

Grandstream Networks, Inc.

CloudUCM – User Manual



INTRODUCTION

CloudUCM is a cloud PBX solution that provides a scalable and secure business communication and collaboration platform with powerful features and integrations that enable teams to be more productive than ever before. This Cloud PBX unifies all business communication into one centralized solution that provides voice and video calling, meetings, chat, data, analytics, mobility, surveillance, facility access, intercoms, and more. CloudUCM supports all SIP endpoints and the Wave app for desktop, mobile, and web, allowing teams to communicate and collaborate from anywhere on nearly any device. This scalable solution can be easily expanded at any time without the need for extra equipment, provides enterprise-level security and reliability, and supports powerful third-party integrations and expansions. By providing a state-of-the-art suite of communication and collaboration features, bank-grade security, advanced customization, and a variety of plan options, CloudUCM is the ideal PBX solution for small-to-medium-sized businesses, retail, hospitality, and residential deployments.

Note

To see the plans offered in CloudUCM in detail, please refer to the following link: <https://ucmrc.gdms.cloud/clouducm/plans>

TECHNICAL SPECIFICATIONS

The following table summarizes all the technical specifications, including the protocols/standards supported, voice codecs, telephony features, and languages for the CloudUCM.

Supported UC Endpoints and Client Devices	Support all SIP endpoint Wave app for desktop (Windows 10+, macOS 10+), web (Firefox, Chrome, Safari, Edge, Opera) and mobile (Android & iOS) Google Chrome extensions.
Call Features	Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, fax to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice conference, video conference, eventlist, feature codes, busy camp-on/ call completion, voice control, post-meeting reports, virtual fax sending/receiving, email to fax
Built-in SBC	Free All plans default to supporting built-in SBC services to protect CloudUCM systems from external attacks
Call with WebRTC Trunk	Supports mobile and desktop web browsers: Chrome, Edge , Safari, Firefox, Opera Supports mobile application which built-in WebRTC WebView, such as Whatsapp, Facebook, Weixin and more
Collaboration	Audio and Video Meetings/Conferences, Instant Messaging and Group Chats with End-to-End Encryption, File Sharing, Screen Sharing, In-Meeting Chat, Voice Detection, Meeting Recording, Polls, Surveys, Message status, Advance Whiteboard with Multiplayer Annotation, Meeting Assistant, Onsite Meeting Room Scheduling, and more
Customer Service Support	• Supports integration with third-party customer service platforms, including Whatsapp and Telegram. And built-in live chat • Includes a built-in live online web chat platform to provide customer service • Provides a web link that can be added to any web page or any browser that supports WebRTC • Compatible with computers, mobile browsers, and mobile apps

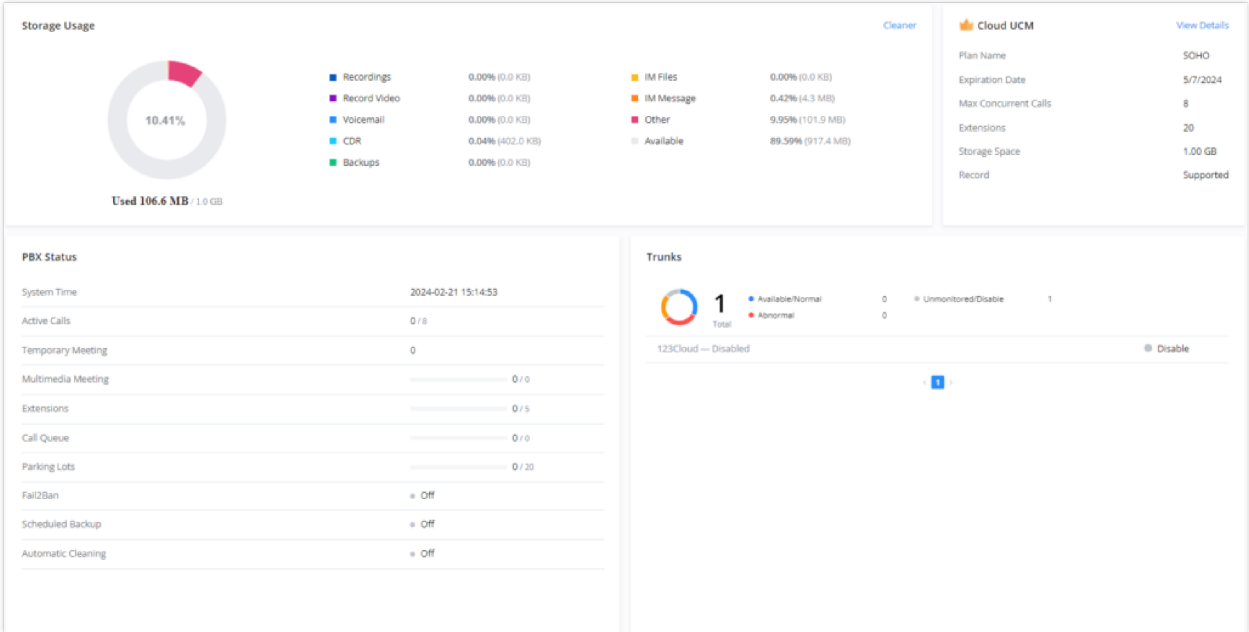
Customer Relationship Management (CRM)	Supports integration with ACT!, Bitrix24, Freshdesk, Hubspot, Salesforce, Sugar, Vtiger, Zendesk, Zoho, Dynamics 365, and more.
Call Center	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/work-load, in-queue announcement.
Customizable Auto Attendant	Up to 5 layers of IVR (Interactive Voice Response) in multiple languages
Property Management System (PMS)	Local PMS Supports integration with char pms.
Cloud Storage	Included, varies by plan, additional add-ons available.
CloudUCM App Store	Supports more than 20+ customized applications, with new apps being regularly added. ● CRM add-ons ● Google Drive and Office 365 ● Whatsapp and Telegram ● Hotdesking (coming soon)
Microsoft Integration	Supports integration with Microsoft Teams (via TeamMate), Outlook, AD Contact, and Office 365
Computer Telephony Integration	CTI Mode to Control GXP, GRP, GXV, GHP Series' IP Phones
Wired and Bluetooth Headset	Supports docking with different types of headphones Supports Microsoft Teams certified Headsets, supports phone call control
High Availability (HA)	Amazon Web Services (AWS) provides 99.99% service guarantee HA between UCM6300 Series IP PBX and CloudUCM (coming soon) HA between multiple CloudUCM systems (coming soon)
Firmware Upgrade and Provision	Supported by Grandstream Device Management System (GDMS), a zero-touch cloud provisioning and management system, GDMS provides a centralized interface to provision, manage, monitor and troubleshoot Grandstream products.
IP Cameras, Intercom and Door Access Integration	Supports Grandstream GSC Series IP Cameras and Intercom/Public Address devices, supports GDS Series Door Access Solutions Supports third party devices, including Hikvision, Dahua, and more
API and SDK	Full CGI API available for third-party platform and application integration Wave add-in SDK Wave Android and iOS SDK Wave H5 Embedded for MAC/Windows application
Multi-Language Support	● Web User Interface: 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 ● Customizable language pack to support any other languages
Security	Frequency Restriction, Fail2ban, Ping Defense, Ping of Death, SYN-Flood, Remote Login Interception, Multi-factor Authentication, SMS Login Authentication
Network Protocols	SIP, TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, HTTP/HTTPS, STUN, SRTP, TLS, LDAP, IPv4/6

Internet Protocol Standards	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028. RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 4582, RFC 4583, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550
DTMF Methods	In-band audio, RFC 2833, and SIP INFO
Transmission Encryption	SRTP, DTLS-SRTP, TLS, HTTPS
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711, NetEQ, FEC 2.0, jitter resilience up to 50% audio packet loss
Voice and Fax Codecs	Opus, G.711 A-law/U-law, G.722, G722.1 G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38
Video Codecs	H.264, H.263, H263+, VP8
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Administration	Call Detail Record, event alert and SMS notifications, event logs, export import extensions, feature codes, LDAP, feedback system, PBX monitor, resource monitor, system prompt, user permission, web-based control panel, user portal, trunk cluster, voice prompt customization, firewall, Fail2ban, IP blacklist, Syslog, gateway and endpoint provisioning, Wave permissions (<i>deploy & configure Wave Desktop, installations en masse, pre-install Wave Add-ons for extensions, manage Wave feature access permissions</i>), local backup

SYSTEM STATUS

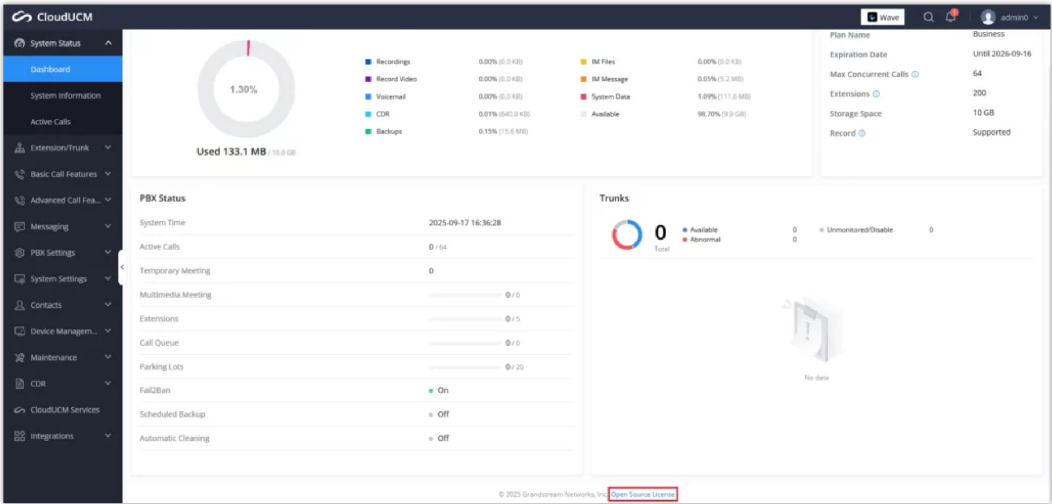
Dashboard

- Storage Usage
- CloudUCM
- PBX Status
- Trunks



Open Source License

As shown in the screenshot below, the open source license for CloudUCM is available at the bottom of the page.



CloudUCM Open Source License

System Information

System Information	
General	Remark
System Information	
Model	CloudUCM
MAC Address	00:0B:82:07:00:37
Serial Number	3420070005
System Time	2024-02-21 15:17:17 UTC-01:00
Up Time	14day (s) 08:32:07
Version Information	
Wave Web	1.0.25.5
Program	1.0.24.23

System Information

System Information

General

Remark

Remark

CloudUCM Boston

Cancel

Save

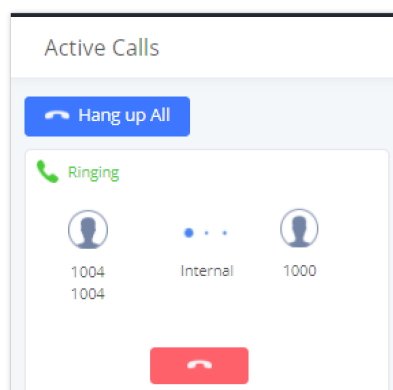
Remark

Active Calls

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

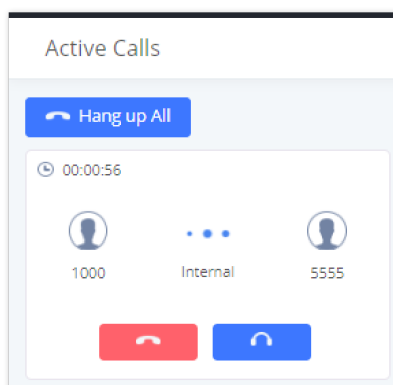
Active Calls Status

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



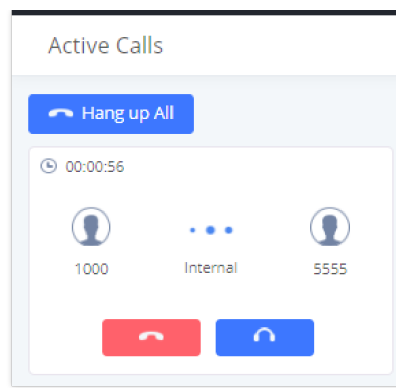
Active Calls Ringing Status

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

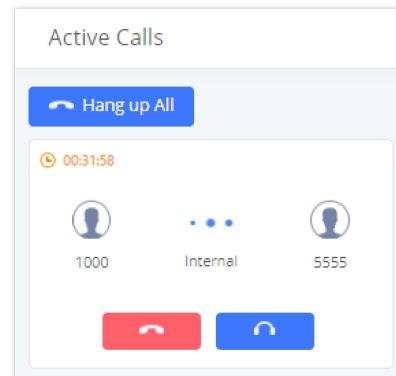


Active Call Established Status

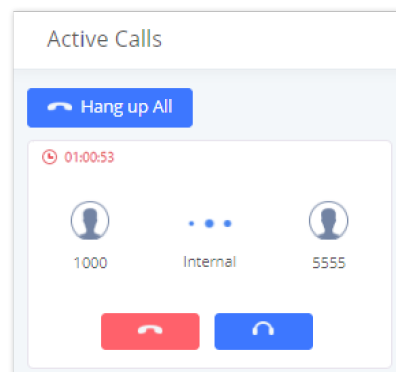
The gray color of the active call means the call time is less than half an hour. It means this call is normal.



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



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



Setup Wizard

When you log in to the CloudUCM Web GUI interface for the first time, the system will automatically start the setup wizard and expand the description.

The setup wizard guides users to complete basic configuration, such as administrator password modification, Email Delivery settings, timezone settings, extension settings, trunks and routes configuration, etc.

Setup Wizard

EXTENSION/TRUNK

Extensions

Create a New SIP Extension

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

Create a New SIP Extension

Extension options are divided into the following categories:

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

- **Follow me**
- **Advanced Settings**

The configuration parameters are as follows.

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Call Privileges	Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”. Note: Users need to have the same level as or higher level than an outbound rule’s privilege to make outbound calls using this rule.
SIP Password	Configure the password for the user. By default, a random secure password will be automatically generated. It is recommended to use this password for security purposes. Note: The password must contain at least one lower-case letter, one upper-case letter, one numeral, and one special character. The password must not contain an ascending or descending consecutive numeric sequence, or a consecutive sequence of the same number/letter.
Concurrent Registrations	The maximum endpoints which can be registered into this extension. For security concerns, the default value is 3. Note: When this option is set to “1(seize)”
Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
Disable This Extension	If selected, this extension will be disabled on the CloudUCM. Note: The disabled extension still exists on the PBX but cannot be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User/Wave 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 Number	Configure the phone number for the extension, user can type the related star code for the phone number followed by the extension number to directly call this number. For example, the user can type *881000 to call the mobile number associated with extension 1000.
Department	Configure the user’s department. The department can be configured in User Management->Address Book Management->Department Management. Job Title: The user’s department position.
Job Title	Enter the job title of the user of the extension.
Contact Privileges	
Same as Department Contact Privileges	When enabled, The extension will inherit the same privilege attributed to the department it belongs to.
Contact View Privileges	Select the privileges regarding the contact view in SIP endpoints and Wave.

Sync Contact	If enabled, this extension will be displayed in the CloudUCM and Wave contact list. If disabled, it will not be shown in the contact list, but Wave users will still be able to manually dial the extension number.
---------------------	---

SIP Extension Configuration Parameters→Basic Settings

SIP Settings	
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.
FECC	Configure to enable Remote Camera Management.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.
QoS	
Jitter Buffer	Select the jitter buffer method. ● Disable: Jitter buffer will not be used. ● Fixed: Jitter buffer with a fixed size (equal to the value of "jitter buffer size") ● Adaptive: Jitter buffer with an adaptive size (no more than the value of "max jitter buffer"). ● NetEQ: Dynamic jitter buffer via NetEQ.
Packet Loss Retransmission	Configure to enable Packet Loss Retransmission. ● NACK ● NACK+RTX(SSRC-GROUP) ● OFF
Video FEC	Check to enable Forward Error Correction (FEC) for Video.
Audio FEC	Check to enable Forward Error Correction (FEC) for Audio.
Silence Suppression	If enabled, the 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.
RTP Encryption	
SRTP	Enable SRTP for the extension. ● Disabled ● Enabled and Enforced ● Optional Note: By default, the SRTP is disabled.

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

SIP Extension Configuration Parameters→Media

Presence Status	
Presence Status	Select which presence status to set for the extension and configure call forward conditions for each status. Six possible options are possible: “Available”, “Away”, “Chat”, “Custom”, “DND” and “Unavailable”. More details at [PRESENCE].
Call Transfer	
Call Forward Always	Enable and configure the Call Forward Unconditional target number. Available options for target number are: • “None”: Call forward deactivated. • “Extension”: Select an extension from the dropdown list as CFU target. • “Custom Number”: Enter a customer number as a target. For example: *97. • “Voicemail”: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension. • “Ring Group”: Select a ring group from the dropdown list as CFU target. • “Queues”: Select a queue from the dropdown list as CFU target. • “Voicemail Group”: Select a voicemail group from the dropdown list as CFU target. • Custom Prompt: The call will be forwarded to a custom prompt. The default setting is “None”.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’. Notes: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time. • Office Time and Holiday could be configured on page System Settings > Time Settings > Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. Available options for target number are: • “None”: Call forward deactivated. • “Extension”: Select an extension from the dropdown list as CFN target. • “Custom Number”: Enter a customer number as a target. For example: *97. • “Voicemail”: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension. • “Ring Group”: Select a ring group from the dropdown list as CFN target. • “Queues”: Select a queue from the dropdown list as CFN target. • “Voicemail Group”: Select a voicemail group from the dropdown list as CFN target. • Custom Prompt: The call will be forwarded to a custom prompt. The default setting is “None”.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’. Notes: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period.

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

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	Enable and configure the Call Forward Unconditional target number. Available options for target number are: ● “None”: Call forward deactivated. ● “Extension”: Select an extension from the dropdown list as CFU target. ● “Custom Number”: Enter a customer number as a target. For example: *97. ● “Voicemail”: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension. ● “Ring Group”: Select a ring group from the dropdown list as CFU target. ● “Queues”: Select a queue from the dropdown list as CFU target. ● “Voicemail Group”: Select a voicemail group from the dropdown list as CFU target. ● Custom Prompt: The call will be forwarded to a custom prompt. The default setting is “None”.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’. Notes: ● “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. ● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time. ● Office Time and Holiday could be configured on page System Settings ☐ Time Settings ☐ Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. Available options for target number are: ● “None”: Call forward deactivated. ● “Extension”: Select an extension from the dropdown list as CFN target. ● “Custom Number”: Enter a customer number as a target. For example: *97. ● “Voicemail”: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension. ● “Ring Group”: Select a ring group from the dropdown list as CFN target. ● “Queues”: Select a queue from the dropdown list as CFN target. ● “Voicemail Group”: Select a voicemail group from the dropdown list as CFN target. ● Custom Prompt: The call will be forwarded to a custom prompt. The default setting is “None”.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’. Notes: ● “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. ● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time. ● Office Time and Holiday could be configured on page System Settings ☐ Time Settings ☐ Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. Available options for target number are: ● “None”: Call forward deactivated. ● “Extension”: Select an extension from the dropdown list as CFB target. ● “Custom Number”: Enter a customer number as a target. For example: *97 ● “Voicemail”: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension. ● “Ring Group”: Select a ring group from the dropdown list as CFB target. ● “Queues”: Select a queue from the dropdown list as CFB target.

	● “Voicemail Group”: Select a voicemail group from dropdown list as CFB target. ● Custom Prompt: The default setting is “None”.
CFB Time Condition	Select time condition for Call Forward Busy. The available time conditions ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’. Notes: ● “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. ● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time. ● Office Time and Holiday could be configured on page System Settings□Time Settings□Office Time/Holiday page.
Do Not Disturb	If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.
DND Time Condition	Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”. Notes: ● “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. ● Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time. Office Time and Holiday could be configured on page System Settings□Time Settings□Office Time/Holiday page.
DND Whitelist	If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported. ● Z match any digit from 1-9. ● N match any digit from 2-9. ● X match any digit from 0-9.
FWD Whitelist	Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported. ● Z match any digit from 1-9. ● N match any digit from 2-9. ● X match any digit from 0-9.
CC Settings	
Enable CC	If enabled, CloudUCM will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.
CC Mode	Two modes for Call Completion are supported: ● Normal: This extension is used as an ordinary extension. ● For Trunk: This extension is registered from a PBX. The default setting is “Normal”.
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 that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.
External Number	Set the external number to ring simultaneously. ‘-’ is the connection character that will be ignored. This field accepts only letters, numbers, and special characters + = * #.
Time Condition for Ring	Ring the external number simultaneously along with the extension based on this time condition.

Simultaneously	
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 Seamless Transfer	Any extensions on the CloudUCM 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 CloudUCM. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under Web GUI ☐ CDR ☐ Recording Files .
Skip Trunk Auth	● If set to “yes”, users can skip entering the password when making outbound calls. ● If set to “By Time”, users can skip entering the password when making outbound calls during the selected time condition. ● If set to “No”, users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If ‘Skip Trunk Auth’ is set to ‘By Time’, select a time condition during which users can skip entering 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 Settings	
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 valid range is from 1 to 20. The default value is 5.
Enable Auto-Answer Support	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
Call Waiting	Allows calls to the extension even when it is already in a call. This only works if the caller is directly dialing the extension. If disabled, the CC service will take effect only for unanswered and timeout calls.
Stop Ringing	If enabled, when the extension has concurrent registrations on multiple devices, upon incoming call or meeting invite ringing, if one end device rejects the call, the rest of the devices will also stop ringing. By default, it's disabled.
Email Missed Call Log	If enabled, the log of missed calls will be sent to the extension's configured email address.
Missed Call Type	If Email Missed Calls enabled, users can select the type of missed calls to be sent via email, the available types are: ● Default: All missed calls will be sent in email notifications. ● Missed Internal Call: Only missed local extension-to-extension calls will be sent in email notifications. ● Missed External Call: Only missed calls from trunks will be sent in email notifications.
Enable SCA	If enabled, (1) Call Forward, Call Waiting and Do Not Disturb settings will not work, (2) Concurrent Registrations can be set only to 1, and (3) Private numbers can be added in Advanced Call Features->SCA page.
Emergency CID	CallerID name and number that will be used when making emergency calls and receiving direct callbacks. If ELIN subnet mapping has been configured, and the extension is registered to a device in a mapped subnet, the configured ELIN will be used for CID number instead.
Language	Select voice prompt language for this extension. If set to "Default", the global setting for voice prompt language will be used.

SIP Extension Configuration Parameters→Features

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

SIP Extension Configuration Parameters→Specific Time

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

	● Follow Global Settings: Uses the language configuration defined under AI Settings. ● Automatic Recognition: Automatically detects the spoken language during the call. This is recommended when multiple languages are expected, though recognition accuracy may vary. ● Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy. <i>Note: This setting controls only the transcription behavior for this extension. It does not enable or disable AI services at the system level.</i>
--	--

SIP Extension Configuration Parameters > AI

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

SIP Extension Configuration Parameters→Wave Client

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

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

SIP Extension Configuration Parameters→Follow Me

Search and Edit Extension

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

Extensions

+ Add

Edit

Delete

Edit All SIP

E-mail Notification

More

Extension Number or Name

Search

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

< 1 >

Total: 5 30 / page Goto 1

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

Manage Extensions

◦ Status

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

- Green: Idle
- Blue: Ringing
- Yellow: In Use
- Grey: Unavailable (the extension is not registered or disabled on the PBX)

◦ Edit single extension

Click on  to start editing the extension parameters.

- **Reset single extension**

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

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

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 a NOTIFY reboot event to the device that has a CloudUCM extension already registered. To successfully reboot the user.

- **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 records. 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 CloudUCM can be exported to XLSX and CSV file formats. Click on the "Export Extensions" button and select the file type in the prompt below.

Status	Presence Status	Extension	Name
Unregistered	Available	1000	
Unregistered	Available	1001	
Unregistered	Available	1002	
Unregistered	Available	1003	
Unregistered	Available	1004	

Export Extensions

Export Basic Settings

Export Basic Information includes:

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

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

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

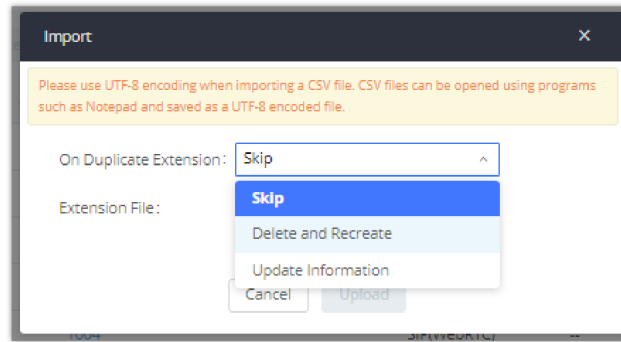
The exported CSV/XLSX file can serve as a template for users to fill in desired extension information to be imported to the CloudUCM.

Import Extensions

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

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

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



Import Extensions

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

- **Skip:** Duplicate extensions in the CSV/XLSX 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/XLSX 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/XLSX file has a different configuration for any options, it will override the configuration for those options in the extension.

5. Click on “Choose file to upload” to select a CSV/XLSX file from a local directory on the PC.

6. Click on “Apply Changes” to apply the imported file on the CloudUCM.

Example of a file to import:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	Extension	First Nam	Last Nam	Technolog	Enable Vo	CallerID N	SIP Passw	Voicemail	Skip	Voice Ring	Time	Auto Reco	SRTP	Fax Mode	Strategy	Local Sub	Local Sub	Local Sub	Local Sub	Local Sub	Local Sub	Local Sub	Local
2	1000	Bonnie	MacFarlar	SIP(WebR	yes	Pas0123!	660408	no		off	no	None	Allow All										
3	1001			SIP(WebR	yes	Pas0123!	623712	no		off	no	None	Allow All										
4	1002			SIP(WebR	yes	rY3s4jp	47962	no		off	no	None	Allow All										
5	1003			SIP(WebR	yes	gU2@m*\$	83232	no		off	no	None	Allow All										
6	1004			SIP(WebR	yes	rw8%008C	5187	no		off	no	None	Allow All										
7																							
8																							
9																							
10																							
11																							
12																							
13																							

Import File

Field	Supported Values
Extension	Digits
Technology	SIP/SIP(WebRTC)
Enable Voicemail	yes/no/remote
CallerID Number	Digits
SIP Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no

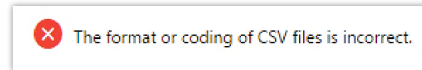
Field	Supported Values
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
DTMF Mode	RFC4733/info/inband/auto
Insecure	Port
Enable Keep-alive	Yes/no
Keep-alive Frequency	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

Field	Supported Values
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

Field	Supported Values
Seamless Transfer Members	Extensions allowed to seamless transfer

SIP extensions Imported File Example

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



Import Error

Extension Details

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

- **Extension:** This shows the Extension number.
- **Status:** This shows the status of the extension.
- **Presence status:** Indicates the Presence Status of this extension.
- **Terminal Type:** This shows the type of the terminal using this extension
- **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.

The image shows a 'More' dialog box with a close button (X) in the top right corner. Inside the dialog is a table with two columns: 'OPTIONS' and 'VALUE'.

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

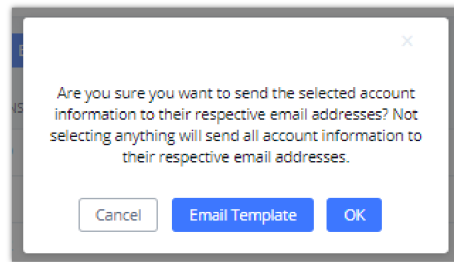
Extension Details

E-mail Notification

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

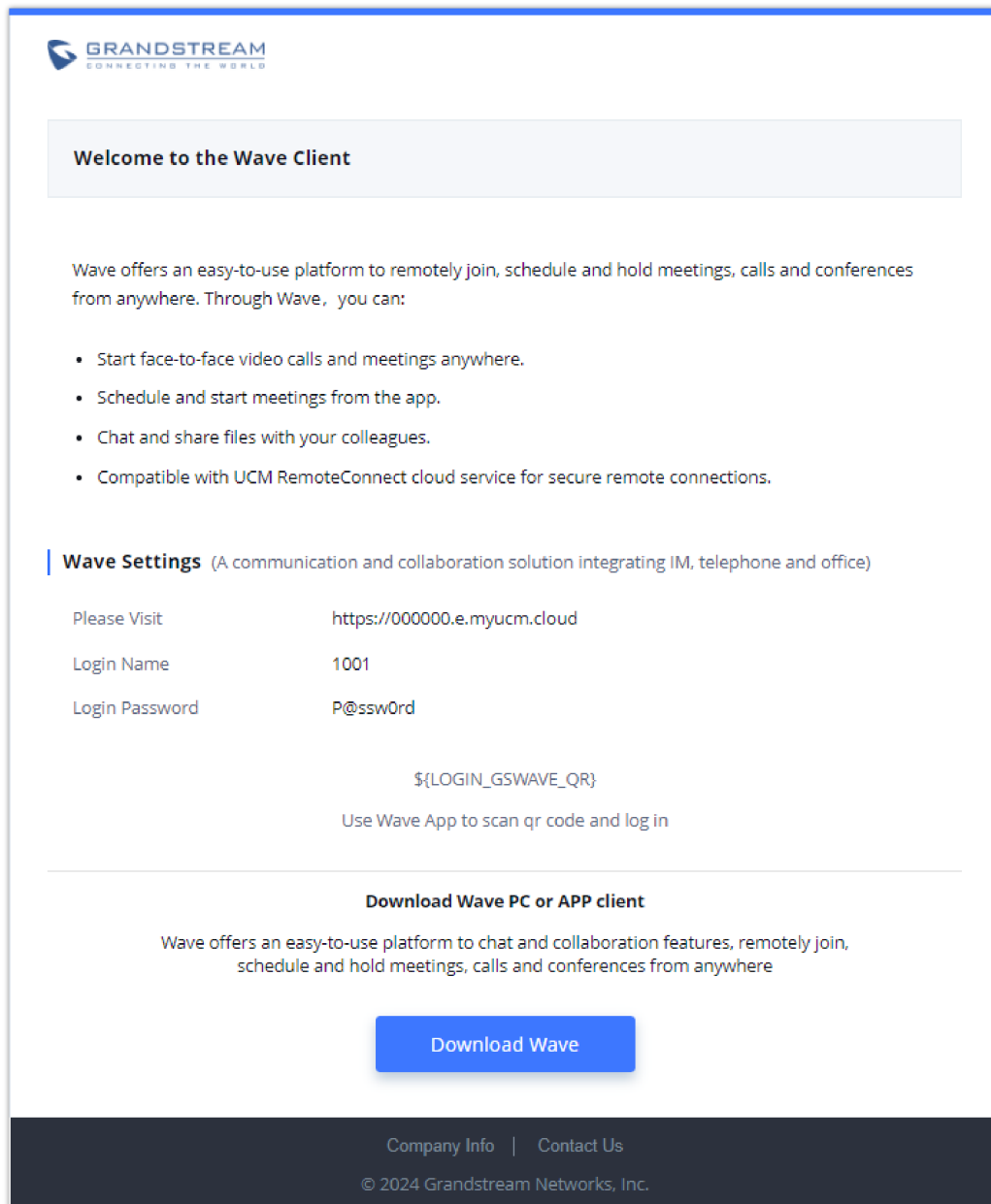
Notification”.

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



E mail Notification Prompt Information

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

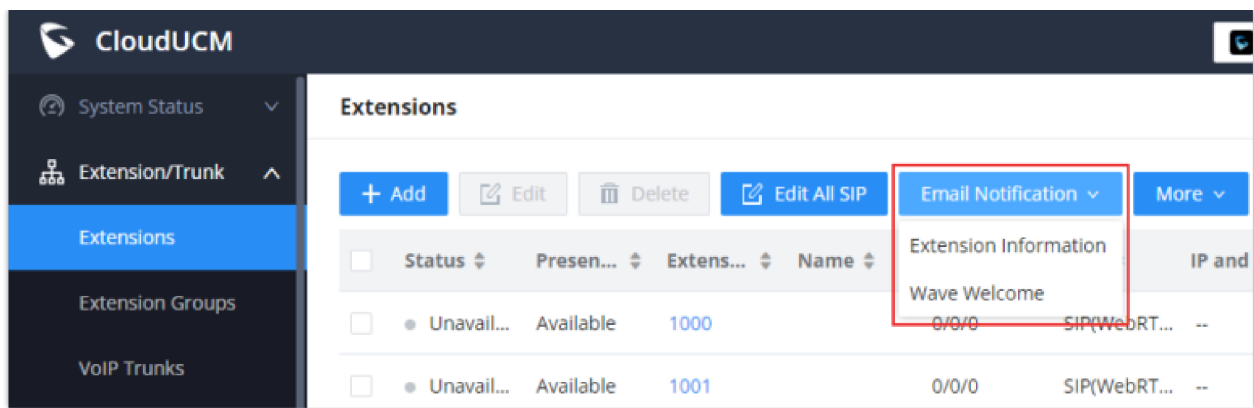


Wave Settings and QR Code

Important Note

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

The CloudUCM admin can also send “Extension Information” mail and “Wave Welcome” mail as the figure below shows



Send Email Notification

Multiple Registrations per Extension

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

This feature can be enabled by configuring the option “Concurrent Registrations” under Web GUI→**Extension/Trunk**→**Edit Extension**. The default value is set to 3 registrations. The maximum is 5 registration.

When the option “1(allowed to seize)” is selected, the UCM will allow newer registration attempts to seize the extension from a previously registered endpoint. To prevent this behavior, please select the option 1.

Extension Concurrent Registration

SMS Message Support

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

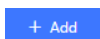
Extension Groups

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

Configure Extension Groups

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

- Click on



to create a new extension group.

- Click on



to edit the extension group.

- Click on



to delete the extension group.

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

Edit Extension Group

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

Using Extension Groups

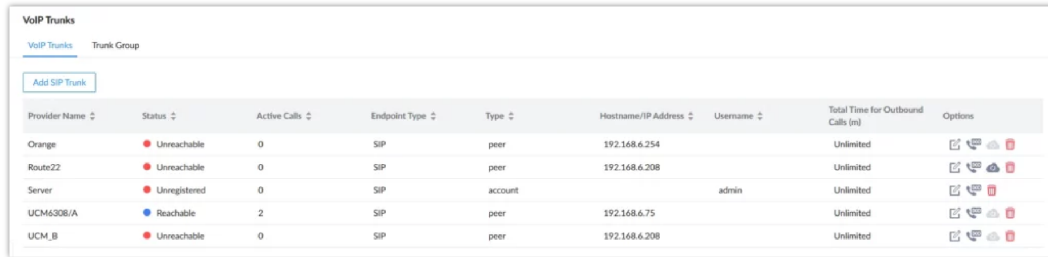
Here is an example where the extension group can be used. Go to Web GUI→**Extension/Trunk**→**Outbound Routes** and select “Enable Source Caller ID Whitelist”. Both single extensions and extension groups will show up for users to select.

Select Extension Group in Outbound Route

VoIP Trunks

VoIP Trunk Configuration

VoIP trunks can be configured on the CloudUCM under **Web GUI→Extension/Trunk→VoIP Trunks**.



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

VoIP Trunks Overview Page

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

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

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

Disable This Trunk	Check this box to disable this trunk.
Type	Select the VoIP trunk type. ● Peer SIP Trunk: A direct IP-to-IP connection between the PBX and another SIP server or device, without requiring registration. ● Register SIP Trunk: A trunk that requires the PBX to register with the SIP server or provider using credentials (username and password). ● Account SIP Trunk: A trunk where the PBX acts as the registrar, allowing remote devices or endpoints to register with it.
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.
Dedicated VLAN	After selecting the corresponding VLAN, the traffic related to the relay will go through the VLAN interface.
Transport	Select the transport protocol to use. ● UDP: if selected, then the option Enable UDP should be checked, under PBX Settings > SIP Settings > Transport Protocol. ● TCP: If selected, then the option TCP Enable should be checked under PBX Settings > SIP Settings > Transport Protocol.

	● TLS: The default Transport protocol.
Trunk Mode	Set the trunk mode for incoming calls. In certain scenarios, service providers do not include a domain in “To” SIP header. In other scenarios, the service providers do not accept SIP INVITE messages from a different port than 5060. The trunk mode options allow to resolve such issues. ● DID Access: When a domain is not included in “To” SIP header, the user can configure a DID which will be used to verify incoming calls. ● Port Access: Choose this option to allow outbound SIP traffic to be sent from port 5060. Choosing this option will change the port used to receive SIP requests for this specific trunk to 6040, this should taken into consideration when interconnecting two PBXs Note: This option is available only for Register Trunk and Peer Trunk when using UDP as transport protocol.
DID Number	Enter the DID number which will be included in the “To” SIP header. This option is mandatory when Trunk Mode is set to <i>DID Access</i> .
Server Address	Use the indicated address to register/peer trunks when configuring other PBXs with the CloudUCM.
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	Enable this setting if the PBX is using public IP and communicating with devices behind NAT. Note 1: This setting will overwrite the Contact header of received messages, which may affect the ability to establish calls when behind NAT. Consider changing settings in PBX Settings > SIP Settings > NAT instead. Note 2: If one is experiencing one-way audio issues, please check the NAT configuration and SIP/RTP ports in the firewall.
TEL URI	If “Enabled” option is selected, TEL URI and Remove OBP from Route cannot be enabled at the same time. If the phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. A “User=Phone” parameter will then be attached to the Request-Line and “TO” header in the SIP request to indicate the E.164 number. If set to “Enable”, “Tel:” will be used instead of “SIP:” in the SIP request.
Need Registration	Defines Whether to register the trunk on the external server. Enabled by default. Note: This option appears when the Type is set to Register Trunk.
Allow outgoing calls if registration fails	Disable to block outgoing calls if registration fails. If “Need Registration” option is disabled, this setting will be ignored. This option is enabled by default. Note: This option appears when the Type is set to Register Trunk.
Caller ID Number	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: From the user (Register Trunk Only) ☐ CID from inbound call (Keep Original CID Enabled) ☐ Trunk Username/CallerID (Keep Trunk CID Enabled) ☐ DOD ☐ Extension CallerID Number ☐ Trunk Username/CallerID (Keep Trunk CID Disabled) ☐ Global Outbound CID.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
Username	The number or username used for registration and authentication with the service provider. Note: You can configure this option for “Account SIP Trunk” and “Register SIP Trunk only”
Password	The password used for registration and authentication with the service provider. Note: You can configure this option for “Account SIP Trunk” and “Register SIP Trunk only”
Auth ID	Enter the Authentication ID for the “Register SIP Trunk” type.
AuthTrunk	If enabled, the PBX 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. Note: the recording functionality is not available on the startup plan.
Direct Callback	Allows external numbers the option to get directed to the extension that last called them. For Example, User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option “Direct Callback” is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.
Domain Connection Mode	If enabled, the following options will be automatically configured: TLS transport, From Domain , Enable Heartbeat Detection and ICE Support . Please ensure that the trunk host name is a GDMS-assigned address and supports TLS.
Monitor 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	This setting defines how long until the time allowed for outgoing calls is reset. ● 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.
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.
FECC	Configure to enable Far-end Camera Control
Silence Suppression	If enabled, the PBX will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint’s OPUS codec supports the reception of DTX packets, the PBX will send DTX packets instead.
SRTP	Enable SRTP for the VoIP trunk. The default setting is “No”.
SRTP Crypto Suite	SRTP encryption suite used by PBX for outbound calls. Priority is based on order of configuration.
ZRTP Encryption Mode	If disabled, the PBX will not support ZRTP encryption. Otherwise, ZRTP will be supported, and if the registered endpoint supports both ZRTP and SRTP, ZRTP will be used first.

Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
Include Special Attributes	If enabled, this trunk's SIP SDP will contain ssrc/msid/mid/as/tias/record attributes. These attributes may cause incompatibility when connecting to other devices and services.
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. If both Send PAI Header and Passthrough PAI Header are enabled, the following will occur: 1. On incoming calls, the Passthrough PAI Header value will be preferred for this PBX's 18x and 200 SIP messages to the caller. 2. On outbound calls, the Send PAI Header value will be preferred for this PBX's INVITE SIP message to the callee.
Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the PBX.
Send PANI Header	If checked, the INVITE sent to the trunk will contain P-Access-Network-Info header.
Send Diversion Header	Configure whether or not send Diversion header on the trunk call. Diversion header indicates that the call has been forwarded, it includes information about the call before the forwarding like the original callee and the type of forwarding. 1. Yes: Include the Diversion header. 2. No Deflection: Do not include Diversion header if the diversion reason is "deflection". "Deflection" is used as a diversion reason when calls are rerouted to an external number, either through Follow Me or on the inbound route level. 3. No: Do not include the Diversion header. The default settings is "Yes".
DID Mode	Configure to obtain the destination ID of an incoming SIP call from SIP Request-line, To-header, or Diversion-Header.
DTMF Mode	Configures the mode for sending DTMF. ● RFC4733 (default): DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream. Backward-compatible with RFC2833. ● Inband: DTMF is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs. List Item 2 ● 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.
Max Outgoing Calls	The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit.
Max Incoming Calls	The max allowed number of concurrent incoming calls through the trunk. Default is 0 (no limit).
Max Concurrent Calls	Configures the maximum allowed number of concurrent incoming and outgoing calls going through this SIP trunk. The default value is 0, and it indicates that no limit has been set.
Response to Blocked Call	Set the response code to the caller when the concurrent calls has reached the upper limit. 1. 480: Temporarily Unavailable 2. 486: Busy Here 3. 503: Service Unavailable The default setting is "480".

Sync LDAP Enable	Automatically sync local LDAP phonebooks to a remote peer (SIP peer trunk only). To ensure successful syncing, the remote peer must also enable this service and set the same password as the local PBX. Port 873 is used by default.
STIR/SHAKEN	Block Spam Calls. • Disabled: Disable STIR/SHAKEN. • Outgoing Attest: Enable STIR/SHAKEN attestation for outgoing calls. • 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.

Trunk Group

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

Trunk Group

Once the new trunk group is created and the SIP settings are configured, users can add multiple accounts within the configured SIP server by pressing the 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 Number / Password / AuthID + Add Username

Line Selection Strategy: Linear

AuthTrunk: ☐

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

Trunk Group Configuration

Disable This Trunk	Check this box to disable this trunk
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. Only TLS is supported, and TLS service must be enabled on the other end.
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.
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: Use lines in the list order for outbound calls. ● Round Robin: Use lines based on rotary line selection for outbound calls. Previously used lines will be remembered.
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.
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.
---	---

Direct Outward Dialing (DOD)

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

Example of how DOD is used:

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

Steps to configure DOD on the CloudUCM:

1. To set up DOD, go to CloudUCM 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. Enter a SIP trunk DID number in the “DOD number” field. In this example, ABC company has a total of 4 DID numbers. Enter the phone number used by the CEO here.
5. When adding extensions, you can choose whether to “Enable Strip” according to your needs. If it is enabled, you can configure the number (0-64) that will be stripped from the extension number before being added to the DOD number. For example, if the entered digit is 2, and the DOD number for extension 4002 is 1122, then dialing out from 4002, 112202 will be used as the caller ID (DOD).
6. Select an extension from the “Available Extensions” list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO’s extension. After making the selection, click on the button to move the extension(s) to the “Selected Extensions” list.

DOD extension selection

7. Click “Save” at the bottom.

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

VoIP Trunks > DOD: Grandstream

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

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

+ Add DOD
Import
Export
Filter

DOD	DOD NAME	EXTENSIONS	OPTIONS
+212555112233	DOD1	1002 1003 1005 1006	

Total: 1

<

1

>

10 / page

Goto

© 2023 Grandstream Networks, Inc.

Edit DOD

+ Add DOD

: Add a DOD.

Import

: Import DODs using a csv/xlsx file.

Export

: Export the DODs using a csv/xlsx file.

Filter

: Filter DODs by number or name.

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

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

DOD CSV file Template

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 CloudUCM supports creating WebRTC trunks to use exclusively with web applications, 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 :

GS_WebRTC_Trunk

Disable This Trunk :

☐

Auto Record :

☒

Enable Concurrent Call Threshold :

☒

* Incoming Concurrent Call Threshold :

150

WebRTC Inbound Link Address :

Automatically generated after saving

Create WebRTC Trunk

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.

