edit single extension**

Click on



to start editing the extension parameters.

- **Reset single extension**

Click on



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

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

 **Note**

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→ **Other Features→Zero Config→Zero Config Settings**.

- **Delete single extension**

Click on



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

 **Notes**

This is the expected behavior when you delete an extension:

- The system will delete all the data of the extension except the CDR and meetings record. All the data on the user side will be erased.

- The extension will be removed from group chats and the messages sent previously by the extension will be kept. However, only other users can search through those messages while the new user of the extension cannot.
- If the extension was in a meeting schedule, the meeting will still be present. The extension will be removed from the meeting and will not be notified about the meeting.

- **Modify selected extensions**

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

- **Delete selected extensions**

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

Export Extensions

The extensions configured on the UCM630xA can be exported to csv format file with selected technology “SIP”, “IAX” or “FXS”. Click on “Export Extensions” button and select technology in the prompt below.

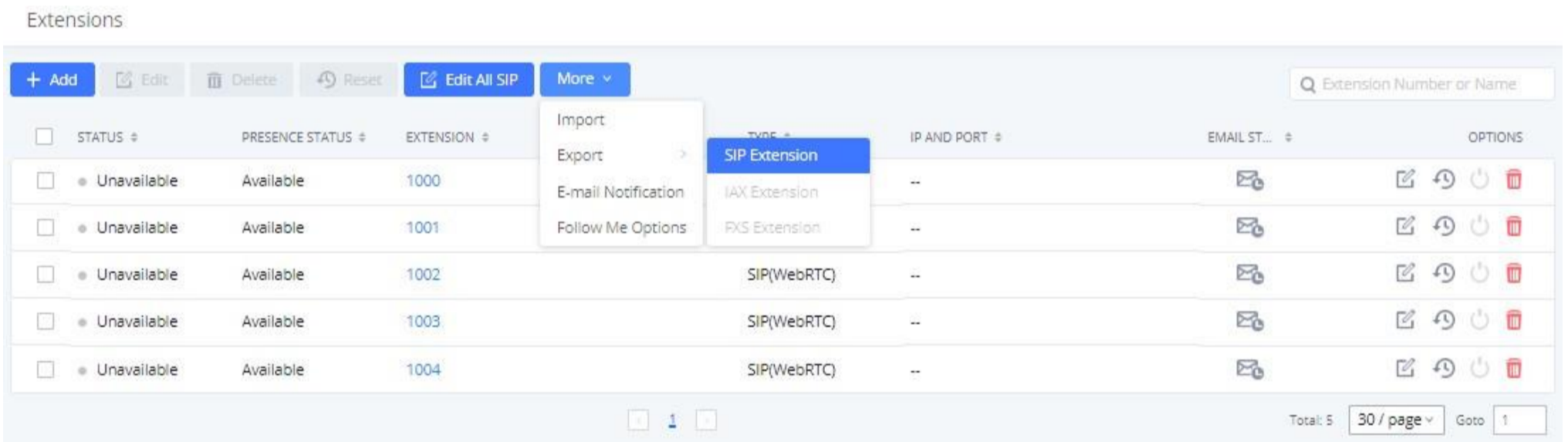


Figure 85: Export Extensions

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.

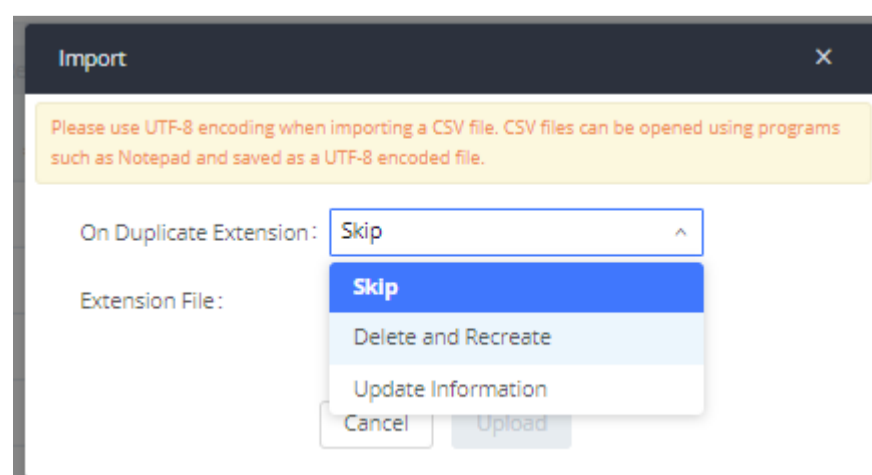


Figure 86: Import Extensions

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 | S RTP | 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 | | |

Figure 87: 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) |
| S RTP | yes/no |
| Strategy | Allow All/Local Subnet Only/A Specific IP Address |
| Local Subnet 1 | IP address/Mask |
| Local Subnet 2 | IP address/Mask |
| Local Subnet 3 | IP address/Mask |
| Local Subnet 4 | IP address/Mask |
| Local Subnet 5 | IP address/Mask |
| Local Subnet 6 | IP address/Mask |
| Local Subnet 7 | IP address/Mask |
| Local Subnet 8 | IP address/Mask |
| Local Subnet 9 | IP address/Mask |
| Local Subnet 10 | IP address/Mask |

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

| | |
|---|---|
| Time Condition for Skip Trunk Auth | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Enable LDAP | Yes/no |
| Enable T.38 UDPTL | Yes/no |
| Max Contacts | Values from 1-10 |
| Enable Wave | Yes/no |
| Alert-Info | None/Ring 1/Ring2/Ring3/Ring 4/Ring 5/Ring 6/Ring 7/ Ring 8/Ring 9/Ring 10/bellcore-dr1/bellcore-dr2/ bellcore-dr3/ bellcore-dr4/ bellcore-dr5/custom |
| Do Not Disturb | Yes/no |
| DND Time Condition | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Custom Auto answer | Yes/no |
| Do Not Disturb Whitelist | Empty/digits |
| User Password | Alphanumeric characters. |
| First Name | Alphanumeric without special characters. |
| Last Name | Alphanumeric without special characters. |
| Email Address | Email address |
| Language | Default/en/zh |
| Phone Number | Digits |
| Call-Barging Monitor | Extensions allowed to call barging |
| Seamless Transfer Members | Extensions allowed to seamless transfer |

Table 55: SIP extensions Imported File Example

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

| | |
|---|--|
| Local Subnet 5 | IP address/Mask |
| Local Subnet 6 | IP address/Mask |
| Local Subnet 7 | IP address/Mask |
| Local Subnet 8 | IP address/Mask |
| Local Subnet 9 | IP address/Mask |
| Local Subnet 10 | IP address/Mask |
| Specific IP Address | IP address |
| Skip Trunk Auth | yes/no/bytime |
| Codec Preference | PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus |
| Permission | Internal/Local/National/International |
| NAT | yes/no |
| Call Forward Busy | Digits |
| Call Forward No Answer | Digits |
| Call Forward Unconditional | Digits |
| Require Call Token | Yes/no/auto |
| Max Number of Calls | Values from 1-512 |
| Dial Trunk Password | Digits |
| Disable This Extension | Yes/no |
| CFU Time Condition | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| CFN Time Condition | |
| CFB Time Condition | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Music On Hold | Default/ringbacktone_default |
| Ring simultaneously | Yes/no |
| External Number | Digits |
| Time Condition for Ring Simultaneously | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Time Condition for Skip Trunk Auth | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Enable LDAP | Yes/no |
| Limit Max time (s) | empty |
| Do Not Disturb | Yes/no |
| DND Time Condition | All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time |
| Do Not Disturb Whitelist | Empty/digits |
| User Password | Alphanumeric characters. |
| First Name | Alphanumeric without special characters. |
| Last Name | Alphanumeric without special characters. |
| Email Address | Email address |

| | |
|----------------------------------|---|
| Language | Default/en/zh |
| Phone Number | Digits |
| Call-Barging Monitor | Extensions allowed to call barging |
| Seamless Transfer Members | Extensions allowed to seamless transfer |

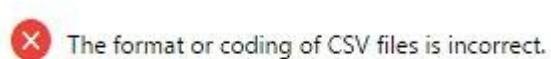
Table 56: IAX extensions Imported File Example

| 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 |

Table 57: FXS Extensions Imported File Example

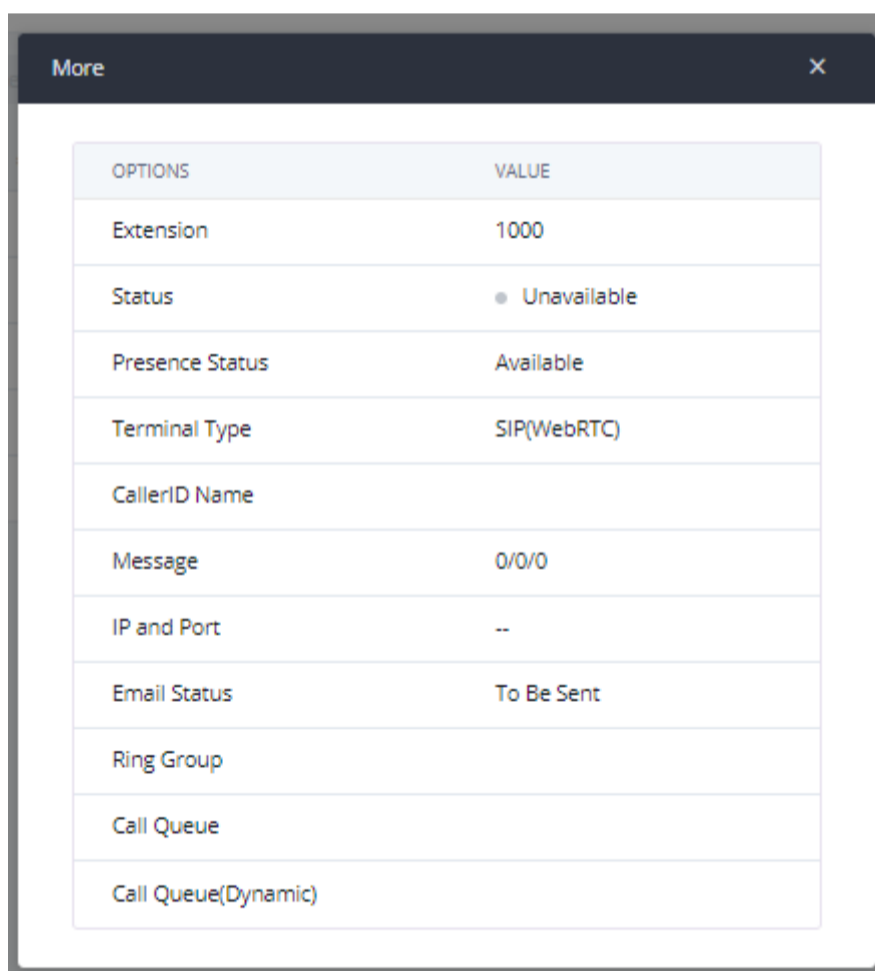
The CSV file should contain all the above fields, if one of them is missing or empty, the UCM630xA will display the following error message for missing fields.



Extension Details

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

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



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

Figure 89: 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.

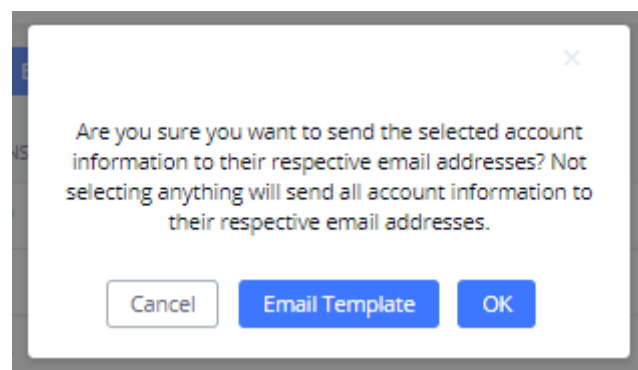


Figure 90: E-mail Notification – Prompt Information

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 |

Figure 91: Account Registration Information

GSWave Settings

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



Use Web App to scan qr code and log in

Figure 92: 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.

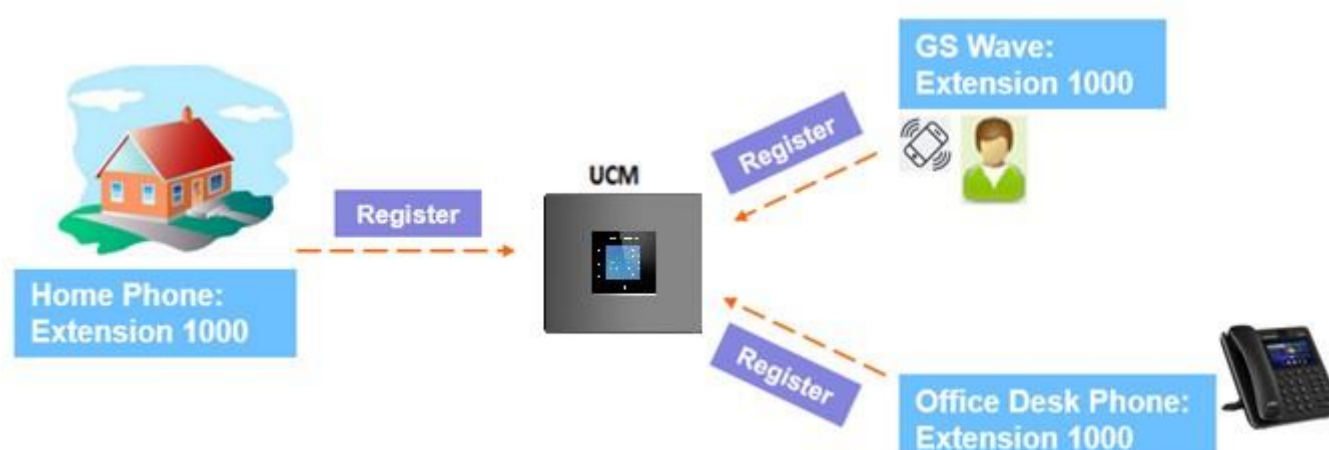


Figure 93: Multiple Registrations per Extension

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 CallerID Number: 1000

* Permission: Internal * SIP/IAX Password: *****

AuthID: Voicemail: Local Voicemail

* Voicemail Password: ***** Skip Voicemail Password:

Send Voicemail to Email: Default Verification: Keep Voicemail after Emailing: Default

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

Disable This Extension: Enable SCA:

Emergency Calls CID:

User Settings

First Name: Last Name:

Email Address: * User Password: *****

* Language: Default * Concurrent Registrations: 3

Mobile Phone Number:

Figure 94: 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.



Figure 95: SMS Message Support

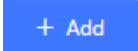
EXTENSION GROUPS

The UCM630xA extension group feature allows users to assign and categorize extensions in different groups to better manage the configurations on the UCM630xA. For example, when configuring “Enable Filter on Source Caller ID”, users could select a group instead of each person’s extension to assign. This feature simplifies the configuration process and helps manage and categorize the extensions for business environment.

Configure Extension Groups

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

- Click on



to create a new extension group.

- Click on



to edit the extension group.

- Click on



to delete the extension group.

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

Create New Extension Group

* Name:

Members:

| <input type="checkbox"/> 0 item Available | <input type="checkbox"/> 6 items Selected |
|---|--|
| <input type="text" value="Search"/> | <input type="text" value="Search"/> |
| None | <input type="checkbox"/> 1000 <input type="checkbox"/> 4001 <input type="checkbox"/> 4002 <input type="checkbox"/> 4003 |

Figure 96: Edit Extension Group

Click on



in order to change the ringing priority of the members selected on the group.



Using Extension Groups

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

Figure 97: 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.

| | |
|-------------------------|---|
| FXO Port | <p>Select the channel for the analog trunk.</p> <ul style="list-style-type: none"> ◦ UCM6300A: 1 channel ◦ UCM6302A: 2 channels ◦ UCM6304A: 4 channels ◦ UCM6308A: 8 channels |
| Trunk Name | Specify a unique label to identify the trunk when listed in outbound rules, incoming rules and etc. |
| Advanced Options | |
| SLA Mode | Enable this option to satisfy two primary use cases, which include emulating a simple key system and creating shared extensions on a PBX. Enable SLA Mode will disable polarity reversal. |

| | |
|--|---|
| Barge Allowed | <p>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.</p> <p>The default setting is Yes.</p> |
| Hold Access | <p>The hold option specifies hold permissions for this trunk. If set to “Open”, any station can place this trunk on hold and any other station is allowed to retrieve the call. If set to “Private”, only the station that places the call on hold can retrieve the call.</p> <p>The default setting is Yes.</p> |
| Enable Polarity Reversal | <p>If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as “Hangup” on a polarity reversal. The default setting is “No”.</p> |
| Polarity on Answer Delay | <p>When FXO port answers the call, FXS may send a Polarity Reversal. If this interval is shorter than the value of “Polarity on Answer Delay”, the Polarity Reversal will be ignored. Otherwise, the FXO will Onhook to disconnect the call. The default setting is 600ms.</p> |
| Current Disconnect Threshold (ms) | <p>This is the periodic time (in ms) that the UCM630xA will use to check on a voltage drop in the line. The default setting is 200. The valid range is 50 to 3000.</p> |
| Ring Timeout | <p>Configure the ring timeout (in ms). Trunk (FXO) devices must have a timeout to determine if there was a Hangup before the line is answered. This value can be used to configure how long it takes before the UCM630xA considers a non-ringing line with Hangup activity. The default setting is 8000.</p> |
| RX Gain | <p>Configure the RX gain for the receiving channel of analog FXO port. The valid range is from -13.5 (dB) to + 12.0 (dB). The default setting is 0.</p> |
| TX Gain | <p>Configure the TX gain for the transmitting channel of analog FXO port. The valid range is from -13.5 (dB) to + 12.0 (dB). The default setting is 0.</p> |
| Use CallerID | <p>Configure to enable CallerID detection.</p> <p>The default setting is “Yes”.</p> |

| | |
|----------------------------|---|
| Caller ID Scheme | <p>Select the Caller ID scheme for this trunk.</p> <ul style="list-style-type: none"> ◦ 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 <p>If you are not sure which scheme to choose, please select “Auto Detect”. The default setting is “Bellcore/Telcordia”.</p> |
| Fax Mode | <p>Configures how faxes to this extension will be handled.</p> <ul style="list-style-type: none"> ◦ 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. <p>The default setting is None.</p> |
| FXO Dial Delay (ms) | <p>Configure the time interval between off-hook and first dialed digit for outbound calls.</p> |
| Auto Record | <p>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.</p> |
| Disable This Trunk | <p>If selected, the trunk will be disabled and incoming/Outgoing calls via this trunk will not be possible.</p> |

| | |
|--|--|
| <p>DAHDI Out Line Selection</p> | <p>This is to implement analog trunk outbound line selection strategy.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> ◦ Ascend <p>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 UCM6302A is used would be port 1→port 2→. Every time it will start with port 1 (if it is idle).</p> <ul style="list-style-type: none"> ◦ Poll <p>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 UCM6302A is used.</p> <ul style="list-style-type: none"> ◦ Descend <p>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 UCM6302A is used would be port 2→port 1. Every time it will start with port 2 (if it is idle).</p> <p>The default setting is “Ascend” mode.</p> |
| <p>Echo Cancellation Mode</p> | <p>The Non-Linear Processing (NLP) in echo cancellation helps to remove/suppress residual echo components that could not be removed by the LEC (Line Echo Canceller). Following modes are supported:</p> <ul style="list-style-type: none"> ◦ 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. |
| <p>Direct Callback</p> | <p>Allows external numbers the option to get directed to the extension that last called them.</p> <p>For Example: User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option “Direct Callback” is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.</p> |
| <p>Tone Settings</p> | |
| <p>Busy Detection</p> | <p>Busy Detection is used to detect far end Hangup or for detecting busy signal. The default setting is “Yes”.</p> |
| <p>Busy Tone Count</p> | <p>If “Busy Detection” is enabled, users can specify the number of busy tones to be played before hanging up. The default setting is 2. Better results might be achieved if set to 4, 6 or even 8. Please note that the higher the number is, the more time is needed to Hangup the channel. However, this might lower the probability to get random Hangup.</p> |
| <p>Congestion Detection</p> | <p>Congestion detection is used to detect far end congestion signal. The default setting is “Yes”.</p> |

| | |
|-------------------------|---|
| 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 | <p>Syntax:</p> <p>f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]];</p> <p>Frequencies are in Hz and cadence on and off are in ms.</p> <p>Frequencies Range: [0, 4000)</p> <p>Busy Level Range: (-300, 0)</p> <p>Cadence Range: [0, 16383].</p> <p>Select Tone Country “Custom” to manually configure Busy Tone value.</p> <p>Default value:</p> <p>f1=480@-50,f2=620@-50,c=500/500</p> |
| Congestion Tone | <p>Syntax:</p> <p>f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]];</p> <p>Frequencies are in Hz and cadence on and off are in ms.</p> <p>Frequencies Range: [0, 4000)</p> <p>Busy Level Range: (-300, 0)</p> <p>Cadence Range: [0, 16383].</p> <p>Select Tone Country “Custom” to manually configure Busy Tone value.</p> <p>Default value:</p> <p>f1=480@-50,f2=620@-50,c=250/250</p> |
| PSTN Detection | Click on “Detect” to detect the busy tone, Polarity Reversal and Current Disconnect by PSTN. Before the detecting, please make sure there are more than one channel configured and working properly. If the detection has busy tone, the “Tone Country” option will be set as “Custom”. |

Table 58: Analog Trunk Configuration Parameters

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.

Figure 98: UCM630xA FXO Tone Settings

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

Figure 99: UCM630xA PSTN Detection

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

Detect Model: Auto Detect.

Source Channel: The source channel to be detected.

Destination Channel: The channel to help detecting. For example, the second FXO port.

Destination Number: The number to be dialed for detecting. This number must be the actual PSTN number for the FXO port used as the destination channel.

The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Detect model:** A dropdown menu with "Auto Detect" selected.
- Source Channel (to be detected):** A dropdown menu with "1" selected.
- Destination Channel:** A dropdown menu with "2" selected.
- * Destination Number:** A text input field containing "123654".
- Dump Call Progress Tone:** An unchecked checkbox.
- File:** A text input field.
- 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."
- Buttons:** "Cancel" and "Detect" buttons at the bottom.

Figure 100: UCM630xA PSTN Detection: Auto Detect

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

The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Detect model:** A dropdown menu with "Semi-auto Detect" selected.
- Source Channel (to be detected):** A dropdown menu with "1" selected.
- * Destination Number:** A text input field containing "123654".
- Dump Call Progress Tone:** An unchecked checkbox.
- File:** A text input field.
- 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."
- Buttons:** "Cancel" and "Detect" buttons at the bottom.

Figure 101: UCM630xA PSTN Detection: Semi-Auto Detect

Detect Model: Semi-auto Detect.

Source Channel: The source channel to be detected.

Destination Number: The number to be dialed for detecting. This number could be a cell phone number or other PSTN number that can be reached from the source channel PSTN number.

5. Click "Detect" to start detecting. The source channel will initiate a call to the destination number. For "Auto Detect", the call will be automatically answered. For "Semi-auto Detect", the UCM630xA Web GUI will display prompt to notify the user to answer or hang up the call to finish the detecting process.

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

| | |
|-------------------------------------|--|
| Detect Model | <p>Select “Auto Detect” or “Semi-auto Detect” for PSTN detection.</p> <ul style="list-style-type: none"> ◦ Auto Detect <p>Please make sure two or more channels are connected to the UCM630xA and in idle status before starting the detection. During the detection, one channel will be used as caller (Source Channel) and another channel will be used as callee (Destination Channel). The UCM630xA will control the call to be established and hang up between caller and callee to finish the detection.</p> <ul style="list-style-type: none"> ◦ Semi-auto Detect <p>Semi-auto detection requires answering or hanging up the call manually. Please make sure one channel is connected to the UCM630xA and in idle status before starting the detection. During the detection, source channel will be used as caller and send the call to the configured Destination Number. Users will then need follow the prompts in Web GUI to help finish the detection.</p> <p>The default setting is “Auto Detect”.</p> |
| 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. |


Table 59: PSTN Detection for Analog Trunk

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

VOIP TRUNKS

VoIP Trunk Configuration

VoIP trunks can be configured in UCM630xA under Web GUI→**Extension/Trunk**→**VoIP Trunks**. Once created, the VoIP trunks will be listed with Provider Name, Type, Hostname/IP, Username and Options to edit/detect the trunk.

- Click on “Add SIP Trunk” or “Add IAX Trunk” to add a new VoIP trunk.
- Click on  to configure detailed parameters for the VoIP trunk.

- Click on



to configure Direct Outward Dialing (DOD) for the SIP Trunk.

- Click on



to start LDAP Sync.

- Click on



to delete the VoIP trunk.

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

The VoIP trunk options are listed in the table below.

| | |
|---------------------------|---|
| Type | Select the VoIP trunk type. <ul style="list-style-type: none"> • Peer SIP Trunk • Register SIP Trunk |
| Provider Name | Configure a unique label (up to 64 characters) 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 method. Using TCP requires local TCP support. Using TLS Requires local TLS support. <ul style="list-style-type: none"> • UDP • TCP • TLS |
| Auto Record | If enabled, calls handled with this extension/trunk will automatically be recorded. |
| Keep Original CID | Keep the CID from the inbound call when dialing out. This setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line. |
| 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 setting when the PBX is using public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall. |
| Disable This Trunk | If checked, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider. |

| | |
|---|--|
| TEL URI | If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled. |
| Caller ID Number | <p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call:</p> <p>From the user (Register Trunk Only) → CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID.</p> |
| CallerID Name | Configure the new name of the caller when the extension has no CallerID Name configured. |
| Auto Record | If enabled, calls handled with this extension/trunk will automatically be recorded. |
| Auth ID | Enter the Authentication ID for the "Register SIP Trunk" type. |
| Direct Callback | <p>Allows external numbers the option to get directed to the extension that last called them.</p> <p>For Example, User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option "Direct Callback" is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.</p> |
| RemoteConnect Mode | If enabled, the RemoteConnect related parameters will be set synchronously. Please make sure the trunk host is allocated by GDMS or supports TLS. |
| Limit Concurrent Calls | If enabled and when the number of concurrent calls exceeds any trunk's configured concurrent call thresholds, an alarm notification will be generated. Note: Please make sure the system alert event "Trunk Concurrent Calls" is enabled. |
| Concurrent Call Threshold | Threshold of all incoming and outgoing concurrent calls through this trunk. |
| Outgoing Concurrent Calls Threshold | Threshold of all outgoing concurrent calls passing through this trunk. |
| Incoming Concurrent Calls Threshold | Threshold of all incoming concurrent calls passing through this trunk. |
| Total Time Limit For Outbound Calls | |
| Enable Total Time Limit For Outgoing Calls | When this setting is activated, the user can set a time limit before calls cannot be initiated through this trunk |
| Period | <p>This setting defines how long until the time allowed for outgoing calls is reset.</p> <ul style="list-style-type: none"> • Monthly: The time allowed will reset every month. • Quarterly: The time allowed will reset every 3 months. |

| | |
|-------------------|---|
| | Example: If the time limit has been set to 4320 minutes, the allowed time will always revert back to 4320 after a month or 3 month based on the period configured. |
| Total Time | Total time allowed in minutes |

Table 60: Create New SIP Trunk

SIP Peer Trunk

SIP 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. |
| Auto Record | Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files. |
| Keep Original CID | Keep the CID from the inbound call when dialing out, this setting will override the "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using the "username" field from the authentication line. |
| 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 public IP and communicating with devices behind NAT. If there is a one-way audio issue, usually it is related to NAT configuration or SIP/RTP port configuration on the firewall. |
| Disable This Trunk | If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider. |
| TEL URI | If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled. |
| Caller ID Number | Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: <ul style="list-style-type: none"> • CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID. |
| CallerID Name | Configure the name of the caller to be displayed when the extension has no CallerID Name configured. |
| Transport | Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". <ul style="list-style-type: none"> • UDP |

| | |
|-----------------------------------|---|
| | <ul style="list-style-type: none"> • TCP • TLS |
| RemoteConnect Mode | If enabled, the RemoteConnect related parameters will be set synchronously. Please make the trunk host is allocated by GDMS or it supports TLS. |
| Direct Callback | <p>Allows external numbers the option to get directed to the extension that last called them.</p> <p>For Example, User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option “Direct Callback” is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.</p> |
| 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. |
| Packet Loss Retransmission | Configure to enable Packet Loss Retransmission. |
| Audio FEC | Configure to enable Forward Error Correction (FEC) for audio. |
| Video FEC | Configure to enable Forward Error Correction (FEC) for video. |
| ICE Support | Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end. |
| TURN Relay | TURN servers are used for media NAT traversal and will be prioritized if ICE is also enabled. |
| 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. The default setting is "No". |
| SRTP Crypto Suite | SRTP encryption suite used by UCM for outbound calls. Priority is based on order of configuration. |
| IPVT Mode | Similar to Enable Direct Media. The PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. Primarily for use with trunks to IPVT. |
| Enable T.38 UDPTL | Enable or disable T.38 UDPTL support. |
| Special attributes | Carry the ssrc/msid/mid/ct/as/tias/record properties of the SDP. These attributes may cause incompatibility when interconnecting with other devices. |
| 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. |
| DOD as From Name | If enabled and "From User" is configured, the INVITE's From header will contain the DOD number. |
| Passthrough PAI Header | If 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 and REGISTER sent to the trunk will contain P-Access-Network-Info header. |
| Send Anonymous | If checked, the "From" header in outgoing INVITE message will be set to anonymous. |
| Outbound Proxy Support | Enable to send outbound signal to the proxy instead of the devices directly. |
| DID Mode | Configure to obtain the destination ID of an incoming SIP call from SIP Request-line or To header. |
| GIN Registration | If enabled, the UCM will send a GIN REGISTER (generate implicit numbers). |
| DTMF Mode | <p>Configure the mode for sending the DTMF.</p> <ul style="list-style-type: none"> ● RFC4833 (default): DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream. Backwards-compatible with RFC2833. ● DTMF is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs ● Info: DTMF is transmitted separately from the media streams. ● RFC4733_info: DTMF is transmitted through both RFC4733 and SIP INFO ● Auto: DTMF mode will be negotiated with the remote peer, only supports RFC4733 and inband. RFC4733 will be used by default unless the remote peer does not indicate support. |
| Enable Heartbeat detection | If enabled, the PBX will regularly send SIP OPTIONS to check if the device is online. |
| The Maximum Number of Call Lines | The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit. |
| Sync LDAP Enable | <p>Automatically sync local LDAP phonebooks to a remote peer (SIP peer trunk only). To ensure successful syncing, the remote peer must also enable this service and set the same password as the local UCM. Port 873 is used by default.</p> <ul style="list-style-type: none"> ● 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: The last successful sync date. |
| STIR/SHAKEN | <p>Block Spam Calls.</p> <ul style="list-style-type: none"> ● Disabled: Disable STIR/SHAKEN. ● Outgoing Attest: Enable STIR/SHAKEN attestation for outgoing calls. |

| | |
|------------------|---|
| | <ul style="list-style-type: none"> ● Incoming Verify: Enable STIR/SHAKEN verification for incoming calls. ● Both: Enable STIR/SHAKEN for both outgoing and incoming calls |
| Enable CC | Check this box to allow the system to automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. If the Call Waiting is disabled, the CC service will take effect only for unanswered and timeout calls. |

Table 63: Create New IAX Trunk

| | |
|---------------------------|--|
| Type | <p>Select the VoIP trunk type.</p> <ul style="list-style-type: none"> ● 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 | <p>The number that the trunk will try to use when making outbound calls.</p> <p>CID priority from highest to lowest is as follows:</p> <p>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.</p> <p>Note 1: Certain providers may ignore this CID.</p> <p>Note 2: If this CID contains an asterisk (*), call recordings from this trunk might be lost when saving them to NAS storage.</p> |
| 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 | <p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call.</p> <p>From the user (Register Trunk Only) → CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID.</p> |
| 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 Trunks [Trunk Group](#)

[+ Add Trunk Group](#)

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

Figure 102: 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
Cancel Save

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.

Figure 103: 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 | <p>Enable this setting if the UCM is using public IP and communicating with devices behind NAT.</p> <p>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.</p> |

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

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

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

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

Important Note

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

Direct Outward Dialing (DOD)

The UCM630xA provides Direct Outward Dialing (DOD) which is a service of a local phone company (or local exchange carrier) that allows subscribers within a company's PBX system to connect to outside lines directly.

Example of how DOD is used:

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

Steps to configure DOD on the UCM630xA:

1. To setup DOD go to UCM630xA Web GUI→**Extension/Trunk**→**VoIP Trunks** page.

2. Click



to access the DOD options for the selected SIP Trunk.

3. Click “Add DOD” to begin your DOD setup

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

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

6. Select an extension from the “Available Extensions” list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO's extension. After making the selection, click on the



button to move the extension(s) to the “Selected Extensions” list.

The screenshot shows a 'Create DOD' configuration window with the following fields and options:

- *DOD Number:** 001122334455
- DOD Name:** Grandstream_Supp
- Add Extension:**
- Available Extensions:** A list with 15 items, showing:
 - 1000
 - 1001 "John Snow"
 - 1002 "Jack Doe"
 - 1003 "Marc Hugzman"
 - 1004 "Pieter Rozfield"
- Selected Extensions:** A list with 0 items, showing "None".

Navigation buttons: Cancel, Save.

Figure 104: DOD extension selection

1. Click “Save” at the bottom.

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

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

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

| DOD | DOD NAME | EXTENSIONS | OPTIONS |
|-----------|----------|----------------|---|
| 918273645 | Test | 1000 1001 1002 | Edit Delete |

Total: 1 Goto

Figure 105: Edit DOD

Note

Users can import and export DOD files.

SLA STATION

The UCM630xA supports SLA that allows mapping the key with LED on a multi-line phone to different external lines. When there is an incoming call and the phone starts to ring, the LED on the key will flash in red and the call can be picked up by pressing this key. This allows users to know if the line is occupied or not. The SLA function on the UCM630xA is like BLF but SLA is used to monitor external line i.e., analog trunk on the UCM630xA. Users could configure the phone with BLF mode on the MPK to monitor the analog trunk status or press the line key pick up call from the analog trunk on the UCM630xA.

Create/Edit SLA Station

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

SLA Station

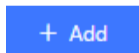
[+ Add](#) [Delete](#)

| STATION NAME | STATION | ASSOCIATED SLA TRUNKS | OPTIONS |
|-------------------------------|---------|-----------------------|--|
| <input type="checkbox"/> FX01 | 1000 | test | <input type="checkbox"/> Edit Delete |

Total: 1 Goto

Figure 106: 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.

Table 66: 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 | <p>Select a trunk for this SLA from the Available SLA Trunks list. Click on</p> <p>↑</p> <p>↕</p> <p>↓</p> <p>to arrange the order. If there are multiple trunks selected, when there are calls on those trunks at the same time, pressing the LINE key on the phone will pick up the call on the first trunk here.</p> |
| SLA Station Options | |
| Ring Timeout | Configure the time (in seconds) to ring the station before the call is considered unanswered. No timeout is set by default. If set to 0, there will be no timeout. |
| Ring Delay | Configure the time (in seconds) for delay before ringing the station when a call first coming in on the shared line. No delay is set by default. If set to 0, there will be no delay. |
| Hold Access | This option defines the competence of the hold action for one particular trunk. If set to “open”, any station could hold a call on that trunk or resume one held session; if set to “private”, only the station that places the trunk call on hold could resume the session. The default setting is “open”. |

Sample Configuration

1. On the UCM630xA, go to Web GUI→**Extension/Trunk**→**Analog Trunks** page. Create analog trunk or edit the existing analog trunk. Make sure “SLA Mode” is enabled for the analog trunk. Once enabled, this analog trunk will be only available for the SLA stations created under Web GUI→**Extension/Trunk**→**SLA Station** page.

* FXO Port: 1 2

* Trunk Name:

| **Advanced Options**



SLA Mode:

Figure 107: Enable SLA Mode for Analog Trunk

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

Analog Trunks

[Analog Trunks](#) [Call Progress Tone File List](#)

| TRUNKS | DISABLE | TRUNK MODE | ANALOG PORTS | OPTIONS |
|--------|---------|------------|--------------|---|
| test | no | sla | 1 |   |

Total: 1 Goto

Figure 108: Analog Trunk with SLA Mode Enabled

1. On the UCM630xA, go to Web GUI→Extension/Trunk→SLA Station page, click on “Add”. Please refer to section [Create/Edit SLA Station] for the configuration parameters. Users can create one or more SLA stations to monitor the analog trunk. The following figure shows two stations, 1002 and 1005, are configured to be associated with SLA trunk “fxo1”.

| STATION NAME | STATION | ASSOCIATED SLA TRUNKS | OPTIONS |
|--------------|---------|-----------------------|---------|
| FX01 | 1000 | test | |

Total: 1 10 / page Goto 1

Figure 109: SLA Example – SLA Station

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

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

Figure 110: SLA Example – MPK Configuration

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

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

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

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

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

- **Answering call using LINE key**

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

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

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

- **Hold/UnHold using BLF key**

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

CALL ROUTES

Outbound Routes

In the following sections, we will discuss the steps and parameters used to configure and manage outbound rules in UCM630xA, these rules are the regulating points for all external outgoing calls initiated by the UCM through all types of trunks: SIP, Analog and Digital.

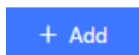
Configuring Outbound Routes

In the UCM630xA, an outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g., “Local” 7-digit dials through an FXO while “Long distance” 10-digit dials through a low-cost SIP trunk). Users can also set up a failover trunk to be used when the primary trunk fails.

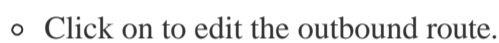
Go to Web GUI→**Extension/Trunk**→**Outbound Routes** to add and edit outbound rules.



Click on



to add a new outbound route.



Click on to delete the outbound route.

On the UCM630xA, the outbound route priority is based on “Best matching pattern”. For example, the UCM630xA has outbound route A with pattern 1xxx and outbound route B with pattern 10xx configured. When dialing 1000 for outbound call, outbound route B will always be used first. This is because pattern 10xx is a better match than pattern 1xxx. Only when there are multiple outbound routes with the same pattern configured.

Table 67: Outbound Route Configuration Parameters

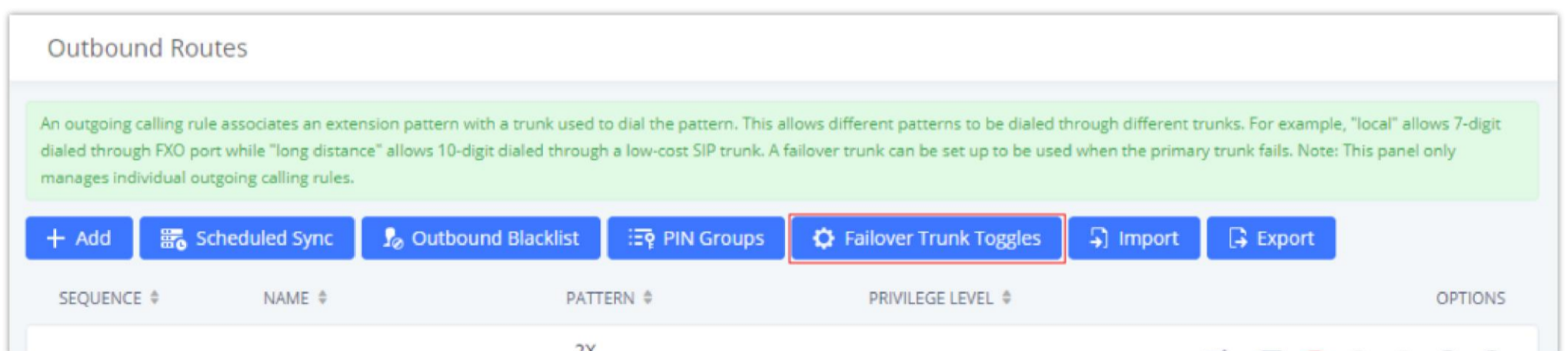
| | |
|---------------------------|---|
| Outbound Rule Name | Configure the name of the calling rule (e.g., local, long_distance, and etc.). Letters, digits, _ and – are allowed. |
| Pattern | <p>All patterns are prefixed by “_” character, but please do not enter more than one “_” at the beginning. All patterns can add comments, such as “_pattern /* comment */”. In patterns, some characters have special meanings:</p> <ul style="list-style-type: none">◦ [12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 is allowed.◦ N ... Any digit from 2-9.◦ Wildcard, matching one or more characters.◦ ! ... Wildcard, matching zero or more characters immediately.◦ X ... Any digit from 0-9.◦ Z ... Any digit from 1-9.◦ – ... Hyphen is to connect characters and it will be ignored.◦ [] Contain special characters ([x], [n], [z]) represent letters x, n, z. |

| | |
|--|---|
| Disable This Route | After creating the outbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in UCM. Users can enable it again when it is needed. |
| Password | Configure the password for users to use this rule when making outbound calls. |
| Local Country Code | If your local country code is affected by the outbound blacklist, please enter it here to bypass the blacklist. |
| Call Duration Limit | Enable to configure the maximum duration for the call using this outbound route. |
| Maximum Call Duration | Configure the maximum duration of the call (in seconds). The default setting is 0, which means no limit. |
| Warning Time | Configure the warning time for the call using this outbound route. If set to x seconds, the warning tone will be played to the caller when x seconds are left to end the call. |
| Auto Record | If enabled, calls using this route will automatically be recorded. |
| Warning Repeat Interval | Configure the warning repeat interval for the call using this outbound route. If set to X seconds, the warning tone will be played every x seconds after the first warning. |
| PIN Groups | Select a PIN Group |
| PIN Groups with Privilege Level | If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied. |
| Privilege Level | <p>Select privilege level for the outbound rule.</p> <ul style="list-style-type: none"> ◦ Internal: The lowest level required. All users can use this rule. ◦ Local: Users with Local, National, or International level can use this rule. ◦ National: Users with National or International level can use this rule. ◦ International: The highest level required. Only users with international level can use this rule. ◦ Disable: The default setting is “Disable”. If selected, only the matched source caller ID will be allowed to use this outbound route. <p>Please be aware of the potential security risks when using “Internal” level, which means all users can use this outbound rule to dial out from the trunk.</p> |

| | |
|---|--|
| <p>Enable Filter on Source Caller ID</p> | <p>When enabled, users could specify extensions allowed to use this outbound route. “Privilege Level” is automatically disabled if using “Enable Filter on Source Caller ID”.</p> <p>The following two methods can be used at the same time to define the extensions as the source caller ID.</p> <ol style="list-style-type: none"> 1. Select available extensions/extension groups from the list. This allows users to specify arbitrary single extensions available in the PBX. 2. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one. <ul style="list-style-type: none"> ◦ All patterns are prefixed with the “_”. ◦ Special characters: <p>X: Any Digit from 0-9.</p> <p>Z: Any Digit from 1-9.</p> <p>N: Any Digit from 2-9.</p> <p>“.”: Wildcard. Match one or more characters.</p> <p>“!”: Wildcard. Match zero or more characters immediately.</p> <p>Example: [12345-9] – Any digit from 1 to 9.</p> <p>Note: Multiple patterns can be used. Patterns should be separated by comma “,”. Example: _X. , _NNXXNXXXXXX , _818X.</p> |
| <p>Outbound Route CID</p> | <p>Attempt to use the configured outbound route CID. This CID will not be used if DOD is configured.</p> |
| <p>Send This Call Through Trunk</p> | |
| <p>Trunk</p> | <p>Select the trunk for this outbound rule.</p> |
| <p>Strip</p> | <p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p>Example:</p> <p>The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.</p> |
| <p>Prepend</p> | <p>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.</p> |
| <p>Use Failover Trunk</p> | |

| | |
|----------------------------|---|
| Failover Trunk | <p>Failover trunks can be used to make sure that a call goes through an alternate route when the primary trunk is busy or down. If “Use Failover Trunk” is enabled and “Failover trunk” is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through.</p> <p>UCM630xA support up to 10 failover trunks.</p> <p>Example:</p> <p>The user’s primary trunk is a VoIP trunk and the user would like to use the PSTN when the VoIP trunk is not available. The PSTN trunk can be configured as the failover trunk of the VoIP trunk.</p> |
| Strip | <p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p>Example:</p> <p>The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.</p> |
| Prepend | <p>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.</p> |
| Time Condition | |
| Time Condition Mode | <p>Use Main Trunk or Failover Trunk: Use the Main Trunk and its settings during the configured time conditions. If the main trunk is unavailable, the Failover Trunk and its settings will be used instead.</p> <p>Use Specific Trunks: Use specific trunks during the configured time conditions. The Strip and Prepend settings of the Main Trunk will be used. If a trunk is unavailable during its time condition, no failover trunks will be used.</p> |

Failover Trunk Toggles



The screenshot shows the 'Outbound Routes' configuration interface. At the top, there is a green informational box explaining that an outgoing calling rule associates an extension pattern with a trunk. Below this, a row of action buttons includes '+ Add', 'Scheduled Sync', 'Outbound Blacklist', 'PIN Groups', 'Failover Trunk Toggles' (which is highlighted with a red box), 'Import', and 'Export'. Below the buttons is a table header with columns for 'SEQUENCE', 'NAME', 'PATTERN', 'PRIVILEGE LEVEL', and 'OPTIONS'. The first row of the table shows a '2X' pattern.

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

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 Page

DOD Configuration by Outbound Route

Outbound Blacklist

The UCM630xA allows users to configure blacklist for outbound routes. If the dialing number matches the blacklist numbers or patterns, the outbound call will not be allowed. The outbound blacklist can be configured under UCM Web GUI → **Extension/Trunk** → **Outbound Routes**: Outbound Blacklist.

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

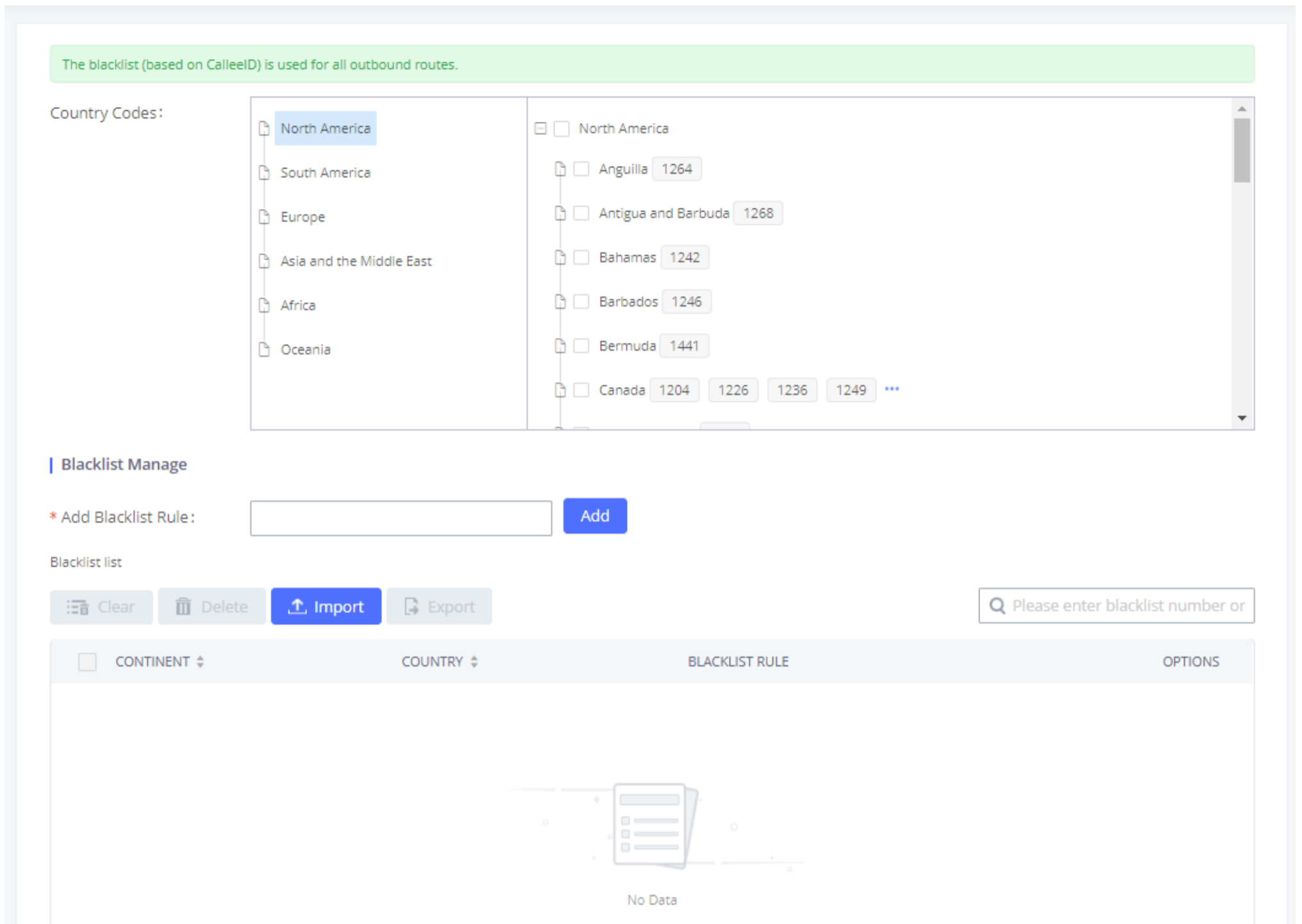


Figure 111: Country Codes

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

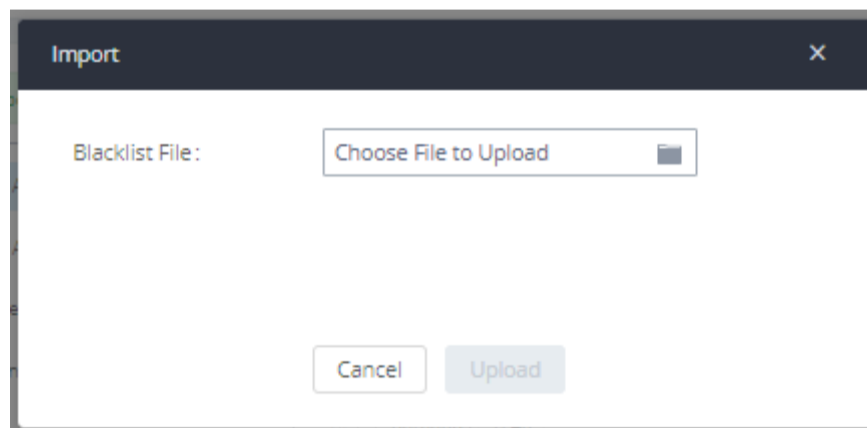


Figure 112: Blacklist Import/Export

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**.

Table 68: 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**.

Table 69: Outbound Routes/PIN Group

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

Once user click on

[PIN Groups](#)

the following figure shows to configure the new PIN.

Create New PIN Group

* Name:

Record in CDR:

Members

* PIN Number:

* PIN Name:

Figure 113: Create New PIN Group

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

| NAME | | RECORD IN CDR | OPTIONS |
|------------|----------|---------------|---------|
| GSEMEA | | yes | |
| PIN NUMBER | PIN NAME | | |
| 125478963 | Dao | | |
| 1596324 | Emily | | |

Total: 1 | 10 / page | Goto 1

Figure 114: PIN Members

Note

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

General

* Calling Rule Name: Disable This Route:

* Pattern: Privilege Level:

PIN Groups: PIN Groups with Privilege Level:

Password:

Figure 115: 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.

| 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 | | - |

Figure 116: CDR Record

o

Importing PIN Groups from CSV files:

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

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

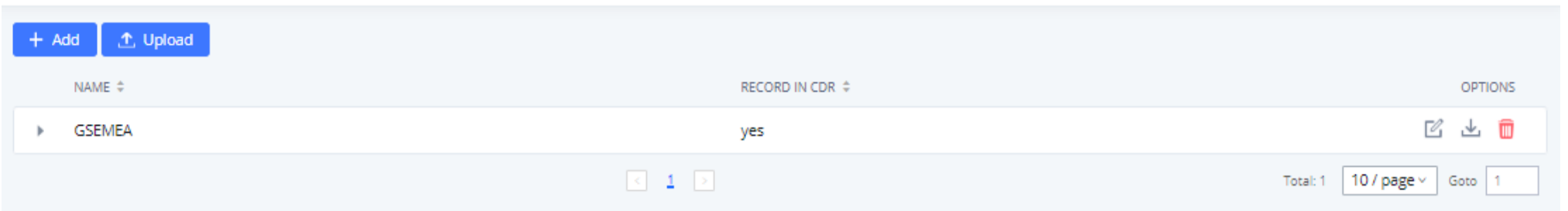


Figure 117: Importing PIN Groups from CSV files

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:

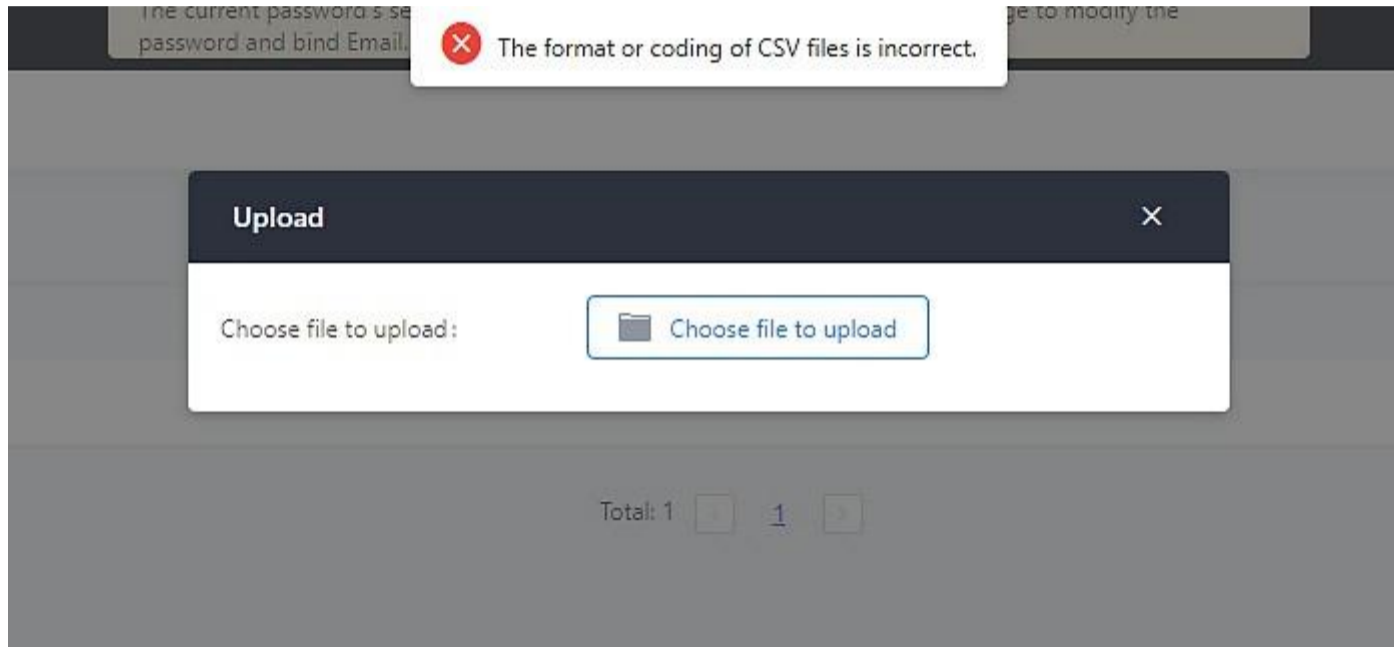


Figure 118: Incorrect CSV File

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

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

Figure 119: 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

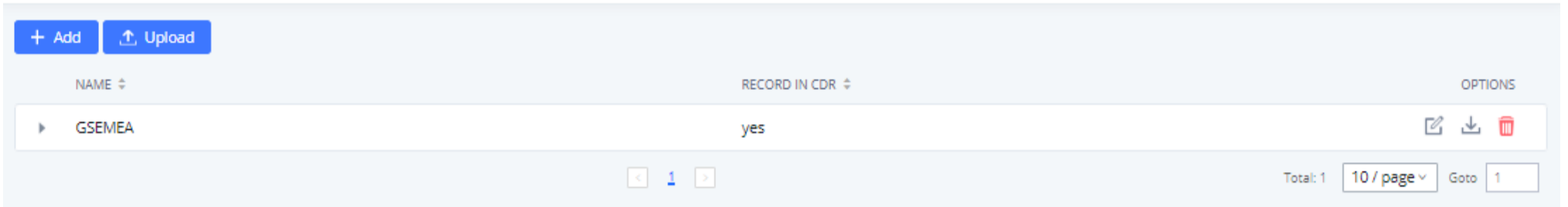


Figure 120: CSV File Successful Upload

Inbound Routes

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

- Click on

to add a new inbound route.

- Click on “Blacklist” to configure blacklist for all inbound routes.

- Click on

to edit the inbound route.

- Click on

to delete the inbound route.

Inbound Rule Configurations

Table 70: Inbound Rule Configuration Parameters

| | |
|---------------------------|--|
| Trunks | Select the trunk to configure the inbound rule. |
| Inbound Route Name | Configure the name of the Inbound Route. For example, “Local”, “LongDistance” etc. |
| Pattern | <p>All patterns are prefixed with the “_”.</p> <p>Special characters:</p> <p>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.</p> <p>Match zero or more characters immediately. Example: [12345-9] – Any digit from 1 to 9.</p> <p>Notes:</p> <p>Multiple patterns can be used. Each pattern should be entered in a new line.</p> <p>Example:</p> <p>_X.</p> <p>_ NNXXNXXXXX /* 10-digit long distance */</p> |

| | |
|------------------------------------|--|
| 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 UCM. 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. |
| 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 UCM receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS. |
| Fax Detection | If enabled, fax signals from the trunk during a call will be detected. |
| Fax Destination | Configures the destination of faxes. <ul style="list-style-type: none"> ● Extension: send the fax to the designated FXS/SIP extension (fax machine) or a FAX extension. ● Fax to Email: send the fax as an email attachment to the designated extension’s email address. If the selected extension does not have an associated email address, it will be sent to the default email address configured in the Call Features->Fax/T.38->Fax Settings page. Note: please make sure the sending email address is correctly configured in System Settings->Email Settings . |
| Prepend Trunk Name | If enabled, the trunk name will be added to the caller id name as the displayed caller id name. |
| Set Caller ID Info | Manipulates Caller ID (CID) name and/or number within the call flow to help identify who is calling. When enabled two 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. <ul style="list-style-type: none"> ● `\${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 | <p>The default string is <code>\${CALLERID(name)}</code>, which means the name of an incoming caller, it is a pattern-matching syntax format. <code>A\${CALLERID(name)}B</code> means Prepend a character ‘A’ and suffix a character ‘B’ to <code>\${CALLERID(name)}</code>.</p> <p>Not using pattern-matching syntax means setting a fixed name to the incoming caller.</p> |
| Enable Route-Level Inbound Mode | <p>Gives uses the ability to configure inbound mode per individual route. When enabled two fields will show allowing to set the Inbound mode and the Inbound mode Suffix.</p> <p>Note: Global inbound mode must be enabled before users can configure route-level inbound mode.</p> |
| Inbound Mode | <p>Choose the inbound mode for this route.</p> <p>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.</p> |
| Inbound Mode Suffix | <p>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.</p> |
| Inbound Multiple Mode | <p>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.</p> |
| CallerID Name Lookup | <p>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.</p> |
| Dial Trunk | <p>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 UCM’s trunk.</p> |
| Privilege Level | <p>This option shows up only when “By DID” is selected.</p> <ul style="list-style-type: none"> ● 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 | <p>This option shows up only when “By DID” is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination is:</p> <ul style="list-style-type: none"> ● Extension ● Conference ● Call Queue ● Ring Group ● Paging/Intercom Groups ● IVR ● Voicemail Groups ● Dial By Name ● All |

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

When “By DID” is used, the UCM will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in “DID destination”. If the dialed number matches the DID pattern, the call will be allowed to go through.

Configure the number of digits to be stripped in 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.

The screenshot displays the configuration interface for an Inbound Route. The main configuration area includes:

- * 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:** (empty text box)
- Allowed to seamless transfer:** (empty text box)
- Prepend Trunk Name:**
- Enable Route-Level Inbound Mode:**
- Allowed DID Destination:** Extension

Below the main configuration, there is a section for **Default Mode** (Mode 1) with the following settings:

- * Default Destination:** By DID
- Strip:** 8
- Prepend:** 2

Figure 121: Inbound Route feature: Prepend

Inbound Route: Multiple Mode

In the UCM630xA, the user can configure inbound route to enable multiple mode to switch between different destinations. The inbound multiple mode can be enabled under Inbound Route settings.

* Trunks: SIPTrunks -- test

* Pattern: _18005251163

Disable This Route:

Alert-info: None

Fax Detection:

Block Collect Calls:

Set CallerID Info:

Inbound Multiple Mode:

CallerID Pattern:

Allowed to seamless transfer:

Prepend Trunk Name:

Enable Route-Level Inbound Mode:

Default Mode | Mode 1

* Default Destination: Extension | 1000

Figure 122: Inbound Route – Multiple Mode

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

SIP end devices that have registered on the UCM630xA can dial feature code *62 to switch to inbound route “Mode 1” and dial feature code *61 to switch back to “Default Destination”. Switching between different mode can be easily done without Web GUI login.

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

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

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

Set Global Inbound Mode

Caution: Disabling Inbound Multiple Mode will switch the inbound mode to default mode.

Enable Inbound Multiple

Mode:

Inbound Mode: Default Mode

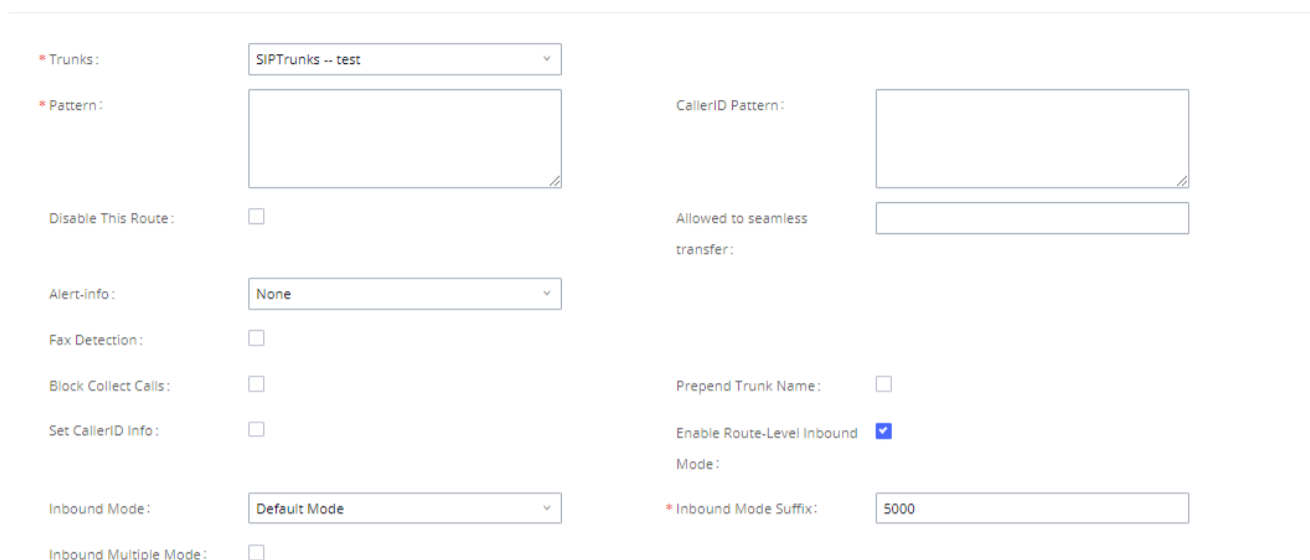
* Inbound Default Mode: *61

* Inbound Mode 1: *62

Figure 123: Inbound Route – Multiple Mode Feature Codes

Inbound Route: Route-Level Mode

In the UCM630xA, users can enable Route-Level Inbound Mode to switch between different destinations for each individual inbound route. The inbound Route-Level mode can be enabled under Inbound Route settings.