Outbound Routes

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

Configuring Outbound Routes

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

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

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

To manage outbound routes:

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

Caller ID Mode	Determines which Caller ID numbers the transformation should apply to, this option supports two modes: ● Original CID: Transform only the forwarded caller’s number. The CloudUCM must have “Keep Original CID” enabled on the trunk for forwarded calls. Otherwise, to avoid overwriting the number before applying the transformation. ● All: Apply transformations to every outbound number on this route The default setting is “<i>Original CID</i>”.
Strip	Specifies the number of leading characters to remove from the Caller ID before sending the call out. Only numeric values (0–2) are allowed.
Prepend	Defines characters to add in front of the Caller ID after stripping. Used to adjust Caller ID format to match ITSP requirements. Supports 0–20 characters (Digits, Letters, + – * # only).
Don’t Call Me Blocklist	If enabled, outgoing calls will first be checked against the “Don’t Call Me” database. If the called number is in the database, the call will be blocked. Please refer to the <i>Don’t Call Me Blocklist Integration</i> section for more information.
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 CloudUCM. Users can enable it again when it is needed.
<i>Outbound Permission</i>	
Password Settings	Configures the authentication method for this outbound route. The options are: ● Password: The configured password will be used. ● PIN Groups: The PIN number related to the configured PIN Group will be used The default option is “<i>Password</i>”.
Password	Configure the password for users to use this rule when making outbound calls.
PIN Groups	Select a PIN Group
PIN Groups with Privilege Level	If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied.
Privilege Level	Select the privilege level for the outbound rule. ● Internal: The lowest level required. All users can use this rule. ● Local: Users with Local, National, or International levels can use this rule. ● National: Users with National or International levels can use this rule. ● International: The highest level required. Only users with the international level can use this rule. ● Disable: The default setting is “Disable”. If selected, only the matched source caller ID will be allowed to use this outbound route. Please be aware of the potential security risks when using the “Internal” level, which means all users can use this outbound rule to dial out from the trunk.
Enable Source Caller ID Allowlist	When enabled, users could specify extensions allowed to use this outbound route. “Privilege Level” is automatically disabled if using “Enable Source Caller ID Allowlist”. The following two methods can be used at the same time to define the extensions as the source caller ID. 1. Select available extensions/extension groups from the list. This allows users to specify arbitrary single extensions available in the PBX. 2. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one. ● All patterns are prefixed with the “_”. ● Special characters X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. “.”: Wildcard. Match one or more characters. “!.”: Wildcard. Match zero or more characters immediately. Example: [12345–9] – Any digit from 1 to 9.

	Note: Multiple patterns can be used. Patterns should be separated by a comma “;”. Example: _X. , _NNXXNXXXXX, _818X.
Call Duration Limit	Enable to configure the maximum duration for the call using this outbound route.
Per-Call Duration Limit	Enable to configure the maximum duration of each call using this outbound route. Once this duration has been reached the call will be terminated.
Maximum Call Duration (s)	Configure the maximum duration of the call (in seconds). The default setting is 0, which means no limit.
Warning Time (s)	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.
Warning Repeat Interval (s)	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.
Total Call Duration Limit	Enables setting a maximum total call time for this outbound route within a specified period.
Period	Configures the cumulative period for total outgoing call duration. At the start of each new cycle, accumulated time resets to 0 and any outbound time limits are lifted. The options are: ● Monthly: cycle is one calendar month. ● Quarterly: cycle is three months from the current month. The default option is “<i>Monthly</i>”.
Total Time (m)	Specifies the maximum total call duration allowed for the route within the selected period, in minutes. Once this limit is reached, further calls through this route will be blocked until the period resets.
<i>Main Trunk</i>	
Trunk	Select the trunk for this outbound rule.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of long-distance calls. In this case, 1 digit should be stripped before the call is placed.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
<i>Failover Trunk</i>	
Failover Trunk	Failover trunks can be used to make sure that a call goes through an alternate route when the primary trunk is busy or down. If “Use Failover Trunk” is enabled and “Failover trunk” is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through. 10 failover trunks are supported.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of long-distance calls. In this case, 1 digit should be stripped before the call is placed.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
<i>Time Condition</i>	
Time Condition Mode	Use Main Trunk or Failover Trunk: Use the Main Trunk and its settings during the configured time conditions. If the main trunk is unavailable, the Failover Trunk and its settings will be used instead. Use Specific Trunks: Use specific trunks during the configured time conditions. The Strip and Prepend settings of the Main Trunk will be used. If a trunk is unavailable during its time condition, no failover trunks will be used.

Outgoing Routing Priority

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

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

Outbound Routes

An outgoing calling rule associates an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks. A failover trunk can be set up to be used when the primary trunk fails. Note: This panel only manages individual outgoing calling rules.

AddScheduled SyncOutbound BlocklistPIN GroupsFailover Trunk TogglesCarrierImportExport

All Levels

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

Total: 1 10 / page

Outgoing routing priority policy ✕

Priority Strategy

Accuracy First

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

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

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

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

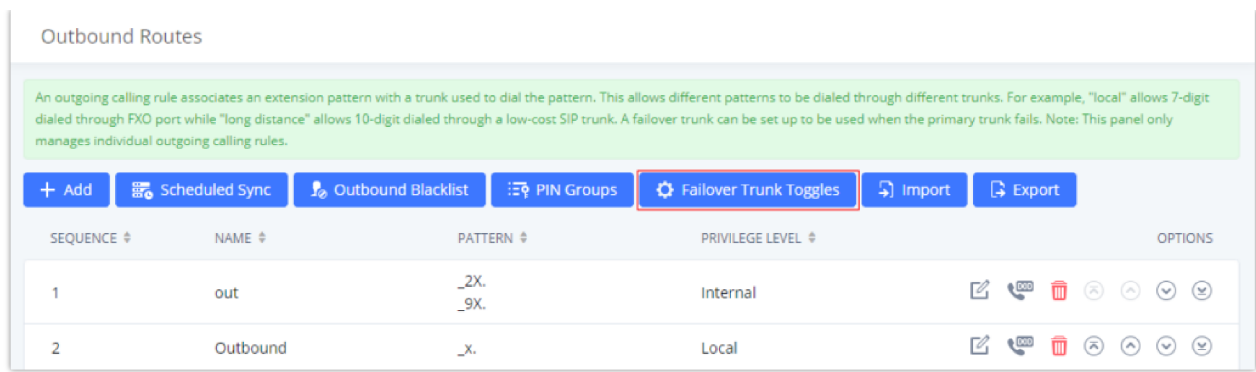
Cancel

OK

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

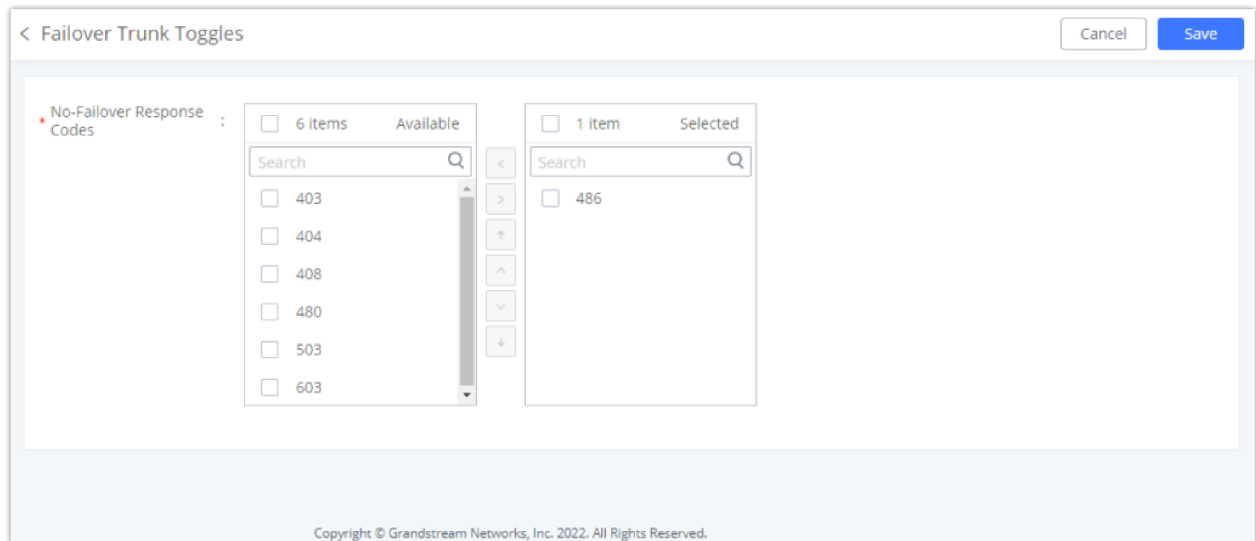
- **List Sorting Priority:** Selecting this option will result in taking the sorting order of the list of outbound routes as a matching criteria for the dial pattern. The route with the first matching dial plan will be used to route the call. Any routes further down the list with a more resembling dial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

Failover Trunk Toggles



Inbound Routes

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



Failover Trunk Toggles

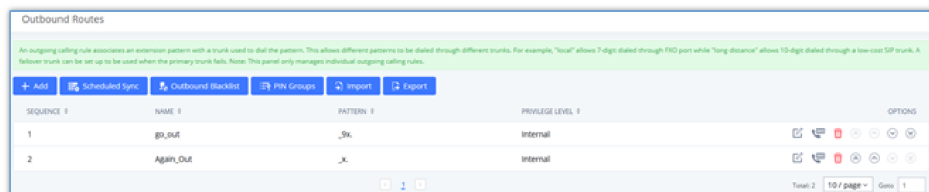
If a call receives the selected response codes, the UCM will redirect it to the call route's failover trunk.

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 the DOD number based on the Outbound Route, as displayed in the screenshot below. For each outbound route.



Outbound Routes Page

< DOD: go_out

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

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

+ Add DOD Import Export

DOD	DOD NAME	EXTENSIONS
369369	first dod	1000 1001 1002

< DOD: Again_Out

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

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

+ Add DOD Import Export

DOD	DOD NAME	EXTENSIONS
852582	second DOD	1000 1001 1002

DOD Configuration by Outbound Route

Outbound Blacklist

The CloudUCM allows users to configure a blacklist for outbound routes. If the dialing number matches the blacklist numbers or patterns, the outbound call will not be allowed. The outbound blacklist can be configured under UCM Web GUI >

Extension/Trunk > Outbound Routes: Outbound Blacklist.

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

< Outbound Blacklist

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

Country Codes:

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

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

| Blacklist Manage

* Add Blacklist Rule:
Add

Blacklist list

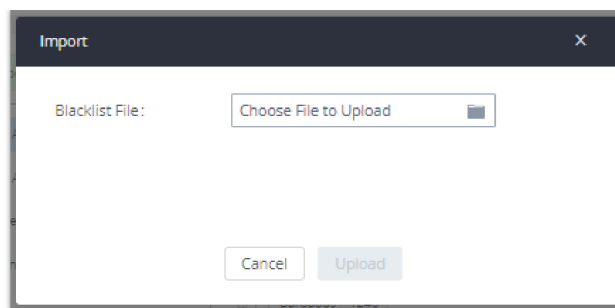
Clear Delete Import Export

Please enter blacklist number or

CONTINENT	COUNTRY	BLACKLIST RULE	OPTIONS
No Data			

Country Codes

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



Blacklist ImportExport

Don't Call Me Blacklist Integration

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

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

Outbound Routes > Outbound Blacklist

Blacklist Manage
Integrate Don't Call Me Blacklist

Integrate Don't Call Me Blacklist ☒

* Authorization Token
This field is required

* Query Timeout Time (s)
This field is required

Query Timeout Handling

Test Connection

Don't Call Me Database Integration

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

PIN Groups

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

Name	Specify the name of the group
-------------	-------------------------------

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

Outbound Routes/PIN Group

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

Create a New PIN Group

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

PIN Members

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

Outbound PIN

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

CDR								
By default, this page displays the CDR entries from the current month. Use the "Filter" button to specify a time range.								
Delete All Delete Search Result (s) Download All Records Download Search Result (s) Automatic Download								
STATUS	CALL FROM	CALL TO	ACTION TYPE	START TIME	CALL TIME	TALK TIME	ACCOUNT CODE	RECORDING FILE OPTIONS
▶	5555	99856352 [Tr...	DIAL	2019-12-04 10:57:47	0:00:08	0:00:08	Emily/G SEMEA	-
▶	1000	*36	DIAL	2019-12-03 10:12:37	0:00:19	0:00:19		-

CDR Record

Importing PIN Groups from CSV/XLSX files:

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

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

< PIN Groups

+ Add

Upload

NAME

RECORD IN CDR

OPTIONS

▶ GSEMEA

yes

<

1

>

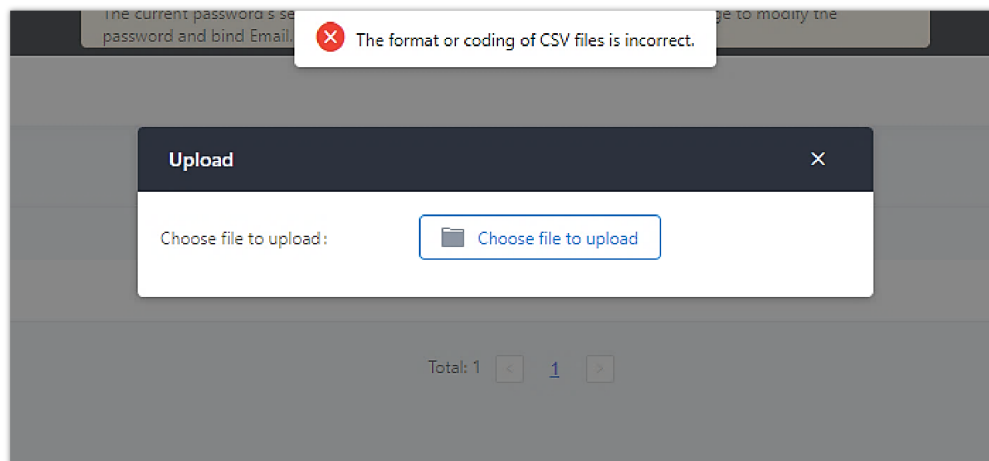
Total: 1

10 / page

Goto 1

Importing PIN Groups from files

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



Incorrect CSV File

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

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

CSV File Format

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

- Once the file is successfully uploaded, the entry will be added to the list of PIN Groups.

< PIN Groups			
+ Add Upload			
NAME	RECORD IN CDR	OPTIONS	
▶ GSEMEA	yes	Edit Download Delete	
1		Total: 1 10 / page Goto 1	

File Successful Upload

Carrier

The **Carrier** page is where you configure **Least Cost Routing (LCR)**. LCR is a method designed to minimize the cost of outbound calls by automatically selecting the cheapest available trunk for each call.

When an outbound route is set to **"Least Cost Routing"**, the system automatically analyzes the cost rates of all available trunks. It then selects and uses the trunk with the **lowest current carrier rate** to place the call.

To configure this option, please follow the steps below:

- Navigate to **Extension/Trunk → Outbound Routes** and click on Carrier.

Outbound Routes

① An outgoing calling rule associates an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks. A failover trunk can be set up to be used when the primary trunk fails. Note: This panel only manages individual outgoing calling rules.

Add

Scheduled Sync

Outbound Blocklist

PIN Groups

Failover Trunk Toggles

Carrier

Import

Export ▾

All Levels ▾

Q Name/Outbound Numbe...

ID ↗	Name	Outbound Number Matching Pattern	Privilege Level	Options
1	Rule_1	_ +212xxxxxxxxx +213xxxxxxxxx _X.	Internal	✎ ☎ 🗑 ↶ ↷ ⌵ ⌶

Total: 1

<

1

>

10 / page ▾

Goto

- On this page, please click on "Add" to configure a carrier.

Outbound Routes > Carrier				
① If "Least Cost Routing" is selected as an outbound route main trunk, the destination number for the outgoing call will be matched according to the table below to find the carrier, trunk, and rate rules that are available and identify the trunk with the lowest cost. If rates are the same, use the preferred carrier.				
Add Global Billing Unit				
All Carrier				
Priority	LCR	Carrier	Number of Trunks	Options
1	Supported	CarrierA	1	Edit Delete Refresh Up Down
2	Supported	CarrierABC	1	Edit Delete Refresh Up Down
Total: 2 < 1 > 10 / page Goto				

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

Note:

For each carrier you want to include in the LCR selection pool, you must enable the "LCR Supported" option.

Outbound Routes > Carrier > Add Carrier

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

* Trunk

☐ 0 Available

None

☐ 0 Selected

None

<

>

⌵

⬆

⬇

⌴

LCR supported ☒

Carrier Rates

☐ Match Prefix	Rate	Expiration Date	Options
---------------------------------------	------	-----------------	---------

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

Add Rate

×

* Match Prefix

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

* Rate

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

Expiration Date

-

Add Call Rate

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

Note:

To learn more about configuring the LCR feature and how it operates in CloudUCM, please refer to the [Grandstream Billing System Guide](#).

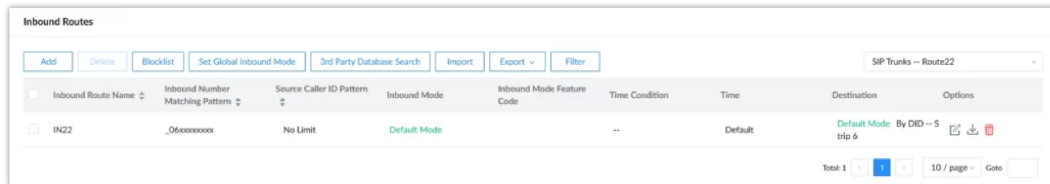
Inbound Routes

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

Configuring Inbound Routes

To manage inbound routes:

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



Inbound Routes Overview Page

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

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

Trunks	Select the trunk to configure the inbound rule.
Inbound Route Name	Configure the name of the Inbound Route. For example, “Local”, “LongDistance” etc.
Pattern	All patterns are prefixed with the “_”. Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. “.”: Wildcard. Match one or more characters. “!”: Wildcard. Match zero or more characters immediately. Example: [12345-9] – Any digit from 1 to 9. Notes: Multiple patterns can be used. Each pattern should be entered in a new line. Example: _X. _ NNXXNXXXXX /* 10-digit long distance */
Disable This Route	After creating the inbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in 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. ● Extension: send the fax to the designated FAX extension. ● Fax to Email: send the fax as an email attachment to the designated extension’s email address. If the selected extension does not have an associated email address, it will be sent to the default email address configured in the Call Features->Fax/T.38->Fax Settings page. Note: please make sure the sending email address is correctly configured in System Settings->Email Settings .
Auto Answer	If enabled, the UCM will automatically answer calls and receive faxes through the inbound route. If disabled, the UCM will not receive a fax until after the call has been answered. Enabling this option will slow down the answering of non-fax calls on the inbound route. The alert tone heard during the detection period can be customized.
Block Collect Calls	If enabled, collect calls will be blocked . Note: Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call". Note: This is affected by Block Set Calls on the SIP Settings -> General Settings page.
Prepend Trunk Name	If enabled, the trunk name will be added to the caller id name as the displayed caller id name.
Set Caller ID Info	Manipulates Caller ID (CID) name and/or number within the call flow to help identify who is calling. When enabled two fields will show allowing to manipulate the CallerID Number and the Caller ID Name.
CallerID Number	Configure the pattern-matching format to manipulate the numbers of incoming callers or to set a fixed CallerID number for calls that go through this inbound route. ● `\${CALLERID(num)}`: Default value which indicates the number of an incoming caller (CID). The CID will not be modified. ● `\${CALLERID(num):n}`: Skips the first n characters of a CID number, where n is a number. ● `\${CALLERID(num):-n}`: Takes the last n characters of a CID number, where n is a number. ● `\${CALLERID(num):s:n}`: Takes n characters of a CID number starting from s+1, where n is a number and s is a character position (e.g. `\${CALLERID(num):2:7}` takes 7 characters after the second character of a CID number). ● `\${n}\${CALLERID(num)}`: Prepends n to a CID number, where n is a number.
CallerID Name	The default string is `\${CALLERID(name)}` , which means the name of an incoming caller, it is a pattern-matching syntax format. A`\${CALLERID(name)}B` means Prepend a character ‘A’ and suffix a character ‘B’ to `\${CALLERID(name)}` . Not using pattern-matching syntax means setting a fixed name to the incoming caller.
Enable Route-Level Inbound Mode	Gives uses the ability to configure inbound mode per individual route. When enabled two fields will show allowing to set the Inbound mode and the Inbound mode Suffix. Note: Global inbound mode must be enabled before users can configure route-level inbound mode.
Inbound Mode	Choose the inbound mode for this route.

	Note: Toggling the global inbound mode will not affect routes that have Route-level Inbound Mode enabled. If all routes have the option enabled, toggling the global inbound mode via BLF will trigger a voice prompt indicating that none of the routes will be affected by the global inbound mode change.
Inbound Mode Suffix	Dial “Global Inbound Mode feature code + Inbound Mode Suffix” or a route’s assigned suffix to toggle the route’s inbound mode. The BLF subscribed to the inbound mode suffix can monitor the current inbound mode.
Inbound Multiple Mode	Multiple mode allows users to switch between destinations of the inbound rule by feature codes. Configure related feature codes as described in [Inbound Route: Multiple Mode]. If this option is enabled, the user can use feature code to switch between different modes/destinations.
CallerID Name Lookup	If enabled, the callerID will be resolved to a name through local LDAP. Note, if a matched name is found, the original callerID name will be replaced. The name lookup is performed before other callerID or callerID name modifiers (e.g., Inbound Route's Set CallerID Info or Prepend Trunk Name). Note: Name lookup may impact system performance.
Dial Trunk	This option shows up only when “By DID” is selected. If enabled, the external users dialing into the trunk via this inbound route can dial outbound calls using the UCM’s trunk.
Privilege Level	This option shows up only when “By DID” is selected. ● Disable: Only the selected Extensions or Extension Groups are allowed to use this rule when enabled Filter on Source Caller ID. ● Internal: The lowest level required. All users are allowed to use this rule, checking this level might be risky for security purposes. ● Local: Users with Local level, National or International level are allowed to use this rule. ● National: Users with National or International Level are allowed to use this rule. ● International: The highest level required. Only users with an international level are allowed to use this rule.
Allowed DID Destination	This option shows up only when “By DID” is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination is: ● Extension ● Conference ● Call Queue ● Ring Group ● Paging/Intercom Groups ● IVR ● Voicemail Groups ● Dial By Name ● All
Default Destination	Select the default destination for the inbound call. ● Extension ● Voicemail ● Conference Room ● Call Queue ● Ring Group ● Paging/Intercom ● Voicemail Group ● DISA ● IVR ● External Number ● By DID When “By DID” is used, the UCM will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in “DID destination”. If the dialed number matches the DID pattern, the call will be allowed to go through. ● Dial By Name

	● Callback
Strip	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Time Condition	
Start Time	Select the start time “hour:minute” for the trunk to use the inbound rule.
End Time	Select the end time “hour:minute” for the trunk to use the inbound rule.
Date	Select “By Week” or “By Day” and specify the date for the trunk to use the inbound rule.
Week	Select the day in the week to use the inbound rule.
Destination	Select the destination for the inbound call under the defined time condition. ● Extension ● Voicemail ● Conference Room ● Call Queue ● Ring Group ● Paging/Intercom ● Voicemail Group ● DISA ● IVR ● By DID When “By DID” is used, the UCM will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, and voicemail groups as configured in “DID destination”. If the dialed number matches the DID pattern, the call will be allowed to go through. Configure the number of digits to be stripped in the “Strip” option. ● Dial By Name ● External Number ● Callback

Inbound Route: Prepend Example

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

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

The screenshot shows the 'Inbound Route' configuration page. The 'Trunks' field is set to 'SIPTrunks -- test'. The 'Pattern' field contains '_18005251163'. The 'Alert-info' is set to 'None'. The 'Fax Detection' checkbox is unchecked. The 'Block Collect Calls' checkbox is unchecked. The 'Set CallerID Info' checkbox is unchecked. The 'Dial Trunk' checkbox is unchecked. The 'Inbound Multiple Mode' checkbox is unchecked. The 'CallerID Pattern' field is empty. The 'Allowed to seamless transfer' checkbox is unchecked. The 'Prepend Trunk Name' checkbox is unchecked. The 'Enable Route-Level Inbound Mode' checkbox is unchecked. The 'Allowed DID Destination' dropdown is set to 'Extension'. The 'Default Mode' tab is selected, and the 'Mode 1' tab is also visible. The 'Default Destination' dropdown is set to 'By DID'. The 'Strip' field contains '8'. The 'Prepend' field contains '2'.

Inbound Route feature Prepend

Inbound Route: Multiple Mode

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

The screenshot shows the 'Inbound Route' configuration page. The 'Trunks' field is set to 'SIPTrunks -- test'. The 'Pattern' field contains '_18005251163'. The 'Alert-info' is set to 'None'. The 'Fax Detection' checkbox is unchecked. The 'Block Collect Calls' checkbox is unchecked. The 'Set CallerID Info' checkbox is unchecked. The 'Inbound Multiple Mode' checkbox is checked. The 'CallerID Pattern' field is empty. The 'Allowed to seamless transfer' checkbox is unchecked. The 'Prepend Trunk Name' checkbox is unchecked. The 'Enable Route-Level Inbound Mode' checkbox is unchecked. The 'Default Mode' tab is selected, and the 'Mode 1' tab is also visible. The 'Default Destination' dropdown is set to 'Extension'. The 'Mode 1' dropdown is set to '1000'.

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 UCM can dial feature code *62 to switch to the inbound route "Mode 1" and dial feature code *61 to switch back to "Default Destination". Switching between different modes can be easily done without a Web GUI login.

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

To customize feature codes for "Default Mode" and "Mode 1", click on [Set Global Inbound Mode](#) under the "Inbound Routes" page, check the "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

Inbound Route Multiple Mode Feature Codes

Inbound Route: Route-Level Mode

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

* Trunks: SIPTrunks -- test

* Pattern:

Disable This Route: ☐

Alert-Info: None

Fax Detection: ☐

Block Collect Calls: ☐

Set CallerID Info: ☐

Inbound Mode: Default Mode

Inbound Multiple Mode: ☐

CallerID Pattern:

Allowed to seamless transfer:

Prepend Trunk Name: ☐

Enable Route-Level Inbound ☒

Mode:

* Inbound Mode Suffix: 5000

Inbound Route Route Level Mode

The global inbound mode must be enabled before configuring Route-Level Inbound Mode. Additionally, 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, the Inbound Default Mode feature code is set to *61, and the Inbound Mode suffix for route 1 is set to 1010. To switch the mode of route 1 to Default Mode, users can dial *611010.

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

Inbound Route: Inbound Mode BLF Monitoring

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

To do this, please refer to the following steps:

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

2. Click on the

Set Global Inbound Mode

button and enable Inbound Multiple Mode.

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

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

BLF Subscription Number:

777

Global Inbound Mode

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



Inbound Mode Default Mode

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



Inbound Mode Mode 1

Inbound Routes: 3rd Party Database Search

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

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

Inbound Route Name	Inbound Number Matching Pattern	Source Caller ID Pattern	Inbound Mode	Inbound Mode Feature Code	Time Condition
--------------------	---------------------------------	--------------------------	--------------	---------------------------	----------------

Inbound Routes Page

Note:

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

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

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

3rd Party Database Search Feature for Inbound Routes

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

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

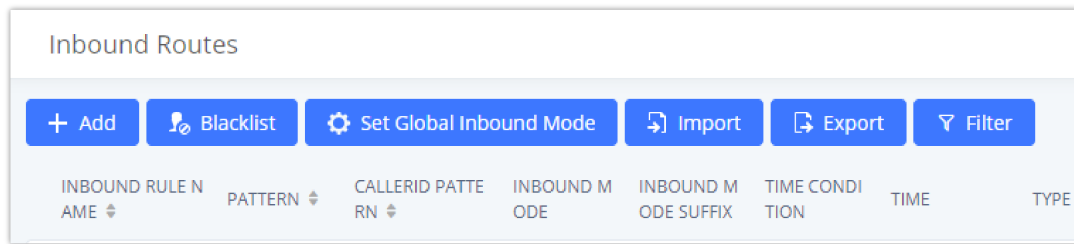
Based on the configured query keys, the CloudUCM automatically generates and executes a SQL query in the following format:

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

The inbound caller number is dynamically substituted at call time.

Inbound Route: Import/Export Inbound Route

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



Import/Export Inbound Route

The imported file should be in CSV/XLSX format and using UTF-8 encoding, the imported file should contain the 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... The user should enter an Alert-info string following the values we have in the Inbound route Alert-Info list.
- Allowed to seamless transfer: [Extension_number]
- Inbound Multiple Mode: Yes/No.
- Default Destination: By DID, Extension, Voicemail... Users should enter a Default Destination string following the values we have in the Inbound route Default Destination list.
- Destination: An Extension number, Ring Group Extension...
- Default Time Condition.
- Mode 1: By DID, Extension, Voicemail... Users should enter a Default Destination string following the values we have in the mode 1 Default Destination list.
- Mode 1 Destination: An Extension number, Ring Group Extension...
- Mode 1 Time Condition.

Blocklist Configurations

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

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

Inbound Routes > Blocklist

✔ This caller ID blocklist is used for all inbound routes.

⚠ Warning: Too many blocklist entries will lower overall system performance.

Enable Blocklist ☒

Blocklist Manage

* Add Blocklist Number

Apply to

Add

Blocklist list

☐	Number ↕	Apply to	Options
			

Blocklist Configuration Parameters

- To add blocklisted numbers in batch, click on "Import" to upload the blocklist file in CSV/XLSX format. The supported CSV/XLSX format is as below.

Paste Format Painter B I U					
Clipboard		Font			
F8		X	✓	f _x	
	A	B	C	D	E
1	13238680006	12135958547	12136268547	6262357999	
2					
3					
4					
5					

Blacklist File

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

BASIC CALL FEATURES

Multimedia Meeting

The UCM supports multimedia meeting rooms, allowing multiple rooms to be used at the same time.

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

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

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

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

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

Notes

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

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

Multimedia Room Configuration

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

Meeting Settings contains the following options:

Extension	The number to dial to reach the meeting room.
Meeting Name	Meeting Name
Privilege	Please select the permission for outgoing calls.
Allow User Invite	If enabled, participants will be able to invite other to the meeting by pressing 1 on their keypad or by clicking the Participants -> Invite option on the Wave bottom bar.
Allowed to Override Most Mute	Allowed to Override Host Mute
Auto Record	Meeting audio and video can be automatically recorded. These recordings can be found under the Meeting Recording or Meeting Video Recordings Page. ● None: Auto record is disabled. ● Record Audio: Record only the meeting Audio.

	● Record video (Focus Mode): Record the focus screen and all audio of the meeting. When a shared source is present in the meeting, only the shared screen is recorded.
Room Password	If meeting room password is configured, meeting participants will need to enter a password to enter the room. Scheduling meetings will not be supported for this room.

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

Multimedia Meeting

[Room](#)
[Meeting](#)
[Meeting Recordings](#)
[Meeting Video Recordings](#)

Meetings may have a significant impact on system performance. Please refer to the UCM user manual for additional details.

[+ Add](#)
[Meeting Settings](#)
[Call Statistics](#)

Room	Meeting Name	Attendee	Start Time	Activity	Options
▶ 6300		0		--	Edit Delete

Multimedia Meeting

Number of Meeting Rooms & Total Number of Participants

	Plan				
	Startup	SOHO	Plus	Pro	Business
Number of Public Meeting Rooms	8				
Total Number of Meeting Participants	4	8	16	32	64

Meetings Settings

To edit the general settings of the meeting rooms created in the UCM, the user can click on the “Meetings Settings” button under the **Room** tab.

Meeting Max Concurrent Audio	Maximum number of participants that can be heard simultaneously in multimedia meetings. If the number of participants talking at any given point exceeds this value, the audio of the excess participants will not be heard.
Meeting Voice Indicator Sensitivity	Configures the sensitivity of the talking indicator in multimedia meetings. Setting this higher will make the talking indicator appear more easily for lower volumes of audio. Note: This does not adjust audio input sensitivity itself. Lower volumes of sounds may still be heard even if the talking indicator does not show the source.
Meeting Audio Quality	Audio quality of multimedia meetings

Meeting Record Prompt	If enabled, system will prompt the user before the start of meeting recording that your meeting will be recorded.
Allow New Participants To View Chat History	Configure whether new attendees joining in the middle of a Wave meeting can view the chat content already in the meeting.
Meeting AGC (beta)	Enabling this option will toggle on Automatic Gain Control for meeting audio. AGC is a system that dynamically reduces the variability of sound levels by adjusting high and low volumes based on the average or peak sound level. High volume sounds will be lowered, and low volume sounds will be boosted.
Silence Suppression	Silence suppression for temporary accounts (e.g., meeting participants that joined the meeting via link). 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.
Enable Talk Detection	If enabled, the AMI will send the corresponding event when a user starts or stops talking.
DSP Talking Threshold (ms)	The amount of time(ms) that sound exceeds what the DSP has established as the baseline for silence 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.
DSP Silence Threshold (ms)	The amount of time(ms) that sound falls within what the DSP has established as the baseline for silence before a user is considered be silent. This value affects several operations and should not be changed unless the impact on call quality is fully understood.
Max Number of Video Feeds	Set the maximum number of video feeds supported per meeting room.
Audio Codec Preference	Configures the preferred codecs for temporary accounts such as meeting participants who joined via link.
Packet Loss Retransmission	Packet Loss Retransmission configuration for temporary accounts (meeting participants without registered extensions who entered the meeting via link).
Jitter Buffer	Select the jitter buffer method for temporary accounts such as meeting participants who joined via link. ● Disabled: 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.

Multimedia Meeting Call Operations

Join a Meeting Call

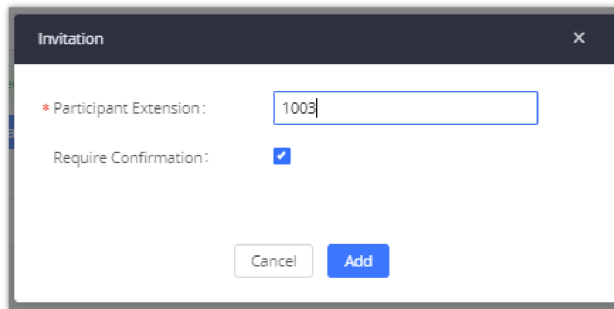
Users could dial the meeting room extension to join the meeting. If the password is required, enter the password to join the meeting as a normal user, or enter the admin password to join the meeting as an administrator.

Invite Other Parties to Join a Meeting

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

- **Invite from Web GUI**

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



Meeting Invitation from Web GUI

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

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

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

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

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

During The Meeting

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

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

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

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

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

Please see the options listed in the table below.

Meeting Administrator IVR Menu	
1	Mute/unmute yourself.
2	Lock/unlock the conference room.
3	Kick the last joined user from the conference.
4	Decrease the volume of the conference call.

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

- When there is a participant in the meeting, the meeting room configuration cannot be modified.
- If only GDS or GSC extensions remain in a meeting, the system will automatically terminate the meeting session.

Google Service Settings Support

CloudUCM supports Google OAuth 2.0 authentication. This feature is used to support the CloudUCM meeting scheduling system. Once OAuth 2.0 is enabled, the CloudUCM conference system can access Google Calendar to schedule or update a conference.

Google Service Settings can be found under Web GUI → **Basic Call Features** → **Multimedia Meeting** → **Google Service Settings** → **Google Service Settings**.

OAuth2.0 Authentication

* OAuth2.0 Client ID:

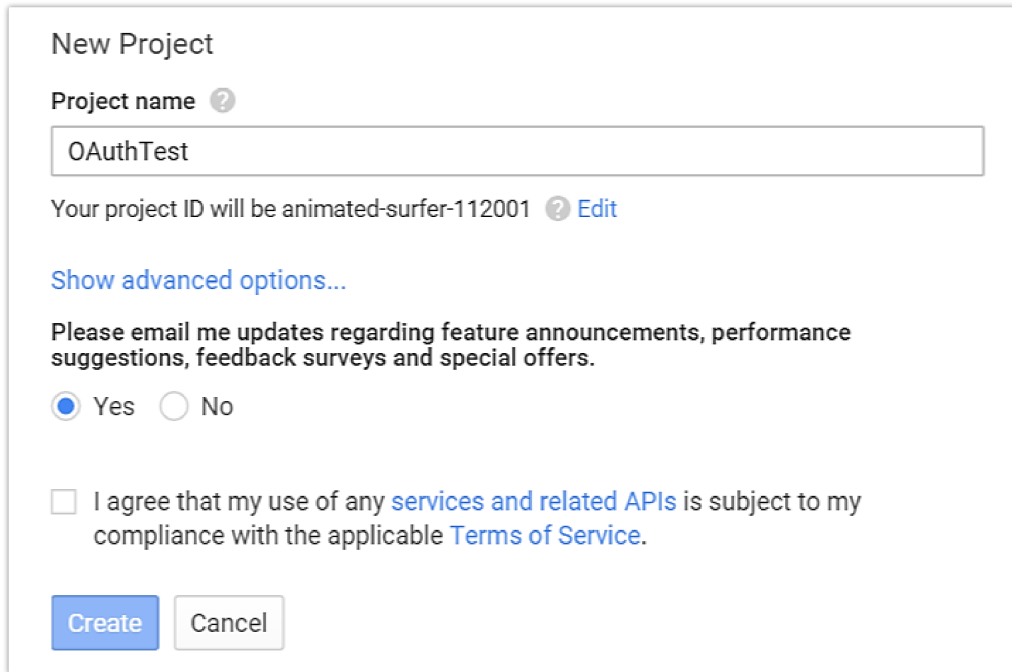
* OAuth2.0 Client Secret:

Google Service Settings → OAuth20 Authentication

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

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

1. Go to the Google Developers page <https://console.developers.google.com/start>. Create a New Project on the Google Developers page.



New Project

Project name [?]

OAuthTest

Your project ID will be animated-surfer-112001 [?] [Edit](#)

[Show advanced options...](#)

Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.

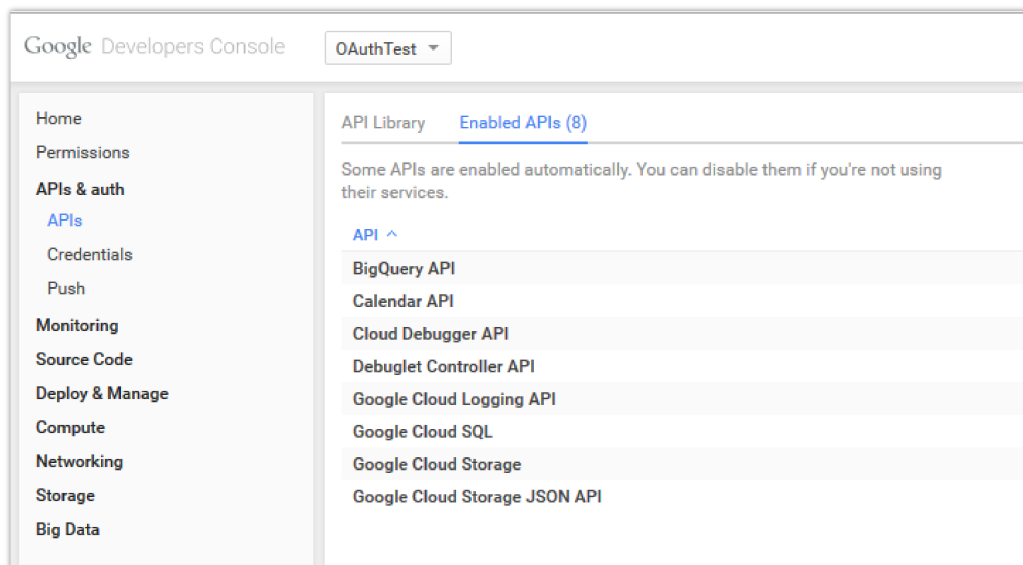
☒ Yes ☐ No

☐ I agree that my use of any [services and related APIs](#) is subject to my compliance with the applicable [Terms of Service](#).

[Create](#) [Cancel](#)

Google Service → New Project

2. Enable Calendar API from the API Library.
3. Click "Credentials" on the left drop-down menu to create new OAuth2.0 login credentials.



Google Service → Create New Credential

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

Google Calendar Authorization

1. Click "Get Authorization Code". [Get Authorization Code](#)
2. Enter the Google account and password (Note: please make sure the account on authorization page is correct, if you have logged in other account, please log out then log in again).
3. Click "Accept" on authorization page.
4. Copy the string to the Authorization Code input box, click the "authorize" button.

* Authorization Code:

[Authorization](#)

Google Service → OAuth20 Login

6. Once this has been done, the CloudUCM will connect to Google services.

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

Schedule Meeting

To manage your multimedia meeting room reservations, log in to the CloudUCM web interface and navigate to **Basic Call Features** → **Multimedia Meeting** → **Meeting**. From this page, you can create, edit, view, and delete all meeting room reservation records. The interface clearly displays a list of both ongoing and upcoming reservations for easy scheduling.

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

Multimedia Meeting > Schedule Meeting

* Meeting Subject		Meeting Room	☐ Public Meeting Room
* Time	2025-01-13	* Time Zone	{ UTC+01:00 } Etc/GMT-1
Password		* Host Password	6940
* Host		Repeat	No Repeat
Allow User Invite	☒	Call Participants	☒
Email Reminder (m)	☒ 60	Allowed to Override Host Mute	☐
Sync to Google Calendar	☐ Google Services	* Auto Record	None
Invitees	Please enter and submit participants with the... 0/23 Add For improved voice audio quality of link users, please add Opus to the meeting room's supported codecs. Warning: Opus is a resource-intensive codec.		
		Meeting Agenda	
Cancel Save			

Schedule meeting Interface

The table below describes the configurable parameters for scheduling a multimedia meeting:

<i>General</i>	
Meeting Subject	Configure the name of the scheduled meeting. Letters, digits, some special characters are also supported. The characters ` % # ? < > @ \$ ^ ~ are not allowed.
Public Meeting Room	Choose which room to have this scheduled meeting.
Time	Configure the meeting date and time.
Time Zone	Select the meeting time zone.
Repeat	Choose when to repeat a scheduled meeting. • No Repeat • Every Day • Weekly • Monthly • Custom: it specifies how often the meeting is repeated per days/weeks. E.g., every 3 days/weeks.
End Repeat	This option appears when a reccurent schedule is configured. Configure the date when the recurrence stops.
Password	Configure the meeting's login password.
Meeting Agenda	The description of this scheduled meeting.
<i>Attendee</i>	
Host	Configure Host.
Host Password	Configure the Host Password. Note: It is randomly generated when first creating a new meeting Schedule.
Invitees	Local extensions, remote extensions, and special extensions are supported.
Allow User Invite	If enabled, participants will be able to invite others to the meeting by pressing 1 on their keypad or by clicking the Participants->Invite option.
<i>Advanced</i>	
Email Reminder (m)	Check to enable scheduled meeting email reminder. Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-120. 60 is the default value. Note: After editing the time of a single recurrence of a scheduled meeting, a cancellation email will be sent out followed by a meeting update email.
Call Participant	If enabled, the invited participants will be called upon meeting start time.
Allowed to Override Host Mute	If enabled, participants will be able to unmute themselves if they have been muted by the host.
Play Joining/Leaving Meeting Announcement	Configure whether the join/leave meeting prompt is played when participants join or leave.
Auto Record	Meeting audio and video can be automatically recorded. These recordings can be found under the <i>Meeting Recordings</i> or <i>Meeting Video Recordings</i> page. • Record Audio: Record only the meeting audio. • Record Video: Record the meeting audio and all video feeds. When there is a shared source (shared screen/shared whiteboard/shared document) or focus, only the shared or focus screen is recorded, and when both are present, the shared screen is recorded. • Record Video (Focus Mode): Record the focus screen and all audio of the meeting. When a shared source is present in the meeting, only the shared screen is recorded.
Sync Google Calendar	Select this option to sync scheduled meeting with Google Calendar.

	Note: Google Service Setting OAuth2.0 must be configured on the IPPBX. Please refer to section [Google Service Settings Support] .
Support AI transcription	Choose whether to support AI transcription for the scheduled meeting. This parameter cannot be controlled if the AI meeting transcription and summary is disabled in the general AI Settings .
Language	Specifies the language recognition behavior used for AI transcription. The options are: ● Automatic Recognition: Automatically detects the spoken language during the meeting. This is recommended when multiple languages are expected, though recognition accuracy may vary. ● Preferred Language: Prioritizes recognition of the selected language, while still allowing multilingual detection with potentially reduced accuracy. Note: This setting controls only the transcription language for this scheduled meeting. It does not apply to the general AI Conference Transcription and Summary feature.
Automatic AI Transcription	Once enabled, meeting audio will be automatically transcribed in real time once the meeting starts. A summary will also be generated after the meeting.

Once the Meeting Schedule is configured, it will be displayed as shown in the below figure.

Multimedia Meeting

RoomMeetingMeeting RecordingsMeeting Video Recordings

Pending MeetingMeeting History

Schedule Meeting

Meeting Su...