The screenshot shows the configuration interface for an inbound route. On the left side, there are several settings: 'Trunks' is set to 'SIPTrunks -- test'; 'Pattern' is an empty text box; 'Disable This Route' is an unchecked checkbox; 'Alert-info' is set to 'None'; 'Fax Detection', 'Block Collect Calls', and 'Set CallerID Info' are all unchecked checkboxes; 'Inbound Mode' is set to 'Default Mode'; and 'Inbound Multiple Mode' is an unchecked checkbox. On the right side, 'CallerID Pattern' is an empty text box; 'Allowed to seamless transfer' is an empty text box; 'Prepend Trunk Name' is an unchecked checkbox; 'Enable Route-Level Inbound Mode' is a checked checkbox; and 'Inbound Mode Suffix' is set to '5000'.

Figure 124: Inbound Route – Route-Level Mode

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

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

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

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

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

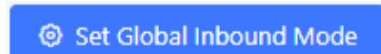
Inbound Route: Inbound Mode BLF Monitoring

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

To do this, please refer to the following steps:

1. Access the UCM web GUI and navigate to Extension/Trunk→Inbound Routes.

2. Click on the



button and enable Inbound Multiple Mode.

3. Edit the subscribe number field to the desired BLF value.

Set Global Inbound Mode

Caution: Disabling Inbound Multiple Mode will switch the inbound mode to default mode.

Enable Inbound Multiple

Mode:

Inbound Mode:

* Inbound Default Mode:

* Inbound Mode 1:

BLF Subscription Number:

Figure 125: Global Inbound Mode

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



Figure 126: Inbound Mode – Default Mode

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



Figure 127: Inbound Mode – Mode 1

Inbound Route: Import/Export Inbound Route

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

Inbound Routes

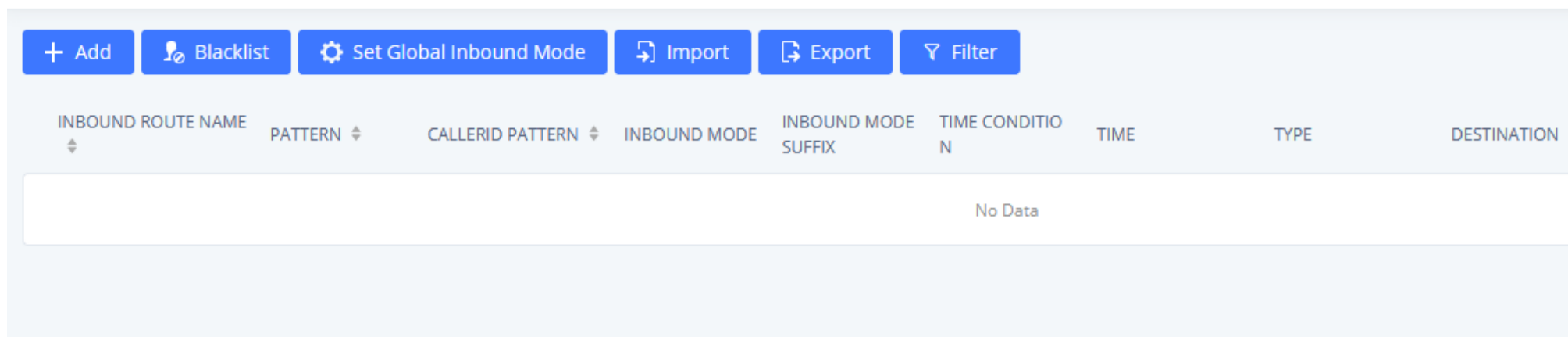


Figure 128: Import/Export Inbound Route

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.

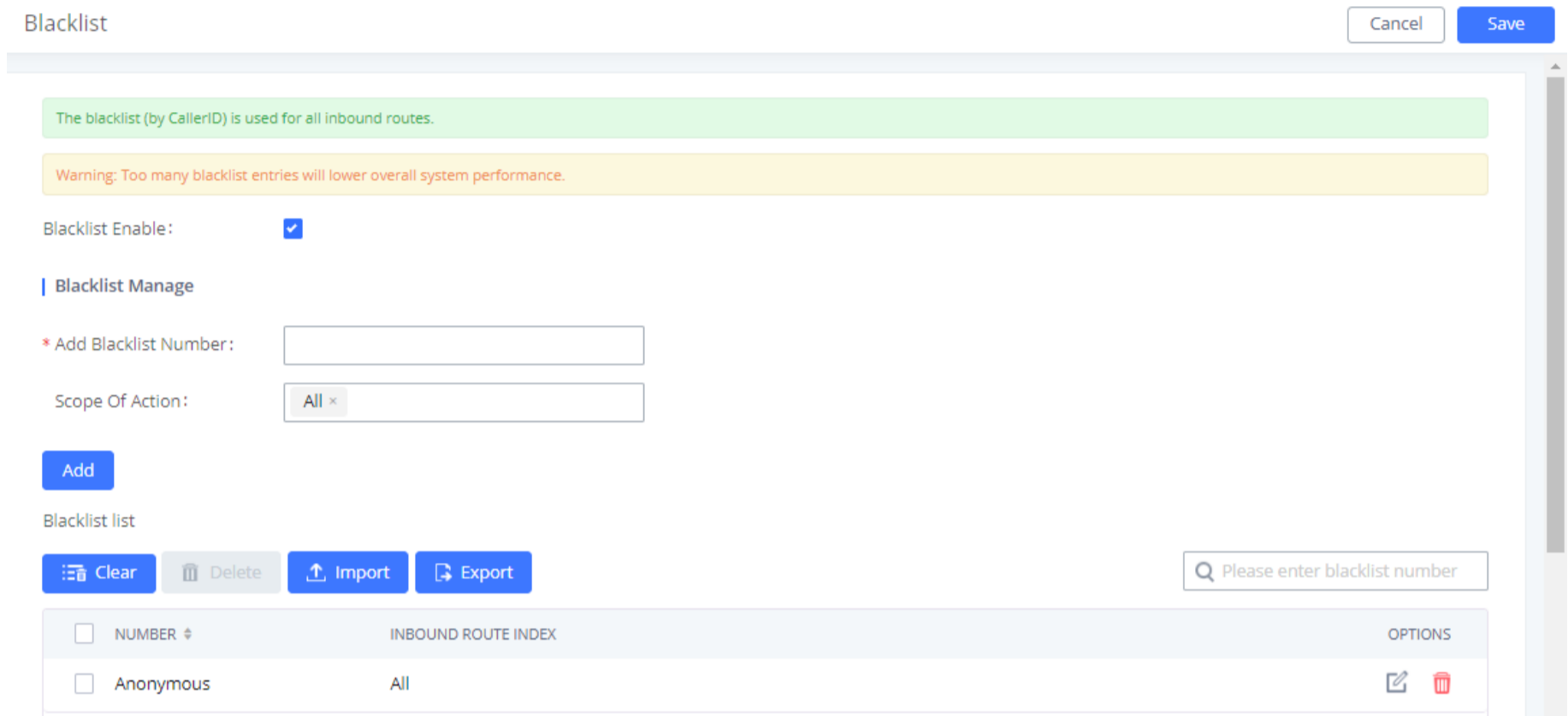


Figure 129: Blacklist Configuration Parameters

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

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

Figure 130: Blacklist csv File

Important Note

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

FAX SERVER

The UCM6300A series supports T.30/T.38 Fax and Fax Pass-through. It can convert the received Fax to PDF format and send it to the configured Email address. Fax/T.38 settings can be accessed via Web GUI→**Call Features**→**FAX/T.38**. The list of received Fax files will be displayed in the same web page for users to view, retrieve and delete.

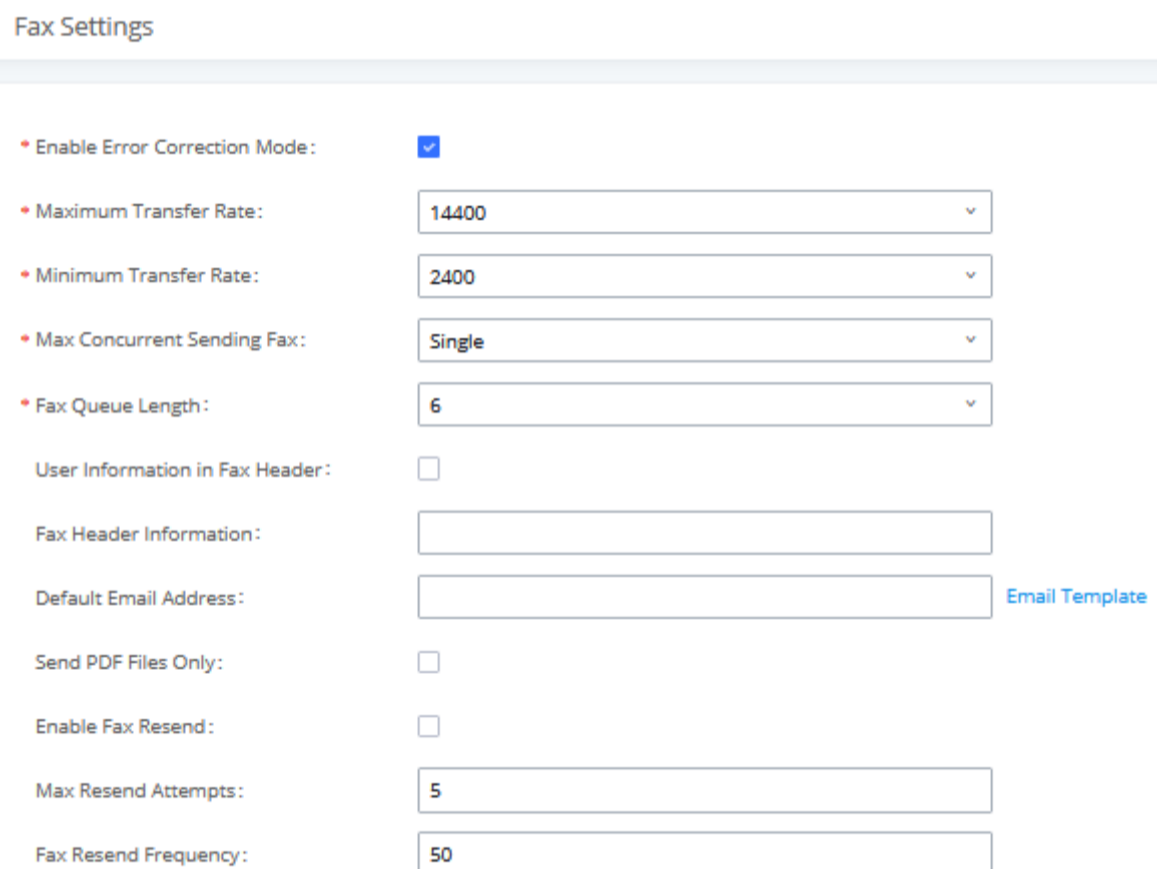
Configure Fax/T.38

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

to edit the Fax extension.

- Click on

to delete the Fax extension.



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

Figure 131: Fax Settings

Table 71: FAX/T.38 Settings

| | |
|-------------------------------------|---|
| Enable Error Correction Mode | Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is “Yes”. |
|-------------------------------------|---|

| | |
|---------------------------------------|---|
| Maximum Transfer Rate | <p>Configure the maximum transfer rate during the Fax rate negotiation.</p> <p>The possible values are 2400, 4800, 7200, 9600, 12000 and 14400.</p> <p>The default setting is 14400.</p> |
| Minimum Transfer Rate | <p>Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14000. The default setting is 2400.</p> |
| Max Concurrent Sending Fax | <p>Configure the concurrent fax that can be sent by UCM6300A. Two modes “Only” and “More” are supported.</p> <ul style="list-style-type: none"> ◦ Only <p>Under this mode, the UCM6300A allows only single user to send fax at a time.</p> <ul style="list-style-type: none"> ◦ More <p>Under this mode, the UCM6300A supports multiple concurrent fax sending by the users.</p> <p>By default, this option is set to “only”.</p> |
| Fax Queue Length | <p>Configure the maximum length of Fax Queue from 6 to 10.</p> <p>The default setting is 6.</p> |
| User Information in Fax Header | <p>If enabled this this will give users the option to send a special header in SIP fax messages.</p> |
| Fax Header Information | <p>Adds fax header into the fax file.</p> |
| Default Email Address | <p>Configure the Email address to send the received Fax to if user’s Email address cannot be found.</p> <p>Note:</p> <p>The extension’s Email address or the Fax’s default Email address needs to be configured in order to receive Fax from Email. If neither of them is configured, Fax will not be received from Email.</p> |

| | |
|-----------------------------|--|
| Template Variables | <p>Fill in the “Subject:” and “Message:” content, to be used in the Email when sending the Fax to the users.</p> <p>The template variables are:</p> <ul style="list-style-type: none"> ◦ <code>{CALLERIDNUM}</code> : Caller ID Number ◦ <code>{CALLERIDNAME}</code> : Caller ID Name ◦ <code>{RECEIVEEXTEN}</code> : The extension to receive the Fax ◦ <code>{FAXPAGES}</code> : Number of pages in the Fax ◦ <code>{VM_DATE}</code> : 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 | <p>Enables the fax resend option which allow the UCM to keep attempting to send faxes up to a specified amount of times.</p> <p>Additionally, if a fax still fails to send, a <i>Resend</i> button will appear in the File Send Progress list in <i>OtherFeatures</i>→<i>Fax Sending</i> to allow manual resending.</p> |
| Max Resend Attempts | <p>Configures the maximum attempts number to resend the fax.</p> <p>Default value is set to 5.</p> |
| Fax Resend Frequency | <p>Configures the Fax Resend Frequency.</p> <p>Default value is set to 50.</p> |

Receiving Fax

Example Configuration to Receive Fax from PSTN Line

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

1. Connect Fax machine to the UCM6300A FXS port.
2. Connect PSTN line to the UCM6300A FXO port.
3.
 - Go to Web GUI→**Extension/Trunk** page.
4. Create or edit the analog trunk for Fax as below.

Fax Detection: Make sure “Fax Detection” option is set to “NO”.

| | | | |
|------------------------------------|--|-------------------------------------|-----------------------------------|
| * FXO Port: | <input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 | * Trunk Name: | <input type="text" value="FAX"/> |
| Advanced Options | | | |
| SLA Mode: | <input type="checkbox"/> | * Ring Timeout: | <input type="text" value="8000"/> |
| Enable Polarity Reversal: | <input type="checkbox"/> | * TX Gain: | <input type="text" value="0dB"/> |
| Current Disconnect Threshold (ms): | <input checked="" type="checkbox"/> <input type="text" value="200"/> | Fax Mode: | <input type="text" value="None"/> |
| * RX Gain: | <input type="text" value="0dB"/> | * FXO Dial Delay (ms): | <input type="text" value="0"/> |
| Use CallerID: | <input checked="" type="checkbox"/> | Disable This Trunk: | <input type="checkbox"/> |
| Caller ID Scheme: | <input type="text" value="Bellcore/Telcordia"/> | * The Maximum Number of Call Lines: | <input type="text" value="0"/> |
| Auto Record: | <input type="checkbox"/> | Direct Callback: | <input type="checkbox"/> |
| DAHDI Out Line Selection: | <input type="text" value="Ascend"/> | | |
| Echo Cancellation Mode: | <input type="text" value="Default"/> | | |

Figure 132: Configure Analog Trunk

1. Go to UCM6300A Web GUI→Extension/Trunk→Extensions page.
2. Create or edit the extension for FXS port.
 - o **Analog Station:** Select FXS port to be assigned to the extension. By default, it is set to “None”.
 - o 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: | <input type="text" value="FXS Extension"/> | | |
| Select Add Method: | <input type="text" value="Single"/> | | |
| General | | | |
| * Extension: | <input type="text" value="1005"/> | Analog Station: | <input type="text" value="FXS 1"/> |
| CallerID Number: | <input type="text"/> | * Privilege: | <input type="text" value="Internal"/> |
| Voicemail: | <input type="text" value="Local Voicemail"/> | * Voicemail Password: | <input type="text" value="96902350"/> |
| Skip Voicemail Password Verification: | <input type="checkbox"/> | Send Voicemail Email Notification: | <input type="text" value="Default"/> |
| Attach Voicemail to Email: | <input type="text" value="Default"/> | Keep Voicemail after Emailing: | <input type="text" value="Default"/> |
| Disable This Extension: | <input type="checkbox"/> | Emergency Calls CID: | <input type="text"/> |

Figure 133: Configure Extension for Fax Machine: FXS Extension

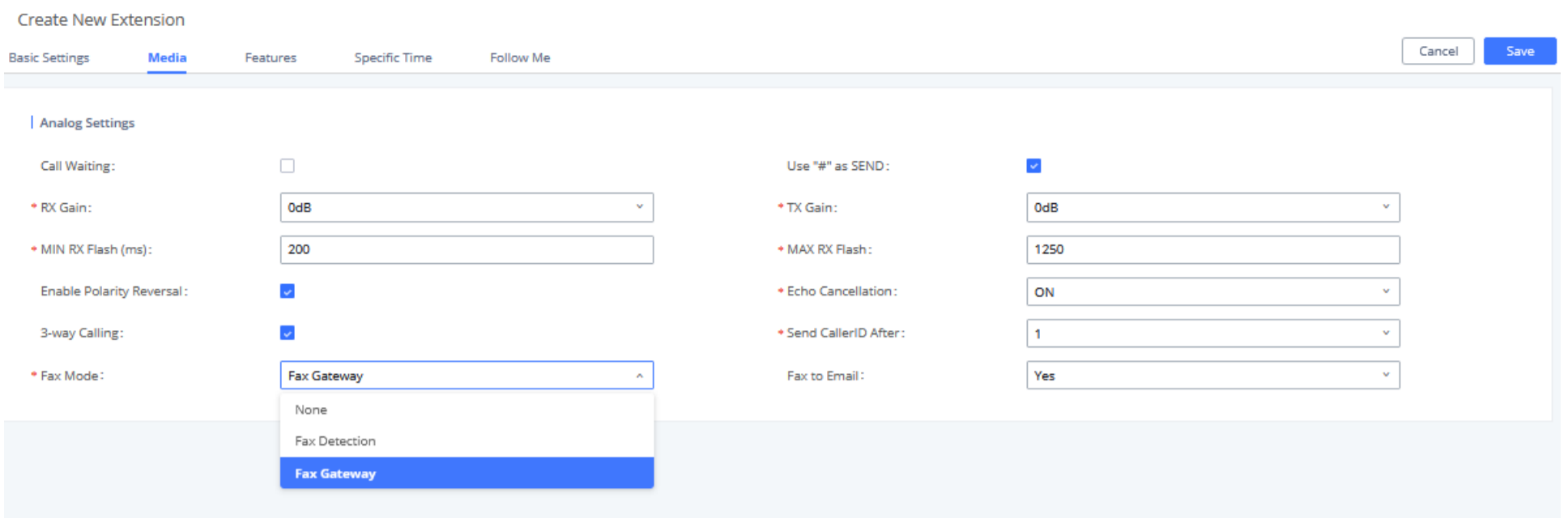


Figure 134: Configure Extension for Fax Machine: Analog Settings

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.

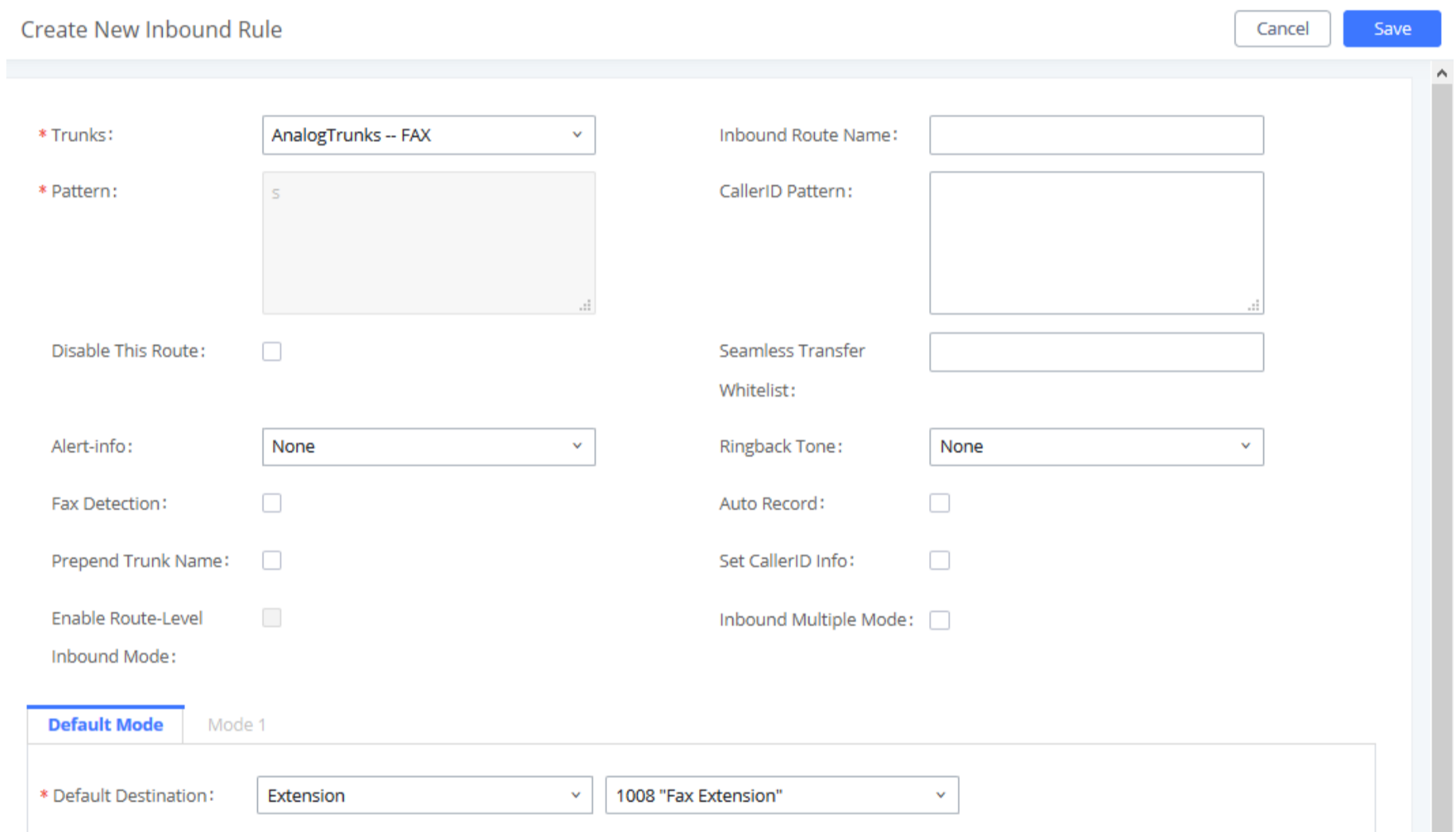


Figure 135: Configure Inbound Rule for Fax

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

Create New Fax Extension

* Extension:

* Name:

* Email Address: -

[Add Email Address](#) +

Figure 136: Create Fax Extension

1. Go to UCM6300A Web GUI→**Extension/Trunk**→**Analog Trunks** page. Create a new analog trunk. Please make sure “Fax Detection” is set to “No”.
2. Go to UCM6300A Web GUI→**Extension/Trunk**→**Inbound Routes** page. Create a new inbound route and set the default destination to the Fax extension.

Create New Inbound Rule

Cancel Save

* Trunks:

* Pattern:

Disable This Route:

Alert-info:

Fax Detection:

Prepend Trunk Name:

Enable Route-Level Inbound Mode:

Inbound Route Name:

CallerID Pattern:

Seamless Transfer Whitelist:

Ringback Tone:

Auto Record:

Set CallerID Info:

Inbound Multiple Mode:

Default Mode Mode 1

* Default Destination:

Figure 137: Inbound Route to Fax Extension

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

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

List of Fax Files

Delete Clear

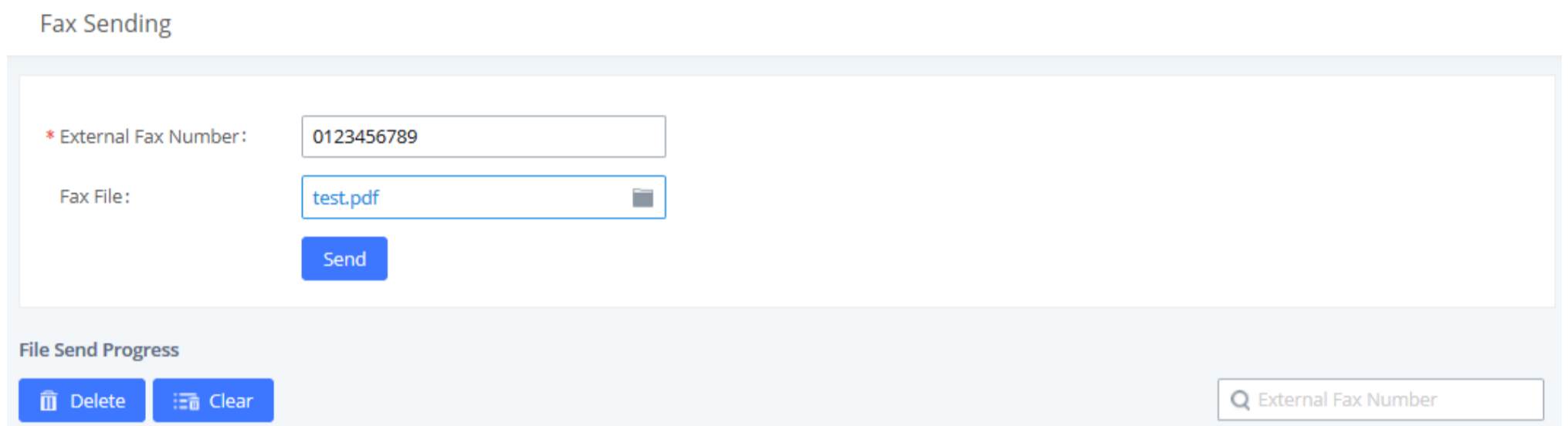
| <input type="checkbox"/> | NAME ↕ | DATE ↕ | SIZE ↕ | OPTIONS |
|--------------------------|--|-------------------------------|---------|---------|
| <input type="checkbox"/> | VFAX-7200-20210125-112246-1611570166.49.pdf | 2021-01-25 11:22:46 UTC+01:00 | 1.49 KB | |
| <input type="checkbox"/> | VFAX-7200-20210125-112246-1611570166.49.tiff | 2021-01-25 11:22:46 UTC+01:00 | 5.69 KB | |

Figure 138: 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→Other 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.

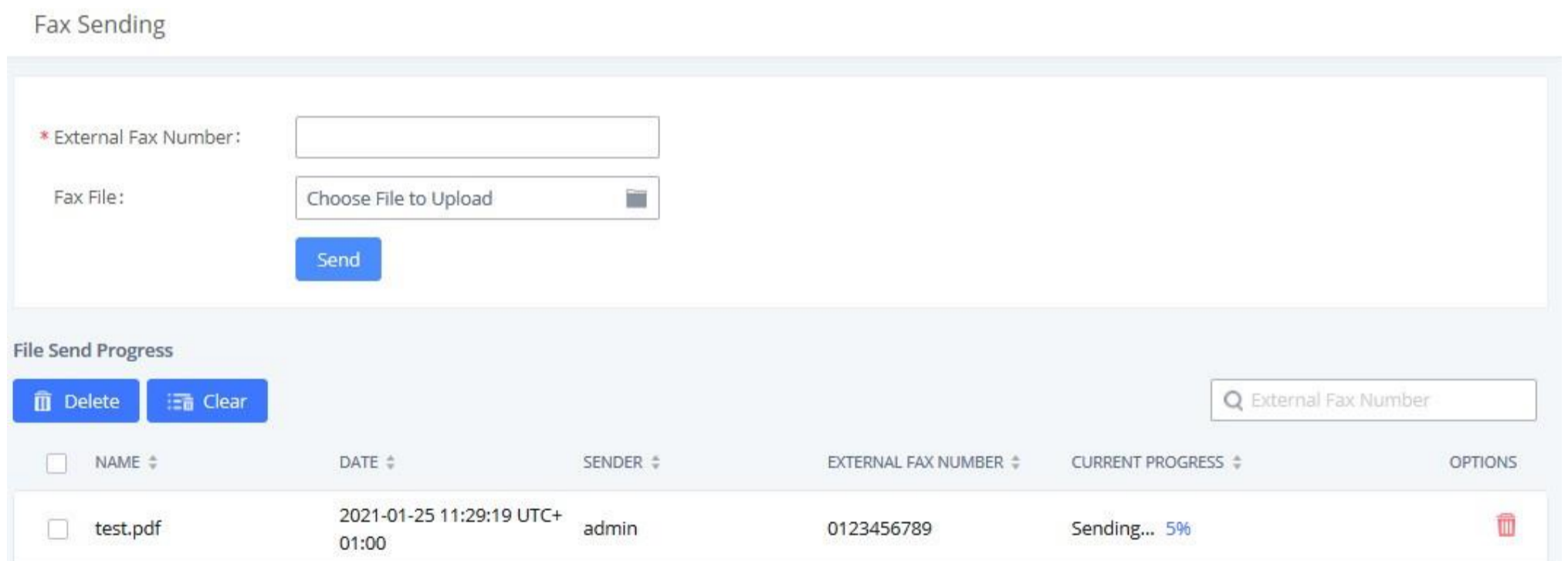
After making sure analog trunk or VoIP Trunk is setup properly and UCM6300A can reach out to PSTN numbers via the trunk, on Fax Sending page, enter the fax number and upload the file to be faxed. Then click on “Send” to start. The progress of sending fax will be displayed in Web GUI. Users can also view the sending history is in the same web page.



The screenshot shows the 'Fax Sending' web GUI. At the top, there is a form with two input fields: '* External Fax Number:' containing '0123456789' and 'Fax File:' containing 'test.pdf'. Below these fields is a blue 'Send' button. Underneath the form is a 'File Send Progress' section with 'Delete' and 'Clear' buttons. On the right side of this section is a search box labeled 'External Fax Number'.

Figure 139: Fax Sending in Web GUI

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



The screenshot shows the 'Fax Sending' web GUI with the progress bar. The form fields are empty. The 'File Send Progress' section contains a table with the following data:

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

Figure 140: Fax Send Progress

Note

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

MEETING

With the UCM you can easily create, schedule, manage, and join meeting calls, from your desktop or laptop computer. UCM conferencing uses [WebRTC technology](#), so all the participants don't have to download and install any additional software or plugins. UCM conferencing must be enabled by the administrator for the concerned extensions. The meeting configurations can be accessed under Web GUI → **Call Features** → **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.

Table 72: 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. |
|----------------------|--|

Note

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

Meeting Settings contains the following options:

Table 73: Meeting Settings

| | |
|-------------------------------|--|
| Enable Talk detection | If enabled, the AMI will send the corresponding event when a user starts or ends talking. |
| DSP Talking Threshold | The time in milliseconds of sound above what the dsp has established as base line silence for a user before a user is considered to be talking. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 200. |
| DSP Silence Threshold | The time in milliseconds of sound falling within the dsp has established as base line silence before a user is considered to be silent. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 2500. |
| Audio Codec Preference | Configures the preferred codecs for temporary accounts such as meeting participants who joined via link. |
| Jitter Buffer | Select jitter buffer method for temporary accounts such as meeting participants who joined via link. <ul style="list-style-type: none"> • Disable: Jitter buffer will not be used. • Fixed: Jitter buffer with a fixed size (equal to the value of "Jitter Buffer Size") • Adaptive: Jitter buffer with an adaptive size that will not exceed the value of "Max Jitter Buffer"). • NetEQ: Dynamic jitter buffer via NetEQ. |

Meeting Schedule

Meeting Schedule can be found under UCM **Web GUI** → **Call Features** → **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.

Table 74: Meeting Schedule Parameters

| Schedule Options | |
|------------------------|---|
| Meeting Subject | Configure the name of the scheduled conference. Letters, digits, Other special characters are also supported. such as #%&@*=- |

| | |
|--------------------------------------|--|
| Meeting Room | <p>Choose which room to have this scheduled meeting.</p> <p>If this option has been enabled, please select an existing room for this meeting. If this option has not been enabled, a new meeting room will be created.</p> |
| Time | Configure the meeting date and time. |
| Time Zone | Select the meeting time zone. |
| Password | Configure the conference login password. |
| Host Password | <p>Configure the Host Password.</p> <p>Note: It is randomly generated when first creating a new meeting Schedule.</p> |
| Host | Configure Host. |
| Repeat | Choose when to repeat a scheduled conference. |
| Allow User Invite | <p>If this option is enabled, the user can:</p> <ul style="list-style-type: none"> • Press '0' to invite others to join the meeting with invited party's permission • Press '1' to invite without invited party's permission • Press '2' to create a multi-meeting room to another meeting room • Press '3' to drop all current multi-meeting rooms. <p>Note: Meeting host is always allowed to access this menu.</p> |
| 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. |
| Email Reminder (m) | <p>Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-1440. 60 is the default value. 0 indicates not to send out email reminders for the meeting.</p> <p>Note: After editing the time of a single recurrence of a scheduled meeting, a cancelation email will now be sent out followed by a meeting update email.</p> |
| Auto Record | <p>If selected, the meeting will be recorded and saved as either a .WAV or .MKV file. The default filename is meeting-$\{Meeting\ Number\}$-$\{UNIQUEID\}$. Recordings can be downloaded from either the Meeting Recordings or the Meeting Video Recordings page. Video recordings require external storage to be available. When recording a screen share, only the screen share and meeting audio will be recorded.</p> <p>Note: Please note that UCM63XX Audio Series doesn't support Screen Sharing, Whiteboard, or PDF file sharing.</p> |
| Enable Google Calendar | <p>Select this option to sync scheduled conference with Google Calendar.</p> <p>Note: Google Service Setting OAuth2.0 must be configured on the UCM630X. Please refer to section <i>[Google Service Settings Support]</i>.</p> |
| Meeting Agenda | Enter information about the meeting, e.g., the purpose of the meeting or the subjects that will be discussed in the meeting. |

| | |
|-----------------|--|
| Invitees | Local extensions, remote extensions, and special extensions are supported. |
|-----------------|--|

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

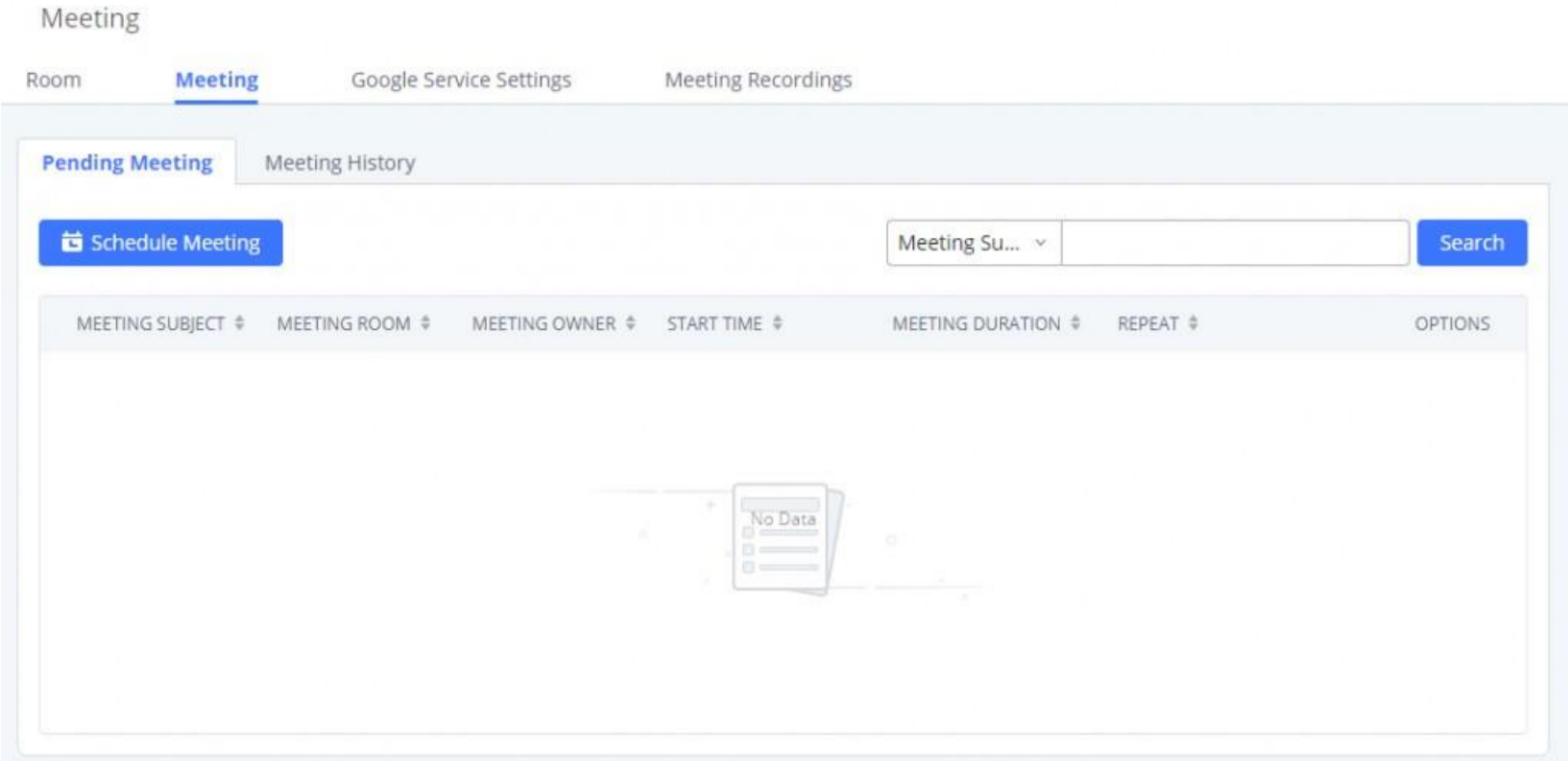


Figure 141: Meeting Schedule

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

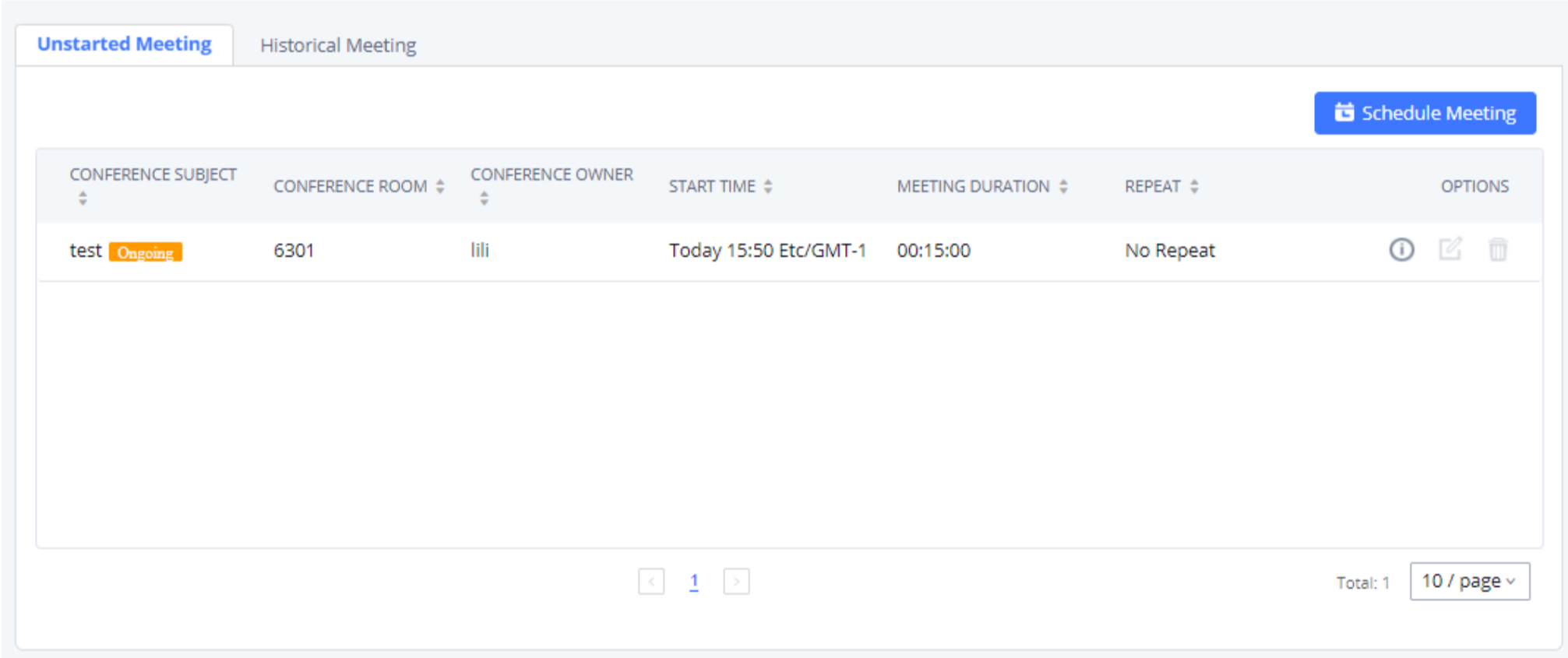





Figure 142: Meeting Scheduled-Ongoing

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

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

< 1 >

Total: 1 10 / page

Figure 143: Meeting Scheduled-Completed

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

Notes

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

Meeting Recordings

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

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

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



to download the recording or click on



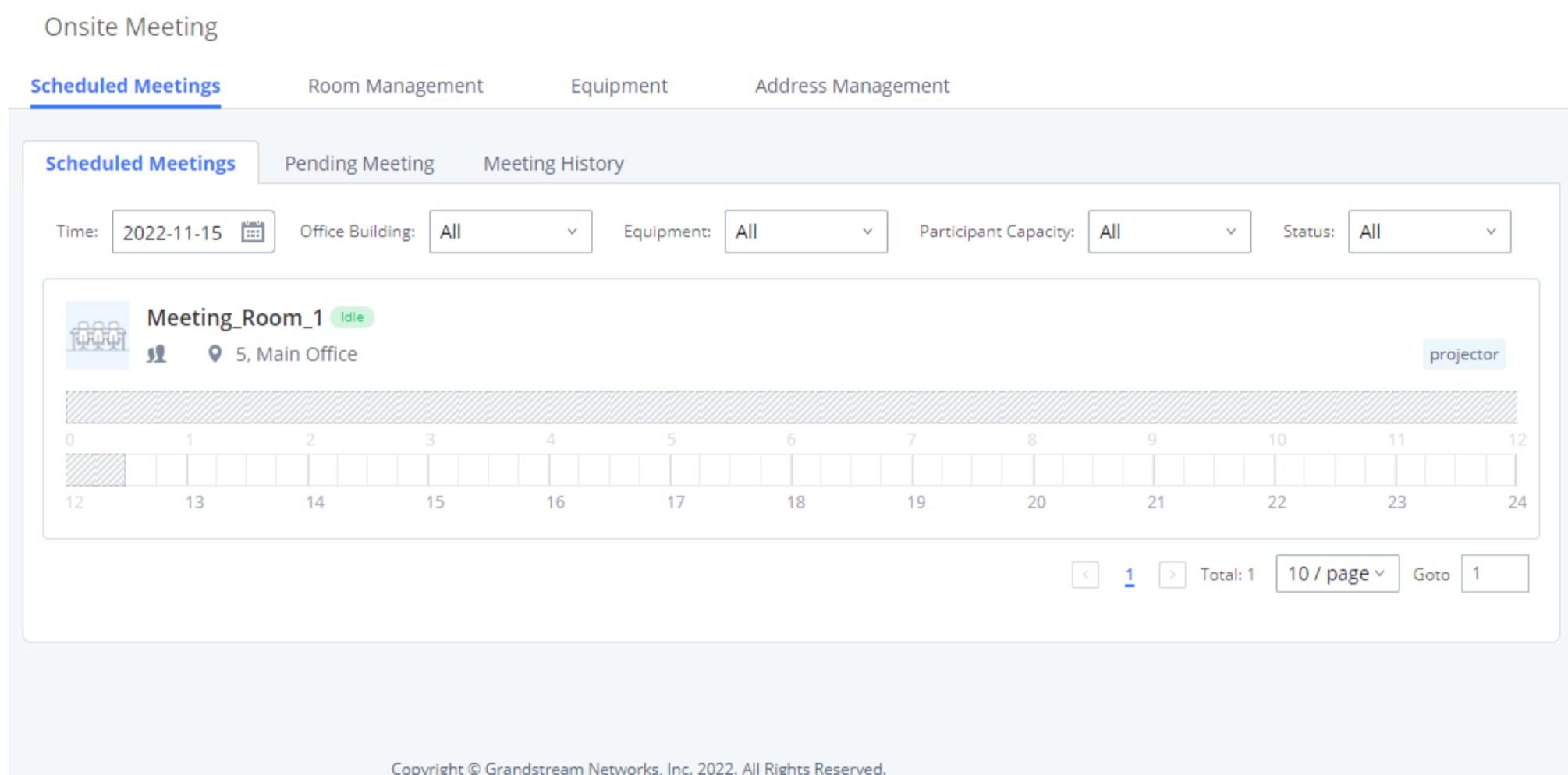
to delete the recording. Users could also delete all recording files by clicking on “Delete All Recording Files” or delete multiple recording files at once by clicking on “Delete” after selecting the recording files.

| Meeting | | | | | | |
|--|---------|-------------------------|--------------------|------|---------|--|
| Room | Meeting | Google Service Settings | Meeting Recordings | | | |
| <input type="button" value="Download"/> <input type="button" value="Download All"/> <input type="button" value="Delete"/> <input type="button" value="Clear"/> | | Local | 2022-05 | | | |
| <input type="checkbox"/> | NAME | ROOM | DATE | SIZE | OPTIONS | |
| No Data | | | | | | |

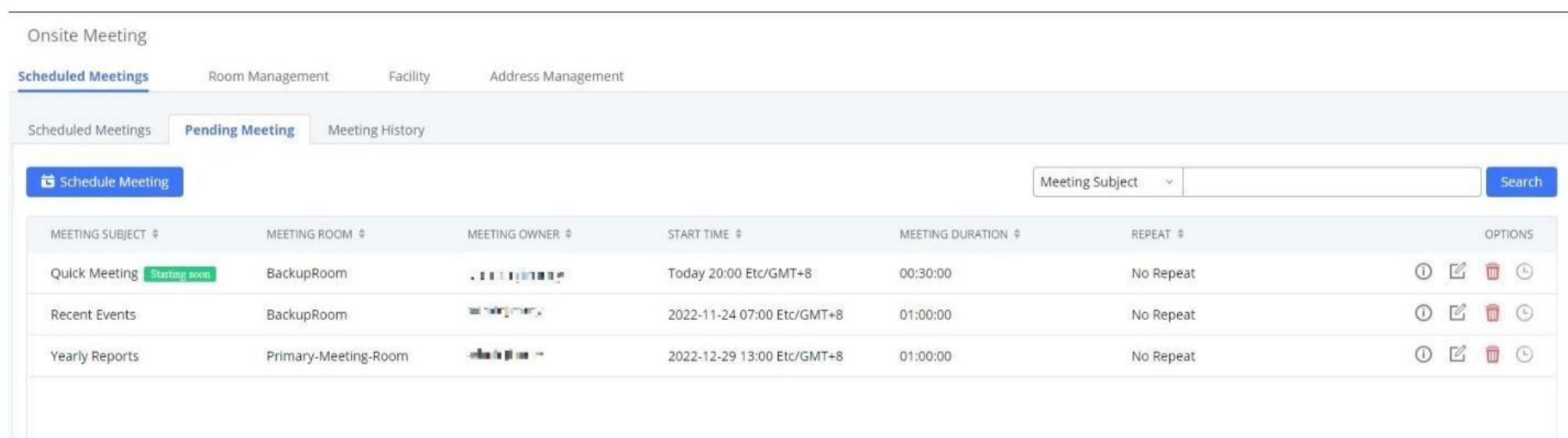
Figure 144: Meeting Recordings

ONSITE MEETING

For workplaces that require employees to return to physical offices for work, Grandstream UCM offers the Onsite Meetings feature, a new way to stay organized and keep up-to-date with in-person meetings. This feature allows administrators to create and manage onsite meeting rooms, specify meeting room locations, schedule meetings, and add conferencing equipment. The new feature can be found under the *Other Features*→*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.



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



IVR

Configure IVR

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

- Click on “Add” to add a new IVR.

- Click on



to edit the IVR configuration.

- o Click on



to delete the IVR.

Create New IVR

Basic Settings Key Pressing Events

• Name:

• Extension:

Dial Trunk:

Auto Record:

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

• IVR Black/Whitelist:

Replace Display Name:

Return to IVR Menu:

Alert-info:

• Prompt: [Upload Audio File](#)

[Add Prompt](#)

• Digit Timeout (s):

• Response Timeout:

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

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

• Response Timeout Prompt Repeats:

• Invalid Input Prompt Repeats:

Language:

Figure 145: Create New IVR

Table 75: IVR Configuration Parameters

| Basic Settings | |
|--------------------|--|
| Name | Configure the name of the IVR. Letters, digits, _ and – are allowed. |
| Extension | Enter the extension number for users to access the IVR. |
| Dial Trunk | If enabled, all callers to the IVR can use trunk. The permission must be configured for the users to use the trunk first. The default setting is “No”. |
| Auto Record | If enabled, calls to this IVR will automatically be recorded. |

| | |
|---------------------------------|--|
| Permission | <p>Assign permission level for outbound calls if “Dial Trunk” is enabled. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level.</p> <p>The default setting is “Internal”. If the user tries to dial outbound calls after dialing into the IVR, the UCM630xA will compare the IVR’s permission level with the outbound route’s privilege level.</p> <p>If the IVR’s permission level is higher than (or equal to) the outbound route’s privilege level, the call will be allowed to go through.</p> |
| Dial Other Extensions | <p>This controls the destination that can be reached by the external caller via the inbound route. The available destinations are:</p> <ul style="list-style-type: none"> ◦ Extension ◦ Meeting ◦ Call Queue ◦ Ring Group ◦ Paging/Intercom Groups ◦ Voicemail Groups ◦ Dial by Name ◦ All |
| IVR Black/Whitelist | If enabled only numbers inside of the Whitelist or outside of the Blacklist can be called from IVR. |
| Internal Black/Whitelist | Contain numbers, either of Blacklist or Whitelist. |
| External Black/Whitelist | This feature can be used only when Dial Trunk is enabled, it contains external numbers allowed or denied calling from the IVR, the allowed format is the following: Number1, number2, number3... |
| Replace Display Name | If enabled, the UCM will replace the caller display name with IVR name. |
| Return to IVR Menu | If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu. |
| Alert Info | When present in an INVITE request, the alert-Info header field specifies an alternative ring tone to the UAS. |
| Prompt | Select an audio file to play as the welcome prompt for the IVR. Click on “Prompt” to add additional audio file under Web GUI→PBX Settings→Voice Prompt→Custom Prompt. |
| Digit Timeout | Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, the UCM630xA will consider the entries complete. Default timeout is 3s. |
| Response Timeout | After playing the prompts in the IVR, the UCM630xA will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout prompt will be played. The default setting is 10 seconds. |
| Response Timeout Prompt | Select the prompt message to be played when timeout occurs. |
| Invalid Input Prompt | Select the prompt message to be played when an invalid extension is pressed. |

| | |
|--|--|
| Response Timeout Prompt Repeats | Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3. |
| Invalid Input Prompt Repeats | Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3. |
| Language | Select the voice prompt language to be used for this IVR. The default setting is “Default” which is the selected voice prompt language under Web GUI→ PBX Settings → Voice Prompt → Language Settings . The dropdown list shows all the current available voice prompt languages on the UCM630xA. To add more languages in the list, please download voice prompt package by selecting “Check Prompt List” under Web GUI→ PBX Settings → Voice Prompt → Language Settings . |
| Key Pressing Events | |
| Key Press Event: | Select the event for each key pressing for 0-9, *, Timeout and Invalid. The event options are: |
| Press 0 | <ul style="list-style-type: none"> ◦ Extension ◦ Voicemail ◦ Meeting Rooms ◦ Voicemail Group |
| Press 1 | <ul style="list-style-type: none"> ◦ IVR |
| Press 2 | <ul style="list-style-type: none"> ◦ Ring Group |
| Press 3 | <ul style="list-style-type: none"> ◦ Queues |
| Press 4 | <ul style="list-style-type: none"> ◦ Page Group |
| Press 5 | <ul style="list-style-type: none"> ◦ Custom Prompt |
| Press 6 | <ul style="list-style-type: none"> ◦ Hangup |
| Press 7 | <ul style="list-style-type: none"> ◦ DISA ◦ Dial by Name |
| Press 8 | <ul style="list-style-type: none"> ◦ External Number |
| Press 9 | <ul style="list-style-type: none"> ◦ Callback |
| Press * | <p>For each key event, time condition can be configured. At the configured time condition, this IVR key event can be triggered. Office time, holiday time or specific time can be configured for time condition. Up to 5 time conditions can be added for each key.</p> <p>The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’ and ‘Specific Time’. If ‘Specific Time’ is selected, a new window will prompt for admin to configure start time, end time and frequency.</p> |
| 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. |

Edit IVR: test

Basic Settings **Key Pressing Events** Cancel Save

Press 0

Destination: Extension 3001 Time Condition: Specific Time

| TIME | WEEK | MONTH | DAY | OPTIONS |
|-------------|-----------------------------|---------|---------|---------|
| 08:00-11:00 | Sun Mon Tue Wed Thu Fri Sat | Default | Default | |

[Add](#) +

Press 1

Destination: Select an Option Time Condition: All Time

[Add](#) +

Press 2

Destination: Select an Option Time Condition: All Time

[Add](#) +

Press 3

Destination: Select an Option Time Condition: All Time

[Add](#) +

Press 4

Destination: Select an Option Time Condition: All Time

[Add](#) +

Figure 146: Key Pressing Events

Blacklist/Whitelist in IVR

In some scenarios, the IPPBX administrator needs to restrict the extensions that can be reached from IVR.

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

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

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

- If the user selects “Blacklist Enable” and adds extension in the list, the extensions in the list will not be allowed to be reached via IVR.
- If the user selects “Whitelist Enable” and adds extension in the list, only the extensions in the list can be allowed to be reached via IVR.

Create New IVR

Basic Settings Key Pressing Events

* Name:

* Extension:

Dial Trunk:

* Permission:

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

* IVR Black/Whitelist:

Internal Black/Whitelist:

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

External Blacklist/Whitelist:

Figure 147: Black/Whitelist

Create Custom Prompt

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

Alert-info:

* Prompt:

[Add Prompt](#)

Figure 148: Click on Prompt to Create IVR Prompt

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

Key Pressing Events

Standard Key Event

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

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

Press 0
Destination: Select an Option
Time Condition: Office Time

Press 0
Destination: Select an Option
Time Condition: Holiday

Press 1
Destination: Select an Option
Time Condition:

Figure 162: Key Pressing Events

Note:

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

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

Specific Time

Time: Start Time - End Time

Frequency: By Week By Month

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

Week Day

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

Excluding Holidays:

Cancel OK

Figure 163: Specific Time

Custom Key Event

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

This new feature supports the following:

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

Note

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

LANGUAGE SETTINGS FOR VOICE PROMPT

The UCM630xA supports multiple languages in Web GUI as well as system voice prompt. Currently, there are 16 languages supported in system voice prompt: *English (United States), Arabic, Chinese, Dutch, English (United Kingdom), French, German, Greek, Hebrew, Italian, Polish, Portuguese, Russian, Spanish, Catalan, Swedish and Turkish.*

English (United States) and Chinese voice prompts are built in with the 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.

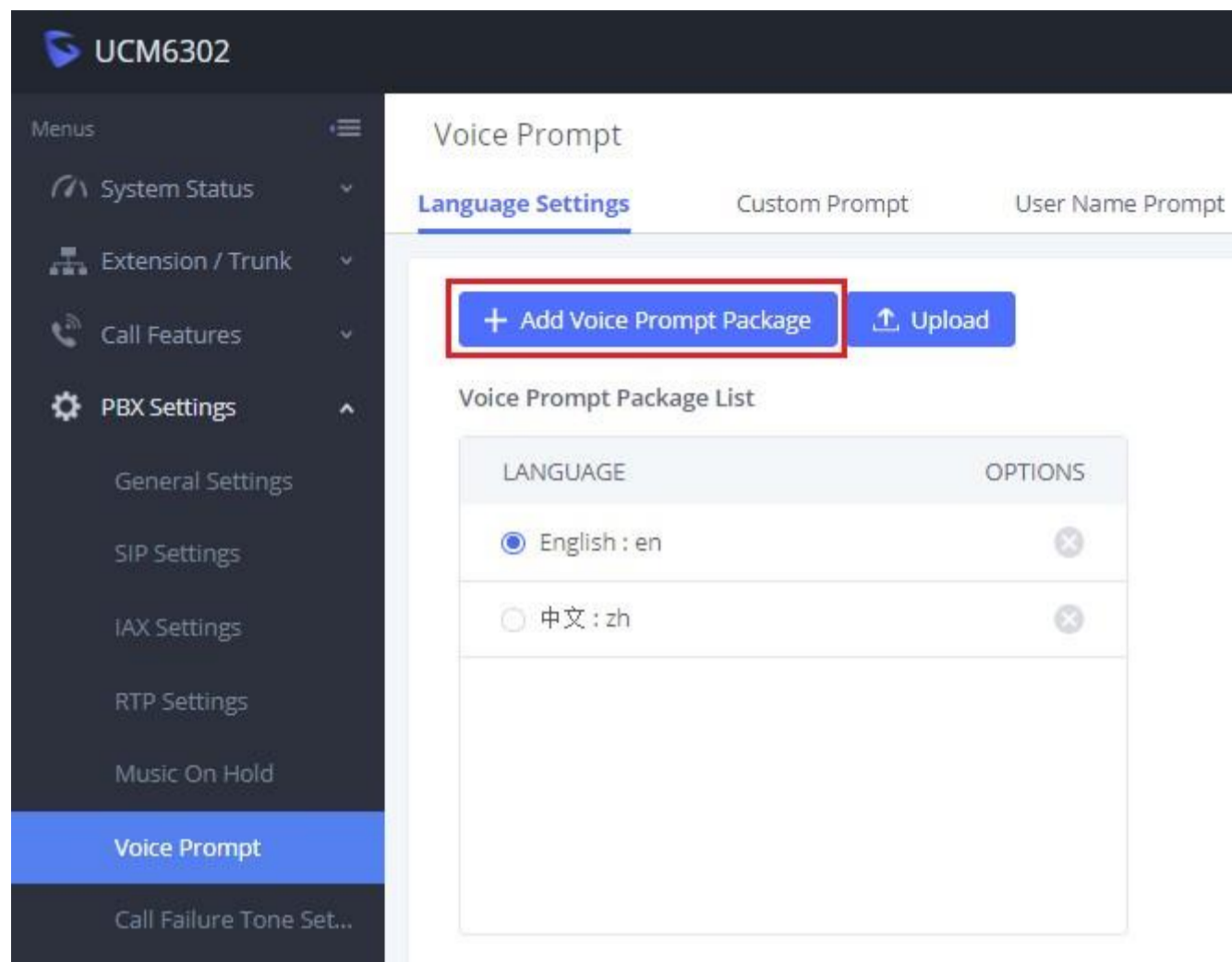


Figure 151: Language Settings for Voice Prompt

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.

The 'Details' dialog window displays a table with the following data:

| VOICE PROMPT PACKAGE LIST | VERSION (REMOTE / LOCAL) | SIZE | OPTIONS |
|---------------------------|--------------------------|------|---------|
| British English | 1.9/- | 4.2M | ↓ |
| Deutsch | 1.8/- | 4.2M | ↓ |
| English | 1.11/1.8 | 6.0M | ⬆ |
| Español | 1.10/- | 4.4M | ↓ |
| Español(Català) | 1.8/- | 3.1M | ↓ |
| Español(Español) | 1.8/- | 4.2M | ↓ |
| Ελληνικά | 1.8/- | 4.4M | ↓ |
| Français | 1.8/- | 4.1M | ↓ |
| Italiano | 1.8/- | 4.0M | ↓ |

Figure 152: Voice Prompt Package List

Click on



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

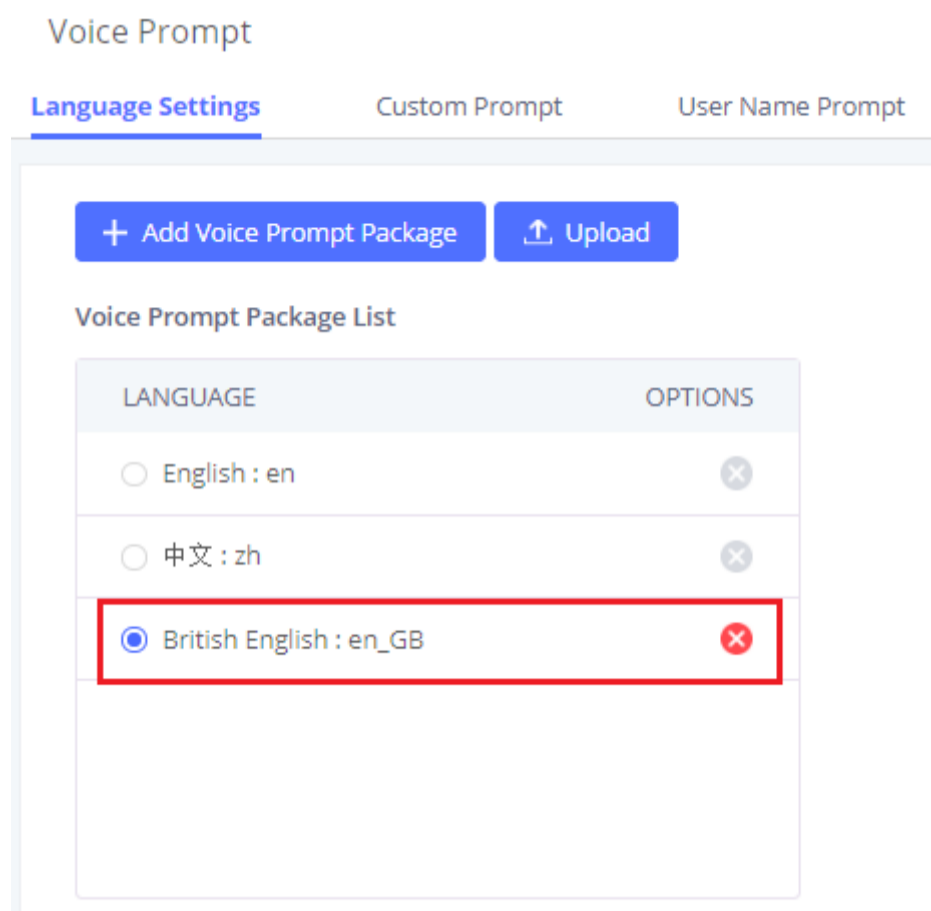


Figure 153: New Voice Prompt Language Added

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

Customize Specific Prompt

On the UCM630xA, if the user needs to replace some specific customized prompt, the user can upload a single specific customized prompt from Web GUI→PBX Settings→Voice Prompt→Language Settings and click on “Upload” instead of the entire language pack.

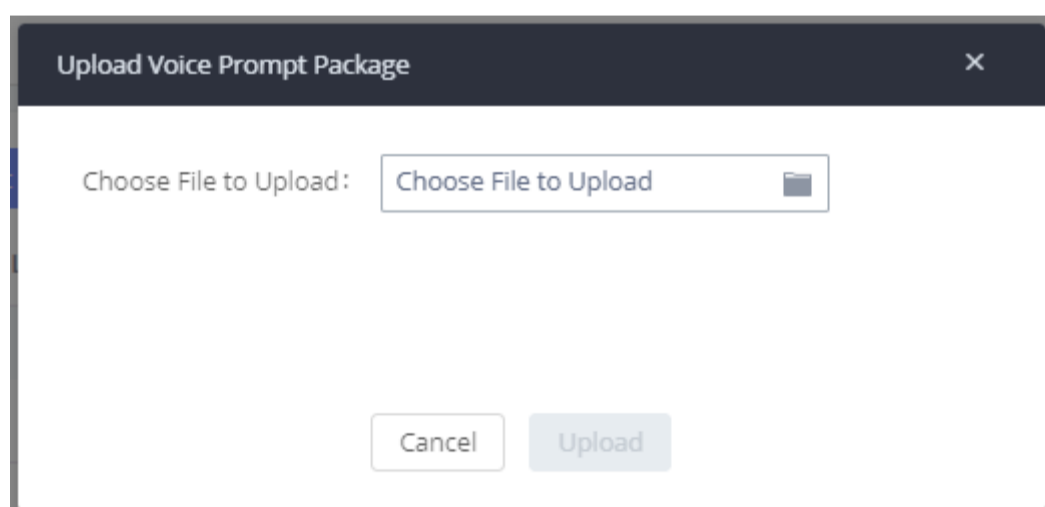


Figure 154: Upload Single Voice Prompt for Entire Language Pack

Username Prompt Customization

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

Upload Username Prompt File from Web GUI

1. First, Users should have a pre-recorded file respecting the following format:

- PCM encoded / 16 bits / 8000Hz mono.
- In .tar/.tar.gz/.tgz format
- File size under 30M.
- Filename must be set as the extension number with 18 characters max. For example, the recorded file name 1000.wav will be used for extension 1000.

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

2. Select the recorded file to upload it and press Save and Apply Settings.

- Click on



to record again the username prompt.

- Click on to play recorded username prompt.

- Select username prompts and press



to delete specific file or select multiple files for deletion using the button **”Delete”** .

Record Username via Voicemail Menu

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

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

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

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

VOICEMAIL

Configure Voicemail

If the voicemail is enabled for UCM630xA extensions, the configurations of the voicemail can be globally set up and managed under Web GUI→**Call Features**→**Voicemail**.

* Max Greeting Time (s):

Dial "0" for Operator:

Operator Type:

Operator Extension:

* Max Messages Per Folder:

Max Message Time:

Min Effective Message Time:

Announce Message Caller-ID:

Announce Message Duration:

Play Envelope:

Play Most Recent First:

Allow User Review:

Voicemail Remote Access:

Forward Voicemail to Peered UCMS:

UCMs:

Voicemail Password:

Format:

Figure 155: Voicemail Settings

| | |
|--------------------------------|---|
| Max Greeting Time (s) | Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds. |
| Dial '0' For Operator | If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator's extension. |
| Operator Type | Configure the operator type; either an extension or a ring group. |
| Operator Extension | Select the operator extension, which will be dialed when users press 0 to exit voicemail application. The operator extension can also be used in IVR. |
| Max Messages Per Folder | Configure the maximum number of messages per folder in users' voicemail. The valid range 10 to 1000. The default setting is 50. |
| Max Message Time | <p>Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the max message time. The default setting is 15 minutes. The available options are:</p> <ul style="list-style-type: none"> ○ 1 minute ○ 2 minutes ○ 5 minutes ○ 15 minutes ○ 30 minutes ○ Unlimited |

| | |
|--|---|
| <p>Min Effective Message Time</p> | <p>Configure the minimum duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Message Time. The default setting is 3 seconds. The available options are:</p> <ul style="list-style-type: none"> ○ No minimum ○ 1 second ○ 2 seconds ○ 3 seconds ○ 4 seconds ○ 5 seconds <p>Note: Silence and noise duration are not counted in message time.</p> |
| <p>Announce Message Caller-ID</p> | <p>If enabled, the caller ID of the user who has left the message will be announced at the beginning of the voicemail message. The default setting is “No”.</p> |
| <p>Announce Message Duration</p> | <p>If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is “No”.</p> |
| <p>Play Envelope</p> | <p>If enabled, a brief introduction (received time, received from, and etc.) of each message will be played when accessed from the voicemail application. The default setting is “Yes”.</p> |
| <p>Play Most Recent First</p> | <p>If enabled, it will play the most recent message first.</p> |
| <p>Allow User Review</p> | <p>If enabled, users can review the message following the IVR before sending.</p> |
| <p>Voicemail Remote Access</p> | <p>If enabled, external callers routed by DID and reaching VM will be prompted by the UCM with 2 options:</p> <ul style="list-style-type: none"> ○ <i>Press 1 to leave a message.</i> <p>To leave a message for the extension reached by DID.</p> <ul style="list-style-type: none"> ○ Press 2 to access voicemail management system. <p>This will allow caller to access any extension VM after entering extension number and its VM password.</p> <p>Note: This option applies to inbound call routed by DID only.</p> <p>The default setting is “Disabled”.</p> |
| <p>Forward Voicemail to Peered UCMs</p> | <p>Enables the forwarding of voicemail to remote extensions on peered SIP trunks.</p> <p>The default setting is “Disabled”.</p> |
| <p>Voicemail Password</p> | <p>Configures the default voicemail password that will be used when an extension is reset.</p> |
| <p>Format</p> | <p>Warning: WAV files take up significantly more storage space than GSM files.</p> |

Table 76: Voicemail Settings

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

Access Voicemail

If the voicemail is enabled for UCM630xA extensions, the users can dial the voicemail access number (by default *97) to access their extension's voicemail. The users will be prompted to enter the voicemail password and then can enter digits from the phone keypad to navigate in the IVR menu for different options.

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

| Main Menu | Sub Menu 1 | Sub Menu 2 |
|---------------------------|---|---|
| 1 – New messages | 3 - Advanced options | 1 - Send a reply |
| | | 2 - Call the person who sent this message |
| | | 3 - Hear the message envelop |
| | | 4 - Leave a message |
| | | * - Return to the main menu |
| | 5 - Repeat the current message | |
| | 7 - Delete this message | |
| | 8 - Forward the message to another user | |
| | 9 – Save | |
| | * - Help | |
| # - Exit | | |
| 2 – Change folders | 0 - New messages | |
| | 1 - Old messages | |
| | 2 - Work messages | |
| | 3 - Family messages | |
| | 4 - Friend messages | |
| | # - Cancel | |

| | | |
|-----------------------------|---|----------------------------|
| 3 – Advanced options | 1 - Send a reply | |
| | 2 - Call the person who sent this message | |
| | 3 - Hear the message envelop | |
| | 4 - Leave a message | |
| | * - Return to the main menu | |
| 0 – Mailbox options | 1 - Record your unavailable message | 1 - Accept this recording |
| | | 2 - Listen to it |
| | | 3 - Re-record your message |
| | 2 - Record your busy message | 1 - Accept this recording |
| | | 2 - Listen to it |
| | | 3 - Re-record your message |
| | 3 - Record your name | 1 - Accept this recording |
| | | 2 - Listen to it |
| | | 3 - Re-record your message |
| | 4 - Record temporary greeting | 1 - Accept this recording |
| | | 2 - Listen to it |
| | | 3 - Re-record your message |
| | 5 - Change your password | |
| | * - Return to the main menu | |

 **Tips**

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

Leaving Voicemail

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

In case if the caller is calling from an internal extension, they will be directly forwarded to the extension’s voicemail box. But if the caller is calling from outside the system and the incoming call is routed by DID to the destination extension, then the caller will be prompted with the choice to either press 1 to access voicemail management or press 2 to leave a message for the called extension. This feature could be useful for remote voicemail administration.

Voicemail Email Settings

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

| | |
|--------------------------------------|---|
| 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 | <p>Fill in the “Subject:” and “Message:” content, to be used in the Email when sending to the user.</p> <p>The template variables are:</p> <ul style="list-style-type: none">◦ \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 |

Table 78: Voicemail Email Settings

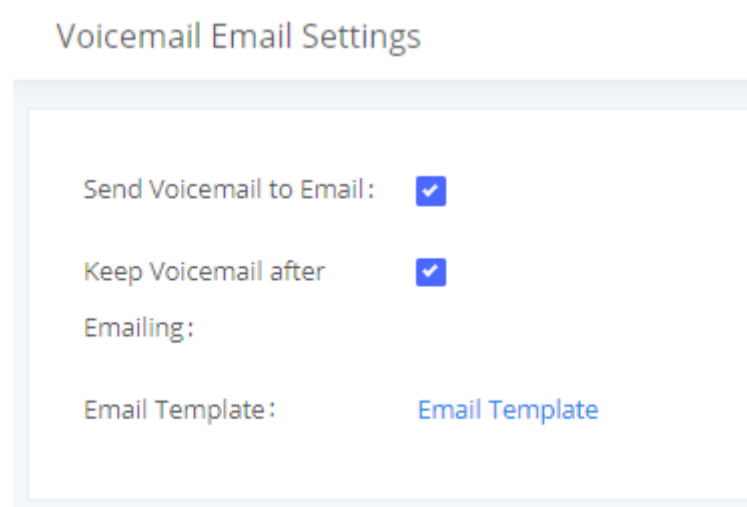


Figure 156: Voicemail Email Settings

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

Configure Voicemail Group

The UCM630xA supports voicemail group and all the extensions added in the group will receive the voicemail to the group extension. The voicemail group can be configured under Web GUI → Call Features → Voicemail → Voicemail Group. Click on “Add” to configure the group.

Voicemail > Edit Voicemail Groups: Voicemail_Group1
Cancel Save

* Extension

* Name

Voicemail Password

Email Address

Shared Voicemail Status

Members

159 items Available

Search

- 1003 "Catherine ...
- 1004 "John Mars...
- 1005 "Abigail Ro...
- 1006 "Mary-Beth...
- 1007 "Hosea Ma...
- 1008

0 item Selected

Search

None

Voicemail prompt will be played when user enters voicemail. Priority: Temporary 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.

Greet Prompt Download Delete

Temporary Prompt Download Delete

Unavailable Prompt Download Delete

© 2023 Grandstream Networks, Inc.

Voicemail Group

| | |
|--------------------------------|--|
| Extension | Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members. |
| Name | Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed. |
| Voicemail Password | Configure the voicemail password for the users to check voicemail messages. |
| Email Address | Configure the Email address for the voicemail group extension. |
| Shared Voicemail Status | If enabled, voicemail group status can be monitored via BLF. Green indicates no unread voicemail, and red indicates existing unread voicemail. |

| | |
|---------------------------|---|
| Member | Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list. |
| Busy Prompt | <p>This voicemail prompt will be played when the callee is in another call or when he/she is in DND mode. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p> |
| Greet Prompt | <p>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</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p> |
| Temporary Prompt | <p>This voicemail prompt will be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p> |
| Unavailable Prompt | <p>This voicemail prompt will be played when user enters voicemail. Priority: Temporary Prompt > Busy Prompt/Unavailable Prompt > Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p> |

RING GROUP

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

Configure Ring Group

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

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

Figure 158: Ring Group

- Click on

to add ring group.

- Click on

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

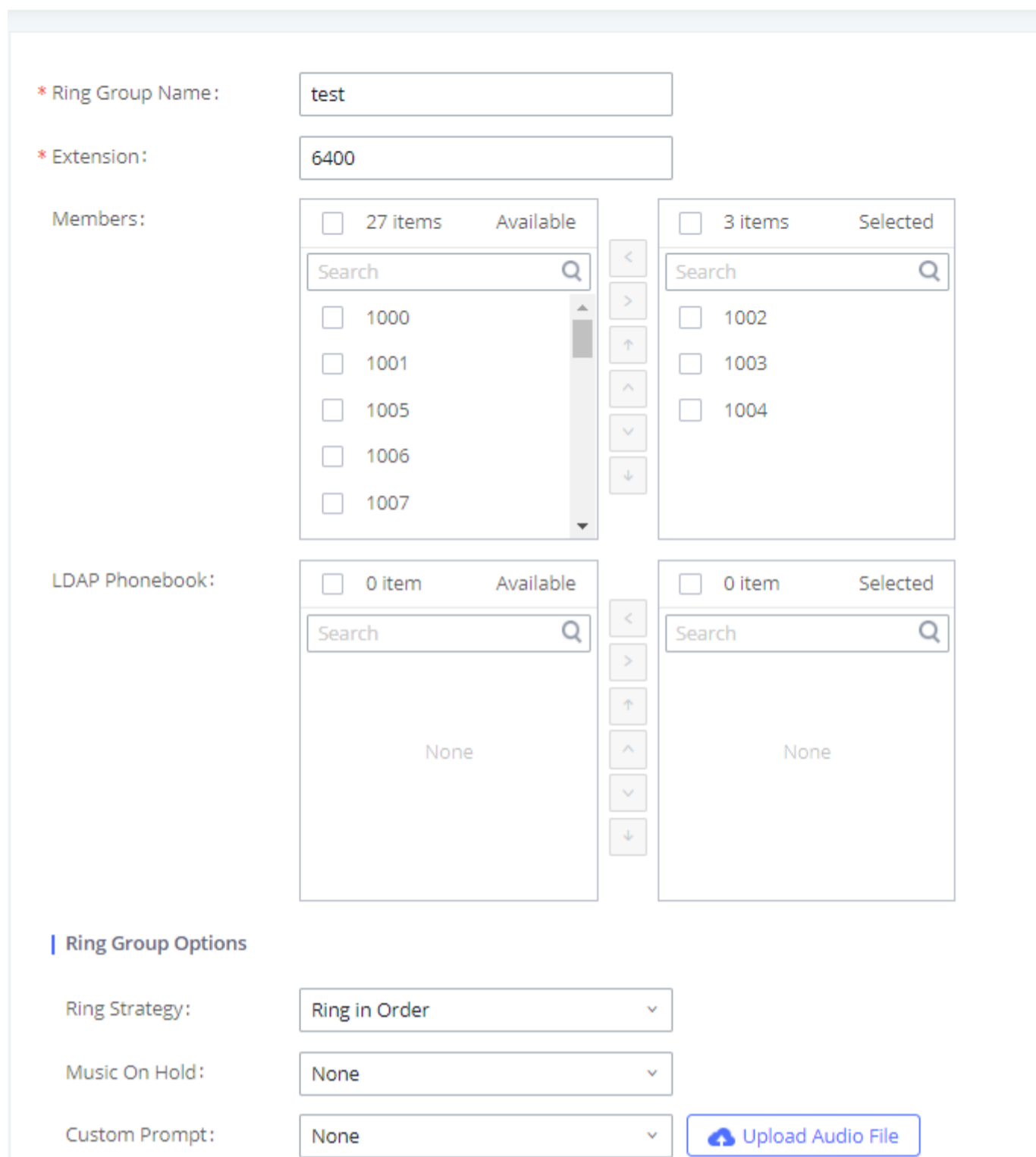
- o Click on

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”. <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● 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 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. |
| 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:

* Extension:

Members:

| 27 items Available | 3 items Selected |
|-------------------------------|-------------------------------|
| <input type="checkbox"/> 1000 | <input type="checkbox"/> 1002 |
| <input type="checkbox"/> 1001 | <input type="checkbox"/> 1003 |
| <input type="checkbox"/> 1005 | <input type="checkbox"/> 1004 |
| <input type="checkbox"/> 1006 | |
| <input type="checkbox"/> 1007 | |

LDAP Phonebook:

| 0 item Available | 0 item Selected |
|------------------|-----------------|
| None | None |

Ring Group Options

Ring Strategy:

Music On Hold:

Custom Prompt: [Upload Audio File](#)

Figure 159: 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:

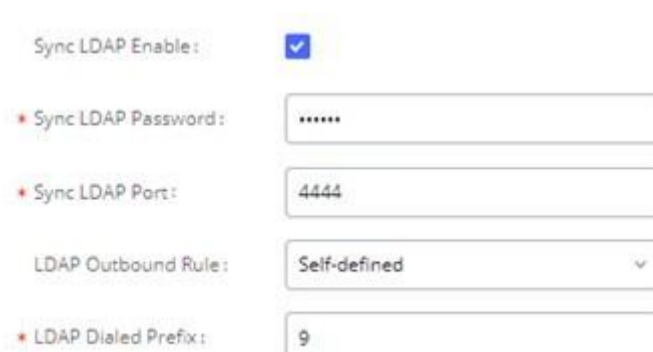
1. Creating SIP Peer Trunk between both UCM630xA_A and UCM630xA_B. SIP Trunk can be found under Web GUI→Extension/Trunk→VoIP Trunks.

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:

Figure 160: 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.

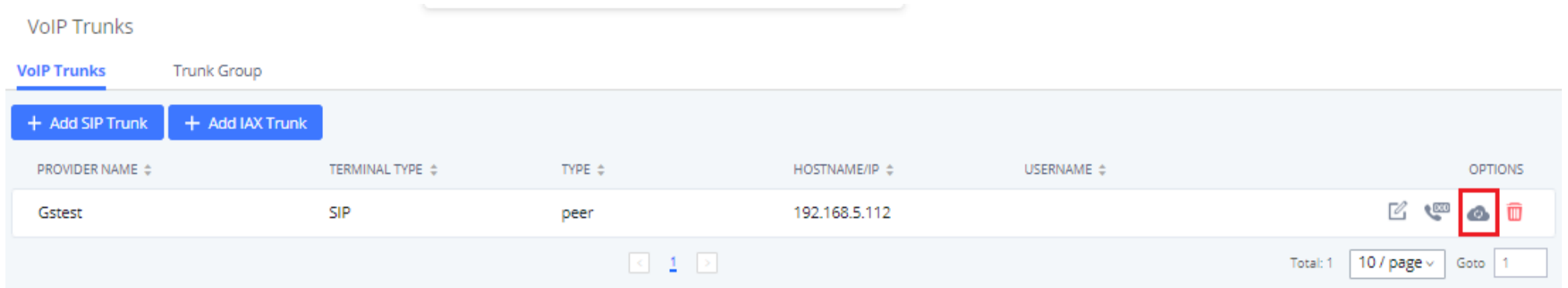


Figure 161: Manually Sync LDAP Server

4. Under Ring Groups setting page, click “Add”. Ring Groups can be found under Web GUI→Call Features→Ring Groups.

5. If LDAP server is synced correctly, Available LDAP Numbers box will display available remote extensions that can be included in the current ring group.

Please also make sure the extensions in the peer UCM630xA can be included into that UCM630xA’s LDAP contact.

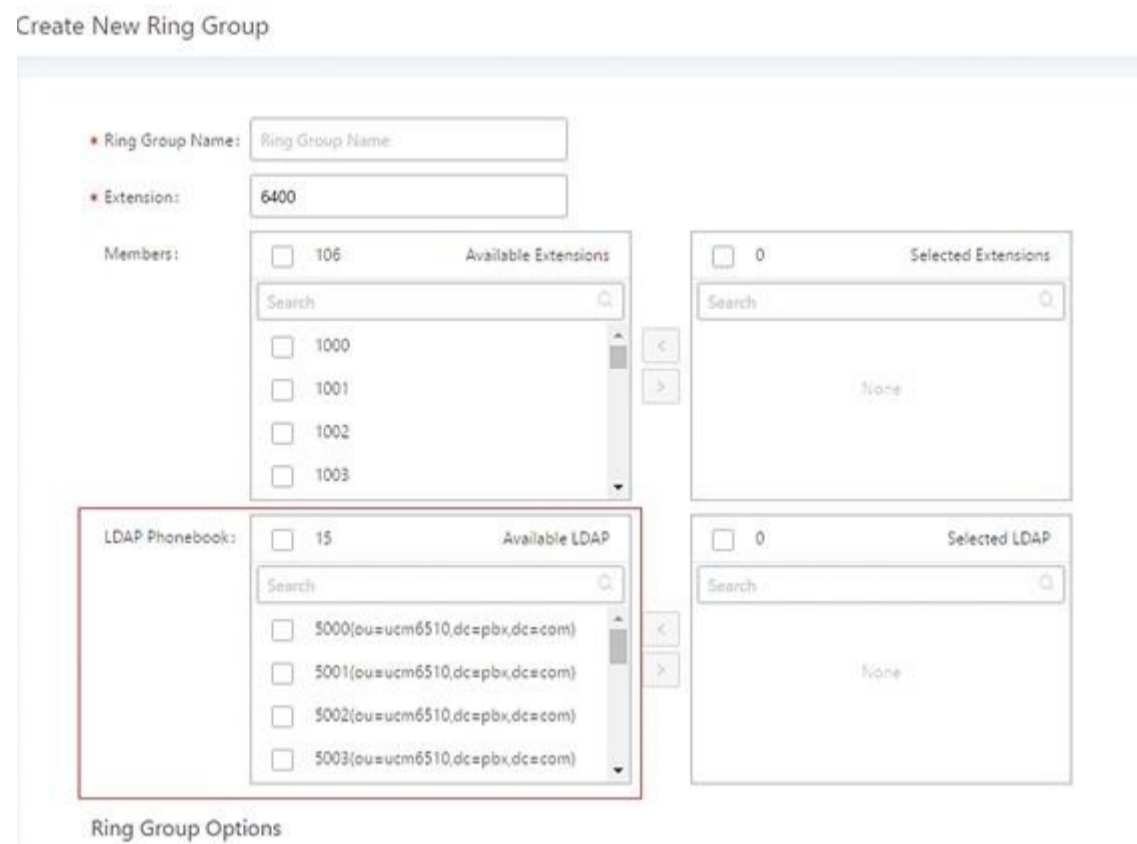


Figure 162: Ring Group Remote Extension

RESTRICT CALLS



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

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

Create New Restrict Calls

Figure 163: Restrict Calls

Configure Restrict Calls

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



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

PAGING AND INTERCOM GROUP

Paging and Intercom Group can be used to make an announcement over the speaker on a group of phones. Targeted phones will answer immediately using speaker. The 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→Call Features→Paging/Intercom.

Configure Paging/Intercom Group

- Click on “Add” to add paging/intercom group.

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

Configure Multicast Paging

* Name:

* Type:

* Extension:

Delayed Paging:

Delay (s):

* Maximum Call Duration (s):

Custom Prompt: [Upload Audio File](#)

* Multicast IP Address:

* Port:

Figure 164: Multicast Paging

| | |
|------------------------------|--|
| Name | Configure paging/intercom group name. |
| Type | Select “Multicast Paging”. |
| Extension | Configure the paging/intercom group extension. |
| Delayed Paging | If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the recorded message will be played, and the call will end after it is finished playing. |
| Delay | Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds. |
| Maximum Call Duration | Specify the maximum call duration in seconds. The default value 0 means no limit. |
| Custom Prompt | This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings→Voice Prompt→Custom Prompt, where they could record new prompt or upload prompt files. |
| Multicast IP Address | The allowed multicast IP address range is 224.0.1.0 – 238.255.255.255. |

| | |
|-------------|--|
| Port | Specify port for multicast paging. Note: This field appears only when “Type” is set to “Multicast Paging”. |
|-------------|--|

Table 81: Multicast Paging Configuration Parameters

Configure 2-way Intercom

The screenshot shows a configuration form for a 2-way intercom. The fields are as follows:

- Name:** Text input field containing "Name".
- Type:** Dropdown menu set to "2-way Intercom".
- Extension:** Text input field containing "6303".
- Auto Record:** Unchecked checkbox.
- Replace Display Name:** Unchecked checkbox.
- Maximum Call Duration (s):** Text input field containing "0".
- Custom Prompt:** Dropdown menu set to "None" with an "Upload Audio File" button next to it.
- Members:** Two columns of checkboxes. The left column is labeled "12 items Available" and lists extensions 1000, 1001, 1002, 1003, and 1004. The right column is labeled "0 item Selected" and is currently empty.

Copyright © Grandstream Networks, Inc. 2021. All Rights Reserved.

Figure 165: 2-way Intercom

| | |
|------------------------------|---|
| Name | Configure paging/intercom group name. |
| Type | Select “2-way Intercom”. |
| Extension | Configure the paging/intercom group extension. |
| Auto Record | Enable this option to record in WAV format. |
| Delayed Paging | Allows the announcement to be played after the configured delay paging. If there are many messages, they will be played in sequence. |
| Replace Display Name | If enabled, the UCM will replace the caller display name with Paging/Intercom name. |
| Maximum Call Duration | Specify the maximum call duration in seconds. The default value 0 means no limit. |
| Custom Prompt | This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings → Voice Prompt → Custom Prompt , where they could record new prompt or upload prompt files. |
| Members | Select available users from the left side to the paging/intercom group member list on the right. |

| | |
|----------------------------------|---|
| Paging/Intercom Whitelist | Select which extensions are allowed to use the paging/intercom feature for this paging group. |
|----------------------------------|---|

Table 82: 2-way Intercom Configuration Parameters

Configure 1-way Paging

Create New Paging/Intercom Groups

• Name:

• Type:

• Extension:

Auto Record:

Delayed Paging:

Replace Display Name:

• Maximum Call Duration (s):

Custom Prompt: [Upload Audio File](#)

Members:

7 items Available

Search

- 1000
- 1001
- 1002
- 1003
- 1004

0 item Selected

Search

None

Paging/Intercom Whitelist:

7 items Available

Search

- 1000
- 1001
- 1002
- 1003
- 1004

0 item Selected

Search

None

1-way Paging

| | |
|------------------------------|--|
| Name | Configure paging/intercom group name. |
| Type | Select “1-way Paging”. |
| Extension | Configure the paging/intercom group extension. |
| Auto Record | Enable this option to record in WAV format. |
| Delayed Paging | If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the recorded message will be played, and the call will end after it is finished playing. |
| Delay (s) | Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds. |
| Maximum Call Duration | Specify the maximum call duration in seconds. The default value 0 means no limit. |

| | |
|----------------------------------|---|
| Custom Prompt | <p>This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts.</p> <p>Note: Users can also refer to the page PBX Settings→Voice Prompt→Custom Prompt, where they could record new prompt or upload prompt files.</p> |
| Members | Select available users from the left side to the paging/intercom group member list on the right. |
| Paging/Intercom Whitelist | Select which extensions are allowed to use the paging/intercom feature for this paging group. |

Table 83: 1-way Paging Configuration Parameters

Configure Private Intercom

Private Intercom feature allows initiating an intercom with the members of an intercom group. The members of the group will be able to hear the intercom initiator, but they will not be able to hear each others’ voices. To configure this feature please navigate to the UCM web UI then go to **Call Features** → **Paging/Intercom** then click on “Add”.

The screenshot shows the configuration interface for a Private Intercom. It includes the following fields and sections:

- * Name:** A text input field with the placeholder "Name".
- * Type:** A dropdown menu currently set to "Private Intercom".
- * Extension:** A text input field with the placeholder "Extension".
- Auto Record:** A checkbox that is currently unchecked.
- Replace Display Name:** A checkbox that is currently unchecked.
- * Maximum Call Duration (s):** A text input field containing the value "0".
- Custom Prompt:** A dropdown menu set to "None" and a blue button labeled "Upload Audio File".
- * Members:** A selection interface with two columns. The left column is titled "161 items Available" and contains a search bar and a list of extensions: 1012, 1013, 1014, 1015, 1016, and 1017. The right column is titled "0 item Selected" and is currently empty, showing "None".
- Paging/Intercom Whitelist:** A selection interface with two columns. The left column is titled "161 items Available" and contains a search bar and a list of extensions: 1001 "Arthur Mo..." and 1002 "Bonnie M...". The right column is titled "0 item Selected" and is currently empty.

© 2023 Grandstream Networks, Inc.

| | |
|----------------------------------|--|
| Name | Configure paging/intercom group name. |
| Type | Select “Private Intercom”. |
| Extension | Configure the paging/intercom group extension. |
| Auto Record | Enable this option to record in WAV format. |
| Replace Display Name | If enabled, the UCM will replace the caller display name with Paging/Intercom name. |
| Maximum Call Duration | Specify the maximum call duration in seconds. The default value 0 means no limit. |
| Custom Prompt | This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings→Voice Prompt→Custom Prompt , where they could record new prompt or upload prompt files. |
| Members | Select available users from the left side to the paging/intercom group member list on the right. |
| Paging/Intercom Whitelist | Select which extensions are allowed to use the paging/intercom feature for this paging group. |

Private Intercom

Configure Announcement Paging

Create New Paging/Intercom Groups

Enable:

* Name:

* Type:

Extension:

Custom Prompt: [Upload Audio File](#)

Repeat:

* Date:

* Time:

Transmission Method:

Members:

30 items Available

Search

- 1000
- 1001
- 1002
- 1003
- 1004

0 item Selected

Search

None

Announcement Paging

| | |
|---------------|-------------------------------------|
| Enable | Enable/Disable Announcement Paging. |
| Name | Configure announcement group name. |

| | |
|----------------------------------|--|
| Type | Select “Announcement Paging” |
| Extension | 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. |
| Transmission Method | Configure Announcement Paging transmission method. Unicast: Depending on members selection. Multicast: Depending on Multicast IP address and Port |
| Maximum Call Duration (s) | The maximum allowed duration of a call in seconds. Default value is 0 (no limit). |
| Announcement File | Configures an audio/video file to play to the paging members in this group. |
| Play Count | Set the number of times to play the audio/video file in this announcement paging. To ensure the intended playback amount of the configured announcements, please set an appropriate maximum paging duration. |
| Repeat | If enabled, the announcement page will be repeated for the selected weekdays. |
| Date | Configure Announcement Paging Date. |
| Time | Configure Announcement Paging Time. |
| Members | Select available users from the left side to the paging/intercom group member list on the right. |

Paging/Intercom Group Settings

Paging/Intercom Group Settings

Please go to [Feature Codes](#) Configure Paging/Intercom Feature Code.

* Alert-info Header :

Custom Prompt: [Upload Audio File](#)

Page/Intercom Group Settings

The UCM630xA has pre-configured paging/intercom feature code. By default, the Paging Prefix is *81 and the Intercom Prefix is *80. To edit page/intercom feature code, click on “Feature Codes” in the “Paging/Intercom Group Settings” dialog. Or users could go to Web GUI→**Call Features**→**Feature Codes** directly.

Configure a Scheduled Paging/Intercom

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

Paging/Intercom Groups

Paging/Intercom Groups [Scheduled Paging/Intercom](#)

+ Add
 Delete

| <input type="checkbox"/> | CALLER ↕ | PAGING/INTERCOM GROUP ↕ | START TIME | TYPE | ACTION STATUS | OPTIONS |
|--------------------------|----------|-------------------------|------------|------|---------------|---------|
| No Data | | | | | | |

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

Table 85: Schedule Paging / Intercom Settings

Creating a scheduled paging/intercom call

OPERATOR PANEL

Configure Operator Panel

Operator Panel settings can be accessed via Web GUI→**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. |

Table 866: Operator Panel Settings

CALL QUEUE

The UCM630xA supports call queue by using static agents or dynamic agents. Call Queue system can accept more calls than the available agents. Incoming calls will be held until next representative is available in the system. This section describes the configuration of call queue under Web GUI→**Call Features**→**Call Queue**.

Configure Call Queue

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

Call Queue

UCM630xA supports custom prompt feature in call queue. This custom prompt will active after the caller waits for a period of time in the Queue. Then caller could choose to leave a message/ transfer to default extension or keep waiting in the queue.

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

◦ Click on “Add” to add call queue.

◦ Click on



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

◦ Click on



to delete the call queue.

Basic Settings

General

| | |
|----------------------------|---|
| Extension | Configure the call queue extension number. |
| Name | Configure the call queue name to identify the call queue. |
| Strategy | <p>Select the strategy for the call queue.</p> <ul style="list-style-type: none">● 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. <p>The default setting is "Ring All".</p> |
| Music On Hold | <p>Select the Music On Hold class for the call queue.</p> <p>Note: Music On Hold classes can be managed from Web GUI→PBX Settings→Music On Hold.</p> |
| Max Queue Length | Configure the maximum number of calls to be queued at once. This number does not include calls that have been connected with agents, only calls that are still in queue. When this maximum value is exceeded, the caller will hear a busy tone and be forwarded to the configured failover destination. Default value is 0 (unlimited). |
| Agent Rest Time (s) | Configure the amount of time in seconds after ending a call where the agent will not receive additional calls. Once this time has passed, the agent will be able to receive calls again. If set to 0, agents can receive additional calls immediately after ending a call. |
| Retry Time (s) | Configure the number of seconds to wait before ringing the next agent. The minimum is 1. |
| Agent Ring Time | Configure the number of seconds to ring an agent. The minimum is 5. |
| Auto Record | If enabled, the calls on the call queue will be automatically recorded. The recording files can be accessed in Queue Recordings under Web GUI→Call Features→Call Queue . |
| Welcome Prompt | |
| Enable | Enable the welcome prompt. |

| | |
|--------------------------------------|---|
| Custom Prompt | Initial tone that plays when the user dials the queue number. Note: The user can upload a custom prompt directly from this parameter. |
| Play Full Welcome Prompt | If enabled, queue agents will not be rung until after the welcome prompt is done playing. Otherwise, queue agents will be rung while the playing the welcome prompt. |
| Satisfaction Survey Prompt | |
| Custom Prompt | After a queue agent hangs up a call, a prompt will play asking the caller to rate their satisfaction on a scale of 1 to 5, with 5 being the highest. Note: The user can upload a custom prompt directly from this parameter. |
| Max Wait Time | |
| Max Wait Time | Configures the amount of time a caller will be kept in queue before the the call is automatically routed to the configured Max Wait Time Destination. If set to 0, callers will be kept in queue indefinitely. |
| Destination | The call will be routed to this destination if no one in this queue answers the call. |
| Destination Prompt Cycle | |
| Enable | Enable Destination Prompt Cycle |
| Destination Prompt Cycle | Configure the voice prompt cycle (in seconds) of this call queue. When playing the voice prompt, you can press 1 to transfer to failover destination. |
| Custom Prompt | When playing a custom prompt, press 1 to enter the failover destination or continue waiting in queue. Note: The user can upload a custom prompt directly from this parameter. |
| Destination | After the specified amount of time, the caller will be prompted to press 1 to immediately get redirected to the configured failover destination. |
| Advanced Settings | |
| Virtual Queue | |
| Enable Virtual Queue | If enabled, system will enable a virtual queue for users waiting in queue. |
| Virtual Queue Mode | When in DTMF mode, pressing 2 will manually trigger virtual queue. When in Timeout mode, virtual queue will automatically be triggered when the configured Virtual Queue Period has passed. DTMF mode and Timeout mode require the caller to manually set a callback number. When in Auto mode, virtual queue will automatically be triggered when the configured Virtual Queue Period has passed. The callback number will automatically be set to the caller's detected CID number. |
| Virtual Queue Period (s) | The amount of time in seconds that must pass before virtual queue is offered to callers when using Timeout mode or Auto mode. |
| Virtual Queue Outbound Prefix | System will add this prefix to dialed numbers when calling back users. |

| | |
|--|---|
| Enable Virtual Queue Position Announcement | If enabled, the system will inform callers waiting in the queue of their positions in line. |
| Enable Virtual Queue Wait Time Announcement | If enabled, the estimated wait time for the call to get answered will periodically be announced to the caller. |
| Enable Virtual Queue Callback Timeout | If enabled, agents will have a set amount of time to answer a virtual queue callback. |
| Virtual Queue Welcome Prompt | Upload the file of your welcome prompt of the virtual queue. |
| Announcement Settings | |
| Enable Position Announcement | If enabled, the system will inform callers waiting in the queue of their positions in line. |
| Enable Wait Time Announcement | If enabled, the estimated wait time for the call to get answered will periodically be announced to the caller. Note: Wait time will not be announced if less than one minute. |
| Announcement Interval | The interval at which caller positions and estimated wait times will be announced. |
| Agent ID Announcement | If enabled, a system prompt containing the agent ID will be played to the caller when answered by an agent. |
| Empty Queue | |
| Leave When Empty | <p>Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict".</p> <ul style="list-style-type: none"> ● Yes: Callers will be disconnected from the queue if all agents are paused or invalid. ● No: Never disconnect the callers from the queue when the queue is empty. ● Strict: Callers will be disconnected from the queue if all agents are paused, invalid or unavailable. |
| Dial in Empty Queue | <p>Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No".</p> <ul style="list-style-type: none"> ● Yes: Callers can always dial into a call queue. ● No: Callers cannot dial into a queue if all agents are paused or invalid. ● Strict: Callers cannot dial into a queue if the agents are paused, invalid or unavailable. |
| Failover Destination | <p>Choose the destination where the call will be directed when the queue is empty or when all the agents are not logged in, here are the destinations that can be configured:</p> <ul style="list-style-type: none"> ● Play Sound. ● Extension. ● Voicemail. ● Queues. ● Ring Group. ● Voicemail Group. ● IVR |

| | |
|--------------------------------------|--|
| | <ul style="list-style-type: none"> • External Number. |
| CTI | |
| Enable Agent Login | Enabling agent login will cause the dynamic agents to be unavailable. |
| Queue Chairman | The queue chairman can log into his web portal to operate the queue. |
| Service Level Agreement (SLA) | |
| Enable SLA | Toggles Service Level Agreement (SLA), which is percentage measurement of the queue group's ability to answer incoming calls within a defined amount of time. If a queue group's calculated SLA percentage is below the configured threshold value, alerts will be generated and sent out via email to the specified recipients. Example: The SLA goal is 80% of calls (Threshold) within 20 seconds (SLA Time). If less than 80% of queue calls are answered within 20 seconds, the specified users will be notified of it. |
| SLA Time (s) | Configures the amount of time in seconds that agents must answer incoming queue calls within to satisfy service quality requirements. Answering calls past this time will negatively affect the SLA measurement, and an alert will be generated once it hits below the specified SLA alert threshold. Supported values are 1 to 180. Default value is 20. |
| SLA Alert Email Notification | Enable SLA alert email notification. |
| Alert Threshold (%) | Configures the SLA alert threshold. If the percentage of queue calls answered within the configured SLA Time go below this value, an alert email will be generated and sent to the configured recipients. Supported values are 1 to 100. Default value is 80. |
| SLA Alert Interval (m) | Configures the minimum amount of time (in minutes) between alert sending. If a new alert is generated within this period, it will not be sent to recipients until the next alert interval. The valid range is from 1 to 120. The default value is 120. |
| SLA Alert Email Template | The template of the SLA alert email notifications. |
| Alert Email Recipients | Send SLA alert notifications to the configured alert email recipients. If a recipient does not have an email address configured, they will not receive the alert notifications. |
| Other Settings | |
| Report Hold Time | If enabled, the UCM630X will report (to the agent) the duration of time of the call before the caller is connected to the agent. The default setting is "No". |
| Replace Display Name | If enabled, the UCM will replace the caller display name with the Call Queue name so that the caller knows the call is incoming from a Call Queue. |
| Enable Feature Codes | Enable feature codes option for call queue. For example, *83 is used for "Agent Pause" |
| Autofill | Configure to enable autofill. |
| Dynamic Login Password | If enabled, the configured PIN number is required for dynamic agent to log in. The default setting is disabled. |

| | |
|----------------------|---|
| Alert-Info | When present in an INVITE request, the Alert-info header field specifies an alternative ring tone to the UAS. |
| Agents | |
| Static Agents | Go to “Agents” Tab and Select the available users to be the static agents in the call queue. Choose from the available users on the left to the static agents list on the right. Click on ◀ or ▶ to choose. And use UP and Down arrow to select the order of the agent within the call queue. |

Agents limitation:

The maximum number of agents which can be assigned varies depending on the model of the UCM6300A used. This limit includes the static and the dynamic agents.

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 |

Table 88: Static Agent Limitation

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

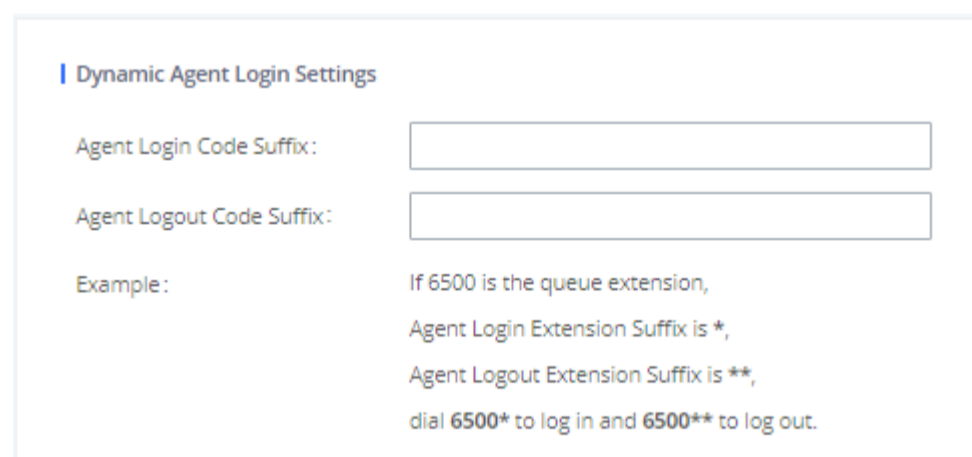


Figure 173: Agent Login Settings

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

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

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

The agent can also dial the feature with the number of the reason of the pause. E.g., if the agent want to perform a pause for lunch, he/she can dial *831 directly instead of waiting for the IVR response.

- Queue recordings are shown on the Call Queue page under “Queue Recordings” Tab. Click on



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



to delete the recording file. To delete multiple recording files by one click, select several recording files to be deleted and click on “Delete Selected Recording Files” or click on “Delete All Recording Files” to delete all recording files.

Call Center Settings and Enhancements

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

To configure call center features, press



on an existing call queue and go under the advanced settings tab.

Following parameters are available:

| | |
|--------------------------------------|---|
| Enable Virtual Queue | Enable virtual queue to activate call center features. |
| Virtual Queue Period | Configure the time in (s) after which the virtual queue will take effect and the menu will be presented to the caller to choose an option. Default is 20s. |
| Virtual Queue Mode | <p>Offered to caller after timeout: After the virtual queue period passes, the caller will enter the virtual call queue and be presented with a menu to choose an option, the choices are summarized below:</p> <ul style="list-style-type: none"> ◦ Press * to set current number as callback number. ◦ Press 0 to set a callback number different than current caller number. ◦ Press # to keep waiting on the call queue. <p>Triggered on user request: In this mode, the callers can activate the virtual queue by pressing 2, then they will be presented with the menu to choose an option as below:</p> <ul style="list-style-type: none"> ◦ Press * to set current number as callback number. ◦ Press 0 to set a callback number different than current caller number. ◦ Press # to keep waiting on the call queue. |
| Virtual Queue Outbound Prefix | System will add this prefix to dialed numbers when calling back users. |
| Enable Virtual Queue Timeout | When this option is enabled and after a caller registers a call back request on the virtual queue. While all the agents are busy, the UCM will call an agent once he/she is idle again, this timeout is used for how long the UCM continues calling the agent and if the agent doesn't answer the call then the callback request will timeout and expire. |
| Write Timeout | Configure the virtual queue callback timeout period in seconds. |

| | |
|--|--|
| Enable Virtual Queue Position Announcement | <p>Enable the announcement of the caller's position periodically.</p> <p>Note: Queue position will now be announced to the caller upon entering the queue.</p> |
| Position Announcement Interval | Configure the period of time in (s) during which the UCM will announce the caller's position in the call queue. |
| Enable Virtual Queue Wait Time Announcement | When enabled the UCM will announce the estimated queue wait time to callers if the estimated wait time is longer than 1 minute. |
| Queue Chairman | Select the extension to act as chairman of the queue (monitoring). |
| Virtual Queue Welcome Prompt | Click on "Upload Audio File" to upload the VQ welcome prompt. |
| Enable Agent Login | <p>When enabled, static agents can conveniently log in and out of a queue by configuring a programmable key on their phones as a shortcut.</p> <p>Notes:</p> <ul style="list-style-type: none"> ◦ This feature is currently available only for GXP21xx phones on firmware 1.0.9.18 or greater. ◦ After enabling the feature, users need to set the option on GXP21XX phone under "Account→SIP Settings→Advanced Features→Special Feature" to "UCM Call Center". A softkey labeled "UCM-CC" will appear on the bottom of the phone's screen. ◦ When this option is enabled, dynamic agent login will be no longer supported. ◦ In case of concurrent registrations, changing agent status on one phone (login/logout) will be reflected on all phones. |

Table 89: Call Center Parameters

Queue Auto fill enhancement:

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

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

Queue Statistics

Along with call center features, users can also gather detailed call queue statistics allowing them to make better changes/decision to manage better the call distribution and handling based on time, agent, and queue.

To access call queue statistics, go to Web GUI→**Call Features**→**Call Queue** and click on "Call Queue Statistics", the following page will be displayed:

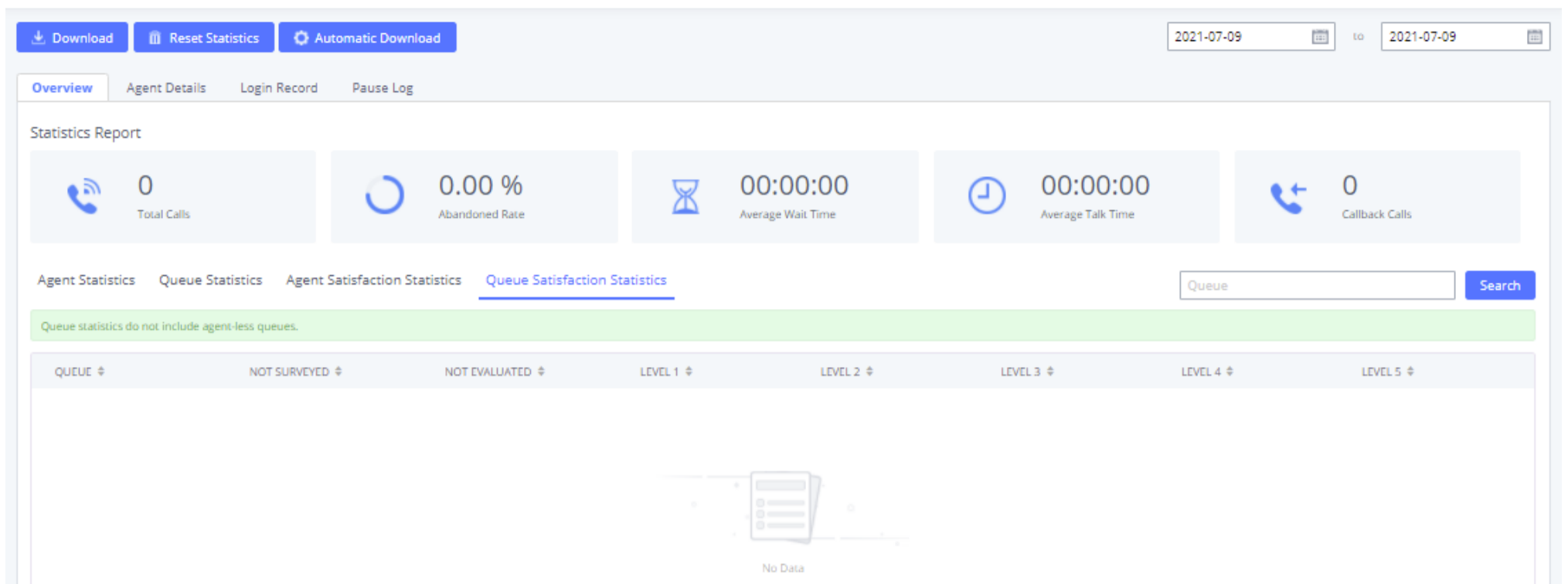


Figure 174: Call Queue Statistics

- **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.

The overview page performs seat statistics, queue statistics, seat satisfaction statistics, and queue satisfaction statistics according to the business. Agent statistics record the number of calls and call-related information of agents; queue counts the number of calls in the queue and information such as calls, waiting, and callback; agent satisfaction statistics are survey statistics based on user ratings of agents; queue satisfaction statistics are user-queue the score survey statistics

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

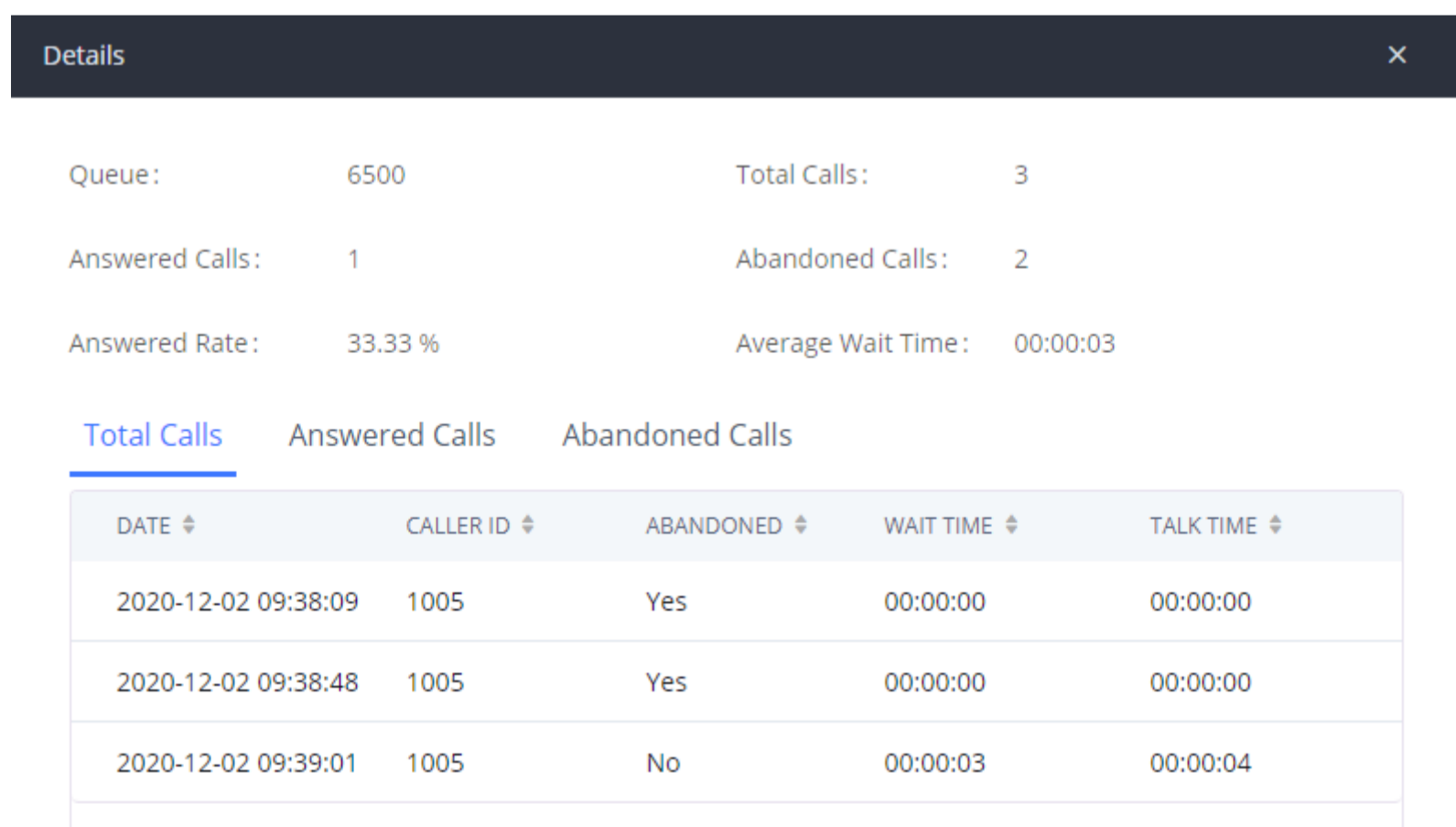


Figure 175: Queue’s call log details

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

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

Figure 176: Automatic Download Settings – Queue Statistics

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

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

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

The screenshot shows the 'Agent Details' tab selected in a navigation menu. Below the menu is a 'Statistics Report' section with a search bar for 'Agent' and a 'Search' button. The main content is a table with the following data:

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

Figure 177: Agent details

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

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

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

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

Figure 178: Login Record

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

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

| AGENT ↕ | QUEUE ↕ | PAUSE TIME ↕ | RESUME TIME ↕ | PAUSE DURATION ↕ |
|---------|---------|---------------------|---------------------|------------------|
| 2000 | 6500 | 2019-11-08 11:32:00 | 2019-11-08 11:33:33 | 00:01:33 |
| 2000 | 6500 | 2019-11-08 11:32:00 | 2019-11-08 11:33:33 | 00:01:33 |

Figure 179: Pause Log

Switchboard

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

Following page will be displayed:

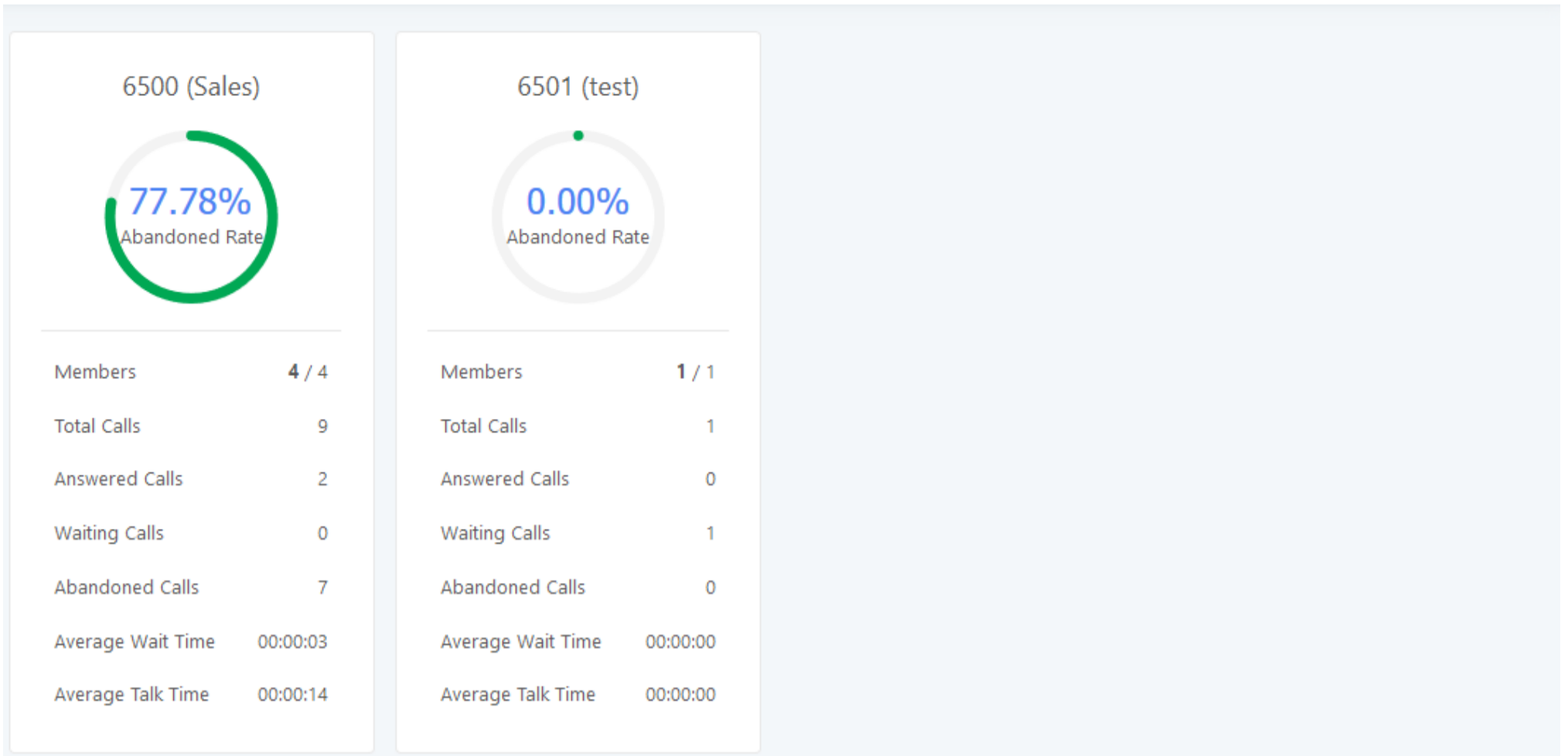


Figure 180: Switchboard Summary

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

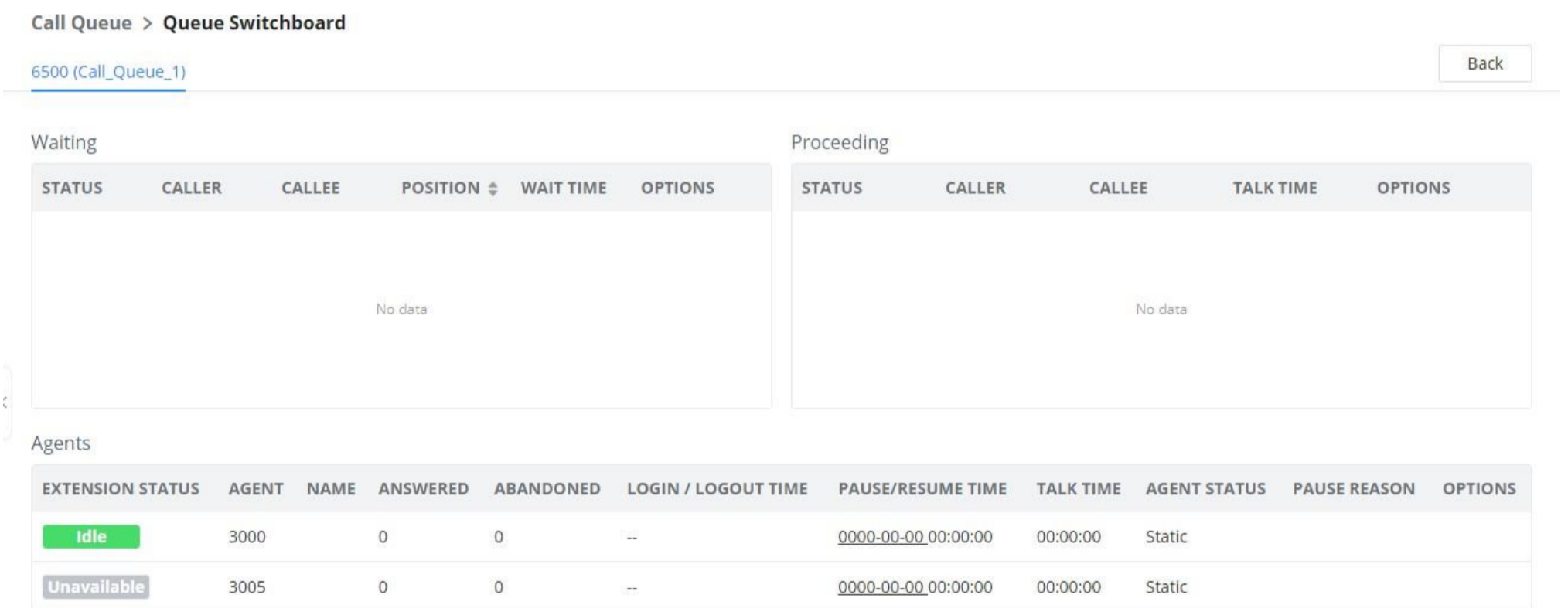


Figure 181: Call Queue Switchboard

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

| | |
|-------------------|---|
| Waiting | This menu shows the current waiting calls along with the caller id and the option to hang-up call by pressing on the button. |
| Proceeding | Shows the current established calls along with the caller id and the callee (agent) as well as the option to hang-up, transfer, add meeting or barge-in the call. |

| | |
|---------------|--|
| Agents | <p>Displays the list of agents in the queue and the extension status (idle, ringing, in use or unavailable) along with some basic call statistics and agent's mode (static or dynamic).</p> <p>Note: the dashboard will show the number of calls (answered and abandoned) of each agent. For dynamic agents, it will count the number of calls starting from the last login time.</p> |
|---------------|--|

Table 90: Switchboard Parameters

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

- **Super Admin** – Default admin of the UCM. Call queue privileges include being able to view and edit all queue agents, monitor, and execute actions for incoming and ongoing calls for each extension in Switchboard, and generate Call Queue reports to track performance.
- **Queue Chairman** – User appointed by Super Admin to monitor and manage an assigned queue extension via Switchboard. The Queue Chairman can log into the UCM user portal with his extension number and assigned user password. To access the Switchboard, click on “Other Features” in the side menu and click on “Call Queue”. In the image below, User 1001 is the Queue Chairman appointed to manage Queue Extension 6500 and can see all the agents of the queue in the Switchboard. The Chariman is also able to log out dynamic agents from call queues.

Call Queue > Queue Switchboard

6500 (Call_Queue_1) Back

Waiting

| STATUS | CALLER | CALLEE | POSITION | WAIT TIME | OPTIONS |
|---------|--------|--------|----------|-----------|---------|
| No data | | | | | |

Proceeding

| STATUS | CALLER | CALLEE | TALK TIME | OPTIONS |
|---------|--------|--------|-----------|---------|
| No data | | | | |

Agents

| EXTENSION STATUS | AGENT | NAME | ANSWERED | ABANDONED | LOGIN / LOGOUT TIME | PAUSE/RESUME TIME | TALK TIME | AGENT STATUS | PAUSE REASON | OPTIONS |
|------------------|-------|------|----------|-----------|---------------------|---------------------|-----------|--------------|--------------|---------|
| Idle | 3000 | | 0 | 0 | -- | 0000-00-00 00:00:00 | 00:00:00 | Static | | |
| Unavailable | 3005 | | 0 | 0 | -- | 0000-00-00 00:00:00 | 00:00:00 | Static | | |

Figure 182: Queue Chairman

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

6500 (test)

| Waiting | | | | | | Proceeding | | | | |
|---------|--------|--------|----------|-----------|---------|------------|--------|--------|-----------|---------|
| STATUS | CALLER | CALLEE | POSITION | WAIT TIME | OPTIONS | STATUS | CALLER | CALLEE | TALK TIME | OPTIONS |
| | 1000 | 6500 | 1 | 00:00:01 | | No Data | | | | |

| EXTENSION STATUS | EXTENSION | ANSWERED | ABANDONED | LOGIN / LOGOUT TIME | PAUSE / RESUME TIME | TALK TIME | AGENT STATUS |
|---|-----------|----------|-----------|---------------------|---------------------|-----------|--------------|
| Ringing | 1001 | 1 | 1 | -- | -- | 00:00:04 | Static |

Figure 183: Queue Agent

Global Queue Settings

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

Figure 184: Global Queue Settings

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

| | |
|--|--|
| Agent Logout Code Suffix | Configure the code to dial after the queue extension to log out of the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log out. |
| Virtual Queue Callback Key Settings | |
| 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. |




Table 91: Global Queue Settings

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→**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.