Meeting Subject	Meeting Room	Meeting Owner	Start Time	Meeting Duration	Repeat	Options
Weekly_Meeting	70709021	admin	2025-01-15 10:00 Etc/GMT-1	01:00:00	No Repeat	

Total: 1

<1>

10 / page

Meetings Schedule

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

Meeting Details

Meeting SubjectWeekly_Meeting

Room Number70709021

Session stateNot started

Start Time2025-01-15 10:00

Time ZoneEtc/GMT-1

Meeting Owneradmin

Password

Host Password9283

Sync to Google CalendarNo

RepeatNo Repeat

Invitees

Status	FirstName	Phone Number	Email	Leave a message
Require Confirmation		1000	morgan.arthur@gmail.com	

OK

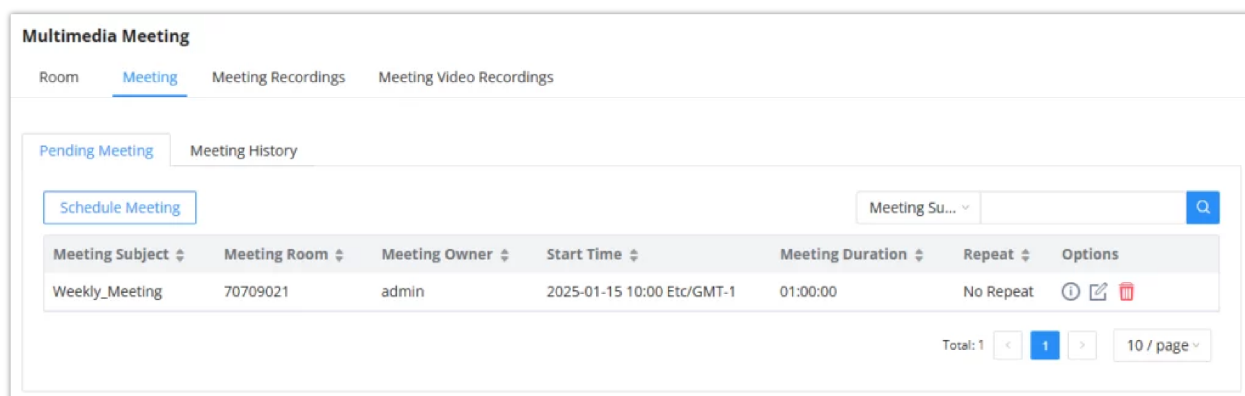
Meeting details

- Click on  to edit the Meeting Schedule.

- Click on  to delete the Meeting Schedule.

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

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



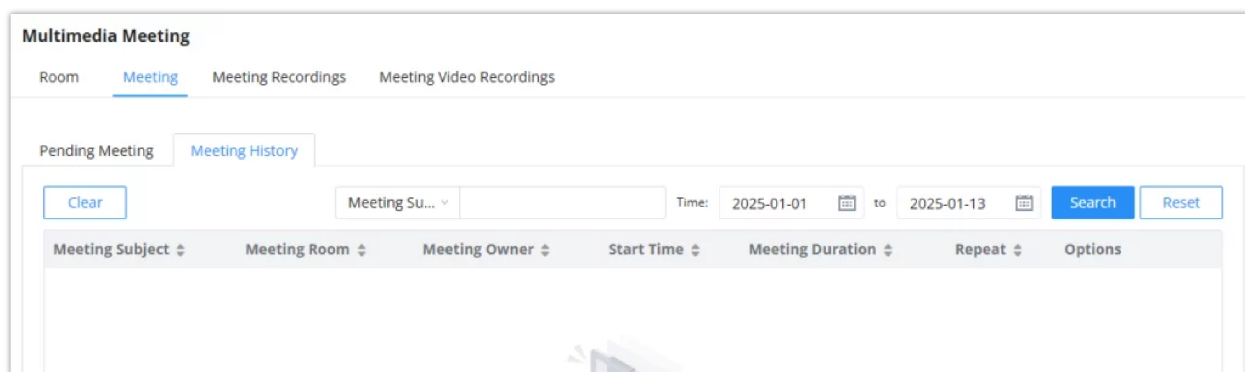
The screenshot shows the 'Multimedia Meeting' interface. The 'Meeting' tab is selected. Under 'Pending Meeting', there is a 'Schedule Meeting' button. A table lists the meeting details:

Meeting Subject	Meeting Room	Meeting Owner	Start Time	Meeting Duration	Repeat	Options
Weekly_Meeting	70709021	admin	2025-01-15 10:00 Etc/GMT-1	01:00:00	No Repeat	  

At the bottom right, it shows 'Total: 1' and '10 / page'.

Meeting Scheduled Ongoing

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



The screenshot shows the 'Multimedia Meeting' interface with the 'Meeting History' tab selected. There is a 'Clear' button and a search bar with filters for 'Meeting Su...', 'Time' (2025-01-01 to 2025-01-13), and buttons for 'Search' and 'Reset'. The table below is empty.

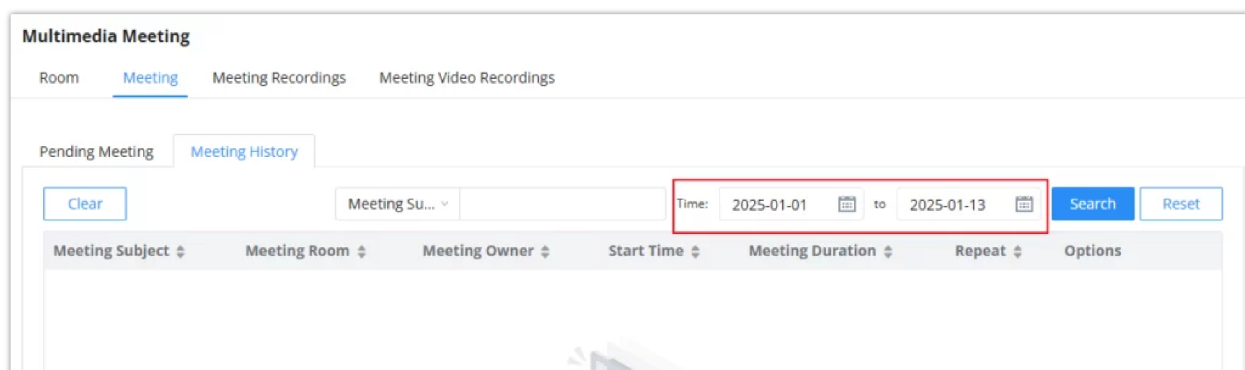
Meeting Subject	Meeting Room	Meeting Owner	Start Time	Meeting Duration	Repeat	Options
-----------------	--------------	---------------	------------	------------------	--------	---------

Meeting Schedule Completed

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

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

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



This screenshot is identical to the previous one, but with a red box highlighting the 'Time' filter section, which is set to '2025-01-01' to '2025-01-13'.

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

Meeting Recordings

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

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

The recording files will be listed 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.

Multimedia Meeting

Room

Meeting

Meeting Recordings

Meeting Video Recordings

Download

Download All

Delete

Clear

Local

2025-01

☐	Name	Room	Date	Size	Options
--------------------------	------	------	------	------	---------

Meeting Recordings

Meeting Video Recordings

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

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

The recording files will be listed 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 Statistics

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

Multimedia Meeting

Room

Meeting

Meeting Recordings

Meeting Video Recordings

Meetings may have a significant impact on system performance. Please refer to the SoftwareUCM user manual for additional details.

Please ensure that ICE Support is enabled and that STUN/TURN server is configured with NAT.

Add

Meeting Settings

Call Statistics

Room	Meeting Name	Attendee	Start Time	Activity	Options
▶ 6300		0		--	 

Meeting Call Statistics

Multimedia Meeting > Call Statistics

Download

Delete Report

Scheduled Export

2025-01-01

to

2025-01-13

Filter

Meeting	Start Time	Duration
▼  6300	2025-01-13 12:14:37	00:00:31
 1000 Name 1000 Number Call In Admission Mode Answered State		

Total: 1

<

1

>

10 / page

Goto

Meeting Report on Web

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

Exported Meeting Report

IVR

IVR (Interactive Voice Response) is a feature that enables triggering certain actions by using DTMF. The recorded prompt of the IVR instructs the numbers and the corresponding actions to the caller, when the caller press a certain number, the PBX will trigger the equivalent action.

Configure IVR

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

- Click on “Add” to add a new IVR.
- Click on the “edit” icon  to configure an existing IVR.
- Click on the trash icon  to delete an IVR.

IVR > Create New IVR

Basic Settings

Key Pressing Events

General

Name 

Support_IVR

Extension 

7000

Auto Record 

☒

Prompt Language 

Default

Prompt 

welcome

Upload Audio File

Add Prompt 

IVR Webhook

IVR Webhook 

☐

Dialed Number

Dial Other Extensions 

☐ All
☒ Extension
☐ External Number

☐ Multimedia Meeting
☐ Call Queue
☐ Ring Group

Create New IVR

The table below describes the configuration parameters that are available when creating a new IVR:

General	
Name	Configure the name of the IVR. Letters, digits, _ and – are allowed.
Extension	Enter the extension number for users to access the IVR.
Auto Record	If enabled, calls to this IVR will automatically be recorded.

Prompt Language	Select voice prompt language for this extension. If set to “Default”, the global setting for Voice Prompt will be used. This configuration only applies to the system prompt, and does not affect the language of custom prompt.
Prompt	Initial tone that plays when the user enters the IVR.
IVR Webhook	
IVR Webhook	If enabled, call event notification and call control can be achieved via URL. Using webhooks, the user can send requests to a specific server to perform actions through DTMF.
Target URL	Target URL address for receiving notification commands as well as sending operation commands. It needs to be the full URL of the web server, static parameters and pages can be included.
Username	Enter the username used to connect to the target URL.
Password	Enter the password used to connect to the target URL.
Call Event	Select the call events to notify the IVR about. • All • Notify IVR of Incoming Calls • Notify IVR of Answer • Notify IVR of DTMF Events • Notify IVR of End
Call Control	If enabled, the predefined IVR flow for the destination URL will be followed. Configurations related to the original IVR flow such as dialed numbers, key events, etc. will be disabled.
Timeout Time (s)	Configure the timeout time for receiving call control, default 2 seconds, the system tries up to three times after the timeout.
Dialed Number	
Dial Other Extensions	If enabled, callers will be allowed to dial extensions other than the ones explicitly defined in the Key Pressing Events page. The options are: • All • Extension • External Number • Multimedia Meeting • Call Queue • Ring Group • Paging/Intercom Groups • Voicemail Groups • Fax Extension • Dial By Name By default only “Extension” is selected.
Privilege	Defines the calling permission level for callers who reach this IVR for external dialing.
Dial Block/Allowlist	Applies a specific list that either explicitly allows or blocks the numbers that can be dialed from this IVR.
Internal Block/Allowlist	Applies a specific list that either allows or blocks calls to internal extensions dialed from this IVR.
External Blocklist/Allowlist	Applies a specific list that either allows or blocks calls to external numbers dialed from this IVR.
Timeout/Invalid Settings	

Digit Timeout (s)	Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, CloudUCM will consider the entries complete. The default timeout is 3s.
Response Timeout (s)	After playing the prompts in the IVR, CloudUCM will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout prompt will be played. The default setting is 10 seconds.
Response Timeout Prompt	Select the prompt message to be played when timeout occurs.
Response Timeout Prompt Repeats	Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3.
Invalid Input Prompt	Select the prompt message to be played when an invalid extension is pressed.
Invalid Input Prompt Repeats	Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3.
PMS Wake-Up Call Service Mode	
PMS Wake-Up Call Service	If enabled, this IVR can be used with Wakeup Service to send notifications to specified destinations based on caller key presses. If enabled, key events will only be supported in standard mode. Time conditions will not be supported.
Other Settings	
Replace Display Name	If enabled, CloudUCM will replace the caller display name with IVR name.
Return IVR Menu	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
Alert-info	When present in an INVITE request, the Alert-info header field specifies an alternative ringtone to the UAS.
Alert-info	When present in an INVITE request, the Alert-info header field specifies an alternative ringtone to the UAS.
Key Pressing Events	
Key Event Type	Choose the operational mode for handling key presses for this IVR. The options are: ● Standard: The IVR will process key presses according to its standard menu mapping (e.g., press 1 for Meeting, 2 for Ring Group). ● Custom: Allows to configure a combination of digits that will be used to interact with the IVR in comparison with the standard Key Pressing Event type which has only one digit input. Note: The “PMS Wake-Up Service Mode” (found in Basic Settings) takes precedence. If it is enabled, the Key Event Type is forced to Standard mode and cannot be changed to Custom until that setting is disabled.
Key Events	Define custom actions or destinations for specific DTMF key presses.
Other Settings	This section contains additional, general configuration options for the IVR’s behavior such as timeout and invalid entry action.

IVR > Create New IVR

Basic Settings Key Pressing Events

Key Event Type ☒ Standard ☐ Custom

Key Events

Key 0

Destination Select an O... Time Condition All Time

Key 1

Destination Select an O... Time Condition All Time

Key 2

Destination Select an O... Time Condition All Time

Key Pressing Events

Block/Allowlist in IVR

In some scenarios, the administrator needs to restrict the extensions that can be reached from IVR. For example, the company CEO and directors prefer to only receive calls transferred by the secretary, and some special extensions are used on IP surveillance endpoints that should not be reached from external calls via IVR for privacy reasons.

For enhanced security, CloudUCM's IVR settings include **Blocklist and Allowlist** management. This enables administrators to restrict dialing to only approved numbers, effectively preventing the misuse of the "Dial Other Extensions" feature.

Up to 500 extensions are allowed on the Block/Allowlist.

To use this feature, log in to CloudUCM Web GUI and navigate to **Basic Call Features→IVR→Create/Edit IVR→Dial Block/Allowlist**.

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

Dialed Number

Dial Other Extensions ⓘ

☐ All
 ☒ Extension
 ☒ External Number

☐ Multimedia Meeting
 ☐ Call Queue
 ☐ Ring Group

☐ Paging/Intercom Groups
 ☐ Voicemail Groups

☐ Fax Extension
 ☐ Dial By Name

* Privilege ⓘ

Internal

Dial Block/Allowlist ⓘ

Allowlist

Internal Block/Allowlist ⓘ

3 Available

Search

☐ 1002
☐ 1003
☐ 1004

2 Selected

Search

☐ 1000
☐ 1001

External Blocklist/Allowlist

0123456

Dial BlockAllowlist

Create Custom Prompt

To record a new IVR prompt or upload an 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 the Custom Prompt page. Or users could go to Web GUI→**PBX Settings**→**Voice Prompt**→**Custom Prompt** page directly.

Alert-info: None

* Prompt: welcome

Upload Audio File

Add Prompt +

Click on Prompt to Create IVR Prompt

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

Key Pressing Events

Standard Key Event

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

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

Key Pressing Events

Key Event Type

☒ Standard
☐ Custom

Key Events

Key

0

Destination

Extension

1003

Time Condition

All Time

Key

1

Destination

Voicemail

1000

Time Condition

Holiday

Key Pressing Events

Note

If you select "Custom 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.

Custom Time

Time

Start Time

End Time

Frequency

☒ By Week
☐ By Month

Sun

Mon

Tue

Wed

Thu

Fri

Sat

☐ Excluding Holidays

Cancel

OK

Specific Time

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

Key Event Type	Select Standard to configure single-key DTMF events (0–9, *). This mode supports time-based routing per key.
Key (0–9, *)	Each section corresponds to a specific DTMF key (for example, Key 0, Key 2). Configuration under a key defines how calls are routed when that key is pressed.
Destination	Select the destination type and target for the key event. Supported destinations include: • Extension • Meeting • Voicemail • Voicemail Group • IVR (Maximum 64 nested IVRs) • Ring Group • Queues • Paging/Intercom Group • Fax

	● Custom Prompt ● Hang-up ● DISA ● Dial By Name ● External Number ● Callback ● Announcement
Time Condition	Assign a time condition to each destination entry. The IVR evaluates the time conditions in order and routes the call to the first matching rule. Common options include <i>All Time</i>, <i>Office Time</i>, <i>Out of Office Time</i>, <i>Holiday</i>, and <i>Specific Time</i>. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for the same key, or the (–) icon to remove an existing rule.
Timeout	Configures the destination when the Timeout Repeat Loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (–) icon to remove an existing rule.
Invalid	Configures the destination when the Invalid Repeat loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (–) icon to remove an existing rule.

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.

The screenshot shows the 'Key Pressing Events' configuration window. At the top, 'Key Event Type' has radio buttons for 'Standard' and 'Custom', with 'Custom' selected. Below this, a section titled 'Key Events' contains 'Add', 'Delete', and 'Clear' buttons. A table below these buttons has columns for 'Key', 'Destination', and 'Time Condition'. The first row shows 'Key' as '123', 'Destination' as 'Voicemail', and 'Time Condition' as 'All Time'. A green plus icon is located at the bottom right of the table area.

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

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

The following options are available for Custom Key Pressing Events:

Key Event Type	Select “ <i>Custom</i> ” to configure multi-digit DTMF key combinations. This mode supports time-based routing and advanced IVR logic.
Key	Defines the DTMF key combination that triggers the event. Notes: • Each key combination can contain up to 8 characters • Supported characters: 0–9 and * • Up to 100 custom key events are supported per IVR
Destination	Select the destination type and target for the custom key event. Supported destinations include: • Extension • Meeting • Voicemail • Voicemail Group • IVR (<i>Maximum 64 nested IVRs</i>) • Ring Group • Queues • Paging/Intercom Group • Fax • Custom Prompt • Hang-up • DISA • Dial By Name • External Number • Callback • Announcement
Time Condition	Assign a time condition to each destination entry. The IVR evaluates the time conditions in order and routes the call to the first matching rule. Common options include <i>All Time</i>, <i>Office Time</i>, <i>Out of Office Time</i>, <i>Holiday</i>, and <i>Specific Time</i>. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for the same key, or the (–) icon to remove an existing rule.
Timeout	Configures the destination when the Timeout Repeat Loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (–) icon to remove an existing rule.
Invalid	Configures the destination when the Invalid Repeat loop is done. Note: A single key can contain multiple destination entries with different time conditions (up to five). Users can click the (+) icon to add another destination with a different time condition for this option, or the (–) icon to remove an existing rule.

Voicemail

Configure Voicemail

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

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

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 the 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 is 10 to 1000. The default setting is 50.
Max Message Time	Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the maximum message time. The default setting is 15 minutes. The available options are: ◦ 1 minute ◦ 2 minutes ◦ 5 minutes ◦ 15 minutes ◦ 30 minutes ◦ Unlimited

Min Effective Message Time	Configure the minimum duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Message Time. The default setting is 3 seconds. The available options are: • No minimum • 1 second • 2 seconds • 3 seconds • 4 seconds • 5 seconds Note: Silence and noise duration are not counted in message time.
Announce Message Caller-ID	If enabled, the caller ID of the user who has left the message will be announced at the beginning of the voicemail message. The default setting is "No".
Announce Message Duration	If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is "No".
Play Envelope	If enabled, a brief introduction (received time, received from, etc.) of each message will be played when accessed from the voicemail application. The default setting is "Yes".
Play Most Recent First	If enabled, it will play the most recent message first.
Allow User Review	If enabled, users can review the message following the IVR before sending.
Voicemail Remote Access	If enabled, external callers routed by DID and reaching VM will be prompted by the CloudUCM with 2 options: ◦ Press 1 to leave a message. To leave a message for the extension reached by DID. ◦ Press 2 to access the voicemail management system. This will allow the caller to access any extension VM after entering the extension number and its VM password. Note: This option applies to inbound calls routed by DID only. The default setting is "Disabled".
Forward Voicemail to Peered UCMs	Enables the forwarding of voicemail to remote extensions on peered SIP trunks. The default setting is "Disabled".
Voicemail Password	Configures the default voicemail password that will be used when an extension is reset.

Format	Warning: WAV files take up significantly more storage space than GSM files.
---------------	---

Voicemail Settings

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 CloudUCM 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 through 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 to access 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 beginning of the message, while forward will not work when there are 3 seconds or less left in the voice message.
- Voice guidance will be automatically played when the voicemail is done playing.

Leaving Voicemail

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

In case 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 CloudUCM can be configured to send the voicemail as an attachment to the Email. Click on the "Voicemail Email Settings" button to configure the Email attributes and content.

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

Voicemail Email Settings

Voicemail Email Settings

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

Configure Voicemail Group

The CloudUCM supports voicemail groups, and all the extensions added to the group will receive voicemail to the group extension. The voicemail group can be configured under Web GUI → **Basic Call Features** → **Voicemail** → **Voicemail Group**. Click on "Add" to configure the group.

Note:

Up to 150 extensions can be configured in a single voicemail group.

Voicemail > Create New Voicemail Groups

* Extension

6600

* Name

Name

* Method

☒ Forwarded
☐ Shared

Voicemail Password

Voicemail Password

Email Address

Email Address

Shared Voicemail Status

☐

Members

☐ 498 Available

☐ 0 Selected

Search

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

Search

None

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

The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.

Name Prompt

Choose File to Upload

Download

Delete

Temporary Prompt

Choose File to Upload

Download

Delete

Unavailable Prompt

Choose File to Upload

Download

Delete

Cancel

Save

Voicemail Group

Extension	Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members.
Name	Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed.
Method	Select the preference for receiving and managing group voicemail. ● Forwarded: Voicemail will be stored in the group voicemail box, and each voicemail group member will be forwarded a copy of it. ● Shared: Voicemail will be stored in the group voicemail box, and voicemail status will be shared among all voicemail group members. If a member deletes a voicemail, it will also be deleted for all members. Likewise, if one member reads a voicemail, it will be considered read for the entire group.
Voicemail Password	Configure the voicemail password for the users to check voicemail messages.
Email Address	Configure the Email address for the voicemail group extension.
Shared Voicemail Status	If enabled, voicemail group status can be monitored via BLF. Green indicates no unread voicemail, and red indicates existing unread voicemail.
Members	Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list.

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

Ring Groups

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

Configure Ring Group

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

Ring Group

+ Add

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

Ring Group

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

Create New Ring Groups

* Ring Group Name:

test

* Extension:

6400

Members:

27 items

Available

Search

☐ 1000
☐ 1001
☐ 1005
☐ 1006
☐ 1007

3 items

Selected

Search

☐ 1002
☐ 1003
☐ 1004

LDAP Phonebook:

0 item

Available

Search

None

0 item

Selected

Search

None

Ring Group Options

Ring Strategy:

Ring in Order

Music On Hold:

None

Custom Prompt:

None

Upload Audio File

Ring Group Configuration

Ring Group Name	Configure ring group name to identify the ring group. Letters, digits, _ and – are allowed.
Extension	Configure the ring group extension.
Members	Select available users from the left side to the ring group member list on the right side. Click on ▲ ▼ to arrange the order.
LDAP Phonebook	Select available remote users from the left side to the ring group member list on the right side. Click on ▲ ▼ to arrange the order. Note: LDAP Sync must be enabled first.
Ring Strategy	Select the ring strategy. The default setting is “Ring in order”. ● Ring Simultaneously: Ring all the members at the same time when there is incoming call to the ring group extension. If any of the member answers the call, it will stop ringing. ● Ring in Order: Ring the members with the order configured in ring group list. If the first member does not answer the call, it will stop ringing the first member and start ringing the second member.
Music On Hold	Select the “Music On Hold” Class of this Ring Group, “Music On Hold” can be managed from the “Music On Hold” panel on the left.
Custom Prompt	This option is to set a custom prompt for a ring group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts. Note: Users can also refer to the page PBX Settings > Voice Prompt > Custom Prompt, where they could record new prompt or upload prompt files.

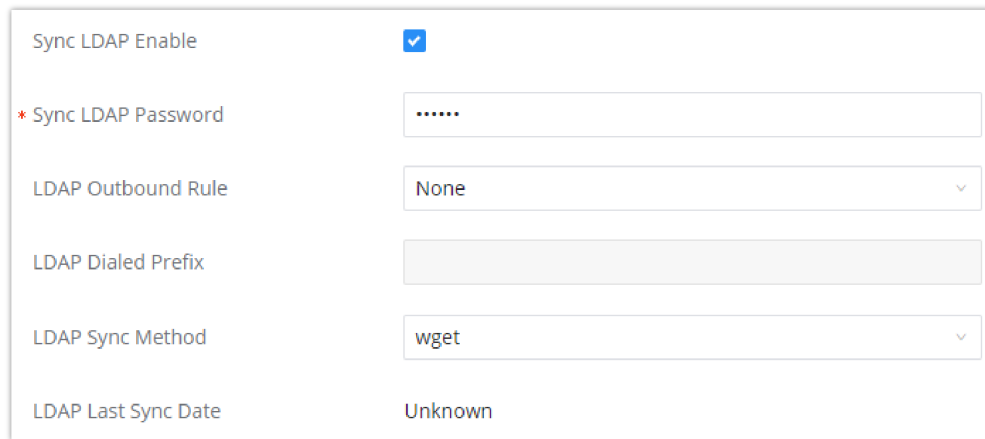
Ring Timeout on Each Member	Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 60 seconds. Note: The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.
Auto Record	If enabled, calls on this ring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

Remote Extension in Ring Group

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

1. Creating SIP Peer Trunk between UCM_A and UCM_B. **SIP Trunk** can be found under Web GUI→**Extension/Trunk**→**VoIP Trunks**. Also, please configure their Inbound/Outbound routes accordingly.
2. Click the edit button in the menu , and check if Sync LDAP Enable is selected. This option will allow UCM_A to update the remote LDAP server automatically from peer UCM_B. In addition, the Sync LDAP Password must match for UCM_A and UCM_B to sync the 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.

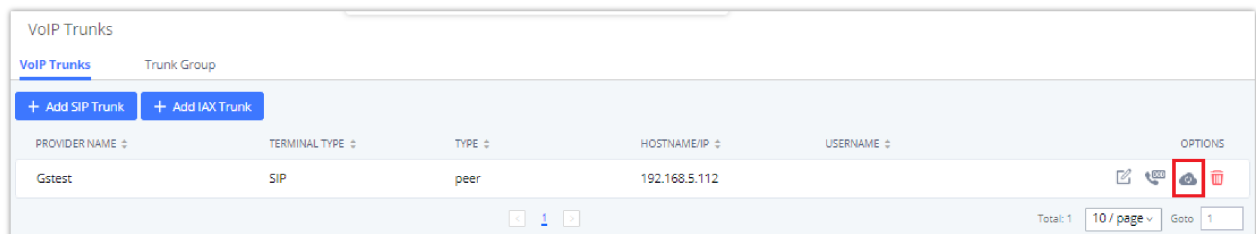


The screenshot shows a configuration window titled "Sync LDAP Server Options". It contains the following fields:

- Sync LDAP Enable**: A checkbox that is checked (indicated by a blue checkmark icon).
- * Sync LDAP Password**: A text input field with masked characters (dots).
- LDAP Outbound Rule**: A dropdown menu currently set to "None".
- LDAP Dialed Prefix**: A text input field that is currently empty.
- LDAP Sync Method**: A dropdown menu currently set to "wget".
- LDAP Last Sync Date**: A text field displaying "Unknown".

Sync LDAP Server Options

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



The screenshot shows the "VoIP Trunks" page in the web GUI. It features a table with the following columns: PROVIDER NAME, TERMINAL TYPE, TYPE, HOSTNAME/IP, USERNAME, and OPTIONS. A single entry is visible in the table:

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

Below the table, there is a pagination bar showing "Total: 1", "10 / page", and "Goto 1". The sync icon in the "OPTIONS" column of the table is highlighted with a red box.

Manually Sync LDAP Server

4. Under the **Ring Groups** setting page, click "Add". **Ring Groups** can be found under Web GUI > **Basic Call Features** > **Ring Groups**.
5. If the LDAP server is synced correctly, the **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 UCM can be included to that UCM's LDAP contact.

Create New Ring Group

• Ring Group Name:

• Extensions:

Members:

☐ 106
☐ 1000
☐ 1001
☐ 1002
☐ 1003

☐ 15
☐ 5000(ou=ucm6510,dc=pbx,dc=com)
☐ 5001(ou=ucm6510,dc=pbx,dc=com)
☐ 5002(ou=ucm6510,dc=pbx,dc=com)
☐ 5003(ou=ucm6510,dc=pbx,dc=com)

LDAP Phonebook:

Ring Group Options

Ring Group Remote Extension

Paging/Intercom

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

Paging/Intercom Groups

2-way Intercom

Paging/Intercom > Create New Paging/Intercom Group

General

• Name:

• Strategy:

• Extension:

Private Intercom: ☐

Auto Record: ☐

Replace Display Name: ☐

• Maximum Call Duration (s):

Disable: ☐

Receiver

• Members:

☐ 10 Items
☐ 1000

☐ 0 item
☐

2 way Intercom

Parameter	Description
General	

Name	Configure intercom group name.
Strategy	Select “2-way Intercom”.
Extension	Configure the intercom group extension.
Private Intercom	If enabled, members can only hear the voice of the initiator and cannot hear the voice of other members. The initiator can hear the voice of all members.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the PBX will replace the caller display name with Intercom name.
First Answer Termination	Enabling this option will result in halting other phones from ringing once the intercom is answered. This option is disabled by default.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Disable	If disabled, the real-time and scheduled intercom will not be triggered.
Recipient	
Members	Select available users from the left side to the paging/intercom group member list on the right.
Initiator	
Paging/Intercom Allowlist	Select which extensions are allowed to use the paging/intercom feature for this paging group.
Paging Sound	
Opening Prompt	This option enables/disables setting a custom opening prompt for a paging/intercom group to announce to callees.
Custom Prompt	Select a custom prompt or click on ‘Upload Audio File’ to upload the customized voice prompts. Notes: • Users can also refer to the page PBX Settings→Voice Prompt→Custom Prompt, where they could record new prompt or upload prompt files. • The audio file must be under 30 MB and use one of the following extensions: .mp3, .wav, .ulaw, .alaw, or .gsm. WAV files must be PCM encoded, 16-bit mono, and 8000 Hz. • For improved audio quality, uploading MP3 files with a 44.1 kHz or 48 kHz sampling rate is recommended. • If uploading a compressed file, it must have a .tar, .tgz, or .tar.gz extension and must not exceed 50 MB. • File names may only include alphanumeric characters, hyphens (-), and underscores (_).
Play Prompt to Caller	When enabled, the caller will hear the prompt in addition to the callee.

Private Intercom

The **Private Intercom** feature enables controlled, one-way communication within an intercom group. When activated, only the initiator’s voice is broadcast to all other members, while the initiator can hear responses from each member individually. **Members cannot hear each other**, ensuring that conversations remain private between each participant and the initiator.

Paging/Intercom > Create New Paging/Intercom Group

General

* Name

* Strategy

* Extension

Private Intercom ☒

ⓘ If enabled, members can only hear the voice of the initiator and cannot hear the voice of other members. The initiator can hear the voice of all members.

Auto Record ☐

Replace Display Name ☐

* Maximum Call Duration (s)

Disable ☐

Private Intercom

1-way Paging

1-way paging allows the user to send a voice message to the endpoints; the user can either directly announce the message or send a prerecorded voice message to the endpoints.

Paging/Intercom > Create New Paging/Intercom Group

General

* Name

* Strategy

* Extension

Video Broadcast ☐

Auto Record ☐

Replace Display Name ☐

* Maximum Call Duration (s)

Disable ☐

1 way Paging

Parameter	Description
General	
Name	Configure paging group name.
Strategy	Select “1-way Paging”.
Extension	Configure the paging group extension.
Video Broadcast	If checked, video paging will be supported. If the caller sends a video page, the paging group members will be able to receive and view the video.

Auto Record	Enable this option to record in WAV format (audio) and MKV format (video). Note: If Auto Record is enabled, recorded video pages will be saved in MKV file format. Saved recordings can be found on the <i>CDR→Recordings→Video Recordings</i> page.
Replace Display Name	If enabled, the PBX will replace the caller display name with paging name.
First Answer Termination	Enabling this option will result in halting other phones from ringing once the paging is answered. This option is disabled by default.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Disable	If disabled, the real-time and scheduled paging will not be triggered.
Recipient	
Members	Select available users from the left side to the paging/intercom group member list on the right.
Initiator	
Paging/Intercom Allowlist	Select which extensions are allowed to use the paging/intercom feature for this paging group.
Paging Sound	
Opening Prompt	This option enables/disables setting a custom opening prompt for a paging/intercom group to announce to callees.
Custom Prompt	Select a custom prompt or click on “Upload Audio File”/“Upload Video” to upload the customized voice prompts or videos. Notes: - Users can also refer to the page PBX Settings→Voice Prompt→Custom Prompt, where they could record new prompt or upload prompt files. - The audio file must be under 30 MB and use one of the following extensions: .mp3, .wav, .ulaw, .alaw, or .gsm. WAV files must be PCM encoded, 16-bit mono, and 8000 Hz. - For improved audio quality, uploading MP3 files with a 44.1 kHz or 48 kHz sampling rate is recommended. Audio encoding must be mono channel and use one of the following codecs: PCMU, PCMA, iLBC, G722, OPUS, GSM, G726, or G729/G723. - Video encoding must be H.264 and formatted as an MKV file. - MKV file size must be less than 30 MB. - If uploading a compressed file, it must have a .tar, .tgz, or .tar.gz extension and must not exceed 50 MB. - File names may only include alphanumeric characters, hyphens (-), and underscores (_).
Play Prompt to Caller	When enabled, the caller will hear the prompt in addition to the callee.
Other Settings	
Delayed Paging	If enabled, a caller can dial *82 before the paging group extension to initiate a delayed paging call. The system will prompt the caller to record a message. After the message is saved and the configured delay has passed, the paging call will be sent. When a group member answers, the recorded message will be played automatically, and the call will end once playback is complete.
Delay (s)	Configure the delay time (in seconds) between the end of the recorded message and when the delayed paging call is sent. The default value is 5 seconds.

Video Broadcast

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

Paging/Intercom > Create New Paging/Intercom Group

General

*

 Name

Video_Page_1

*

 Strategy

1-way Paging

*

 Extension

Extension

Video Broadcast

☒

Auto Record

☐

Video Broadcast Configuration

The user can upload the video in the “Announcement File” section, as shown in the screenshot below.

Paging Sound

Opening Prompt

☒

?

When a paging/intercom is initiated, the opening prompt is played first, and then the shout prompt is supported.

*

 Announcement File

Upload Video

Play Prompt to Caller

☐

Upload Announcement File

Scheduled Paging/Intercom

Pending Paging/Intercom

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

Paging/Intercom > Create New Scheduled Paging/Intercom

*

 Paging/Intercom

*

 Name

*

 Caller

*

 Start Date

2024-03-07

*

 Start Time

Select time

Add Start Time

Repeat

No Repeat

Sync to Google Calendar

☐

Google Services

Cancel

Save

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

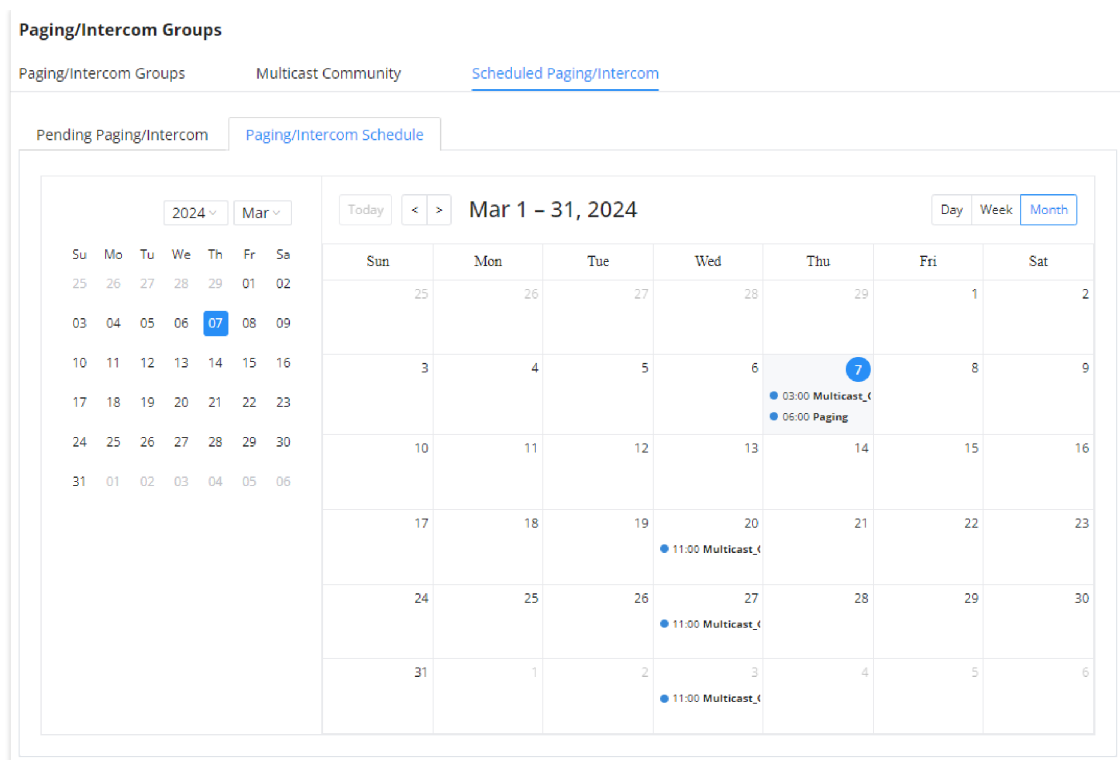
Once the paging and intercom have been created, they can be viewed on the same page.

Pending Paging/Intercom		Paging/Intercom Schedule					
+ Add		Name		Time: Start Time to End Time		Search	Reset
Name	Caller	Paging/Intercom Extension	Paging/Intercom Name	Strategy	Start Time	Repeat	Options
Multicast_Group	1000	1077	Multicast_Group	Multicast Paging	2024-03-07 15:00	No Repeat 15:00	
Paging	1003	1055	Paging	1-way Paging	2024-03-07 18:00	No Repeat 18:00	
Multicast_Group	1006	1077	Multicast_Group	Multicast Paging	2024-03-20 11:00	Wed, Tue, Thu, Fri, Mon 11:00	
Total: 3 <1> 10 / page Goto							

Pending Paging/Intercom

Paging/Intercom Schedule

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



Scheduled Paging/Intercom

Call Queue

CloudUCM supports call queues by using static agents or dynamic agents. The Call Queue system can accept more calls than the available agents. This section describes the configuration of the call queue under **Basic Call Features→Call Queue**.

Add Call Queue

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

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

Call Queue Page

- Click on “Add” to add a call queue.
- Click on  to edit the call queue.
- Click on  to delete the call queue.

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

Basic Settings	
General	
Extension	Configure the call queue extension number.
Name	Configure the call queue name to identify the call queue.
Proficiency Routing	If enabled, incoming calls will be routed to the agents with the highest available proficiency level (lower number = higher proficiency). If multiple agents have the same level, the Ring Strategy for Same Proficiency

	Level will be used to route calls among those agents. Please make sure to assign proficiency levels to the agents. Note: This option applies to both static and dynamic agents.
Strategy (Ring Strategy of Equal Skill Level when Proficiency Routing is enabled)	Select the strategy for the call queue. ● Ring All: Ring all available Agents simultaneously until one answers. ● Linear: Ring agents in the specified order. ● Least Recent: Ring the agent who has been called the least recently. ● Fewest Calls: Ring the agent with the fewest completed calls. ● Random: Ring a random agent. ● Round Robin: Ring the agents in Round Robin scheduling with memory. The default setting is “Ring All”.
Music On Hold	Select the Music On Hold class for the call queue. Note: Music On Hold classes can be managed from Web GUI > PBX Settings > Music On Hold.
Max Queue Length	Configure the maximum number of calls to be queued at once. This number does not include calls that have been connected with agents, 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. Default value is 10 seconds.
Retry Time (s)	Configure the number of seconds to wait before ringing the next agent. The minimum is 1 and the default setting is 5 seconds. Since only 3 digits can be entered, the max value is 999.
Agent Ring Time	Configure the number of seconds to ring an agent. The minimum is 5 and the default setting is 30 seconds. Since only 3 digits can be entered, the max value is 999.
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. Users can choose whether to automatically record only internal calls, external calls or all calls. By default, Auto Record is disabled.
Prompt Language	Choose the language of the prompt which will be played to the caller. When the option “default” is selected, the language defined in PBX Settings > Voice Prompt > Language Settings will be selected.
Welcome Prompt	
Enable	Enable the welcome prompt.
Custom Prompt	Choose the initial tone that plays when the user dials the queue number. Note: The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
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 welcome prompt is being played to the caller.
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. Notes: The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw ● The user can upload a custom prompt directly from this parameter. ● Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw ● Super administrator, administrators and queue chairmen can access agent satisfaction statistics by going to Call Queue Statistics > Overview > Agent Satisfaction Statistics/Queue Satisfaction Statistics. ● The service satisfaction information can also be downloaded from Call Queue Statistics.
Max Wait Time	

Max Wait Time	Configures the amount of time (in seconds) a caller will be kept in queue before the the call is automatically routed to the configured Max Wait Time Destination. If set to 0, callers will be kept in queue indefinitely. Default is 60 seconds.
Destination	The call will be routed to this destination if no one in this queue answers after the max wait time expires.
Reset Agent Call Counter	
Enable	Specifies the frequency at which the agent call counter will be reset. This will affect counter data used for agent ring strategies and the queue switchboard data.
Repeat	Set the repeat frequency to One-time, Daily, Weekly or Monthly.
Date/Time	Set the date and time.
Destination Prompt Cycle	
Enable	If enabled, the callers will hear the configured custom prompt at set intervals while waiting. If they press “1,” they are immediately routed to a predefined failover destination.
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. Otherwise, continue waiting in queue. Note: The user can upload a custom prompt directly from this parameter. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
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, the system will activate a virtual queue for users, allowing them to opt for a callback instead of waiting. Callers will be prompted to either remain in the queue or choose a number that the PBX will use to reach them, ensuring they retain their position in line.
Virtual Queue Mode	• DTMF mode: pressing 2 will manually trigger virtual queue and callers will hear a prompt to manually set a callback number. • Timeout mode: virtual queue will automatically be triggered when the configured Virtual Queue Period has passed and the users can choose a callback number. • Auto mode: virtual queue will automatically be triggered when the configured Virtual Queue Period has passed but the callback number will automatically be set to the caller’s detected CID number.
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.
Write Timeout	The amount of time in seconds that agents will have to answer a virtual queue callback. If the value is less than the Agent Ring Time, then the Agent Ring Time will take effect.

Virtual Queue Welcome Prompt	Upload the file of your welcome prompt of the virtual queue. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
<i>Queue Announcement</i>	
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. Valid range is between 20 and 600 seconds. Default value is 20.
Agent ID Announcement	If enabled, a system prompt containing the agent ID will be played to the caller when answered by an agent.
Premium Code	Callers can increase their priority in queue by entering their premium code and # within 5 seconds of the premium code prompt ending.
Premium Code Prompt	After enabling the position announcement, the premium code related functions can be set to share the same announcement cycle with the position announcement.
<i>Custom Announcement</i>	
Custom Prompt	The system will periodically play this announcement to callers that enter the queue. Only the following file formats are supported: .tar, .tgz, .tar.gz, .mp3, .wav, .gsm, .alaw, .ulaw
Announcement Interval (s)	Configures the interval for playing the queue's custom announcement. Valid range is between 20 and 600 seconds. Default value is 60.
<i>Empty Queue</i>	
Leave When Empty	Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict". ● Yes: Callers will be disconnected from the queue if all agents are paused or invalid. ● No: Never disconnect the callers from the queue when the queue is empty. ● Strict: Callers will be disconnected from the queue if all agents are paused, invalid or unavailable.
Dial in Empty Queue	Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No". ● Yes: Callers can always dial into a call queue. ● No: Callers cannot dial into a queue if all agents are paused or invalid. ● Strict: Callers cannot dial into a queue if the agents are paused, invalid or unavailable.
Failover Destination	Choose the destination where the call will be directed when the queue is empty or when all the agents are not logged in, here are the destinations that can be configured: ● Play Sound. ● Extension. ● Voicemail. ● Queues. ● Ring Group. ● Voicemail Group. ● IVR ● External Number.
<i>CTI</i>	
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.
<i>Service Level Agreement (SLA)</i>	

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 PBX will report (to the agent) the duration of time of the call before the caller is connected to the agent. The default setting is “No”.
Replace Display Name	If enabled, the PBX will replace the caller display name with the Call Queue name so that the caller knows the call is incoming from a Call Queue.
Enable Feature Codes	Enable feature codes option for call queue. For example, *83 is used for “Agent Pause”
Autofill	Enable/Disable the Autofill feature which distributes calls automatically to available agents as soon as they become free instead of having callers wait in a traditional queue.
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.
Call Memory	If enabled, the system will remember the last agent a caller has talked to. If the caller enters the queue again within the configured Retrieval Time (Days), the remembered agent will be prioritized for answering the call.
Memory Retention Time (Days)	Sets the amount of time that callers will be remembered for Call Memory agent matching. Calls to the queue after this period of time will no longer prioritize the caller’s last agent. Valid range is 1 to 30 days. Default value is 7.
Enable RPID Header	Toggles the sending of Remote-Party-ID header to the caller. Requires enable Send Remote Party ID configuration in ToS page.
Agents	
Dynamic Agents	Configure the dynamic agents of this queue, allowing dynamic agents to sign into the queue and receive incoming calls from the queue. The total number of static agents and logged in dynamic agents needs to meet the number limit of the agents on this device.
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.