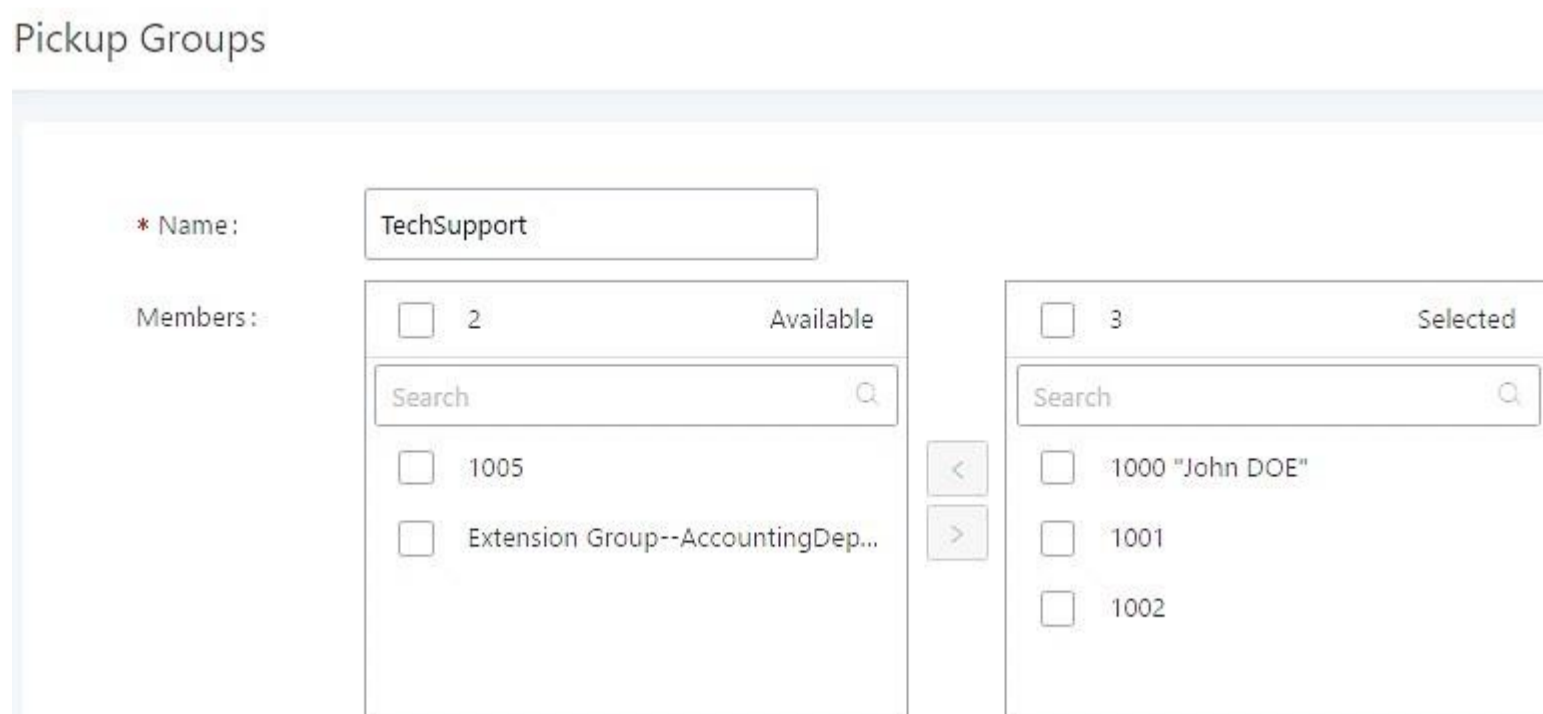


Figure 185: Edit Pickup Group

Configure Pickup Feature Code

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

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

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

Figure 186: 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

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

Figure 187: 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

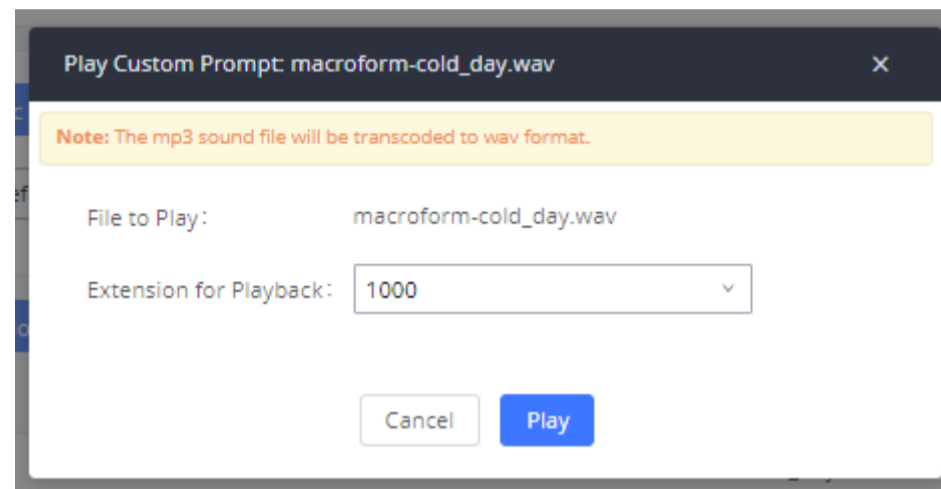


Figure 188: Play Custom Prompt

3. The selected extension will ring.

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

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

1. Click on

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

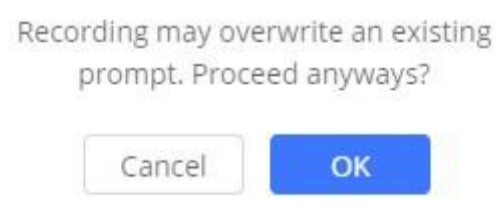


Figure 189: Information Prompt

3. Click

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

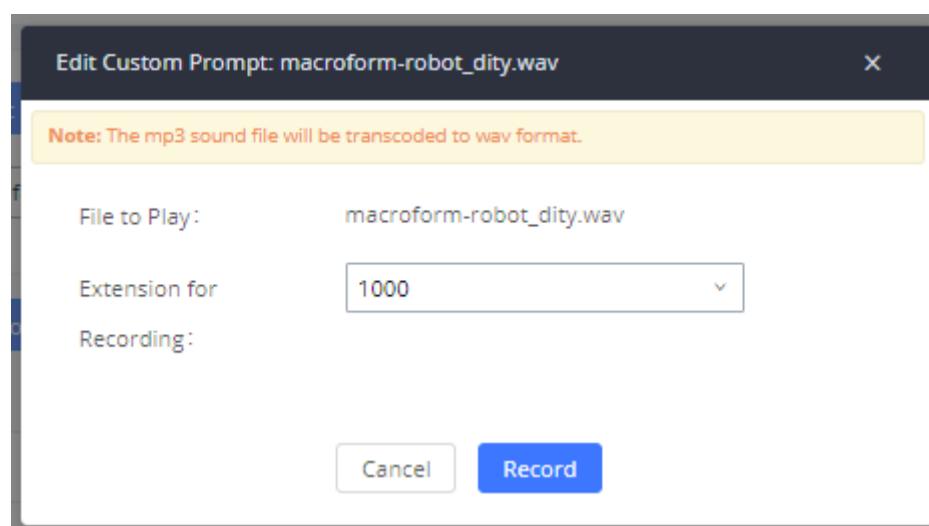


Figure 190: Record Custom Prompt

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

i Note

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

- Users could download the MOH file from this link:

<http://downloads.asterisk.org/pub/telephony/sounds/releases/asterisk-moh-opsound-wav-2.03.tar.gz>

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

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

BUSY CAMP-ON

The UCM630xA supports busy camp-on/call completion feature that allows the PBX to camp on a called party and inform the caller as soon as the called party becomes available given the previous attempted call has failed.

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

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

PRESENCE

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

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

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

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

OR

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

Figure 191: 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. |

Table 92: 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→**Call Features**→**Feature Codes**.

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

Figure 192: 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.

| STATUS | CALL FROM | CALL TO | ACTION TYPE | START TIME | CALL TIME | TALK TIME | ACCOUNT C ODE | 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 | | - |

Figure 193: 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.

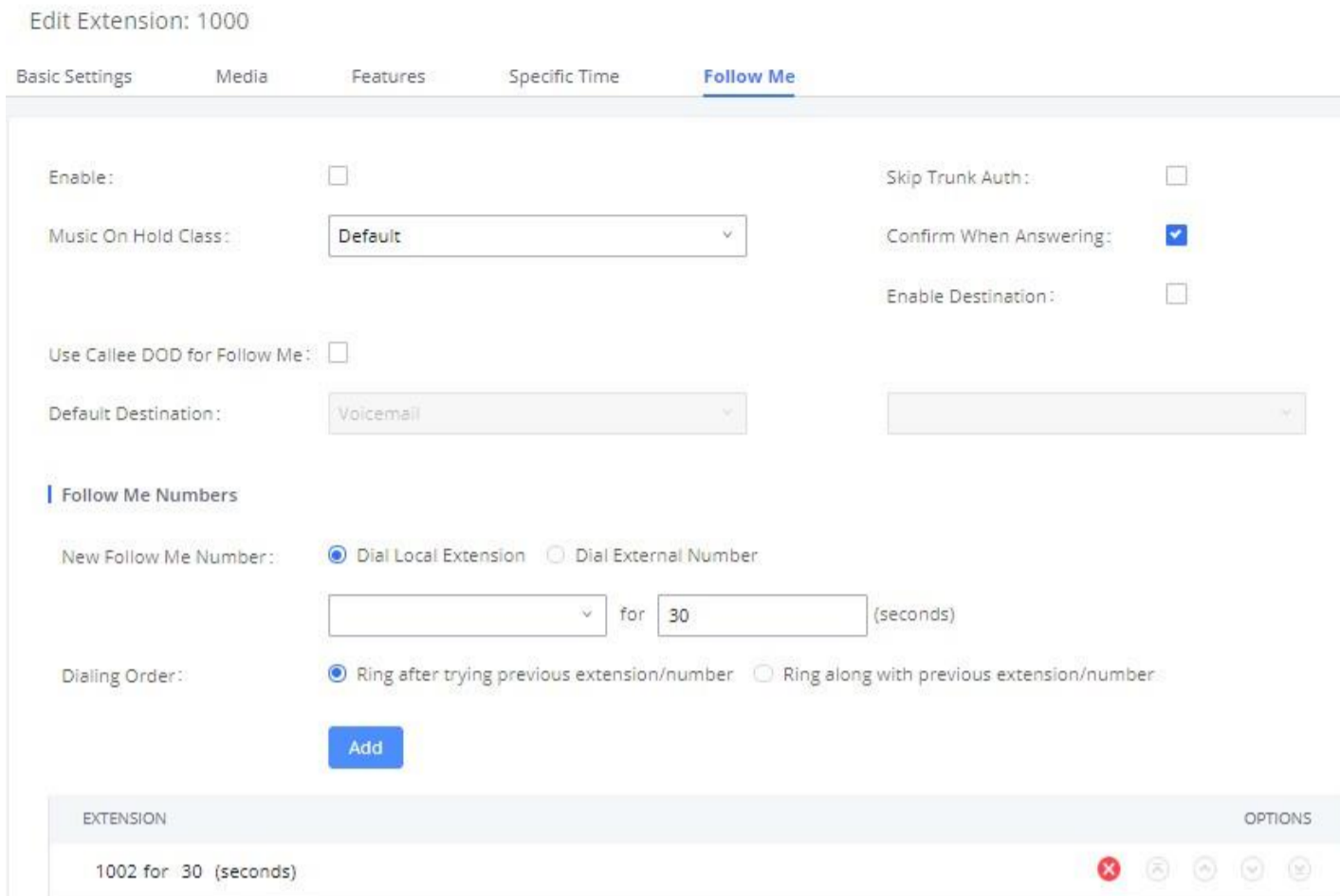


Figure 194: Edit Follow Me

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 | <p>Configure the destination if no one in the Follow Me extensions answers the call. The available options are:</p> <ul style="list-style-type: none"> ◦ Extension ◦ Voicemail ◦ Queues ◦ Ring Group ◦ Voicemail Group ◦ IVR ◦ External Number |
| Follow Me Numbers | <p>The added numbers are listed here. Click on</p> <p>to arrange the order. Click on</p> <p>to delete the number. Click on</p> <p>to add new numbers.</p> |
| 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. |

Table 93: 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. |

Table 94: 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→**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.

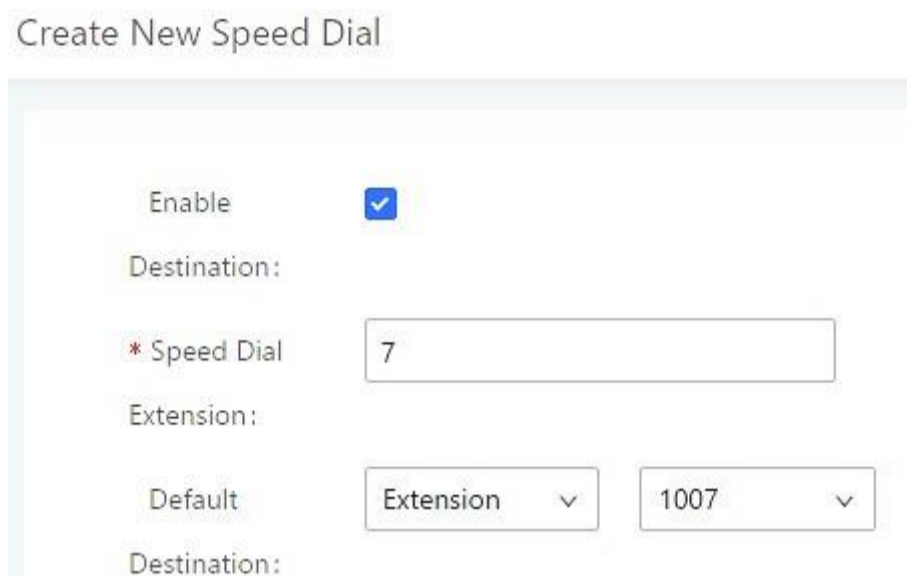
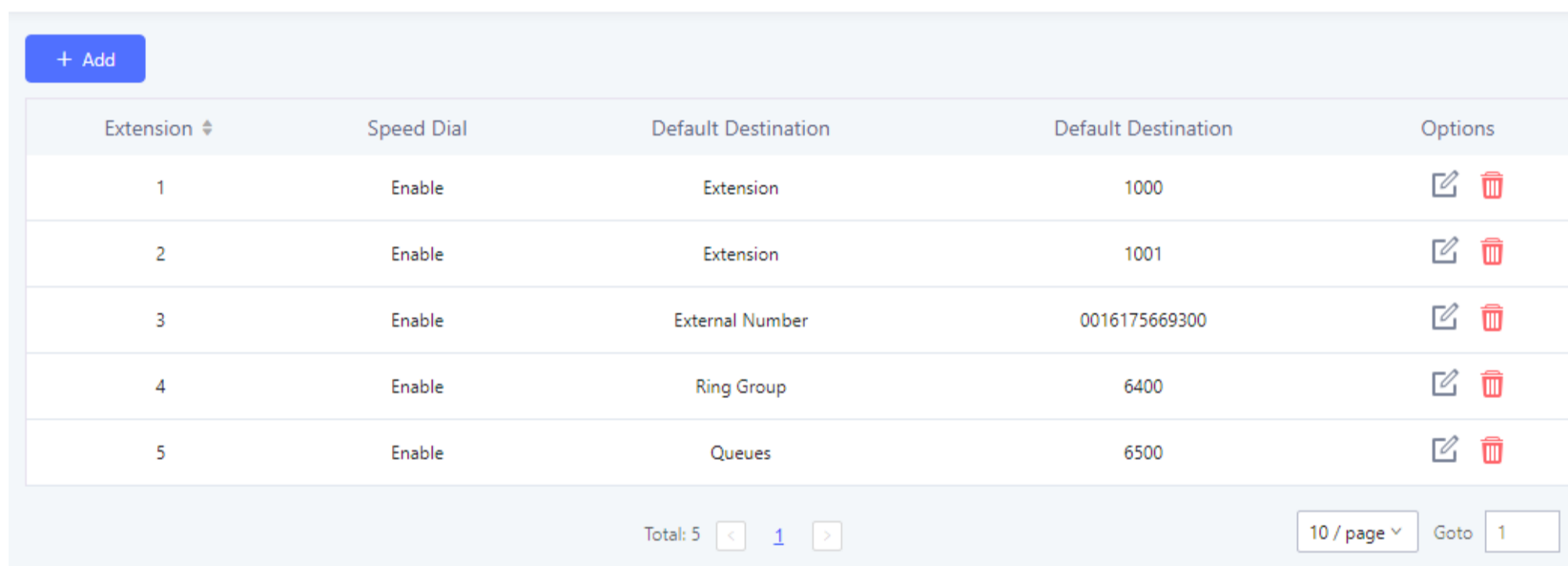


Figure 195: Speed Dial Destinations

Speed Dial













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

Figure 196: 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.

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

! **Important**

Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.

! **Alert**

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

i **Note**

The number of speed dial entries is limited to 100, therefore, the maximum number of entries you can import is 100. However, if the UCM had already more than a 100 entries, the limit will be set to that specific number.

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.

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→**Call Features**→**DISA**.

- Click on

to add a new DISA.

- Click on

to edit the DISA configuration.

- Click on

to delete the DISA.

Create New DISA

The screenshot shows a 'Create New DISA' form with the following fields and values:

- * Name: [Name]
- * Password: []
- Permission: [Internal]
- * Response Timeout: [10]
- * Digit Timeout: [5]
- Allow Hang-up:
- Replace Display Name:

Figure 197: 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 | <p>Configure the permission level for DISA.</p> <p>The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level.</p> <p>The default setting is “Internal”.</p> <p>If the user tries to dial outbound calls after dialing into the DISA, the UCM630xA will compared the DISA’s permission level with the outbound route’s privilege level. If the DISA’s permission level is higher than (or equal to) the outbound route’s privilege level, the call will be allowed to go through.</p> |
| Response Timeout | <p>Configure the maximum amount of time the UCM630xA will wait before hanging up if the user dials an incomplete or invalid number.</p> <p>The default setting is 10 seconds.</p> |
| Digit Timeout | <p>Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.</p> |
| Allow Hangup | <p>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”.</p> |
| Replace Display Name | <p>If enabled, the UCM will replace the caller display name with the DISA name.</p> |

Table 95: DISA Settings

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

EMERGENCY

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

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

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

<https://documentation.grandstream.com/knowledge-base/emergency-calls/>

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

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

Emergency Calls

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

1. Navigate on the web GUI under “**Call Features → Emergency Calls**”

2. Click on

to add a new emergency number.

3. Configure the required fields “Name, Emergency Number and Trunk(s) to be used to reach the number”.

4. Save and apply the configuration.

The screenshot shows a web form titled "Create New Emergency Call". The form contains the following fields and options:

- Name:** Text input field containing "911".
- Emergency Number:** Text input field containing "911".
- Emergency Level:** Dropdown menu with "1 - Not Urgent" selected.
- Disable Hunt on Busy:** Unchecked checkbox.
- Custom Prompt:** Dropdown menu with "None" selected, and a "Prompt" link.
- Use Trunks:** Empty text input field.
- Members Notified:** Two selection panes. The left pane is titled "11 items Available" and contains a search bar and a list of items: "1001 'John Doe'", "1002", "1003", and "1004". The right pane is titled "1 item Selected" and contains a search bar and one item: "1000 'James tuan'".
- Strip:** Empty text input field.
- Prepend:** Empty text input field.
- Auto Record:** Checked checkbox.
- Send Recording File:** Checked checkbox.
- Email Address:** Text input field containing "admin@domain.local" and a "+" icon.

Figure 198: 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 prependded 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. |



Table 96: Emergency Numbers Parameters

Emergency Calls

[Emergency Calls](#) [Emergency Recordings](#) [Emergency Location Mapping](#)

[+ Add](#)

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


[1](#)


Total: 1 Goto

Figure 199: 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 Calls

Emergency Recordings

Emergency 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 Location Mapping

In compliance with Kari’s Law and the Ray Baum’s Act, UCM’s Emergency Calls feature now 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 **Call Features**→**Emergency Calls**→**Emergency Location Mapping**.

Create New Emergency Location Mapping Cancel Save

* ELIN:

* Subnet:

* Location:

Geolocation Routing: No

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

- **ELIN:** The emergency location identification number registered with the E911 provider. This number will be sent out as the emergency call’s CID number.
- **Subnet:** The network subnet that the ELIN will be associated with. The ELIN that is sent to E911 providers is based on the subnet that a calling endpoint is registered from. Example: “xxx.xxx.xxx.xxx/24” or “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/64”.
- **Location:** Location associated with the configured subnet. This is used for the UCM administrator’s reference.

- **Geolocation Routing:** Toggles whether to include the *Geolocation* header in the emergency call SIP INVITE message. The *Location* field value will be used as the *Geolocation* header value.

Important Note

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

CALLBACK

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

The callback feature works as follows:

1. Configure a new callback on the UCM630xA.
2. On the UCM630xA, configure destination of the inbound route for analog trunk to callback.
3. Save and apply the settings.
4. The user calls the PSTN number of the UCM630xA using the mobile phone, which goes to callback destination as specified in the inbound route.
5. Once the user hears the ringback tone from the mobile phone, hang up the call on the mobile phone.
6. The UCM630xA will call back the user.
7. The user answers the call.
8. The call will be sent to DISA or IVR which directs the user to dial the destination number.
9. The user will be connected to the destination number.

In this way, the calls are placed and connected through trunks on the UCM630xA instead of to the mobile phone directly. Therefore, the user will not be charged on mobile phone services for long distance or international calls.

To configure callback on the UCM630xA, go to Web GUI→**Call Features**→**Callback** page and click on

. Configuration parameters are listed in the following table.

Table 97: Callback Configuration Parameters

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

| | |
|--------------------|--|
| Destination | <p>Configure the destination which the callback will direct the caller to. Two destinations are available:</p> <ul style="list-style-type: none"> ◦ IVR ◦ DISA <p>The caller can then enter the desired number to dial out via UCM630xA trunk.</p> |
|--------------------|--|

BLF AND EVENT LIST

BLF

The UCM630xA supports BLF monitoring for extensions, ring group, call queue, meeting room and parking lot. For example, on the user’s phone, configure the parking lot number 701 as the BLF monitored number. When there is a parked call on 701, the LED for this BLF key will light up in red, meaning a call is parked against this parking lot. Pressing this BLF key can pick up the call from this parking lot.

Note

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

Event List

Besides BLF, users can also configure the phones to monitor event list. In this way, both local extensions on the same UCM630xA and remote extensions on the VOIP trunk can be monitored. The event list setting is under Web GUI→**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

Table 98: Event List Settings

The screenshot shows the 'Create New Event List' configuration page. It features several sections: a URI field containing 'test', an Event Type dropdown set to 'Dialog', and three extension management panels. The 'Local Extensions' panel shows 9 available items with a search bar and a list of extensions: 1003 'Betty', 1004, 1005 'Will', 1006 'Iala', and 1007 'Kiki'. The 'Remote Extensions' panel shows 0 available items and is currently empty. The 'Special Extensions' field is an empty text area. Navigation buttons (left, right, up, down, add, remove) are located between the extension panels. The 'Selected' panels for both Local and Remote Extensions show 3 and 0 items respectively, with '1002 'Chris'' selected in the Local list.

Figure 200: 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.

Notes

- To configure LDAP sync, please go to UCM630xA Web GUI→**Extension/Trunk**→**VoIP Trunk**. You will see “Sync LDAP Enable” option. Once enabled, please configure password information for the remote peer UCM630xA to connect to the local UCM630xA. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM630xA and remote UCM630xA need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM630xAs.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM630xA PBX. However, it might not work the other way around depending on whether the non-UCM630xA PBX supports event list BLF or remote monitoring feature.

- To configure LDAP sync, please go to UCM630xA Web GUI→**Extension/Trunk**→**VoIP Trunk**. You will see “Sync LDAP Enable” option. Once enabled, please configure password information for the remote peer UCM630xA to connect to the local UCM630xA. Additional information such as port

number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM630xA and remote UCM630xA need enable LDAP sync option with the same password for successful connection and synchronization.

- Currently LDAP sync feature only works between two UCM630xAs.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM630xA PBX. However, it might not work the other way around depending on whether the non-UCM630xA PBX supports event list BLF or remote monitoring feature.

DIAL BY NAME

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

Dial by Name Configuration

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

Create New Dial By Name

* Name:

* Extension:

Custom Prompt: [Upload Audio File](#)

Members: 30 items Available 0 item Selected

LDAP Phonebook: 1 item Available 0 item Selected

Options

* Prompt Wait Time:

Query Type: By Last Name + First Name By First Name + Last Name

Select Type: By Order By Menu

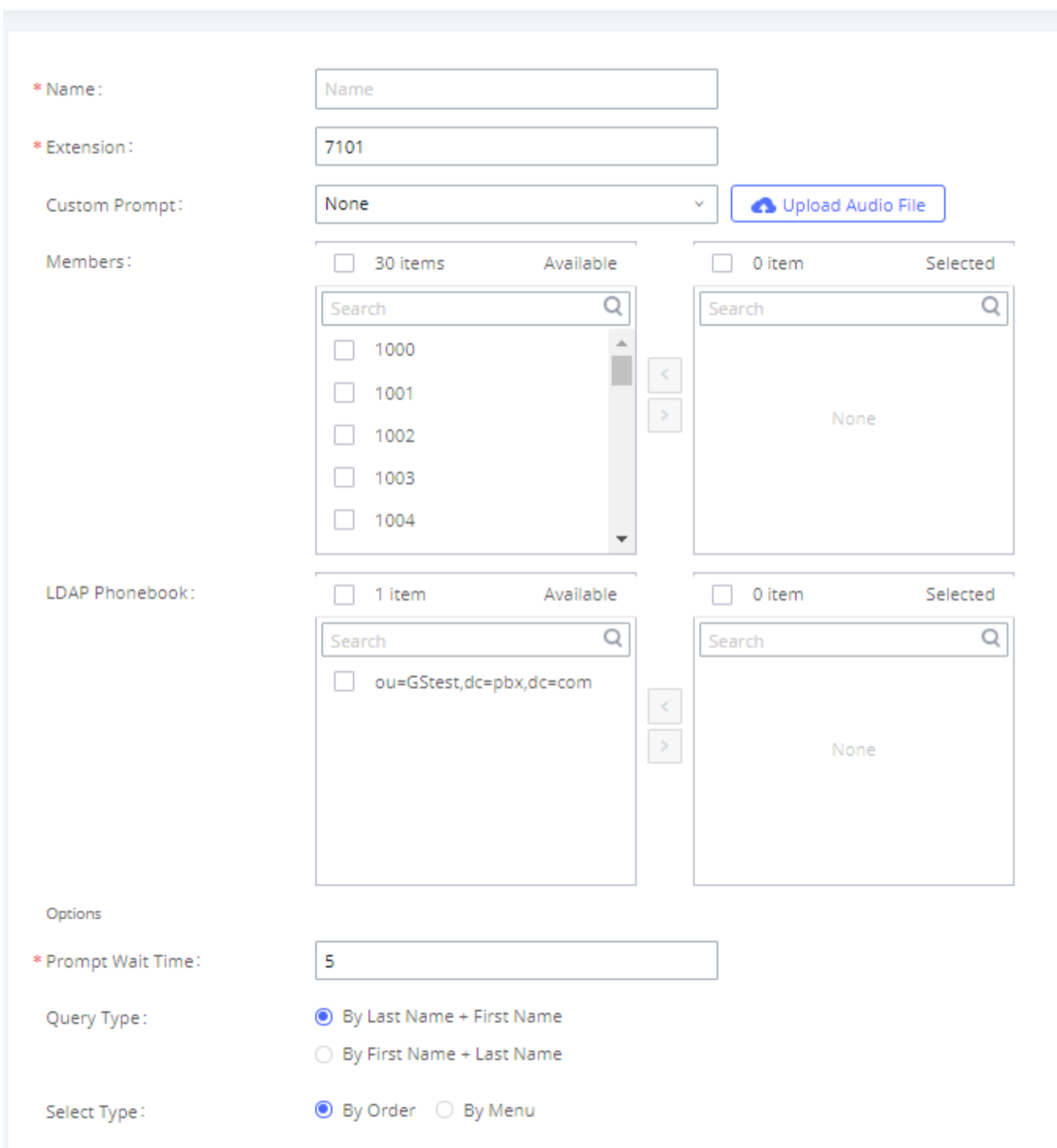


Figure 201: Create Dial by Name Group

User Settings

| | | | |
|----------------------|--------------------------------------|------------------------------|--|
| First Name: | <input type="text" value="John"/> | Last Name: | <input type="text" value="DOE"/> |
| Email Address: | <input type="text"/> | * User Password: | <input type="password" value="*****"/> |
| * Language: | <input type="text" value="Default"/> | * Concurrent Registration... | <input type="text" value="1"/> |
| Mobile Phone Number: | <input type="text"/> | | |

Figure 202: Configure Extension First Name and Last Name

1. Name

Enter a Name to identify the Dial by Name group.

1. Extension

Configure the direct dial extension for the Dial By Name group.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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... ▾ | |

Figure 203: Dial By Name Group In IVR Key Pressing Events

Edit Inbound Rule

Save

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

Figure 204: 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.

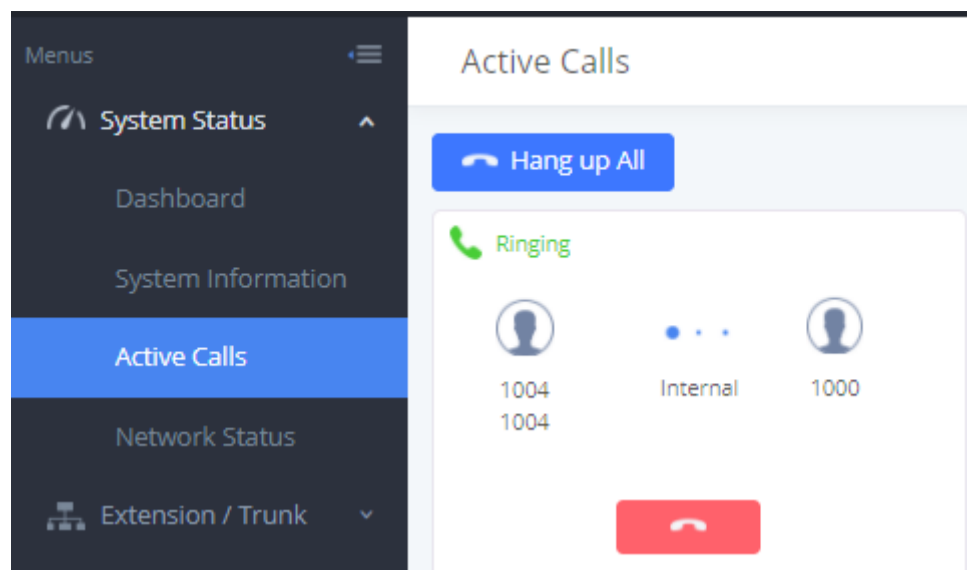


Figure 205: Status→PBX Status→Active Calls – Ringing

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

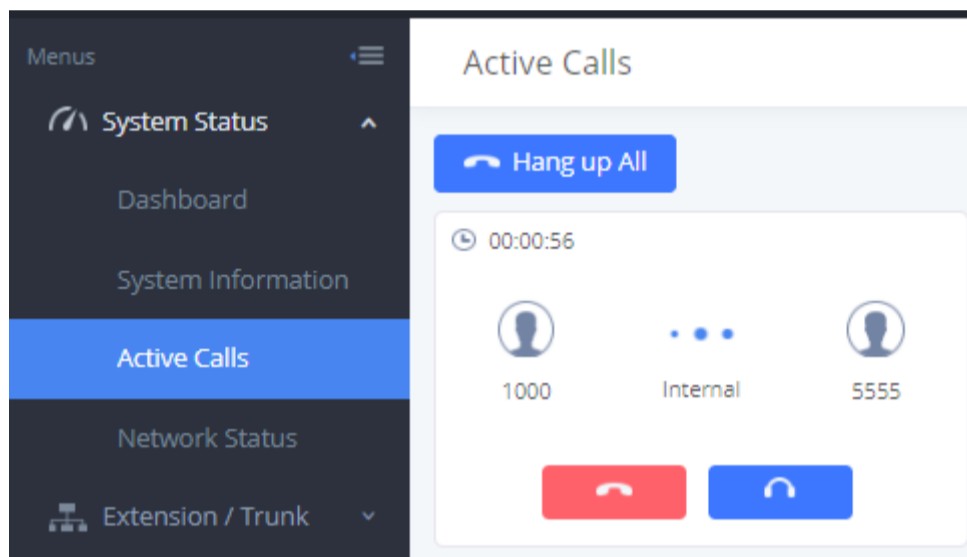


Figure 206: Status→PBX Status→Active Calls – Call Established

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

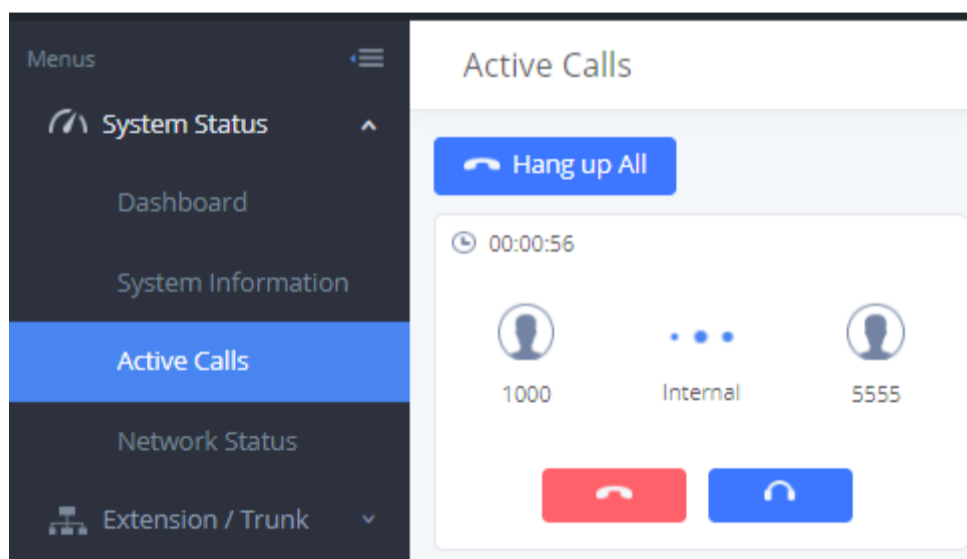


Figure 207: Call Connection less than half hour

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

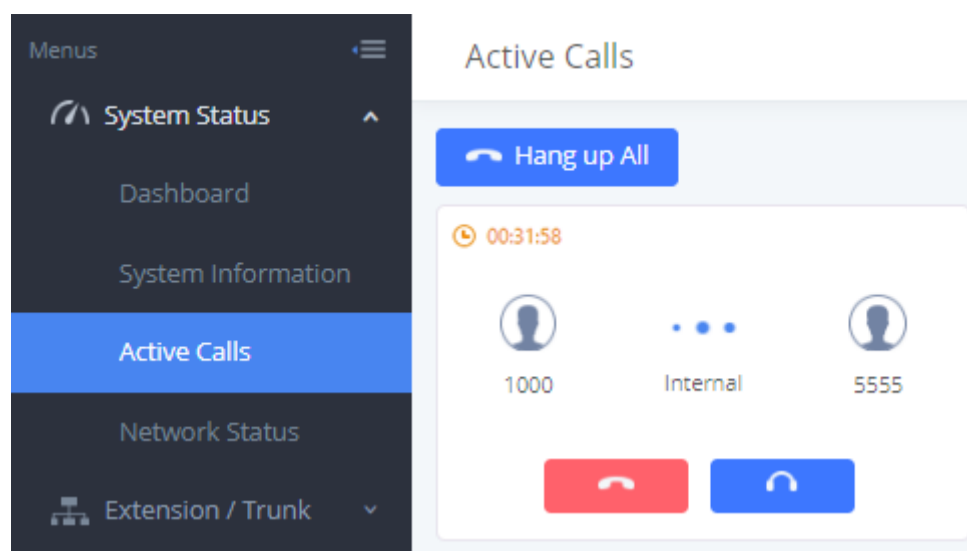


Figure 208: Call Connection between half an hour and one hour

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

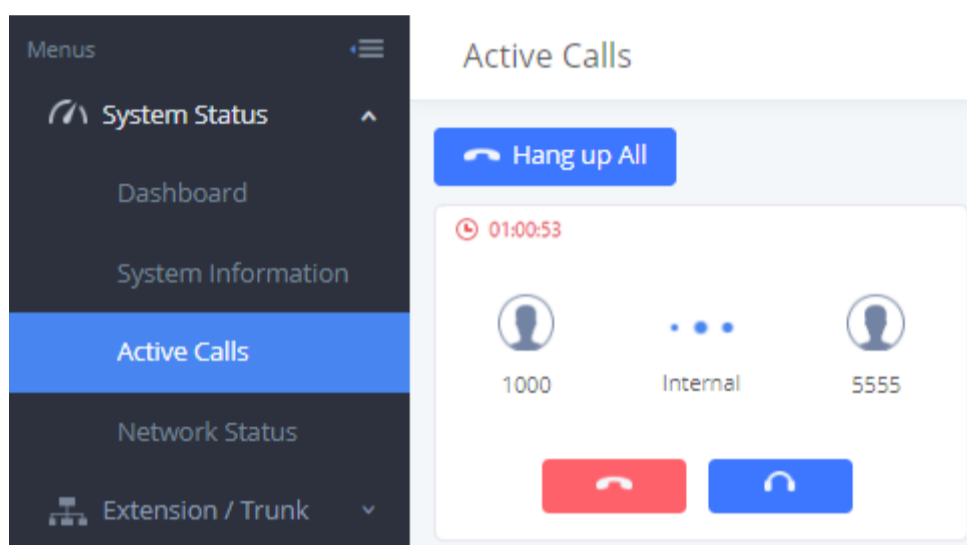


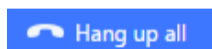
Figure 209: Call Connection more than one hour

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.

Figure 210: 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 *[Table 99: UCM630xA Feature Codes]* and *[Call Recording]* section for instructions.

CALL FEATURES

The UCM630xA supports call recording, transfer, call forward, call park and other call features via feature code. This section lists all the feature codes in the UCM630xA and describes how to use the call features.

Feature Codes

Table 99: UCM630xA Feature Codes

| Feature Maps | |
|--------------------------|---|
| Blind Transfer | <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> ● 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 | <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee. |
| Seamless Transfer | <ul style="list-style-type: none"> ● Default code: *44 (Disabled by default). ● Seamless Transfer allows user to perform blind transfer using UCM feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple. ● During an active call use the feature code (*44 by default) followed by the number you want to transfer to in order to perform the seamless transfer. |
| Disconnect | <ul style="list-style-type: none"> - Default code: *0 - Enter the code during active call. It will disconnect the call. - Options: <ul style="list-style-type: none"> ● 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 | <ul style="list-style-type: none"> - Default code: #72 - Enter the code during active call to park the call. - Options: <ul style="list-style-type: none"> ● Disable ● Allow Caller: Enable the feature code on caller side only. |

| | |
|--|---|
| | <ul style="list-style-type: none"> ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee. |
| Start/Stop Call Recording | <p>-Default code: *3</p> <p>- Enter the code followed by # or SEND to start recording the audio call and the UCM630X will mix the streams natively on the fly as the call is in progress.</p> <p>- Options:</p> <ul style="list-style-type: none"> ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee. |
| Enable Recording Whitelist | Enable the Recording Whitelist feature |
| Recording Operation Whitelist | Select extension in the whitelist that can use the *3 recording function. |
| Feature Code Digits Timeout | Set the maximum interval (ms) between digits for feature code activation |
| DND/Call Forward | |
| Do Not Disturb (DND) Activate | Default code: *77 |
| Do Not Disturb (DND) Deactivate | Default code: *78 |
| Call Forward Busy Activate | <p>- Default Code: *90</p> <p>- Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.</p> |
| Call Forward Busy Deactivate | Default Code: *91 |
| Call Forward No Answer Activate | <p>- Default Code: *92</p> <p>- Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.</p> |
| Call Forward No Answer Deactivate | Default Code: *93 |
| Call Forward Unconditional Activate | <p>- Default Code: *72</p> <p>- Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.</p> |
| Call Forward Unconditional | Default Code: *73 |

| | |
|--|--|
| Deactivate | |
| 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 | Configures and enables CFB for any extension. |
| Remote Call Forward No Answer Enable | Configures and enables CFNA for any extension. |
| Remote Call Forward Always Enable | Configures and enables CFU for any extension. |
| Remote DND Enable | Enables Do Not Disturb for any extension. |
| Remote Call Forward Busy Disable | Disables CFB for any extension. |
| Remote Call Forward No Answer Disable | Disables CFNA for any extension. |
| Remote Call Forward Always Disable | Disables CFU for any extension. |
| Remote DND Disable | 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. |

| | |
|-------------------------------------|---|
| My Voicemail | - Default Code: *97 - Press *97 to access the voicemail box. |
| Voicemail Group Access Code | Dial this code to access group voicemail. If password is required, enter password followed by the pound (#) key. |
| 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. |
| Agent Unpause | - Default Code: *84 - Unpause the agent in all call queues. |
| Dynamic Agent Logout | 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. |
| 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. |
| Barge Spy | This is the feature code to join in on the call to assist both parties. The default setting is *56. |
| 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. |
| PMS | |
| PMS Wakeup | Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service. |

| | |
|--|--|
| Service | |
| PMS Remote Wakeup Service | Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions. |
| Update PMS Room Status | <p>2 methods are available:</p> <p>1. Dial the room status feature code + maid code, listen to the prompt and then dial the appropriate key for the desired room status. Example: Maid with maid code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available.</p> <p>2. Dial room status feature code*maid code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: Maid with maid code 0001 dials *23*0001*1 to change room status Available.</p> |
| 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. |
| 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. |
| Blacklist Add | Follow the voice prompt to add a caller ID 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. |
| 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 | <ul style="list-style-type: none"> - 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 UCM Wakeup Service. You can add, update, activate or deactivate UCM Wakeup Service. |
| Remote Extension Privilege Update | <p>Whitelisted extensions will be able to use the Remote Extension Privilege Update feature code to remotely change any extension's outgoing call privilege.</p> <p>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.</p> |
| Remote Extension Privilege Update Whitelist | <p>Remote Extension Privilege Update Whitelist</p> <p>Procedure:</p> |

1. Dial *26 on the whitelisted extension, hear the prompt "Change extension's outgoing permission level, please enter the phone number, then enter # key."
2. After the process, voice will prompt "Press 1 to set to internal, press 2 to set to local, press 3 to set to national, press 4 to set to international."
3. After selecting, it will prompt "Change extension XXXX outgoing permission to XXX", and hang up.

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

Figure 211: Enable/Disable Feature codes

Parking Lot

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

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

Figure 212: Parking Lot

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

Create New Parking Lot Cancel Save

| | | | |
|------------------------------------|----------------------------------|-------------------------------|--------------------------------------|
| * Parking Lot Extension: | <input type="text"/> | * Parking Lot Name: | <input type="text"/> |
| * Parking Slots: | <input type="text"/> | Use parklot as extension: | <input type="checkbox"/> |
| * Parking Timeout (s): | <input type="text" value="300"/> | Music on Hold Playlists: | <input type="text" value="Default"/> |
| Fallover Destination: | <input type="text"/> | Ring-All Callback on Timeout: | <input type="checkbox"/> |
| Forward to Destination on Timeout: | <input type="checkbox"/> | | |

Figure 213: New Parking Lot

Table 100 : Parking Lot

| | |
|--|---|
| Parking Lot Extension | <ul style="list-style-type: none"> ◦ Default Extension: 700 ◦ During an active call, initiate blind transfer and then enter this code to park the call. |
| Parking Lot Name | <ul style="list-style-type: none"> ◦ Set a name to the parking lot |
| Parked Slots | <ul style="list-style-type: none"> ◦ 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 | <ul style="list-style-type: none"> ◦ 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) | <ul style="list-style-type: none"> ◦ 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.

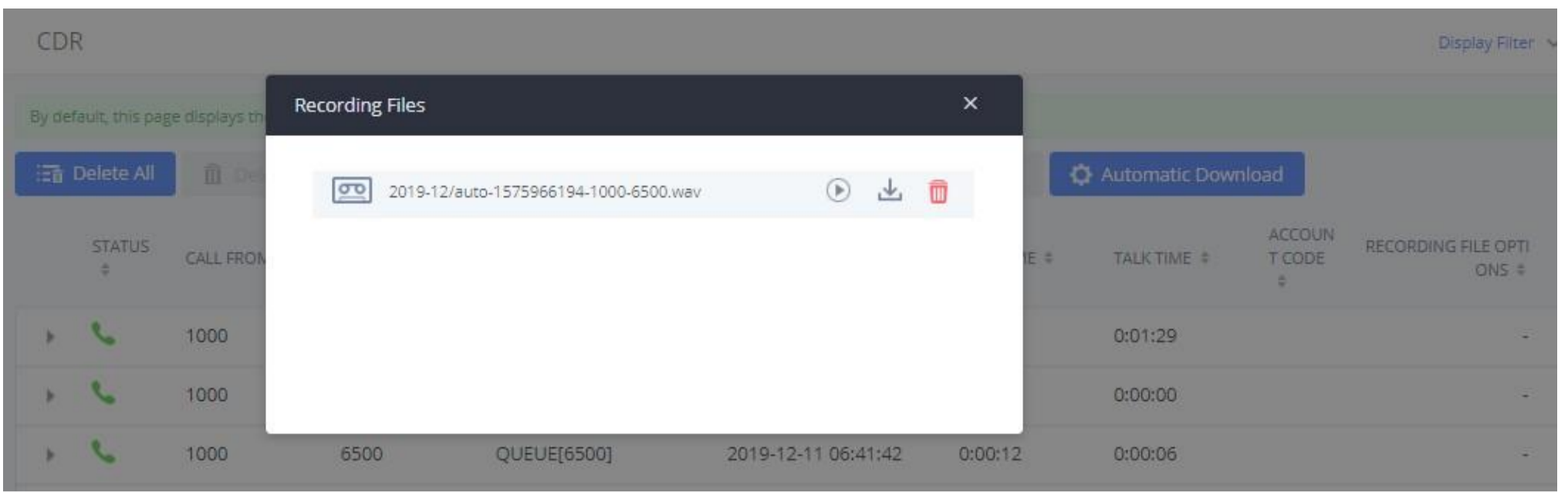


Figure 215: Download Recording File from CDR Page

The above recorded call's recording files are also listed under the UCM630xA Web GUI → CDR → Recording Files.

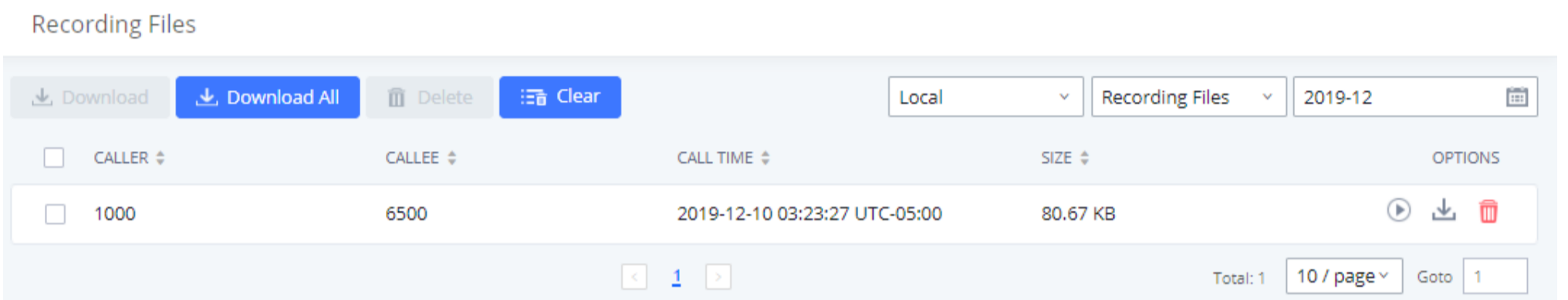


Figure 216: Download Recording File from Recording Files Page

Enable Spy

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

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

Caution:

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

Shared Call Appearance (SCA)

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

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

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

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:

Figure 217: Enabling SCA option under Extension's Settings

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

SCA

SCA Number Group | SCA Line Status

| STATUS | SHARED LINE | ROLE | IP AND PORT | SUBSCRIBED | OPTIONS |
|-------------|-------------|--------|-------------|------------|----------|
| Unavailable | 1000 | shared | -- | no | + [edit] |

Total: 1 | 10 / page | Goto 1

Figure 218: SCA Number Configuration

1. 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

Figure 219: SCA Private Number Configuration

1. 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

Figure 220: SCA Options

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

The following table describe the SCA Number configuration setting:

Table 101: Add SCA Private Number

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

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

Table 102: Editing the SCA Number

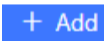
| | |
|---|---|
| Shared Line Number | While SCA is enabled, this number will be the same as the extension number. |
| Allow Call Retrieve from Another Location | Allows remote call retrieval. Must be enabled in public hold. By default, it is enabled. |
| Alert All Appearances for Group Paging Calls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

| | |
|---|--|
| Allow Bridging between Locations | Allows location bridging for SCA group. Must be enabled when using the Barge-In feature. By default, it is disabled. |
| Bridge Warning Tone | <p>Configures the notification in the bridge when another party join.</p> <ul style="list-style-type: none"> ◦ 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. <p>By default, it is set to “Barge-In Only”.</p> |

ANNOUNCEMENT

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

To configure Announcement, users need to follow below steps:

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

Save and apply the configuration.

Create New Announcement

* Name:

Prompt:

Default Destination:

Figure 221: Announcement settings

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

Table 103: Announcement Parameters

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


PBX SETTINGS

This section describes internal options that have not been mentioned in previous sections yet. The settings in this section can be applied globally to the UCM630xA, including general configurations, jitter buffer, RTP settings, ports config and STUN monitor. The options can be accessed via Web GUI→**PBX Settings**→**General Settings**.

PBX Settings/General Settings

Internal Options/General

| General Preferences | |
|---|---|
| Global Outbound CID | Configure the global CallerID used for all outbound calls when no other CallerID is defined with higher priority. If no CallerID is defined for extension or trunk, the global outbound CID will be used as CallerID. |
| Global Outbound CID Name | Configure the global CallerID Name used for all outbound calls. If configured, all outbound calls will have the CallerID Name set to this name. If not, the extension's CallerID Name will be used. |
| Ring Timeout | Configure the number of seconds to ring an extension before the call goes to the user's voicemail box. The default setting is 60 . Note: This is the global value used for each extension if "Ring Timeout" field is left empty on the extension configuration page. |
| Call Duration Limit | Block calls for the configured duration. If Extensions->Features->Call Duration Limit and Outbound Routes->Call Duration Limit are not configured, General Settings->Call Duration Limit will be used. |
| Record Prompt | If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the UCM630X will play voice prompt "The call will be recorded". The default setting is "No". |
| Allow External Numbers to Cancel Recording | If enabled, external call parties will be given the option to decline the recording of calls. The IVR will prompt the user to dial *3 in order to cancel the call recording. |
| Stereo Recording | If enabled, the caller and callee's audio will be split into two channels during call recording. Not applicable to calls with more than 2 parties. |
| Calling Channel | Configure the audio channels for the calling party and the called party. If the caller is selected as the right channel, the callee will be used for the left channel, and vice-versa. Note: This option will be available when "Stereo Recording" is enabled. |
| International Call Prefix | When this configuration is empty, International Call Prefix can be empty or +. |
| Extension Preferences | |
| Enforce Strong Password | If enabled, a strong password policy will be enforced. This does not affect user login passwords, which must be strong. |

| | |
|---|---|
| Enable Random Password | If enabled, the extension will be created with a randomly generated password. |
| Send Extension Update Emails | If enabled, an email will be sent to an extension's configured email address after creating it or modifying that extension's settings. |
| Disable Extension Range | If set to "Yes", users could disable the extension range pre-configured/configured on the UCM630X. The default setting is "No". Note: It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues. |
| Extension Ranges | <p>The default extension range assignment is:</p> <ul style="list-style-type: none"> ● User Extensions: 1000-6299 User Extensions is referring to the extensions created under Web GUI → Extension/Trunk → Extensions page. ● Pick Extensions: 4000-4999 This refers to the extensions that can be manually picked from end device when being provisioned by the UCM630X. There are two related options in zero config page → Zero Config Settings, "Pick Extension Segment" and "Enable Pick Extension". If "Enable Pick Extension" under zero config settings is selected, the extension list defined in "Pick Extension Segment" will be sent out to the device after receiving the device's request. This "Pick Extension Segment" should be a subset of the "Pick Extensions" range here. This feature is for the GXP series phones that support selecting extension to be provisioned via phone's LCD. ● Auto Provision Extensions: 5000-6299 This sets the range for "Zero Config Extension Segment" which is the extensions can be assigned on the UCM630X to provision the end device. ● Meeting Extensions: 6300-6399 This extension range is used for creating meeting rooms. ● Ring Group Extensions: 6400-6499 This extension range is used for ring groups ● Queue Extensions: 6500-6599 This range of extensions is used for queueing ● Voicemail Group Extensions: 6600-6699 This extension range is used for voicemail groups. ● IVR Extensions: 7000-7100 This extension range is used for ● Dial By Name Extensions: 7101-7199 This extension range is used for Dial by Name feature ● FAX Extension: 7200-8200 This extension range is used for T.38 Fax. |
|  | Clicking this button will reset the extension range to their 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.

Table 106: Internal Options/Payload

| | |
|-------------------------------|--|
| AAL2-G.726 | Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112. |
| DTMF | Configured payload type for DTMF. The default setting is 101. |
| G.721 Compatible | Configure to enable/disable G.721 compatible. The default setting is Yes. |
| G.726 | Configure the payload type for G.726 if “G.721 Compatible” is disabled. The default setting is 111. |
| iLBC | Configure the payload type for iLBC. The default setting is 97. |
| OPUS | Configure the payload type for OPUS. The default setting is 123. |
| Audio FEC Payload Type | Configure the Audio FEC Payload Type. The default setting is 127 |
| Audio RED Payload Type | Configure the Audio RED Payload Type. Default setting is 122 |

| | |
|-----------------------|--|
| H.264 | Configure the payload type for H.264. The default setting is 99. |
| H.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.

Figure 222: 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.

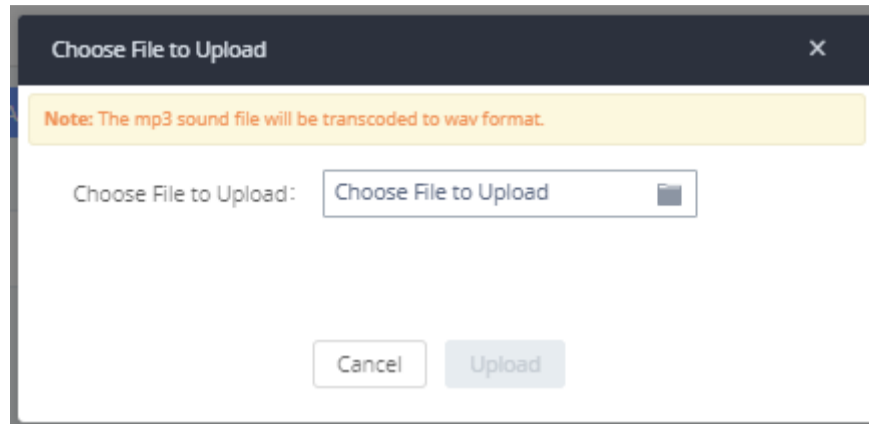


Figure 223: Upload Custom Prompt

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

Download All Custom Prompt

On the 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.

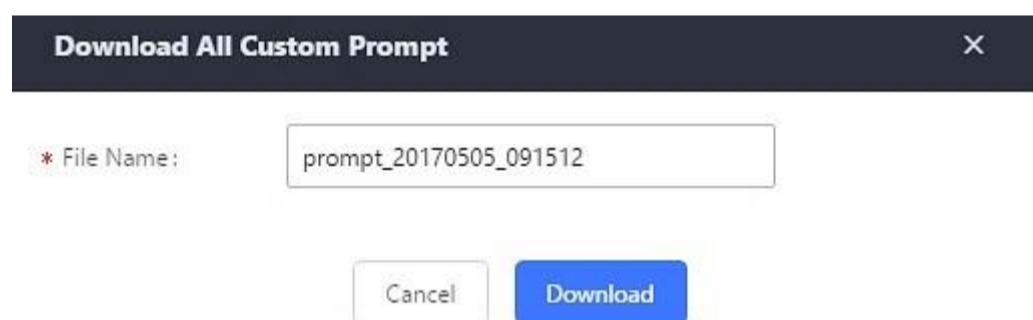


Figure 224: Download All Custom Prompt

Figure 224: Download All Custom Prompt

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

PBX Settings/ Call Failure Tone Settings

SIP Trunk Prompt Tone

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

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

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

Call Failure Tone Settings

SIP Trunk Prompt Tone General Call Failure 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 |
| 485: | sip-trunk-out-busy | 486: | sip-trunk-out-busy |
| 487: | sip-trunk-out-busy | 488: | sip-trunk-out-busy |
| 491: | sip-trunk-out-busy | 493: | sip-trunk-out-busy |

Reset All Default All

| | | | |
|------|----------------------------|------|----------------------------|
| 500: | sip-trunk-out-server-error | 501: | sip-trunk-out-server-error |
| 502: | sip-trunk-out-server-error | 503: | sip-trunk-out-server-error |
| 504: | sip-trunk-out-server-error | 505: | sip-trunk-out-server-error |
| 513: | sip-trunk-out-server-error | | |

Reset All Default All

| | | | |
|------|---------------------------|------|------------------------|
| 600: | sip-trunk-out-busy | 603: | sip-trunk-out-rejected |
| 604: | sip-trunk-out-wrong-nu... | 606: | sip-trunk-out-busy |

Figure 225: SIP Trunk Prompt Tone

General Call Prompt Tones

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

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

Call Prompt Tones

SIP Trunk Prompt Tone

General Call Prompt Tones

Cancel

Save

Specify the tones to play for various general call scenarios.

Reset All

Default All

Bad Number: wrong-number

Out Of Service: out-of-service

User Busy: user-busy

Trunk Busy: trunk-busy

No Answer: no-answer

No Permission: no-permission

Do Not Disturb: user-busy

General Failed: general-failed

Call Waiting: Default Ringback Tone

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

Figure 226: General call Failure Prompts

File Manager

UCM supports automatic or manual recording of calls and storage of IM chat files. Files are allowed to be saved in UCM local or external storage devices, and can even be stored in GDMS cloud storage. The chat files are only allowed to be saved in UCM local or external storage devices, users can go to UCM630xA Web GUI→PBX Settings→File Manager page and select whether to store the recording files in USB Disk, SD card, GDMS or locally on the UCM630xA.

File Manager

Save

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:

Storage Path Priority: GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > USB 1 (Unavailable) > USB (Unavailable) > SD Card (Unavailable) > Local (In Use) Custom

Video Recording Files

Enable Auto Change:

Current Path:

IM Files

Enable Auto Change:

Current Path: Local GDMS Cloud Storage

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

Figure 227: Settings→File Manager

Note

Once a storage device has filled up, the UCM will choose the next available storage device based on the *Storage Path Priority*.

- If “**Enable Auto Change**” is selected, the files will be automatically saved in the available USB Disk or SD card plugged into the UCM630xA. If both USB Disk and SD card are plugged in, the files will be always saved in the USB Disk.
- When “Enable Auto Change” is enabled, the option “**Storage Path Priority**” will appear. It allows the user to configure the priority of each storage unit in the priority list (The storage on top of the list has the highest priority). The default priority list is *GDMS Cloud Storage > NAS > USB 1 > USB > SD Card > Local*
- If “**Local**” is selected, the files will be stored in UCM630xA internal storage.
- If “**GDMS Cloud Storage**” is selected, data will no longer be stored locally and if you need to listen to the recording, download the file to the computer side and play it offline.

Once “USB Disk” or “SD Card” is selected, click on “OK”. The user will be prompted to confirm to copy the local files to the external storage device.

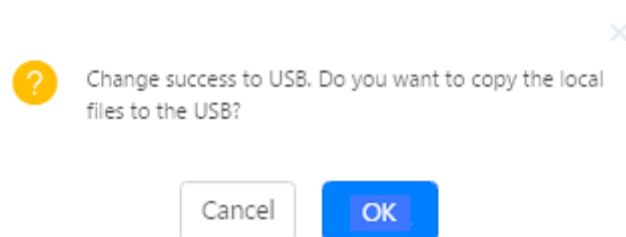


Figure 228: Recordings Storage Prompt Information

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

Edit Please select the files that you want to copy.:

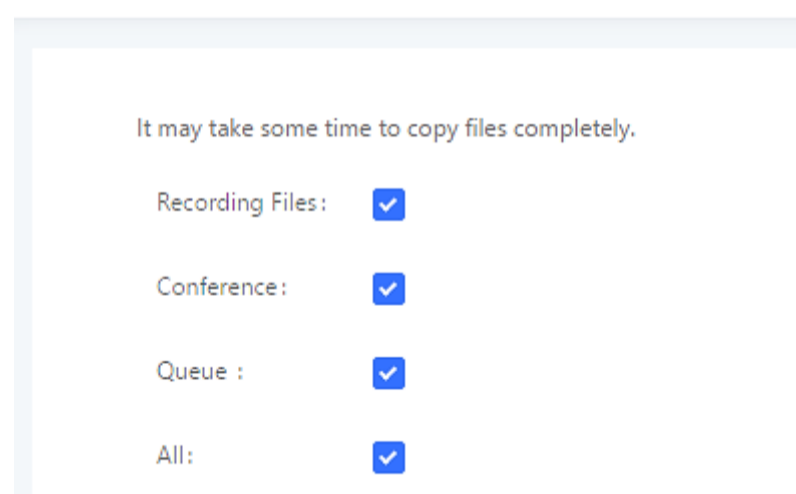


Figure 229: Recording Storage Category

On the UCM630xA, users have the following options when select the categories to copy the files to the external device:

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

PBX Settings/NAS

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

Table 107: NAS Settings

| | |
|----------------------|--|
| Enable | Enabled / Disable the NAS recording functionality. |
| Host | Configure the Domain or IP address of the NAS server. Note: Currently, only IP addresses are supported in the Host/IP field. |
| Share Name | Specify the name of the shared folder. |
| Username | Specify the account username to access the NAS server. |
| Password | Configure the account password to access the NAS server. |
| Security Mode | Select a security mode based on the server settings to ensure proper connection establishment. The default value is ntlmssp. |
| Status | If configured correctly, the Status field will show “Mounted”, and the newly added NAS server will be shown on the Mounted Netdisk List. Additionally, the NAS will appear as a selectable storage option in the PBX Settings→Recording Storage page and CDR→Recording Files page. |

Note

If Network Storage Device has 1GB of storage space left, it will be considered unavailable the UCM will trigger the external disk usage alert.

SIP SETTINGS

The UCM630xA SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

SIP Settings/General

Table 108: 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 | <p>If enabled, the UCM630xA allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is “No”.</p> <p>Warning:</p> <p>Please be aware of the potential security risk when enabling “Allow Guest Calls” as this will allow any user with the UCM630xA address to dial into the UCM630xA.</p> |
| Allow Transfer | <p>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”.</p> |
| MWI From | <p>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.</p> |
| Enable Diversion Header | <p>If disabled, the UCM will not forward the diversion header.</p> |
| Block Collect Calls | <p>If enabled, collect calls will be blocked.</p> <p>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”.</p> |

SIP Settings/MISC

Table 109: SIP Settings/Misc

| Outbound SIP Registrations | |
|-----------------------------------|---|
| Register Timeout | Configure the register retry timeout (in seconds). The default setting is 20. |
| Register Attempts | Configure the number of registration attempts before the UCM630X gives up. The default setting is 0, which means the UCM630X will keep trying until the server side accepts the registration request. |
| Trunk Register Period (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. |
| Video | |
| Max Bit Rate (kb/s) | Configure the maximum bit rate (in kb/s) for video calls. The default setting is 384. |
| Support SIP Video | Select to enable video support in SIP calls. The default setting is “Yes”. |
| 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 enable, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passthrough. |
| Early Media | |
| Enable Use Final SDP | If enabled, call negotiation will use final response SDP. |
| Ignore 180 Response | If enabled, ringing indication after 183 response will be ignored. |
| Blind Transfer | |
| Allow callback when blind transfer fails | If enabled, the UCM will call back to the transferrer when blind transfer fails (reason of failure includes busy and no answer). Note: This feature takes effect only on internal calls. |
| Blind transfer timeout | Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s. |
| Hold | |
| Forward HOLD Requests | Configure the UCM to forward HOLD requests instead of processing holds internally. This serves to meet the standards set by some providers that require HOLD requests to be passed along from endpoint to endpoint. This option is disabled by default. Note: Enabling this option may cause hold retrieval issues and MOH to not be heard. |

SIP Settings/Session Timer



Table 110: SIP Settings/Session Timer

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

SIP Settings/TCP and TLS

SIP Settings/TCP and TLS

| | |
|------------------------------|--|
| TCP Enable | Configure to allow incoming TCP connections with the UCM630X. The default setting is “No”. |
| TCP Bind IPv4 Address | Configure the IP address for 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 UCM630X. The default setting is “Yes”. |
| TLS Bind IPv4 Address | Configure the IPv4 address for TLS server to bind to. “0.0.0.0” means binding to all interfaces. The port number is optional, and the default port number is 5061. For example, 192.168.1.1:5063. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses. |
| TLS Bind IPv6 Address | Configure the IPv6 address for TLS server to bind to. “[::]” means bind to all interfaces. The port number is optional with default being 5061. For example, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5061. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses. |
| TLS Do Not Verify | If enabled, the TLS server’s certificate will not be verified when acting as a client. The default setting is “Yes”. |
| TLS Self-Signed CA | This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server’s public key. This |

| | |
|---|---|
| | file will be renamed as “TLS.ca” automatically. |
|  | Clicking on this button will reset the certificates. |
| Private Certificate and Key | |
| TLS Cert | This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as “TLS.pem” automatically. Note: The size of the uploaded certificate file must be under 2MB. |
| TLS 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. Note: The size of the uploaded CA certificate file must be under 2MB. |
|  | 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

Table 112: 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

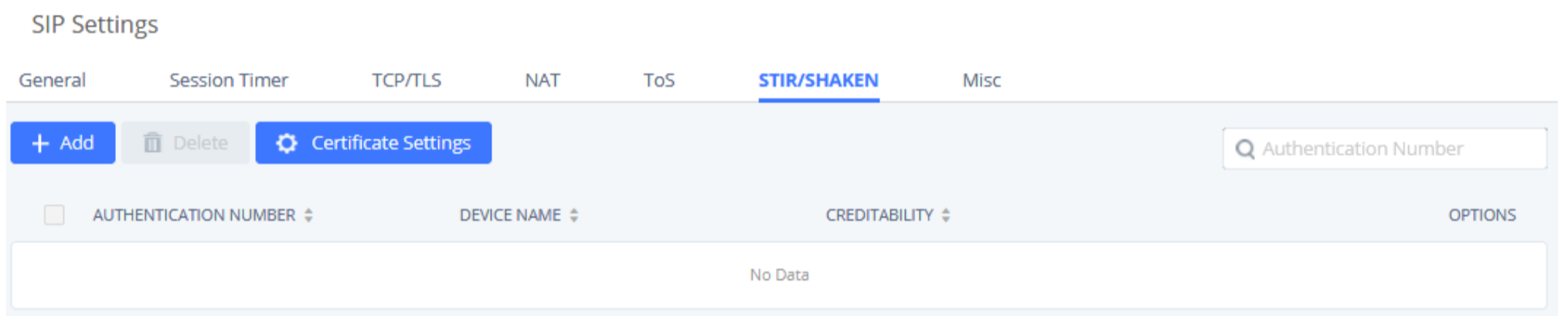
Table 113: SIP Settings/ToS

| | |
|--|--|
| ToS for SIP | Configure the Type of Service for SIP packets. The default setting is None. |
| ToS for RTP Audio | Configure the Type of Service for RTP audio packets. The default setting is None. |
| ToS for RTP Video | Configure the Type of Service for RTP video packets. The default setting is None. |
| Default Incoming/Outgoing Registration Time | Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120. |
| Max Registration/Subscription Time | Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the 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 | <p>Configure whether the UCM630xA should generate Inband ringing or not. The default setting is “Never”.</p> <ul style="list-style-type: none"> ◦ 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.