Static and Dynamic Agents

There are two types of agents that can be part of a call queue:

- **Dynamic Agents:** Can log in and out of the call queue at any time by using preset codes (e.g., dialing *31*100 to log into queue 100).
- **Static Agents:** Manually added by an administrator when configuring the call queue.

Agent Limit Specification

The total number of agents (combined static and dynamic) across all queues on the CloudUCM is controlled by your CloudUCM plan. This limit is calculated as follows:

- If your plan supports **fewer than 100 extensions**, the maximum total number of agents is equal to the number of supported extensions.
- If your plan supports **100 or more extensions**, the maximum total number of agents is capped at **100**.

Note:

This is a system-wide limit for the entire CloudUCM, not a per-queue limit.

Static Agents

Static agents are configured manually within each queue's settings under **Basic Call Features**→**Call Queue**→**Create/Edit Queue**→**Agents**.

Call Queue Static Agents

Dynamic Agents

While static agents need to be manually configured in the call queue settings, dynamic agents only need a Login and Logout suffix to be able to join a queue.

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

Call Queue > Global Queue Settings

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

Dynamic Agent Login Settings

Agent Login Code Suffix

Agent Logout Code Suffix

Example

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

Dynamic Agent Login Settings

Note:

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

Call Queue Feature Codes

Users can leverage feature codes to perform different call queue-related actions by accessing Basic Call Features → Feature Codes → Feature Codes. Below is the description of each code along with its default values:

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

Note:

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

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

Queue Recordings

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

Call Queue

Call QueueQueue RecordingsQueue SwitchboardCall Queue Statistics

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

DownloadDownload AllDeleteClear

Local2024-10

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

Queue Recordings Page

- Click on



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



to delete the recording file.

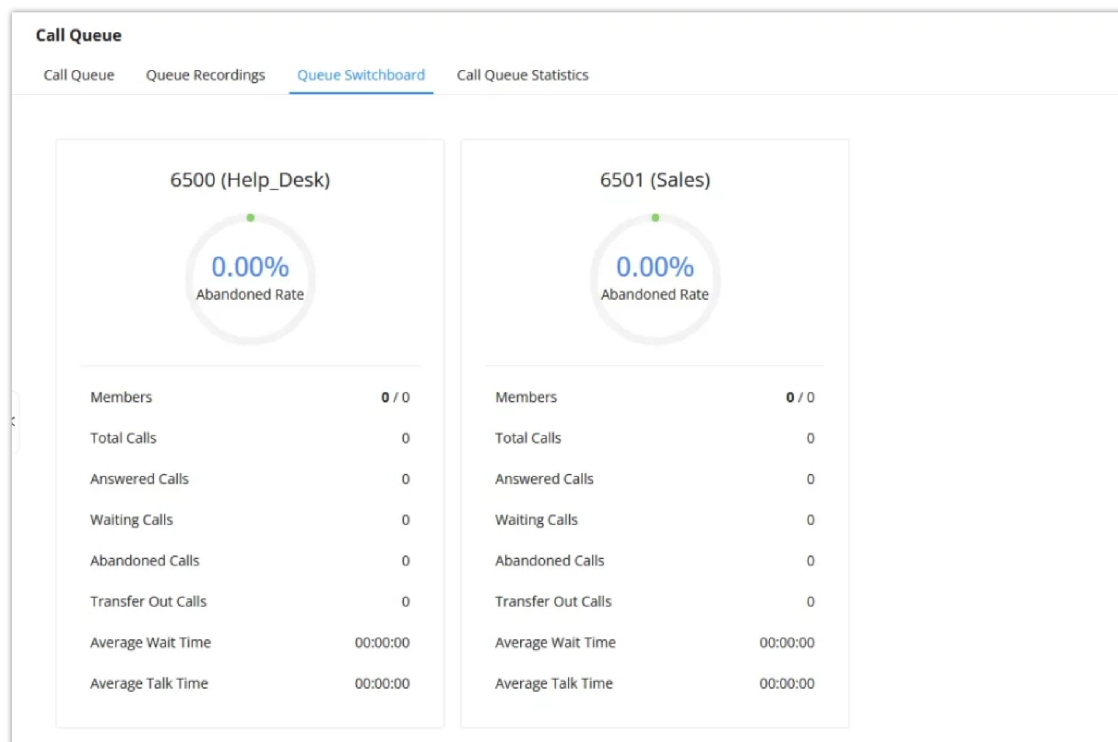
Note:

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

Queue Switchboard

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

Following page will be displayed:



Switchboard Summary

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

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		

© 2023 Grandstream Networks, Inc.

Call Queue Switchboard

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

Super Admin	Default admin of the PBX. Call queue privileges include: - Viewing and edit all queue agents. - Monitor and execute actions for incoming/outgoing calls for all queues. - 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 PBX user portal with their extension number and assigned user password. Call Queue privileges include: - Viewing status and information related to all agents in the assigned queue. - Perform actions on calls such as hang-up, transfer or barge-in. - Manual Login/Logout of static and dynamic agents. - Viewing CDR
Queue Agent	User appointed by Super Admin to be a member of a queue extension. A queue agent can log into the PBX user portal with their extension number and assigned user password to manage their calls only.

Queue Switchboard Privilege

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

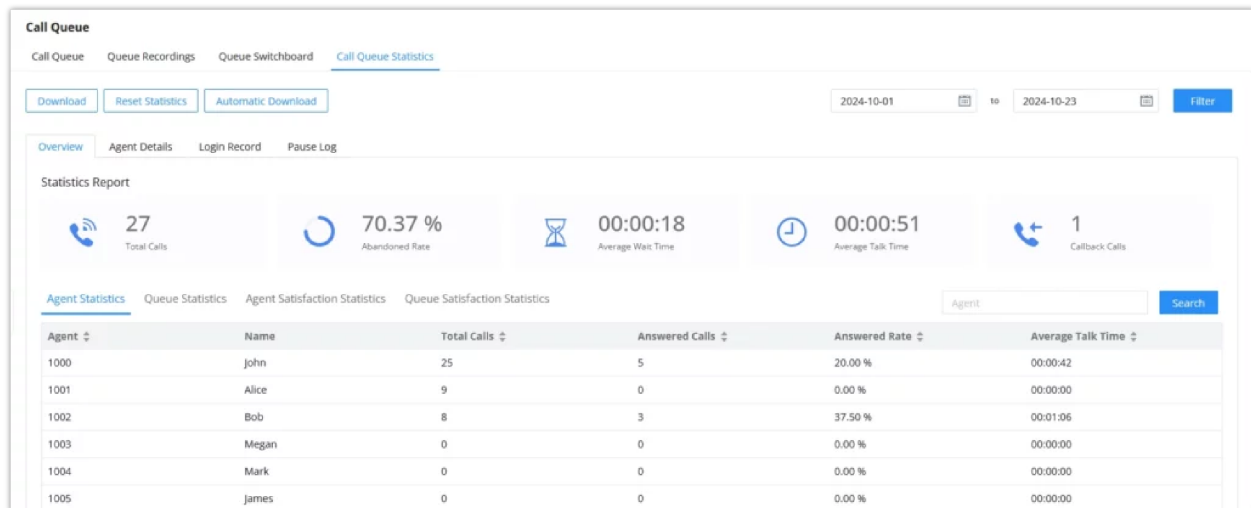
Super Admin	Default admin of the UCM. Call queue privileges include: - Viewing and edit all queue agents. - Monitor and execute actions for incoming/outgoing calls for all queues. - Generate Call Queue reports to track performance.
Queue Chairman	User appointed by Super Admin to monitor and manage an assigned queue extension via Switchboard. The Queue Chairman can log into the UCM user portal with their extension number and assigned user password. The Queue chairman privileges include: - Viewing status and information related to all agents in the assigned queue. - Perform actions on calls such as hang-up, transfer or barge-in. - Manual Login/Logout of static and dynamic agents. - Viewing CDR of their respective queues.

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 their extension number and assigned user password to manage their calls only.
--------------------	---

Call Queue Statistics

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

To access call queue statistics, go to **Basic Call Features > Call Queue** and click on **“Call Queue Statistics”**. The following page will be displayed:



Call Queue Statistics

Users can download statistics in CSV/XLSX format by clicking the **Download** button. They can also set up automatic email deliveries of these statistics at regular intervals by clicking on **Automatic Download**.

Additionally, users can clear the statistics using the **Reset Statistics** button.

Call Queue > Automatic Download

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

Automatic Download ☒

Report Type ☐ All ☐ Overview ☒ Agent Details ☒ Login Record ☒ Pause Log

Automatic Download Period

Email [Email Template](#)

Call Queue Statistics Automatic Download

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

Overview Tab

The overview page shows the following information:

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

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

Abandoned Call Calculation:

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

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

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

Details

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

Total Calls

Answered Calls

Abandoned Calls

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

Queue Statistics Details

Agent Details Tab

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

- **Time:** the date and time the call was received.
- **Agent:** the agent extension that was rung for the call.
- **Name:** the name of to agent that received the call.
- **Queue:** the queue that the call went to.
- **Caller ID Number:** the CID of the caller

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

Time	Agent	Name	Queue	Caller ID Number	Abandoned	Wait Time	Talk Time	Service Satisfaction
2024-10-21 13:37:52	1000	John	6500	5004	Yes	00:00:10	00:00:00	Not Surveyed
2024-10-21 14:12:08	1000	John	6500	5004	Yes	00:00:10	00:00:00	Not Surveyed
2024-10-21 14:13:19	1000	John	6500	5004	Yes	00:00:20	00:00:00	Not Surveyed
2024-10-21 14:13:56	1000	John	6500	5004	Yes	00:00:15	00:00:00	Not Surveyed
2024-10-22 10:06:28	1000	John	6500	4002	No	00:00:10	00:00:59	Not Evaluated
2024-10-21 12:13:44	1001	Alice	6500	5004	Yes	00:00:11	00:00:00	Not Surveyed
2024-10-21 13:32:36	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:39:33	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:34:05	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed
2024-10-21 13:34:26	1001	Alice	6500	5004	Yes	00:00:01	00:00:00	Not Surveyed

Agent details

Login Record Tab

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

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

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

Login Record

Pause Log Tab

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

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

Call Queue

Call Queue

Queue Recordings

Queue Switchboard

Call Queue Statistics

Download

Reset Statistics

Automatic Download

2024-10-01to2024-10-24Filter

Overview

Agent Details

Login Record

Pause Log

Statistics Report

Agent

Search

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

Total: 410 / page

Pause Log

Global Queue Settings

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

Call Queue > Global Queue Settings

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

Dynamic Agent Login Settings

Agent Login Code Suffix

Agent Logout Code Suffix

Example

If 6500 is the queue extension,
Agent Login Extension Suffix is *,
Agent Logout Extension Suffix is **,
dial **6500*** to log in and **6500**** to log out.

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

Agent Pause Reason

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

Agent Pause Reason

Default

Cancel

Save

Global Queue Settings

Dynamic Agent Login Settings	
Agent Login Code Suffix	Configure the code to dial after the queue extension to log into the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log in.
Agent Logout Code Suffix	Configure the code to dial after the queue extension to log out of the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log out.
Agent Pause Reason	
Agent Pause Reason Settings	Select the agent pause reason settings. Default: Use the default settings for the agent pause reason.

	Custom: User the custom settings. These settings should be configured using they corresponding key for each status. The user can upload a custom prompt which will be played for the agent once they set the pause reason.
Key Settings	Enter which key to press to set the different pause reasons.
Virtual Queue Callback Key Settings	
Enable	Select whether to enable or disable virtual queue callback feature. By default it's disabled.
Call Back Current Number	Press the feature key configured to set your current number as callback number.
Custom Callback Number	Press these feature key configured to set a custom callback number.
Continue Waiting	Press the feature key configured to continue waiting.

Speed Dial

Add Speed Dial

The CloudUCM supports the 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 CloudUCM.

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

The user should first click on "Add", then decide from one-digit up to four-digit combinations used for Speed Dial, and select a dial destination from "Default Destination". The supported destinations include extension, voicemail, conference room, voicemail group, IVR, ring group, call queue, page group, DISA, Dial by Name, and external number.

Note

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

Speed Dial > Create New Speed Dial

Enable Speed Dial

☒

* Speed Dial Extension

Speed Dial Name

Default Destination

Extension

1000

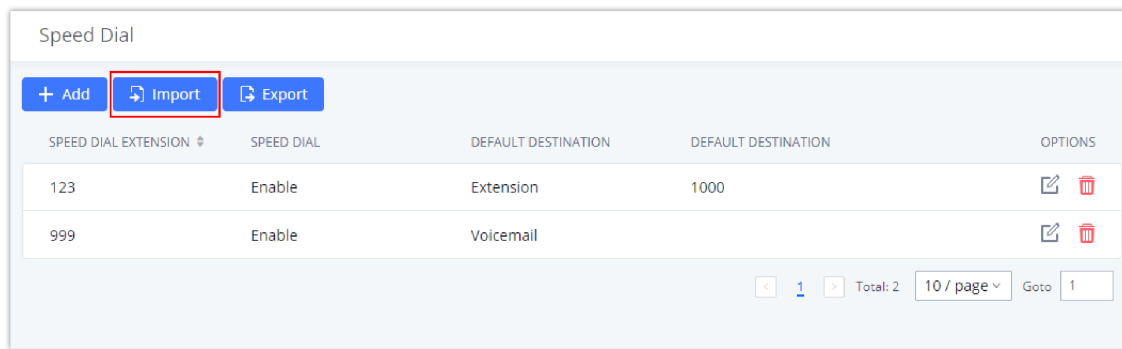
Speed Dial Destinations

Speed Dial				
+ Add Import Export				
SPEED DIAL EXTENSION	SPEED DIAL	DEFAULT DESTINATION	DEFAULT DESTINATION	OPTIONS
123	Enable	Extension	1000	 
999	Enable	Voicemail		 
< 1 > Total: 2 10 / page Goto 1				

List of Speed Dial

Import Speed Dial

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



Import Dial Speed

Then select the csv/xlsx file of the speed dial entries and click [Upload](#)

Important

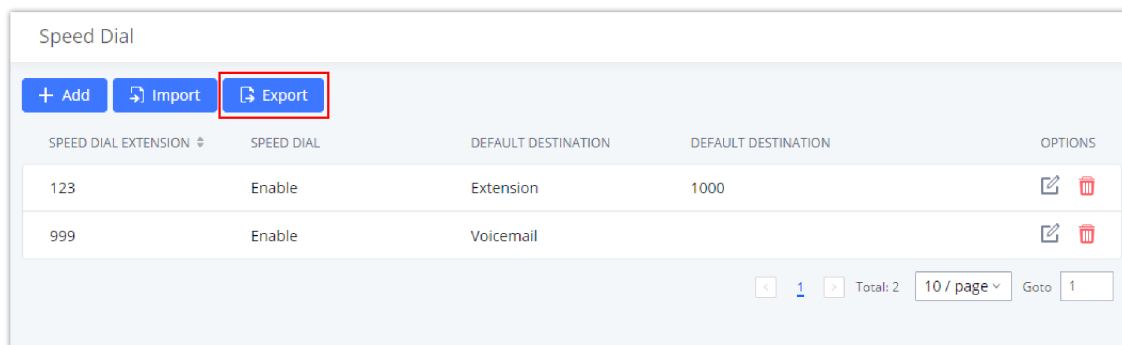
Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.

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 them.

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/xlsx file.



Export Dial Speed

Event List

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

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

URI	Configure the name of this event list (for example, office_event_list). Please note the URI name cannot be the same as the extension name on the IPPBX. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions/Extension Groups listed on the local IPPBX to be monitored in the event list.
Remote Extensions	If LDAP sync is enabled between the IPPBXs, 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

The screenshot shows the 'Create New Event List' configuration page. It features several sections:

- URI:** A text field containing 'test'.
- Event Type:** A dropdown menu set to 'Dialog'.
- Local Extensions:** A list of 9 available extensions (1003 'Betty' through 1007 'Kiki') and a 'Selected' list containing 3 items (1000 'Mia', 1001 'John', and 1002 'Chris').
- Remote Extensions:** Two empty lists for 'Available' and 'Selected' remote extensions.
- Special Extensions:** A large text area for manually entering extension numbers.

Create New Event List

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

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

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

Feature Codes

Feature Maps	
Blind Transfer	- Default code: #1 - Enter the code during active call. After hearing "Transfer", you will hear dial tone. Enter the number to transfer to. Then the user will be disconnected, and transfer is completed. - Options: ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee.
Attended Transfer	- Default code: *2 - Enter the code during active call. After hearing "Transfer", you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. In case of the called party does not answer, users could press *0 to cancel the call and retrieve the first call leg. - Options: ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee.
Transfer Dialing Timeout Period (s)	Configures the dial timeout period of blind and attended transfers.
Seamless Transfer	● Default code: *44 (Disabled by default). ● Seamless Transfer allows user to perform blind transfer using UCM feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple. ● During an active call use the feature code (*44 by default) followed by the number you want to transfer to in order to perform the seamless transfer.
Disconnect	- Default code: *0 - Enter the code during active call. It will disconnect the call. - Options: ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee.
Call Park	- Default code: #72 - Enter the code during active call to park the call. - Options: ● Disable ● Allow Caller: Enable the feature code on caller side only. ● Allow Callee: Enable the feature code on callee side only. ● Allow Both: Enable the feature code on both caller and callee.
Feature Code Input Timeout (ms)	Configure the maximum interval (ms) between digits for feature code activation.
Start/Stop Call Recording	-Default code: *3 - Enter the code followed by # or SEND to start recording the audio call and the PBX will mix the streams natively on the fly as the call is in progress. - Options:

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

Call Forward No Answer Deactivate	Default Code: *93 Disables Call Forward No Answer (CFNA) for the dialing extension. Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
Call Forward Unconditional Activate	Default Code: *72 Enables Call Forward Always (CFA) for the dialing extension. Assuming feature code is xxx, the following call forward setting methods are available: Method 1: Dial xxx and follow the system prompts. Method 2: Dial xxx + target extension (e.g., xxx6000). Method 3: Dial xxx + 0/1/2 + target extension (e.g., xxx16000). Methods 1 and 2 are supported in Basic. Methods 1 and 3 are supported in Advanced. (This feature code cannot be nested by other feature codes)
Call Forward Unconditional Deactivate	Default Code: *73 Disables Call Forward Always (CFA) for the dialing extension. Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: Basic: Dial xxx. Advanced: Dial xxx + 0/1/2.
Remote Call Forward Enable	Enable this option and configure the Remote Call Forward Whitelist below to allow specific extensions to dial the remote call forwarding feature codes to set call forwarding for any extension.
Remote DND / Call Forward Settings	
Enable	Enable this option and configure the Whitelist below to allow specific extensions to dial feature codes to set DND or call forwarding for any extension.
Remote Call Forward Busy Enable	Default code: *65 Configures and enables CFB for any extension.
Remote Call Forward No Answer Enable	Default code: *66 Configures and enables CFNA for any extension.
Remote Call Forward Always Enable	Default code: *67 Configures and enables CFU for any extension.
Remote DND Enable	Default code: *68 Enables Do Not Disturb for any extension.
Remote Call Forward Busy Disable	Default code: *651 Disables CFB for any extension.
Remote Call Forward No Answer Disable	Default code: *661 Disables CFNA for any extension.
Remote Call Forward Always Disable	Default code: *671 Disables CFU for any extension.

Remote DND Disable	Default code: *681 Disables Do Not Disturb for any extension.
Whitelist	Extensions in this whitelist can configure DND or call forwarding for any extension via feature codes.
Feature Codes	
Voicemail	
Voicemail Access Code	Default Code: *98 Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box. (This feature code cannot be nested by other feature codes)
My Voicemail	Default Code: *97 Press *97 to access the voicemail box.
Voicemail Group Access Code	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. (This feature code cannot be nested by other feature codes)
Agent Unpause	- Default Code: *84 - Unpause the agent in all call queues.
Dynamic Agent Logout	Default code: *85 Log the dynamic agent out of all queues.
Call Pickup	
Pickup on Ringing Prefix	Picks up a ringing call for another extension. Example: If the prefix is **, and there is a call ringing ext 1008, dial **1008 from a different extension to pick up the call to 1008. (This feature code cannot be nested by other feature codes)
Pickup In-call Prefix	Picks up an ongoing call for another extension. Example: If the feature code is *45, and ext 1008 is in a call, dialing *45 and then 1008 following the prompt will take that call . Note: The feature code user must be in the extension's Allowed to seamless transfer list to pick up calls for it.
Pickup Extension	This is the feature code to pick up incoming calls for other extensions in the same pickup group. The default setting is *8.
Call Barging	
Enable Spy	Check this box to enable spy feature codes.
Listen Spy	This is the feature code to listen in on a call to monitor performance. Your line will be muted, and neither party will hear you. The default setting is *54.

	(This feature code cannot be nested by other feature codes)
Barge Spy	This is the feature code to join in on the call to assist both parties. The default setting is *56. (This feature code cannot be nested by other feature codes)
Whisper Spy	This is the feature code to speak to only one party in the call. For example, you could whisper to employees to help them handle a call. Only an employee on your account will be able to hear you. The default setting is *55. (This feature code cannot be nested by other feature codes)
PMS	
PMS Wakeup Service	Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service.
PMS Remote Wakeup Service	Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions.
Update PMS Room Status	2 methods are available: 1. Dial the room status feature code + housekeeper code, listen to the prompt and then dial the appropriate key for the desired room status. Example: The housekeeper with the housekeeper code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available. 2. Dial room status feature code*housekeeper code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: The housekeeper with housekeeper code 0001 dials *23*0001*1 to change room status Available.
Misc	
Paging Prefix	Configure the paging prefix for paging. For example, if the Paging Prefix is set to *81, dial *816000 to initiate a paging call to extension 6000. (This feature code cannot be nested by other feature codes)
Intercom Prefix	Configure the intercom prefix for intercom calls. For example, if the Intercom Prefix is set to *80, dial *806000 to initiate an intercom call to extension 6000. (This feature code cannot be nested by other feature codes)
Blacklist Add	Follow the voice prompt to add a caller ID to blacklist.
Blacklist Last Caller	Add the last inbound caller ID number to blacklist.
Blacklist Remove	Follow the voice prompt to remove a caller ID from blacklist.
Direct Dial Mobile Phone Prefix	If calling mobile phone numbers is permitted, use this prefix plus the extension number to dial the mobile phone number of this extension directly. (This feature code cannot be nested by other feature codes)
Call Completion Request	If the caller wants to use CC to complete a call, he/she can dial this code. After the CC has been registered successfully, the system will start to monitor the status of the callee. The system will call back the caller when the callee's extension is available.
Call Completion Cancel	If the caller has requested CC successfully, and he/she doesn't need to call back anymore, he/she can dial this code to cancel the request.
Presence Status	Dial this feature code to set the presence status of the extension.
Call Flip	- Default code: *46 - Dial this code to move the call of this extension from another device to the current device.

Wakeup Service	Dial this feature code to access UCM Wakeup Service. You can add, update, activate or deactivate UCM Wakeup Service.
Remote Extension Privilege Update	Whitelisted extensions will be able to use the Remote Extension Privilege Update feature code to remotely change any extension's outgoing call privilege. Note: After this function has been enabled, the extension in the whitelist can set the privilege for outgoing calls of any extension by dialing the feature code.
Remote Extension Privilege Update Whitelist	Remote Extension Privilege Update Whitelist Procedure: 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.
Privileged Call	Dial the feature code + extension number, for example *001002 to hang up the current call of extension 1002 with privilege, and then call extension 1002.
Privileged Call Whitelist	The extensions in this white list can use the feature code of the privileged call.
Priority Call	Makes a high priority call to a specified extension by dialing the feature + extension number. If the specified extension is an ongoing call, it will be forcibly hung up to allow the caller to ring the extension.
Priority Call Whitelist	Extension in the whitelist will be allowed to use this feature code to make priority calls.

The CloudUCM also allows users to one-click enable/disable specific feature code, as shown below:

Feature Codes

Feature Maps

DND / Call Forward

Feature Codes

Cancel

Save

Default: All

Voicemail

Voicemail Access Code:

*98

☒

Voicemail Group Access Code:

*99

☒

My Voicemail:

*97

☒

Direct Dial Voicemail Prefix:

*

☒

Call Queue

Agent Pause:

*83

☒

Dynamic Agent Logout:

*85

☒

Agent Unpause:

*84

☒

Call Pickup

Pickup on Ringing Prefix:

**

☒

Pickup Extension:

*8

☒

Pickup In-call Prefix:

*45

☐

Call Barging

Enable Spy:

☐

Barge Spy:

*56

Listen Spy:

*54

Whisper Spy:

*55

PMS

PMS Wakeup Service:

*35

☒

PMS Remote Wakeup:

*37

☒

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

Enable/Disable Feature codes

Parking Lot

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

Parking Lot

Parking Lot Settings

Parking Lot Status

+ Add

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

1

Total: 2 10 / page Goto 1

Parking Lot

The user can create a new Parking lot by clicking on the button "Add" :

Create New Parking Lot		Cancel	Save
* Parking Lot Extension:		* Parking Lot Name:	
* Parking Slots:		Use parklot as extension:	☐
* Parking Timeout (s):	300	Music on Hold Playlists:	Default
Fallover Destination:		Ring-All Callback on Timeout:	☐
Forward to Destination on Timeout:	☐		

New Parking Lot

Parking Lot Extension	• Default Extension: 700 • During an active call, initiate blind transfer and then enter this code to park the call. Note: The user change the default extension for the parking lot to a different extension.
Parking Lot Name	Set a name to the parking lot
Parked Slots	• Default Extension: 701-720 • These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.
Use Parking lot as Extension	If checked, the parking lot number can be used as extension. The user can transfer the call to the parking lot number to park the call. Please note this parking lot number range might conflict with extension range.
Parking Timeout (s)	• Default setting is 300 seconds, and the maximum limit is 99.999 seconds. • This is the timeout allowed for a call to be parked. After the timeout, if the call is not picked up, the extension who parks the call will be called back.
Music On Hold Classes	Select the Music on Hold Class.
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 CloudUCM provides call park and call pickup features via feature code.

Park a Call

Two feature codes 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)**

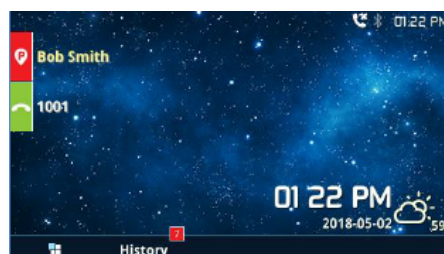
During an active call, initiate blind transfer (default code #1) and then dial 700 to park the call. Parking lot number (default range 701 to 720) will be announced after parking the call.

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 that parks the call will be called back.

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

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



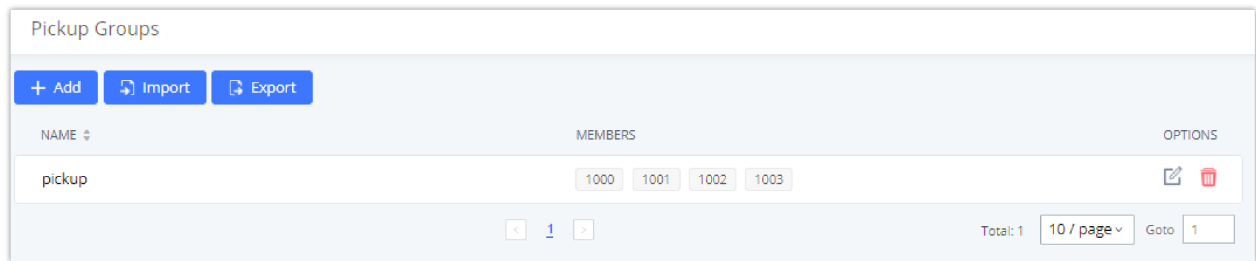
Monitored Call Park CID name

ADVANCED CALL FEATURES

Pickup Groups

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

Configure Pickup Groups

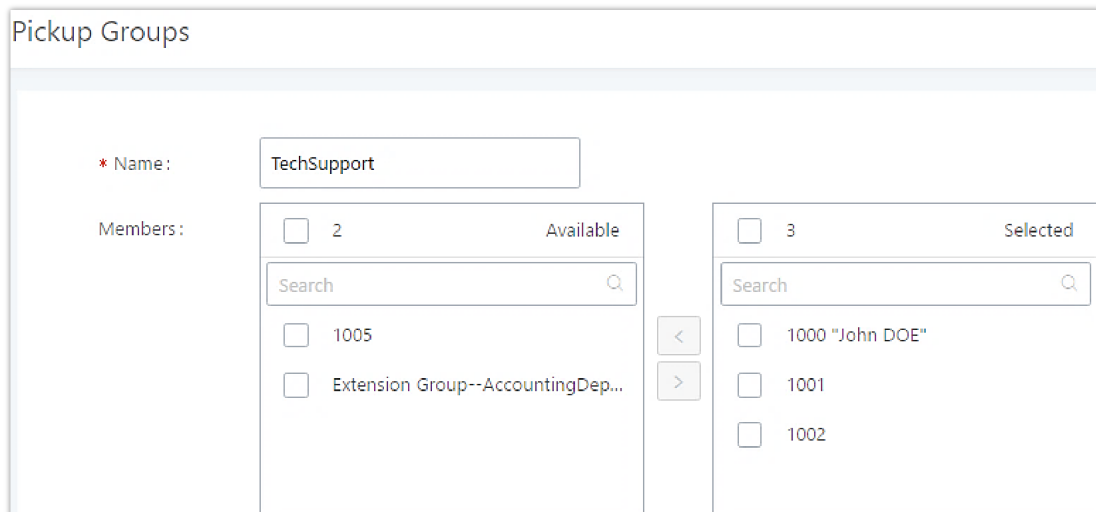


Pickup Groups interface

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

- Click on **+ Add** to create a new pickup group.
- Click the **Import** button to upload the pickup group information in CSV/XLSX format.
- Click the **Export** button to generate pickup group information in CSV/XLSX format.
- Click on  to edit the pickup group.
- Click on  to delete the pickup group.

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



Edit Pickup Group

Configure Pickup Feature Code

When picking up the call for the pickup group member, the user only needs to dial the pickup feature code. It is not necessary to add the extension number after the pickup feature code. The pickup feature code is configurable under Web GUI→**Advanced 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 to perform the call pickup operation. The following figure shows where you can customize these feature codes.

Feature Codes
Feature Maps
DND/Call Forward
Feature Codes

Reset All
Default All

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

Edit Pickup Feature Code

Dial By Name

Dial by Name is a feature on the PBX that allows the caller to search for 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 the business image for the enterprise.

Dial by Name Configuration

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

Create New Dial By Name

* Name:

Name

* Extension:

7101

Custom Prompt:

None

Upload Audio File

Members:

30 items

Available

Search

1000

1001

1002

1003

1004

0 item

Selected

Search

None

LDAP Phonebook:

1 item

Available

Search

ou=GStest,dc=pbx,dc=com

0 item

Selected

Search

None

Options

* Prompt Wait Time:

5

Query Type:

By Last Name + First Name

By First Name + Last Name

Select Type:

By Order

By Menu

Create Dial by Name Group

User Settings

First Name:

John

Last Name:

DOE

Email Address:

* User Password:

* Language:

Default

* Concurrent Registration...

1

Mobile Phone Number:

Configure Extension First Name and Last Name

1. Name

Enter a Name to identify the Dial by Name group.

2. Extension

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

3. Custom Prompt

This option sets a custom prompt for the directory to announce to a caller. The file can be uploaded from the page "Custom Prompt". Click "Upload Audio File" to add record.

4. Available Extensions/Selected Extensions

Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have a valid first name and last name configured under Web GUI→**Extension/Trunk**→**Extensions** to be searchable in the 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 do not want to receive them directly.

5. Prompt Wait Time

Configure "Prompt Wait Time" for the Dial By Name feature. During a Dial By Name call, the caller will need to input the first letters of the First/Last name before this wait time is reached. Otherwise, a timeout will occur, and the call might hang up. The timeout range is between 3 and 60 seconds.

6. Query Type

Specify the query type. This defines how the caller will need to enter to search the directory.

By First Name: enter the first 3 digits of the first name to search the directory.

By Last Name: enter the first 3 digits of the last name to search the directory.

7. Select Type

Specify the selected type on the search 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 numbers 1 to 8 to select and call, or press 9 for results on the 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, the user could use '*' to exit from Dial by Name, then re-enter IVR and start a new event. The following example shows how to use this option.

Edit IVR: Test

Basic Settings Key Pressing Events

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

Dial By Name Group In IVR Key Pressing Events

Edit Inbound Rule

Save

* Pattern:

CallerID Pattern:

Separate patterns by commas, such as "._":

Disable This Route:

☐

Prepend Trunk Name:

☐

Prepend User Defined Nam...

☐

Inbound Multiple Mode:

☐

Alert-info:

None

▼

Dial Trunk:

☐

Privilege Level:

Internal

▼

DID Destination:

Allowed to seamless transfe...

Default Mode

* Default Destination:

Dial By Name

▼

DialByNameGP1

▼

Dial by Name Group In Inbound Rule

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

DISA

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

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

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

Create New DISA

* Name:

* Password:

Permission:

Internal

▼

* Response Timeout...

* Digit Timeout:

Allow Hang-up:

☐

Replace Display Nam...

☐

Create New DISA

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

Name	Configure DISA name to identify the DISA.
------	---

Password	Configure the password (digit only) required for the user to enter before using DISA to dial out. Note: The password must be at least 4 digits.
Permission	Configure the permission level for DISA. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the DISA, the IPPBX will compared the DISA's permission level with the outbound route's privilege level. If the DISA's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Response Timeout	Configure the maximum amount of time the IPPBX will wait before hanging up if the user dials an incomplete or invalid number. The default setting is 10 seconds.
Digit Timeout	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
Allow Hangup	If enabled, during an active call, users can enter the IPPBX hangup feature code (by default it is *0) to disconnect the call or hang up directly. A new dial tone will be heard shortly for the user to make a new call. The default setting is "No".
Replace Display Name	If enabled, the UCM will replace the caller display name with the DISA name.

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

Callback

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

The callback feature works as follows:

1. Configure a new callback on the CloudUCM.
2. On the CloudUCM, configure the destination of the inbound route for callback.
3. Save and apply the settings.
4. The user calls the number of the CloudUCM using the mobile phone, which goes to the 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 CloudUCM 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 CloudUCM instead of to the mobile phone. Therefore, the user will not be charged on mobile phone services for long-distance or international calls.

To configure callback on the CloudUCM, go to the Web GUI→**Advanced Call Features**→**Callback** page and click on [+ Create New Callback](#) . Configuration parameters are listed in the following table.

Name	Configure a name to identify the Callback. (Enter at least two characters)
CallerID Pattern	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the CallerID match this pattern so that the caller can get callback after hanging up the call.

	Note: If leaving as blank, all numbers are allowed to use this callback.
Outbound Prepend	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.
Delay Before Callback	Configure the number of seconds to be delayed before calling back the user.
Destination	Configure the destination which the callback will direct the caller to. Two destinations are available: • IVR • DISA The caller can then enter the desired number to dial out via IPPBX trunk.

Scheduled Call

The call scheduler feature allows the user to schedule a wakeup call to a specific extension. The user can choose the time and date of the call, and when the time arrives, a call will be initiated to the designated extension(s). When the call is answered, the chosen prompt will be played.

Scheduled Call > Create New Scheduled Call

Enable Scheduled Call



* Name

Prompt



Upload Audio File

Custom Date



* Date



* Time



* Members



5

Available



1000



1001



1002



1003



1004



0

Selected



None

Cancel

Save

Scheduled Call

Fax Sending

The CloudUCM supports sending Fax via the Web GUI. This feature can be found on **Advanced Call Features > Fax Sending** page. The user can enter the number of the destination, then the fax will be sent to a fax gateway on the receiving end.

After entering the fax number, please upload the PDF file that you wish to send as a fax.

Fax Sending

* External Fax Number:

0123456789

Fax File:

test.pdf

Send

File Send Progress

Delete

Clear

External Fax Number

Fax Sending in Web GUI

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

Fax Sending

* External Fax Number:

Fax File:

Choose File to Upload

Send

File Send Progress

Delete

Clear

External Fax Number

☐	NAME	DATE	SENDER	EXTERNAL FAX NUMBER	CURRENT PROGRESS	OPTIONS
☐	test.pdf	2021-01-25 11:29:19 UTC+01:00	admin	0123456789	Sending... 5%	

Fax Send Progress

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

Fax/T.38

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

Fax/T.38 > Create New Fax Extension

* Extension

7200

* Name

* Email Address

Add Email Address

Cancel

Save

Create New Fax Extension

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

Fax Settings

• Enable Error Correction Mode :

☒

• Maximum Transfer Rate :

14400

• Minimum Transfer Rate :

2400

• Max Concurrent Sending Fax :

Single

• Fax Queue Length :

6

User Information in Fax Header :

☐

Fax Header Information :

Default Email Address :

Email Template

Send PDF Files Only :

☐

Enable Fax Resend :

☐

Max Resend Attempts :

5

Fax Resend Frequency :

50

Fax Settings

Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is “Yes”.
Maximum Transfer Rate	Configure the maximum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000, and 14400. The default setting is 14400.
Minimum Transfer Rate	Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000, and 14000. The default setting is 2400.
Max Concurrent Sending Fax	Configure the concurrent fax that can be sent by CloudUCM. Two modes, “Only” and “More”, are supported. Only: Under this mode, the CloudUCM allows only a single user to send a fax at a time. More: Under this mode, the CloudUCM supports multiple concurrent fax sending by the users. By default, this option is set to “only”.
Fax Queue Length	Configure the maximum length of Fax Queue from 6 to 10. The default setting is 6.
User Information in Fax Header	If enabled, this will give users the option to send a special header in SIP fax messages.
Fax Header Information	Adds fax header into the fax file.

Default Email Address	Configure the Email address to send the received Fax to if the user's Email address cannot be found. Note: The extension's Email address or the Fax's default Email address needs to be configured to receive Fax from Email. If neither of them is configured, Fax will not be received from email.
Template Variables	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users. The template variables are: ◦ \${CALLERIDNUM} : Caller ID Number ◦ \${CALLERIDNAME} : Caller ID Name ◦ \${RECEIVEEXTEN} : The extension to receive the Fax ◦ \${FAXPAGES} : Number of pages in the Fax ◦ \${VM_DATE} : The date and time when the Fax is received. (Format: MM/dd/yyyy hh:mm:ss)
Send PDF Files Only	If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.
Enable Fax Resend	Enables the fax resend option which allows the UCM to keep attempting to send faxes up to a specified amount of times. Additionally, if fax still fails to send, a <i>Resend</i> button will appear in the File Send Progress list in <i>Advanced Call Features > Fax Sending</i> to allow manual resending.
Max Resend Attempts	Configures the number of the maximum attempts to resend the fax. The default value is set to 5.
Fax Resend Frequency	Configures the Fax Resend Frequency. The default value is set to 50.

FAX/T.38 Settings

Announcement Center

The CloudUCM supports the Announcement Center feature, which allows users to pre-record and store voice messages in the CloudUCM with a specified code. The users can also create group with specified extensions. When the code and the group number are dialed together in the combination of **code + group number**, the specified voice message is sent to all group members and only extensions in the group will hear the voice message. To access the Announcement Center configuration page, please navigate to **Feature Codes → Announcement Center**

Announcement Center

+ Add Announcement Center

Code	Name	Options
55	Announcement_1	 

Total: 1 < 1 > 10 / page Goto

+ Add Group

Number	Name	Members	Options
33	Group_1	1001 1002	 

Total: 1 < 1 > 10 / page Goto

Announcement Center

Announcement Center Settings

Users can configure the following settings when creating an Announcement Center:

Announcement Center > Create New Announcement Center

Name

Code

Custom Prompt

Upload Audio File

Ring Timeout (s)

30

Auto Answer

No

Call Privileges

Internal

Announce Message Caller-ID

☐

Create a New Announcement Center

Name	Configure a name for the newly created Announcement Center to identify this announcement center.
Code	Enter a code number for the custom prompt. This code will be used in combination with the group number. For example, if the code is 55, and group number is 666. The user can dial 55666 to send prompt 55 to all members in group 666. Note: The combination number must not conflict with any number in the system such as extension number or conference number.
Custom Prompt	This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page ‘Custom Prompt’. Click ‘Prompt’ to add additional record. Note: When uploading a custom, please ensure that the custom prompt file respect the following requirements. • The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. • If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB. File name can only contain alphanumeric characters and special characters - _
Ring Timeout (s)	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. The default setting is “No”.
Call Privileges	Please select the permission level for outgoing calls.
Announce Message Caller-ID	If enabled, the caller’s CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.

Group Settings

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

1. Click

+ Add Group

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

Create New Group

* Name:

GStest

* Number:

666

Members:

☐

27 items

Available

☐

3 items

Selected

Search

☐ 1003

☐ 1004

☐ 1005

☐ 1006

☐ 1007

Search

☐ 1000

☐ 1001

☐ 1002

Announcement Center Group Configuration

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

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

- Click [+ Add Announcement Center](#) to create a new Announcement Center.
- Give a name to the newly created Announcement Center.
- Specify the code that will be used with the group number to send the voice message to.
- Select the message that will be used by the code from the Custom Prompt drop-down menu. To create a new Prompt, please click the "Prompt" link and follow the instructions on that page.

Announcement Center > Create New Announcement Center

* Name

* Code

* Custom Prompt [Upload Audio File](#)

* Ring Timeout (s)

* Auto Answer

Announce Message Caller-ID ☐

Announcement Center Code Configuration

Code and Group number are used together to direct a 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 CloudUCM. All the members in group 666 who 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	Edit Delete

Total: 1

[+ Add Group](#)

NUMBER	NAME	MEMBERS	OPTIONS
666	GStest	1000 1001 1002	Edit Delete

Total: 1

Announcement Center Example

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 the steps below:

1. Navigate on the web GUI under **Advanced Call Features → Announcement**
2. Click on [+ Add](#) to add a new Announcement.
3. Configure the required fields Name, Prompt, and Default Destination to be used for the announcement.

Save and apply the configuration.

Create New Announcement

* Name:

Prompt: [Upload Audio File](#)

Default Destination:

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

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.

Announcement Parameters

Shared Call Appearance (SCA)

Shared Call Appearance (SCA) functionality has been added to the CloudUCM. With SCA, users can assign multiple devices to one extension, configure endpoints to monitor that extension, take 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 SCA option under the "Feature" tab, and in the "Other Settings" category.

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

Other Settings

Ring Timeout (s)		Auto Record	OFF
* Skip Trunk Auth	No	Dial Trunk Password	
Support Hot-desking Mode	☐	Enable LDAP	☒
Use MOH as IVR ringback tone.	☐	* Music On Hold	Default
Call Waiting	☒	Stop Ringing	☐
Email Missed Call Log	☐	Enable SCA	☒
Emergency CID		* Language	Default

Enabling the SCA option under Extension > Features

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

SCA					
SCA Number Group			SCA Line Status		
STATUS	SHARED LINE	ROLE	IP AND PORT	SUBSCRIBED	OPTIONS
Unavailable	1000	shared	--	no	+ -
1 Total: 1 10 / page Goto 1					

SCA Number Configuration

3. Configure the private number as desired.

Add Private Number

* Private Number:

Related Shared Line:

Enable This Number: ☒

Allow Origination from This Number: ☒

Allow Termination to This Number: ☒

SCA Private Number Configuration

4. Once the private number has been created, users must now register a device to it. To properly register a device to the private number, use the configured private number as the SIP User ID. Auth ID and Password will be the same as the main extensions. Once registration is complete, SCA is now configured.

Edit SCA Number Group:

* Shared Line Number:

Allow Call Retrieve from Another Location: ☒

Alert All Appearances for Group Paging Calls: ☐

Multiple Call Arrangement: ☐

Allow Bridging between Locations: ☐

Bridge Warning Tone:

SCA Options

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

The following table describes the SCA Number configuration setting:

Private Number	Configures the private number for the SCA.
Related Shared Line	Display the related shared line.
Enable This Number	Whether enable this private number. If not enabled, this private number is only record in DB, it will not affect other system 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.

Add SCA Private Number

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

Shared Line Number	While SCA is enabled, this number will be the same as the extension number.
Allow Call Retrieve from Another Location	Allows remote call retrieval. Must be enabled in public hold. By default, it is enabled.
Alert All Appearances for Group Paging Calls	Allows all SCA group members to ring when the SCA shared number is paged. If disabled, only the SCA shared number will ring when paged. By default, it is disabled.
Multiple Call Arrangement	Allows simultaneous calls in an SCA group. By default, it is disabled.
Allow Bridging between Locations	Allows location bridging for SCA group. Must be enabled when using the Barge-In feature. By default, it is disabled.
Bridge Warning Tone	Configures the notification in the bridge when another party join. ◦ None: No notification sound. ◦ Barge-In only: Notification sound will play when another party join. ◦ Barge-In and Repeat: Notification sound will play when another party joins and repeat every 30 seconds. By default, it is set to "Barge-In Only".

Editing the SCA Number

Emergency Calls

Emergency Calls

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

The CloudUCM is fully compliant 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 sent to the configured email address(es).

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

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

1. Navigate on the web GUI under **Advanced Call Features → Emergency Calls**
2. Click on  to add a new emergency number.
3. Configure the required fields "Name, Emergency Number, and Trunk(s) to be used to reach the number".
4. Save and apply the configuration.

Create New Emergency Call

* Name:

* Emergency Number:

Emergency Level:

Disable Hunt on Busy: ☐

Custom Prompt: [Prompt](#)

* Use Trunks:

* Members Notified:

☐ 11 items Available

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

☐ 1 item Selected

☐ 1000 "James tuan"

Strip:

Prepend:

Auto Record: ☒

Send Recording File: ☒

Email Address: [+](#)

Emergency Number Configuration

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

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

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

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

10 / page

Goto

1

911 Emergency Sample

Emergency Recordings

The CloudUCM 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 ↕
No Data				
Options				
Copyright © Grandstream Networks, Inc. 2022. All Rights Reserved.				

Emergency Recordings

Emergency Location Mapping

To ensure compliance with Kari's Law and the Ray Baum's Act, CloudUCM's Emergency Calls feature supports comprehensive emergency location mapping. This allows administrators to associate both **individual extensions** and **IP subnets** with Emergency Location Identification Numbers (ELINs).

These ELINs are provided to E911 service providers, enabling them to identify a caller's precise location based on their specific device or network segment. This feature can be configured under **Advanced Call Features** → **Emergency Calls** → **Emergency Location Mapping**.

Emergency Calls > Create New Emergency Location Mapping

* ELIN

Geolocation Routing

Send PAI Header ☐

Type

Location Mapping

☐ Subnet	Location	Options
 No data		

Emergency Location Mapping

- **ELIN:** The emergency location identification number registered with the E911 provider. This number will be sent out as the emergency call's CID number.
- **Geolocation Routing:** Toggles whether to include the *Geolocation* header in the emergency call SIP INVITE message. The *Location* field value will be used as the *Geolocation* header value.
- **Send PAI Header:** PAI stands for P-Asserted-Identity. Once enabled, the ELIN number will be sent via the PAI header field to ensure accurate location tracking for emergency services. This PAI header field takes precedence over the PAI header field of the trunks.
- **Type:**
 - **Network Method:** Click add then enter the subnet address and the position.
 - **Extension Method:** Click add then enter the extension number and the position.

Important Note

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

Restrict Calls

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

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

Restrict Calls

Configure Restrict Calls

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

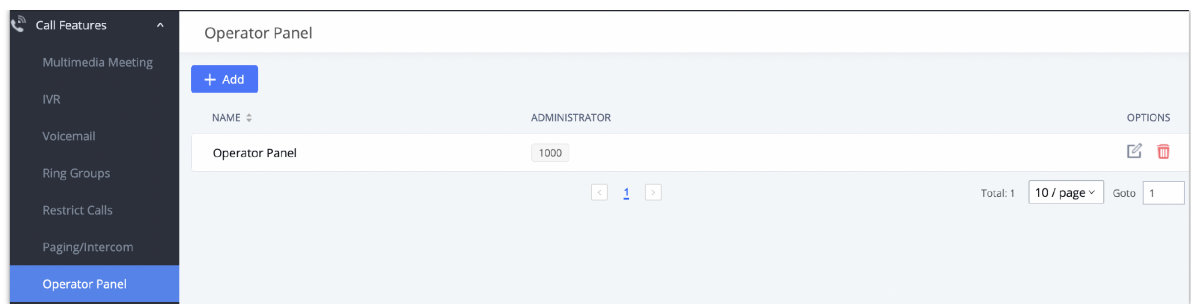
Name	Configure Restrict call's name
Restrict Calls between extensions	When enabled, members of the group cannot dial other extension, only the numbers in the Allowed List. By default it's enabled.
Members	Configure the members that will not be able to call any extensions besides those in the Allowed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

Operator Panel

Configure Operator Panel

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

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



Operator Panel Configuration Page

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



to edit the operator panel.

- Click on



to delete the operator panel.

Name	The Operator panel name.
Administrator	The operator of the call console can select extensions, extension groups, and departments. 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 checked Ring Groups will be supervised by the administrator. Select “All”, all Ring Groups and subsequent updates will be automatically supervised by the administrator.
Voicemail Groups	The checked Call Queue will be supervised by the administrator. Select “All”, all Call Queue and subsequent updates will be automatically supervised by the administrator.
Call Queue	The checked Call Queue will be supervised by the administrator. Select “All”, all Call Queue and subsequent updates will be automatically supervised by the administrator.
Parking Lot	The checked Parking Lot will be supervised by the administrator. Select “All”, all Parking Lot and subsequent updates will be automatically supervised by the administrator.

Time Condition Routing

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

Time Condition Routing > Create New Time Condition Routing

* Name

Name

* Time

Create new time groups in [Time Settings -> Custom Time Groups.](#)

Time Match

* Default Destination

Extension

Time Mismatch

* Default Destination

Extension

Cancel

Save

Time Condition Routing

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

MESSAGING

IM Settings

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

IM Settings

Read Receipts

☒

Notify Inactive Users of New Messages

☒
[Email Template](#)

* Max File Size Upload (MB)

50

Cancel

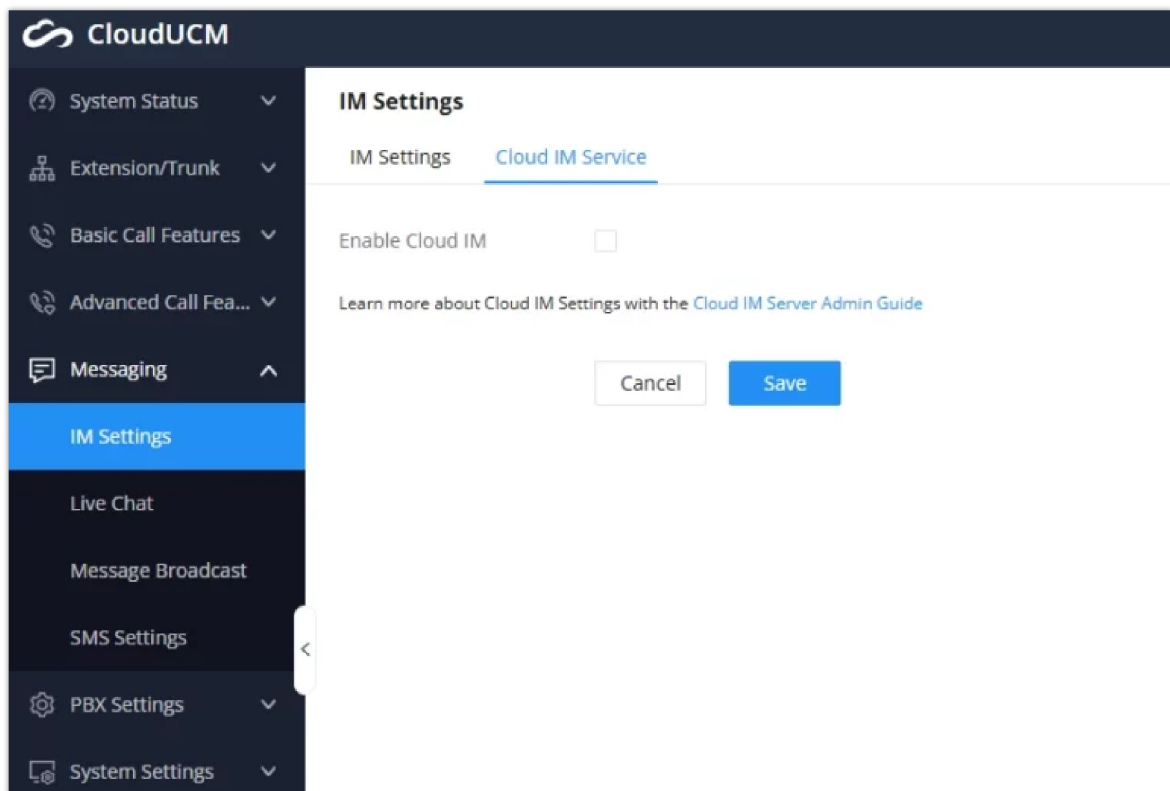
Save

IM Settings

Read Receipts	1. Configures whether Wave users can see the read status of sent messages when using local IM. 2. If using Cloud IM, read receipts must be configured on the IM server (GDMS or custom IM server) being used. To configure this on GDMS, navigate to the top right corner of the GDMS page Plan & Services->My Plans->Edit Cloud IM page.
New Message Email Notification	Regardless of whether you are currently using local IM or Cloud IM, when Wave is offline under this domain for more than 7 days after enabling it, an email notification of new messages will be sent when a new message is received.
Maximum Chat File Size (MB)	1. Configures whether Wave users can see the maximum chat file size when using local IM. 2. If using Cloud IM, maximum chat file size must be configured on the IM server (GDMS or custom IM server) being used. To configure this on GDMS, navigate to the top right corner of the GDMS page Plan & Services->My Plans->Edit Cloud IM page

Cloud IM Service

The Cloud IM Service allows administrators to configure and manage instant messaging for CloudUCM instances. Using this page, users can enable Cloud IM, connect the CloudUCM to a Cloud IM server, and define essential parameters to control messaging behavior.



Cloud IM Service

Enable Cloud IM	Activate Cloud IM for this CloudUCM instance if your plan includes the Cloud IM Service. Local chat data will no longer be stored on the CloudUCM.
Local Proxy	Use the CloudUCM as a proxy to forward messages and files if the Cloud IM server is temporarily unreachable due to certificate issues.
Cloud IM Server Address	Required. Enter the address of the external Cloud IM server. This can be a server you host yourself or the IM server address from another CloudIM-enabled UCM device.

Service ID	Unique ID used by the CloudUCM to authenticate with the Cloud IM server.
Key	Key used by the CloudUCM to authenticate with the Cloud IM server.
Site Name	Name of the site or location associated with this CloudUCM instance.
Trusted User	Specify trusted users allowed to access Cloud IM. Only letters, numbers, and special characters are allowed.
Prefix	Extension prefix 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

Note:

For more information on the Cloud IM service and configuration details, please refer to the [IPPBX Cloud IM Server – Admin Guide](#).

Live Chat

Live Chat feature allows to create chat channels that can be embedded on your website to enable your client to reach your customer service more easily. The client can chat with the support agent either through text or through a voice call.

Live Chat > Create New Live Chat

* Name

* Destination

Extension

Web Page Language

Use Browser Language

Visitor Information

Require Visitor Info

☐

Privacy Control

☐

Call Settings

Allow Visitor to Call

☐

Customer Service Agent Information

Avatar



Please select a file in png, jpg, jpeg format.

* Name

Support

Show Agent's Real Name

☐

Cancel

Save

Create New Live Chat

Name	Enter the name of the Live Chat
Destination	Configure the destination of this Live Chat.
Web Page Language	Configure the language of visitor page.
Visitor Information	
Require Visitor Info	Configure the visitor information required to start a live chat session.
Privacy Control	If enabled, visitors must consent to allow the processing of personal data and cookies before entering Live Chat.
Call Settings	
Allow Visitor To Call	If enabled, visitors will have the option to call the configured destination from this Live Chat.
Customer Service Agent Information	

Avatar	Upload the avatar of the agent. Please select a png, jpg, or jpeg format file.
Name	Enter the name of the agent.
Show Agent's Real Name	Enable this option to show the agent's real name in the live chat.
Chat Settings	
Welcome Message	Configure the initial message to display to visitors when they first enter the live chat session.
Reply to First Message	Configure the message to send to visitors in response to their first message.
Visitor Chat Log Retention Time (days)	This value determines how long a visitor's chat history will be kept before it's deleted automatically. Note:
Live Chat Link Address	This link can be embedded onto web pages. Clicking it will connect visitors to the configured Live Chat destination. This link can also be entered directly into the browser address bar for testing purposes.

Message Broadcast

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

Message Broadcast > Send Message Broadcast

* Name

* Sender

* Message Content

* Recipients

Selected(0)

Company Contact

☐ All
☐ Technical Support
☐ Quality Control
☐ Sales
☐ IT
☐ Marketing
☐ Human Resources
☐ Finance
☐ 1000 " "

Cancel

Send

© 2023 Grandstream Networks, Inc.

Send Message Broadcast

Name	Configure the name of this broadcast.
-------------	---------------------------------------

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

SMS Settings

SMS Settings

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

SMS Settings > SMS Settings

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

Cancel
Save

Enable SMS ☒

SMS Carrier

Region

Account ID

Secret

From

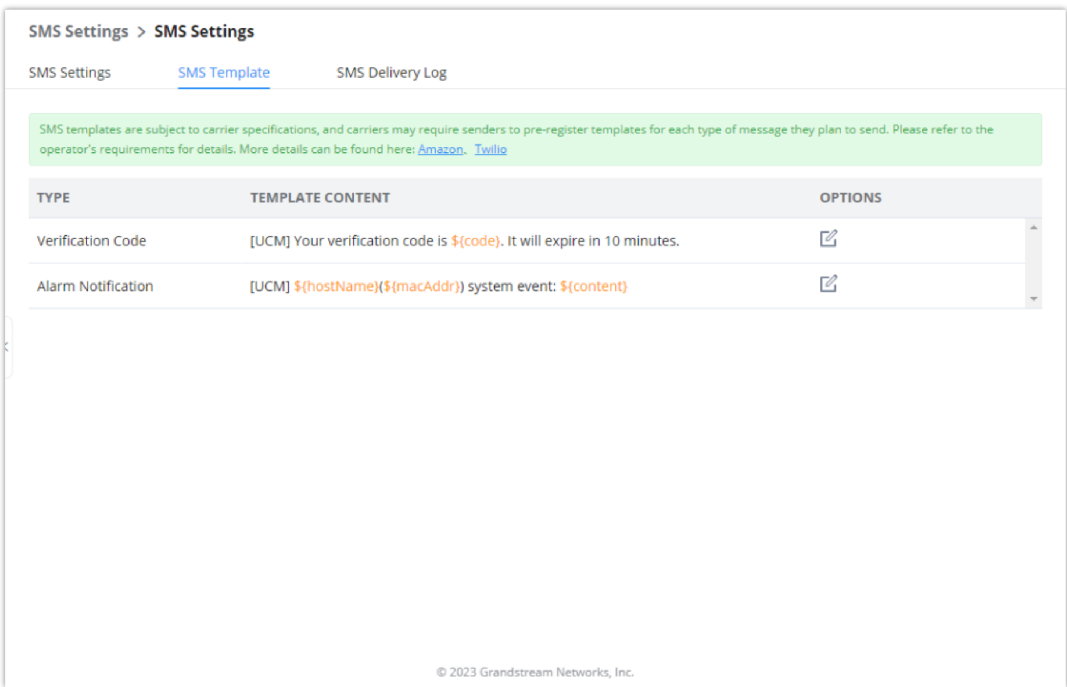
Test

SMS Settings

Enable SMS	Tick this box to enable SMS service.
SMS Carrier	Choose the SMS carrier: ● Amazon ● Twilio
Region	Choose the region.
Account ID	Enter the ID of the account created at the carrier.
Secret	Enter the secret code.
Account ID	Configures Twilio account ID.
Auth Token	The key of the Twilio account.
Messages Server ID	Twilio SMS Server ID
From	Enter the number phone allocated for the UCM.

SMS Template

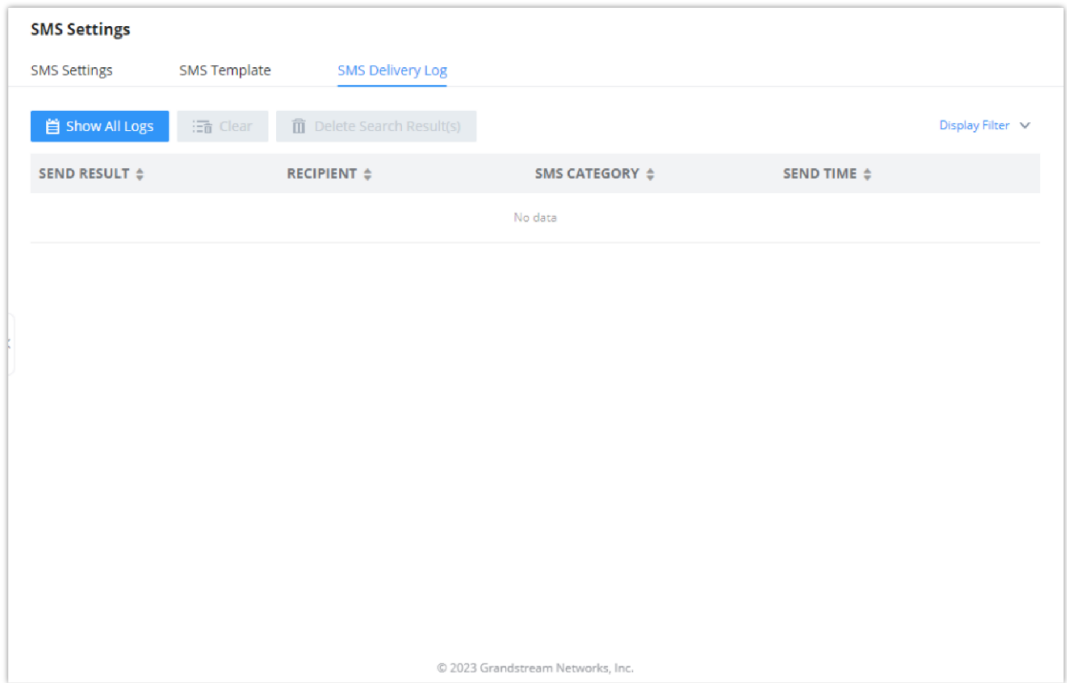
The template of the SMS can be modified in “SMS Template” tab. Please note that carriers may require to pre-register the templates for SMS that the UCM will send. Refer to the [Amazon](#) and [Twilio](#) documentation for more information.



SMS Templates

SMS Delivery Log

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



SMS Delivery Log

Advanced Messaging

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

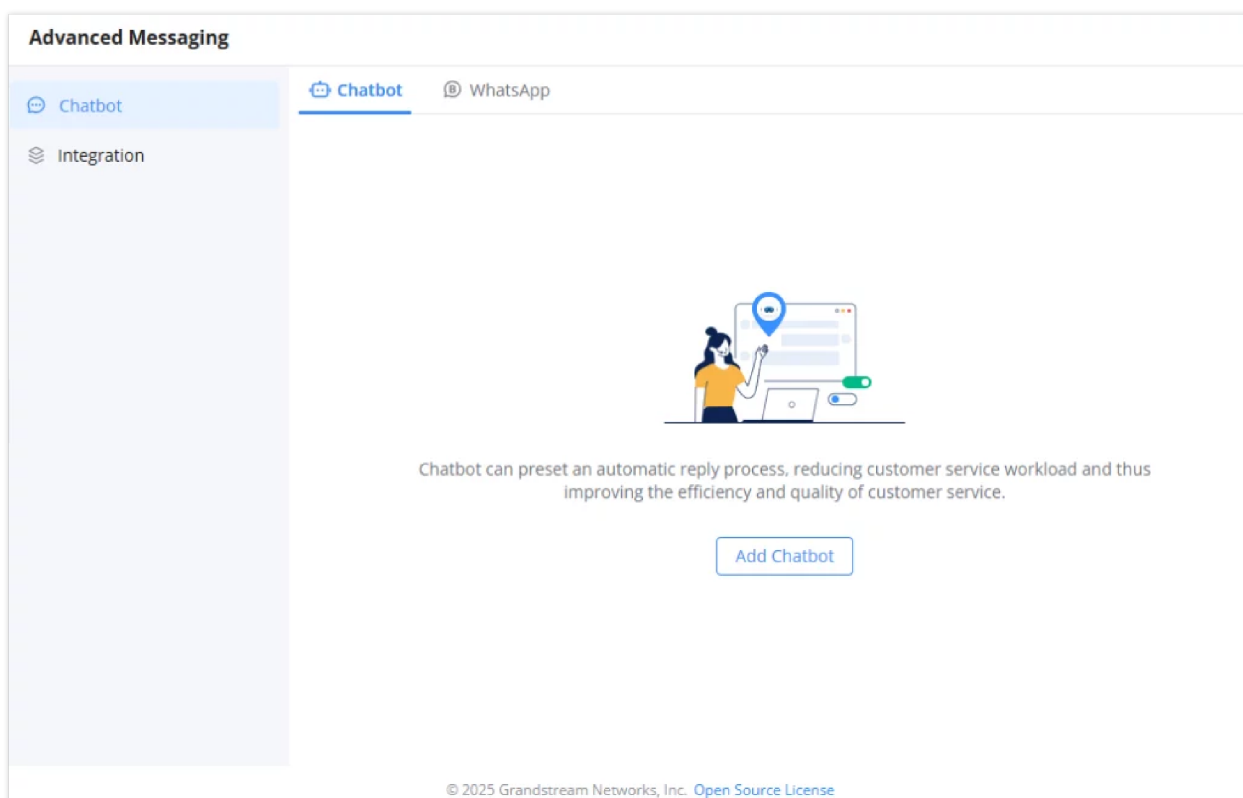
The advanced messaging feature supports configuring:

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

Chatbot

General Chatbot

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



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

Advanced Messaging

Chatbot

Integration

< Add Chatbot

1

2

Basic Settings

Configure Reply Flow

*Name

Description

Apply to Channel ⓘ

Select ▼

Save and Continue

© 2025 Grandstream Networks, Inc. [Open Source License](#)

- After saving the basic settings, the chatbot will be created successfully. A **Default Reply Flow** is automatically applied, starting with a standard greeting (e.g., *Hello! How can I help you?*).
 - To customize this behavior, click **Edit Reply Process** and define the conversation flow according to your needs.
 - If no changes are required, click **Back to List** to return to the chatbot overview page.

Advanced Messaging

Chatbot

Integration

< Add Chatbot

✓

2

Basic Settings

Configure Reply Flow



Added successfully

Default Reply Flow

Automatically send this content to visitors upon entering the session

• Robot

Hello! How can I help you?

Edit Reply Process

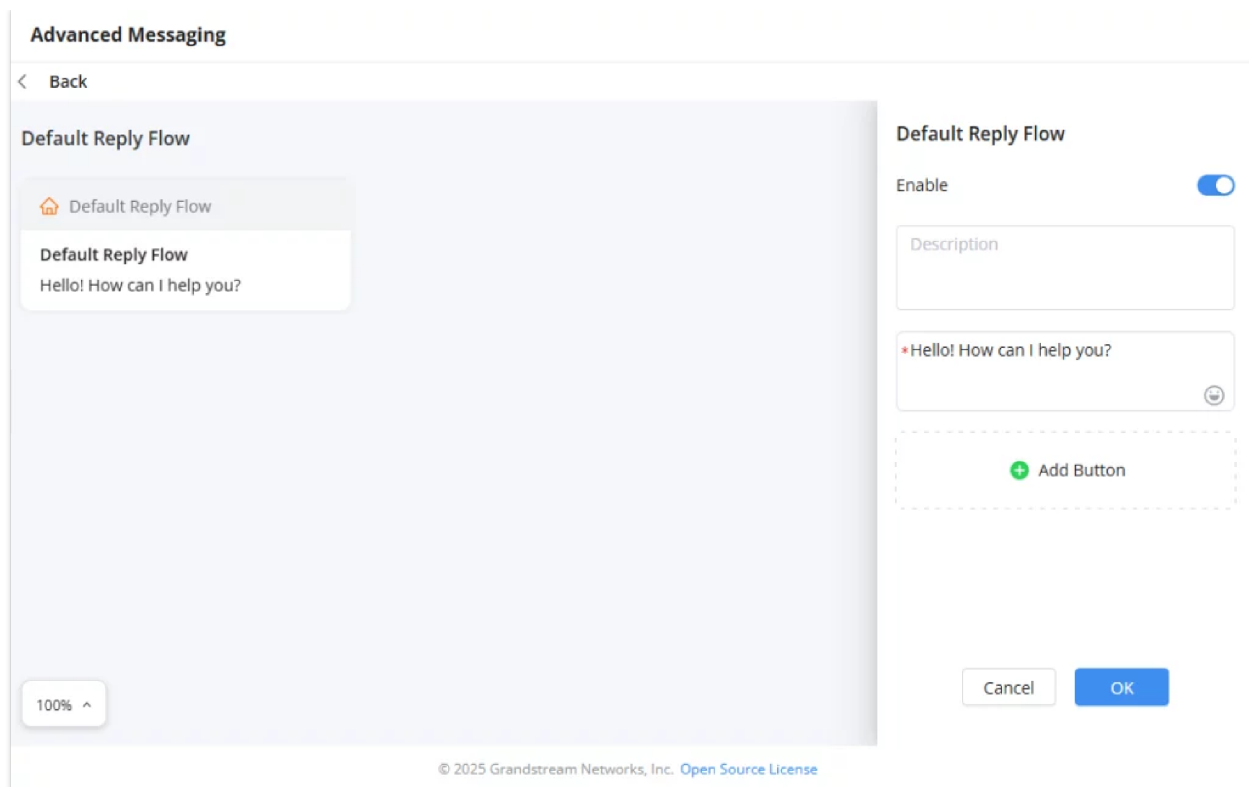
Back to List

© 2025 Grandstream Networks, Inc. [Open Source License](#)

In the **Default Reply Flow** editor:

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

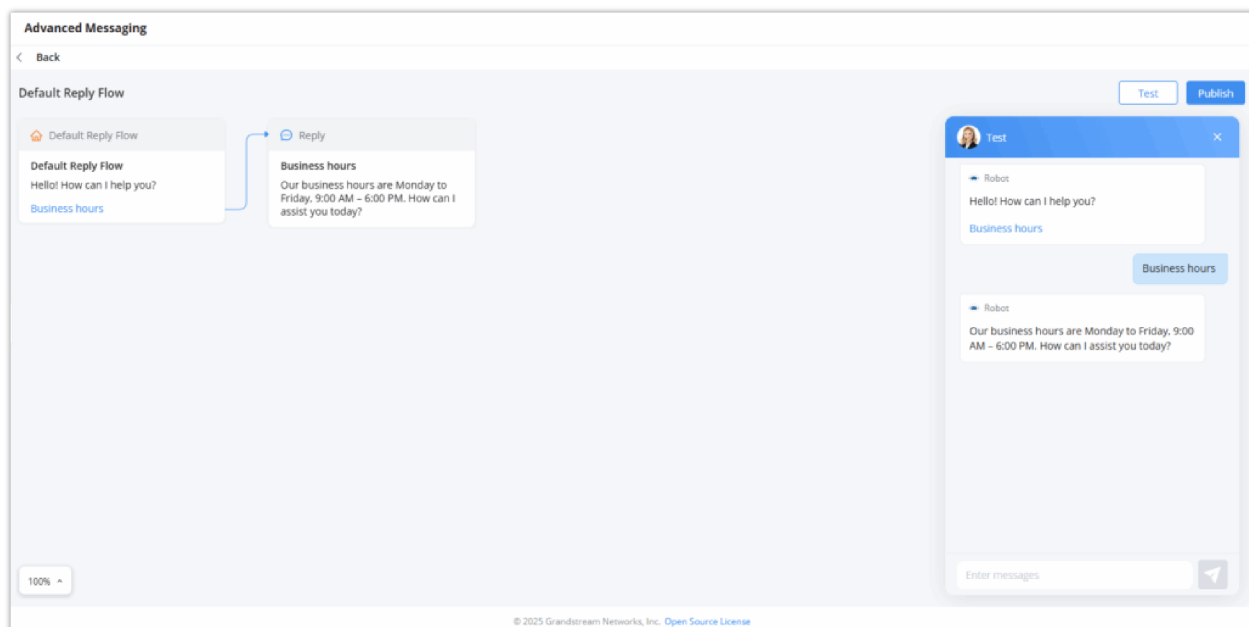
Click **OK** to save the changes.



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

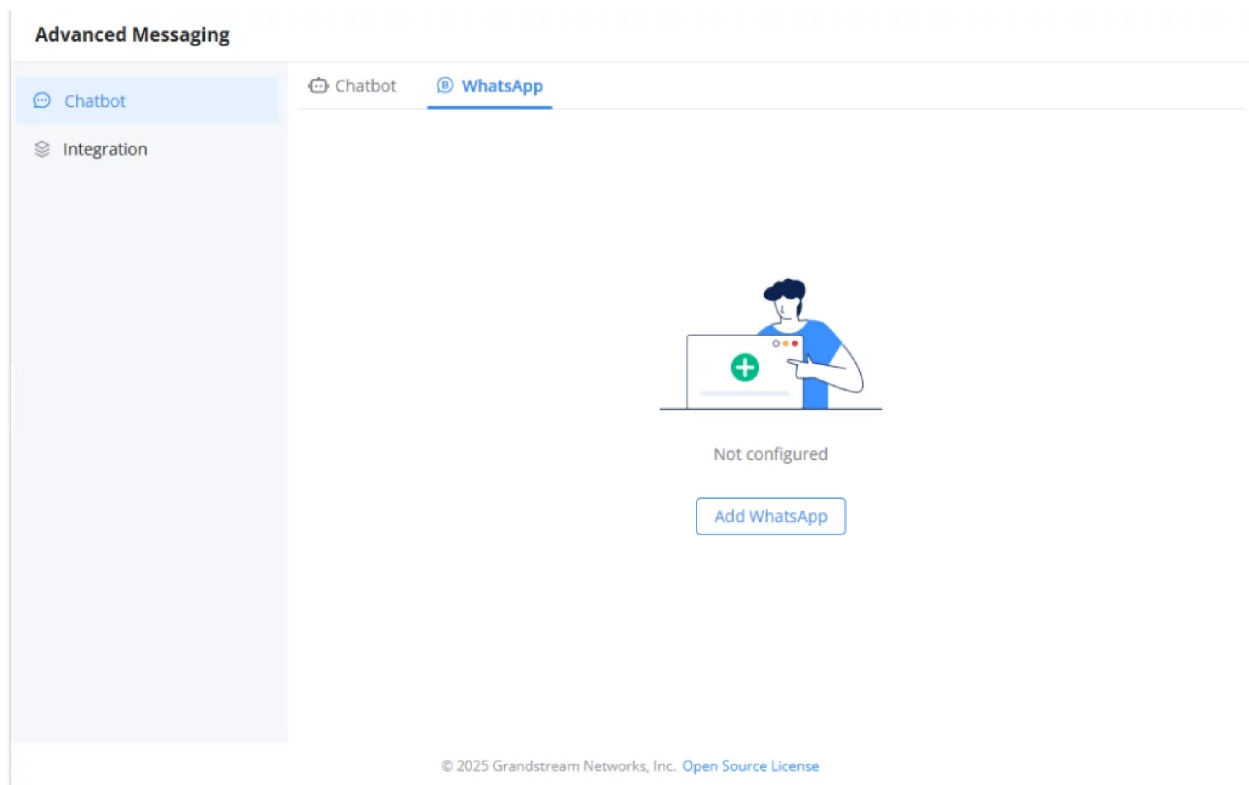
- Under the default greeting, click **Add Button** and label it (e.g., *Business Hours*).
- Link the button to a **Reply** block that contains the desired response (e.g., *Our business hours are Monday to Friday, 9:00 AM – 6:00 PM. How can I assist you today?*).
- Use the **Test** panel on the right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

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



Whatsapp Chatbot

From the **Advanced Messaging** → **WhatsApp** tab, click **Add WhatsApp**. This opens the configuration page to register your WhatsApp account with the UCM.



Fill in the required fields:

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

Advanced Messaging

Chatbot

Integration

< Add WhatsApp

Enable

1 - 64 Characters

1 - 1000 Characters

https://.b.gdms.cloud/gsim/webhooks/0-eb25f8d7e6

Secret key

1 - 24 Characters

Add

Destination Number

Select

Display sessions taken by other agents

Enable Chatbot

Cancel

OK

© 2025 Grandstream Networks, Inc. Open Source License

Define Chatbot Behavior

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

Advanced Messaging

Chatbot

Integration

< Add WhatsApp

1 - 24 Characters

Add

Destination Number

1000 (1000) ✕

Display sessions taken by other agents

Enable Chatbot

Chatbot

View Reply Process

TEST

Chatbot Mode

Automatic Reception

Chat Assistance

Transfer to Agent

If messages from visitors do not match the automatic reply flow, the message contents below will be sent in response.

Robot

Click "Transfer to Agent" to start chatting with customer service

Transfer to Agent

Example

After Hours Prompt

Add

Cancel

OK

© 2025 Grandstream Networks, Inc. Open Source License

Integration

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

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

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

Advanced Messaging

Chatbot Integration

The interface link is used to send notification messages to Wave users. Please refer to [API Document](#) for more details.

Interface Link ☒

Interface Link

Add

App ID	App Name	Token	URL	Options
No data				

When creating a new integration, enter the following details:

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

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

Advanced Messaging

Chatbot Integration

< Add

* App ID

d79bd40c728c11ec90d60242ac120003

* App Name

TEST

Token

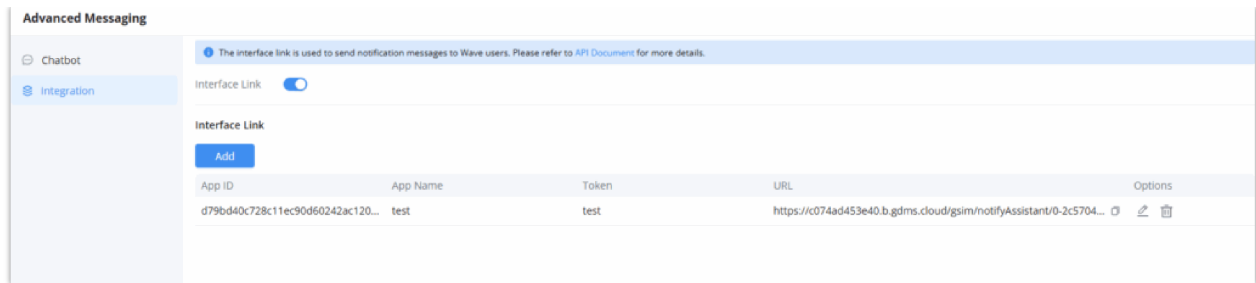
test

Cancel Generate Interface Link

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

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

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



PBX SETTINGS

General Settings

The General Settings allows configuring system-wide behaviors and default parameters that govern call handling, security, and extension management for CloudUCM.

The following table describes all the configuration options on that page:

General Preferences	
Global Outbound CID Number	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 (s)	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.
International Call Prefix	Digits users dial before a country code to place an international call (e.g., 00 or 011). The PBX uses this prefix to detect and classify a dialed number as international for routing, permissions, and (when applicable) PMS billing/records. Input: digits only (no +, no country code).
Domestic Long Distance Call Prefix	Digits users dial to reach a national (out-of-area) number within the same country (commonly 0 in many regions or 1 in NANP countries). The PBX uses this prefix to identify national long-distance calls versus local calls for policy and rating purposes. Input: digits only; leave blank if your country does not use one.
Local Area Code	The area/city code of the PBX's location, used to normalize local dialing. When callers dial a local number without an area code, the PBX can use this value to complete the number and to distinguish <i>local</i> from <i>long-distance</i> calls. Input: the area/city code without the domestic long-distance prefix (e.g., enter 212, not 0212).
Recording Settings	
Record Prompt	If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the IPPBX 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.
Merge Same Call Recordings	If enabled, the system will merge all recordings created during a call regardless of how many times a user starts and stops recording during a call.
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.
Start/Stop Recording Feature Codes	Users can use this as a shortcut to navigate to the Feature Codes configuration page to set recording related codes.
Extension Preferences	
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.
Enable Extension Range	If set to "Yes", which is the default behavior, users could enable the extension range configured on the IPPBX. Note: It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.
Extension Ranges	The default extension range assignment is: ● User Extensions: 1000-6299 User Extensions is referring to the extensions created under Web GUI > Extension/Trunk > Extensions page. ● 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.
Default Extension Segment	Clicking this button will reset the extension range to their default values.

SIP Settings

General

Realm For Digest Authentication	Configure this as the host name or domain name of the PBX. Realms MUST be globally unique according to RFC3261.
MWI From Header	If disabled, the server will not transfer the Diversion Header
Enable Diversion Header	If set to "No", all transfers initiated by the endpoint in the IPPBX will be disabled (unless enabled in peers or users). The default setting is "Yes".
Send Deflection Diversion	If 'Enable Diversion Header' and this option enabled, the INVITE request will contain Diversion with reason 'deflection' while the inbound call been routed to an external number.
Block Collect Calls	If enabled, collect calls will be blocked.

	Note: Collect calls are indicated by the header “P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call”.
Unavailable Extension Cause	Sets the cause code to respond with when calling an unavailable extension.

Session Timer

Force Timer	Always request and run session timer. By default, this option disabled.
Timer	Run session timer only when requested by other UA.
Session Expiration (s)	Configure the session refresh interval (in seconds). The default setting is 600 seconds.
Min SE (s)	Configure the minimum session refresh interval (in seconds). The default setting is 90 seconds.

Transport Protocol

Choose the supported transport protocol used for SIP packets.

TLS Enable	Allow incoming TLS (secure) connections with the PBX. Note: This option cannot be disabled.
SIP Server (TLS)	Use the following server address on the endpoints to for SIP packet transport over TLS.
TCP Enable	Allow incoming TCP connections with the PBX. Note: This option is disabled by default.
SIP Server (TCP)	Use the following server address on the endpoints to for SIP packet transport over TCP.
Enable UDP	Allow incoming TCP connections with the PBX. Note: This option is disabled by default.
SIP Server (UDP)	Use the following server address on the endpoints to for SIP packet transport over UDP.

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 UCM. The default setting is 3600.
Min Registration/Subscription Time	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM. 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 UCM. The default setting is "Yes".
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted. The default setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
Generate In-Band Ringing	Configure whether the CloudUCM should generate Inband ringing or not. The default setting is "Never". ◦ Yes: The CloudUCM will send 180 Ringing followed by 183 Session Progress and in-band audio. ◦ No: The CloudUCM 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 UCM 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 CloudUCM.
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/ToS

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:

STIRSHAKEN

STIRSHAKEN Add Authorized CID and Attestation level

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

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

Certificate Settings

* Certificate Download

2

Time (s):

* Signature Valid Time (s):

15

* Private Key:

private.key

* Public Key:

public.crt

Cancel

Save

STIRSHAKEN Certificate Settings

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

SIP Settings/STIR/SHAKEN – Certificate 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 CloudUCM gives up. The default setting is 0, which means the CloudUCM 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	
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 CloudUCM 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.
Transfer	
Allow Transfer	Configure to allow transfer. When disallowed, all transfers initiated by the endpoint digit will be disabled.
Allow callback to transferer when blind transfer fails	If enabled, the UCM will call back the transferer when a blind transfer fails (i.e., no answer or busy).
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.

RTP Settings

RTP Settings

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.

Payload Type Settings

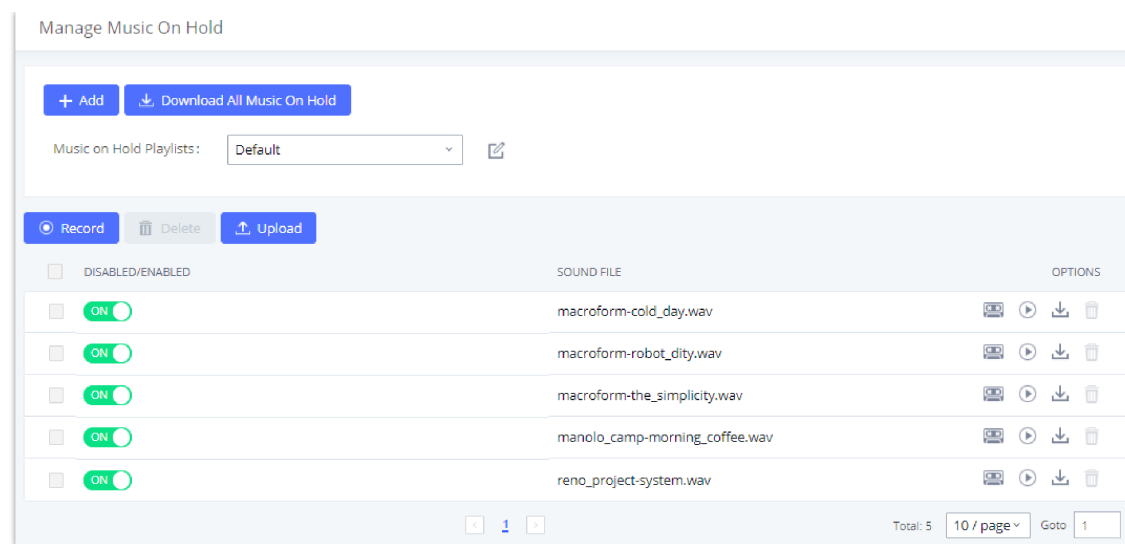
The CloudUCM payload type for audio codecs and video codes can be configured here.

Audio Codecs	
AAL2-G.726	ADPCM (G.726, 32kbps, AAL2 codeword packing).
DTMF	Dual-tone Multi-frequency.

G.721 Compatible	G.721 Compatible
G.726	ADPCM (G.726, 32kbps, RFC3551 codeword packing).
ILBC	ILBC Free Compression.
Opus	Opus
G.722.1	G.722.1: Low-complexity coding, 24kbps
G.722.1C	G.722.1C: Low-complexity coding, 48kbps
Audio FEC Payload Type	Audio FEC Payload Type
Audio RED Payload Type	Audio RED Payload Type
Video Coding	
H.264	H.264 Video.
H.265	H.265 Video.
H.263P	H.263+ Video.
VP8	VP8 Video.
Other Settings	
Main Video FEC	Main Video FEC.
RTP FECC	RTP FECC
RTX	Used for packet retransmission. PBX supports only video RTP retransmission.

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.



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



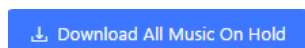
next to the selected Music On Hold class to delete this Music On Hold class.

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

Steps to play the Music On Hold file:

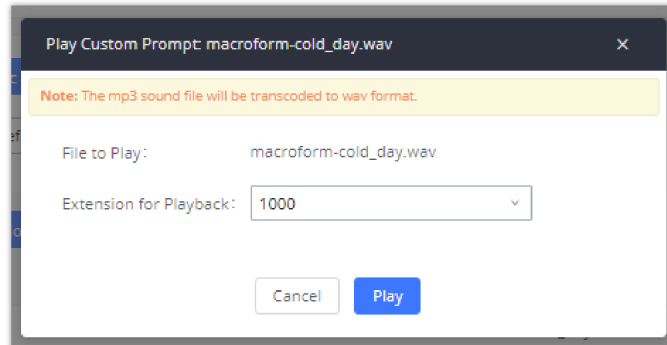
1. Click on the



button for the Music On Hold file.

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

Play



Play Custom Prompt

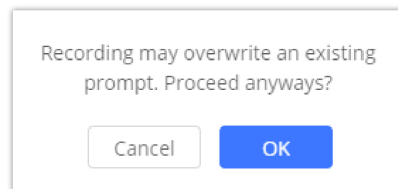
3. The selected extension will ring.
4. Answer the call to listen to the music playback.

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

1. Click on



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



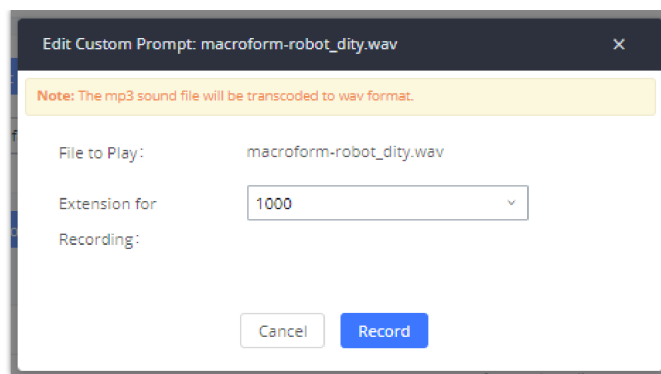
Information Prompt

3. Click

OK

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

Record



Record Custom Prompt

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

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

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

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

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

Voice Prompt

The CloudUCM 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 preloaded in with the CloudUCM already. The other languages provided by Grandstream can be downloaded and installed from the CloudUCM Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the CloudUCM.

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 CloudUCM, click on “Add Voice Prompt Package” button.

Voice Prompt

Language Settings

Custom Prompt

Username Prompt

Add Voice Prompt Package

Upload

Voice Prompt Package List

LANGUAGE	OPTIONS
☒ English : en	x
☐ 中文 : zh	x

Cancel

Save

Language Settings for Voice Prompt

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

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

Voice Prompt Package List

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

Voice Prompt

[Language Settings](#)
[Custom Prompt](#)
[Username Prompt](#)

Add Voice Prompt Package

Upload

Voice Prompt Package List

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

Cancel

Save

New Voice Prompt Language Added

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

Custom Prompt

Record New Custom Prompt

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

Record New Custom Prompt

Note: The mp3 sound file will be converted to wav format.