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

Add Authentication Number
×

* Authentication Number:

* Device Name:

* Creditability:

Figure 230: SIP Settings/STIR/SHAKEN – Add Authentication Number

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

| | |
|------------------------------|--------------------------------------|
| Authentication Number | Configure the Authentication Number. |
| Device Name | Configure the device name. |

| | |
|----------------------|--|
| Creditability | <p>Configure the attestation level, which is the level of confidence of the carrier that the CID has not been spoofed. The following options are available:</p> <ul style="list-style-type: none"> ○ 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:

The screenshot shows a 'Certificate Settings' dialog box with the following fields and values:

- * Certificate Download Time (s):** 2
- * Signature Valid Time (s):** 15
- * Private Key:** private.key
- * Public Key:** public.crt

Buttons: Cancel, Save

Figure 231: SIP Settings/STIR/SHAKEN – Certificate Settings

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

| | |
|--------------------------------------|---|
| Certificate Download Time (s) | Configure the public key download timeout period, the default value is 2 seconds. |
| Signature Valid Time (s) | Configure the validity period of the digital signature, the default value is 15 seconds. |
| Private Key | <p>Configure the Private key.</p> <p>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”.</p> |
| Public Key | <p>Configure the Public Key.</p> <p>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”.</p> |

Transparent Call-Info header

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

```
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:3001@192.168.6.36:5064 SIP/2.0
Message Header
  Via: SIP/2.0/UDP 192.168.6.187:5060;rport;branch=z9hG4bKPj3217e67b-e74f-4f9f-b06f-afd3dcbbe29b
  From: "3002" <sip:3002@192.168.6.187>;tag=202dca4f-2b9d-4880-924c-d48cea7d0596
  To: <sip:3001@192.168.6.36>
  Contact: <sip:68aae6ea-f1d4-4e62-9987-446e718a2448@192.168.6.187:5060>
  Call-ID: 7f66bb20-0b9f-4828-a355-698853b8d9fb
  CSeq: 17559 INVITE
  Allow: OPTIONS, INFO, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REGISTER, REFER
  Supported: 100rel, timer, replaces, noferesub
  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
```

Figure 232: Transparent Call-Info

IAX SETTINGS

The UCM630xA IAX global settings can be accessed via Web GUI→PBX Settings→IAX Settings.

IAX Settings/General

Table 116: IAX Settings/General

| | |
|--------------------------------|--|
| Bind Port | Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569. |
| Bind IPv4 Address | Force IAX2 to bind to a specific address instead of all addresses. |
| Bind IPv6 address | Configure the IPv6 address to bind to. “[:]” means to bind to all IP addresses. |
| IAX1 Compatibility | Select to configure IAX1 compatibility. The default setting is “No”. |
| No Checksums | If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this feature. The default setting is “No”. |
| Delay Reject | If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is “No”. |
| ADSI | Select to enable ADSI phone compatibility. The default setting is “No”. |
| Music On Hold Interpret | Specify which Music On Hold class this channel would like to listen to when being put on hold. This music class is only effective if this channel has no music class configured and the bridged channel putting the call on hold has no “Music On Hold Suggest” setting. |
| Music On Hold Suggest | Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold. |
| Bandwidth | Configure the bandwidth for IAX settings. The default setting is “Low”. |

IAX Settings/Registration

Table 117: IAX Settings/Registration

| | |
|---------------------------------|--|
| IAX Registration Options | |
| Min Reg Expire | Configure the minimum period (in seconds) of registration. 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 | <p>Configure codec negotiation priority. The default setting is “Reqonly”.</p> <ul style="list-style-type: none">◦ Caller Consider the callers preferred order ahead of the host’s.◦ Host Consider the host’s preferred order ahead of the caller’s.◦ Disabled Disable the consideration of codec preference all together.◦ Reqonly This is the same as “Disabled”, except when the requested format is not available. The call will only be accepted if the requested format is available. |
| Type of Service | Configure ToS bit for preferred IP routing. |
| IAX Trunk Options | |
| Trunk Frequency | Configure the frequency of trunk frames (in milliseconds). The default is 20. |
| Trunk Time Stamps | If enabled, time stamps will be attached to trunk frames. The default is “No”. |

IAX Settings/Security

Table 118: IAX Settings/Static Defense

| | |
|----------------------------|---|
| Call Token Optional | Enter a single IP address (e.g., 1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) for which call token validation is not required. |
|----------------------------|---|

| | |
|-------------------------------------|--|
| Max Call Numbers | Configure the maximum number of calls allowed for a single IP address. |
| Max Unvalidated Call Numbers | Configure the maximum number of Unvalidated calls for all IP addresses. |
| Max Call Numbers | Configure to limit the number of calls for a give IP address of IP range. |
| IP or IP Range | Enter the IP address (1.1.1.1) or a range of IP addresses (1.1.1.1/255.255.255.255) to be considered for call number limits. |

INTERFACE SETTINGS

Analog Hardware

The analog hardware (FXS port and FXO port) on the 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.

Figure 233: 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

Figure 234: FXO Ports ACIM Settings

Table 119: PBX Interface Settings

| | |
|--------------------|---|
| Tone Region | Select country to set the default tones for dial tone, busy tone, ring tone and etc. to be sent from the FXS port. The default setting is “United States of America (USA)”. |
|--------------------|---|

| Advanced Settings | |
|--------------------------------|---|
| FXO Opermode | Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)". |
| FXS Opermode | Select country to set the On-Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country's analog line characteristics. The default setting is "United States of America (USA)". |
| FXS TISS Override | Configure to enable or disable override Two-Wire Impedance Synthesis (TISS). The default setting is No. If enabled, users can select the impedance value for Two-Wire Impedance Synthesis (TISS) override. The default setting is 600Ω. |
| PCMA Override | Select the codec to be used for analog lines. North American users should choose PCMU. All other countries, unless already known, should be assumed to be PCMA. The default setting is PCMU. Note: This option requires system reboot to take effect. |
| Boost Ringer | Configure whether normal ringing voltage (40V) or maximum ringing voltage (89V) for analog phones attached to the FXS port is required. The default setting is "Normal". |
| Fast Ringer | Configure to increase the ringing speed to 25HZ. This option can be used with "Low Power" option. The default setting is "Normal". |
| Low Power | Configure the peak voltage up to 50V during "Fast Ringer" operation. This option is used with "Fast Ringer". The default setting is "Normal". |
| Ring Detect | If set to "Full Wave", false ring detection will be prevented for lines where Caller ID is sent before the first ring and proceeded by a polarity reversal, as in UK. The default setting is "Standard". |
| FXS MWI Mode | Configure the type of Message Waiting Indicator on FXS lines. The default setting is "FSK". <ul style="list-style-type: none"> ◦ FSK: Frequency Shift Key Indicator ◦ NEON: Light Neon Bulb Indicator. |
| FXO Frequency Tolerance | Allows users to adjust the tolerance of the FXO ringing frequency. 63Hz is considered the standard value and is selected by default. |

DAHDI Settings

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

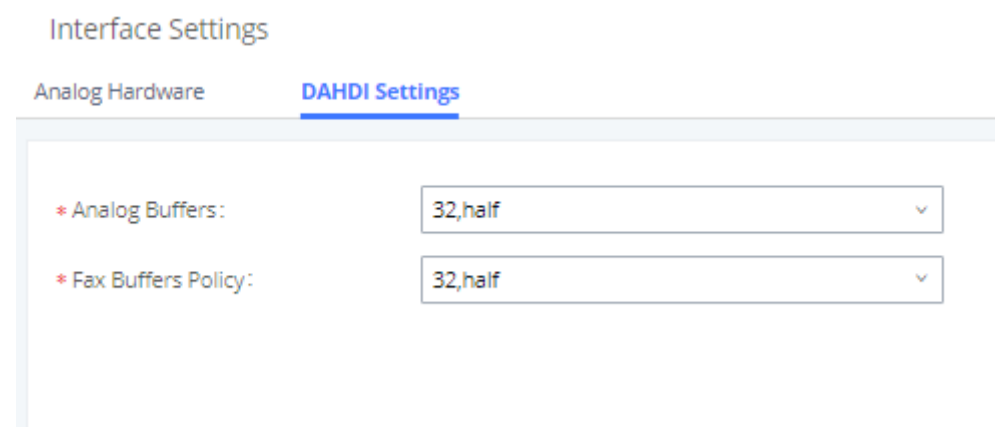


Figure 235: DAHDI Settings

For the value of the option such as “32, half”:

The number in the option indicates the number of read/write buffers for TDM (DAHDI).

The “Half”, “Immediate” or “Full” option indicates the strategy when reading/writing data from buffer.

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

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

Contacts

Address book management is under UCM web UI->Maintenance, and it has two sections “Contact Management” and “Department management”.

Contact Management

Contact management page displays extension contacts and external contacts information.

- Extension contacts

Extension contacts page shows all the extensions that has “Sync Contact” option enabled in extension settings page. The extension contacts here can be edited or deleted individually or in batch. No new extension contact can be added directly from this page. If an extension contact is deleted from this page, “Sync Contact” option is disabled from this extension. This will not delete the extension from UCM.

Note

“Delete” extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

Contact Management

Extension Contacts

External Contacts





















Change Department

Contact Privilege Settings

Delete

Extension Number or Name

Search

| <input type="checkbox"/> | EXTENSION | NAME | DEPARTMENT | EMAIL ADDRESSES | CONTACT PRIVILEGES | OPTIONS |
|--------------------------|-----------|---------------|------------|-----------------|----------------------------------|---|
| <input type="checkbox"/> | 1000 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 1001 | John Doe | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 1002 | Jane Doe | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 1003 | Arthur Morgan | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 1004 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 1005 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 2000 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 2001 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 2002 | | --- | | All Contacts(Same as Department) |   |
| <input type="checkbox"/> | 2003 | | --- | | All Contacts(Same as Department) |   |

< 1 2 >

Total: 11

10 / page

Goto 1

Extension Contacts

Note

“Delete” extension contact will only remove this extension from extension contact page and it will not sync to contacts on UCM. The extension itself still exists on UCM.

Click Edit icon to configure name, department, email address and etc for each extension contact.

* Extension:

First Name:

Last Name:

Department:

Job Title:

Email Address:

Mobile Phone Number:

Home Number:

Fax:

| Contact Privileges

Same as Department

Contact Privileges:

* Contact View [Add / Edit Privileges](#)

Privileges:

Edit Extension Contact

| | |
|--|--|
| Extension | Displays extension number. |
| First Name | Configure first name for the extension contact. |
| Last Name | Configure last name for the extension contact. |
| Department | Select department for the extension contact. Department can be created in “Department Management” page. |
| Department Title | Configure the job title for the extension contact. |
| Email Address | Configure email address for the extension contact. |
| Mobile Phone Number | Configure mobile phone number for the extension contact. |
| Home Number | Configure home number for the extension contact |
| Fax | Configure Fax for the extension contact. |
| Same as Department Contact Privileges | When this option is enabled, the contact extension will inherit the same privilege as the department it belongs to. |
| Contact View Privileges | This option allows configuring privileges for the contact extension. Note: This option will be disabled if “ Same as Department Contact Privileges ” has been enabled. |

- External contacts

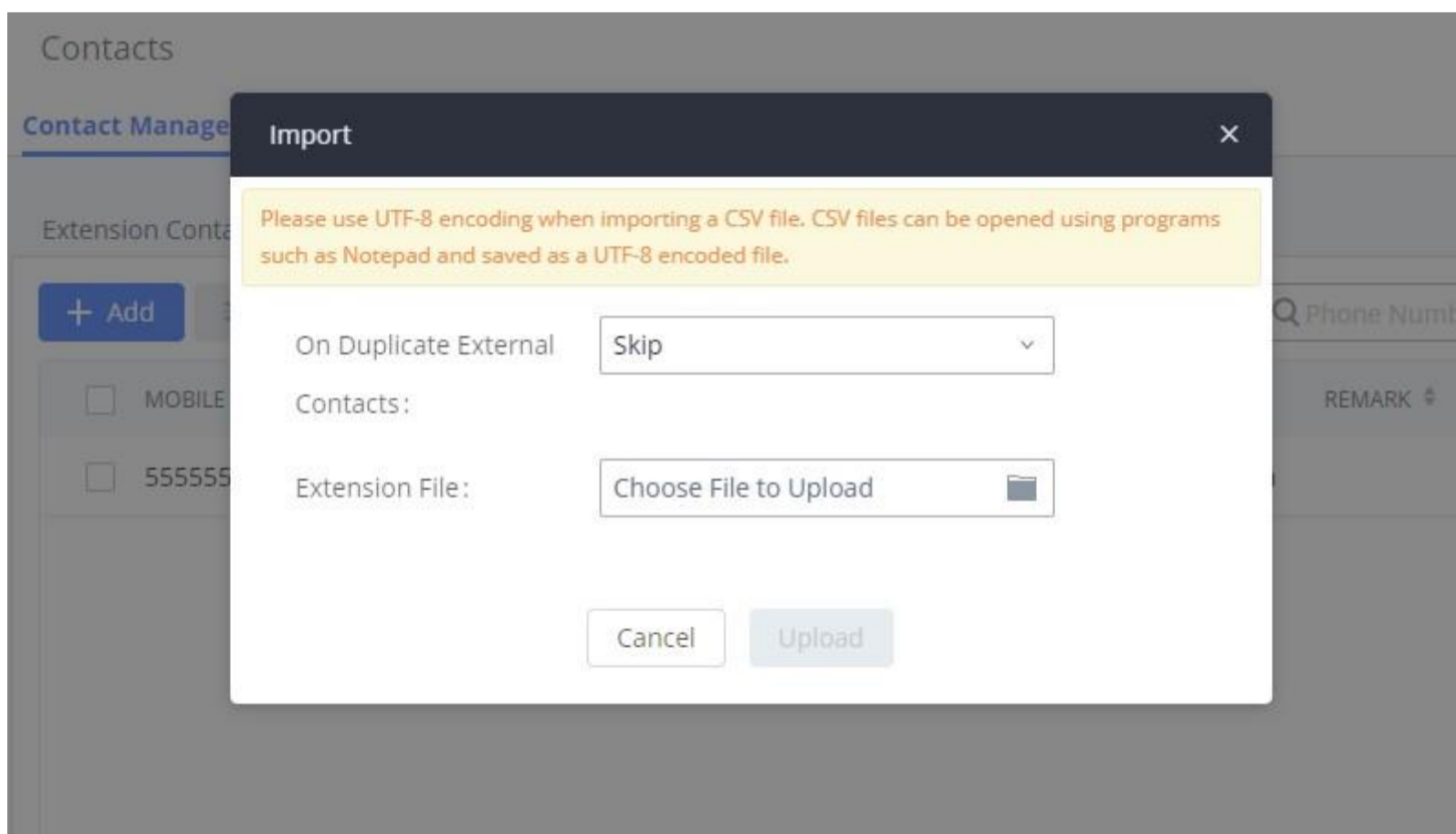
On external contacts page, the admin can create single external contact, import contacts in batch, edit contacts, delete contacts and export contacts.

External Contacts

Click on “Export” icon, a 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.



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.

Figure 337: 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.

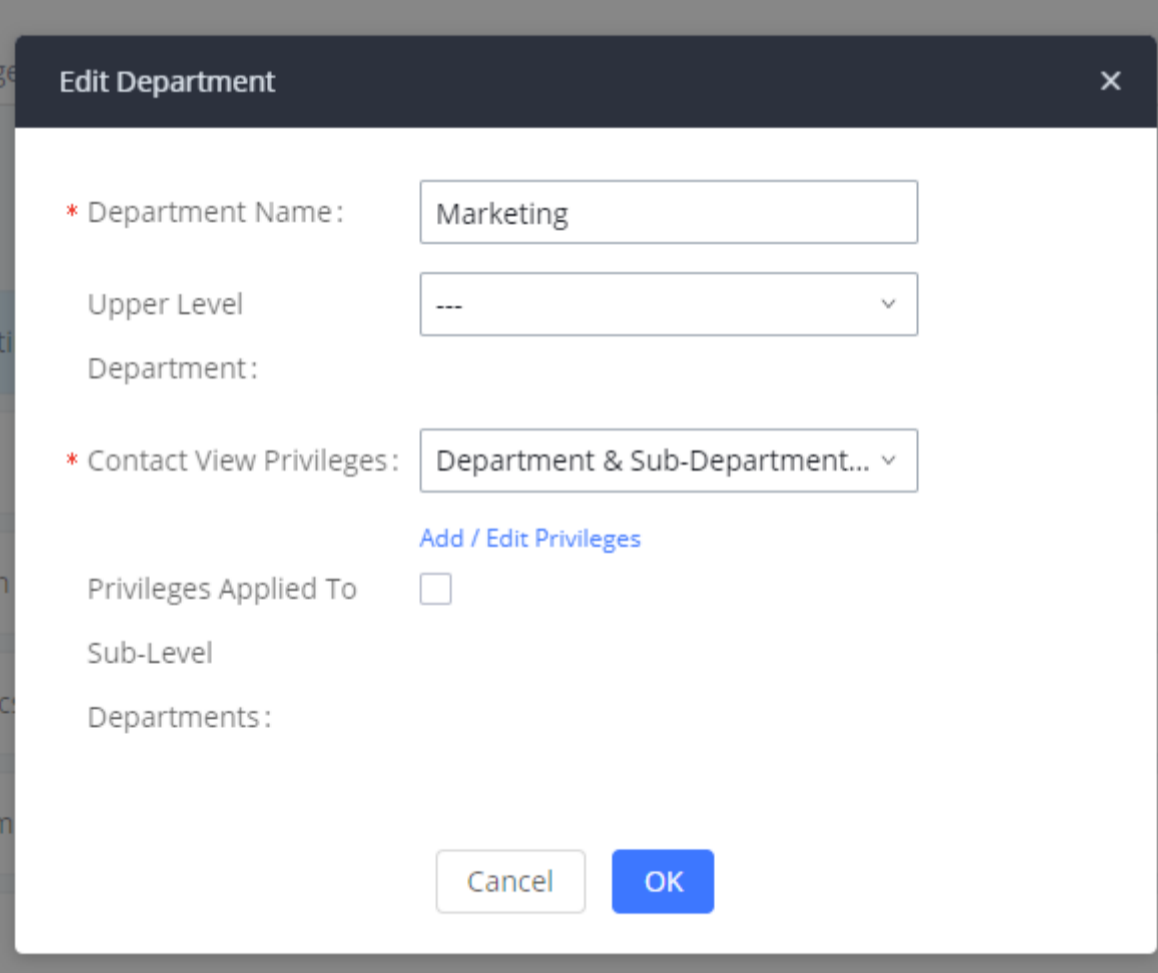


Figure 338: Edit Department

| | |
|--------------------------------|--|
| 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 | <ul style="list-style-type: none"> ● All Contacts: The extensions in this department will be able to see all the contacts. |

| | |
|---------------------------------|--|
| | <ul style="list-style-type: none"> • 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. |

Note

The user can create up to 100 departments with up to 4 levels of nested departments.

Important

To be able to use shared department, the UCM devices will have to be subscribed to a RemoteConnect plan that offers Cloud IM service. For more information please refer to: <https://ucmrc.gdms.cloud/plans>

Privilege Management

The user can configure custom privileges other than the default ones (All contacts, Departments and sub-departments contacts). These custom privileges allow more flexible ways of allowing contacts to view all or specific contacts from other departments.

UCM admin can add or edit Privilege Management; under UCM web UI → **Contacts Privilege Management**, there are 2 default privileges:

- Visible to all contacts.
- Only the contact person's department and sub-department contacts are visible.

When Cloud IM is enabled on the UCM, a third privilege becomes available to choose:

- Local Contacts: Restricts the contacts shown to the contacts of the local UCM.

Privilege Management

[+ Add](#)

| NAME | PRIVILEGE STATUS | OPTIONS |
|--------------------------------------|---|---|
| All Contacts | ● In Use | Edit Share Delete |
| Department & Sub-Department Contacts | ● Not Applied | Edit Share Delete |

< 1 > Total: 2 10 / page Goto 1

Privilege Management — Cloud IM Disabled

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.

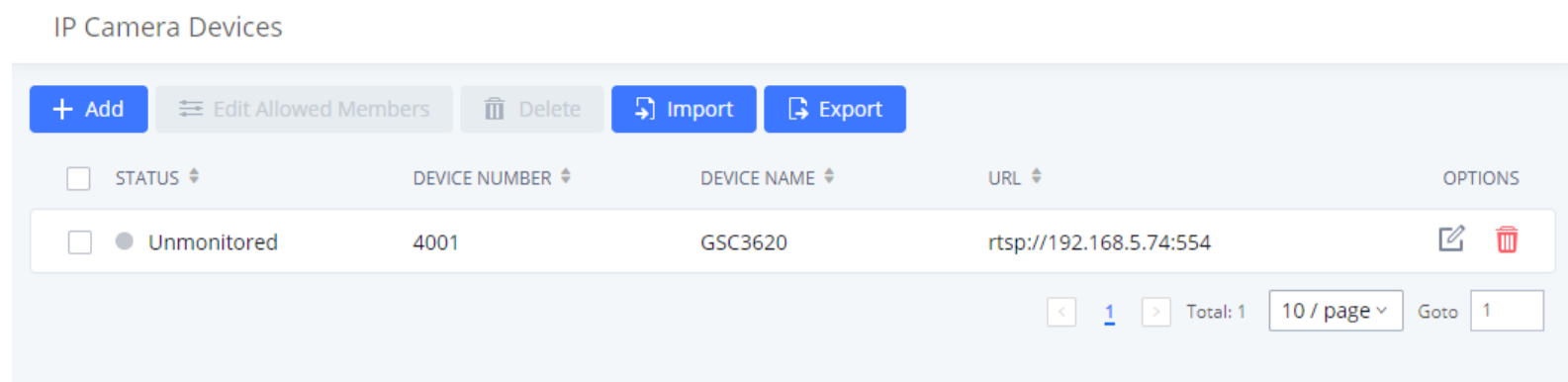


Figure 236: IPC Devices

Edit the IPC device settings in the table below.

Table 120: 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 protocol that will be used. |
| 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:

* IP Address:

* Port:

Channel Path:

Username:

Password:

* Transmission Protocol :

Heartbeat Detection :

User Settings

* Allowed Members:

| Search | Selected(0) |
|-------------------------------|-------------|
| Company Contact | |
| <input type="checkbox"/> All | |
| <input type="checkbox"/> 1005 | |
| <input type="checkbox"/> 2004 | |
| <input type="checkbox"/> 2003 | |

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

Figure 237: IPC Devices Settings

UCM RemoteConnect

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

The RemoteConnect can be configured under **WebGUI→RemoteConnect** After purchasing the RemoteConnect package.

UCM RemoteConnect



For improved call quality and service, please purchase a Remote Work Suite package.

- ✓ Intelligent NAT penetration service will allow for stable and clear remote audio/video calls.
- ✓ Cloud storage service
- ✓ Easily manage remote devices

Go to GDMS to learn more. You can also sign up for a 3-month trial after linking a UCM to GDMS.

[Learn more](#)

[Remote Link Diagnosis](#)

Figure 238: RemoteConnect

On GDMS platform, sign in and go to Device→PBX Device page, click on “Add Device” to add your UCM6300A device to GDMS system, once done an open beta plan will be assigned to the UCM.

In daily operation, the user can click the “Diagnosis” button to diagnose the remote service system. The specific diagnosis content includes media service (STUN/TURN), GDMS link and heartbeat detection, tunnel service (SIP/Web Socket), Cloud IM, UCM bandwidth speed measurement.

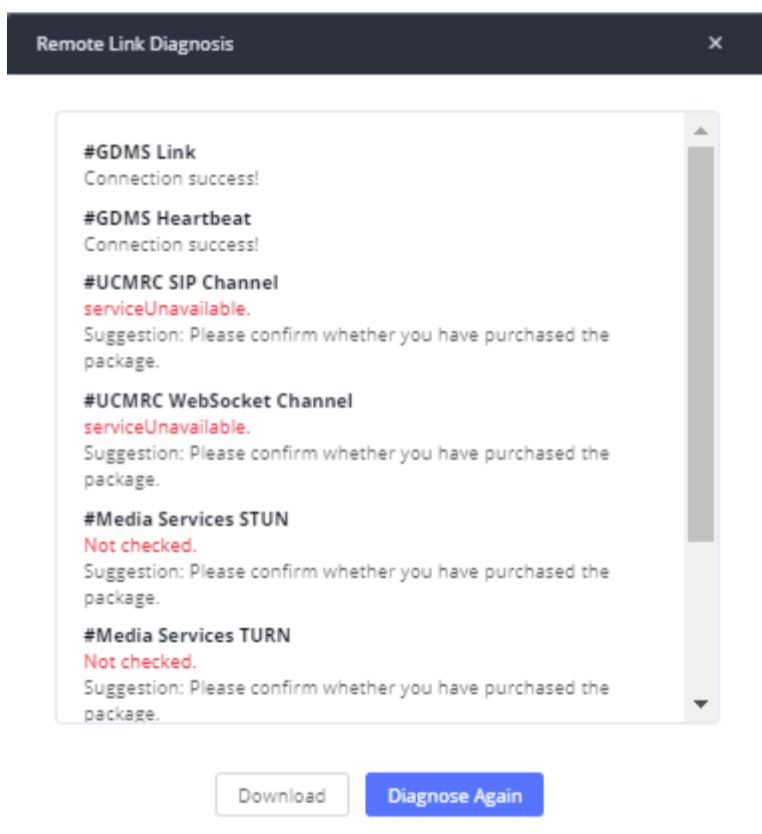


Figure 239: Remote Diagnosis

Figure 240:
UCM
RemoteConnect
– Effective
Plan

Note

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

Plan Settings

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

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

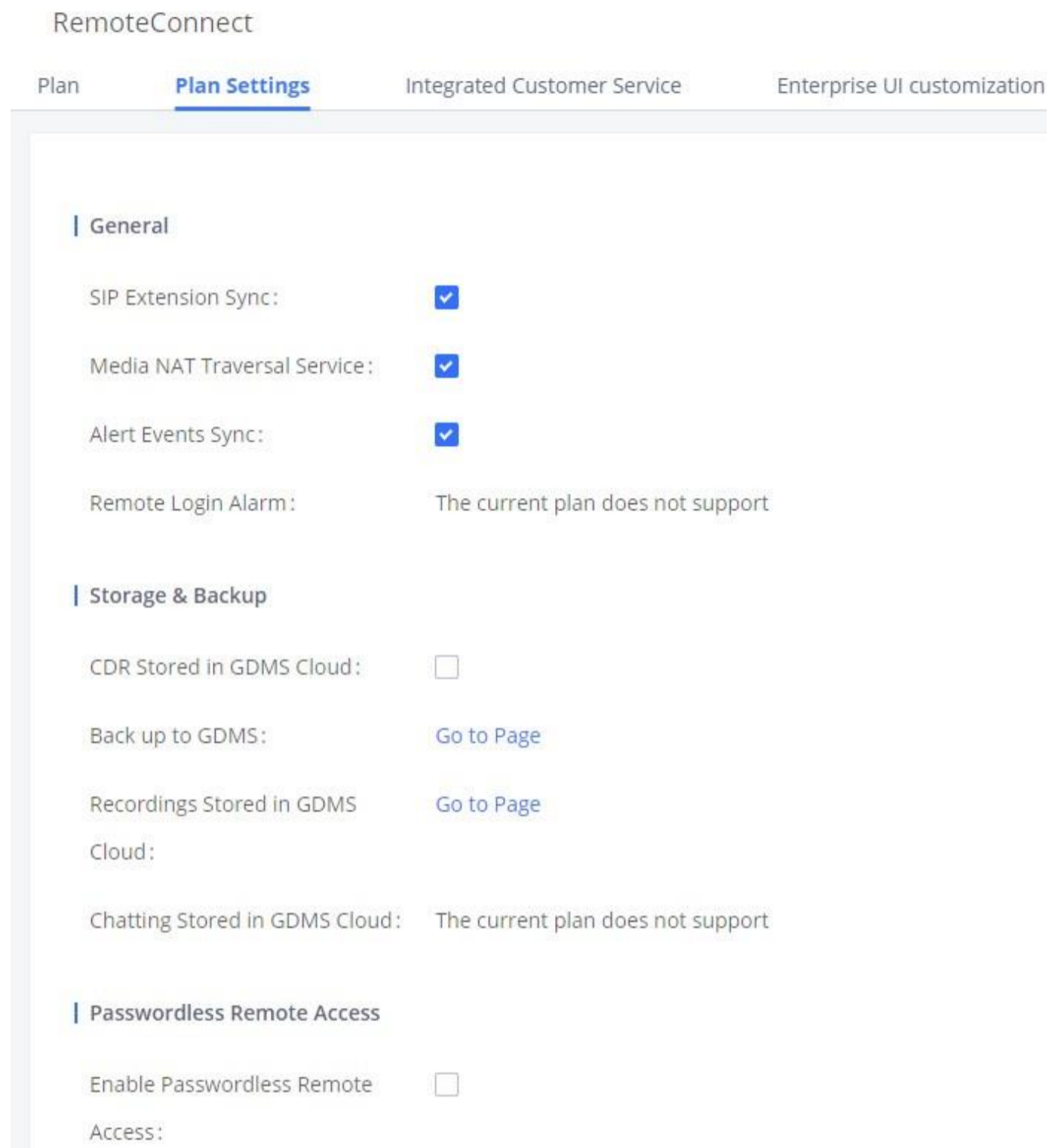


Figure 241: UCM RemoteConnect Plan Settings

After adding UCM to the GDMS platform, UCM will synchronize all SIP extensions to the GDMS platform, this allows to use the GDMS platform for account allocation and terminal management.

The accounts synchronized to GDMS platform can be viewed on the GDMS-> VoIP Account->SIP Account page. As shown in the figure below:

| <input type="checkbox"/> | User ID | Account Name | Display Name | SIP Server | Status | Date Modified | Options |
|--------------------------|----------|--------------|--------------|--------------------------------|------------|------------------|---------|
| <input type="checkbox"/> | 1000 UCM | 1000 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/11/02 10:18 | |
| <input type="checkbox"/> | 1009 UCM | 1009 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/29 10:07 | |
| <input type="checkbox"/> | 1008 UCM | 1008 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/29 10:07 | |
| <input type="checkbox"/> | 1007 UCM | 1007 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/29 10:07 | |
| <input type="checkbox"/> | 1006 UCM | 1006 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/29 10:07 | |
| <input type="checkbox"/> | 1001 UCM | 1001 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/28 16:08 | |
| <input type="checkbox"/> | 1005 UCM | 1005 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/21 10:42 | |
| <input type="checkbox"/> | 1004 UCM | 1004 | — | 192.168.5.167:5060 (192.168... | Unassigned | 2021/10/21 10:42 | |

Figure 242: UCM SIP Extensions synchronized to GDMS

The Media NAT Traversal provides a fully automatic intelligent external network penetration service to ensure that you can make normal calls/conferences on the external network.

CDR data cloud storage provides a service of dumping to GDMS to prevent CDR from continuously increasing occupying UCM storage space.

Alarm event synchronization is to synchronize the alarm information generated on UCM to the GDMS server.

UCM supports GDMS passwordless remote access. When this button is checked, GDMS remote access UCM does not need to enter the account password, and no login is required.

Allow the administrator/super administrator to open it. After clicking on open with an account, the subsequent passwordless login will use the account. All administrators and super administrators can see whether this UCM is enabled.

Super administrators can check and uncheck all the exemption lists; administrators can check and uncheck the exemption status of this account, and the corresponding account exemption access function will be closed after cancellation.

Notes

- Deleting an account on GDMS only removes the association between the account and the device, and does not delete the SIP account information on UCM.
- Any creation, deletion or modification of the SIP account on UCM will be automatically synchronized to the GDMS cloud platform.
- After checking the “Media NAT traversal service”, the TURN service and other related traversal settings set by the user will not take effect.

Integrated Customer Service

To configure the Integrated Customer Service SDK, go to the **Other Features** → **UCM RemoteConnect** → **Integrated Customer Service SDK** page that allows users to download the SDK provided by the customer service system and integrate it on the website, so that the website can contact customer service for call operations. The call queue is used as the customer service number.

RemoteConnect

< Plan Plan Settings Integrated Customer Service Enterprise UI customiza >

WebRTC Trunks [Go to Page](#)

Enable Click2Call

Destination Extension

[Download](#)

© 2023 Grandstream Networks, Inc.

Integrated Customer Service interface

Enabling Click2Call will allow users to initiate a direct call from the web browser by clicking on the call button embedded on the website graphical interface. The calls initiated can be directed to call queues or a specific extension.

Enterprise UI Customization

With a remote connect plan, on the value-added service → UCM RemoteConnect → UI Customization page, users can edit the company name and select a local image file as the new logo. The company name acts on the text part with the trend logo, and the pictures are in different formats and sizes according to the logo position, which are 64*64px (only ico format is supported), 256*256px, 80*80px, which supports users in the “UCM management platform/login” “”, “Reset Password”, “Email Template”, “Wave_PC”, “Wave Login”, “Browser Label”, “Guide Page” interface preview.

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

Figure 244: UI Customization

Statistics

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

Figure 245: Concurrent Remote Calls

For more information, please visit <http://ucmrc.gdms.cloud/intro.html> and read our UCM63XXA RemoteConnect guides

GDMS Cloud Storage Space

GDMS Cloud Storage Space feature on the UCM630x offers an overview about how you are using the storage space offered by RemoteConnect. It displays the amount of storage occupied, the amount of free space, also the percentage taken by each type of files. The type of files displayed are the following: CDR Data, Backup Data, Recording Files, and IM Files.

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 **Other Features**→**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.

Table 121: 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, 3 rd 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". |

Table 122: 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.

Table 123: New API Supported Queries

| Queries Supported |
|--------------------------|
| getSystemStatus |
| getSystemGeneralStatus |
| listAccount |
| getSIPAccount |
| updateSIPAccount |
| listVoIPTrunk |
| addSIPTrunk |
| getSIPTrunk |
| updateSIPTrunk |
| deleteSIPTrunk |
| listOutboundRoute |
| addOutboundRoute |
| getOutboundRoute |
| updateOutboundRoute |
| deleteOutboundRoute |
| listInboundRoute |
| addInboundRoute |
| getInboundRoute |
| updateInboundRoute |
| deleteInboundRoute |
| playPromptByOrg |
| listBridgedChannels |
| listUnBridgedChannels |
| Hangup |
| callbargе |
| listQueue |
| getQueue |
| updateQueue |
| addQueue |
| deleteQueue |
| loginLogoffQueueAgent |
| pauseUnpauseQueueAgent |
| listPaginggroup |
| addPaginggroup |
| getPaginggroup |

| |
|------------------------------|
| updatePaginggroup |
| deletePaginggroup |
| MulticastPaging |
| MulticastPagingHangup |
| listIVR |
| addIVR |
| getIVR |
| updateIVR |
| deleteIVR |
| cdrapi |
| recapi |
| pmsapi |
| queueapi |
| getPinSets |
| addPinSets |
| updatePinSets |
| deletePinSets |
| cleanTerminalChatInformation |
| getSIPAccountQR |
| getCallQueuesMemberMessage |
| getQueueCalling |

Table 124: 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

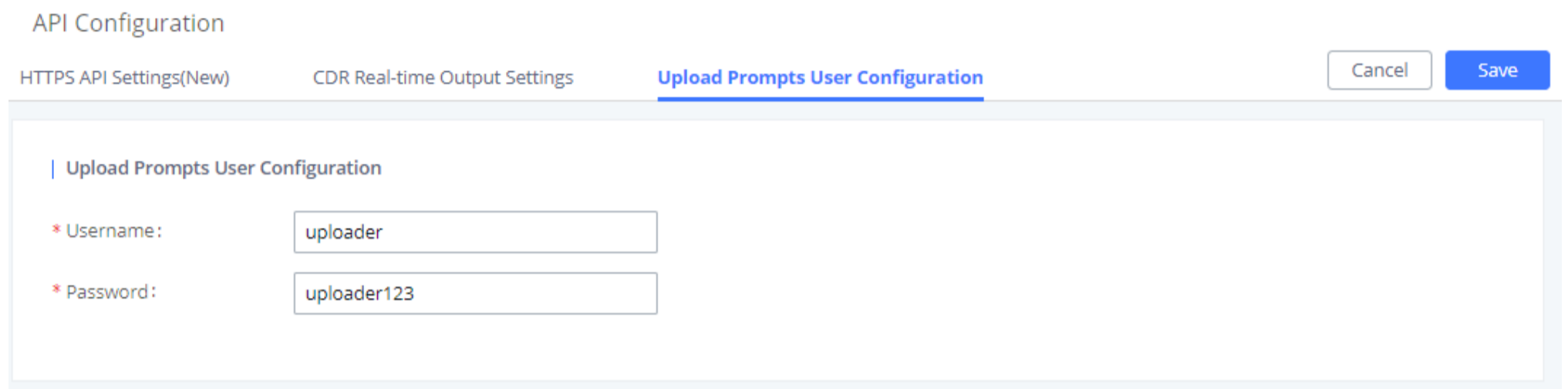
Customers now can use the “Upload Prompts User Configuration” to upload/replace voice prompt files as an alternative method to the manual upload method on **UCM PBX Settings** → **Voice Prompt** → **Custom Prompt**.

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



The screenshot shows a web interface for configuring the UCM. At the top, there are three tabs: 'HTTPS API Settings(New)', 'CDR Real-time Output Settings', and 'Upload Prompts User Configuration' (which is selected). To the right of the tabs are 'Cancel' and 'Save' buttons. Below the tabs, there is a section titled 'Upload Prompts User Configuration'. It contains two input fields: '* Username:' with the value 'uploader' and '* Password:' with the value 'uploader123'.

Figure 246: 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:



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=9191a6394c21b3abd779213c7179462&filename=test.mp3>

Note: If the File name on the HTTP/HTTPS request exists already on the UCM’s Custom voice prompts list the existing file will be overwritten by the new file downloaded from the FTP server.

CTI SERVER

UCM does support CTI server capabilities which are designed to be a part of the CTI solution suite provided by Grandstream, including GXP21XX and GXP17XX enterprise IP phones along with GS Affinity app.

Mainly the UCM will by default listening on port TCP 8888 for the connections from GS affinity application in order to interact, modify and serve data requests by the application which includes setting call features for the connected extension as call forward and DND.

Users can change the listening port under the menu page, Web GUI→**Other Features**→**CTI Server** as shown on below screenshot:

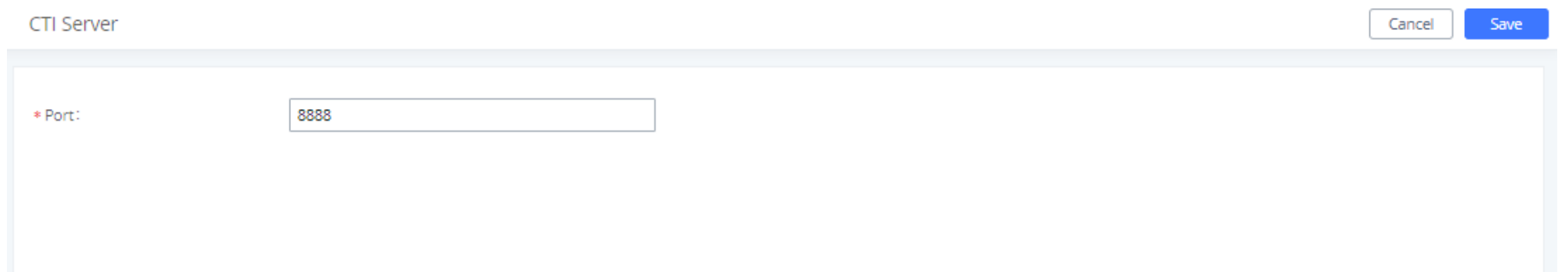


Figure 247: CTI Server Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link:

<https://documentation.grandstream.com/knowledge-base/gs-affinity-user-guide/>

ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)

The UCM630xA supports Asterisk Manager Interface (AMI) with restricted access. AMI allows a client program to connect to an Asterisk instance commands or read events over a TCP/IP stream. It is particularly useful when the system admin tries to track the state of a telephony client inside Asterisk.

User could configure AMI parameters on UCM630xA Web GUI→**Other Features**→**AMI**. For details on how to use AMI on UCM630xA, please refer to the following AMI guide:

<https://documentation.grandstream.com/knowledge-base/ami-asterisk-management-interface/>

Warning:

Please do not enable AMI on the UCM630xA if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM630xA system. Please be cautious when enabling AMI access on the UCM630xA and restrict the permission granted to the AMI user. By using AMI on UCM630xA you agree you understand and acknowledge the risks associated with this.

CRM INTEGRATION

Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers.

The UCM630xA support the following CRMs: SugarCRM, vTigerCRM, ZohoCRM, Salesforce CRM and ACT! CRM, which allows users to look for contact information in the Contacts, Leads and / or Accounts tables, shows the contact record in CRM page, and saves the call information in the contact's history.

Sugar CRM

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

CRM

CRM System:

* CRM Server Address:

* Add Unknown Number:



Contact Lookups:

| 1 item | Available | 2 items | Selected |
|--------------------------|---------------------------|--------------------------|---------------------------|
| <input type="checkbox"/> | Look up in Accounts table | <input type="checkbox"/> | Look up in Contacts table |
| <input type="checkbox"/> | | <input type="checkbox"/> | Look up in Leads table |

Figure 248: Sugar CRM Basic Settings

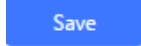
1. Select “Sugar CRM” from the CRM System Dropdown in order to use SugarCRM.

Table 125: Sugar CRM Settings

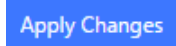
| | |
|---------------------------|--|
| CRM System | Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM. |
| CRM Server Address | Enter the IP address of the CRM server. |
| Add Unknown Number | Add the new number 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



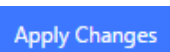
2. Logout from admin access.

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:

Figure 249: CRM User Settings

Vtiger CRM

Configuration page of the VtigerCRM can be accessed via admin login, on the UCM WebGUI→Other Features→CRM.

CRM

CRM System:

* CRM Server Address:

* Add Unknown Number:

Contact Lookups:

| <input type="checkbox"/> 0 item | Available | <input type="checkbox"/> 3 items | Selected |
|---------------------------------|-----------|----------------------------------|---------------------------|
| None | | <input type="checkbox"/> | Look up in Organizatio... |
| | | <input type="checkbox"/> | Look up in Leads table |
| | | <input type="checkbox"/> | Look up in Contacts ta... |

Figure 250: Vtiger CRM Basic Settings

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

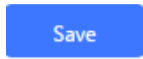
Table 126: Vtiger CRM Settings

| | |
|---------------------------|--|
| 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. |

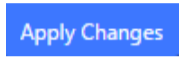
| | |
|------------------------|---|
| Contact Lookups | <p>Select from the “Available” list of lookups and press</p> <p><input type="radio"/></p> <p><input type="radio"/></p> <p>to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.</p> |
|------------------------|---|

Once settings on admin access are configured:

1. Click on



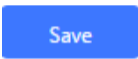
and



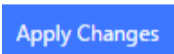
2. Logout from admin access.

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:

Figure 251: CRM User Settings

Zoho Telephony

Due to changes related to authenticating with ZohoCRM, Zoho’s CRM integration setup process has been updated. The *Other Features*→*CRM* page will appear as such when **Zoho Telephony** is selected.

CRM

CRM System: Zoho Telephony

CRM Server Region: United States

* Add Unknown Number:

Contact Lookups:

China

United States

Japan

India

Australia

European Union

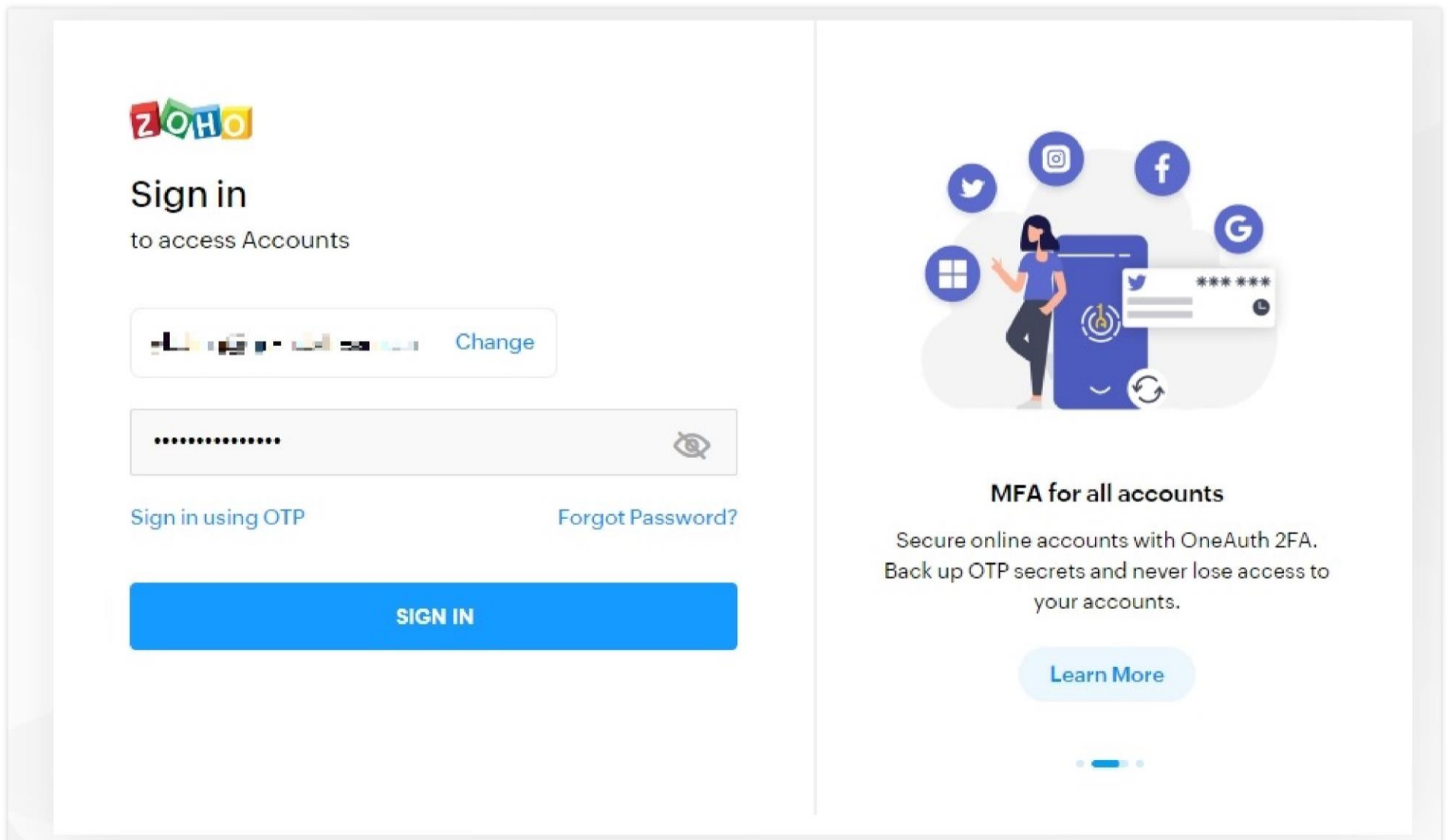
Once the desired settings have been configured, save and apply changes. Next, log into the User Portal and navigate to *Other Features*→*CRM User Settings*.

CRM User Settings

CRM Validation

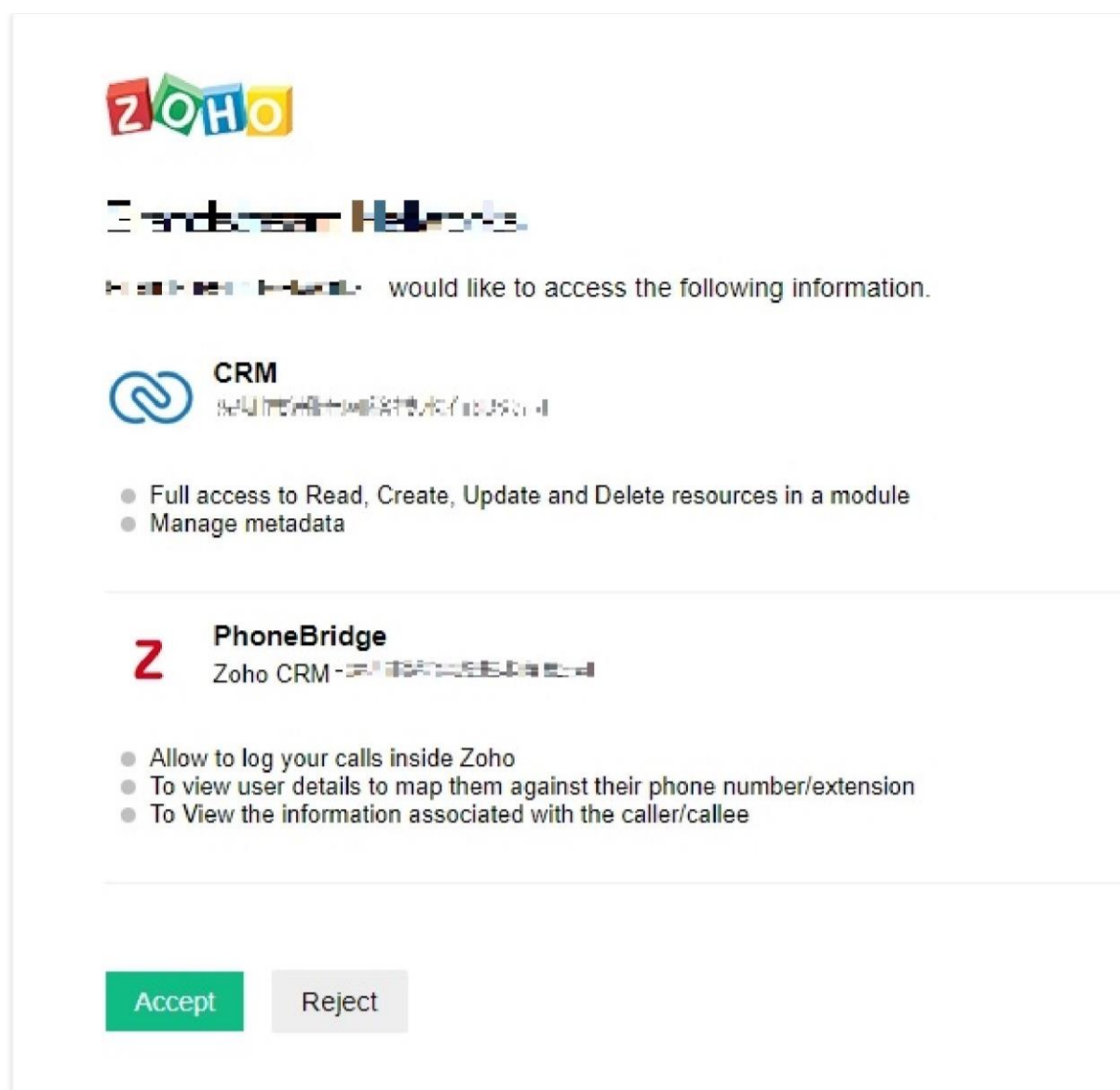
Login Status:

Click on the **CRM Validation** button, and the user will be redirected to the following page:

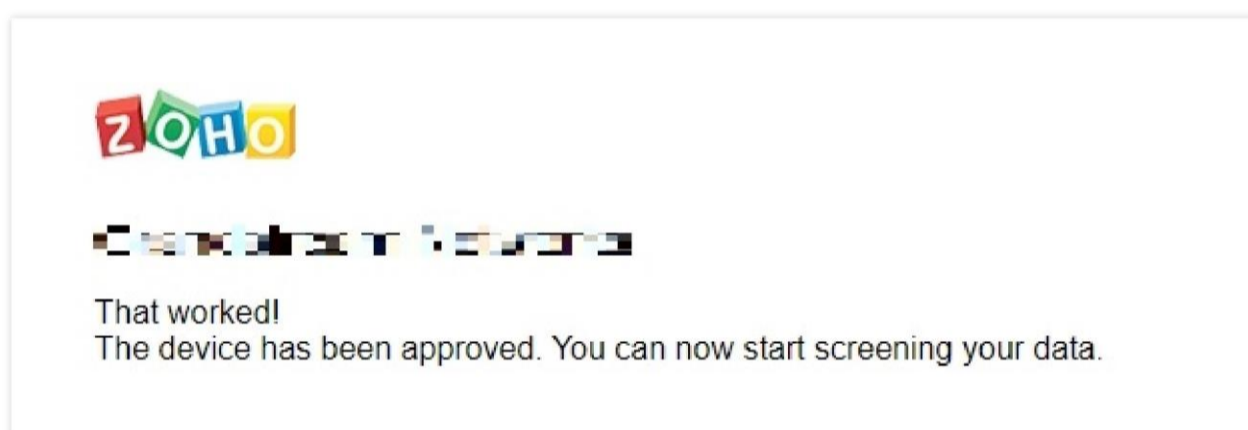


The image shows a Zoho sign-in page. On the left, there is a sign-in form with the Zoho logo, the text "Sign in to access Accounts", a phone number field with a "Change" link, a password field with a visibility toggle, and a "SIGN IN" button. Below the password field are links for "Sign in using OTP" and "Forgot Password?". On the right, there is a banner for "MFA for all accounts" featuring an illustration of a person with a smartphone and social media icons. The banner text reads: "Secure online accounts with OneAuth 2FA. Back up OTP secrets and never lose access to your accounts." Below the banner is a "Learn More" button.

Enter your CRM account details and log in.





Click on **Accept**.



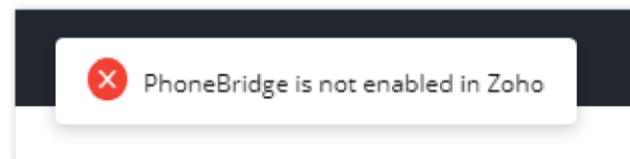
Return to the UCM User Portal page. The **CRM User Settings** page should now look like the following:

Users can then click on the **enable integrate** and **enable clicktodial** buttons to fully enable Zoho Telephony integration, which allows users to click on a call button next to contacts in the CRM Contacts page to initiate calls between UCM extensions and CRM contacts.

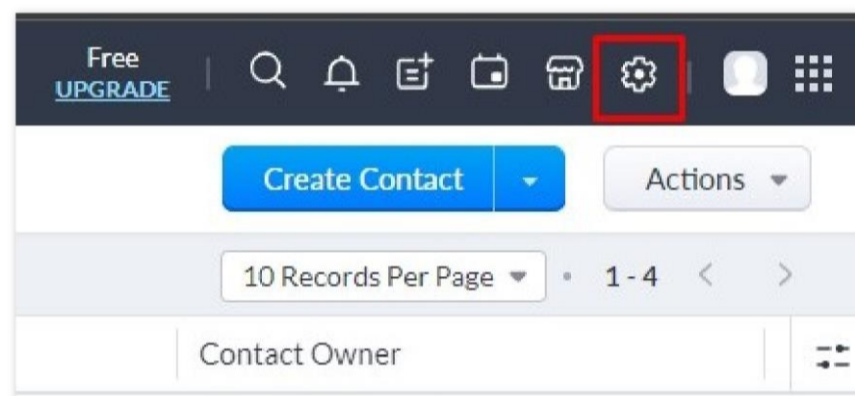
| Contact Name (Asc) | Unsort | 30 R |
|--------------------------|----------------------|--|
| <input type="checkbox"/> | Contact Name All ▾ ▲ | Phone |
| <input type="checkbox"/> | 1602015172 | [469] 781-5172  |
| <input type="checkbox"/> | 4702811172 | [469] 701-5172  |

Installing Zoho Phonebridge

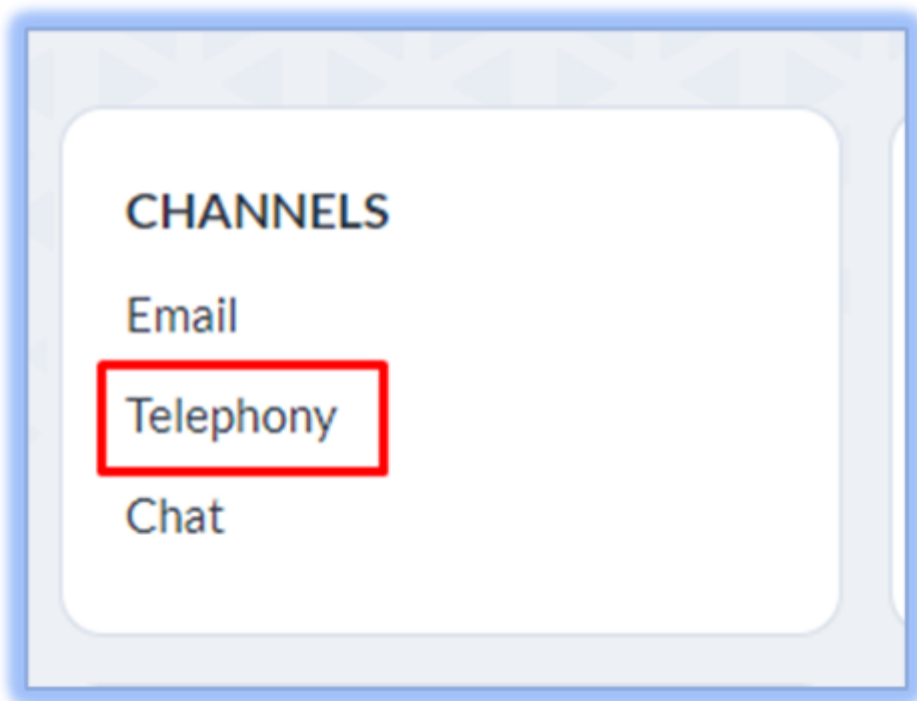
In the scenario where an error is received saying that Phonebridge has not been enabled, users may need to reinstall it.



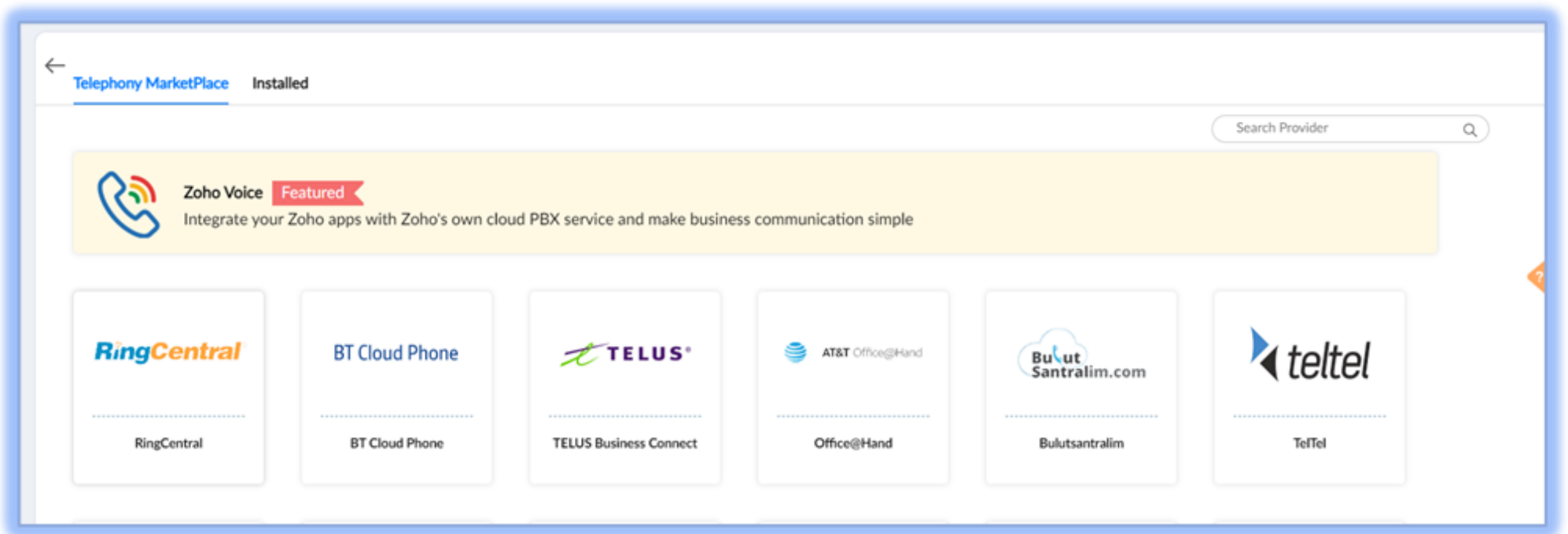
To do so, go to <https://crm.zoho.com/> click on the *Settings* icon in the top right corner of the Zoho CRM page.



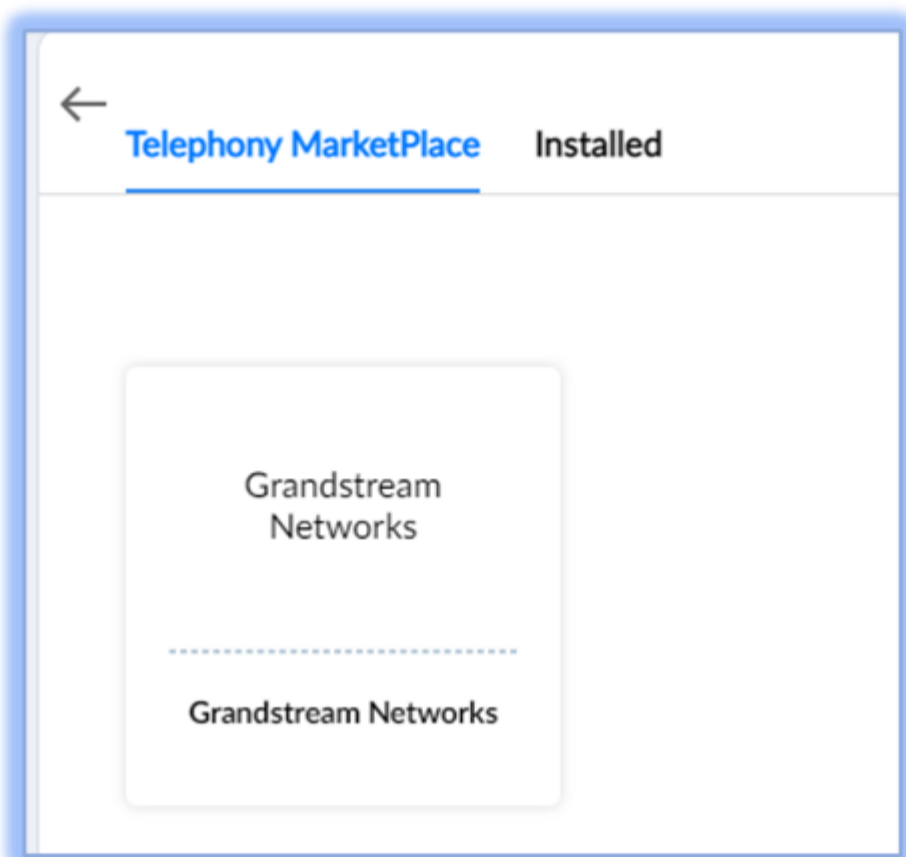
Under the *Channels* section, click on *Telephony*.



The following page will appear:



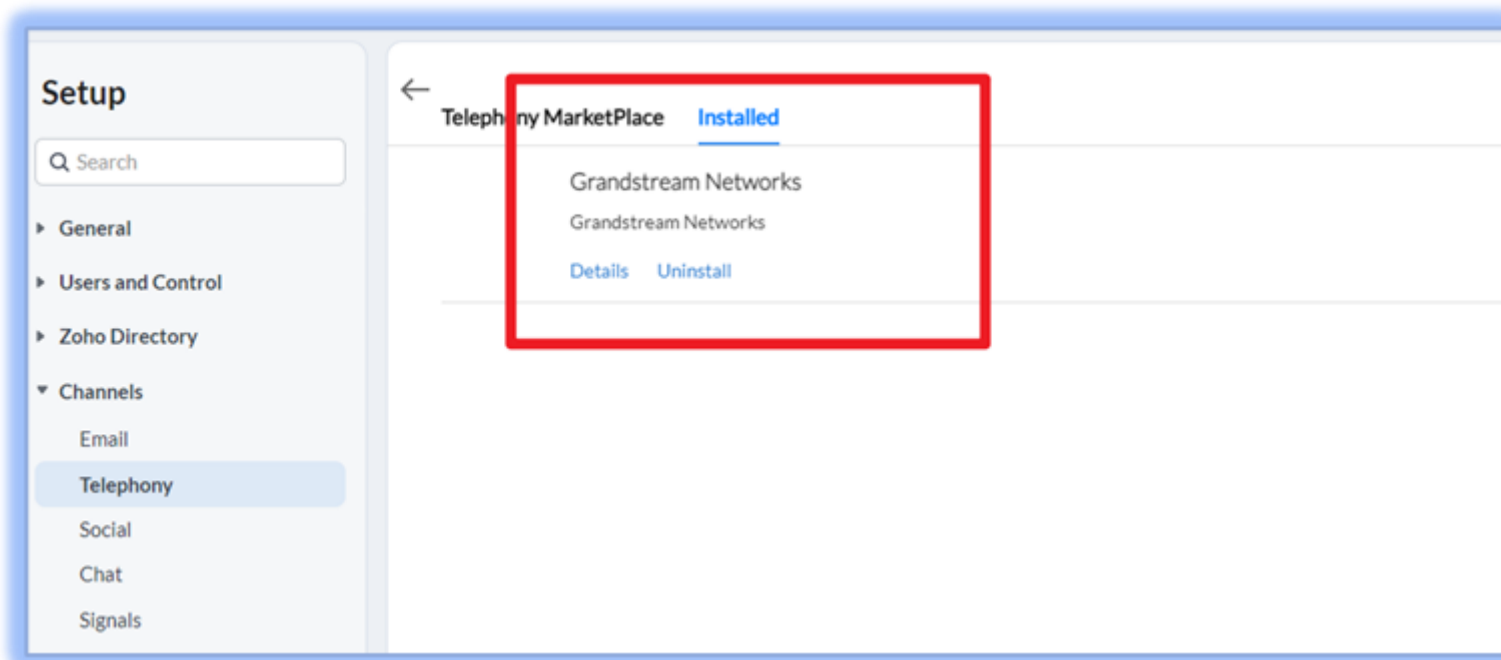
Click on the search bar in the top right and search for "Grandstream". The following entry should appear:



Click on it to see the following:



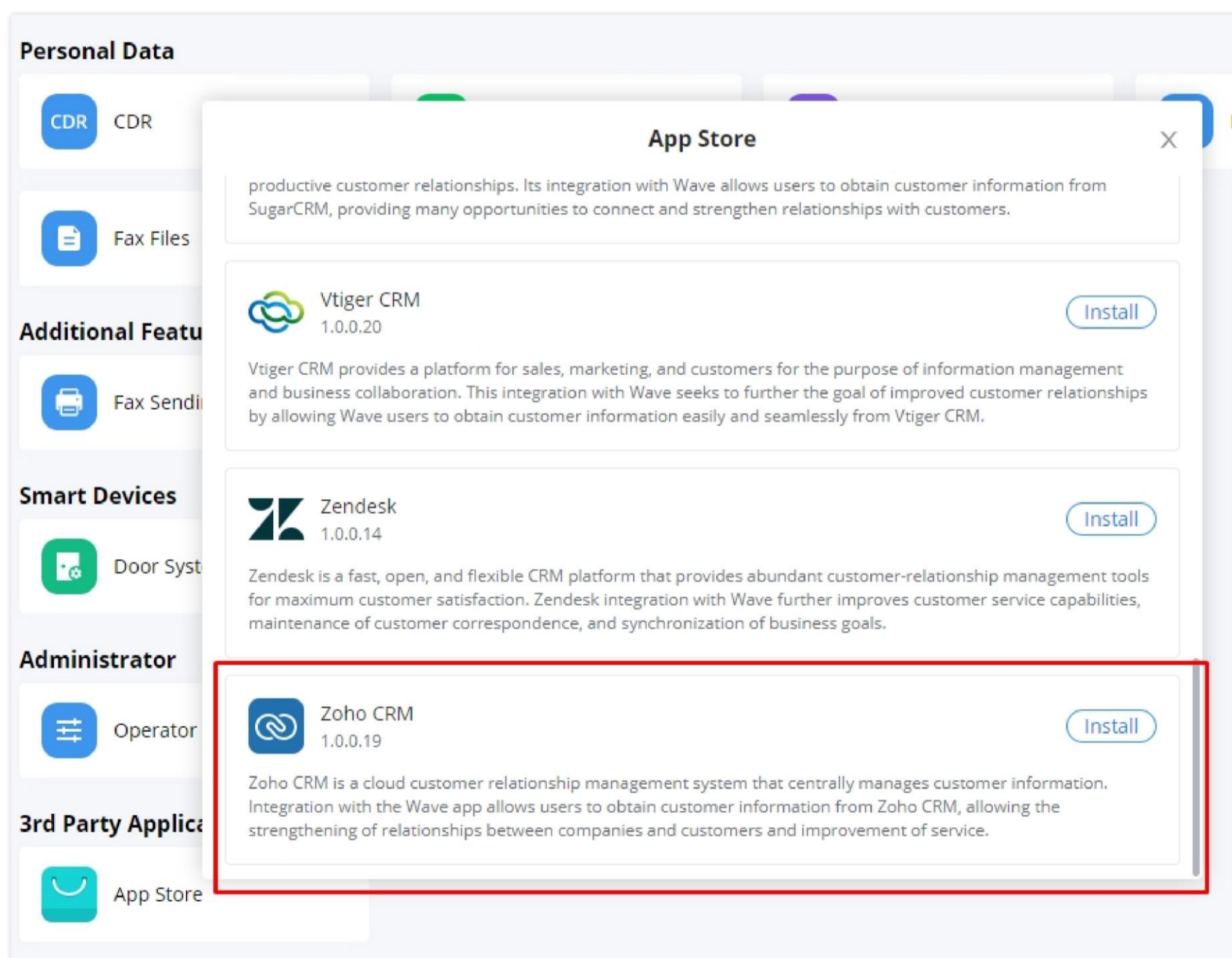
Finally, click on the green **Install** button.



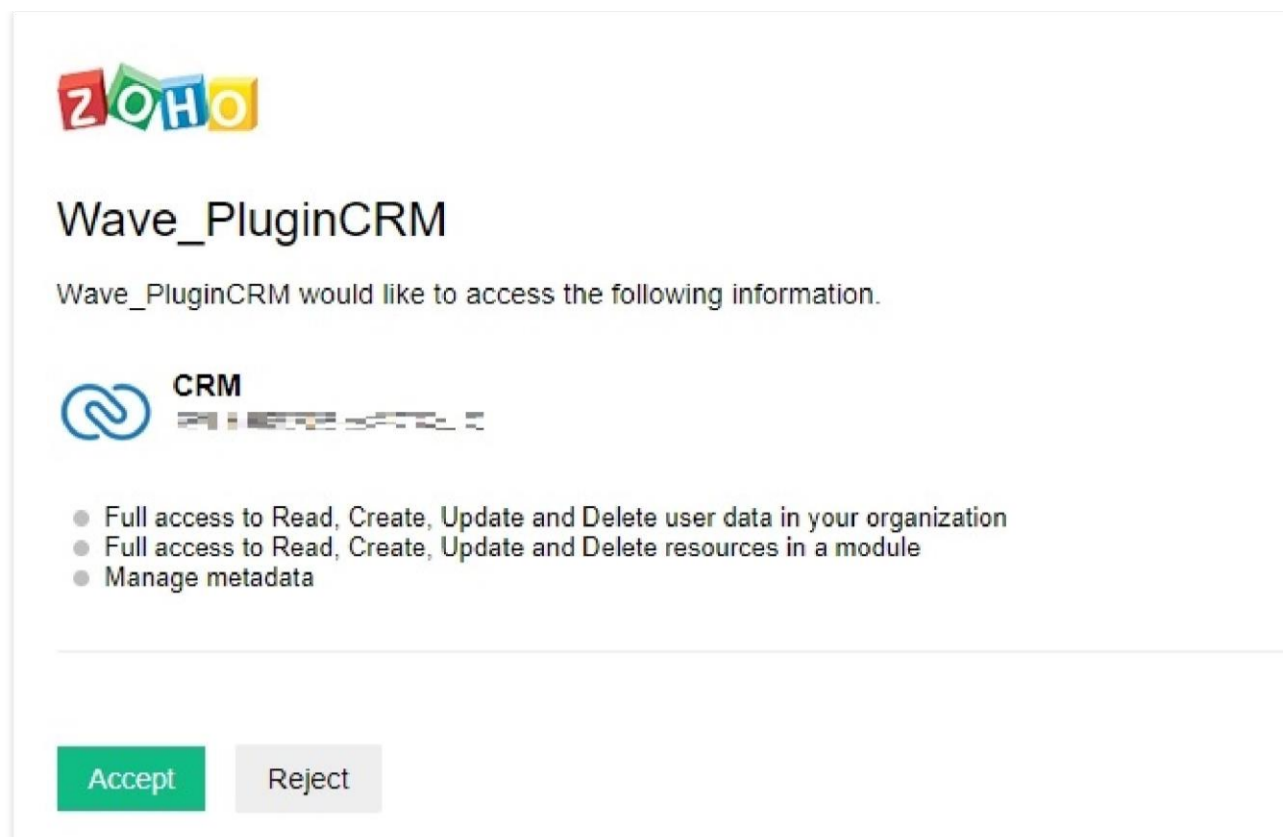
Zoho Telephony Phonebridge is now installed. Users can now go back to the UCM User Portal to enable the integration and click-to-dial.

Installing Zoho Wave Add-in as an Alternative

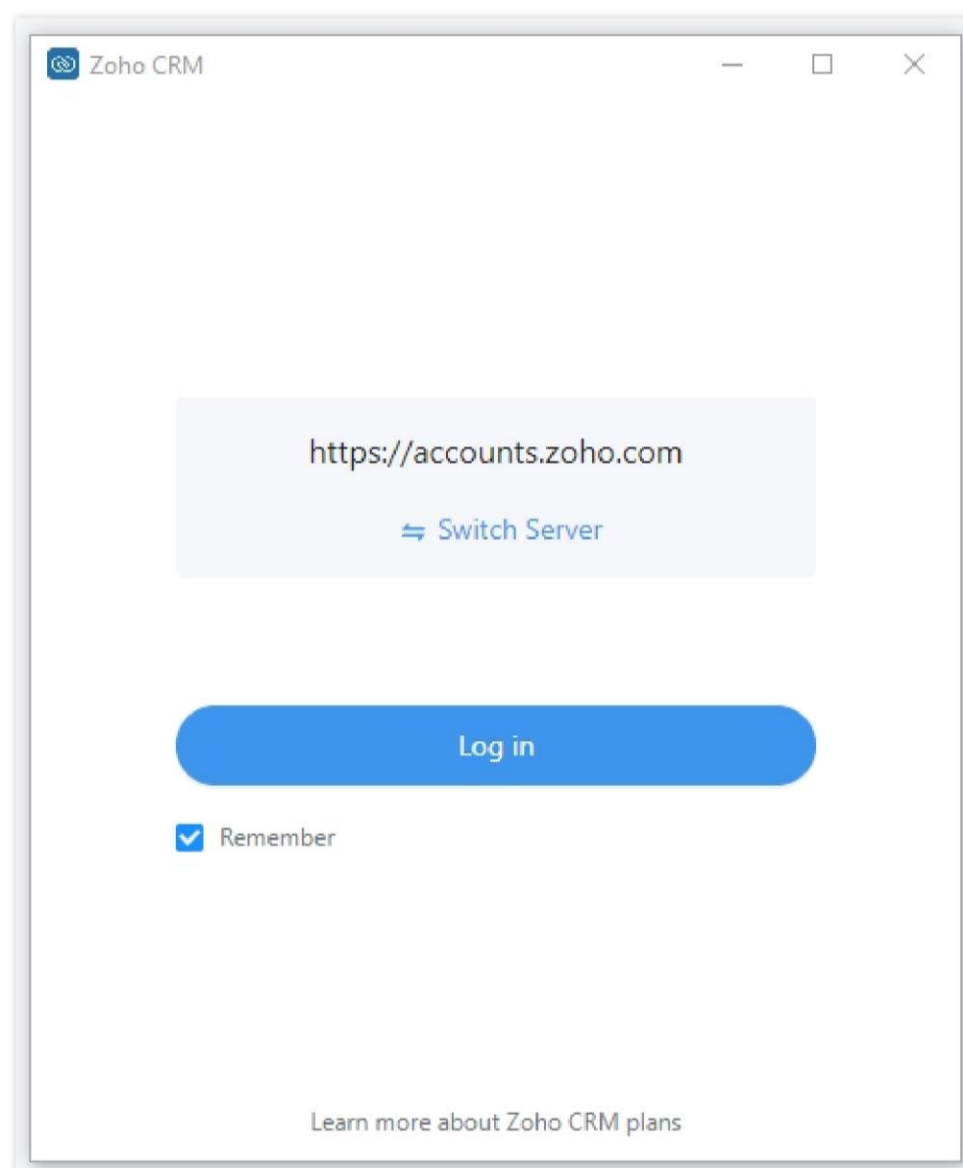
Wave Desktop supports the installation of an add-in that works with UCM's Zoho Telephony integration to provide convenient access to CRM contact information. This is redundant with setting up integration from the User Portal. If Wave is used, it would be best to set up Zoho integration using only this method instead of the steps mentioned above. The add-in can be installed from the Wave App Store.



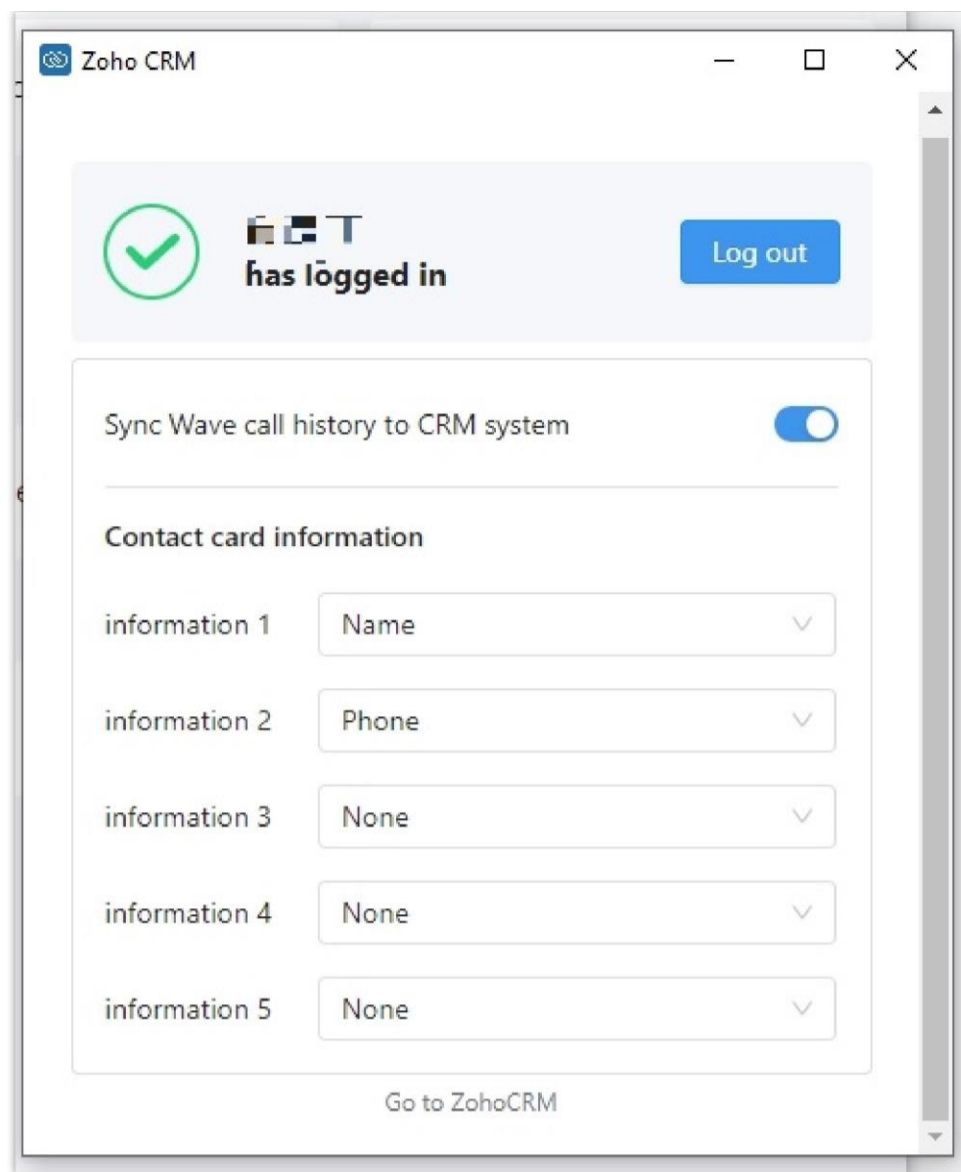
After selecting the desired server and clicking the **Identity Authorization** button, the following page will appear:



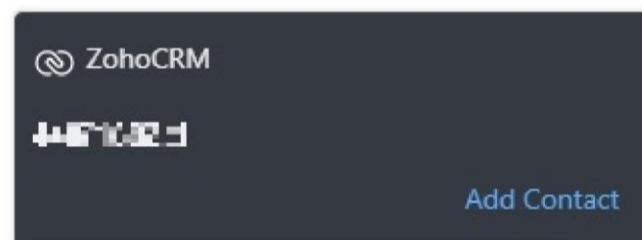
Click on **Accept**. The Wave authentication window should now change to this:



Click on the **Log In** button. The following will be displayed:



From here, users will be able to select the information they would like to see on call notification cards when receiving calls from CRM contacts. This information can be modified from the CRM portal.



If the caller is an unknown number, users can add it as a new contact into the CRM system. Clicking on the **Add Contact** button will redirect users to the Zoho CRM portal's **Create Contact** page, where users can manually fill in the contact information.

A screenshot of the 'Create Contact' form in Zoho CRM. The form has a title 'Create Contact' and a link 'Edit Page Layout'. At the top right are buttons for 'Cancel', 'Save and New', and 'Save'. Below the title is a 'Contact Image' section with a placeholder icon. The main section is 'Contact Information' and contains two columns of fields. The left column includes: 'Contact Owner' (a dropdown menu with '寅锡丁' selected), 'First Name' (a dropdown menu with '-None-' selected), 'Account Name' (a text field with a document icon), 'Email', 'Phone', 'Other Phone', 'Mobile', and 'Assistant'. The right column includes: 'Lead Source' (a dropdown menu with '-None-' selected), 'Last Name' (a text field), 'Vendor Name' (a text field with a document icon), 'Title', 'Department', 'Home Phone', 'Fax', and 'Date of Birth' (a text field with the format 'MMMD, YYYY').

Note: It seems like Wave cannot automatically fill in the phone number information of an unknown caller. However, if the UCM admin portal's CRM settings were configured to automatically add unknown numbers as contacts, then this step would be redundant as the contact would already be created upon receiving the call. The users would need to locate the newly created contact in the **Contacts** page and edit the contact information accordingly.

Salesforce CRM

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

The screenshot shows the 'CRM' configuration page. It includes a dropdown for 'CRM System' set to 'Salesforce', a dropdown for '* Add Unknown Number' set to 'Contacts', and a 'Contact Lookups' section with two columns: 'Available' and 'Selected'. The 'Available' column has one item, 'Look up in Leads table', and the 'Selected' column has two items, 'Look up in Contacts table' and 'Look up in Accounts table'. Navigation arrows are visible between the columns.

Figure 270: Salesforce Basic Settings

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

Table 129: Salesforce Settings

Once settings on admin access are configured:

2. Click on [button] and [button].
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 [button] and [button]. The status will change from "Logged Out" to "Logged In". User can start then using Salesforce CRM features.

The screenshot shows the 'CRM User Settings' page. It features a checked checkbox for 'Enable CRM', and three input fields: '* Username' with the value 'user@domain', '* Password' with the value 'pjdajlka123@!', and '* Security Token' with the value 'mkjhamjkhndfjkeFZEfljxwa!@jkjhbamklcel'. A 'Login Status' field is also present at the bottom.

Figure 271: Salesforce User Settings

Salesforce CRM

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

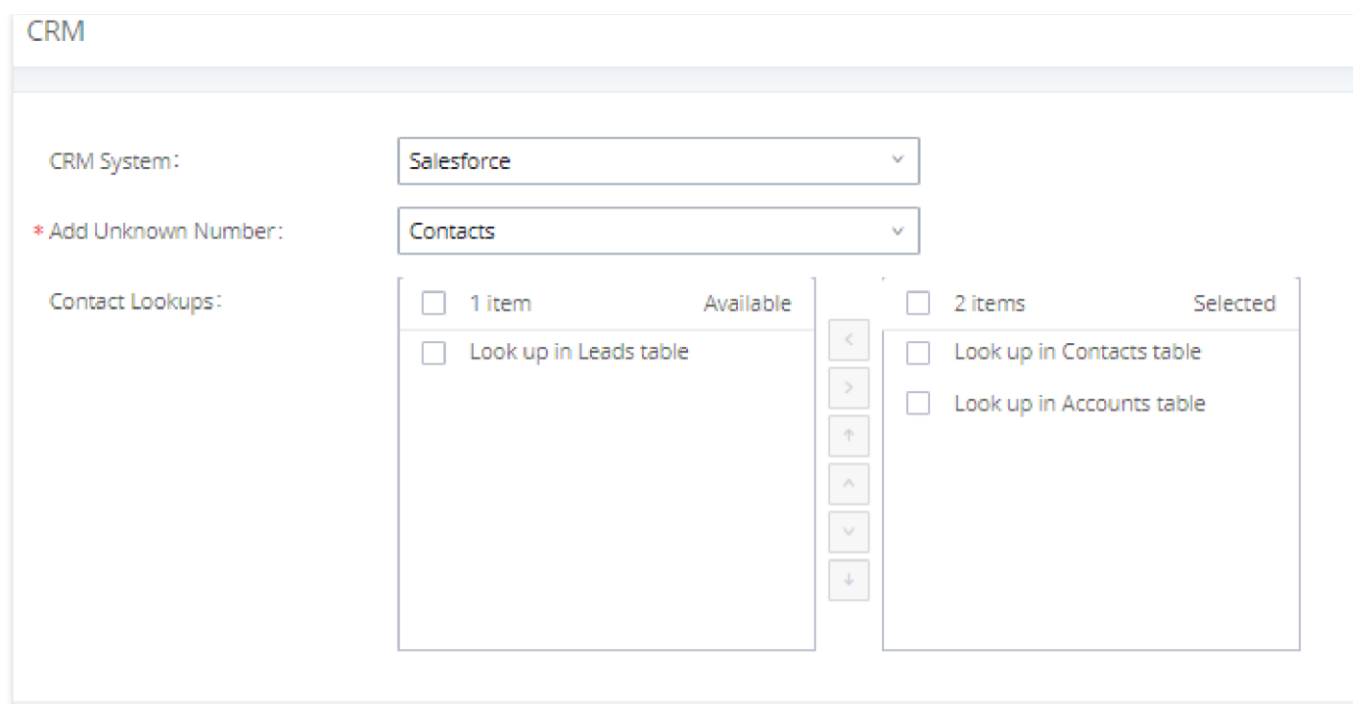


Figure 254: Salesforce Basic Settings

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

Table 128: Salesforce Settings

| | |
|---------------------------|---|
| CRM System | Select a CRM system from the dropdown menu, four CRM systems are available: SugarCRM, vTigerCRM, ZohoCRM (v1&v2), Salesforce and ACT! CRM. |
| Add Unknown Number | Add the new number to this module if it cannot be found in the selected module. |
| Contact Lookups | Select from the “ Available ” list of lookups and press to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts. |

Once settings on admin access are configured:

1. Click on

and

2. Logout from admin access.

3. Login to the UCM as user and navigate under “User Portal→Value-added Feature→CRM User Settings”.

Click on “**Enable CRM**” and enter the **username**, **password** and **Security Token** associated with the CRM account then click on

and

. The status will change from “Logged Out” to “Logged In”. User can start then using Salesforce CRM features.

CRM User Settings

Enable CRM:

* Username:

* Password:

* Security Token:

Login Status:

Figure 255: Salesforce User Settings

ACT! CRM

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

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

1. Navigate to Other Features→CRM and select the "ACT! CRM" option.

CRM

CRM System:

Figure 256: Enabling ACT! CRM

1. 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://mycloud.act.com/act/Help>

CRM User Settings

Enable CRM:

Username:

Password:

Login Status:

Figure 257: Enabling CRM on the User Portal

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

PMS INTEGRATION

UCM630xA supports Hotel Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI→**Other Features**→**PMS**.

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

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

Table 129: PMS Supported Features

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

HMobile PMS Connector

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

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

Grandstream UCM6XXX series have integrated HMobile Connect PMSI which supports a large variety of PMS software providing following hospitality features: Check-in, Check-out, set Room Status, Wake-up call and more.

The following figure illustrates the communication flow between the UCM and PMS software, which is done through a middleware system (HMobile Connect) acting as interface between both parties.

PMS Software

PMSI Middleware

(HMobile Connect)

Grandstream UCM

HSC PMS

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

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series have integrated HSC PMS providing following features:

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

Notes:

1. Added support for receiving HTTP GET keep-alive messages from HSC PMS. This will allow the PMS to be aware of its connection to the UCM and take the appropriate actions such as raising alarms, sending notifications, etc.
2. Added support for HTTP GET requests from HSC PMS to retrieve UCM extension information. UCM can provide the following information:
 - extension – UCM extension number
 - name – extension display name / CID name
 - mwi – MWI state
 - permission – permission level of the extension
 - 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.

1. Added HTTPS support

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

HSC PMS Software

Grandstream UCM

Figure 259: UCM & HSC PMS interaction

Mitel PMS

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

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series have integrated Mitel PMS providing following hospitality features: Check-in, Check-out, set Room Status, Wake-up call and more.

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

Mitel PMS Software

Grandstream UCM

Figure 260: UCM & Mitel PMS interaction

IDS PMS

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

- PMS (Property Management System)
- PBX

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

IDS PMS Software

Grandstream UCM

Figure 261: UCM & IDS PMS interaction

PMS API

The PMS API allows users to use their own middleware to work with PMS systems instead of currently supported integrations.

Additionally, this API allows access to read and modify certain UCM parameters that current supported PMS integrations cannot. To use this, users must first enable and configure the HTTPS API settings.

For more details, please refer to online <https://documentation.grandstream.com/knowledge-base/https-api/>, Pmsapi section.

Connecting to PMS

On the UCM WebGUI→**Other Features**→**PMS**→**Basic Settings**” set the connection information for the PMS platform.

Table 130: PMS Basic Settings

| Field | Description |
|---|--|
| PMS Module | Users can select the desired PMS module from the drop-down list. <ul style="list-style-type: none">• Hmobile• Mitel• HSC• IDS• PMS API |
| 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 |
| Username | This username is used to authenticate into the PMS API. |
| Password | This password is used to authenticate into the PMS API. |
| Back Up Voicemail Recordings | Back up voicemail recordings to external storage after check-out. |
| Automatically Clear Wakeup Calls | Scheduled wakeup calls for rooms can be cleared upon checking in or checking out. <ul style="list-style-type: none">• 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. |

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

- Update PMS Room Status
- PMS Wake Up Service

PMS Features

Room Management

In Room Management tab, the user can create a room and affect up to two extensions to it. This will appear in Room Status tab, and from there the user can change the Check-in/Check-out

Call Privileges allows the administrator to set the level of call privilege of the room.

Room Status

Figure 278: Check-in a Client

After clicking “OK” the client entry will be added to the list.

The user can click on **Check-in/Check-out Records** to view the history of the checked-in and checked-out guests.

Note

The Call Privilege configured during a guest’s check-in will be reset to the room’s default call privilege upon guest check-out.

Wake Up Service

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

Figure 265: Create New Wake Up Service

Table 131: PMS Wake up Service

| Field | Description |
|----------------------|---|
| Room Number | Select the room number where to call with a limitation of 63 characters. |
| Select Time | Set the time of the wakeup call |
| Action Status | <p>Show the status of the call:</p> <ul style="list-style-type: none"> ◦ Programmed: the call is scheduled for the time set ◦ Cancelled: the call is canceled ◦ Executed: the wakeup call is made <p>Note: Editing an already executed wakeup service will automatically change the service’s status to “Programmed”.</p> |
| Type | <ul style="list-style-type: none"> ◦ Single: The call will be made once on the specific time. ◦ Daily: The call will be repeated every day on the specific time |

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

| ROOM NUMBER | ACTION STATUS | TYPE | ANSWER STATUS | DATE | TIME | OPTIONS |
|-------------|---------------|--------|---------------|------------|-------|---------|
| 1000 | Programmed | Single | No action | 2019-12-12 | 08:00 | |

Figure 266: Wakeup Call executed

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

Mini Bar

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

Figure 267: Create New Mini Bar

Table 132: Create New Mini Bar

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

In order to create a new maid, click on

under UCM WebGUI→**Other Features**→**PMS**→**Maid**.

Figure 268: Create New Maid

Table 133: Create New Maid

| | |
|------------------|--|
| Maid Code | Enter the Code to use when the maid wants to use the Mini Bar. |
|------------------|--|

| | |
|-----------------|--|
| Password | Enter the password associated with the maid. |
|-----------------|--|

In order to create a new consumer goods, click on

under UCM WebGUI→**Other Features**→**PMS**→**Mini Bar**, the following window will popup.

Create New Consumer Goods

* Code:

* Name:

Figure 269: Create New Consumer Goods



| | |
|-------------|-----------------------------|
| Code | Enter the Goods Code. |
| Name | Enter the Name of the Goods |

The Minibar page displays as:

PMS

Basic Settings Room Status Wakeup Service **Mini Bar** Maid

+ Add Mini Bar

| CODE | NAME | OPTIONS |
|------|---------|---|
| 4000 | MiniBar |   |

+ Add Consumer Goods



| CODE ↕ | NAME ↕ | OPTIONS |
|--------|--------|---|
| 1000 | cola |   |

Figure 270: Mini Bar

Local PMS

UCM6300 series offer a local Property Management System to give the user basic management features without having to purchase a PMS for the most basic property management actions. In addition to Room Management, Rooms Status for checking-in and checking-out, Wakeup Service, Mini Bar, and Maid functions, the UCM6300 allows a number of additional functions upon checking-out, like backing up voicemail recordings, clearing wakeup calls and Wave history automatically, in addition to resetting Wave's password. The user can use the Local PMS feature to check-in and check-out clients from the web user interface.

PMS

Basic Settings Room Management Room Status Wakeup Service Mini Bar

Cancel Save

PMS Module: Local PMS

Wakeup Prompt: Wake Call Upload Audio File

Back Up Voicemail Recordings:

Automatically Clear Wakeup Calls: None

Automatically Clear Wave Chat History: None

Automatically Reset User/Wave Password:

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

WAKEUP SERVICE

The Wake Up service can be used to schedule a reminder or wake up calls to any valid destination. This service is available on the 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→**Other Features**→**Wakeup Service**, click on "Add" to create a new wakeup service. The following window will pop up.

Create New Wakeup Service

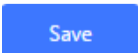
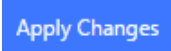
The screenshot shows a web form for creating a new wakeup service. The 'Enable Wakeup Service' checkbox is checked. The 'Name' field contains 'GS_Wakeup'. The 'Prompt' dropdown is set to 'wakeup-call'. The 'Custom Date' checkbox is unchecked. The 'Date' field shows '2017-08-11' and the 'Time' field shows '14:00'. The 'Members' section has two panes: 'Available' with 3 items (1002, 1003, 1004) and 'Selected' with 2 items (1000, 1001).

Figure 271: Create New Wakeup Service

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

Table 134: Wakeup Service

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

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.

Table 135: Max Wakeup Members

| UCM Model | Max members in a Wakeup Service |
|-----------|---------------------------------|
| UCM6300A | 50 |
| UCM6302A | 100 |
| UCM6304A | 150 |
| UCM6308A | 200 |

Wake Up Service from User Portal

1. Login to the user portal on the UCM630xA.
2. Wake Up service can be found under “**Other Features**→**Wakeup Service**”, click on ”Add” to create a new wakeup service.
3. Configures the Name, Prompt, Date and Time for the user to make the wakeup to.
4. Click

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 “**Call Features**→**Feature Codes**”.

The screenshot shows a list of feature codes in the UCM WebGUI. On the left, there are four entries: '* Listen Spy:' with code '*54', '* Barge Spy:' with code '*56', '* PMS Wakeup Servi...' with code '*35' and a checkmark, and '* Presence Status:' with code '*48' and a checkmark. On the right, there are three entries: '* Whisper Spy:' with code '*55', '* Wakeup Service:' with code '*36' and a checkmark (highlighted with a red box), and '* Update PMS Room...' with code '*23' and a checkmark.

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.

ANNOUNCEMENTS CENTER

The UCM630xA supports Announcements 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.

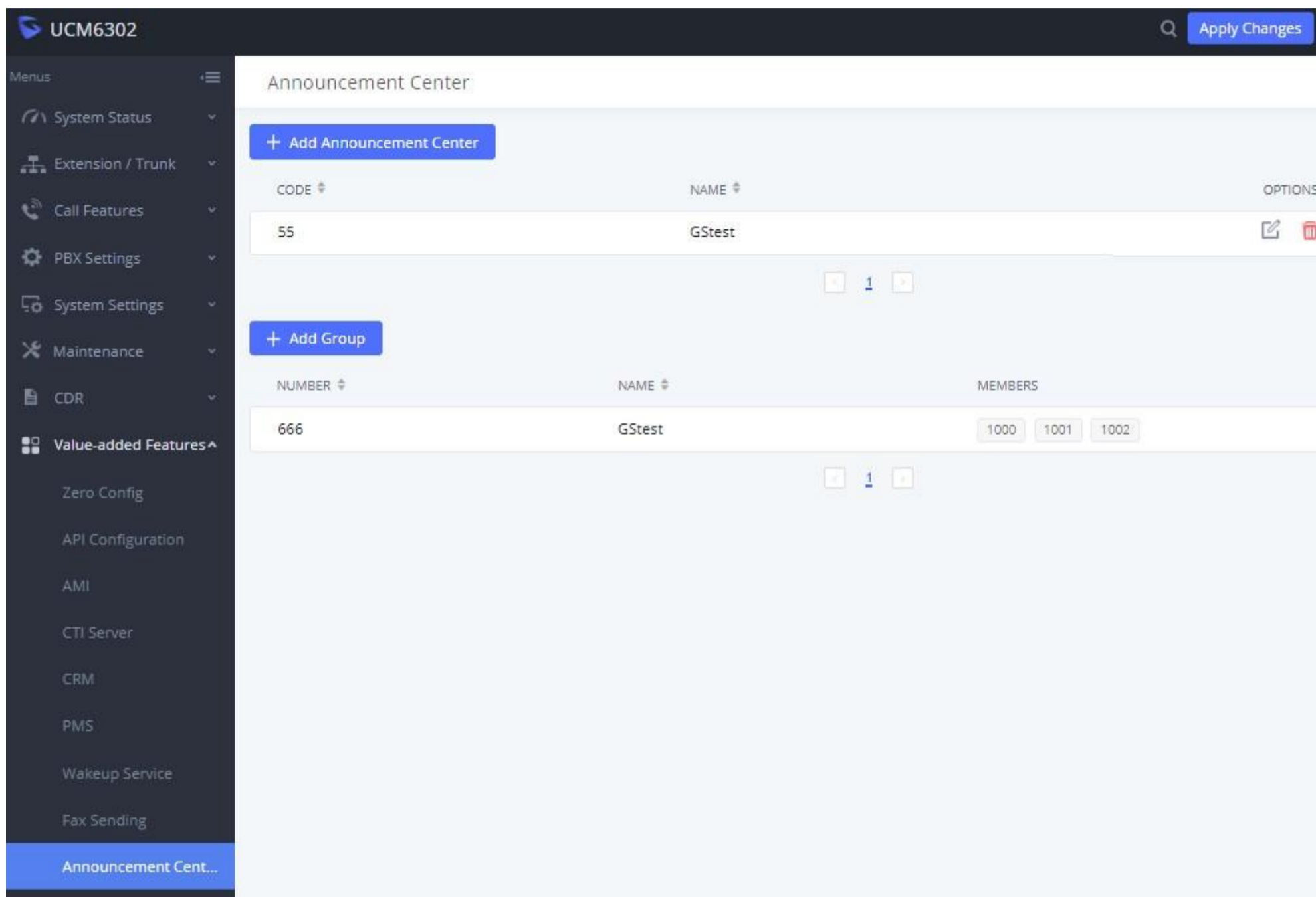


Figure 272: Announcements Center

Announcements Center Settings

Table 136: Announcements Center Settings

| | |
|----------------------|--|
| Name | Configure a name for the newly created Announcements Center to identify this announcement center. |
| Code | <p>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.</p> <p>Note:</p> <p>The combination number must not conflict with any number in the system such as extension number or meeting number.</p> |
| Custom Prompt | <p>This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page 'Custom Prompt'. Click 'Prompt' to add additional record.</p> |

| | |
|---------------------|--|
| Ring Timeout | Configure the ring timeout for the group members. The default value is 30 seconds. |
| Auto Answer | If set to Yes the Auto answer will be enabled by the members. |

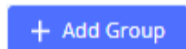
Group Settings

Table 137: 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 meeting number and cannot exceed 64 characters. |
| Members | Select the group members from the available list. |

Announcements Center feature can be found under Web GUI→**Other Features**→**Announcements Center**. The following example demonstrates the usage of this feature.

1. Click



to add new group.

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

Create New Group

* Name:

* Number:

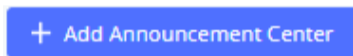
Members:

| <input type="checkbox"/> 27 items Available | <input type="checkbox"/> 3 items Selected |
|---|---|
| <input type="checkbox"/> 1003 | <input type="checkbox"/> 1000 |
| <input type="checkbox"/> 1004 | <input type="checkbox"/> 1001 |
| <input type="checkbox"/> 1005 | <input type="checkbox"/> 1002 |
| <input type="checkbox"/> 1006 | |
| <input type="checkbox"/> 1007 | |

Figure 273: Announcements Center Group Configuration

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

1. Click



to create a new Announcement Center.

2. Give a name to the newly created Announcement Center.

3. Specify the code which will be used with group number to send the voice message to.

4. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click “Prompt” link and follow the instructions in that page.

Create New Announcement Center

* Name:

* Code:

* Custom Prompt:

* Ring Timeout:



* Auto Answer:

Figure 274: Announcements Center Code Configuration

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the 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 v Goto 1

+ Add Group

| NUMBER ↕ | NAME ↕ | MEMBERS | OPTIONS |
|----------|--------|--------------------|---|
| 666 | GStest | 1000 1001 1002 |   |

< 1 >

Total: 1 10 / page v Goto 1

Figure 275: Announcements Center Example

QUEUE METRICS

The Queue Metrics docking tool provides an interface for UCM system and QM docking. Pass the UCM call queue report to QM in a richer form. Queue Metrics 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.

Enable QueueMetrics

Integration:

* QueueMetrics URL:

* Username:

* Webqloader Password:

Partition:

Figure 276: Queue Metrics

Table 138: Queue Metrics configuration parameters

| | |
|----------------------------|---|
| Enable QueueMetrics | Disabled by default. |
| Integration | |
| QueueMetrics URL | Enter the URL of the QueueMetrics on-premise server you have installed. (i.e. http://xxx.xxx.xxx.xxx:8080/queuemetrics .) Note: Under normal circumstances, the user is a webqloader type user of Queue Metrics. You must ensure that the user is enabled, otherwise the connection will fail. |
| username | Configure the username |
| Webqloader Password | Configure the user password. |
| Partition | Configure the data storage partition identifier. |

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.

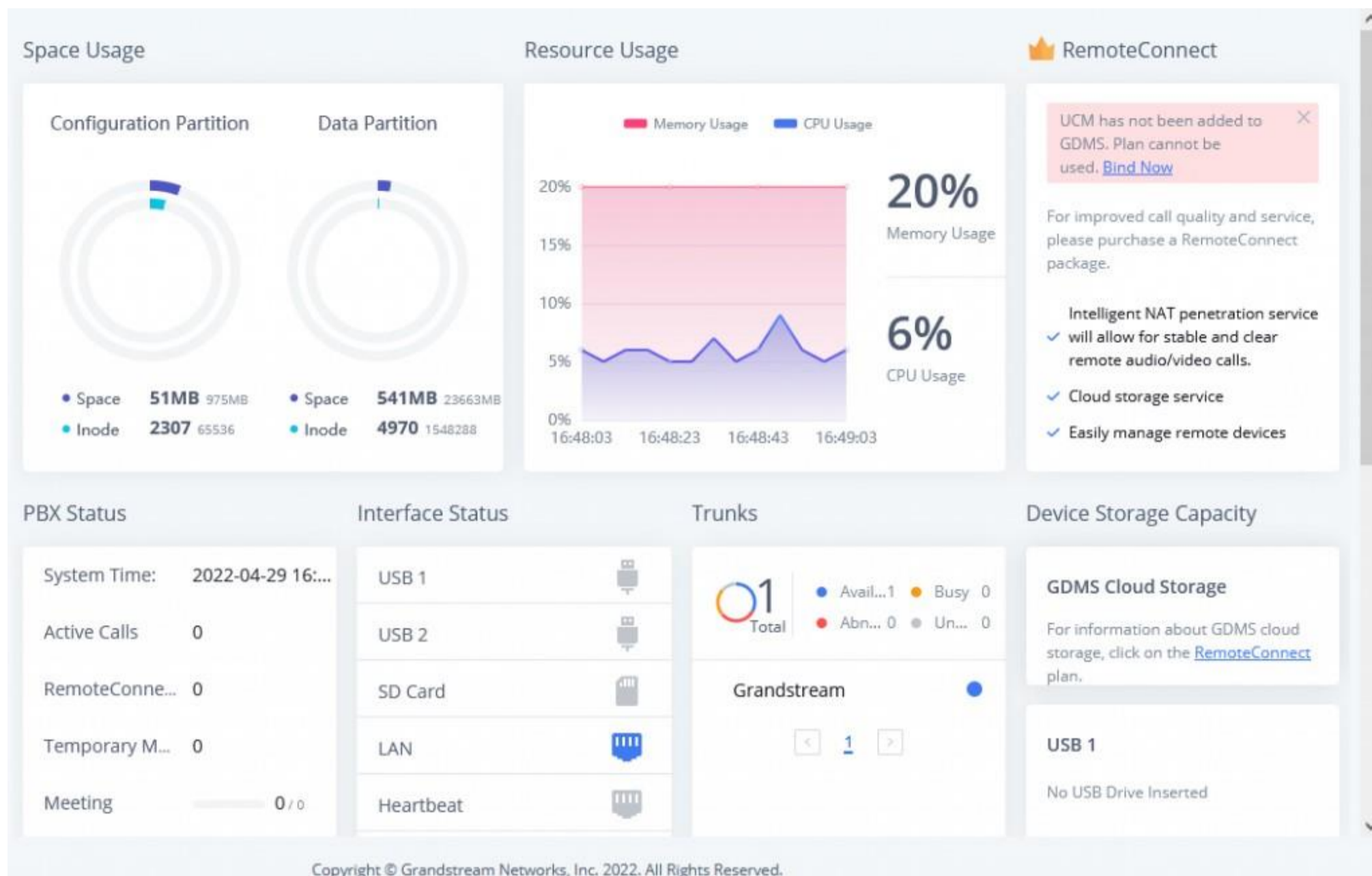


Figure 277: Status→PBX Status

Trunks

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

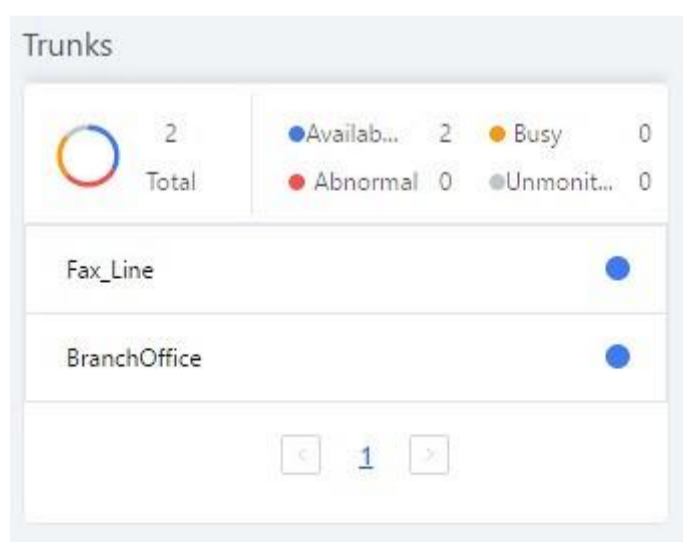


Figure 278: Trunk Status

Table 139: Trunk Status

| | |
|-------------------------|--|
| Status | <p>Display trunk status.</p> <ul style="list-style-type: none"> ◦ Analog trunk status: <p>Available</p> <p>Busy</p> <p>Unavailable</p> <p>Unknown Error</p> <ul style="list-style-type: none"> ◦ SIP Peer trunk status: <p>Unreachable: The hostname cannot be reached.</p> <p>Unmonitored: Heartbeat feature is not turned on to be monitored.</p> <p>Reachable: The hostname can be reached.</p> <ul style="list-style-type: none"> ◦ SIP Register trunk status: <p>Registered</p> <p>Unrecognized Trunk</p> |
| Trunks | Display trunk name |
| Type | <p>Display trunk Type:</p> <ul style="list-style-type: none"> ◦ Analog ◦ SIP ◦ IAX |
| Username | Display username for this trunk. |
| Port/Hostname/IP | Display Port for analog trunk, or Hostname/IP for VoIP (SIP/IAX) trunk. |

Extensions

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

| <input type="checkbox"/> STATUS | PRESENCE STA... | EXTENSION | NAME | TYPE | IP AND PORT | EMAIL... | OPTIONS |
|--|-----------------|-----------|------|-------------|---------------------|----------|---------|
| <input type="checkbox"/> ● Ringing | Available | 1000 | | SIP(WebRTC) | 192.168.5.199:5070 | | |
| <input type="checkbox"/> ● Unavailable | Available | 1001 | | SIP(WebRTC) | -- | | |
| <input type="checkbox"/> ● In Use | Available | 5555 | | SIP(WebRTC) | 192.168.5.199:63827 | | |

Figure 279: Extension Status

Table 140: Extension Status

| | |
|------------------------|--|
| Status | <p>Display extension number (including feature code). The color indicator has the following definitions.</p> <ul style="list-style-type: none"> ○ 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 | <p>Display Email Notification status for the extension.</p> <p>When notification is waiting for be sent, shows</p> <p>and once sent it will display</p> |
| Terminal Type | <p>Displays extension type.</p> <ul style="list-style-type: none"> ○ SIP User ○ IAX User ○ Analog User ○ Ring Groups ○ Voicemail Groups |

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.

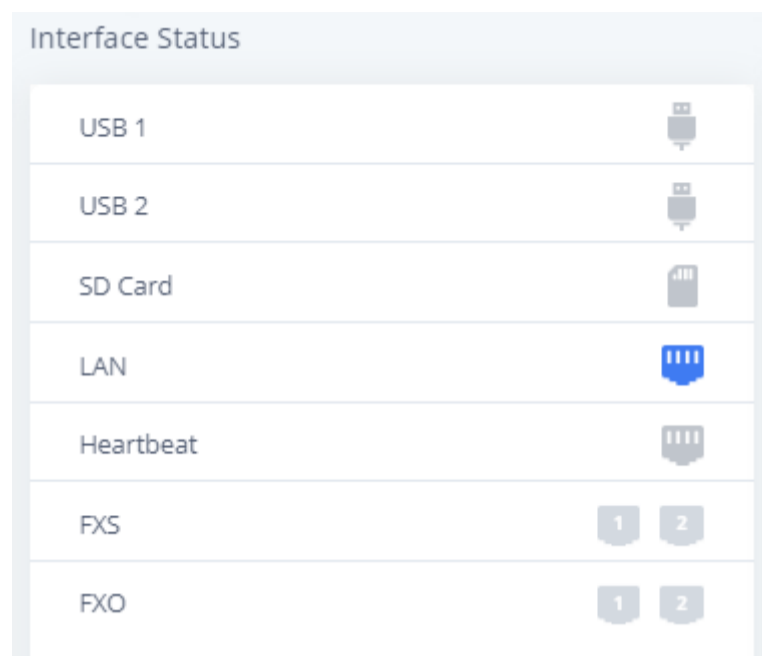


Figure 280: UCM6304A Interfaces Status

Table 141: Interface Status Indicators

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

System Status

The 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.

Table 142: System Status→General

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

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.

Table 143: System Status→Network

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

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.

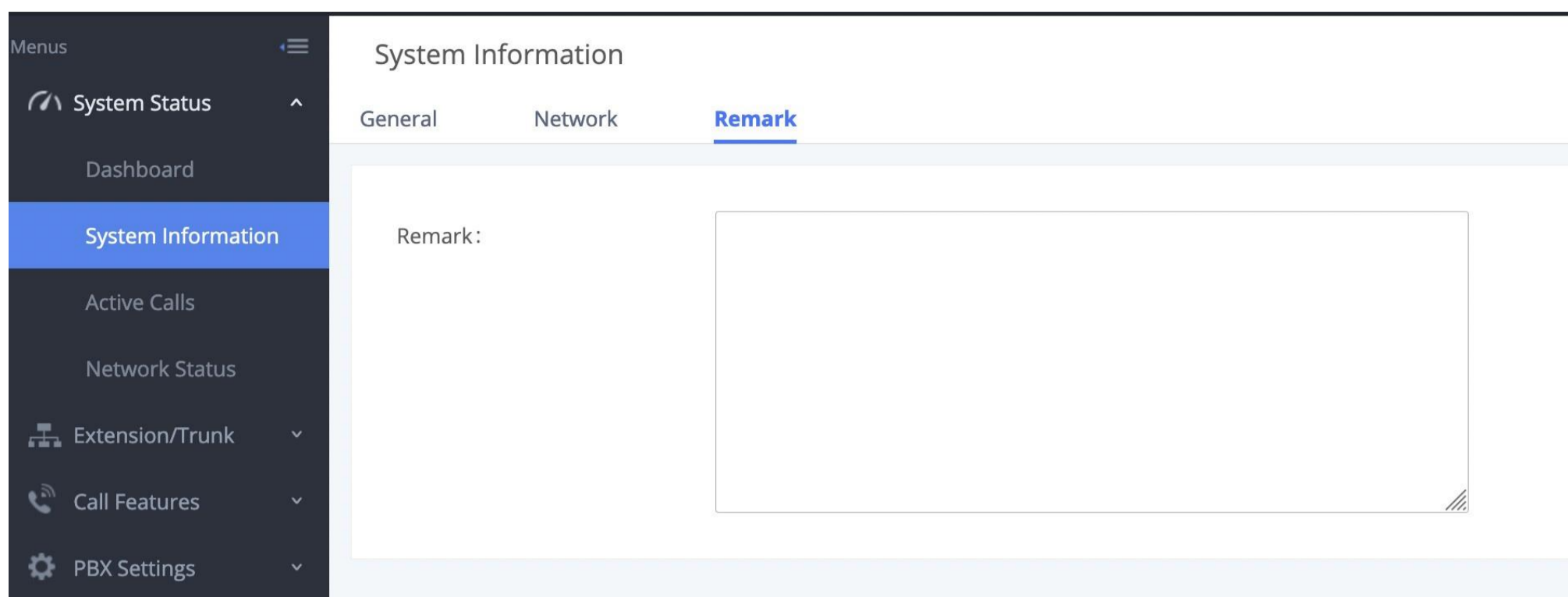


Figure 281: System Status → System Information → Remark

Storage Usage

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

Space Usage includes:

- **Configuration partition**

This partition contains PBX system configuration files and service configuration files.

- **Data partition**

Voicemail, recording files, IVR file, Music on Hold files etc.

- **USB disk**

USB disk will display if connected.

- **SD Card**

SD Card will display if connected.

Inode Usage includes:

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

Note:

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

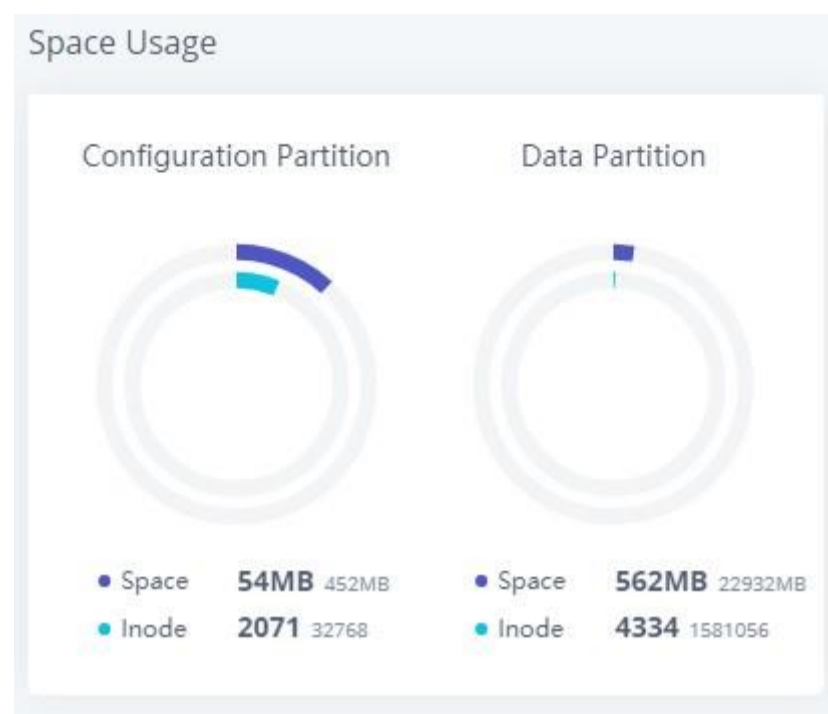


Figure 282: System Status→Storage Usage

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.

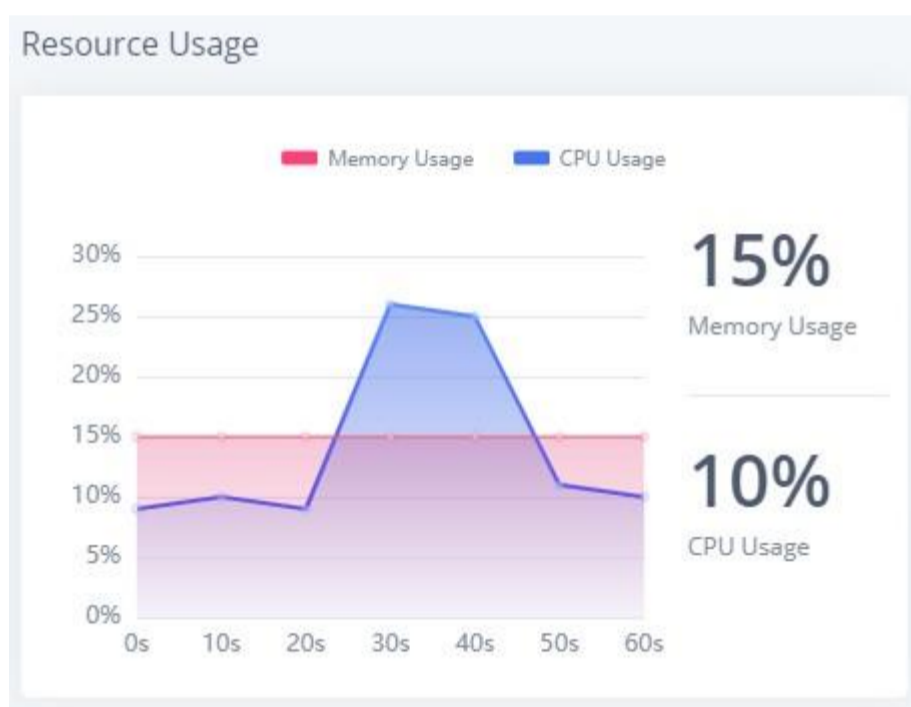


Figure 283: System Status→Resource Usage

System Events

The UCM630xA can monitor important system events, log the alerts, and send Email notifications to the system administrator.

Alert Events List

The system alert events list can be found under Web GUI → **Maintenance** → **System Events**. The following event and their actions are currently supported on the UCM630xA which will have alert and/or Email generated if occurred:

Figure 284: Alert Event List

Table 144: Alert Events

| Alert Events |
|-----------------------|
| Fail2ban Blocking |
| Flood Attacks |
| Network Traffic Storm |
| User Login Banned |
| Remote Login |
| User Login Success |
| User Login Failed |
| System Crash |
| Restore Config |
| System Update |
| System Reboot |
| TLS Cert Expiration |

| |
|---|
| HA Failure Warning |
| Cloud IM Abnormal |
| Modify Super Admin Password |
| Data Sync Backup |
| Local Disk Usage |
| External Disk Usage |
| Extended Disk Status |
| Emergency Calls |
| SIP Outgoing Call through Trunk Failure |
| SIP Internal Call Failure |
| Remote Concurrent Calls |
| Excessive Outbound Calls |
| Long Outbound Call Duration |
| Trunk Outbound Call Duration Usage |
| Trunk Concurrent Calls |
| Register SIP trunk failed |
| SIP Peer Trunk Status |
| Register SIP failed |
| SIP Lost Registration |

Note: For users who have purchased a GDMS package, once the option **Alert Events Sync** is enabled under **RemoteConnect**, the triggered events will be pushed to their GDMS platform.

<https://documentation.grandstream.com/knowledge-base/ucm-remoteconnect-user-guide/>

Click on



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

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

2. **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 it will be pushed to the GDMS.
3. **Network Traffic Storm:** An alert will be generated in case there is an excessive amount of packets on the LAN. Network Traffic Storms consume the resources of the network components and saturate the bandwidth, which will bring the whole network to a halt. This event will be registered in events log and a notification will be pushed to the GDMS.
4. **User login banned:** If user login is blocked, the event will be recorded in the alert log.
5. **Remote Login:**
6. **System Crash:**

Alert Settings: System Crash



* Detect Cycle: minute... ▾

Figure 285: System Events → Alert Events Lists: System Crash

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

Click on the switch



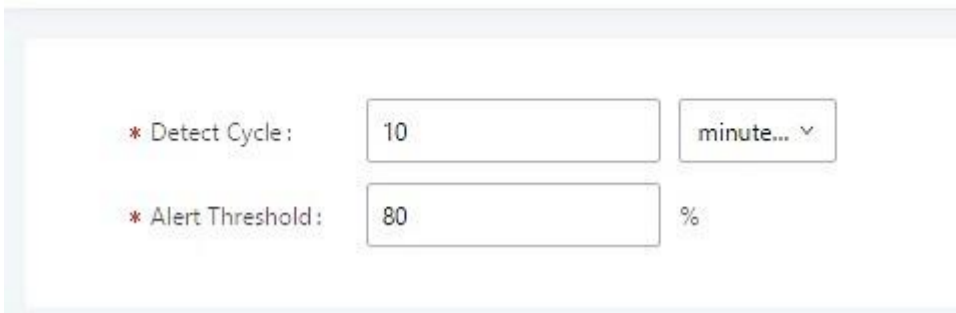
to turn on/off the alert and Email notification for the event. Users could also select the checkbox for each event and then click on button “Alert On”, “Alert Off”, “Email Notification On”, “Email Notification Off” to control the alert and Email notification configuration.

7. **Restore Config:** Once the system configuration is restored, the configuration restoration event will be recorded in the alert log.
8. **System Update:** Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
9. **System Reboot:** UCM will detect the system restart and will send an alert for it. There are two kinds of reboots that the UCM detects, normal and abnormal reboots. Normal reboots are the reboots that are done when you press the restart button on the web UI, reboot that occur after updating the firmware, HA backup reboot etc... Abnormal reboots are the reboots that occur due to a system failure. Normal reboots are registered in the alert log and they are not pushed to GDMS, while abnormal reboots are registered in the alert list and are pushed to GDMS.
10. **TLS Cert Expiration:** Starting 7 days before the HTTP Server TLS certificate in the UCM device expires, an expiration countdown notification is sent every day; the certificate has expired, an expiration notification is sent; after the alarm notification is generated, a valid new certificate is uploaded, and a notification to restore the TLS certificate is generated.
11. **HA failure warning:** After the HA dual-system hot backup disaster recovery function is enabled in the UCM device, the HA fault alarm is automatically turned on. When the device has a software and hardware related fault, an HA fault alarm is generated.
12. **Cloud IM Abnormal:** An alert message will be generated if the Cloud IM encounter any issue or exhibit any abnormal behavior.
13. **Modify Super Admin Password:** Once the super administrator password is modified, the system will record the password modification event in the alarm log.

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

15. **Disk Usage :**

Alert Settings: Disk Usage



The screenshot shows the 'Alert Settings: Disk Usage' configuration page. It contains two rows of settings. The first row is labeled '* Detect Cycle:' and has a text input field containing the number '10' and a dropdown menu currently set to 'minute...'. The second row is labeled '* Alert Threshold:' and has a text input field containing the number '80' followed by a '%' symbol.