* File Name

Custom_Prompt_1

Format

WAV

* Extension

1000

Cancel

Record

Record New Custom Prompt

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

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



Custom Prompt Page

Upload Custom Prompt

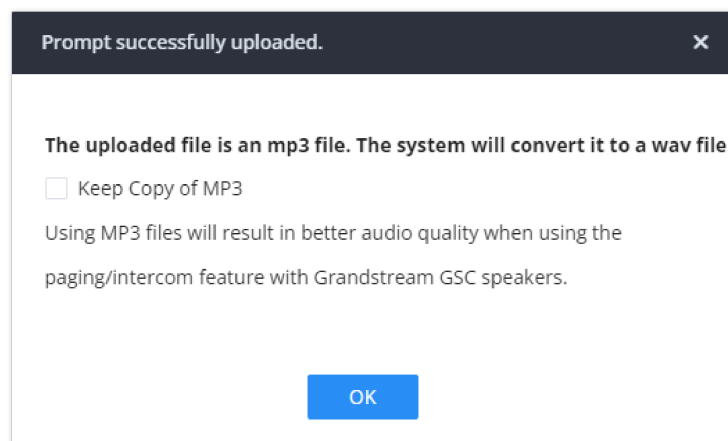
If the user has a pre-recorded IVR prompt file, click on "Upload" in **Web GUI → PBX Settings → Voice Prompt → Custom Prompt** page to upload the file to CloudUCM.

The following are required for the prompt file to be successfully uploaded:

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

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

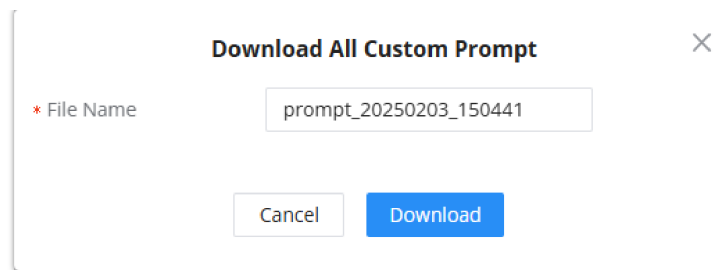
If the file uploaded is mp3, the following prompt will appear.



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

Download All Custom Prompt

On CloudUCM, the users can download all custom prompts from the Web GUI to local PC. To download all custom prompt, navigate to **PBX Settings → Voice Prompt → Custom Prompt** and click on "Download All". The following window will pop up in order to set a name for the downloaded file.



Download All Custom Prompt

The downloaded file will have a .tar extension.

Username Prompt

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

Upload Username Prompt File from Web GUI

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

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

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

- Click on



to record again the username prompt.

- Click on to play recorded username prompt.
- Select username prompts and press



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

Record Username via Voicemail Menu

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

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

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

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

Call Prompt Tones

SIP Trunk Prompt Tone

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

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

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

SIP Trunk Prompt Tone	
Specify the tones to play for various SIP trunk call failure scenarios.	
<button>Reset All</button> <button>Default All</button>	
400:	sip:trunk-out-busy
402:	sip:trunk-out-busy
404:	sip:trunk-out-wrong nu...
406:	sip:trunk-out-busy
408:	sip:trunk-out-busy
413:	sip:trunk-out-busy
415:	sip:trunk-out-busy
420:	sip:trunk-out-busy
423:	sip:trunk-out-busy
481:	sip:trunk-out-busy
483:	sip:trunk-out-busy
485:	sip:trunk-out-busy
487:	sip:trunk-out-busy
491:	sip:trunk-out-busy
<button>Reset All</button> <button>Default All</button>	
500:	sip:trunk-out-server-error
502:	sip:trunk-out-server-error
504:	sip:trunk-out-server-error
513:	sip:trunk-out-server-error
<button>Reset All</button> <button>Default All</button>	
600:	sip:trunk-out-busy
604:	sip:trunk-out-wrong nu...
603:	sip:trunk-out-rejected
606:	sip:trunk-out-busy

SIP Trunk Prompt Tone

General Call Prompt Tones

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

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

Call Prompt Tones

SIP Trunk Prompt Tone

General Call Prompt Tones

Cancel

Save

Specify the tones to play for various general call scenarios.

Reset All

Default All

Bad Number :	wrong-number	Out Of Service :	out-of-service
User Busy :	user-busy	Trunk Busy :	trunk-busy
No Answer :	no-answer	No Permission :	no-permission
Do Not Disturb :	user-busy	General Failed :	general-failed
Call Waiting :	Default Ringback Tone		

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

General Call Prompt Tones

Alert-Info Prompt

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

Alert-info Prompt

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

Upload

Download All

Delete

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

Total: 4

<

1

>

10 / page

Goto

Alert info Prompt

Storage Device Management

The Storage Device Management module allows you to integrate your CloudUCM with external cloud storage services. This page provides the option to configure a connection to a third-party Amazon S3 bucket to archive a copy of your critical data, specifically backup files.

This feature is designed for organizations that require an additional, independent copy of their configuration and data for long-term retention, compliance, or disaster recovery purposes, separate from the primary Grandstream cloud storage.

Note:

This integration is used for storing backup files to your own S3 bucket. All other system data, such as call recordings and voicemails, will continue to be stored in your primary CloudUCM storage space.

Amazon S3 Storage Settings

The table below describes the parameters that can be found on the Amazon S3 configuration tab:

Enable	Enables or disables Amazon S3 integration. When enabled, the configuration fields below become editable.
Region	Manually enter, or select from the drop-down list the AWS region where the bucket is located.
Bucket	Enter the name of the S3 bucket. Must be 3–63 characters, lowercase letters, numbers, and hyphens only.
Key ID	Enter the AWS Access Key ID generated after creating an account on the AWS platform. This value is encrypted and cannot be viewed after saving.
Secret Key	Enter the AWS Secret Access Key generated after creating an account. This value is encrypted and cannot be viewed after saving.
Test Connection	Click on this button to Test the connection to AWS S3 with the current settings. Note: It is recommended to perform a connection test during the initial configuration to ensure your that CloudUCM can successfully communicate with the Amazon S3 bucket.

SYSTEM SETTINGS

This section will explain the available system-wide parameters and configuration options on the CloudUCM. This includes settings for the following items: General Settings, HTTP server, Security Settings, LDAP Server, Time Settings, and Email Settings.

General Settings

On general settings, the user can configure the **Device Name** and **Enterprise Contact Number**.

General Settings

Device Name

Enterprise Contact Number

+

Add

+

Cancel

Save

CloudUCM General Settings

Device Name	Enter the device's name.
Enterprise Contact Number	Enter the contact number of the enterprise.

HTTP Server

In this section, the administrator can modify the settings regarding the HTTP server of the CloudUCM. The settings include restricting access to specific public IP addresses.

HTTP Server

UCM Web Settings

Enable IP Address Whitelist

☐

Permitted IP (s)

IP Address

/

Subnet Mask

+

Add IP Address

+

Wave Settings

Cross-origin Address Whitelist

https://wave.gdms.cloud

Cancel

Save

HTTP Server Settings

Enable IP Address Whitelist	P Whitelist restricts all IP addresses except for those in the whitelist from accessing the device via HTTP(S) (i.e., web portal, API).
Permitted IP (s)	Enter a list of IP addresses permitted by the device (e.g., "xxx.xxx.xxx.xxx/255.255.255.255" or "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/64").
Cross-origin Address Whitelist	The UCM will accept cross-server requests from addresses in the whitelist, which should be formatted as https://domain, https://ip:port or *. Entering * will allow cross-server requests from all addresses.

Security Settings

Geo-IP Access Control

This security feature allows administrators to block all access to the CloudUCM from specific countries or geographic regions. When enabled, the system will deny connections from any IP address associated with the blocked countries.

The restriction is comprehensive and applies to:

- **Web GUI** access (admin and user portals)
- **API** requests
- **Extension** registration and communication

The list of blocked countries can be maintained through manual updates or configured to refresh automatically at scheduled intervals.

Important Note:

Once enabled, this is a global setting. To avoid locking access, it is critical to ensure your own administrative IP address (or your company's IP range) is not located within a blocked country before activating this feature.

The screenshot shows the 'Security Settings' page with the 'Geo-IP Access Control' tab selected. A blue banner at the top states: 'The defense priority is as follows: Geo-IP Defense (Strict Defense) > Fail2Ban > Extension/Feature Configurations > Geo-IP Defense (Non-Strict Defense). Note: Extension/Feature Configurations refers to the extension ACL, CloudUCM Web access allowlist, API allowlist, etc.' Below this, the 'Geo-IP Access Control' toggle is turned on. The 'Strict Defense Mode' checkbox is unchecked. The 'Update Country/Region' button is visible. The 'Scheduled Update' section shows a 'Scheduled Task' link, 'Last Detect: No update history', and 'Country/Region Updates: -'. At the bottom, the 'Country/Region Allowlist' table is shown with columns for 'Continent', 'Country/Region', and 'Allow Access'. The table lists several countries with their 'Allow Access' toggle set to 'off'.

Continent	Country/Region	Allow Access
Asia	Afghanistan	off
Europe	Aland Islands	off
Europe	Albania	off
Africa	Algeria	off
Oceania	American Samoa	off

CloudUCM Geo IP Access Control Page

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

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

Notes:

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

Fail2Ban

Fail2ban allows to protect the CloudUCM from brute-force attacks by sending multiple SIP register attempts or login attempts using a dictionary of passwords. By limiting the attempts, the administrator can ensure that the password guessing attempts are limited in a period of time.

Note:

Before enabling this feature, it is highly recommended to add your administrator's IP address to the Fail2Ban whitelist. This step is essential to prevent administrative access from being accidentally blocked.

The screenshot shows the 'Security Settings' page with the 'Fail2Ban' tab selected. Under 'Basic Protection', 'SIP Defense' and 'Login Attack Defense' are both disabled. Under 'Customer Service Protection', 'Customer Service System Call Defense' and 'Live Chat Protection' are also disabled. In the 'Global Protection Settings', the 'Banned Duration (s)' is set to 600. Below this, there are 'Cancel' and 'Save' buttons. The 'Fail2ban Allowlist' section has an 'Add' button and a table with columns 'IP' and 'Description / Comment'. The 'Blocklist' section also has an 'Add' button and a table with columns 'Banned Type', 'IP', 'Time', and 'Description / Comment'. A 'No data' message is displayed in the center of the page.

Fail2Ban Settings

The table below describes the Fail2Ban configuration options for CloudUCM:

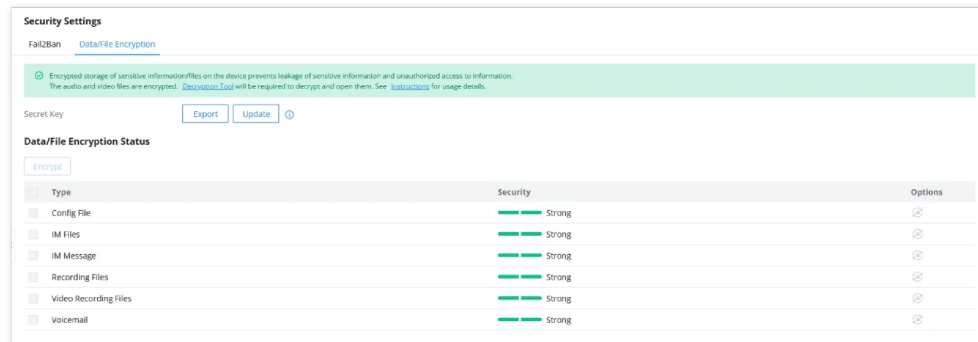
SIP Defense	If enabled, which is the default setting, CloudUCM will monitor failed SIP registration attempts and heartbeat timeouts based on the security logs. Once the number of failed attempts from an IP address has reached SIP Defense's configured <i>Max Retries</i> value, the IP address will be banned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

Blocklist	Users will be able to manually add or view the IPs that have been automatically blocked by CloudUCM.
------------------	--

Data/File Encryption

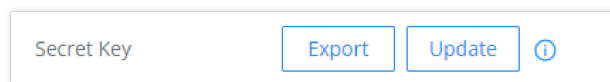
By default, CloudUCM provides encryption for all data/files. This ensures that sensitive information and files are securely encrypted, protecting them from unauthorized access and preventing potential data leaks.

To access this feature, please navigate to **System Settings** → **Security Settings** → **Data/File Encryption**.



DataFile Encryption Status

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



Secret Key Export/Update

The secret key can be updated by clicking on the “Update” button, this would require entering the administrator’s password.

Notes:

- Encryption is applied to all data and files stored on CloudUCM by default, and users cannot select specific types for encryption.
- When upgrading to a firmware version that supports Data/File encryption, all previously stored data on the CloudUCM will be automatically encrypted.
- After setting a new secret key, all future data and files will be encrypted with the new key, and any existing encrypted data will be re-encrypted with the updated key.
- It is recommended to export and securely store the current secret key as a backup before updating it.
- Only the super administrator has the authority to change the secret key.

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

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

[IP PBX – CDR Tool Guide](#)

LDAP Server

The CloudUCM has an embedded LDAP/LDAPS server for users to manage the corporate phonebook in a centralized manner.

- By default, the LDAP server has generated the first phonebook with **PBX DN** “ou=pbx,dc=pbx,dc=com” based on the CloudUCM 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 CloudUCM 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 CloudUCM, 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 CloudUCM. If the CloudUCM 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 CloudUCM LDAP server, or use a specific phonebook DN, for example "ou=people,dc=pbx,dc=com", to access to phonebook with Phonebook DN "ou=people,dc=pbx,dc=com " only.

UCM can also act as an LDAP client to download phonebook entries from another LDAP server.

To access the LDAP server and client settings, go to Web GUI→**Settings→LDAP Server**.

LDAP Server Configurations

The following figure shows the default LDAP server configurations on the CloudUCM.

LDAP Server

LDAP Server Configurations

LDAP Phonebook

LDAP Server

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

LDAP Server Address

ldap://192.168.1.100:389

LDAPS Server Port

636

Base DN

ou=070199,dc=pbx,dc=com

PBX DN

ou=pbx

,ou=070199,dc=pbx,dc=com

Root DN

cn=admin

,ou=070199,dc=pbx,dc=com

Root Password

Hide

Confirm Root Password

Hide

TLS Compression

LDAP Server Configurations

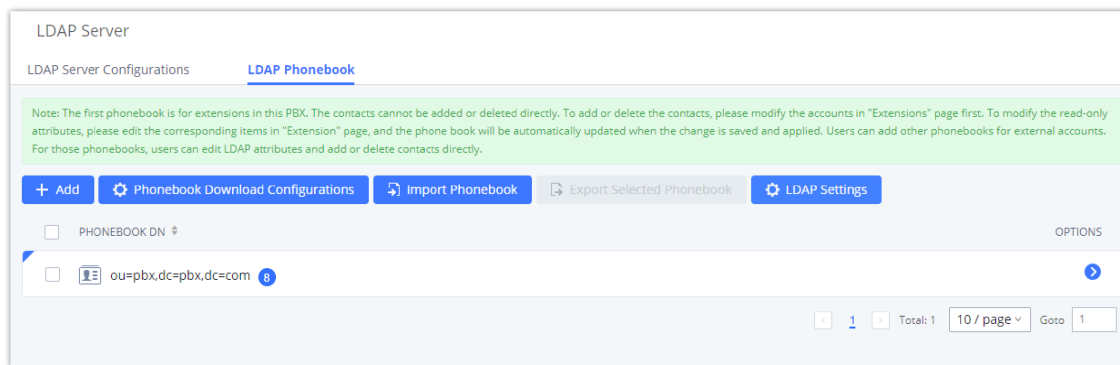
Enable LDAP Server	Enable LDAP Server
LDAP Server Address	LDAP server address is predefined by the datacenter chosen for the IPPBX. The user cannot modify this option.
LDAPS Server Port	LDAPS server port is predefined and cannot be set by the user. The port number is 636.
Base DN	Specifies the location in the directory where the search is requested to begin. It is predefined and cannot be modified.
PBX DN	Specifies the location in the directory where the search for PBX entry is requested to begin. It narrows the search scope and decreases directory lookup time.

Root DN	Specifies the location in the directory where the search for the admin user entry is requested to begin. It narrows the search scope and decreases directory lookup time.
Root Password	Defines the root password for authentication.
Confirm Root Password	Confirms the root password for authentication.
TLS Compression	If this option is enabled, compression will be performed when transmitting the data. Enabling this option is not recommended since it may present a security risk. Note: This option is disabled by default.

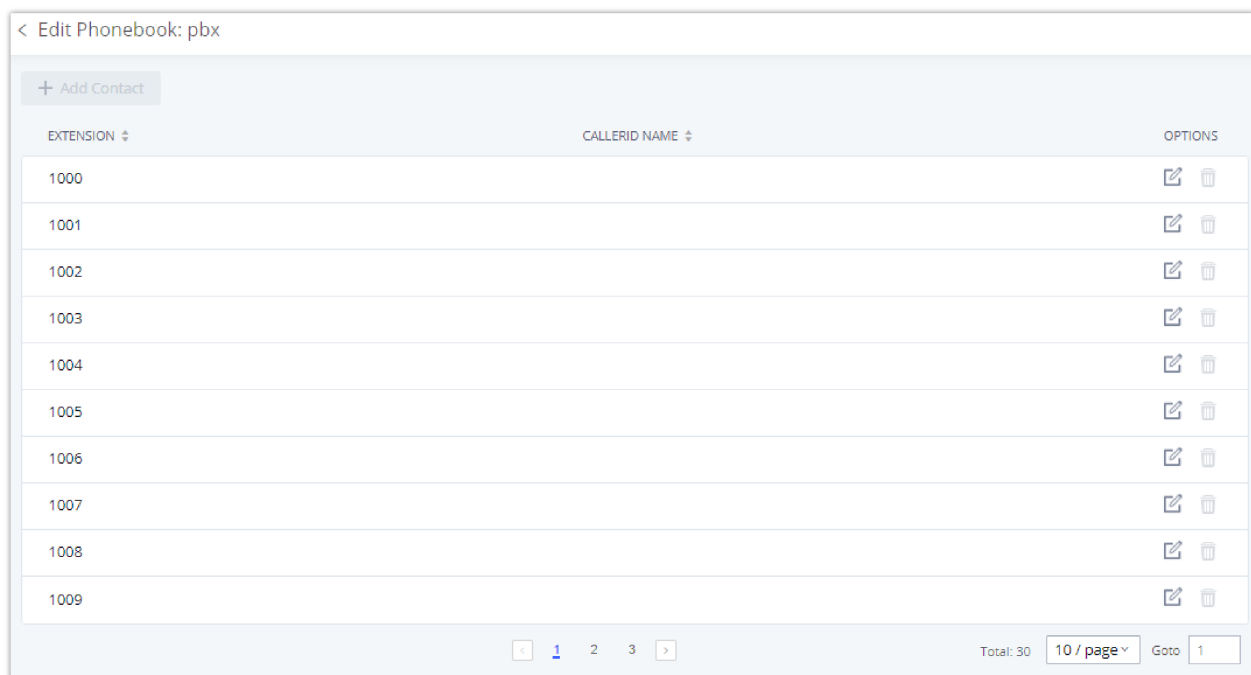
The CloudUCM LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client does not have to configure a username and password to access the phonebook directory. The “Root DN” and “Root Password” here are for LDAP management and configuration where users will need to provide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

The default phonebook list in this LDAP server can be viewed and edited by clicking on/for the first phonebook under LDAP Phonebook.

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



Default LDAP Phonebook DN



Default LDAP Phonebook Attributes

LDAP Phonebook

Users could use the default phonebook, edit the default phonebook, add new phonebook, import phonebook on the LDAP server as well as export phonebook from the LDAP server. 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.

LDAP Server

LDAP Server Configurations

LDAP Phonebook

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

Add

Phonebook Download Configurations

Import Phonebook

Export Selected Phonebook

LDAP Settings

☐

Phonebook DN

Options

☐

ou=pbx,dc=pbx,dc=com

10

Total: 1

<

1

>

10 / page

Goto

LDAP Phonebook

LDAP Server > Edit Phonebook: pbx

Local Extension Contacts

External Contacts

AccountNumber	CallerID Name	Email	Options
1000	Arthur Morgan	morgan.arthur@email.com	
1001	Abigail Stevens		
1002			
1003			
1004			
4000			
4001			
4002			
4003			
4004			

Total: 10

<

1

>

10 / page

Goto

© 2024 Grandstream Networks, Inc.

Create LDAP Phonebook

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

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

LDAP Phonebook: pbx

Local Extension Contacts

External Contacts

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

LDAP Phonebook Search Bar

◦ Add new phonebook

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

A dialog box titled "Add Phonebook" with a close button (X) in the top right corner. It contains two input fields: "Phonebook Prefix:" with an asterisk indicating it is required, and "Phonebook DN:". Below the fields are two buttons: "Cancel" and "Save".

Add LDAP Phonebook

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

Once added, users can select  to edit the phonebook attributes and contact list (see figure below) or select  to delete the phonebook.

A web interface titled "Edit Phonebook: GStest". It features a blue "+ Add Contact" button. Below it is a table with columns: ACCOUNTNUMBER, CALLERID NAME, EMAIL, and OPTIONS. The first row contains the values: 062514356, Dr. Smith, and empty cells for EMAIL and OPTIONS. At the bottom right, there are pagination controls showing "Total: 1", "10 / page", and "Goto 1".

Edit LDAP Phonebook

o Import phonebook from your computer to LDAP server

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

A dialog box titled "Import Phonebook" with a close button (X) in the top right corner. It contains a yellow warning box with the text: "Please use UTF-8 encoding when importing CSV, VCF, or XML files. Import file: Account Number and Phonebook DN are required." Below the warning box are two fields: "File Type:" with a dropdown menu set to "CSV", and "File:" with a "Choose File to Upload" button.

Import Phonebook

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

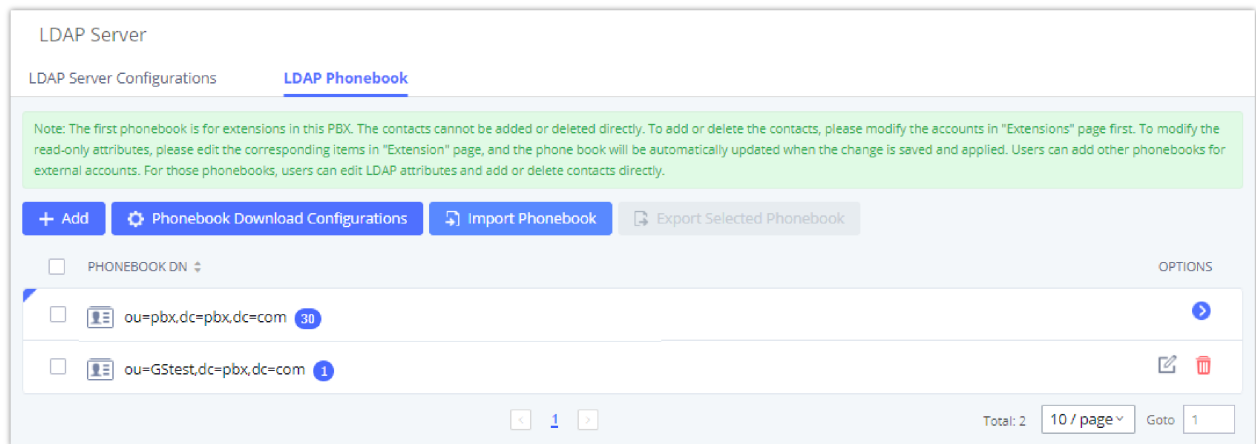
	A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo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

Phonebook CSV File Format

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

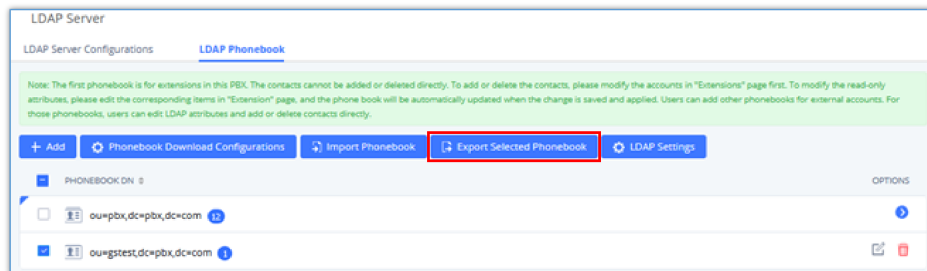


LDAP Phonebook After Import

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 CloudUCM LDAP server**

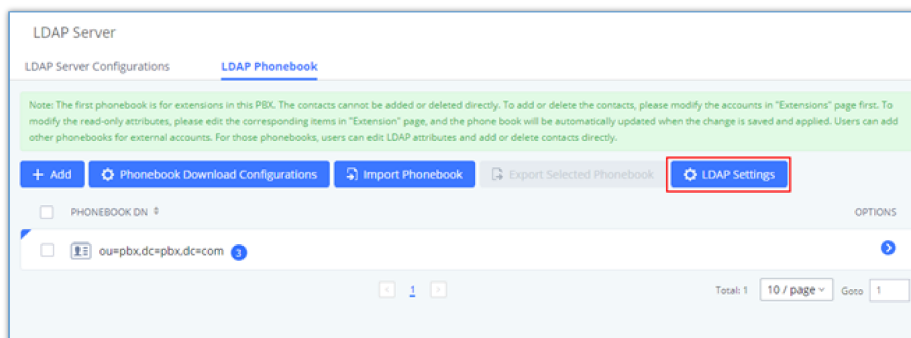
Select the checkbox for the LDAP phonebook and then click on "Export Selected Phonebook" to export the selected phonebook. The exported phonebook can be used as a record or a sample CSV, XLSX, VFC or XML file for the users to add more contacts in it and import to the CloudUCM again.



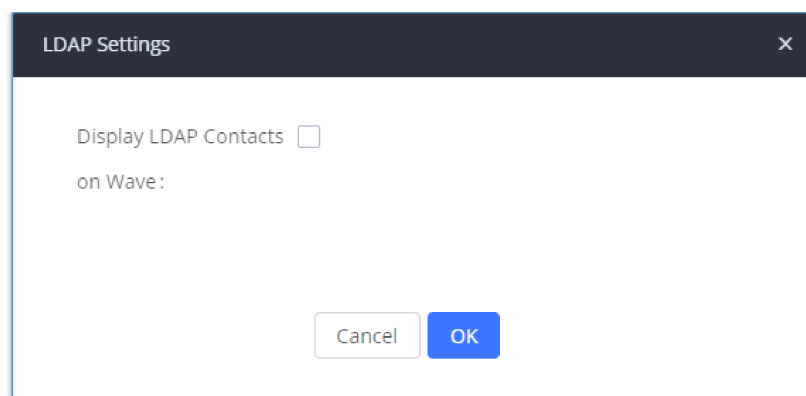
Export Selected LDAP Phonebook

LDAP Settings

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



Display LDAP Contacts on Wave

LDAP Client Configuration

The LDAP client configuration enables CloudUCM to integrate with external LDAP servers for centralized user management. This is useful for synchronizing user accounts, credentials, or directories from services like OpenLDAP.

Note:

To set up an integration with a Windows Active Directory (AD) server, please navigate to the dedicated Windows AD section.

The table below describes the key parameters for configuring CloudUCM as an LDAP client:

LDAP Client Configurations

Server Address	The IP address of the LDAP server
Port	Enter the port number. Default port is 389
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.
Phonebook Name	Enter a name for the phonebook
Client Type	Choose the client type. For encrypted data transfer please choose LDAPS.

Download Settings	
Filter	Enter the filter. Ex: ((CallerIDName=%)(AccountNumber=%))
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.
Source LDAP Number Attributes	Enter the number attributes for the LDAP server. Using the default attributes must include AccountNumber, other optional attributes are MobileNumber, HomeNumber, Fax, Position.
Source LDAP Name Attributes	Enter the name attributes for the LDAP server.
LDAP Attribute Conversion	When enabled, this feature automatically converts and maps OpenLDAP contact attributes (like name, telephone number, email, etc.) into the native format used by CloudUCM’s internal LDAP structure. This option is disabled by default.
Attribute Mapping	Defines how attributes (e.g., HomeNumber, Email) from an external LDAP server (like OpenLDAP) are mapped to the corresponding attribute names used internally by the CloudUCM LDAP server. Note: Supports mapping for up to 10 attributes.

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

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

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

LDAP

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

GXP2170 LDAP Phonebook Configuration

The CloudUCM LDAP server is no longer supporting the anonymous binding of the LDAP client.

Time Settings

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

Time Zone Settings

To configure the CloudUCM timezone, go to Web GUI → **System Settings** → **Time Settings** → **Time Zone Settings**.

Time Settings

[Time Zone Settings](#) [Set Date and Time](#) [Office Time](#) [Holiday](#) [Custom Time Groups](#)

Time Zone

(UTC+08:00) Etc/GMT-8 ▾

Update Time Zone

Scheduled Update

Scheduled Task

Last Update: No update history

Time Zone Update: -

Time Zone Settings

The time zone settings are described in the table below:

Parameter	Description
Time Zone	Choose the correct time zone according to your location.
Update Time Zone List	Clicking this button updates the list of timezones.
Scheduled Update	Click to move to the Task Management page and schedule a task for automatic time zone update.

Set Date and Time

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

Time Settings

Time Zone Settings

Set Date and Time

Office Time

Holiday

Date Format

yyyy-mm-dd

Time Format

Use 24-hour Format

Cancel

Save

Time Auto Updating

Office Time

On the CloudUCM, the system administrator can define “office time” which can be used to configure time condition for extension call forwarding and inbound rules. To configure office time, log in to the Web GUI, enter the **System Settings**→**Time Settings**→**Office Time**, and click the “Add” button to see the following configuration page.

Time Settings

Time Zone Settings

Set Date and Time

Office Time

Holiday

+ Add

Delete

Import

Export

☐

Index

Time

Week

Month

Day

Options

No data

Office Time

Time Settings > Create New Office Time

Time -

Week

Sun	Mon	Tue	Wed
Thu	Fri	Sat	

Show Advanced Options ☐

Create New Office Time

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

Create New Office Time

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

The office hour feature support import/export CSV/XLSX files.

Time Settings

Time Zone SettingsSet Date and TimeOffice TimeHoliday

+ Add

Delete

Import

Export

☐	Index	Time	Week	Month	Day	Options
☐	1	09:00-18:00	Mon Tue Wed Thu Fri	Default	Default	

Total: 1

<

1

>

10 / page

Goto

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

From this page, the administrator can:

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

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

Time Settings > Create New Holiday

* Name

New_Year

Description

Year

All

Month

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

Configuration Method ⓘ

☒ By Date ☐ By Week

Day

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

Time

00:00

-

23:59

Cancel

Save

Create a New Holiday Entry

Name	Specifies the name of the holiday. Used to identify the holiday in related features.
Description	Optional description for the holiday.
Year	Specifies the year in which the holiday applies. Select <i>All</i> to configure a recurring annual holiday.

Month	Select the month in which the holiday occurs.
Configuration Method	Defines how the holiday date is determined. The options are: ● By Date: Used for holidays with a fixed calendar date. ● By Week: Used for holidays defined by a weekday pattern within a month (for example, the fourth Thursday of a month).
Day	Displayed when Configuration Method is “ <i>By Date</i> ”. Choose one or more calendar dates within the selected month to be treated as holidays.
Sequence	Displayed when Configuration Method is “ <i>By Week</i> ”. Select the occurrence of the weekday within the month, such as First, Second, Third, Fourth, or Fifth.
Week	Displayed when Configuration Method is “ <i>By Week</i> ”. Select the day of the week (Sunday through Saturday).
Time	Specifies the effective time range of the holiday. The holiday is active from the start time to the end time on the configured date(s).

Custom Time Groups

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

Note

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

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

Time Settings > Create New Custom Time Groups

★ Name

Description

Time Groups

Time

Start Time

-

End Time

Frequency

☒ By Week

☐ By Month

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Add

Cancel

Save

Custom Time Groups

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

Email Settings

Email Settings

The Email application on CloudUCM 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**.

The table below describes the configuration parameters for common mail service providers:

Parameter	Description
Mail Server Providers	Select the mail server provider type.

	● Common: Select this option when integrating email service such as Gmail and on-premise email servers. ● Microsoft: Select this option when integrating email service provided by Microsoft Outlook. Note: The settings below appear when selecting “Common”.
TLS Enable	If enabled, TLS will be used when forwarding emails to the SMTP server.
Type	● MTA: Mail Transfer Agent. The configured domain will be used in the sender address. Warning: Emails sent by MTA may be considered spam by the destination SMTP server. ● Client: Send emails to the configured SMTP server, which will then forward the emails to the destination address.
Email Template Sending Format	Select the email template format to be sent. The “HTML” format is compatible with most mail clients and is recommended. If the mail client does not support the “HTML” format, please select the “Plain Text” format.
SMTP Server	Enter the SMTP server. For example, smtp.mydomain.com:587. Port number is optional.
Enable SASL Authentication	Toggles SASL authentication. If disabled, IPPBX will not use the username and password for email client authentication. Most email servers require login authentication while private email servers may allow anonymous login. If using Microsoft Exchange Server or if credentials are not required, please disable this option.
Username	Enter the username of the email account.
Password	Enter the password of the email account. It is highly recommended to use HTTPS when saving and applying password changes.
Enable Email-to-Fax	Monitors the inbox of the configured email address for the specified subject. If detected, the IPPBX 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 Blocklist/Allowlist	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.
Fax Sending Success/Failure Confirmation	If enabled, the UCM will send an email notification to the sender about the fax sending result.
Internal Block/Allowlist	Email address blacklist/whitelist for local extensions. This option is displayed after enabling Email-to-Fax Blocklist/Allowlist.
External Blocklist/Allowlist	Email address blacklist/whitelist for non-local contacts. Separate multiple addresses with semicolon (;) (i.e. “xxx;yyy”). This option is displayed after enabling Email-to-Fax Blocklist/Allowlist.
POP/POP3 Server Address	Enter the IP address of the POP/POP3 server.
POP/POP3 Server Port	Enter the port of the POP/POP3 server.
Display Name	Enter the name of the PBX that will be displayed in sent emails.

Sender	Enter the email used to send the emails.
Email Settings	Use “Test” button to test if the email integration is working correctly. Note: Before running the test, please save the configuration first by clicking on “Save” then “Apply Changes”.

The table below describes the configuration parameters for Microsoft Outlook:

Parameter	Description
Mail Server Providers	Select the mail server provider type. ● Common: Select this option when integrating email service such as Gmail and on-premise email servers. ● Microsoft: Select this option when integrating email service provided by Microsoft Outlook. Note: The settings below appear when selecting “Microsoft”.
Server Authorization	
Redirect URIs	Enter a redirect URI which will receive the OAuth2 token. Make sure that the URI is secure and is accessible.
Tenant ID	Enter the ID of the tenant of the directory in Microsoft Entra
Username	Enter Microsoft Entra login username.
Application (Client) ID	Enter the ID of the application created on Microsoft Entra
Client Password	Enter the client secret of the application created on Microsoft Entra.
Email Delivery Settings	
Email Template Sending Format	Select the email template format to be sent. The “HTML” format is compatible with most mail clients and is recommended. If the mail client does not support the “HTML” format, please select the “Plain Text” format.
Display Name	Enter the name of the PBX that will be displayed in sent emails.
Email Settings	Use “Test” button to test if the email integration is working correctly. Note: Before running the test, please save the configuration first by clicking on “Save” then “Apply Changes”.

Note

For a step-by-step configuration of Microsoft Outlook email services, please refer to the following guide:

<https://documentation.grandstream.com/knowledge-base/grandstream-ippbx-microsoft-outlook-authentication-guide/>

The following figure shows a sample Email setting on CloudUCM:

Email Settings

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

Mail Server Providers

Common

TLS Enable ⓘ

☒

Email Template Sending Format ⓘ

HTML

✱ Mail Server Domain ⓘ

example.com

✱ SMTP Server ⓘ

smtp.mycompany.com:587

Enable SASL Authentication ⓘ

☒

✱ Username ⓘ

user@mycompany.com

ⓘ

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

✱ Password ⓘ

••••••••

Copy

Enable Email-to-Fax ⓘ

☐

✱ Display Name ⓘ

PBX

Email Setting Configuration

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 CloudUCM.

Email Template

The Email templates on the CloudUCM can be used for email notification, the configuration parameters can be accessed via Web GUI→**Settings**→**Email Settings**→**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	Time	Options
Extension	2024-10-15 10:46:00	
Wave Welcome	2024-10-15 10:46:00	
Missed Calls	2024-10-15 10:46:00	
Multimedia Meeting Schedule	2024-10-15 10:46:00	
Scheduled Meeting Report	2024-10-15 10:46:00	
Meeting Report	2024-10-15 10:46:00	
Alert Events	2024-10-15 10:46:00	
Emergency Calls	2024-10-15 10:46:00	
Reset Password	2024-10-15 10:46:00	
Voicemail	2024-10-15 10:46:00	
Call Queue Statistics	2024-10-15 10:46:00	
SLA Alert	2024-10-15 10:46:00	
CDR	2024-10-15 10:46:00	
Fax	2024-10-15 10:46:00	
Fax Sending	2024-10-15 10:46:00	
Onsite Meeting	2024-10-15 10:46:00	

Email Template

Email Footer Hyperlink

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

Email Settings

Email Settings

Email Template

Email footer hyperlink

Email Send Log

Cancel

Save

Text:

Company Info

URL:

https://www.grandstream.com

Text:

Contact Us

URL:

https://www.grandstream.com/contact-us?

Add

Email Footer Hyperlink

Email Send Log

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

Email Settings

Email SettingsEmail TemplateEmail Footer HyperlinkEmail Send Log

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

Show All Logs

Clear

Delete Search Result(s)

Display Filter

Send Result

Recipient

Email Send Module

Email Generated Time

Last Send Time

Details

No data

Email Send Log

Start Time	Enter the start time for the filter
End Time	Enter the end time for the filter
Receivers	Enter the email recipient, while searching for multiple recipients, please separate them with a comma and no spaces.
Send Result	Enter the status of the send result to filter with
Return Code	Enter the email code to filter with
Email Send Module	Select the email module to filter with from the drop-down list, which contains: • All Modules • Extension • Voicemail • Conference Schedule • User Password • Alert Events • CDR • Test

Email Log – Display Filter

Email logs will be shown at bottom of the “Email Send Log” page, as shown in the following figure.

Email Settings

Email Template

Email Footer Hyperlink

Email Send Log

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

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

Show All Logs

Clear

Delete Search Result(s)

Display Filter

EMAIL GENERATED TIME	EMAIL SEND MODULE	RECEIVERS	LAST SEND TIME	LAST SEND ADDRESS	SEND RESULT	RETURN CODE	OPTIONS
2022-04-21 09:59:25	Wave Welcome	grandstream.com	04-21 09:59:32	@grandstream.com	sent	250	①
2022-04-21 09:59:06	Remote Registration	grandstream.com	04-21 09:59:08	@grandstream.com	sent	250	①
2022-04-20 12:39:32	SLA Alert	gmail.com	04-20 12:39:34	@gmail.com	sent	250	①
2022-04-19 17:45:07	SLA Alert	gmail.com	04-19 17:45:09	@gmail.com	sent	250	①
2022-04-19 17:39:59	SLA Alert	grandstream.com	04-19 17:40:01	@grandstream.com	sent	250	①
2022-04-19 17:34:43	Test	gmail.com	04-19 17:34:45	@gmail.com	sent	250	①
2022-04-19 17:19:30	Test	gmail.com	04-19 17:19:31	@gmail.com	sent	250	①

1

2

Total: 18

10 / page

Goto 1

Email Logs

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

Email Codes

Code	Description
250	Mail sent successfully
501	Address format parsing error, 501 will be returned when there are unacceptable characters in the recipient's email address in MTA mode. Please check if the recipient's email address format is correct. The “sender” configured on the client is your mail account.

Code	Description
535	The username and password verification in the client mode is incorrect. Please check whether the username and password are configured correctly.
550	Possible reasons: 1. The recipient's mailbox username does not exist or is in a banned state, please check whether the email recipient is the correct email address. 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	This indicates that there is no return code. If the sending result is "deferred", the general reason is that the mail service area is configured incorrectly. Please check whether the server configuration is correct. If the sending result is "bounced", the general reason is that the receiving email address domain name is wrong, please check whether the email recipient is the correct email address. If it is in MTA mode, please check whether the "domain" is configured to be in the same domain name as the "recipient".

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
☐	EXTENSION	NAME	DEPARTMENT	EMAIL ADDRESSES	CONTACT PRIVILEGES	OPTIONS
☐	1000		---		All Contacts(Same as Department)	 
☐	1001	John Doe	---		All Contacts(Same as Department)	 
☐	1002	Jane Doe	---		All Contacts(Same as Department)	 
☐	1003	Arthur Morgan	---		All Contacts(Same as Department)	 
☐	1004		---		All Contacts(Same as Department)	 
☐	1005		---		All Contacts(Same as Department)	 
☐	2000		---		All Contacts(Same as Department)	 
☐	2001		---		All Contacts(Same as Department)	 
☐	2002		---		All Contacts(Same as Department)	 
☐	2003		---		All Contacts(Same as Department)	 
				 1 2 		
				Total: 11 10 / page Goto 1		

Extension Contacts

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 :

1000

First Name :

John

Last Name :

Doe

Department :

Marketing

Job Title :

Graphic Designer

Email Address :

Mobile Phone

Number :

Home Number :

Fax :

Contact Privileges

Same as Department

☐

Contact Privileges :

* Contact View

All Contacts

Add / Edit Privileges

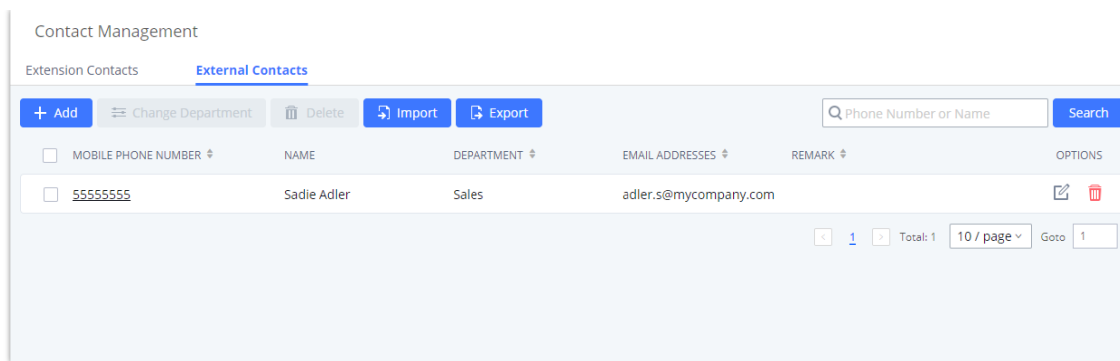
Privileges :

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.

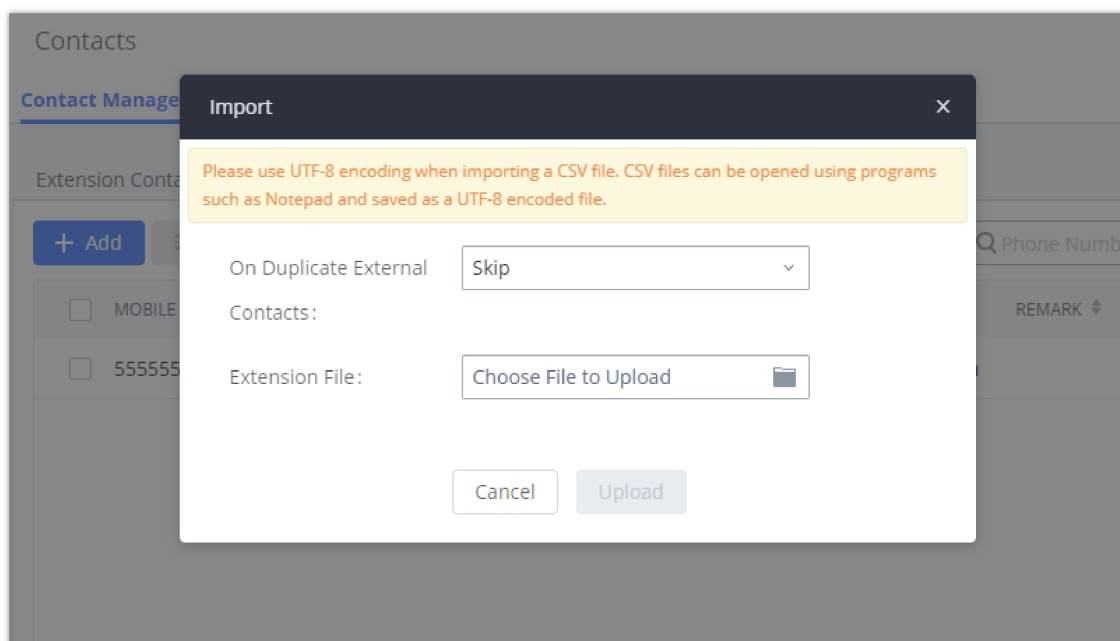


External Contacts

Click on "Export" icon, a CSV/XLSX 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/XLSX file or update the duplicate CloudUCM contact with the information in the CSV/XLSX.
- **Step 2:** Choose file from local PC to upload.
- **Step 3:** Click on "Upload".
- **Step 4:** Click on "Apply" to complete importing external contacts.