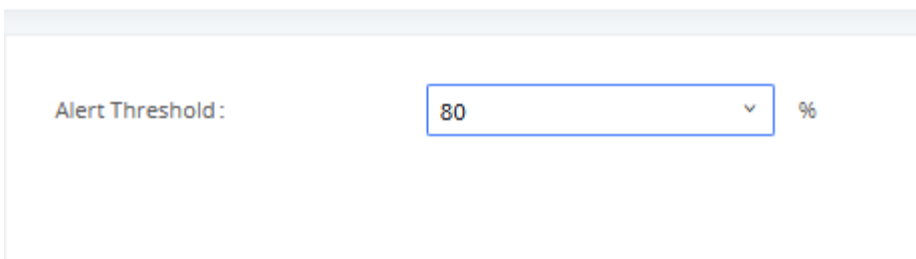
Figure 286: System Events→Alert Events Lists: Disk Usage

- **Detect Cycle:** The UCM630xA will perform the internal disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM630xA system will send the alert.

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

16. **Memory Usage**

Alert Settings: Memory Usage



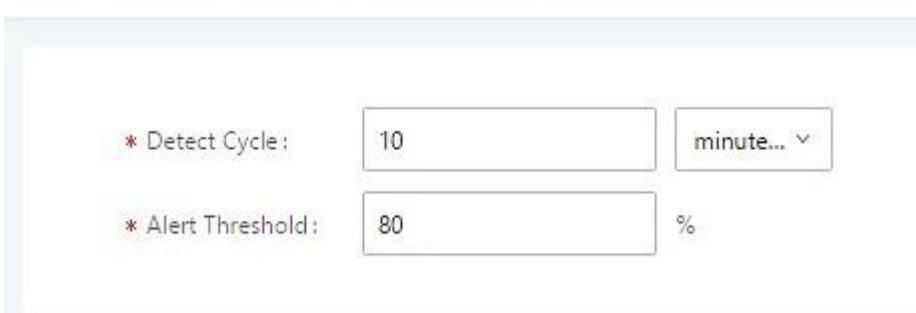
The screenshot shows the 'Alert Settings: Memory Usage' configuration page. It contains one row of settings labeled 'Alert Threshold:' with a dropdown menu currently set to '80' followed by a '%' symbol.

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

- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM630xA system will send the alert.

17. **External Disk Usage**

Alert Settings: External Disk Usage



The screenshot shows the 'Alert Settings: External Disk Usage' configuration page. It contains two rows of settings. The first row is labeled '* Detect Cycle:' and has a text input field containing the number '10' and a dropdown menu currently set to 'minute...'. The second row is labeled '* Alert Threshold:' and has a text input field containing the number '80' followed by a '%' symbol.

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

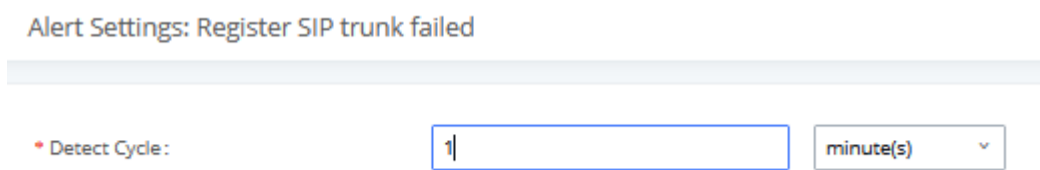
- **Detect Cycle:** The UCM630xA will perform the External disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM630xA system will send the alert.

18. **External disk status:** If the external disk of the system is Connected/Disconnected, the event will be recorded in the alarm log.

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

20. **Emergency Calls:** If the system generates an emergency call, the event will be recorded in the alert log.

21. Register SIP trunk failed



The screenshot shows the configuration page for 'Alert Settings: Register SIP trunk failed'. It features a light blue header bar with the title. Below the header, there is a label 'Detect Cycle:' followed by a text input field containing the number '1' and a dropdown menu currently set to 'minute(s)'.

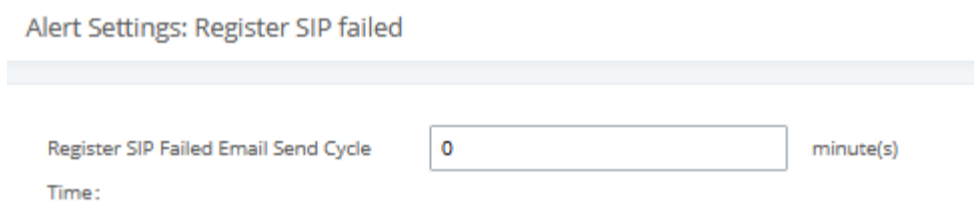
Figure 289: System Events → Alert Events Lists: Register SIP Trunk Failed

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

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

23. **SIP Outgoing Call through Trunk Failure:** If the system SIP trunk outgoing call fails, the event will be recorded in the alert log.

24. Register SIP failed



The screenshot shows the configuration page for 'Alert Settings: Register SIP failed'. It features a light blue header bar with the title. Below the header, there is a label 'Register SIP Failed Email Send Cycle' followed by a text input field containing the number '0' and a dropdown menu currently set to 'minute(s)'. Below this, there is a label 'Time:'.

Figure 290: System Events → Alert Events Lists: Register SIP Failed

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

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

26. **SIP Internal Call Failure:** If the system SIP extension call fails within the office, the event will be recorded in the alert log.

27. **High Frequency Outgoing Call:** When an extension initiates calls frequently, an alert will be logged in the alert log and a notification will be pushed to the GDMS and through email as well.

28. **Remote concurrent calls:** If the remote concurrent call fails, the event will be recorded in the alert log.

29. **Trunk Outbound Call Duration Usage:**

30. **Trunk Concurrent calls:** When the system detects that the number of concurrent calls of a certain relay exceeds the threshold set by the relay within a certain period of time, the event will be recorded in the alarm log. Calls are not restricted if the threshold is exceeded.

31. **User login success:** Successful user login events will be recorded in the alert log.

32. **User login failed:** User login failure events will be recorded in the alert log.

33. **Data Sync Backup:** If the system performs data synchronization and backup abnormalities, the event will be recorded in the alert log.

Alert Log

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

| TIME | EVENT NAME | TYPE | CONTENT |
|---------------------|-------------------|----------------|--|
| 2019-12-11 23:04:56 | User login failed | Generate Alert | Logged in system failed! The username is: admin, IP:41.250.198.175 |

Figure 291: System Events→Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on

. Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.
2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

User could filter out alert logs of “Generate Alert” or “Restore to Normal” by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of “Restore to Normal”.

Start Time: 2020-11-03 00:00

End Time: 2020-11-10 14:31

Event Name: All

Type: All

Reset Filter

Figure 292: Filter for Alert Log

Alert Contact

This feature allows the administrator to be notified when one of the Alert events mentioned above happens. Users could add administrator’s Email address under Web GUI→**Maintenance**→**System Events**→**Alert Contact** to send the alert notification to an email (Up to 10 Email addresses can be added) or also specify an HTTP server where to send this alert.

Table 145: Alert Contact

| | |
|------------------------------|--|
| Super Admin Email | <p>Configure the email addresses to send alert notifications to.</p> <p>Up to 10 email addresses can be added.</p> |
| Admin Email | <p>Configure the email addresses to send alert notifications to.</p> <p>Up to 10 email addresses can be added.</p> |
| Email Template | Please refer to section Email Templates |
| Protocol | <p>Protocol used to communicate with the server. HTTP or HTTPS.</p> <p>Default one is HTTP.</p> |
| HTTP Server | The IP address or FQDN of the HTTP/HTTPS server. |
| HTTP Server Port | HTTP/HTTPS port |
| Warning Template | <p>Customize the template used for system warnings.</p> <p>By default: <code>{"action": "\${ACTION}", "mac": "\${MAC}", "content": "\${WARNING_MSG}"}</code></p> |
| Notification Template | <p>Customize the notification template to receive relevant alert information.</p> <p>By default:</p> <pre><code>{"action": "\${ACTION}", "cpu": "\${CPU_USED}", "memory": "\${MEM_USED}", "disk": "\${DISK_USED}", "external_disk": "\${EXTERNAL_DISK_USED}"}</code></pre> <p>Note: <i>The notification message with “action:0” will be sent periodically if Notification Interval is set.</i></p> |
| Notification Interval | <p>Modifies the frequency at which notifications are sent in seconds.</p> <p>No notifications will be sent if the value is “0”. Default value: 20</p> |

| | |
|--|--|
| Template Variables | <i>\${MAC}</i> : MAC Address |
| | <i>\${WARNING_MSG}</i> : Warning message |
| | <i>\${TIME}</i> : Current System Time |
| | <i>\${CPU_USED}</i> : CPU Usage |
| | <i>\${MEM_USED}</i> : Memory Usage |
| | <i>\${ACTION}</i> : Message Type. Refer to [Table 144: Alert Events] |
| | <i>\${DISK_USED}</i> : Disk Usage |
| <i>\${EXTERNAL_DISK_USED}</i> : Disk Usage | |

CDR

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

On the 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.

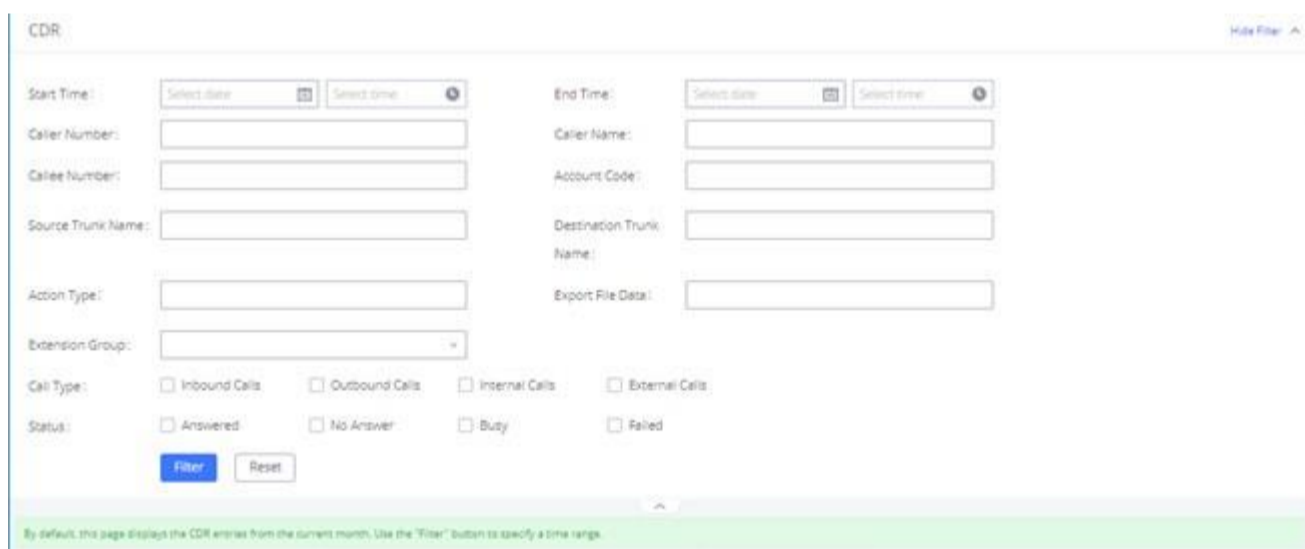


Figure 293: CDR Filter

Table 146: CDR Filter Criteria

| | |
|-------------------------------|---|
| Call Type | <p>Groups the following:</p> <ul style="list-style-type: none"> ◦ Inbound calls: Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension. ◦ Outbound calls: Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension. ◦ Internal calls: Internal calls are calls from one internal extension to another extension, which are not sent over a trunk. ◦ External calls: External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension. |
| Status | <p>Filter with the call status, the available statuses are the following:</p> <ul style="list-style-type: none"> ◦ Answered ◦ No Answer ◦ Busy ◦ Failed |
| Source Trunk Name | <p>Select source trunk(s) and the CDR of calls going through inbound the trunk(s) will be filtered out.</p> |
| Destination Trunk Name | <p>Select destination trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.</p> |

| | |
|------------------------|---|
| Action Type | <p>Filter calls using the Action Type, the following actions are available:</p> <ul style="list-style-type: none">◦ Announce◦ Announcement page◦ Dial◦ Announcements◦ Callback◦ Call Forward◦ Meeting◦ DISA◦ Follow Me◦ IVR◦ Page◦ Parked Call◦ Queue◦ Ring Group◦ Transfer◦ VM◦ VMG◦ VQ_Callback◦ Wakeup◦ Emergency Call◦ Emergency Notify◦ SCA |
| Extension Group | Specify the Extension Group name to filter with. |

| | |
|-------------------------|---|
| Export File Data | <p>Select the fields that will be exported, the following fields are available:</p> <ul style="list-style-type: none"> ◦ Account Code ◦ Session ◦ Premier caller ◦ Action type ◦ Source trunk name ◦ Destination trunk name ◦ Caller number ◦ Caller ID ◦ Caller name ◦ Callee number ◦ Answer by ◦ Context ◦ Start time ◦ Answer time ◦ End time ◦ Call time ◦ Talk time ◦ Source channel ◦ Dest channel ◦ Call status ◦ Dest channel extension ◦ Last app ◦ Last data ◦ AMAFLAGS ◦ UIQUEID ◦ Call type ◦ NAT |
| Account Code | <p>Select the account Code to filter with. If pin group CDR is enabled, the call with pin group information will be displayed as part of the CDR under Account Code Field.</p> |
| Start Time | <p>Specify the start time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.</p> |
| End Time | <p>Specify the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.</p> |

| | |
|----------------------|---|
| Caller Number | <p>Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out.</p> <p>User could specify a particular caller number or enter a pattern. ‘.’ matches zero or more characters, only appears in the end. ‘X’ matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end.</p> <p>For example:</p> <p>3XXX: It will filter out CDR that having caller number with leading digit 3 and of 4 digits’ length.</p> <p>3.: It will filter out CDR that having caller number with leading digit 3 and of any length.</p> |
| Caller Name | Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out. |
| Callee Number | <p>Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out.</p> <p>Note: The “Callee Number” filter field supports specifying Pattern (example: 3XXX) or using Leading digits (example: 3.) as filtering options.</p> |

The call report will display as the following figure shows.

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

Figure 294: Call Report

The CDR report has the following data fields:

- **Start Time**

Format: 2019-12-11 09:53:03

- **Action Type**

Example:

IVR

DIAL

WAKEUP

- **Call From**

Example format: 5555

- **Call To**

Example format: 1000

- **Call Time**

Format: 0:00:11

- **Talk Time**

Format: 0:00:06

- **Account Code**

Example format:

Grandstream/Test

- **Status**

Answered, Busy, No answer or Failed.

Users could perform the following operations on the call report.

- **Sort by “Start Time”**

Click on the header of the column to sort the report by “Start Time”. Clicking on “Start Time” again will reverse the order.

- **Download Searched Results**

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

- **Download All Records**

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

- **Delete All**

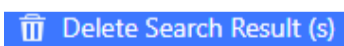
Click on



button to remove all the call report information.

- **Delete Search Result**

On the bottom of the page, click on



button to remove CDR records that

appear on search results.

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

- **Play/Download/Delete Recording File (per entry)**

If the entry has audio recording file for the call, the three icons on the rightest column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

Click on



to play the recording file; click on



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

to delete the recording file (the call record entry will not be deleted).

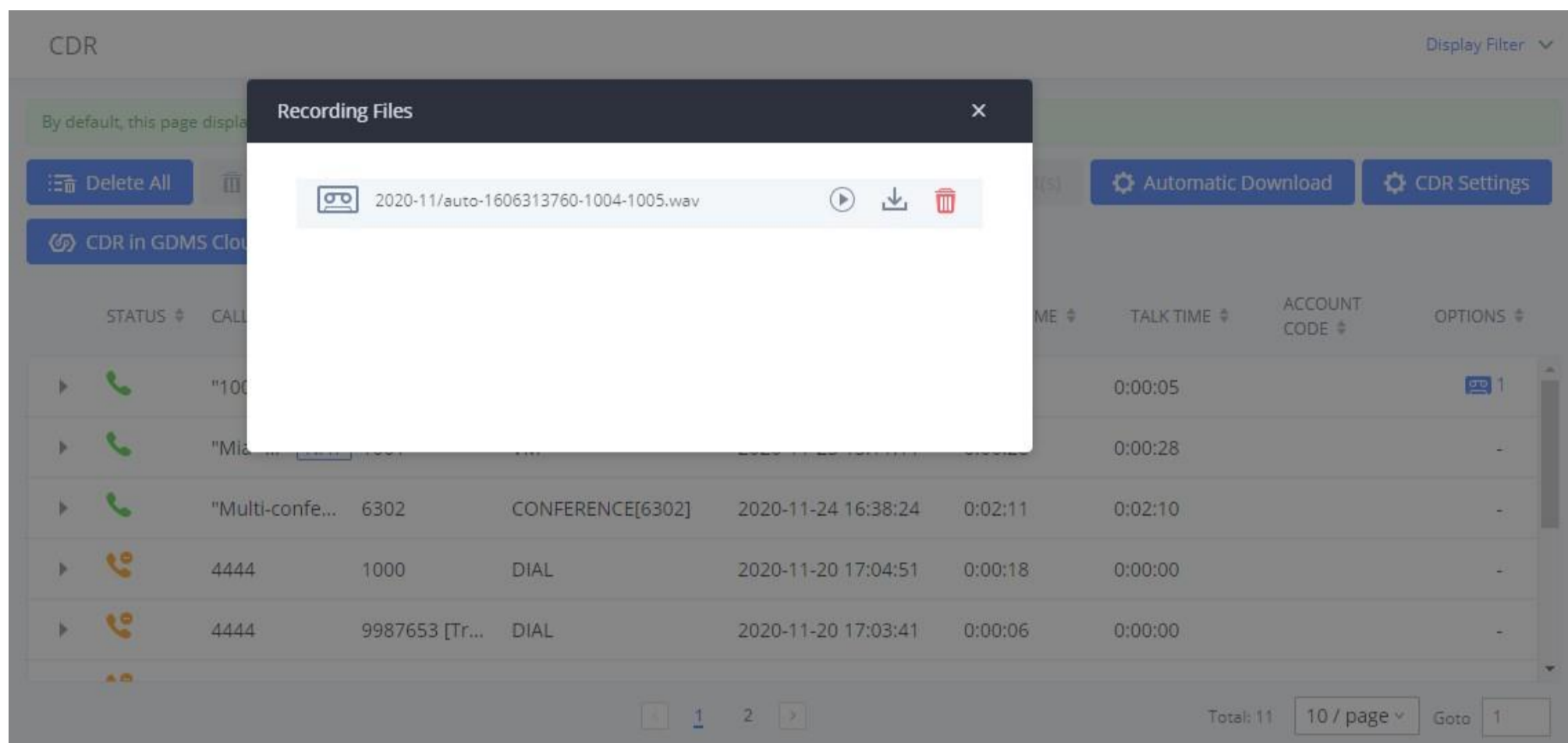


Figure 295: Call Report Entry with Audio Recording File

- **Automatic Download CDR Records**

User could configure the UCM630xA to automatically download the CDR records and send the records to multiple Email recipients in a specific hour. Click on “Automatic Download Settings” and configure the parameters in the dialog below.

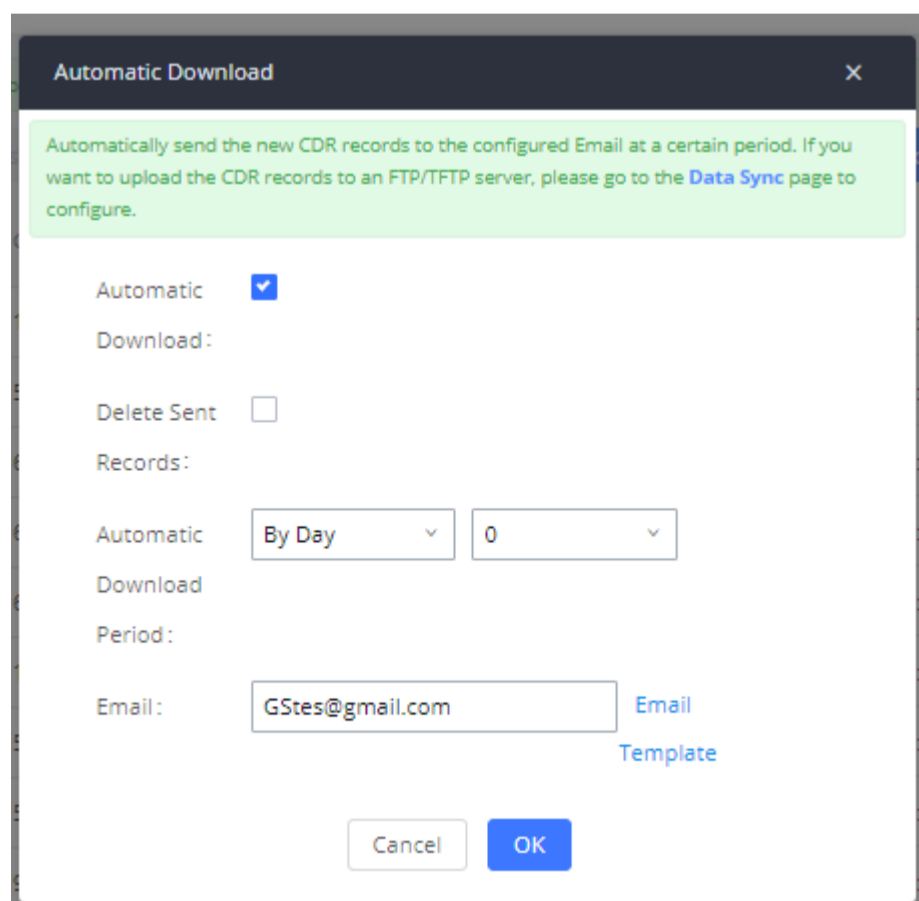


Figure 296: Automatic Download Settings

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

Note: users have the option to delete the sent records “Delete Sent Records”

Starting from UCM630xA firmware 1.0.10.x, transferred call will no longer be displayed as a separate call entry in CDR. It will display within call record in the same entry. CDR new features can be found under Web GUI→CDR→CDR. The user can click on the option icon for a specific call log entry to view details about this entry, such as premier caller and transferred call information.

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

Figure 297: CDR Report

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

Figure 298: Detailed CDR Information

Downloaded CDR File

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

- **Caller number, Callee number**

“Caller number”: the caller ID.

“Callee number”: the callee ID.

If the “Source Channel” contains “DAHDI”, this means the call is from FXO/PSTN line.

| caller number | callee number | context | calerid | source channel | dest channel | lastapp |
|---------------|---------------|-----------------|-------------------------|-------------------------------------|------------------------|---------|
| | 2009 | from-internal | "Wake Up Call" <WakeUp> | Local/2009@from-internal-00000001;2 | PJSIP/2009-00000013 | Dial |
| 2007 | 31100 | from-internal | "" <2007> | PJSIP/2007-00000014 | DAHDI/1-1 | Dial |
| 2009 | 1100 | from-internal | "John Doe" <2009> | PJSIP/2009-00000015 | PJSIP/trunk_1-00000016 | Dial |
| 1100 | 2014 | from-did-direct | "1100" <1100> | DAHDI/1-1 | PJSIP/2014-00000017 | Dial |

Figure 299: Downloaded CDR File Sample

- **Context**

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.

ext-did-XXXXX: inbound calls. It starts with “ext-did”, and “XXXXX” content varies case by case, which also relate to the order when the trunk is created.

ext-local: internal calls between local extensions.

- **Source Channel, Dest Channel**

Sample 1:

| caller number | callee number | context | calerid | source channel | dest channel | disposition |
|---------------|---------------|---------------|-----------|---------------------|--------------|-------------|
| 2007 | 31100 | from-internal | "" <2007> | PJSIP/2007-00000014 | DAHDI/1-1 | ANSWERED |

Figure 300: 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 |

Figure 301: Downloaded CDR File Sample – Source Channel and Dest Channel 2

- “SIP” means it is a SIP call. There are three format:
- (a) **PJSIP/NUM-XXXXXX**, where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.
- (c) **PJSIP/trunk_X/NUM**, where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.
- (c) **PJSIP/trunk_X-XXXXXX**, where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

There are some other values, but these values are the application name which are used by the dialplan.

IAX2/NUM-XXXXXXXX: 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

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 shows a web interface for filtering CDR data. It includes several input fields: 'End Time' with a date picker, 'Caller Name', 'Account Code', and 'Destination Trunk Name'. Below these is the 'Export File Data' dropdown menu, which is currently open and shows a list of data fields: ACCOUNT CODE, SESSION, ACTION OWNER, ACTION TYPE, SOURCE TRUNK NAME, DEST TRUNK NAME, CALLER NUMBER, and CALLERID. To the left of the dropdown are checkboxes for 'Outbound Calls', 'Internal Calls', 'No Answer', and 'Busy'. At the bottom, there are buttons for 'All Records' and 'Download Search Result (s)', and a table header with columns like 'type', 'Start Time', 'Call Time', 'Talk Time', 'Account Code', and 'Recording File'.

Figure 302: CDR Export File data

CDR in GDMS Cloud

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

The screenshot shows a web interface titled 'CDR in GDMS Cloud' with a 'Cancel' button in the top right. Below the title is a 'Delete' button. The main area is a table with the following structure:

| <input type="checkbox"/> | NAME | DATE | SIZE | OPTIONS |
|--------------------------|------|------|------|---------|
| No Data | | | | |

Figure 303: CDR in GDMS Cloud

Statistics

CDR Statistics is an additional feature on the UCM630xA which provides users a visual overview of the call report across the time frame. Users can filter with different criteria to generate the statistics chart.

Action Type: All SIP Calls PSTN Calls IAX Calls

Time: By Month By Week By Day By Hour By Range

2019

CDR Statistics

All Calls Inbound Calls Outbound Calls Internal Calls External Calls



Figure 304: CDR Statistics

Table 147: CDR Statistics Filter Criteria

| | |
|--------------------------|--|
| <p>Trunk Type</p> | <p>Select one of the following trunk type.</p> <ul style="list-style-type: none"> <input type="radio"/> All <input type="radio"/> SIP Calls <input type="radio"/> PSTN Calls |
| <p>Call Type</p> | <p>Select one or more in the following checkboxes.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Inbound calls <input type="checkbox"/> Outbound calls <input type="checkbox"/> Internal calls <input type="checkbox"/> External calls <input type="checkbox"/> All calls |

| | |
|-------------------|--|
| Time Range | <ul style="list-style-type: none"> ◦ By month (of the selected year). ◦ By week (of the selected year). ◦ By day (of the specified month for the year). ◦ By hour (of the specified date). ◦ By range. For example, 2016-01 To 2016-03. |
|-------------------|--|

Recording Files

This page lists all the recording files recorded by “Auto Record” per extension/ring group/call queue/trunk, or via feature code “Audio Mix Record”. If external storage device is plugged in, for example, SD card or USB drive, the files are stored on the external storage. Otherwise, internal storage will be used on the UCM630xA.

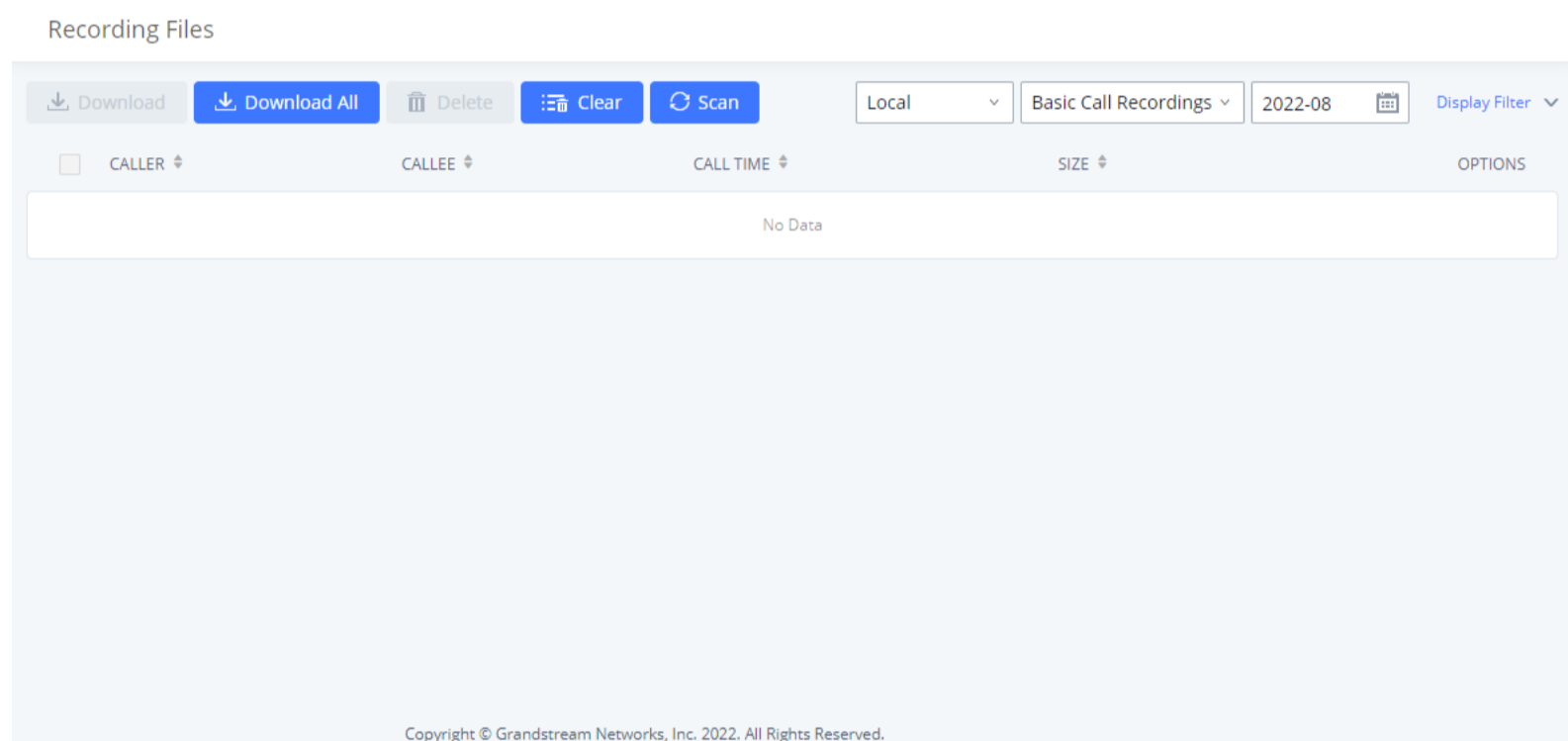




Figure 305: CDR→Recording Files

- Click on “**Download**” to batch-download the selected recording files.
- Click on “**Download All**” to download all the recording files.
- Click on “**Delete**” to batch-delete the selected recording files.
- Click on “**Clear**” to delete all the recording files.
- Click on “**Scan**” to retrieve the file information and display all the recording files on external storage. The UCM automatically retrieves the info of the first 5000 files from external storage already. This button can be used when the number of files stored on the external storage exceeds 5000 files and it requires manual file scanning.
- Select either “**USB Disk**” or “**Local**” to show recording files stored on external or internal storage, depending on selected storage space.
- Select whether to show call recordings, queue recordings or conference recordings.
- Click on  to download the recording file in .wav format.
- Click on  to delete the recording file.
- To sort the recording file, click on the title “Caller”, “Callee” or “Call Time” for the corresponding column. Click on the title again can switch the sorting mode between ascending order or descending order.

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: | <input type="text" value="1000"/> | * User Password: | <input type="text" value="mYpassWord!"/> |
| Privilege: | <input type="text" value="Consumer"/> | Department: | <input type="text" value="Support"/> |
| Fax: | <input type="text"/> | Email Address: | <input type="text" value="user1000@domain.local"/> |
| First Name: | <input type="text" value="John"/> | Last Name: | <input type="text" value="DOE"/> |
| Home Number: | <input type="text"/> | Mobile Phone Numb...: | <input type="text"/> |

Figure 306: Edit User Information by Super Admin

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

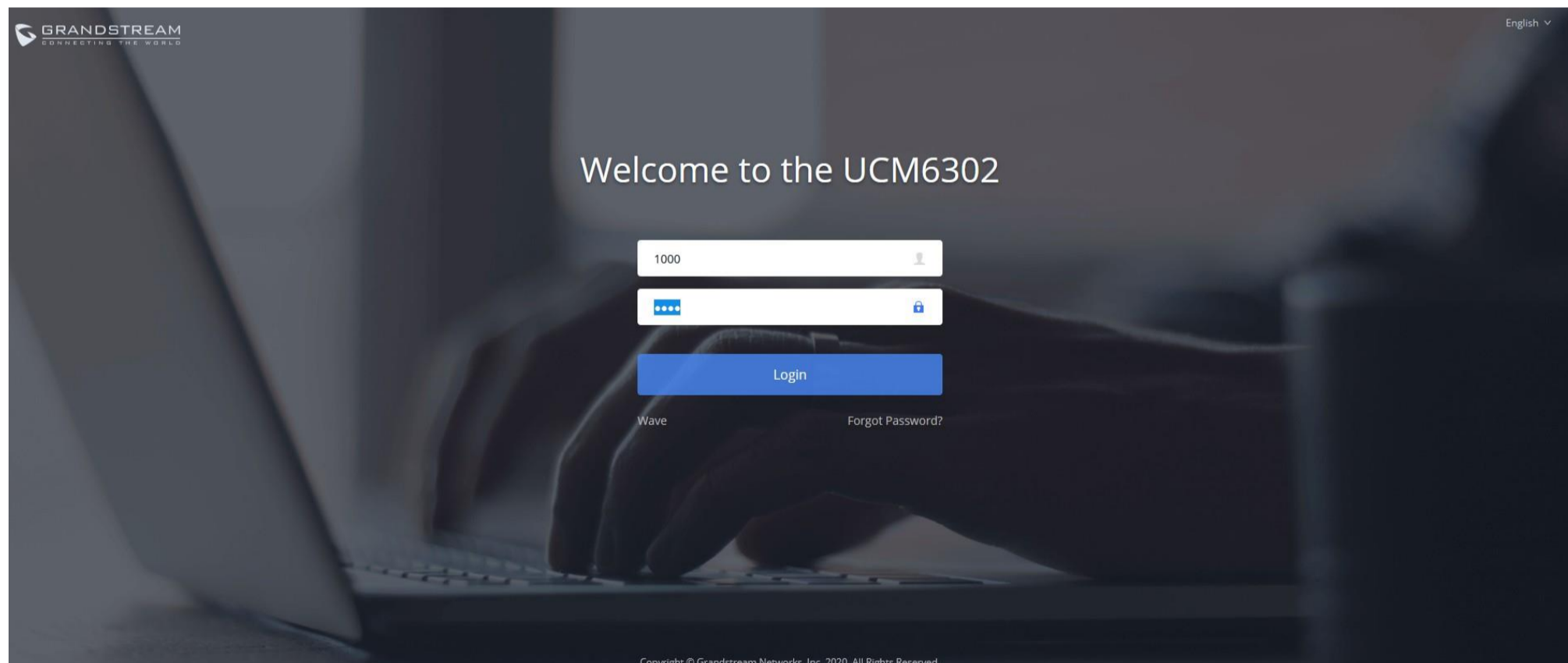


Figure 307: User Portal Login

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

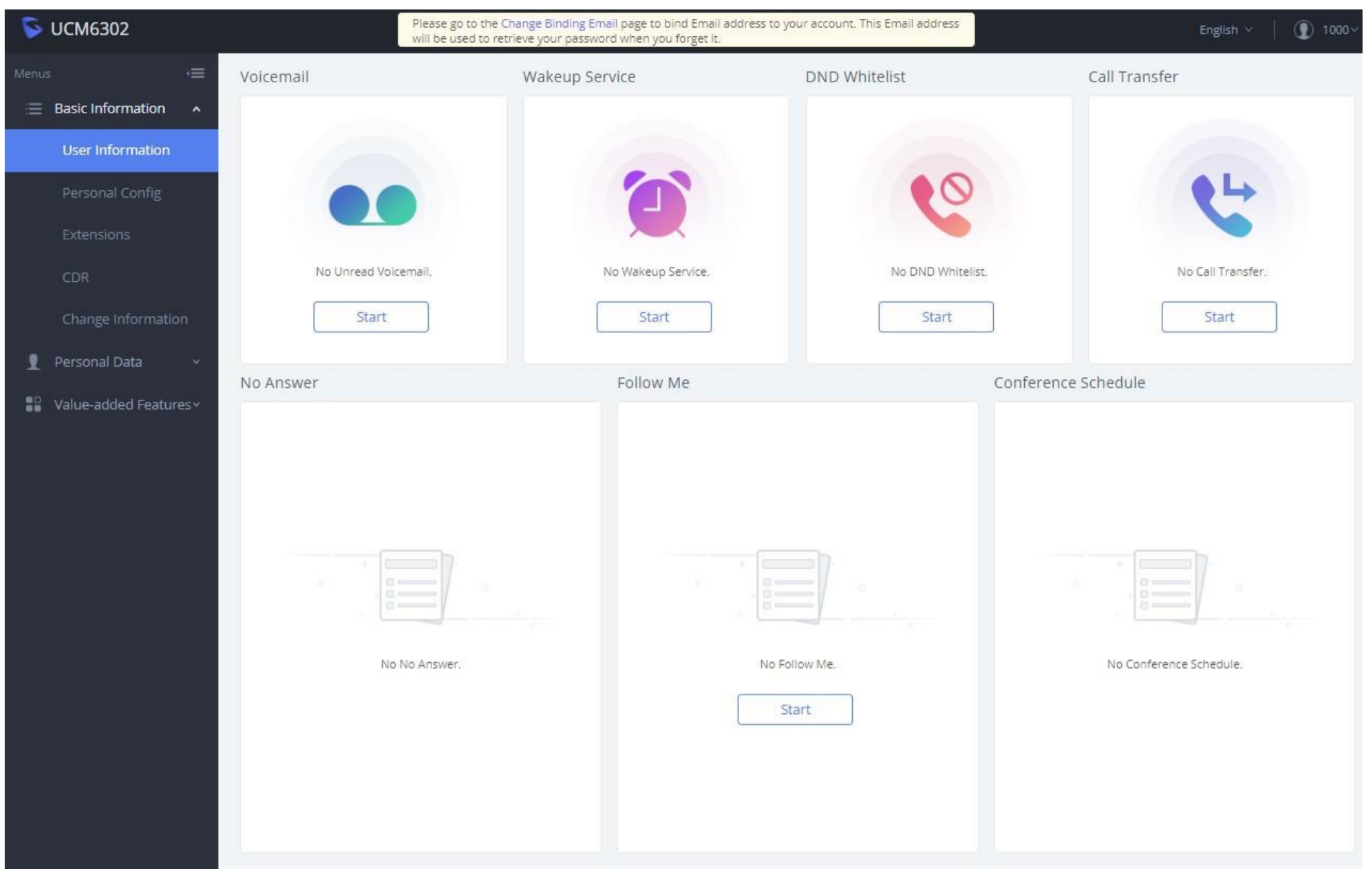


Figure 308: User Portal Layout

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 [Table 148: 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.

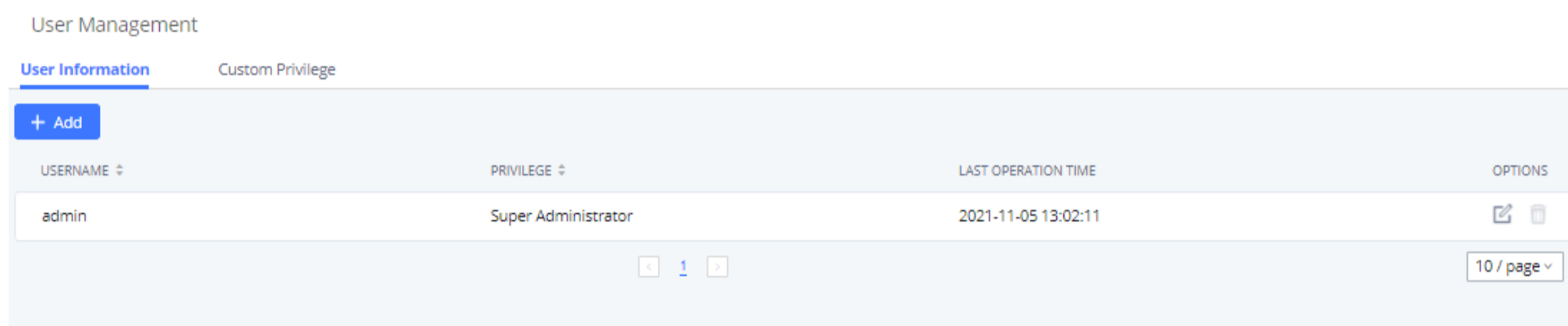


Figure 309: User Management Page Display

User Information

When logged in as Super Admin, click on "Add" to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.

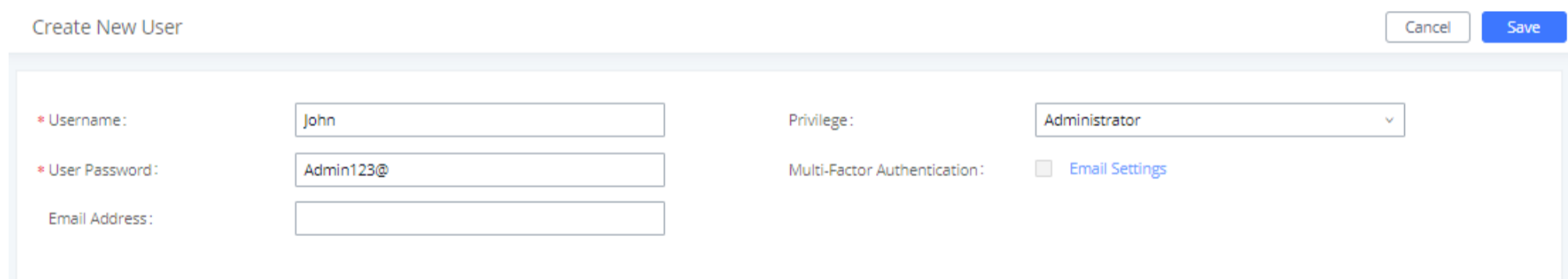


Figure 310: Create New User

Table 148: User Management→Create New User

| | |
|------------------------------------|---|
| Username | Configure a username to identify the user which will be required in Web GUI login. Letters, digits, and underscore are allowed in the username. |
| User Password | Configure a password for this user which will be required in Web GUI login. English input is allowed without space, ' and “. |
| Privilege | This is the role of the Web GUI user. 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. |
|----------------------|---|

Once created, the Super Admin can edit the users by clicking on



or delete the user by clicking on



User Management

User Information Custom Privilege

+ Add

| USERNAME ↕ | PRIVILEGE ↕ | LAST OPERATION TIME | OPTIONS |
|------------|---------------------|---------------------|---------|
| admin | Super Administrator | 2021-11-05 13:08:50 | |
| John | Administrator | -- | |

10 / page

Figure 311: 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.

Choose authentication method

For more information about multi-factor security certification, see [Instructions for use](#)

Virtual MFA device certification
Install the app on your phone

Hardware MFA device certification
All devices that support the development of TOTP standards

Cancel Next

Figure 312: MFA Settings

Custom Privilege

Four privilege levels are supported:

- **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 “Admin” privilege.
- Super Admin can edit and delete one or more users with “Consumer” privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account “admin” is configured with “Super Admin” privilege and it is the only user with “Super Admin” privilege. The Username and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on Web GUI→**Maintenance**→**Login Settings** page.
- Super Admin could view operations done by all the users in Web GUI→**Maintenance**→**User Management**→**Operation Log**
- **Administrator**
- Users with “Admin” privilege can only be created by “Super Admin” user.
- “Admin” privilege users are not allowed to access the following pages:

Maintenance→**Upgrade**

Maintenance→**Cleaner**

Maintenance→**Reset/Reboot**

Settings→**User Management**→**Operation Log**

- “Admin” privilege users cannot create new users for login.

Note: By default, administrator accounts are not allowed to access backup menu, but this can be assigned to them by editing the option “**Maintenance** → **User Management** → **Custom Privilege**” then press



to edit the “Admin” account and include backup operation permission for these types of users.

* Privilege Name:


Custom Privilege:

| | |
|---|--|
| <input type="checkbox"/> 1 item Available | <input type="checkbox"/> 0 item Selected |
| <input type="checkbox"/> Backup | None |

Navigation: < >

Figure 313: Assign Backup permission to “Admin” users

- **Consumer**

- A user account for Web GUI login is created automatically by the system when a new extension is created.
- The user could log in the Web GUI with the extension number and password to access user information, extension configuration, CDR of that extension, personal data, and other features. For more details; please refer to <https://documentation.grandstream.com/knowledge-base/user-portal/>.
- The Super Admin user can click on  on the “General User” in order to enable/disable the custom privilege from deleting their own recording files, changing SIP credentials, and disabling voicemail service in their user portal account.

Edit Custom Privilege: General_User



* Privilege Name:

Enable Delete Recording

Files:

Allowed to change Auth ID
and SIP password:

Allow to Enable Voicemail:

Figure 314: General User

- **Custom Privilege**

The Super Admin user can create users with different privileges. 38 items are available for privilege customization.

- API Configuration
- Backup
- Callback
- Call Queue
- Queue Statistics
- Queue Recordings
- CDR Recording Files
- CDR Records
- CDR Statistics
- Dial By Name
- DISA
- Emergency Calls
- Event List
- Extensions
- Outbound Routes
- Inbound Routes
- Fax/T.38
- Feature Codes

- IVR
- Paging/Intercom
- Parking Lot
- Pickup Groups
- PMS – Wakeup Service
- Ring Groups
- SCA
- Speed Dial
- System Status
- System Events
- LDAP Server
- Time Settings
- Meeting
- Voicemail
- Voice Prompt
- Wakeup Service
- Zero Config
- Announcement.
- UCM RemoteConnect

Figure 315: Create New Custom Privilege

Log in UCM630xA as super admin and go to **Maintenance**→**User Management**→**Custom Privilege**, create privilege with customized available modules.

When you add CDR Records and CDR Recording Files custom privileges, additional privileges will appear (All Deletion of CDR and Allow Deletion of DCR Recordings , respectively). This offers more flexibility on the privileges that the admin assigns to the user.

Create New Custom Privilege

* Privilege Name:

Allow Deletion of CDR:
Allow Deletion of CDR Recordings:

* Custom Privilege:

| <input type="checkbox"/> 37 items Available | <input type="checkbox"/> 2 items Selected |
|---|--|
| <input type="checkbox"/> Queue Statistics | <input type="checkbox"/> CDR Records |
| <input type="checkbox"/> Queue Recordings | <input type="checkbox"/> CDR Recording Files |
| <input type="checkbox"/> CDR Statistics | |
| <input type="checkbox"/> Dial By Name | |
| <input type="checkbox"/> DISA | |
| <input type="checkbox"/> Emergency Calls | |

To assign custom privilege to a sub-admin, navigate to UCM Web GUI→Maintenance→User Management→User Information→Create New User/Edit Users, select the custom privilege from “Privilege” option.

Concurrent Multi-User Login

When there are multiple Web GUI users created, concurrent multi-user login is supported on the UCM630xA. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on “Apply Changes”), a prompt will pop up as shown in the following figure.


 Operating too frequently or other users are doing the same operation. Please retry after 15 seconds.

Figure 316: Multiple User Operation Error Prompt

User Portal/Wave Privilege

The user can create customize privileges related to an extension’s User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.

User 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.

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.

* Enter Old Password:

| Change Password

Change Password:

* Enter New Password:

* Re-enter New Password:

| Change Username

Change Username:

| Change Binding Email

* Email Address: [Email Template](#)

Figure 323: Change Password

| | |
|----------------------------------|--|
| 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 Username

UCM630xA allows users now to change Super Administrator username.

| Change Username

Change Username:

* Please enter the username:

Figure 324: Change Username

Change binding Email

UCM630xA allows user to configure binding email in case login password is lost. UCM630xA login credential will be sent to the designated email address.

The feature can be found under Web GUI → **Maintenance** → **Login Settings** → **Change Password / Email**

| Change Binding Email

* Email Address: [Email Template](#)

Table 150: Change Binding Email option

| | |
|----------------------|--|
| Email Address | Email Address is used to retrieve password when password is lost |
|----------------------|--|

Login Security

After the user logs in the UCM630xA 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 UCM630xA web GUI→Maintenance→Login Settings→Login Security page.

The “**User Login Timeout**” value is in minute and the default setting is 10 minutes. If the user does not make any operation on Web GUI within the timeout, the user will be logged out automatically. After that, the Web GUI will be redirected to the login page and the user will need to enter username and password to log in.

If set to 0, there is no timeout for the Web GUI login session and the user will not be automatically logged out.

“**Maximum number of login attempts**” can prevent the UCM630xA from brutal force decryption, if this number is exceeded user IP address will be banned from accessing the UCM for a period of time based on user configuration, the default value is 5.

“**User ban period**” specify the period of time in minutes an IP will be banned from accessing the UCM if the User max number of try login is exceeded, the default value is 5.

“**Login Banned User List**” show the list of IPs’ banned from the UCM.

“**Login Whitelist**” User can add a list of IPs’ to avoid the above restriction, thus, they can exceed the User max number of try login.

The screenshot displays the 'Login Security' configuration page. At the top, there are tabs for 'Change Password / Email' and 'Login Security', with 'Login Security' being the active tab. A 'Cancel' button and a 'Save' button are located in the top right corner. Below the tabs, there are three input fields with red asterisks indicating required fields: 'User Login Timeout' (value: 10), 'Maximum number of login attempts' (value: 5), and 'User ban period' (value: 5). The 'Login Banned User List' section features a search bar with the placeholder text 'Please enter ip address' and a table with columns for 'IP ADDRESS', 'USER NAME', 'BANNED TIME', and 'OPTIONS'. The table currently contains 'No Data'. The 'Login Whitelist' section includes a green informational message: 'The IP addresses in the Login Whitelist will not be restricted. This option doesn't support network segment format.' Below this is a '+ Add' button and a table with columns for 'IP ADDRESS' and 'OPTIONS', also showing 'No Data'.

Figure 326: Login Timeout Settings

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.

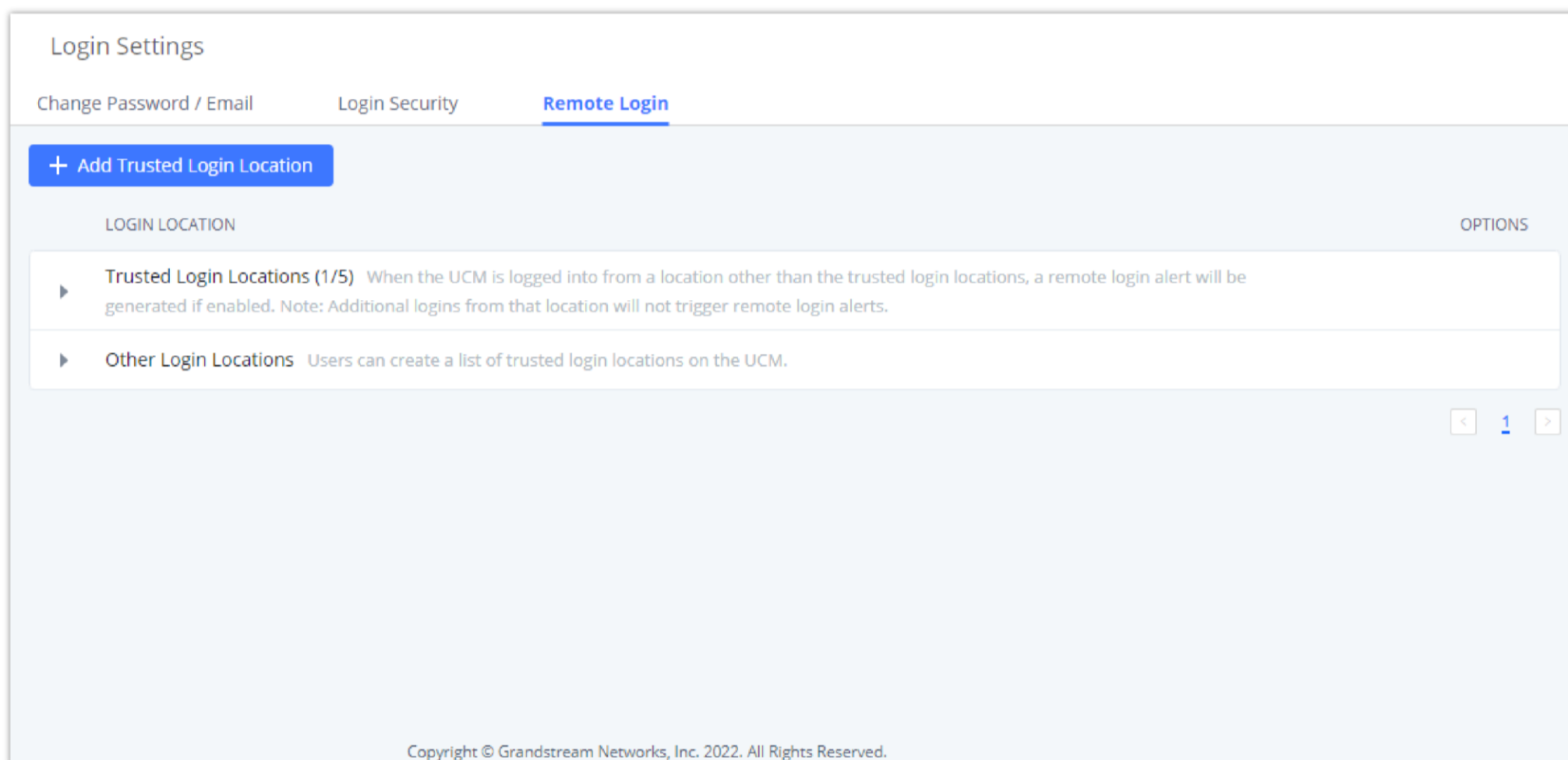


Figure : Remote Login

To add a trusted login location, the user must click on [+ Add Trusted Login Location](#)

Then add the public IP address of the location, click on “**Check Location**” to verify if it’s the correct location then click “**OK**”.

i Note

The system administrator can add up to 5 Trusted Login Locations, while Other Login Locations can have an unlimited number of entries.

Operation Log

Super Admin has the authority to view operation logs on UCM630xA Web GUI→**Settings**→**User Management**→**Operation Log** page. Operation logs list operations done by all the Web GUI users, for example, Web GUI login, creating trunk, creating outbound rule and etc. There are 7 columns to record the operation details “Date”, “Username”, “IP Address”, “Results”, “Page Operation”, “Specific Operation” and “Remark”.

| DATE | USERNAME | IP ADDRESS | RESULTS | PAGE OPERATION | SPECIFIC OPERATION | REMARK |
|---------------------|----------|---|---|--------------------|--------------------|---------------------------------------|
| 2022-08-04 15:48:02 | admin | 192.168.5.111 (Marrakesh, Marrakech-Safi, MA) | Operation successful | Extensions: Login | Username: admin. | 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 |

Figure 327: Operation Logs

The operation log can be sorted and filtered for easy access. Click on

or

at the top of each column to sort. For example, clicking on

for “Date” will sort the logs according to newer operation date and time. Clicking on

for “Date” will reverse the order.

Table 151: 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 ^

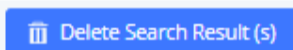
Start Time: 2019-12-10 00:00
End Time: 2019-12-11 00:00
IPv4/IPv6 Address:
User Name: admin

| DATE | USER NAME | IP ADDRESS | RESULTS | PAGE OPERATION | SPECIFIC OPERATION | REMARK |
|---------|-----------|------------|---------|----------------|--------------------|--------|
| No Data | | | | | | |

Figure 328: Operation Logs Filter

The above figure shows an example that operations made by user "support" on device with IP 192.168.40.173 from 2014-11-01 00:00 to 2014-11-06 15:38 are filtered out and displayed.

To delete operation logs, users can perform filtering first and then click on



to delete the filtered result of operation logs. Or users can click on



to delete all operation logs at once.

Upgrading

The UCM630xA can be upgraded to a new firmware version locally. And in order to do that, please follow the below steps:

1. Download the latest UCM630xA firmware file from the following link and save it in your PC.

<https://www.grandstream.com/support/firmware>

1. Log in the Web GUI as administrator in the PC.
2. Go to Web GUI→**Maintenance**→**Upgrade**, upload the firmware file by clicking on "choose file to upload" and select the firmware file from your PC.

The default firmware file name is UCM630xAfw.bin

Firmware File Path:

Figure 329: Local Upgrade

Upgrade Firmware Cancel Save

Upgrade Via: HTTP
Firmware Server Path: fw.ipvideotalk.com/gs

Figure 330: Upgrading Firmware Files

1. Wait until the upgrading process is successful and a window will be popped up in the Web GUI.

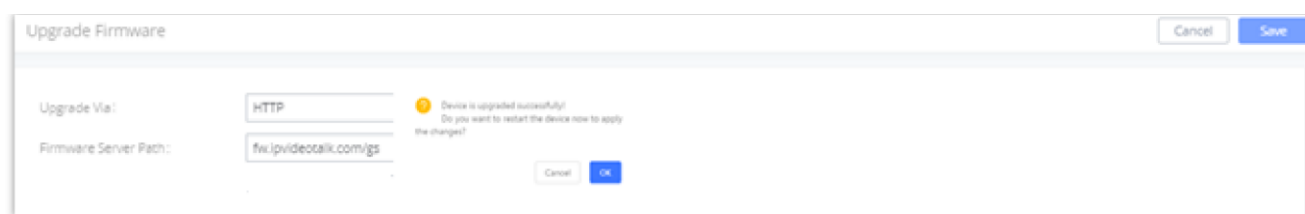


Figure 331: Reboot UCM630xA

1. Click on “OK” to reboot the UCM630xA and check the firmware version after it boots up.

Notes

- Please do not interrupt or power cycle the UCM630xA during upgrading process.
- The firmware file name allows the use of the special characters besides the following restricted characters: # \$ ^ & * + () [] / ; ' | , < > ?

No Local Firmware Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have TFTP/HTTP/HTTPS server, some free windows version TFTP servers are available for download from

http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

<http://tftpd32.jounin.net>

Please check our website at <https://www.grandstream.com/support/firmware> for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the UCM630xA to the same LAN segment;
3. Launch the TFTP server and go to the File menu → Configure → Security to change the TFTP server’s default setting from “Receive Only” to “Transmit Only” for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the UCM630xA web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the UCM630xA.

End users can also choose to download a free HTTP server from <http://httpd.apache.org/> or use

Microsoft IIS web server.

Backup

The UCM630xA configuration can be backed up locally or via network. The backup file will be used to restore the configuration on UCM630xA when necessary.

Backup/Restore

Users could backup the UCM630xA configurations for restore purpose under Web GUI → Maintenance → Backup → Backup/Restore.

Click on "Backup" to create a new backup file. Then the following dialog will show.

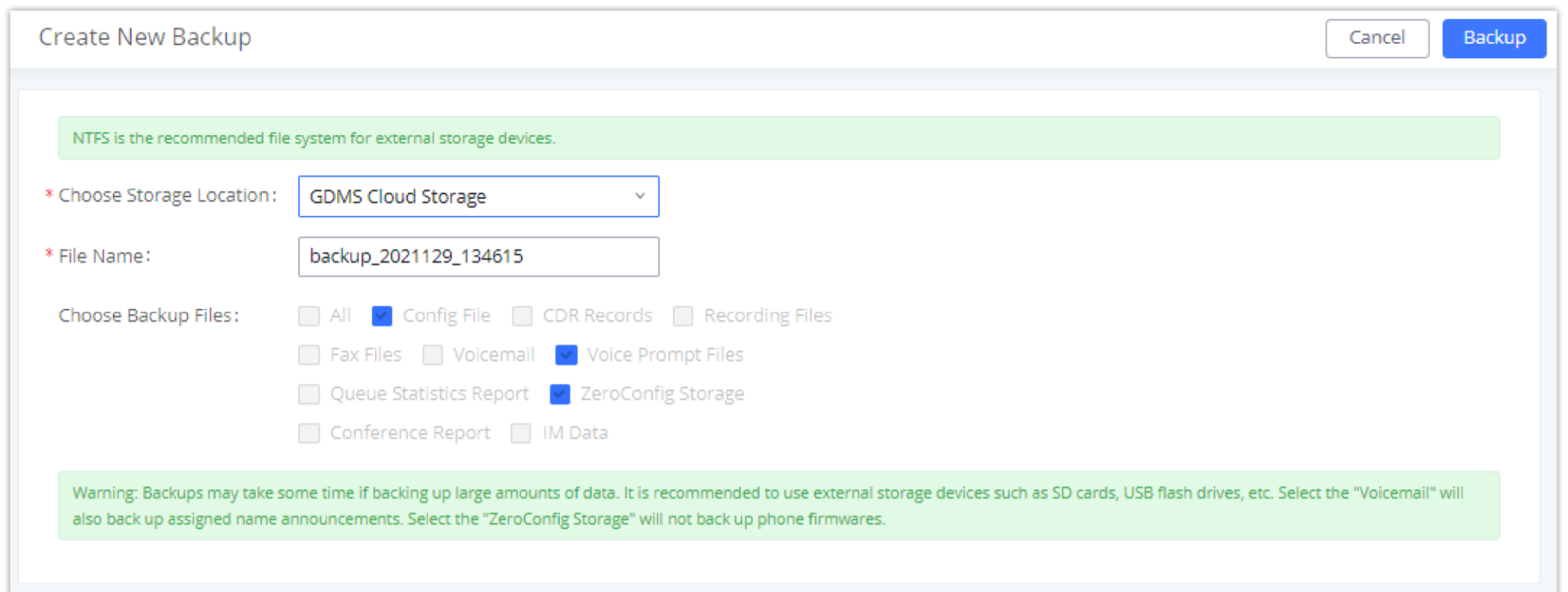


Figure 332: Create New Backup

1. Choose the type(s) of files to be included in the backup.
2. Choose where to store the backup file: USB Disk, SD Card, Local, NAS or GDMS.
3. Name the backup file.
4. Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download

, restore

, or delete

it from the UCM630xA internal storage or the external device.

Click on

to upload backup file from the local device to UCM630xA. The uploaded backup file will also be displayed in the web page and can be used to restore the UCM630xA.

Note: users can restore backups of models with more FXO ports to models with less FXO ports as long as the configurations related to the extra FXO ports are removed.

Please make sure the FXO port settings, total number of extensions and total number of meeting rooms are compactable before restoring to another UCM model. Otherwise it will prompt a warning and stop the restore process as shown below:

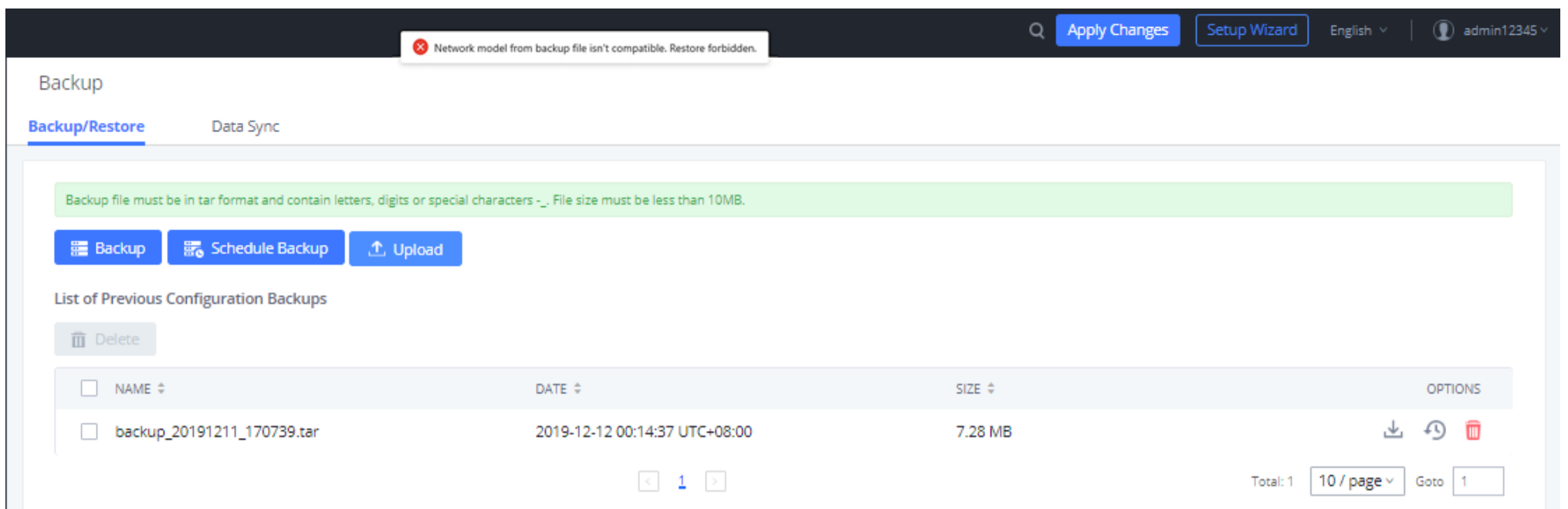


Figure 333: Restore Warning

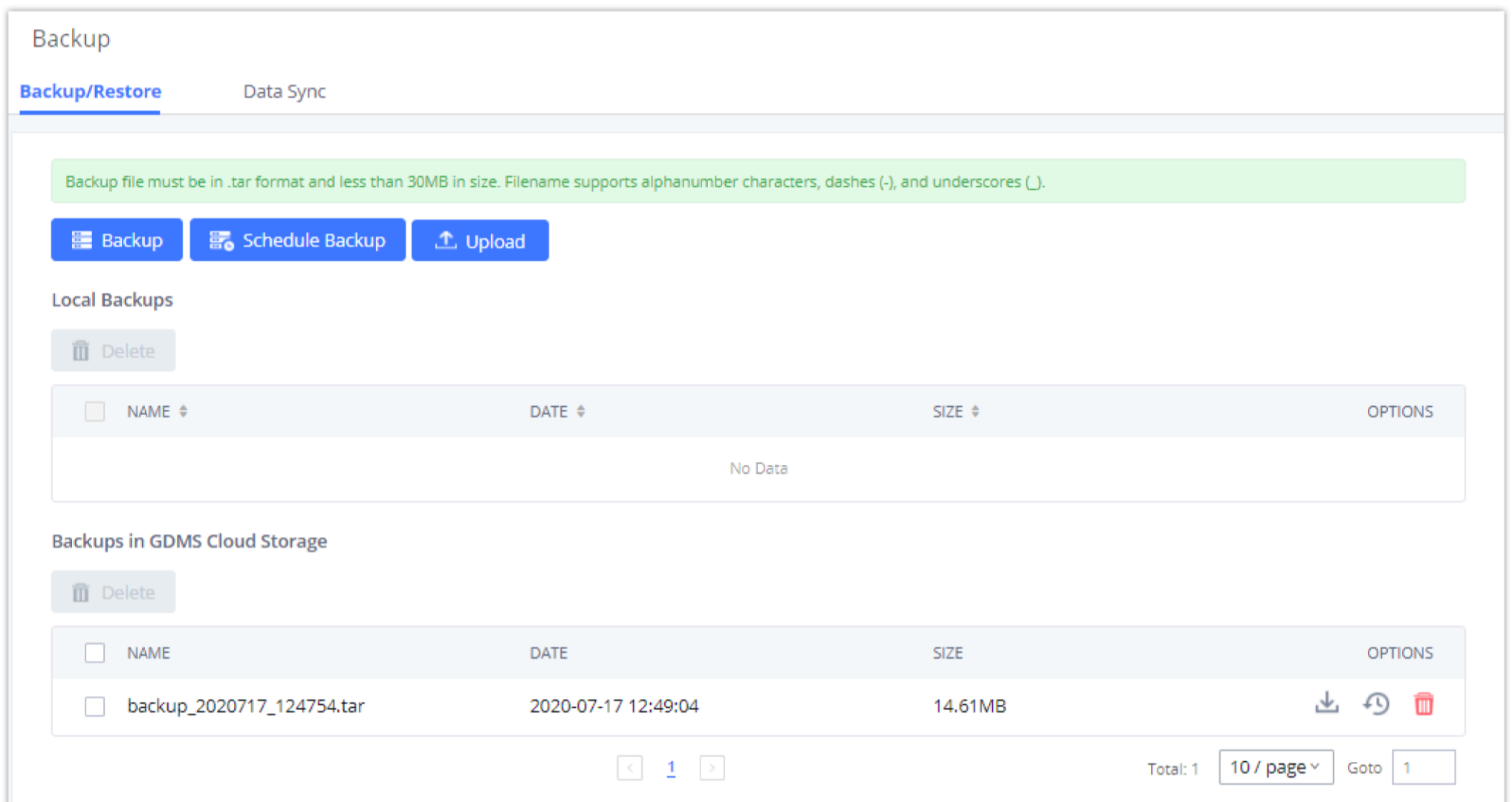


Figure 334: Backup / Restore

The

option allows UCM to perform automatically backup on the user specified time. Regular backup file can only be stored in USB / SD card / SFTP server. User is allowed to set backup time from 0-23 and how frequent the backup will be performed.

Schedule Backup

NTFS is the recommended file system for external storage devices.

Enable Scheduled Backup:

Choose Storage Location: SFTP Server

* Account:

Password:

* Server Address:

Destination Directory:

* Backup Time: 00:00

* Backup Frequency: 1

Choose Backup Files:

All
 Config File
 CDR Records
 Recording Files
 Voicemail
 Voice Prompt Files
 Queue Statistics Report
 ZeroConfig Storage
 Conference Report

+ Test Connection

Figure 335: Local Backup

Data Sync

Besides local backup, users could backup the voice records/voice mails/CDR in a daily basis to a remote server via SFTP protocol automatically under Web GUI→Maintenance→Backup→Data Sync.

The client account supports special characters such as @ or “.” Allowing the use email address as SFTP accounts. It allows users as well to specify the destination directory on SFTP server for backup file. If the directory does not exist on the destination, UCM630xA will create the directory automatically

Figure 336: Data Sync

Table 152: 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.

The screenshot shows a web interface for backup management. At the top, there are tabs for 'Backup/Restore' and 'Data Sync'. A green notification bar states: 'Backup file must be in .tar format and less than 30MB in size. Filename supports alphanumeric characters, dashes (-), and underscores (_).' Below this are three buttons: 'Backup', 'Schedule Backup', and 'Upload'. The interface is divided into two sections: 'Local Backups' and 'Backups in GDMS Cloud Storage'. The 'Local Backups' section has a 'Delete' button and an empty table with columns for NAME, DATE, SIZE, and OPTIONS. The 'Backups in GDMS Cloud Storage' section also has a 'Delete' button and a table with one entry: 'backup_2020717_124754.tar' with a date of '2020-07-17 12:49:04' and a size of '14.61MB'. The table includes download, refresh, and delete icons in the options column. At the bottom, there are pagination controls showing 'Total: 1', '10 / page', and 'Goto 1'.

Figure 337: Restore UCM630xA from Backup File

Note

The uploaded backup file must be a tar file with no special characters like *,!,#,@,&,\$,%^,(,)/,\,space in the file name. The uploaded back file size must be under 10MB.

System Cleanup/Reset

Reset and Reboot

Users could perform reset and reboot under Web GUI→Maintenance→System Cleanup/Reset→Reset and Reboot.

- To reboot the device, click on reboot icon.
- To factory reset the device, click on reset icon, then all the configurations and data will be reset to factory default.

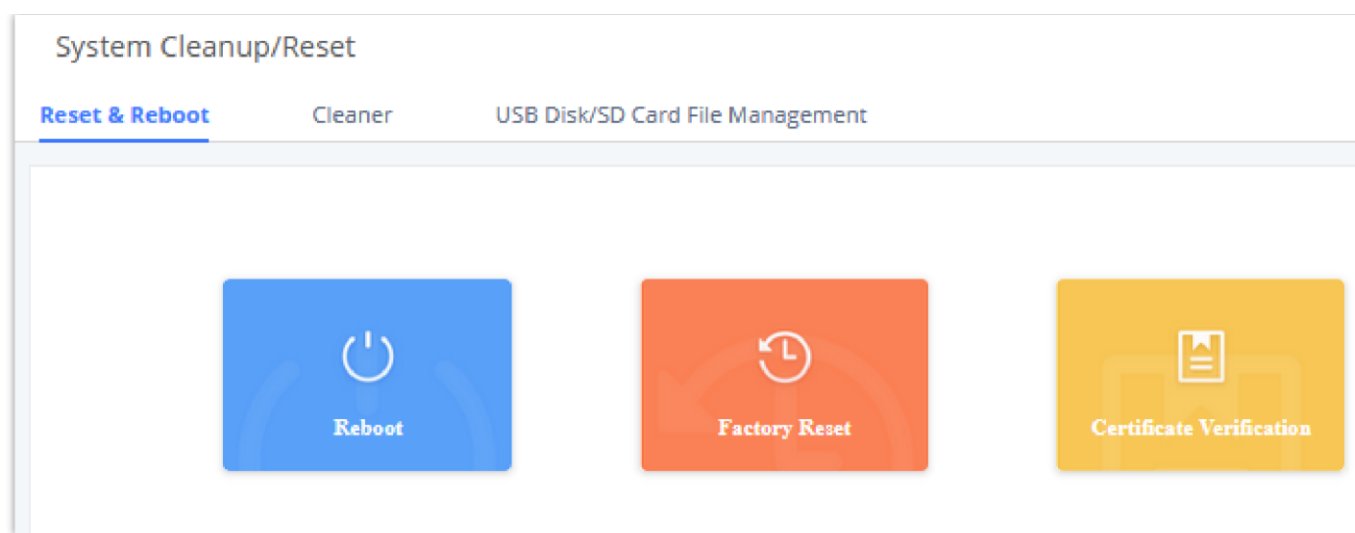


Figure 338: Reset and Reboot

- User can also verify UCM certificate under the same path.

Cleaner

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails etc... manually and automatically under Web GUI → **Maintenance** → **System Cleanup/Reset** → **Cleaner**.

The following screenshot show the settings and parameters to configure the manual cleaner feature on UCM630xA.

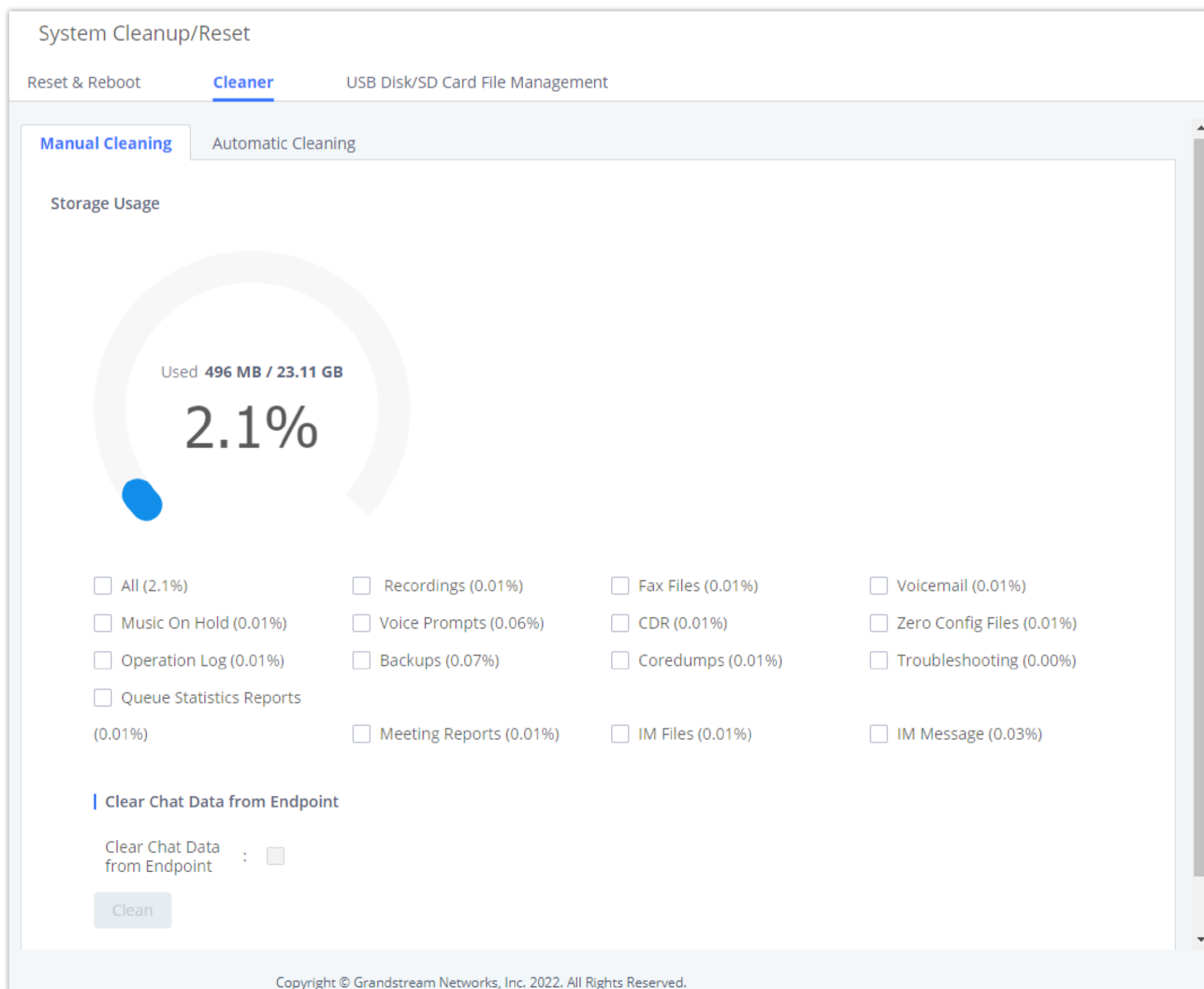


Figure 339: Manual Cleaning

Users can either clean all the data on the UCM or specify the modules to clean such as: Recordings, Fax Files, Voicemail, Music on Hold, Voice Prompts, CDR, ZeroConfig Files, Operation Log, Backups, Coredumps, Troubleshooting, Queue Statistics Reports, Meeting Reports, IM Data.

User can also set an automatic cleaning under **Cleaner**→**Automatic Cleaning**. The following screenshot show the settings and parameters to configure the cleaner feature on UCM630xA.

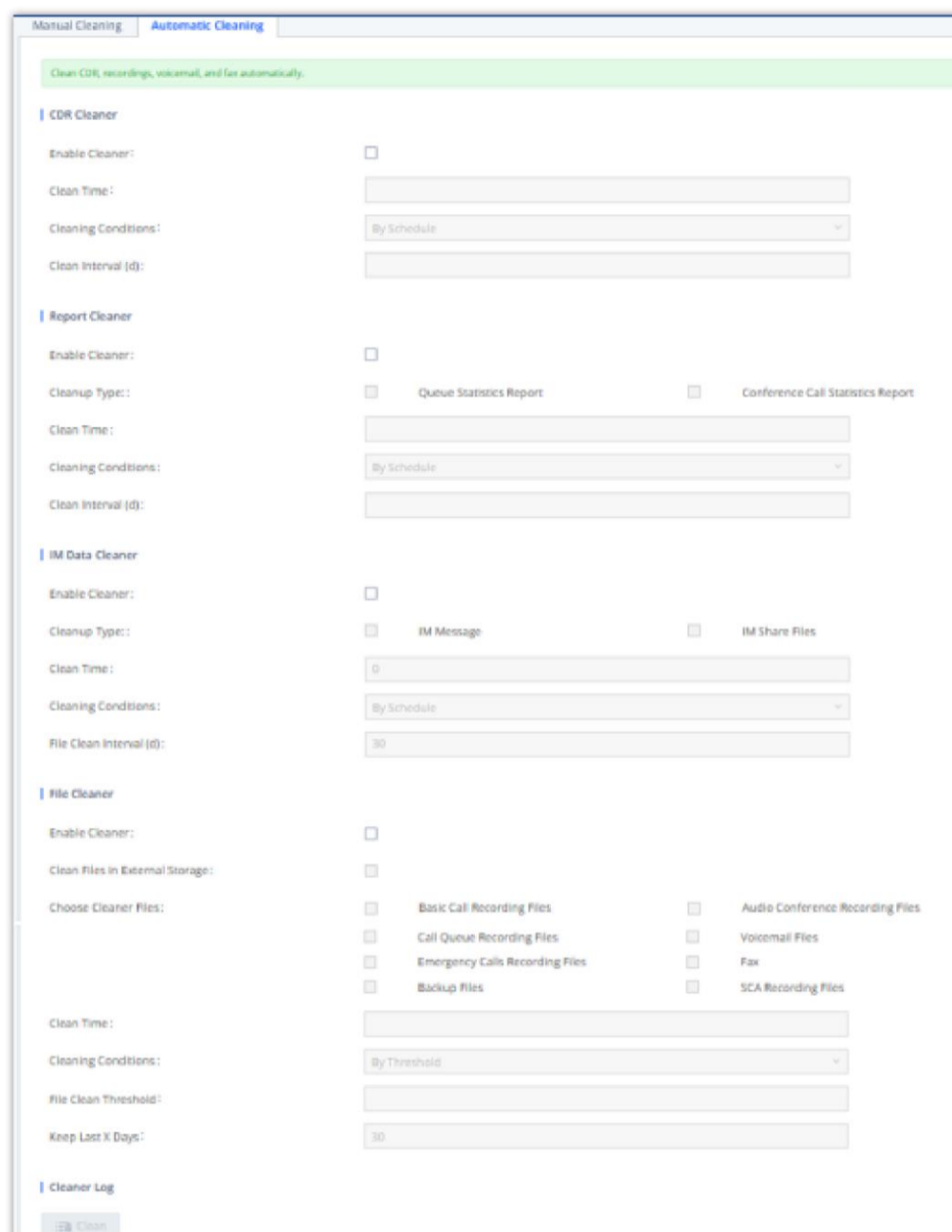


Figure 340: Automatic Cleaning

Table 153: Automatic Cleaning Configuration

| | |
|---------------------------|--|
| Enable CDR Cleaner | Enable the CDR Cleaner function. |
| CDR Clean Time | Enter 0-23 to specify the hour of the day to clean up CDR. |

| | |
|--|---|
| <p>Cleaning Conditions</p> | <p>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.</p> <p>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.)</p> <p>Keep Last X Days: Delete all entries older than X days.</p> |
| <p>Clean Interval</p> | <p>Enter 1-30 to specify the day of the month to clean up CDR when By Schedule is selected as Cleaning Conditions.</p> |
| <p>Max Entries</p> | <p>Set the maximum number of CDR entries to keep when Keep Last X Records is selected as Cleaning Conditions.</p> |
| <p>Keep Last X Day</p> | <p>Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions.</p> |
| <p>Enable Queue Statistics</p> <p>Report Cleaner</p> | <p>Enable scheduled queue log cleaning. By default, is disabled.</p> |
| <p>Queue Statistics</p> <p>Report Cleaner Clean Time</p> | <p>Enter the hour of the day to start the cleaning. The valid range is 0-23.</p> |

| | |
|--|---|
| <p>Cleaning Conditions</p> | <p>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.</p> <p>Keep Last X Records: If the max number of Queue Statistics has been reached, Queue Statistics will be deleted starting with the oldest entry at the configured cleaning time.(Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)</p> <p>Keep Last X Days: Delete all entries older than X days.</p> |
| <p>Clean Interval</p> | <p>Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.</p> |
| <p>Max Entries</p> | <p>Set the maximum number of Queue Statistics entries to keep when Keep Last X Records is selected as Cleaning Conditions.</p> |
| <p>Keep Last X Day</p> | <p>Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions.</p> |
| <p>Enable Meeting Statistics</p> <p>Report Cleaner</p> | <p>Enable scheduled Meeting log cleaning. By default, is disabled.</p> |
| <p>Cleaning Conditions</p> | <ul style="list-style-type: none"> ◦ 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 Meeting Statistics Report has been reached, Meeting Statistics Report will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.) ◦ Keep Last X Days: Delete all entries older than X days. |
| <p>Clean Interval</p> | <p>Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.</p> |
| <p>Max Entries</p> | <p>Set the maximum number of Meeting Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions.</p> |
| <p>Keep Last X Day</p> | <p>Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions.</p> |
| <p>Enable File Cleaner</p> | <p>Enter the Voice Records Cleaner function.</p> |

| | |
|---------------------------------------|--|
| Clean Files in External Device | If enabled the files in external device (USB/SD card) will be atomically cleaned up as configured. |
| Choose Cleaner File | Select the files for system automatic clean. <ul style="list-style-type: none"> ◦ Basic Call Recording Files. ◦ Meeting Recording Files. ◦ Call Queue Recording Files. ◦ Voicemail Files. ◦ Backup Files. |
| Clean time | Enter the hour of the day to start the cleaning. The valid range is 0-23. |
| Cleaning Conditions | <ul style="list-style-type: none"> ◦ By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to delete all files. ◦ By Threshold: Check at the configured cleaning time every day to see if the storage threshold has been exceeded and perform cleaning of all files if it has. ◦ Keep Last X Days: Delete all files older than X days. |
| File Clean Interval | Enter 1-30 to specify the day of the month to clean up the files. |
| File Clean Threshold | Enter the internal storage disk usage threshold (in percent). Once this threshold is exceeded, the file cleanup will proceed as scheduled. Valid range is 0-99. |
| Keep Last X Days | Automatically delete all recordings older than this x days when the threshold is reached. If not set, all data is cleared |
| Cleaner Log | Press Clean “button” to clean cleaner log. |

All the cleaner logs will be listed on the bottom of the page.

USB/SD Card Files Cleanup

Users could configure to clean or download the Call Detail Report/Voice Records/Voice Mails automatically under Web GUI→**Maintenance**→**System Cleanup/Reset**→**USB / SD Card Files Cleanup**.

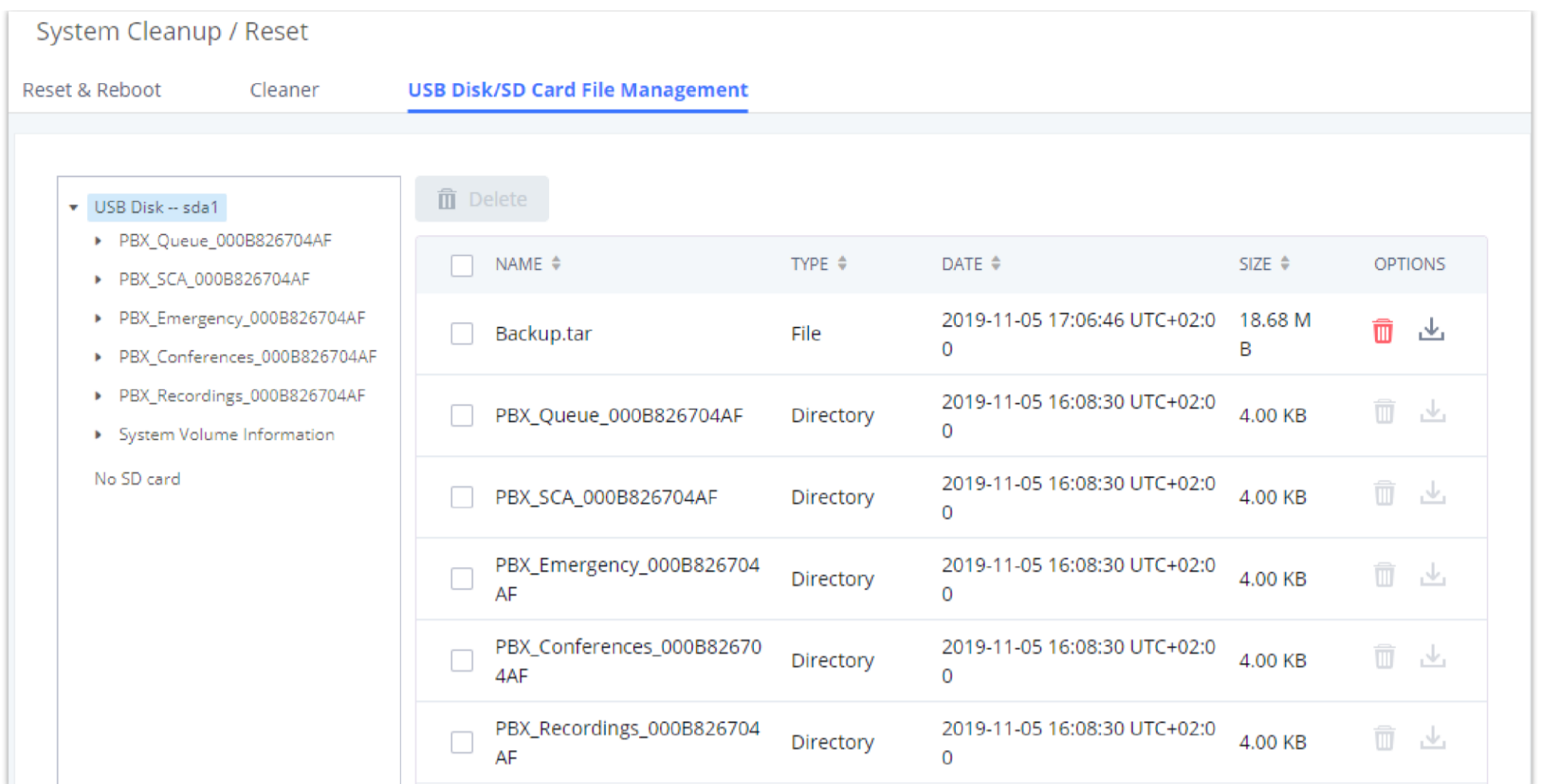


Figure 341: USB/SD Card Files Cleanup

Table 154: USB/SD Card Files Cleanup

| | |
|-----------------------------|--|
| Current Path | Displays the current path. |
| Directory | Select the directory user want to clean. |
| Delete Selected File | Select multiple entries to delete from USB or SD card. |

System Recovery

In some cases (for example after wrong upgrading procedure where the user doesn't follow the correct steps to perform an upgrade) the system may go into some hardware/software issues where the web UI access is lost as well as SSH, in this case the only solution would be to perform a full system recovery in order to reset or update the software version of the device in order to use it again.

1. To access recovery mode on UCM, please follow below steps:
2. Remove the power from the unit and keep the network cable connected.
3. Press using a PIN the reset button and keep holding.
4. Plug back the power supply while maintaining the reset button pressed.
5. Wait for couple of seconds until you hear a click sound.
6. Release the reset button, and the system should display on the LCD a message "Recovery Mode" along with an IP address.

Once at this stage, the administrator can access the recovery mode web portal by typing in either the IP0 address (typically WAN) or IP1 address (typically LAN) into a browser address bar. The following page should appear:



Figure 342: UCM6302A Recovery Web Page

Make sure to enter the correct admin password, and press login to access the recovery mode page :

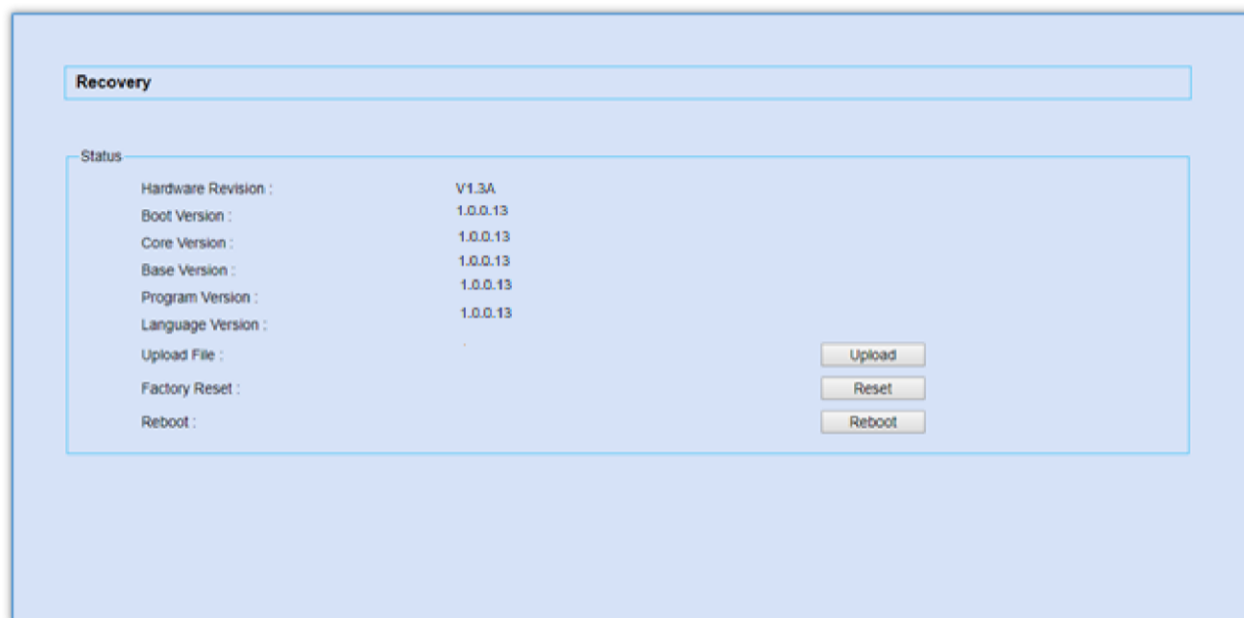


Figure 343: Recovery Mode

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).

Note

Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog prints might cause traffic and affect system performance.

The reserved size for Syslog entries on the cache memory of the UCM is 50M, once this sized is reached the UCM will clean up 2M of the oldest Syslog entries to

allow to save new logs.</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 information needs to be configured/modified in PBX Settings->Online Storage -> SFTP module.

Regular Debugging

Capture Type: Ethernet Capture

Interface Type: LAN

Capture Filter:

Storage Location: Local

Start **Download**

Output Result

✓ Capture Success!
Done! Click on "Download" to download the captured packets.

S RTP Debugging

Enable S RTP Debugging:

Download




© 2023 Grandstream Networks, Inc.

Figure 344: Ethernet Capture

The capture packets can be stored locally and downloaded for analysis. However, if the user is diagnosing a randomly-occurring issue, he/she can run a continuous packet capture which can be limited by the size of the packet capture and the number of packet capture instances

Important

When the maximum packet capture file size is reached, a new packet capture file will be created. When the maximum number of capture files number is reached, then the UCM will delete the oldest file created file and replace it with the new one

| | |
|---|---|
| Capture Type | <p>Ethernet Capture: Gets a packet capture of all network traffic going through the device.</p> <p>WebSocket Capture: Gets a packet capture of WebSocket protocol. Mainly used for troubleshooting Wave Web calling and conferencing issues.</p> |
| 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 | <ul style="list-style-type: none"> • 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 UCM. File formats supported are FAT32 and ExFat. |
| Save to External Storage | <p>When or more external storage units are connected to the UCM6300 series, the user will be able to pick which one to use.</p> <p>Note: This option is available only when you choose "External Storage" as the storage destination of the capture trace.</p> |
| 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 | <p>This option appears only when "External Storage" or "SFTP" options are selected.</p> <p>Define the packet capture size, the option available are: 50MB, 100MB, and 200MB.</p> |
| Number of Packet Capture | Define the maximum number of the packets captured. The available options are 5, 10, and 20 packets. |
|  | Start capturing network traffic. |
|  | Stop capturing network traffic. |
|  | 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.

Note

Capture files saved on external devices will now have "capture" prepended to file names.

IP Ping

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.

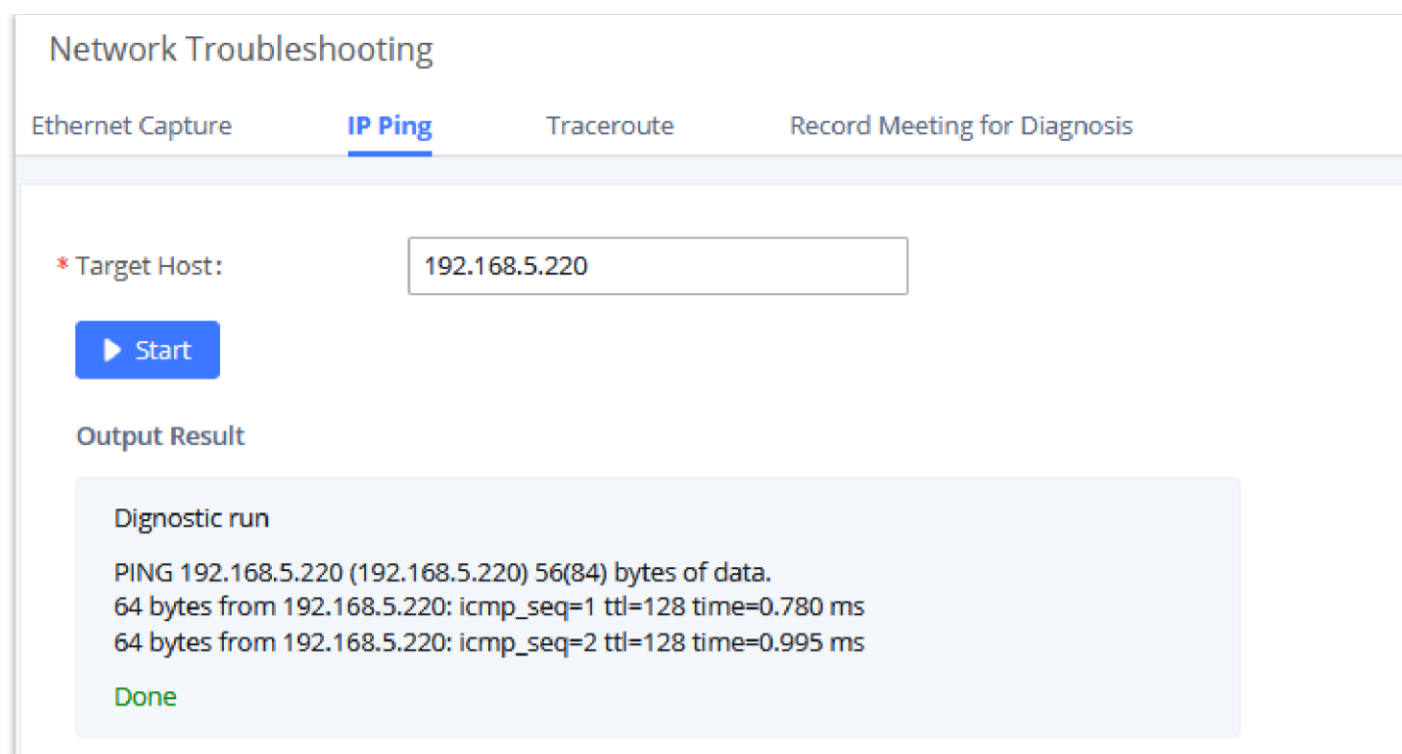


Figure 345: Ping

Traceroute

Enter the target host in host name or IP address. Then press “Start” button. The output result will dynamically display in the window below.

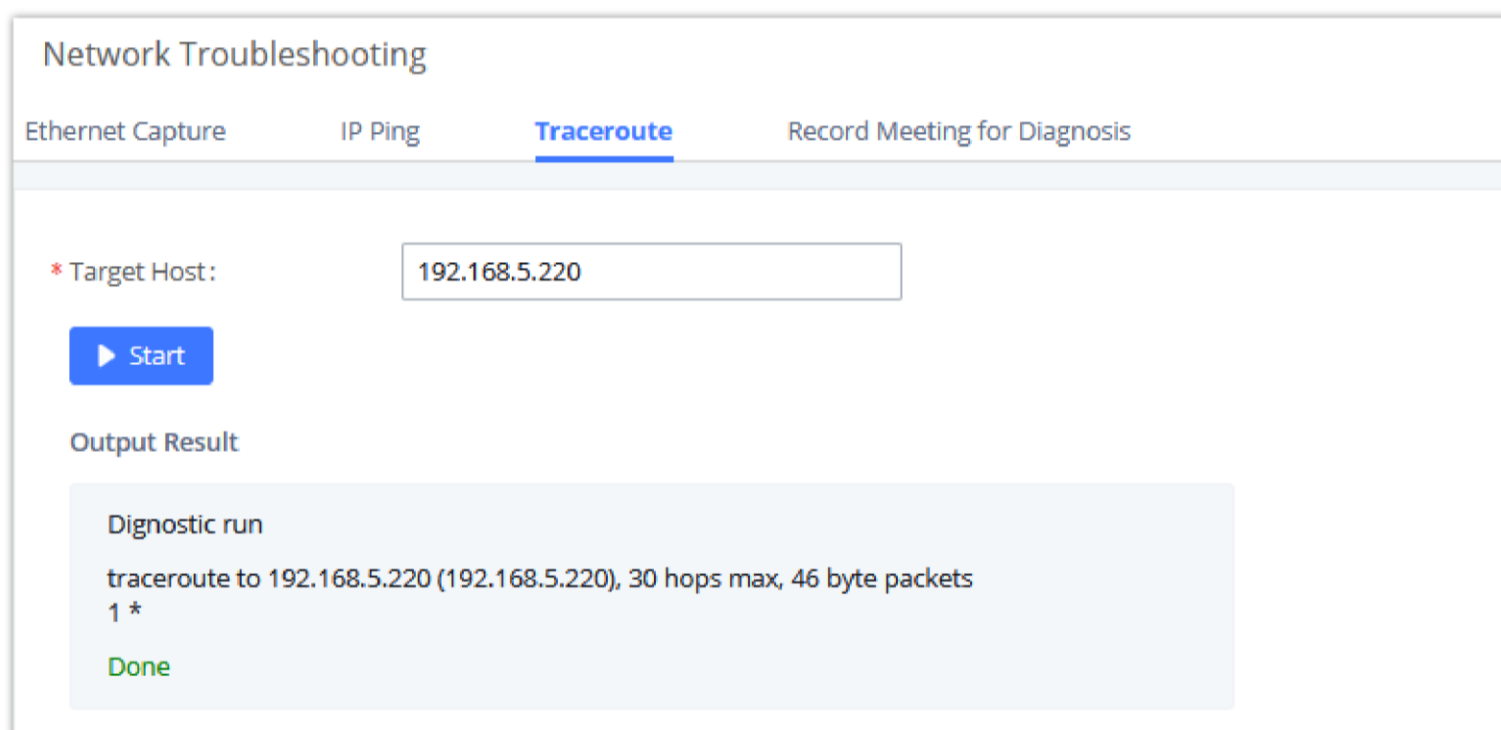


Figure 346: Traceroute

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.

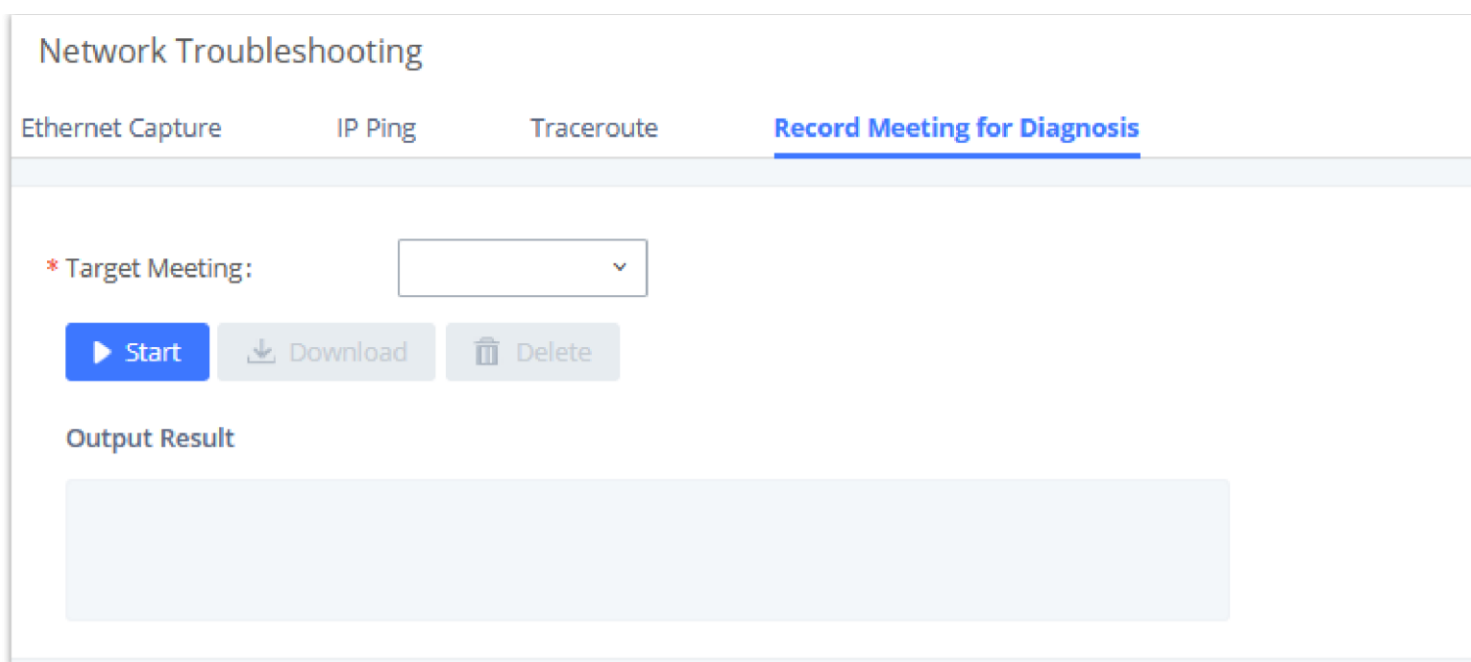


Figure 347: Record Meeting for Diagnosis

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.

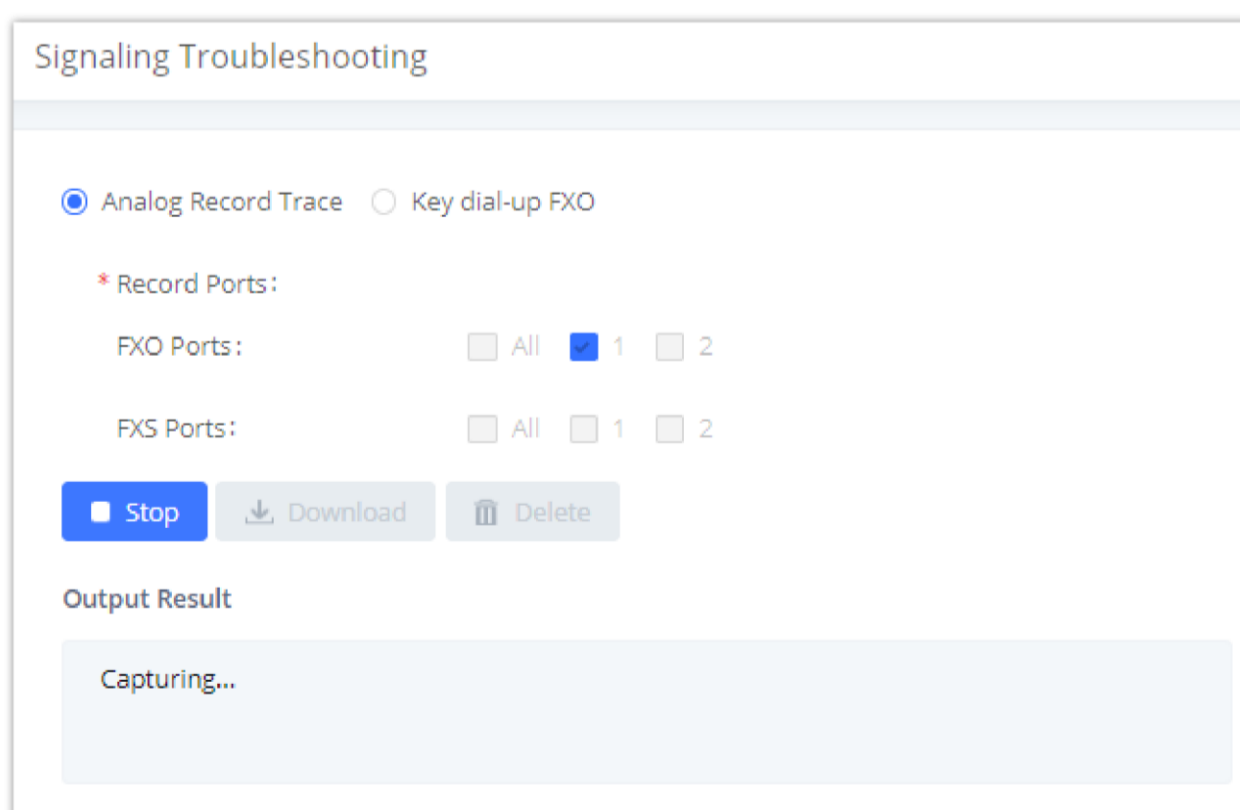


Figure 348: Troubleshooting Analog Trunks

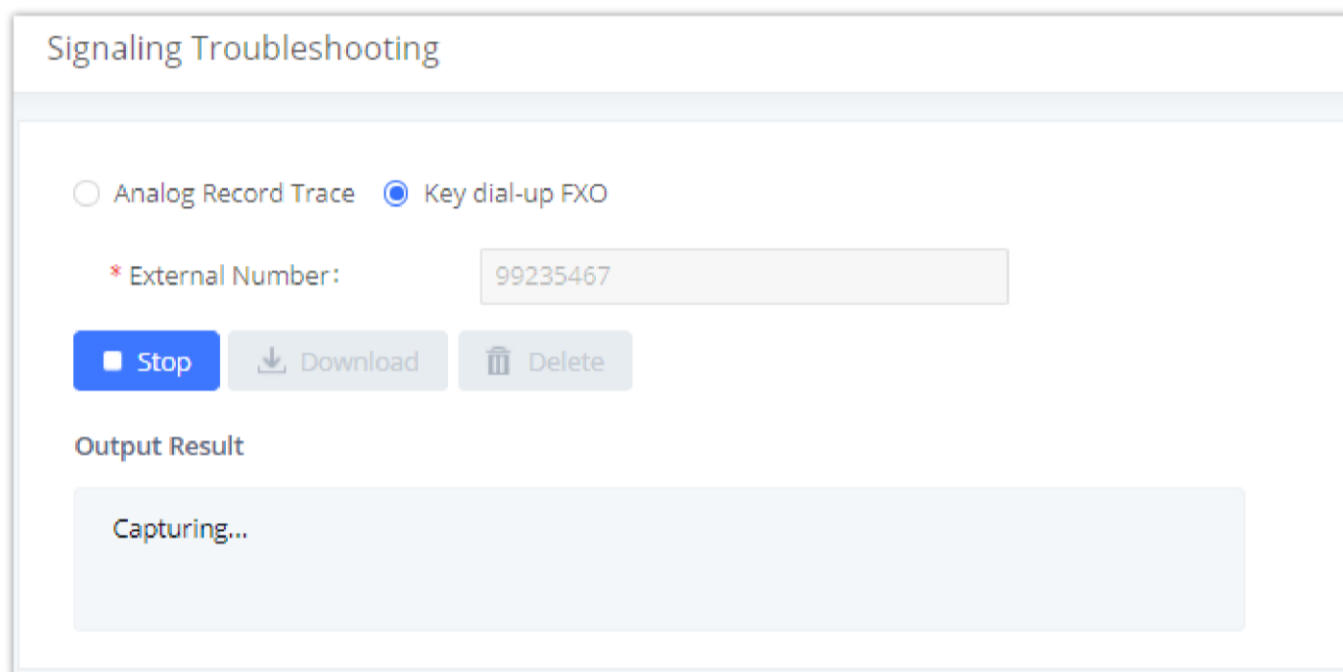
o

A key Dial-up FXO

Users can directly set a PSTN number on the “**External Extension**” text box to troubleshoot issues related to the analog trunk easily, the following steps shows how to use this feature:

1. Configure analog trunk on UCM, including outbound route.
2. Enter a reachable external number in “**External Extension**”.
3. Press “**Start**” button. The call will be initiated to the external number.
4. Answer and finish the call before pressing “**Stop**” button.

The trace will be available for analysis to download after output result shows “Done! Click on Download to download the captured packets”.



The screenshot shows a web interface titled "Signaling Troubleshooting". It features two radio buttons: "Analog Record Trace" (unselected) and "Key dial-up FXO" (selected). Below this is a text input field labeled "* External Number:" containing the value "99235467". There are three buttons: a blue "Stop" button, a "Download" button with a download icon, and a "Delete" button with a trash icon. Underneath is a section titled "Output Result" with a light blue box containing the text "Capturing..."

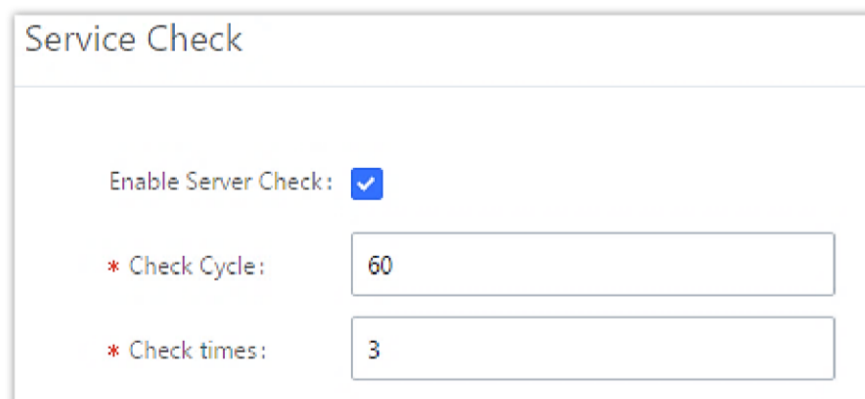
Figure 349: A Key Dial-up FXO

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.



The screenshot shows a configuration panel titled "Service Check". It includes a checkbox for "Enable Server Check:" which is checked. Below it are two text input fields: "* Check Cycle:" with the value "60" and "* Check times:" with the value "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.



Figure 351: 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 1.0.21.9

- 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 Meetings feature. [[Onsite Meeting](#)]
- Added ability to customize extension call waiting tone [[General Call Prompt Tones](#)]
- Updated Zoho CRM authentication process [[Zoho Telephony](#)]
- {VM_DATE} date value format has been changed to MM/dd/yyyy hh:mm:ss from DDD yyyy MMM hh:mm:ss. [[Configure Fax/T.38](#)] [[Voicemail Email Settings](#)]
- Added Device Name \${DEVICE_NAME} variable to Alert Events and Emergency Calls email templates
- Added Geolocation header support [[Emergency Location Mapping](#)]
- Added P-Called-Party-ID header option to the *Add/Edit Extension -> Features* page [[Create New SIP Extension](#)]
- Added *Allow Operator Panel Monitoring* extension option to toggle whether the Operator Panel can monitor the extension. [[Create New SIP Extension](#)]
- Added *Basic* extension export option [[Export Extensions](#)]
- *Allow Call-barging Extension List* option changed to *Call Monitoring Whitelist* [[Create New SIP Extensions](#)] [[Create New IAX Extension](#)]
- Added *Silence Suppression* option to *Extensions/VoIP Trunks* page [[Create New SIP Extension](#)] [[VoIP Trunk Configuration](#)]
- If a storage device is full, the UCM will mark it as unavailable and automatically change file storage path to the next available location based on the *Storage Path Priority*. Previously, UCM would change the file storage path to its own local storage if external storage was full. [[File Manager](#)]
- Added new commands related to call queue and Wave [[API Configuration Parameters](#)]
- Added support for multiple API (new) users [[API Configuration Parameters](#)]
- Added the *Default Certificate Auto Renewal* option. If enabled, the default browser certificate will be automatically renewed after 398 days (the max certificate validity period of Chrome, Firefox, and Safari browsers). User-defined certificates are not affected. [[HTTP Server](#)]
- Added ability to sync local IM data to Cloud IM [[Cloud IM Service](#)]
- Added ability create custom IVR key presses [[Custom Key Event](#)]
- Added *Chat Data from Endpoint* option to the Maintenance -> System Cleanup/Reset -> Cleaner page. If enabled, this option will clean out chat data from Wave clients at the same time as the UCM's server-side automatic/manual cleaning of chat data. [[Cleaner](#)]
- Added support for meeting room passwords. However, meetings cannot be scheduled for rooms with meeting password enabled. [[Room](#)]
- Meeting kick warning interval has been changed from 30 mins to 20 mins. Note: This kick warning will only play when there is only 1 person in a meeting room, and if they do not opt to stay in the meeting room after the warning, they will be removed from the meeting room after 5 minutes.
- ARP will now be used instead of ping to check NAS connectivity.
- Upgrade logs will now contain firmware version information.
- Queue chairmen can now log out dynamic agents
- Added option to automatically reset user/Wave password upon check-in/check-out. [[Local PMS](#)]
- Added option to clear Wave chat history automatically upon check-in or check-out. [[Local PMS](#)]
- Added Local PMS functionality [[Local PMS](#)]
- Check-out will no longer reset the "Skip Voicemail Password Verification" extension setting

- Added ability to assign two extensions to a room [[Room Management](#)]
- Added option to clear scheduled wakeup calls on both check-in and check-out. [[Local PMS](#)]
- Added the ability to change the default call privilege of a room. A room's privilege will be reset to this value after a guest checks out of it.
- Added support for stereo audio recording [[General Settings](#)]
- Added option to route calls based on a caller's Diversion header value [[Inbound Rule Configuration](#)]
- Added ability to control whether to use failover trunks based on the call response codes [[Failover Trunk Toggles](#)]
- Added support for H.264 with multiple payload types in SDP
- When receiving an INVITE with no SDP, following INVITEs with SDP will offer H.264 1080p resolution by default.
- In the scenario where an inbound external call is forwarded from an extension to an external number, the Contact header will now use the CID of the forwarding extension instead of the caller's CID.
- Removed *External Device Usage Threshold* option. If a connected NAS has only 1GB remaining available storage space, it will be considered unavailable and trigger the external disk usage alert. [[NAS](#)]
- Added *User Endpoint Access History* page [[User Endpoint Access History](#)]
- Added User Portal/Wave privilege control [[User Portal/Wave Privilege](#)]
- *Dial Trunk* option has been renamed to *Dial External Number* and moved to the *Dial Other Extensions* section
- The Wave Welcome email will now use the port number configured in System Settings->HTTP Server->Wave Settings->Port if the Wave Settings->External Host value is not a RemoteConnect address or does not contain a port number.
- Added links to relevant online documentation to various pages of the UCM webUI.
- Added Phonebook VMPK mode to GRP261x template
- Added Firmware tab for improved firmware management [[Firmware](#)]
- Added ability delete downloaded base model templates in the Model Update page
- Added ability to search for templates via the device model name
- Added ability to select either LAN1 or LAN2 to scan for devices on when using dual network method

Firmware Version 1.0.17.11

- Several system process optimizations

Firmware Version 1.0.17.8

- Updated python version to 3.8 and related processes.
- Improved speed of applying changes
- Updated lighttpd version to 1.4.61.
- The Privilege Name field now supports parenthesis ().
- The Contacts page has been moved to its own category in the sidebar.
- Added <https://www.zohoapis.in> option to CRM Server Address list.
- Added Channel Path option for accessing specific IP camera channels via URL. [[Device Management](#)]
- Improved alert email sending process.
- Updated Remote Registration email template.

- Emergency calls will no longer be restricted by the RemoteConnect call limit.
- The default highest priority codec is now G.722.
- Added Remote Extension Privilege Update feature code and Remote Extension Privilege Update Whitelist field to allow specified users to remotely change extensions' privileges. [[Feature Codes](#)]
- Automatic file migration after file storage path failure to the next storage location in the storage priority path.
- Users can now customize the storage path priority for recordings, and IM files. [[File Manager](#)]
- FXO FSK CID detection now uses spandsp.
- If SIP extensions synced from UCMs are deleted on GDMS, they will no longer be synced again.
- If HA is enabled, the HA cluster IP address will now be provisioned as the config server to endpoints instead of the active UCM's IP address.
- Added support for configuring inbound route blacklist via HTTPS API.
- If dialing into a Dial by Name directory, the call will end automatically after failing 3 times.
- Added Server Type option to the LDAP Server→LDAP Phonebook→Phonebook Download Configurations page. Users can select between LDAP and Active Directory. [[LDAP Server](#)]
- Added Department field to LDAP phonebook contacts. [[LDAP Server](#)]
- Added meeting room extensions to LDAP phonebooks. [[LDAP Server](#)]
- External Contacts created from the Contacts page will now be added to the system's internal LDAP phonebook. [[LDAP Server](#)]
- Added Remote Login tab to the Maintenance→Login Settings page. [[Maintenance](#)]
- Created new Meetings Settings page under the Multimedia Meetings page and moved several meeting-related options to it. [[Multimedia Meeting](#)]
- Regular meeting participants can now invite other members to join the meeting by dialing 1 if "Allow User Invite" is enabled. [[Multimedia Meeting](#)]
- Meetings will become "Pending" after rescheduling.
- Pending meetings are now sorted by start time by default.
- Added the Allowed to Override Host Mute option to the Edit Meeting Room and Schedule Meeting pages to allow participants to unmute themselves even after the meeting host mutes them. [[Multimedia Meeting](#)]
- Added support for user authentication. [[OpenVPN](#)]
- Operation Log entries will now contain the IP address and location information from which the operation originated. [[Operation Log](#)]
- Added option Automatically Clear Wakeup Calls for deleting scheduled wakeup calls after either guest check-in and check-out. [[PMS Features](#)]
- Users can now dial the Update PMS Room Status feature code, the maid code, and the room status code all at once to change room status. [[PMS Features](#)]
- Added a Scan button to manually retrieve the list of recordings on external storage. The UCM automatically displays up to 5000 recordings on attached external storage, but pressing this button will allow the UCM to display more. [[Recording Files](#)]
- Added ability to batch delete cloud storage files.
- If IP endpoints cannot connect to the GDMS TURN server via UDP, UCM will use TCP to connect them.
- Added Trunk Registration Period (s) option to SIP Settings->Misc. [[SIP Settings](#)]
- Added option Special Attributes to the Extension/Trunk→VoIP Trunks→Edit SIP Trunk→Advanced Settings page. If enabled, the following attributes will be included in the SIP SDP: ssrc, msid, mid, ct, as, tias, record. Enabling this may cause compatibility issues with non-Grandstream devices. [[VoIP Trunk Configuration](#)]
- Added CEI msid for audio calls.

- Added trickle-ice param to SIP OPTION's 200 OK.
- profile-level-id will be added to 200 OK when receiving INVITEs without SDP.
- Added ability to import/export speed dials. [[Speed Dial](#)]
- Improved processes to avoid duplicate alerts for the following events: Registered SIP Trunk failed, Local Disk Usage and External Disk Usage.
- Separated Allow Deletion of CDR and Recordings option to Allow Deletion of CDR and Allow Deletion of CDR Recordings. [[User Management](#)]
- Added the Call Waiting option to the User Portal.
- Added support for voicemail message seeking. When listening to voicemail, users can press star (*) to rewind 3 seconds or pound (#) to fast forward 3 seconds. [[Voicemail](#)]
- Added Line Selection Strategy option for Trunk Groups. [[VoIP Trunks](#)]
- Changed register trunk Username field name to Trunk Registration Number. [[VoIP Trunks](#)]
- [Web] General web UI improvements
- [Web] Added Help option under the username dropdown menu that will redirect to the UCM6300 Series FAQ.
- [Web] Updated some tooltips.
- [Web] Optimized search functionality
- [Zero Config] Added GMT+2:00 (Israel) option to Time Zone drop down list in all Zero Config pages.
- [ZeroConfig] Added support for WP22 and WP825 model templates.

Firmware Version 1.0.15.13

- Added SNMP monitoring feature. [[SNMP](#)]
- Added support to configure the time of a holiday. [[Holiday](#)]
- Added ability to determine the maximum total call duration per trunk for outbound calls. [[VoIP Trunk Configuration](#)]
- Added contact viewing privilege (independent from Department Contact Privilege). [[Contact Management](#)]
- Added support for agent ID announcement. [[Configure Call Queue](#)]
- Added support for Service Level Agreement for Call Queue. [[Service Level Agreement](#)]
- Added support for changing the Meeting room's name. [[Room](#)]
- Added WebRTC Trunk feature. [[WebRTC Trunks](#)]
- Extension data cleaning has been improved. [[Search and Edit an Extension](#)]
- Added support for SRTP Crypto Suite. [[VoIP Trunk Configuration](#)]
- STIR/SHAKEN has been improved. [[STIR/SHAKEN](#)]
- Added support for displaying the extension that initiated an emergency call in the emergency email notification. [[EMERGENCY](#)]
- Added support for collecting ICE candidates when an RTP connection is requested. [[RTP Settings](#)]
- Flood Attacks and Network Traffic Storm alerts have been added to the Alert Events List. [[Alert Events List](#)]
- Added support for Network Port Traffic Control for the ports of the UCM63xx Audio Series. [[Network Settings](#)]
- Added Support for limiting the frequency of calls that can be made in a period of time. [[Create New SIP Extension](#)]
- Added support for storing the local chat files in the GDMS. [[File Manager](#)]
- UCM RemoteConnect plan expiry screen has been improved.

- GDMS Cloud Storage Space details can now be viewed in the RemoteConnect menu. [[GDMS Cloud Storage Space](#)]

Firmware Version 1.0.13.9

- Added option to enable/disable DND status remotely for an extension. [[CALL FEATURES](#)]
- Added local proxy in IM settings. [[Cloud IM Service](#)]
- Added support for enabling/disabling auto audio recording for meeting. [[Auto Record](#)]
- Added privilege management for contacts. [[Privilege Management](#)]
- Improved fail2ban blacklist display. [[Fail2ban](#)]
- Improved email template for scheduling meeting. [[Email Templates](#)]
- Contacts sync-up between UCM and end points (wave/IP phones). [[LDAP Settings](#)]
- Added ability to specify DOD number based on outbound route. [[Outbound Routes DOD](#)]
- Fixed an issue where updating model templates will result in deleting the existing ones.
- Added support to use TURN Relay as an option to allow hosts behind NAT firewalls to communicate. [[VoIP Trunk Configuration](#)]

Firmware Version 1.0.11.10

- Added Operator Panel. [[OPERATOR PANEL](#)]
- Added time condition support for IVR key events. [[Key Press Event](#)]
- Added cloud IM abnormal alert event. [[Alert Events List](#)]
- Support setting to choose whether to play Follow Me.
- Add Fail2Ban whitelist comment information. [[Fail2ban](#)]
- Support Call Flip feature code. [[Feature Codes](#)]
- Added Multi-Factor Authentication for UCM login. [[Multi-Factor Authentication](#)]
- Added support for IoT device management. [[DEVICE MANAGEMENT](#)]
- Added option to enable and disable password-less remote access. [[UCM RemoteConnect Plan Settings](#)]
- Added option “Stop Ringing”. [[Stop Ringing](#)]
- Add option “Email Missed Call Log”. [[Email Missed Call Log](#)]
- Added remark for UCM system status. [[Remark](#)]
- Added option to enable and disable virtual queue call back keys settings. [[Virtual Queue Callback Key Setting](#)]
- Added Contacts section. [[Contacts](#)]
- Add option “Security Mode” for NAS settings. [[Security Mode](#)]
- Removed display for consumer users in user management page. [[User Management](#)]
- Support custom ignoring 180 response after 183 response. [[SIP Settings/MISC](#)]
- Added option to enable IPv6 for HA settings. [[Enable IPv6](#)]

Firmware Version 1.0.9.10

- Added Support for import/export Zero Config. [[Global Policy](#)]
- Added support for enable Wave and Sync Contact under the extension. [[Create New SIP Extension](#)]

- Added support for Custom time supplement time conditions. [[Create New SIP Extension](#)]
- Added support for Call Restriction. [[RESTRICT CALLS](#)]
- Added support for Queue Metrics. [[QUEUE METRICS](#)]
- Added support for CDR API add whitelist. [[Permitted IP \(s\)](#)]
- Added support for Call queue satisfaction survey. [[Queue Statistics](#)].
- The old API Configuration is reopened for use. [[HTTPS API Settings \(Old\)](#)]
- Custom permissions support the function of deleting CDR and recording files. [[Custom Privilege](#)]
- Added support to adjust recording file storage path. [[File Manager](#)]
- Added support to High Availability feature on UCM6300A series. [[HA](#)]
- Paging/Intercom supports delayed paging. [[Configure Paging/Intercom](#)]
- UCMRC remote service diagnosis. [[Figure 239: 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.