Import External Contacts

Department Management

Departments are organizational units that allows organizing extensions within groups that specify the specialty of a the extension owners within a company. This makes finding contacts easier within the UCM contact books.

Department Management	
+ Add --- (9)	
Quality Control	
Finance	
Marketing	
Technical Support	
Sales (1)	
Human Resources	
IT	
Logistics	

Department Management

Click on "Add" to create a new department. Configure the department name and select the superior department. By default the superior department is the root directory.

On the department list:

- Click on



to create sub department.

- Click on



to add member to the department.

- Click on



to edit the department.

Edit Department

* Department Name

Quality Control

Upper Level Department

* Contact View Privileges

All Contacts

Add / Edit Privileges

Privileges Applied To Sub-Level Departments

Cancel

OK

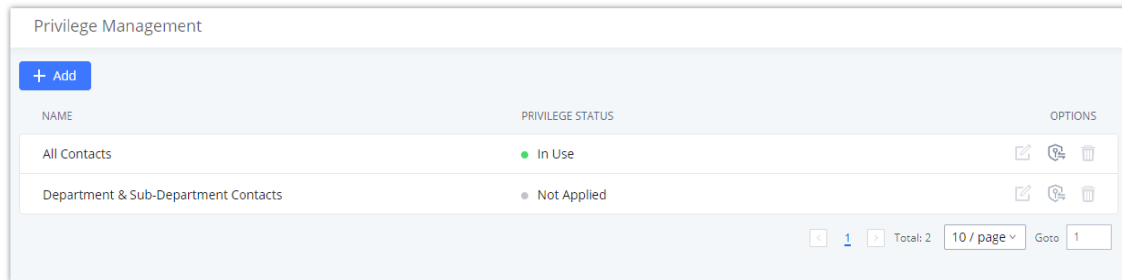
Edit Department

Privilege Management

The user can configure custom privileges other than the default ones (All contacts, Departments and sub-departments contacts). These custom privileges allow more flexible ways of allowing contacts to view all or specific contacts from other departments.

UCM admin can add or edit Privilege Management; under UCM web UI → **Contacts Privilege Management**, there are 2 default privileges:

- Visible to all contacts.
- Only the contact person's department and sub-department contacts are visible.

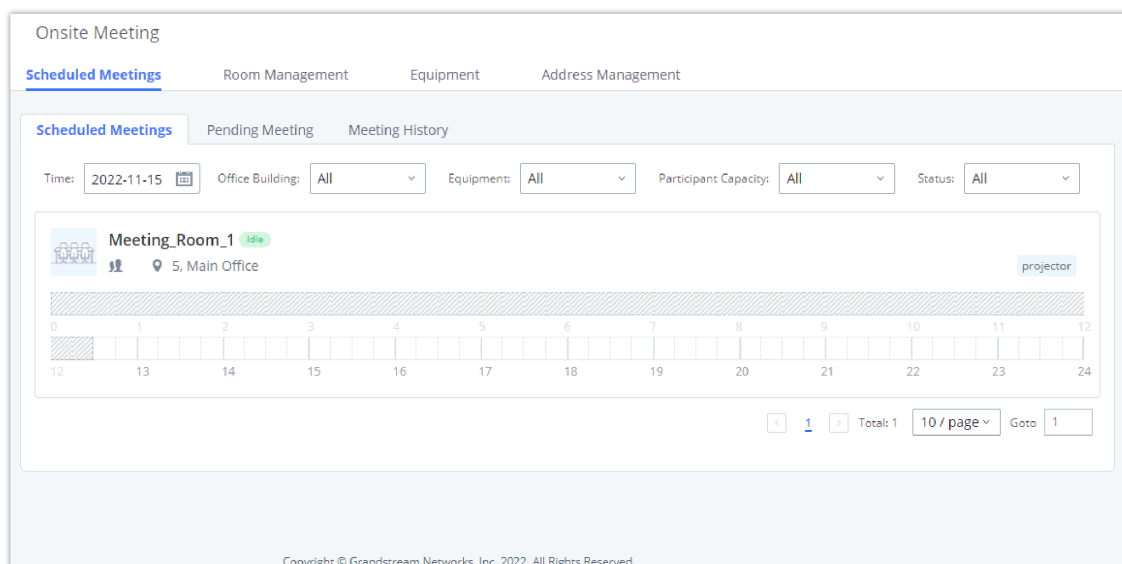


Privilege Management

DEVICE MANAGEMENT

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 **Device Management > Onsite Meeting** page. The first page that appears is the **Scheduled Meetings** page and tab page, which provide an overview of all created meeting rooms. It provides information about the rooms' meeting schedules for the day, their locations, their member capacity, and their equipment.



Schedule Onsite Meetings

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

Onsite Meeting						
Scheduled Meetings Room Management Facility Address Management						
Scheduled Meetings Pending Meeting Meeting History						
Schedule Meeting Meeting Subject Search						
MEETING SUBJECT #	MEETING ROOM #	MEETING OWNER #	START TIME #	MEETING DURATION #	REPEAT #	OPTIONS
Quick Meeting Starts soon	BackupRoom		Today 20:00 Etc/GMT+8	00:30:00	No Repeat	
Recent Events	BackupRoom		2022-11-24 07:00 Etc/GMT+8	01:00:00	No Repeat	
Yearly Reports	Primary-Meeting-Room		2022-12-29 13:00 Etc/GMT+8	01:00:00	No Repeat	

Pending Onsite Meetings

IP Camera Devices

The UCM admin can add IPC devices and edit accessible extensions so these extensions can view the surveillance streams for the IPC devices.

Click on "Add" to add IPC device.

IP Camera Devices

+ Add

Edit Allowed Members

Delete

Import

Export

☐ STATUS	DEVICE NUMBER	DEVICE NAME	URL	OPTIONS
☐ Unmonitored	4001	GSC3620	rtsp://192.168.5.74:554	

<

1

>

Total: 1

10 / page

Goto

1

IPC Devices

Create New IP Camera Devices

Cancel

Save

General

* Device Number:

* Device Name:

* Protocol:

RTSP

* IP Address:

* Port:

554

Channel Path:

Username:

Password:

* Transmission Protocol:

UDP

Heartbeat Detection:

☐

User Settings

* Allowed Members:

Search

Company Contact

☐ All

☐ 1005

☐ 2004

☐ 2003

Selected(0)

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

IP Camera Devices Settings

Edit the IPC device settings in the table below.

Device Number	The number that allowed members can dial to access the IP camera.
Device Name	Enter the name that you want to allocate for the device.
Protocol	The media control protocol used. ● RTSP
IP Address	Enter the IP address of the IP camera.
Port	Enter the port of the IP camera. The default is 554
Channel Path	If you want to view the stream of the specified channel, please configure the path of this stream.
Username	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Password	If a username and password are set on this device, fill in this field to allow the UCM to access the device.
Transmission Protocol	Transport protocol of the IP camera. Default is UDP.
Heartbeat Detection	If enabled, the PBX will regularly send RTSP OPTIONS to check of the device is still online.
Allowed Members	Extensions, Extension Groups, and Departments can be selected to access this IP camera by dialling the configured Device Number.

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 CloudUCM Web GUI. Additionally, the system will automatically create user accounts along with creating new extensions for extension users to login to the Web GUI using their extension number and password. All existing user accounts for Web GUI login will be displayed on User Management page as shown in the following figure.

User Information

In this section, the super administrator can create administrator accounts. The user can assign either the role of the admin of the UCM, or create custom privileges for the administrators.

User Management			
User Information	Custom Privilege	User Portal/Wave Privileges	User Endpoint Access History
+ Add			
Username	Privilege	Last Operation Time	Options
admin	Super Administrator	2024-11-07 13:41:39	 
Total: 1 < 1 > 10 / page ▼ Goto			

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.

User Management > Create New User

Cancel

Save

✖ Username

✖ User Password

Email Address

Privilege

Administrator ▾

Multi-Factor Authentication

☐

Mobile Number

+1 ▾

© 2023 Grandstream Networks, Inc.

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.
Privilege	This is the role of the Web GUI user. When super admin creates new user, “Adminstrator” or customized privilege can be selected.
User Password	Configure a password for this user which will be required in Web GUI login. English input is allowed without space,’ and “. Note: The password should contain at least 10 characters, with at least, one lower-case letter, one upper-case letter, one numeral, and one special character.
Email Address	Configure the email address for the user. This is optional.
Mobile Number	The user’s mobile phone number. This can be used for scenarios such as SMS verification code login and resetting password. It is recommended to configure country code to avoid potential SMS sending issues.
Multi-Factor Authentication	If enabled, the user account will be required to enter an MFA code in addition to login credentials when logging into the CloudUCM management web portal.

When the super admin creates new user, the email address for the new user is optional. However, when the admin user created by super admin logs in to edit user information, email address is mandatory. This email address is the same and will be sync up with the email address configured in login settings.

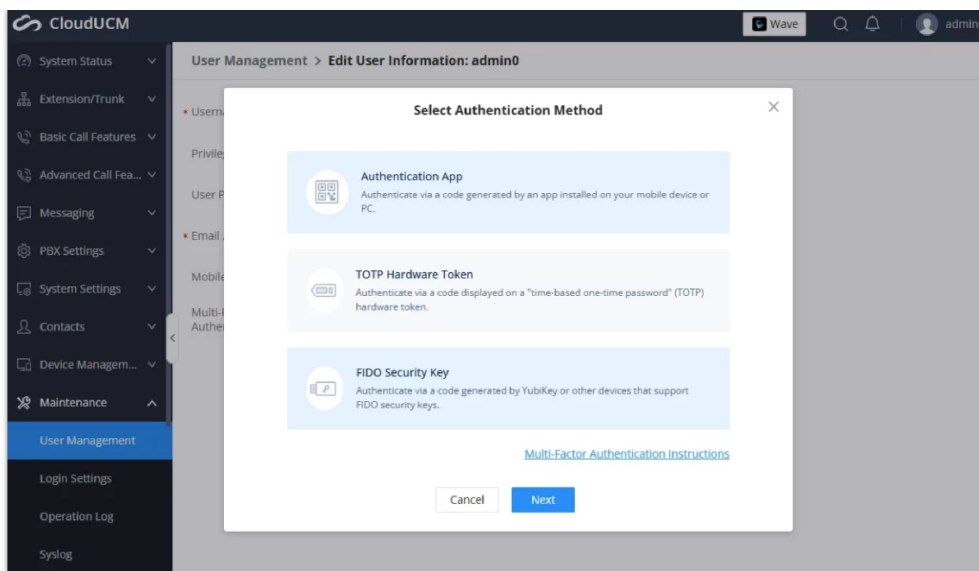
Once created, the Super Admin can edit the users by clicking on  or delete the user by clicking on .

Multi-factor Authentication

To enhance the security for CloudUCM, super admin and admins can select to use multi-factor authentication method for login to protect the login information.

CloudUCM supports three kinds of multi-factor authentication:

- **Authentication App:** refers to a software application (such as Google Authenticator or Microsoft Authenticator) that generates a unique temporary code for the users to access CloudUCM.
- **TOTP Hardware Token:** a hardware token that displays a time-sensitive one-time password to allow users to login to CloudUCM.
- **FIDO Security Key:** a physical device that allows users to login to CloudUCM without the need of a password, instead the device communicates with the Cloud UCM system via a cryptographic handshake, verifying the user’s identity.



Authentication Methods

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.
- 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.

Custom Privilege

By default, three levels are supported: **Super Administrator**, **Administrator**, **Wave Administrator**.

User Management			
User Information	Custom Privilege	User Portal/Wave Privileges	Extension Login Management
Add			
Privilege Name	Privilege Type	Options	
Super_Admin	Super Administrator	✎ ✖	
Admin	Administrator	✎ ✖	
Wave_Admin	Wave Administrator	✎ ✖	

Custom Privilege

Super Administrator

- This is the highest privilege. Super Admin can access all pages on the CloudUCM, change configuration for all options and execute all the operations.
- Super Admin can create, edit, and delete one or more users with the "Admin" privilege
- Super Admin can edit and delete one or more users with the "Consumer" privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account "admin" is configured with the "Super Admin" privilege and it is the only user with the "Super Admin" privilege. The Username and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on Web GUI→**Maintenance**→**Login Settings** page.

- Super Admin could view operations done by all the users in Web GUI→**Maintenance**→**User Management**→**Operation Log**
- The Super Admin can allow administrators to view Email Account passwords.

User Management > Edit Custom Privilege: Admin

Privilege Name: Admin

Password Visibility Toggle: ☒ Email Account Password

Custom Privilege: ☒ All, ☒ Basic Privileges, ☐ Backup, ☐ Upgrade, ☐ CloudUCM Services

Password Visibility Toggle

Administrator

- Users with "Admin" privilege can only be created by "Super Admin" user.
- "Admin" privilege users cannot create new users for login.
- "Admin" privilege users are by default not allowed to access the following pages:

Maintenance → Backup

Maintenance → Upgrade

RemoteConnect

Settings→User Management→Operation Log

Note: By default, administrator accounts are not allowed to access backup menu, but this can be assigned to them by editing the option "**Maintenance → User Management → Custom Privilege**" then press to edit the "Admin" account and include backup operation permission for these types of users.

User Management > Edit Custom Privilege: Admin

Privilege Name: Admin

Password Visibility Toggle: ☒ Email Account Password

Custom Privilege: ☒ All, ☒ Basic Privileges, ☒ Backup, ☐ Upgrade, ☐ CloudUCM Services

Assign Backup permission to Admin users

Wave Administrator

- This permission type does not support editing or deletion.
- This includes management of Wave-related function settings only and does not involve access to the CloudUCM module.
- Users can set the Wave Admin privilege for specific extension under **Extension/Trunk → Extensions → Edit Extension**

For more information, please refer to the [Wave Administrator Guide](#) guide.

Extensions > **Edit Extension: 1000**

[Basic Settings](#) | Media | Features | Voicemail | Custom Time | Wave Client | Follow Me | Advanced Settings

AuthID * Concurrent Registrations

Disable This Extension ☐

User Settings

First Name Last Name

Email Address * User/Wave Password

* User Portal/Wave Privileges Mobile Number

[Add / Edit Privileges](#)

Department Job Title

Contact Privileges

Same as Department Contact Privileges ☒ * Contact View Privileges

Sync Contact ☒ [Add / Edit Privileges](#)

User Portal/Wave Privilege

Add Custom Privilege

User Management

[User Information](#) | [Custom Privilege](#) | [User Portal/Wave Privileges](#) | [Extension Login Management](#) | [User Endpoint Access History](#)

Privilege Name	Privilege Type	Options
Super_Admin	Super Administrator	Edit Delete
Admin	Administrator	Edit Delete
Wave_Admin	Wave Administrator	Edit Delete

Add New Custom Privilege

The Super Admin user can create users with different privileges. Below are the items available for privilege customization.

All	System Status	Extensions	Extension Groups
Outbound Routes	Inbound Routes	Multimedia Meeting	IVR
Voicemail	Ring Groups	Paging/Intercom	Call Queue
Queue Recordings	Queue Statistics	Speed Dial	Event List
Feature Codes	Parking Lot	Pickup Groups	Dial By Name
DISA	Callback	Scheduled Call	Fax Sending
Fax/T.38	Announcement	SCA	Emergency Calls
Restrict Calls	Music On Hold	Music On Hold	Time Settings
LDAP Server	Contacts	System Events	Backup
CDR Recordings	CDR Records	CDR Statistics	CloudUCM Services
API Configuration	PMS – Room Management	PMS – Room Status	PMS – Wakeup Service
PMS – Housekeeper			

1.

Log into CloudUCM 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 CDR Recordings, respectively). This offers more flexibility on the privileges that the admin assigns to the user.

User Management > Create New Custom Privilege

* Privilege Name

☒ Allow Deletion of CDR

☒ Allow Deletion of Recordings

* Custom Privilege

☐ 38 items Available

Search

☐ API Configuration

☐ Backup

☐ Callback

☐ Call Queue

☐ Queue Statistics

☐ Queue Recordings

☐ 3 items Selected

Search

☐ CDR Recordings

☐ CDR Records

☐ CDR Statistics

Cancel Save

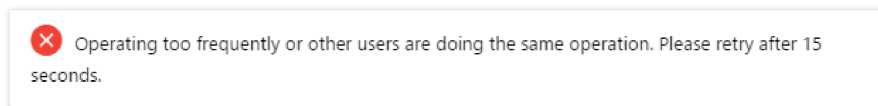
Create New Custom Privilege

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 CloudUCM. 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.



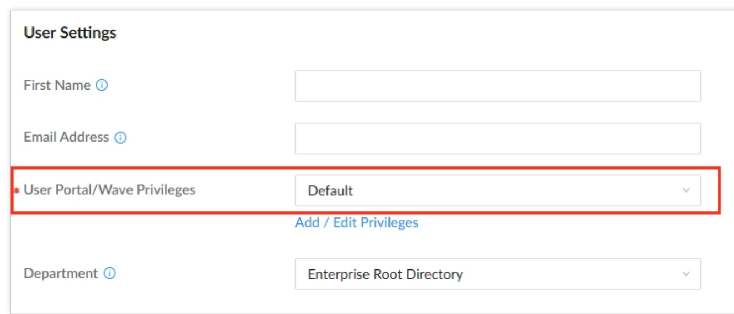
Note

Only one session can be opened per user. If a new session has been opened for an account that had already been opened. The older session will be terminated upon the login of the user.

User Portal/Wave Privileges

The administrator can create customized privileges related to an extension's User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.

After the creation of the privilege, the administrator can assign the privilege to a specific extensions by navigating to **Extension/Trunk→Extensions→Basic Settings→User Portal/Wave Privileges**.

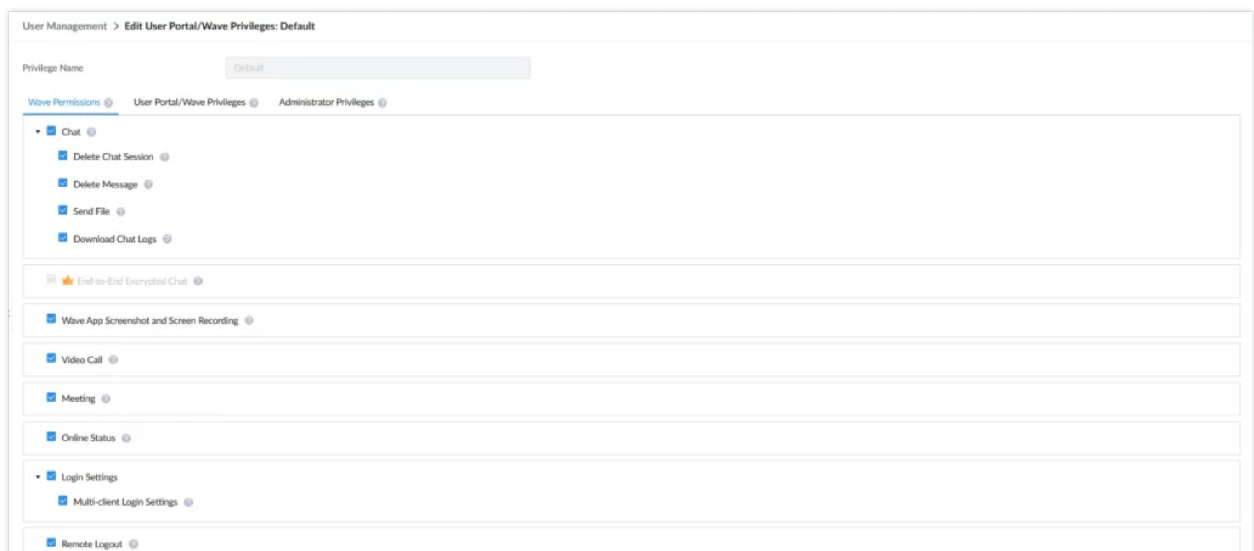


The image shows a 'User Settings' form. It has four main input fields: 'First Name', 'Email Address', 'User Portal/Wave Privileges', and 'Department'. The 'User Portal/Wave Privileges' field is highlighted with a red rectangular box and currently shows 'Default'. Below this field is a blue link that says 'Add / Edit Privileges'. The 'Department' field shows 'Enterprise Root Directory'.

User Portal/Wave Configuration

Wave Permissions

Under Wave Permissions category, the user can configure the various permissions for the basic features of Wave such as using the chat, making audio/video calls, meeting, use application store, etc...



The image is a screenshot of the 'Wave Permissions' tab within the 'Edit User Portal/Wave Privileges: Default' configuration page. At the top, there's a 'Privilege Name' field with 'Default' selected. Below this are three tabs: 'Wave Permissions', 'User Portal/Wave Privileges', and 'Administrator Privileges'. The 'Wave Permissions' tab is active, showing a list of permissions with checkboxes. The permissions listed are: Chat (expanded to show sub-items: Delete Chat Session, Delete Message, Send File, Download Chat Logs), End-to-End Encrypted Chat, Wave App Screenshot and Screen Recording, Video Call, Meeting, Online Status, Login Settings (expanded to show sub-items: Multi-client Login Settings, Remote Logout), and Remote Logout.

Wave Permissions Tab

- **Chat:** Toggles ability to use the Wave Chat feature.
 - **Delete Chat Session:** Toggles support for Wave to delete chats and chat history. This data will only be deleted on the Wave client side.
 - **Delete Message:** Controls whether Wave users will be allowed to delete messages that have been sent. Deleted messages will not be visible to anyone.
 - **Send File:** Toggles file/image sending support in Wave chat. If disabled, users will still be able to download, view and forward chat files.
 - **Download Chat Logs:** If enabled, chat logs will be downloadable from the Wave client, including chat logs from Wave/WhatsApp/Telegram/LiveChat sessions.
- **End-to-End Encrypted Chat*:** Toggles ability to use the Wave End-to-End Encrypted Chat feature.
- **Wave App Screenshot and Screen Recording:** Controls whether users are allowed to take screenshots and perform screen recordings in the Wave mobile app.
- **Video Call:** Toggles ability to use the Wave Video Call feature.
- **Meeting:** Toggles ability to use the Wave Meeting feature.
 - **Start Video During Meeting:** Toggles ability to use the Wave Start During Meeting feature.
- **Online Status:** Toggles ability to set Wave online status such as "Busy", "Appear Away", "Do Not Disturb", "Appear Offline", etc. If unchecked, the status will be displayed as only either "Online" or "Idle".

- **Login Settings**
 - **Multi-client Login Settings:** If enabled, users will be allowed to enable or disable the option “Allow Simultaneous Logins from the Same Client Type”.
- **Remote Logout:** If enabled, Wave users will be able to log out of their accounts from other logged-in devices.
- **Recording Status:** Controls whether the recording status is displayed in all calls/conferences of the extensions. **Note:** If the call recording prompt is enabled, it will be played as this setting affects the indicator that shows that a call is being recorded on Wave.
- **Clear Recent Call History:** Toggles ability to delete recent call history entries and entire recent call history on Wave.
- **Application:** Toggles ability to access the “Applications” page under Wave Desktop and Wave Web.
- **Smart Devices:** Toggling off privileges will hide the corresponding pages and options in Wave.
 - **Door System**
 - **Monitor**
 - **Call Device (CTI)**
- **3rd Party Applications**
 - **App Store:** Toggles ability to install applications from Wave application store. If unchecked, the application store will be hidden, but installed apps can still be used.

User Portal/Wave Privileges

Under User Portal/Wave Privileges, the administrator can configure the access privileges to certain settings and feature such as adjusting account settings, changing SIP/IAX password and AuthID, setting DND. Or access to personal data such as accessing the CDR of the user, configuring Follow me or Voicemail, etc...

User Management > Edit User Portal/Wave Privileges: Default

Privilege Name: Default

Wave Permissions ? User Portal/Wave Privileges ? Administrator Privileges ?

- ☒ Account Settings ?
- ☒ Extension Settings ?
 - ☒ Do Not Disturb ?
 - ☐ SIP/IAX Password & AuthID ?
 - ☐ Configuration Voicemail
- ☒ Manage Recordings ?
 - ☐ Delete Recordings ?
- ☒ Personal Data ? Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
 - ☒ CDR
 - ☒ Follow Me
 - ☒ Voicemail
 - ☒ Recording Files ?
 - ☒ Fax Files

Cancel Save

User PortalWave Privileges

- **Account Settings:** If unchecked, the *User Portal*→*Basic Information*→*Account Settings* page and the *Wave*→*Sidebar*→*User*→*Account Settings* option will be hidden.
- **Extension Settings:** If unchecked, the extension’s *User Portal*→*Basic Information*→*Extensions* page and the *Wave*→*Sidebar*→*User*→*Call Settings* option will be hidden.

- **Do Not Disturb:** Toggles ability to set DND through the User Portal.
- **Change Password Or Verify ID:** Toggles ability to access the **Password** and **AuthID** settings under the *User Portal→Basic Information→Extensions→Basic Settings* page.
- **Configuration Voicemail:** Toggles ability to configure the extension voicemail options.
- **Manage Recordings:** Toggles ability to view recordings through the User Portal and Wave, including the recordings in call logs, meeting details, and Wave application.
 - **Deleting Recordings:** Toggles ability to delete recordings through the User Portal and Wave. For Wave, this includes the ability to delete call logs, meeting details, and recordings.
- **Personal Data:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
 - CDR
 - Follow Me
 - Voicemail
 - Recordings files
 - Fax Files
 - SCA
- **Other Features:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
 - Fax Sending
 - Call Queue
 - Schedule Call

*: Features which are marked by an asterisk are a part of RemoteConnect plans.

Administration Privileges

Under Administrator Privileges, the administrator can configure enabling certain extensions to view a designated team's CDR.

User Management > Edit User Portal/Wave Privileges: Default

Privilege Name: Default

Wave Permissions ⓘ User Portal/Wave Privileges ⓘ **Administrator Privileges ⓘ**

☐ View Team CDRs And Recordings ⓘ Team

☐ Download Team Recording Files

Cancel Save

Administrator Privileges

- **View Team CDRs and Recordings:** Define whether certain extensions can view each other's CDR. Click on "Team" to designate the extensions.
 - **Download Team Recording:** When this option is enabled, the extensions selected in the team will be allowed to access each other's CDR and call recording files.

Pre-installed Plugins

The administrator can set the plug-ins which will be installed when the user logs into Wave Desktop.

To configure the pre-installed plugins, follow the steps below.

1. Navigate to **Maintenance→User Management→User Portal/Wave Privileges** then click "Pre-installed Plug-ins".

User Management

System User Information

User Portal/Wave Privileges

Extension Login Management

User Endpoint Access History

Add

Pre-installed plugins

Privilege Name	Options
Default	

Total: 1

< 1 >

10 / page

Goto

2. Click on "Add Add-in" button.

User Management > Pre-installed plugins

Pre-install the Wave add-in for extension users. After users sign in to Wave, the assigned add-ins will be automatically installed.

Add Add-in

Pre installed Plug ins

User Management > Pre-installed plugins

< Add

*Add-in

Please enter

Configure Parameters

Only json format is supported. Please refer to the user manual for rules

User Manual

*Users

☒ All Users
☐ Specific Users

Cancel

OK

Add Pre installed Plug ins

Parameter	Description
Add-in	Select an add-in. 1. Act! CRM 2. Bitrix24 3. Capsule CRM 4. Dynamics 365 5. Freshdesk 6. Google Drive 7. Hubspot 8. IPVideoTalk 9. Less Annoying CRM

	10. Monday Sales CRM 11. Odoo CRM 12. Office365 13. OfficeRnD Hybrid Work 14. Oracle NetSuite 15. Salesforce 16. SugarCRM 17. Telegram 18. Vtiger CRM 19. Whatsapp Business 20. Zendesk 21. Zoho CRM 22. Zoho Desk
Configure Parameters	Enter the configuration parameters. The configuration parameters consist of authentication information, database name, webhook url etc... Note: Please note that only JSON format is supported. Example: Whatsapp Business <pre>{ "config": [{ "name": "xxxxx", "accessToken": "xxxxx", "payloadKey": "xxxxx", "webhooksUrl": "xxx", "phoneNumIDList": ["xxxxx", "xxxxx"] }] }</pre>
Users	Select which extension(s) to apply this rule to. • All Users • Specific Users

Info

For the complete steps and information about pre-installing plug-ins, please refer to the following guide:
<https://documentation.grandstream.com/knowledge-base/pre-install-wave-add-ins-on-the-ucm63xx/>

Extension Login Management

Extension Login Management allows the administrator to review the logged-in sessions of SIP devices and Wave.

User Management

User Information

Custom Privilege

User Portal/Wave Privileges

Extension Login Management

User Endpoint Access History

Updated based on SIP registration status.

Extension Number or Name

Q

Extensions	Name	Registration Device	Endpoint Type	Registration Time	SIP Registered Address	Options
4003		GRP2612P	SIP device	2024-09-11 10:19:16	192.168.6.8:5060	
4002			SIP device	2024-09-11 10:06:46	192.168.5.194:63532	
4004		WP826	SIP device	2024-09-11 09:55:44	192.168.5.163:5060	
4000		GDS3710	SIP device	2024-09-06 16:59:37	192.168.6.86:5060	

Total: 4

<

1

>

10 / page

Goto

Extension Login Management

For Wave sessions, the administrator can click on  to terminate a Wave session. SIP sessions cannot be logged out.

User Endpoint Access History

The User Endpoint Access History tab allows the administrator to view the access history of all extensions, the time on which the access has occurred, the IP addresses from which the extensions were accessed, and whether they were accessed from the User Portal, Wave Web/Desktop, or mobile. Extension access from the SIP endpoints won't be logged in this page.

User Management					
User Information		Custom Privilege	User Portal/Wave Privileges	User Endpoint Access History	
EXTENSIONS ⚙	NAME ⚙	EXTENSION TYPE ⚙	TERMINAL TYPE	LAST OPERATION TIME	IP ADDRESS
1000	Arthur Morgan	SIP(WebRTC)	Android/iOS	2022-11-14 18:15:35	192.168.5.137
1001		SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-11-11 10:18:22 2022-11-14 16:10:37 2022-08-10 09:26:40	192.168.5.119 192.168.5.76 192.168.5.111
1002		SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-11-11 10:18:22 2022-11-14 16:53:03 2022-08-23 15:49:30	192.168.5.93 192.168.5.79 192.168.5.111
1003	Catherine Braitwaite	SIP(WebRTC)	Wave Web/Desktop Android/iOS User portal	2022-10-18 14:14:12 2022-11-14 20:34:59 2022-11-17 09:19:44	192.168.5.111 192.168.5.76 192.168.5.168
1004	John Marston	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-08-16 15:32:37 2022-11-16 11:26:44	192.168.5.111 192.168.5.91
1005	Abigail Roberts	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-11-16 17:42:47 2022-11-16 18:11:34	 192.168.5.79
1006	Mary-Beth Gaskill	SIP(WebRTC)	Wave Web/Desktop Android/iOS	2022-11-16 16:21:14 2022-11-16 17:37:50	192.168.5.165 192.168.5.79
1007	Hosea Matthews	SIP(WebRTC)	Wave Web/Desktop	2022-11-16 17:50:35	192.168.5.63

< 1 > Total: 8 10 / page Goto 1

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

User Endpoint Access History

Login Settings

In this category, the user can change information regarding their account user, as well as the login general settings and the login settings.

Change Password/Email

Change Password

After logging in the CloudUCM Web GUI for the first time, it is highly recommended for users to change the default password to a more complicated password for security purpose. Follow the steps below to change the Web GUI access password.

1. Go to Web GUI→**Maintenance**→**Login Settings**→**Change Password / Email** page.
2. Enter the old password first.
3. Enter the new password and re-type the new password to confirm. The new password has to be at least 4 characters. The maximum length of the password is 30 characters.
4. Configure the Email Address that is used when login credential is lost.
5. Click on "Save" and the user will be automatically logged out.
6. Once the web page comes back to the login page again, enter the username "admin" and the new password to login.

Login Settings

[Change Password / Email](#)
[Login Security](#)
[Remote Login](#)

To remove the security warning message at the top of the page, both username and password must be changed.

Change Password

Change Password ☐

Change Username

Change Username ☐

Change Email Address

* Email Address [Email Template](#)

Change Phone Number

Mobile Number [SMS Template](#)

Enter Current Password

* Enter Current Password

Change Password

Enter Old Password	Enter the Old Password for CloudUCM
Change Password	Enable Change Password
Enter New Password	Enter the New Password for CloudUCM
Re-enter New Password	Retype the New Password for CloudUCM
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

CloudUCM allows users to change Super Administrator username.

Change Username

Change Username: ☒

* Please enter the username:

Change Email Address

CloudUCM allows user to configure binding email in case login password is lost. CloudUCM login credential will be sent to the designated email address. The feature can be found under Web GUI→ **Maintenance**→**Login Settings**→**Change Password / Email**

Change Binding Email

* Email Address :
[Email Template](#)

Change Binding Email

Email Address	Email Address is used to retrieve password when password is lost
----------------------	--

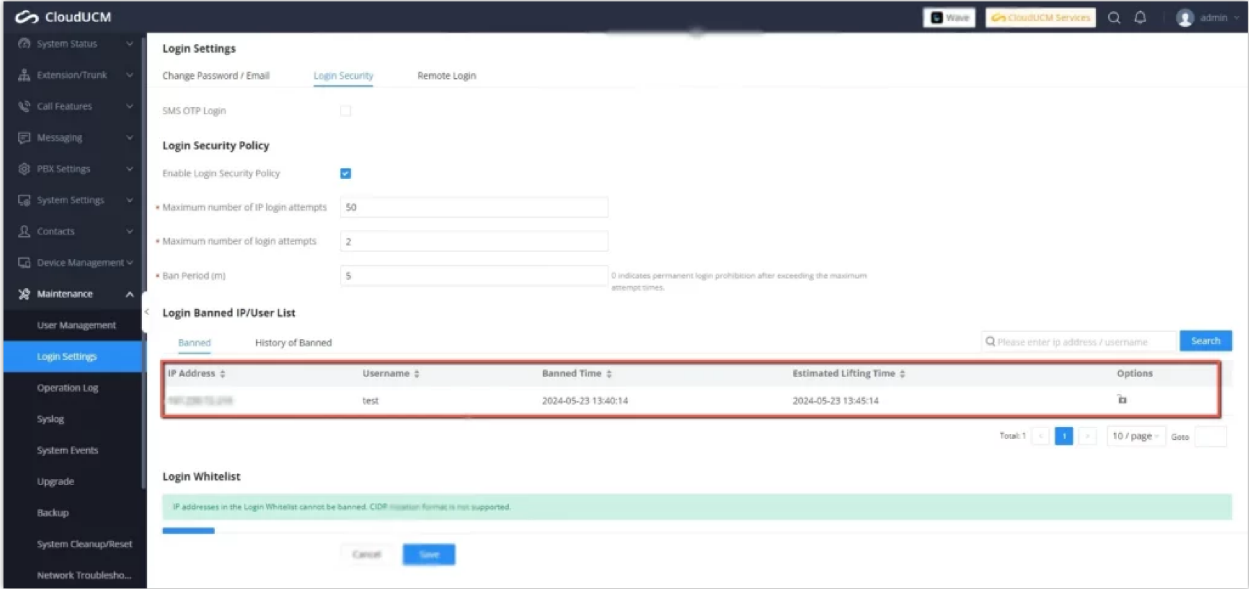
Change Binding Email option

Login Security

After the user logs in the CloudUCM 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 CloudUCM 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.

The CloudUCM admin have the possibility to lift the ban on a specific user by clicking the icon  under banned users.



Login Settings

Change Password / Email | **Login Security** | Remote Login

SMS OTP Login ☐

Login Security Policy

Enable Login Security Policy ☒

Maximum number of IP login attempts: 50

Maximum number of login attempts: 2

Ban Period (m): 5 (0 indicates permanent login prohibition after exceeding the maximum attempt times)

Login Banned IP/User List

Banned | History of Banned

Please enter ip address / username:

IP Address	Username	Banned Time	Estimated Lifting Time	Options
192.168.1.100	test	2024-05-23 13:40:14	2024-05-23 13:45:14	

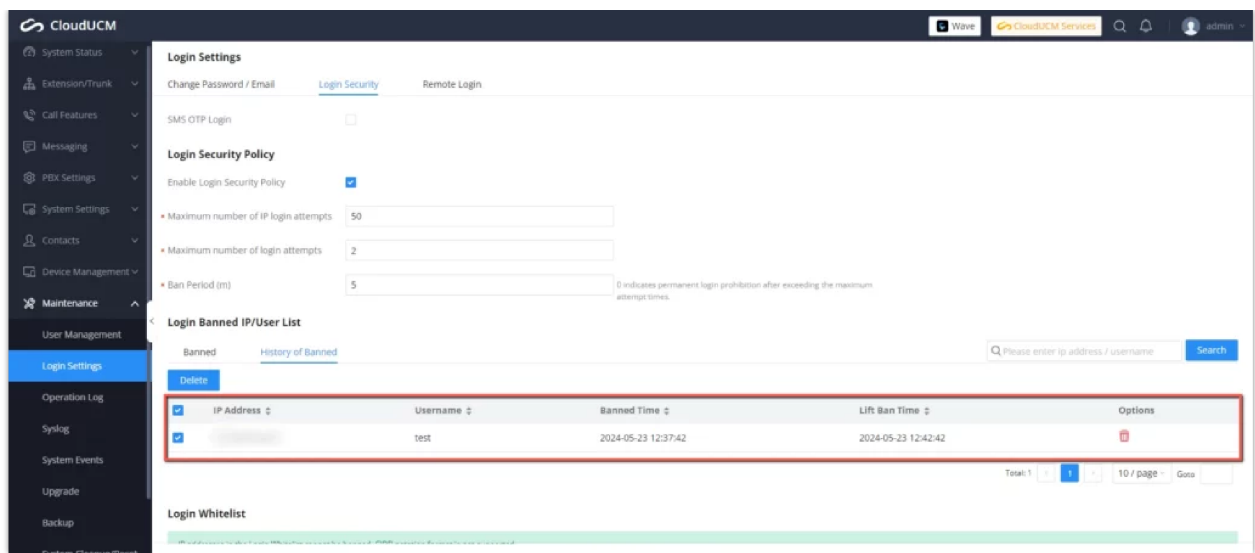
Total: 1 / 10 / page

Login Whitelist

IP addresses in the Login Whitelist cannot be banned. CIDR notation format is not supported.

Log in Settings

After the Ban period is completed, the banned user will be displayed under the history of banned. The admin can delete the history query by selecting the banned users and clicking on “Delete”



CloudUCM History of Banned

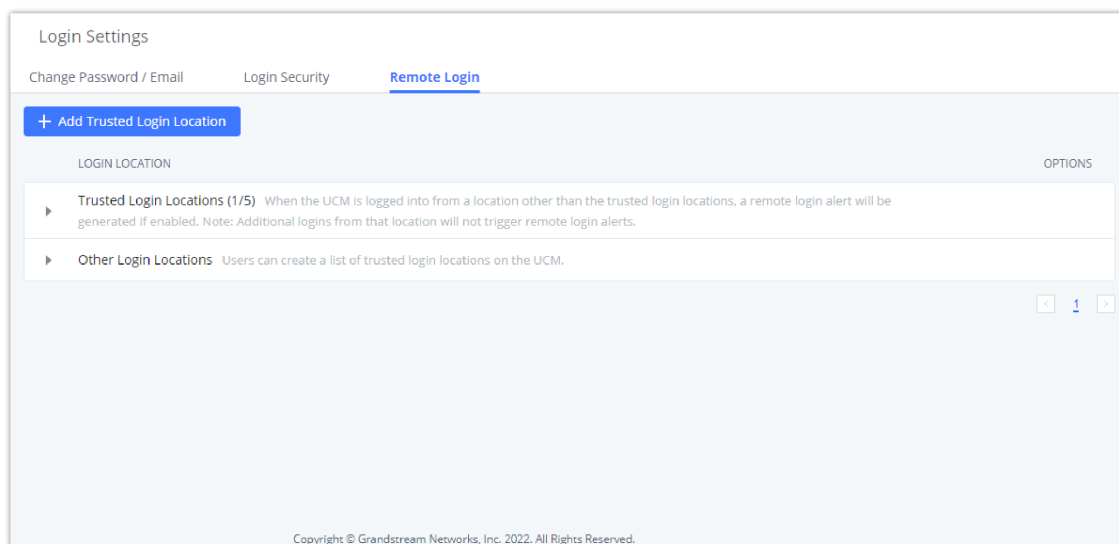
Login Settings	
User Login Timeout (m)	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. If set to 0, the user will not be logged out automatically.
SMS OTP Login	If enabled, users will be able to log in and reset password via SMS verification code. Mobile phone numbers will need to be configured for administrators and extensions.
Login Security Policy	
Enable Login Security Policy	Enables/Disables Login Security Policy
Maximum number of IP login attempts	The maximum number of consecutive login errors allowed for one or more users using a certain IP address. After exceeding this number, all users will be prohibited from using this IP address to log in.
Maximum number of login attempts	The maximum number of consecutive failed login attempts. When exceeded, the user will not be able to log in for the amount of time specified in "User ban period". A value of 0 means unlimited attempts.
Ban Period (m)	The number of minutes for after exceeding the maximum allowed a number of consecutive failed login attempts. A value of 0 indicates a permanent ban.
Login Banned IP/User List	List of IP addresses that are banned from making any further login attempts.
Banned	Displays currently banned IP addresses and usernames with details like ban time and estimated lifting time. It helps administrators manage active bans to enhance security. Note: The administrator has the option to lift the ban, by selecting the option "Lift Ban"
History of Banned	Shows past bans of IP addresses and usernames with relevant details, even after bans are lifted. It helps in reviewing historical security incidents and identifying patterns. Note: The verification code error is not accumulated when the login fails
Login Whitelist	List of IP addresses that can make unlimited login attempts, users can define the whitelisted IP Address.

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 CloudUCM would be directly connected to the Internet, and the public IP address would be used for the remote login. This feature adds a layer of visibility and control, thus enhancing the security of the UCM.

In this tab there are two types of lists of locations:

- Trusted Login Locations: These are the trusted login locations that are added manually by the admin. Any added trusted login location will not generate any remote login alert upon the first time login.
- Other Login Location: This list will show all the remote login locations that are not trusted, logging in for the first time from an untrusted login location will generate an alert, but the subsequent remote logins from the same location will not generate alerts.



Remote Login

To add a trusted login location, the user must click on



Add Trusted Login Location

If a public IP address is entered as the trusted login location, the UCM will automatically detect the location of the IP address.

IP Address:

Check Location

Format: xxx.xxx.xxx.xxx

Close

OK

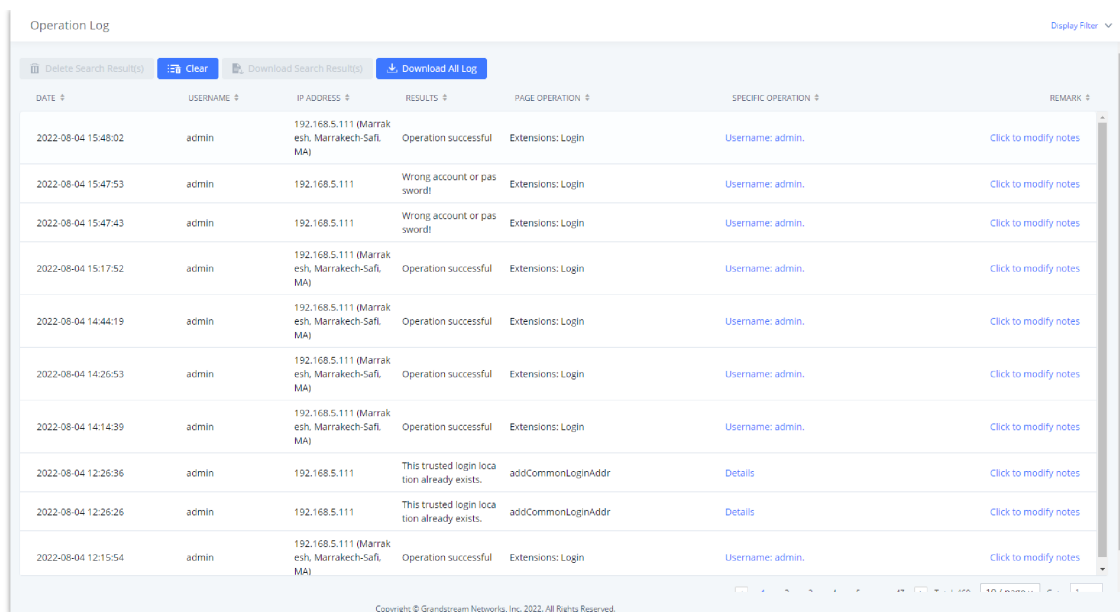
Then add the public IP address of the location, click on **"Check Location"** to verify if it's the correct location then click **"OK"**.

Note

The system administrator can add up to 5 Trusted Login Locations, while Other Login Locations can have an unlimited number of entries.

Operation Log

Super Admin has the authority to view operation logs on CloudUCM 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 etc. There are 7 columns to record the operation details "Date", "Username", "IP Address", "Results", "Page Operation", "Specific Operation" and "Remark".



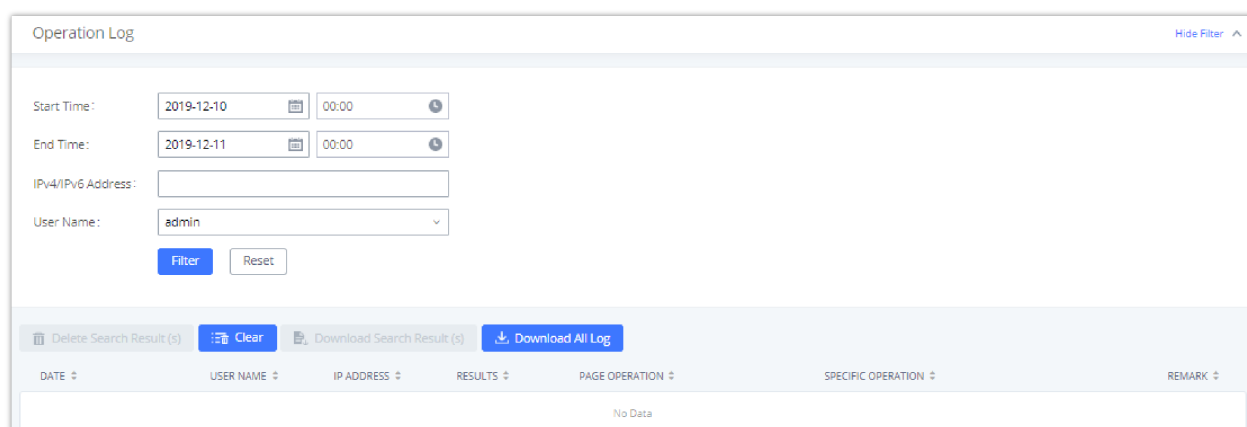
DATE	USERNAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
2022-08-04 15:48:02	admin	192.168.5.111 (Marrakesh, Marrakech-Safi, MA)	Operation successful	Extensions: Login	Username: admin.	Click to modify notes
2022-08-04 15:47:53	admin	192.168.5.111	Wrong account or password!	Extensions: 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

Operation Logs

The operation log can be sorted and filtered for easy access. Click on  or  at the top of each column to sort. For example, clicking on  for “Date” will sort the logs according to newer operation date and time. Clicking on  for “Date” will reverse the order.

Date	The date and time when the operation is executed.
Username	The username of the user who 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.

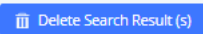
User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on “Display Filter”.



DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
No Data						

Operation Logs Filter

The above figure shows an example that operations made by user “support” on device with IP 192.168.40.173 from 2014-11-01 00:00 to 2014-11-06 15:38 are filtered out and displayed.

To delete operation logs, users can perform filtering first and then click on  to delete the filtered result of operation logs. Or users can click on  to delete all operation logs at once.

Syslog

On the CloudUCM, 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 CloudUCM settings because it can be helpful to locate the issues when errors happen.

Some typical modules for CloudUCM functions are as follows and users can turn on “NOTICE” and “VERBOSE” levels besides “error” level.

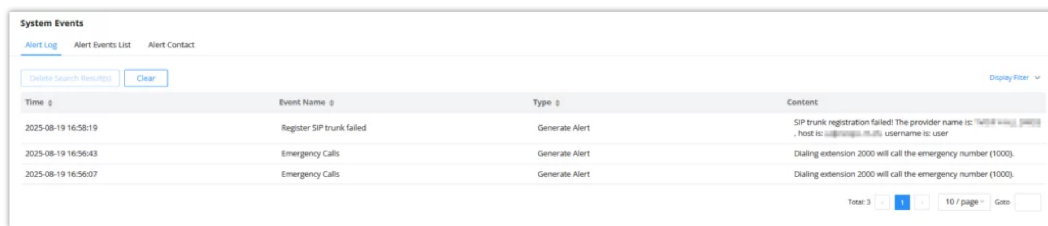
- **pbx**: This module is related to general PBX functions.
- **pjsip**: This module is related to SIP calls.
- Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog prints might cause traffic and affect system performance.
- The reserved size for Syslog entries on the cache memory of the UCM is 50M, once this sized is reached the UCM will clean up 2M of the oldest Syslog entries to allow to save new logs.

System Events

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

Alert Log

Under **Maintenance** → **System Events** → **Alert Log**, system messages from triggered system events are listed as alert logs.



Time	Event Name	Type	Content
2025-08-19 16:58:19	Register SIP trunk failed	Generate Alert	SIP trunk registration failed! The provider name is: [redacted], host is: [redacted], username is: user
2025-08-19 16:56:43	Emergency Calls	Generate Alert	Dialing extension 2000 will call the emergency number (1000).
2025-08-19 16:56:07	Emergency Calls	Generate Alert	Dialing extension 2000 will call the emergency number (1000).

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 “Display Filter”. Alert logs are classified into two types by the system:

1. **Generate Alert**: Created when an alert condition is triggered (e.g., unauthorized access attempt, system threshold reached).
2. **Restore to Normal**: Created when the alert condition is cleared (e.g., system status returns to normal).

Users can filter alert logs by type to display only **Generate Alert** or only **Restore to Normal**, depending on their needs.

[Hide Filter](#)

Start Time

Date

Time

End Time

Date

Time

Event Name

All

Type

All

Reset

Filter

Filter for Alert Log

Alert Events List

The system alert events list is located under **Maintenance** → **System Events** → **Alert Events List**. The events described in this section, along with their corresponding actions, are currently supported on CloudUCM.

When these events occur, the system can generate alerts, email notifications, SMS notifications, and HTTP notifications.

Click on to adjust the parameters of events that support configuration.

System Events
Alert Log Alert Events List Alert Contact

Some alerts will display the following icons when toggled on: indicates that the alert is associated with other settings that must be configured; indicates that the alert is active for the enabled settings, and other related settings can be enabled.

When alert events with the GOMS logo are triggered, alert information will be synced to GOMS.

Alert On
Alert Off
Email Notification On
Email Notification Off
SMS Notification On
SMS Notification Off

Event Name	Alert	Alert Contact	Options
Security			
☐ Fail2ban Blocking	☐	Email ☐ SMS ☐	
☐ User Login Banned	☐	Email ☐ SMS ☐	
☐ Remote Login	☐	Email ☐ SMS ☐	
☐ User Login Success	☐	Email ☐ SMS ☐	
☐ User Login Failed	☐	Email ☐ SMS ☐	
☐ Modify Super Admin Password	☐	Email ☐ SMS ☐	
System			
☐ System Update	☐	Email ☐ SMS ☐	
☐ System Reboot	☐	Email ☐ SMS ☐	
☐ Cloud IM Abnormal	☐	Email ☐ SMS ☐	
☐ Data Sync Backup	☐	Email ☐ SMS ☐	
☐ Restore Config	☐	Email ☐ SMS ☐	
Storage			
☐ Storage Usage	☐	Email ☐ SMS ☐	
Call Features			
☐ Emergency Calls	☐	Email ☐ SMS ☐	

Alert Event List

Security	
Fail2ban Blocking	If the system Fail2ban is blocking, the event will be recorded in the alert log.
User Login Banned	If user login is blocked, the event will be recorded in the alert log.
Remote Login	An alert will be generated upon a remote login.
User Login Success	Successful user login events will be recorded in the alert log.
User Login Failed	User login failure events will be recorded in the alert log.
Modify Super Admin Password	An alert will be generated when the super admin password is changed.
System	
System Update	Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
System Reboot	CloudUCM will detect the system restart and will send an alert for it.

Cloud IM Abnormal	An alert message will be generated if the Cloud IM encounters any issue or exhibits any abnormal behavior.
Data Sync Backup	If the system performs data synchronization and backup abnormalities, the event will be recorded in the alert log.
Restore Config	Once the system configuration is restored, the configuration restoration event will be recorded in the alert log.
Storage	
Storage Usage	If CloudUCM's storage usage reaches the active plan's capacity, the system will generate an alert and log the event.
Call Features	
Emergency Calls	If the system generates an emergency call, the event will be recorded in the alert log.
SIP Outgoing Call through Trunk Failure	If the system SIP trunk outgoing call fails, the event will be recorded in the alert log.
SIP Internal Call Failure	If the system SIP extension call fails within the office, the event will be recorded in the alert log.
Max Concurrent Call Limit	Allows configuring the minimum amount of time (in seconds, minutes, hours or days) between alert sending when the concurrent calls reach the package limit.
Excessive Outbound Calls	When an extension initiates calls frequently, an alert will be logged in the alert log and a notification will be pushed.
Outbound Call Duration	This alert is triggered if a call reaches the duration limit set on the outbound rule.
Trunk Outbound Call Duration Usage	This alert is triggered if a call reaches the duration limit set on the trunk.
Trunk Concurrent Calls	This alert is triggered if the number of concurrent calls is reached on a specific trunk.
Extension/Trunk Status	
Register SIP trunk failed	CloudUCM will detect the failure of SIP trunk registration at a set interval.
SIP Peer Trunk Status	If the SIP peer trunks status is abnormal, the event will be recorded in the alert log.
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.
SIP Lost Registration	If System SIP extension registration is lost, the event will be recorded in the alert log. Clicking on the edit button, the user can access to enable or disable Ignore Wave App Registration Loss.

Alert Contact

This feature allows the administrator to be notified when one of the Alert events mentioned above happens. Users could add administrator's Email address under **Maintenance → System Events → Alert Contact** to send the alert notification to an email (Up to 10 Email addresses can be added) or also specify an HTTP server where to send this alert.

System Events
Alert Log
Alert Events List
Alert Contact

Email Notification

Email Notification
Real-time

Notification Interval
minute(s)
"0" means no notification will be sent.

Super Admin Email
Add Super Admin Email

Admin Email
Add Admin Email

Email Template
[Email Template](#)

SMS Notification

Super Admin Phone Number
+1
Add Super Admin Phone Number

Admin Phone Number
+1
Add Admin Phone Number

SMS Template
[SMS Template](#)

Cancel
Save

Alert Contact

Email Notification	
Email Notification	Alert email notification delivery method: Real-time: Notifications will be sent out as soon as the alerts are generated. Periodic: Alerts generated within the configured “Notification Interval” time window will be queued up and sent all at once in a single notification.
Notification Interval	When the notification delivery method chosen is Periodic, this option will be available. The sending frequency of alert email notifications. All alert events that have occurred within a send cycle will be sent.
Super Admin Email	Configure the email addresses to send alert notifications to. Up to 10 email addresses can be added.
Admin Email	Configure the email addresses to send alert notifications to. Up to 10 email addresses can be added.
Email Template	Please refer to section [Email Templates]
SMS Notification	
Super Admin Phone Number	Send alert notifications via SMS. Multiple phone numbers are supported.
Admin Phone Number	Send alert notifications via SMS. Multiple phone numbers are supported.

SMS Template	Click on the link to access the SMS templates page.
HTTP Notification	
Protocol	Protocol used to communicate with the server. HTTP or HTTPS. Default one is HTTP.
HTTP Server	The IP address or FQDN of the HTTP/HTTPS server.
HTTP Server Port	HTTP/HTTPS port
Warning Template	Customize the template used for system warnings. By default: {"action":"\${ACTION}","mac":"\${MAC}","content":"\${WARNING_MSG}"}
Alarm Notification	Alert notification delivery method: ● Real-time: Notifications will be sent out as soon as the alerts are generated. ● Periodic: Alerts generated within the configured "Notification Interval" time window will be queued up and sent all at once in a single notification.
Notification Interval	When Alarm Notification method is set to Periodic , this option will be available. The frequency at which HTTP alert notifications are sent. All alert events that have occurred within a send cycle will be sent.
Resource Usage Notification Template	Customize the notification template to receive relevant alert information. By default: {"action":"\${ACTION}","cpu":"\${CPU_USED}","memory":"\${MEM_USED}","disk":"\${DISK_USED}","external_disk":"\${EXTERNAL_DISK_USED}"}
Notification Interval	Modifies the frequency at which notifications are sent in seconds. No notifications will be sent if the value is "0". Default value: 20
Template Variables	<code>\${MAC}</code> : MAC Address <code>\${WARNING_MSG}</code> : Warning message <code>\${STATUS}</code> : Alarm Status <code>\${TIME}</code> : Current System Time <code>\${CPU_USED}</code> : CPU Usage <code>\${MEM_USED}</code> : Memory Usage <code>\${ACTION}</code> : Message Type <code>\${DISK_USED}</code> : Local Disk Usage <code>\${EXTERNAL_DISK_USED}</code> : Disk Usage

Task Management

The Task Management feature allows users to schedule various tasks to be performed at a configured date and time. Each task can be set to run either once or repeatedly, depending on user requirements.

The tasks that can be scheduled include:

- **Paging/Intercom:** Schedule automated paging or intercom announcements at specific times.
- **Backup:** Schedule automatic backups of system data to Local or Amazon S3. Users can configure multiple backup tasks, each with its own schedule and storage location.
- **Data Sync:** Schedule synchronization of system data with remote servers to ensure data consistency.
- **Cleaner:** Schedule cleaning tasks for system data, such as CDR records, reports, IM messages, and other files, to maintain storage efficiency.
- **Detect New Firmware:** Schedule automatic checks for new firmware versions.
- **Update Country/Region:** Schedule updates for system country/region settings, which are used for Geo-IP Access Control.

- **Update Time Zone:** Schedule updates for the system time zone configuration.

Task List

In the Task List, users can schedule tasks to be performed either once or repeatedly all of the above task types can be scheduled with specific parameters.

To schedule a task, please follow the steps below:

- 1. Navigate to **Maintenance→Task Management→Task List→Pending Task**
- 2. Click on the “Add” button.

Add Task

- 3. Select the type of task from the drop-down menu.
- 4. Click *Next* and configure the required parameters for the task, such as date, time, frequency, and additional options specific to the task type.

Create New Task

The Pending Tasks section displays all tasks that have been scheduled but not yet executed. Users can review, edit, or delete tasks from this list before execution.

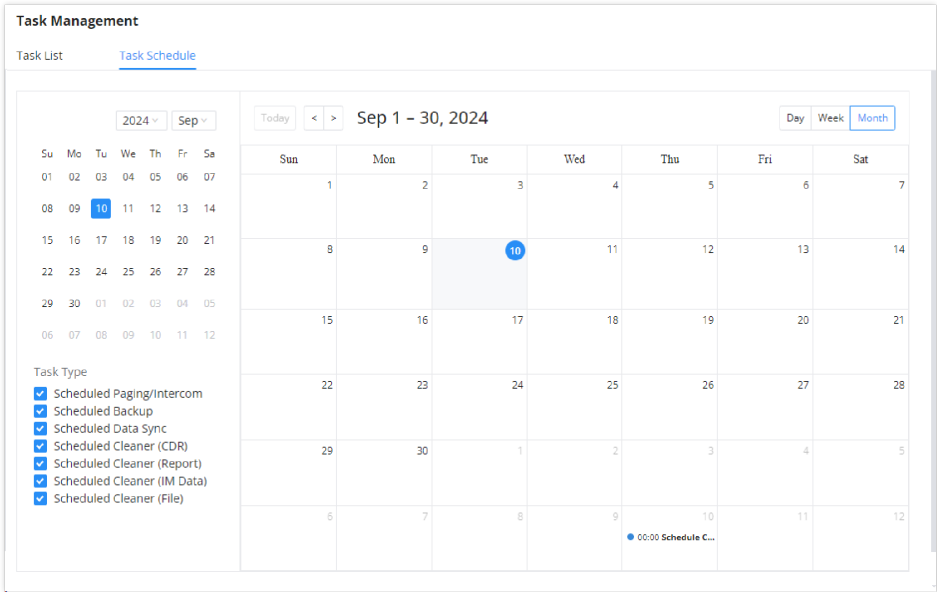
Pending Tasks

The Task History section logs all tasks that have been performed, including execution time, task type, and status. Users can use this log to verify completed tasks and troubleshoot any issues.

Task History

Task Schedule

To get an overview about all the tasks which have been scheduled, the user can click on **Task Schedule** tab to view the full schedule.

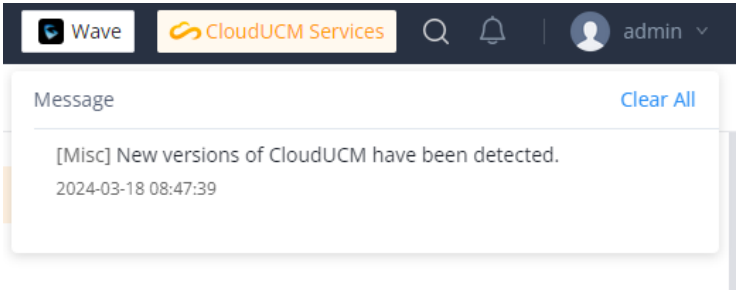


Task Schedule

Upgrade

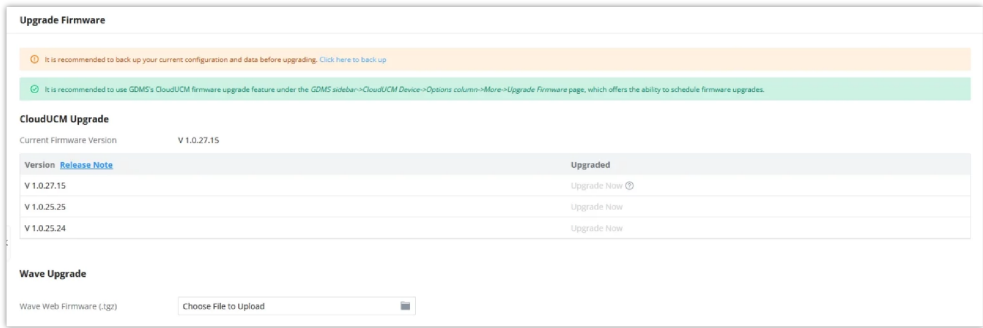
During its lifetime, the CloudUCM models will receive regular updates. These updates include new features and functionalities, bug fixes, security patches, and general improvements to the security and performance of the device. It is highly recommended that you keep the software of the CloudUCM up to date.

When a new CloudUCM software is detected, the administrator will receive a notification as shown in the screenshot below.



New CloudUCM Software Version

The administrator can either click on the notification or navigate to **Maintenance** → **Upgrade** then click on "Upgrade Now".



Upgrade Firmware

Users can easily access the release notes for the latest firmware, by simply clicking on "Release Notes". This allows them to view detailed information about the latest updates, including bug fixes, performance enhancements, new features, and any other improvements made to the firmware.

Important Note

Please note that once the CloudUCM has upgraded to a new firmware version, rolling back to a previous version would not be possible.

Backup

Backup/Restore

Users could backup the CloudUCM 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.

Backup

[Backup/Restore](#) [Data Sync](#)

i Backup files must be .tar or .tgz, named with alphanumeric characters, dashes (-) and underscores (_).

[Backup](#) [Schedule Backup](#) [Upload](#)

Scheduled Backup Task List

[Delete](#)

Task Management

[Task List](#) [Task Schedule](#)

[Add](#) [Task History](#)

Name

Schedule Amazon Backup

Schedule Backup

Schedule Cleaning

Group1

Create New Task

* Type

Scheduled Backup

[Cancel](#) [Next](#)

2. Check the *Schedule Backup* option checkbox to activate backup scheduling.
3. Enter a name for the task (*should be between 2 and 64 characters. Names can include alphanumeric characters, Chinese characters, spaces, and the special characters _ and -*).
4. Select the desired storage destination, such as Local or Amazon S3. The same location can be used for multiple tasks as long as each task is scheduled at a different time.
5. Specify the date and time for the backup. Scheduled backup times must be at least one hour apart.

Backup > Create New Schedule Backup

i SFTP server can be configured in the PBX Settings → Storage Device Management → SFTP page.

☒ Schedule Backup

* Name 2-64 character, only alphanumeric characters, Chinese characters, space and special characters _ and - are supported

* Choose Storage Location

* Date

* Time

* Repeat

Choose Backup Files

☐ All ☐ Config File ☐ IM Message ☐ IM Files ☐ CDR Records ☐ Recording Files ☐ Video Recording Files ☐ Fax Files ☐ Voicemail ☐ Voice Prompt Files ☐ Queue Statistics Report

☐ ZeroConfig Storage ☐ Meeting Report

i Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

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

Schedule New Backup

Note:

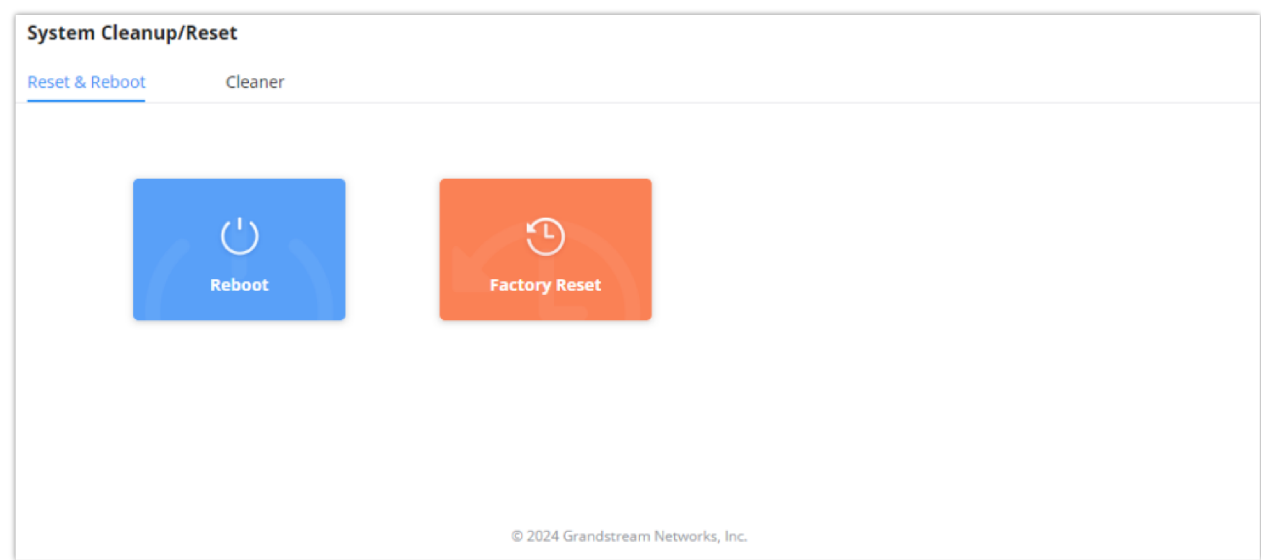
The system does not allow two backup tasks to be scheduled at the same time. If users attempt to create overlapping tasks, the configuration will be blocked because simultaneous backups can affect system performance.

6. Choose how often the backup should occur: Every Day, Weekly, Monthly, or Custom.
7. Choose which data to include in the backup. Options include: *All, Config File, IM Message, IM Files, CDR Records, Recording Files, Fax Files, Voicemail, Voice Prompt Files, Queue Statistics Report, ZeroConfig Storage, and Meeting Report.*
8. Users can view both scheduled backup tasks and completed backup tasks in the **Maintenance→Task Management** page. Within this page, the **Task List** displays all the pending and completed tasks, while the **Task Schedule** shows the timing and recurrence of upcoming backups.

System Cleanup/Reset

Reset and Reboot

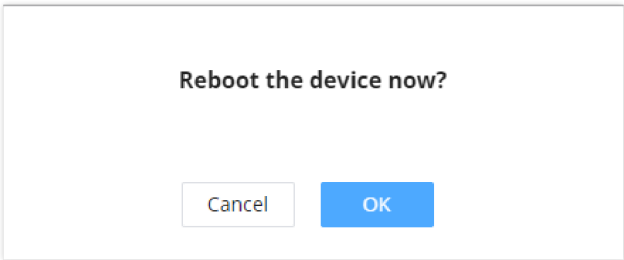
Users could perform reset and reboot under Web GUI→Maintenance→System Cleanup/Reset→Reset and Reboot.



Reset and Reboot

Reboot

When the user clicks on reboot, a confirmation prompt will appear. To proceed with rebooting the device, please click "OK".

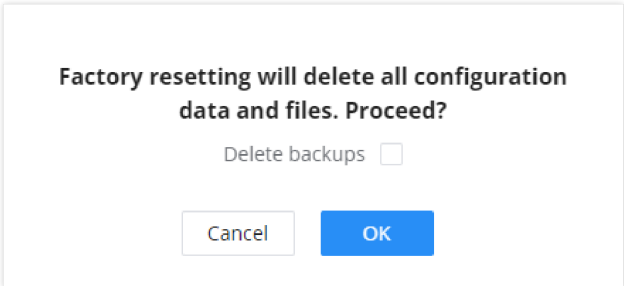


Reboot Confirmation Prompt

Reset

Reset function will delete all the configuration and data store in the CloudUCM device. After reset, the data and configuration cannot be recovered, please use this function with caution and always make sure that you have done a data and configuration backup before resetting the device to its initial configuration.

When performing a reset, the user can choose to remove the backup files. Once the user has chosen to remove the backup files, all the configuration, data, and backup files will be deleted and cannot be recovered. If you have taken a backup that you intend to restore after the reset, please do not tick the option "Delete Backups" as shown in the screenshot below.



It is highly recommended that you download all the backup files and store the files locally before resetting the device, to avoid accidental removal of the backup files..

Warning

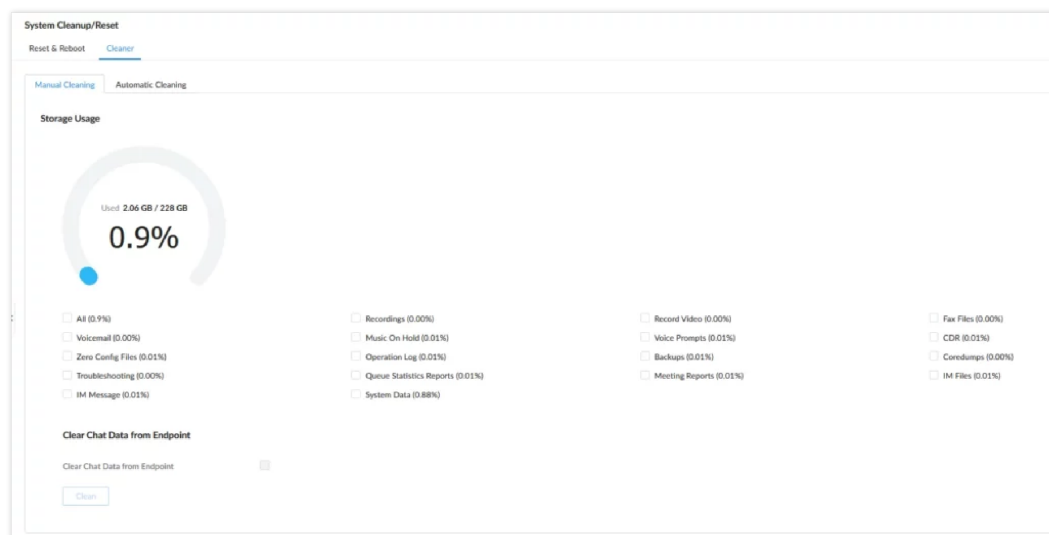
- Resetting the device will remove all the configuration and data of the device. Please proceed with caution.
- Ticking the option "Delete Backups" will result in deleting all the backup files store in the device. Please proceed with caution.

Cleaner

Users can configure the system to clean Call Detail Records (CDRs), voice recordings, voicemails, reports, chat data, meeting history, fax files, backup files, and other stored data either manually or automatically. The Cleaner feature is available under **Maintenance→System Cleanup/Reset→Cleaner**.

CloudUCM provides the ability to manually clean a variety of data types, including CDRs, report data, chat messages and shared files, recording files, meeting history records, voicemails, fax files, and backup files.

The following screenshot illustrates the settings and parameters available for configuring the Manual Cleaning feature on CloudUCM.



Manual Cleaning Tab

Automatic cleanup is not enabled by default. When configured, automatic cleanup supports scheduled deletion of file data based on parameters such as cleanup time, cleanup conditions, and cleanup intervals.

Users can configure Automatic Cleaning by navigating to **Maintenance→System Cleanup/Reset→Cleaner→Automatic Cleaning**, or by creating an automated cleaning task under **Maintenance→Task Management**.

The following screenshot shows some available parameters for configuring automatic cleanup on CloudUCM.

System Cleanup/Reset
Reset & Reboot
Cleaner

Manual Cleaning
Automatic Cleaning

Clean CDR, recordings, voicemail, fax, statistics report and IM data automatically.

CDR Cleaner

Enable Cleaner ☒

* Clean Time

Cleaning Conditions

* Clean Interval (d)

Report Cleaner

Enable Cleaner ☒

* Data Type ☐ Queue Statistics Report ☐ Meeting Call Statistics Report ☒ Multimedia Meeting History ☐ IVR Statistics Report

* Clean Time

Cleaning Conditions

* Clean Interval (d)

IM Data Cleaner

Enable Cleaner ☐

Clear Chat Data from Endpoint ☐

Automatic Cleaning Tab

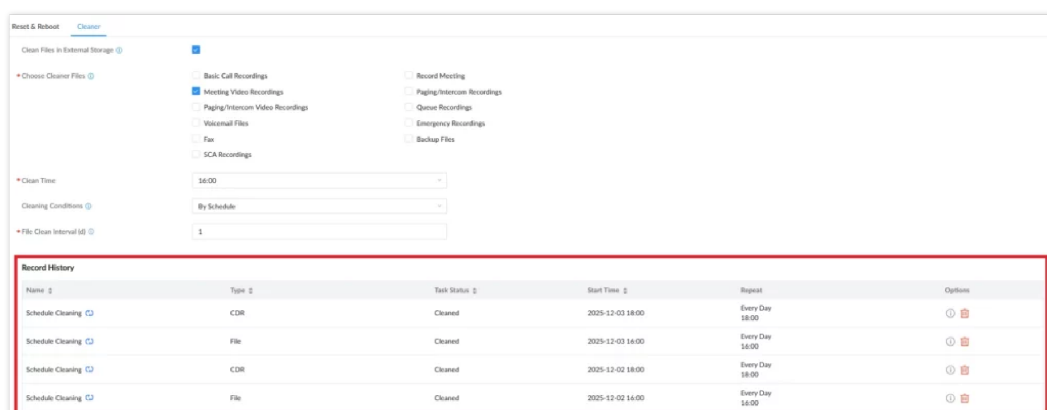
The table below describes all the configurable options that can be configured for automatic cleaning:

CDR Cleaner	
Enable Cleaner	Enable the CDR Cleaner function.
Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Cleaning Conditions	• By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated in the past 3 days. • Keep Last X Records: If the max number of CDR has been reached, CDR will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.) • Keep Last X Days: Delete all entries older than X days.
Clean Interval (d)	Enter 1-30 to specify the day of the month to clean up CDR when By Schedule is selected as Cleaning Conditions .
Max Entries	Set the maximum number of CDR entries to keep when Keep Last X Records is selected as Cleaning Conditions . Default is 50000. Valid range: 10000 – 100000.
Keep Last X Days	Enter the number of days of call log entries to keep when Keep Last X days is selected as Cleaning Conditions . Default is 30. Valid range: 1 – 100.
Report Cleaner	
Enable Cleaner	Enable scheduled queue log cleaning.
Data Type	Select a type of data to clean. • Queue Statistics Report

	● Meeting Call Statistics Report ● Meeting History ● IVR Statistics Report
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	● By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago. ● Keep Last X Records: If the max number of Queue Statistics Report entries has been reached, Queue Statistics Report entries will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.) ● Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions . The valid range is 1-30.
Max Entries	Set the maximum number of Queue Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions . Default is 50000. Valid range: 10000 – 100000.
Keep Last X Days	Enter the number of days of Queue Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions . Default is 30. Valid range: 1 – 730.
IM Data Cleaner	
Enable Cleaner	Enable IM data cleaner
Clear Chat Data from Endpoint	This option allows users to clean endpoint chat data and is only available when the selected data type includes IM messages. It is disabled by default.
Data Type	Select a type of file to clean. ● IM Files ● IM Messages
Clean time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	● By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago. ● Keep Last X Records: If the max number of Conference Call Statistics Report has been reached, Conference Call Statistics Report will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.) ● Keep Last X Days: Delete all entries older than X days.
Clean Interval	Enter how often (in days) to clean queue logs when By Schedule is selected as Cleaning Conditions. The valid range is 1-30.
Max Entries	Set the maximum number of CDR Conference Call Statistics Report entries to keep when Keep Last X Records is selected as Cleaning Conditions. Default is 50000. Valid range: 10000 – 100000.
Keep Last X Days	Enter the number of days of Conference Call Statistics Report entries to keep when Keep Last X days is selected as Cleaning Conditions. Default is 30. Valid range: 1 – 100.
File Cleaner	
Enable Cleaner	Enabling files cleaning.

Clean Files in External Device	If enabled the files in external device will be automatically cleaned up as configured.
Choose Cleaner File	Select the files for system automatic clean. ● Basic Call Recording Files ● Meeting Recording Files ● Paging/Intercom Recordings ● Call Queue Recording Files ● Voicemail Files ● Emergency Calls Recording Files ● Fax ● Backup Files ● SCA Recording Files
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	● By Schedule: If the clean interval is 3, cleaning will be performed every 3 days to delete all files. ● By Threshold: Check at the configured cleaning time every day to see if the storage threshold has been exceeded and perform cleaning of all files if it has. ● Keep Last X Days: Delete all files older than X days.
File Clean Interval	Enter 1-30 to specify the day of the month to clean up the files.
File Clean Threshold	Enter the internal storage disk usage threshold (in percent). Once this threshold is exceeded, the file cleanup will proceed as scheduled. Valid range is 0-99.
Keep Last X Days	Automatically delete all recordings older than this x days when the threshold is reached. If not set, all data is cleared. Valid range: 1 – 100.
Record History	
Name	Shows the identifier for the cleanup task.
Type	Specifies the category of cleanup the task performs
Task Status	Shows the final state of the cleanup task.
Start Time	The exact date and time when the cleanup task was triggered.
Repeat	Indicates the schedule for automatic repetition (if enabled).
Options	Provides the available actions for each task, such as <i>Info</i> and <i>Delete</i> . The <i>Delete</i> action removes the task from the record history, while the <i>Info</i> action displays details about the cleaned files.

When automatic cleaning tasks run, the system logs the cleaning results, allowing users to review each task results, including the total size cleaned and number of items removed, by checking either the **Cleaner** page or the **Task Management** sections (**Task History**).



Name	Type	Task Status	Start Time	Repeat	Options
Schedule Cleaning	CDR	Cleaned	2025-12-03 18:00	Every Day 18:00	 
Schedule Cleaning	File	Cleaned	2025-12-03 18:00	Every Day 18:00	 
Schedule Cleaning	CDR	Cleaned	2025-12-02 18:00	Every Day 18:00	 
Schedule Cleaning	File	Cleaned	2025-12-02 18:00	Every Day 18:00	 

Checking Cleaning Records from the Cleaner Page

Name	Type	Task Status	Start Time	Repeat	Options
Schedule Cleaning	File	Cleaned	2025-12-03 16:00	Every Day 16:00	
Schedule Cleaning	File	Cleaned	2025-12-02 16:00	Every Day 16:00	

Checking Cleaning Records from Task History

Network Troubleshooting

Ethernet Capture

Ethernet Capture tool allows to capture the ethernet packets from the CloudUCM to inspect them for troubleshooting purposes.

SRTP Debugging

Enabling this option allows saving SRTP keys which will be used to decrypt the SRTP packets. This is useful when troubleshooting issues related to encrypted RTP packets.

Enable TLS Key

Enabling this option allows downloading TLS key which can be used to decrypt the packets captured to be able to analyze them. The only case where this key will be required is when the transport protocol used for SIP is TLS, otherwise, this key would not be necessary. To learn how to use the TLS key to decrypt capture packets, please follow the steps below. In this example, we are using the packet analyzer Wireshark.

Important

To be able to decrypt the packets captured, they must include the TLS handshake. Otherwise, the packets cannot be decrypted.

1. Before capturing the packet trace, please tick the box "TLS Key".

Regular Debugging

☒ TLS Key Download

Ethernet Capture Start

Enable TLS Key

2. Click start, then enter a password. This password will be used to extract or access the files the archive of the packet capture.

Secret Key

Set the key to encrypt your capture file.
After the network data capture has stopped, please share the capture file with Grandstream technical support to decrypt the packet and analyze your feedback.

* Secret Key

Cancel Capture

Secret Key

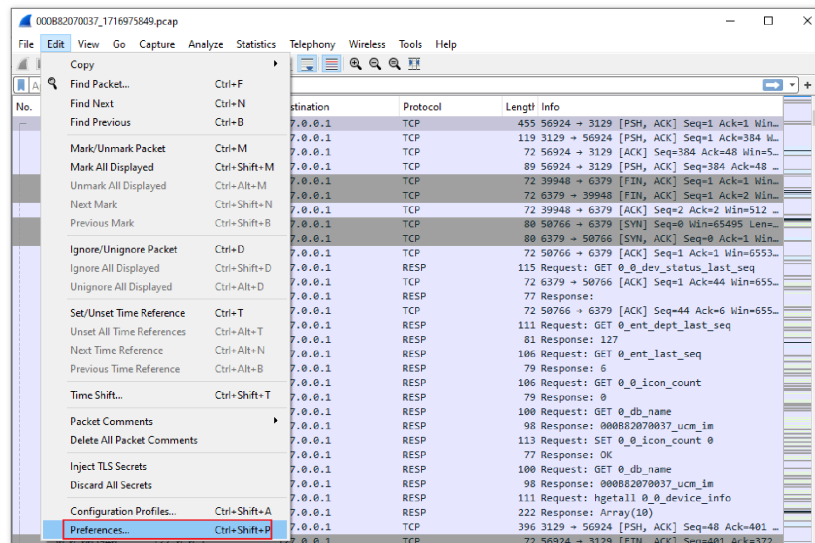
3. Start the TLS connection in the following scenario: (Prerequisites: The SIP transport is "TLS".)

1. SIP Signaling Messages for IP phones: You can disable and enable the SIP account on the IP phone, reproduce the issue such as testing calls
2. Wave App: Log out and log back into the account, reproduce the issue such as testing calls.
3. SIP Trunk: Delete the SIP trunk and configure the trunk again, reproduce the issue such as testing calls.
4. Stop capturing and download the captured trace
5. Extract the archive using an archive opener like Winrar or Winzip, then enter the password of the archive. A folder will be extracted and will contain two files: One is the captured trace, and the other one is the "sslkeylogfile.txt" file of the CloudUCM.

Name	Size	Packed	Type	Modified	CRC32
File folder					
000B82070037_1716975849.pcap *	5,057,828	5,057,840	Wireshark capture file	29-May-24 12:28	1EB22CBE
sslkeylogfile.txt *	37	49	TXT File	29-May-24 12:28	4FCBFD45

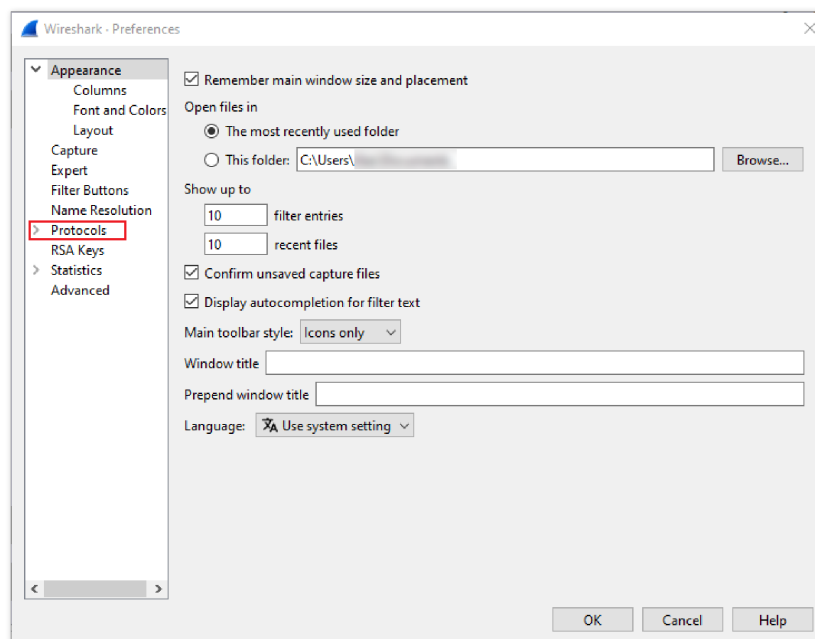
Packet Capture Archive

6. Use Wireshark to open the packet capture file, then select "Edit" Wireshark's interface. Select "Preferences"



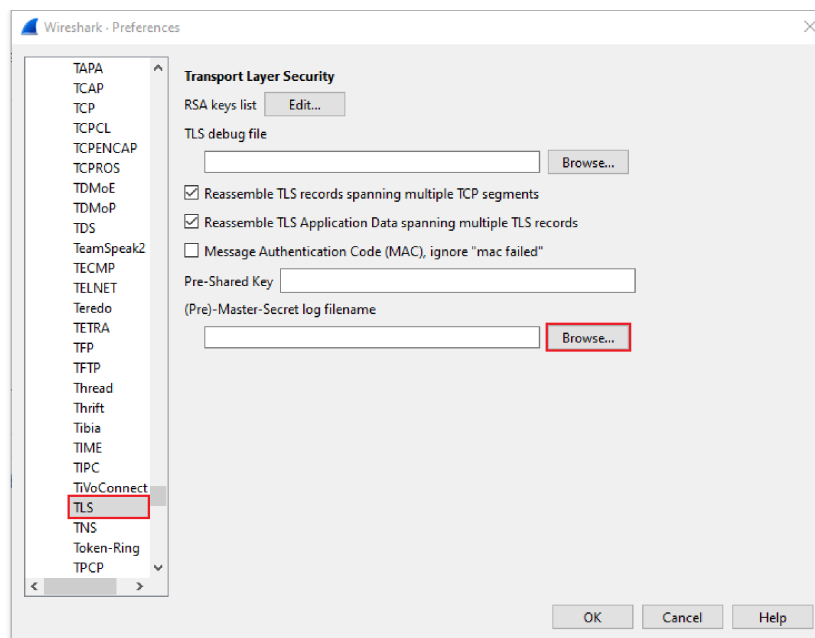
Wireshark

7. Click on "Protocols" to open the list of protocols.



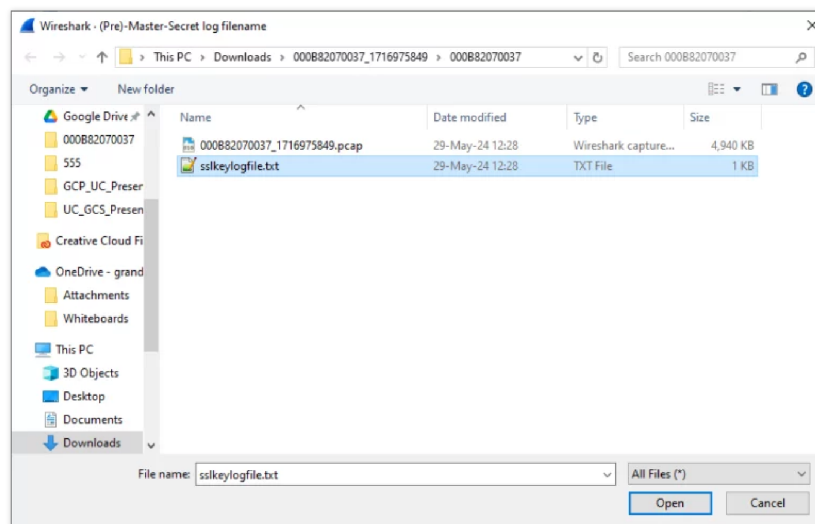
Protocols Preferences

8. From the list of protocols, please select "TLS", then click **browse** button on the "(Pre)-Master-Secret log filename", as shown in the screenshot below.



TLS Protocol Preferences

9. Navigate to the folder where the TLS key is stored then select it and click "Open", then click "OK".



TLS Key File

Then the packets can be inspected.

- **Ethernet Capture:** Starts the Ethernet capture. The user must enter a password that will be used to open the archive of the packet capture.
- **Download:** Once the capture is completed, you have the option to download the trace.

Service Check

Enable Service Check to periodically check CloudUCM service status. 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 CloudUCM. The default setting is 3. If there is no response from CloudUCM after 3 attempts (default) to check, current status will be stored and the internal service in CloudUCM will be restarted.

Service Check

Enable Server Check: ☒

* Check Cycle:

60

* Check times:

3

CDR

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

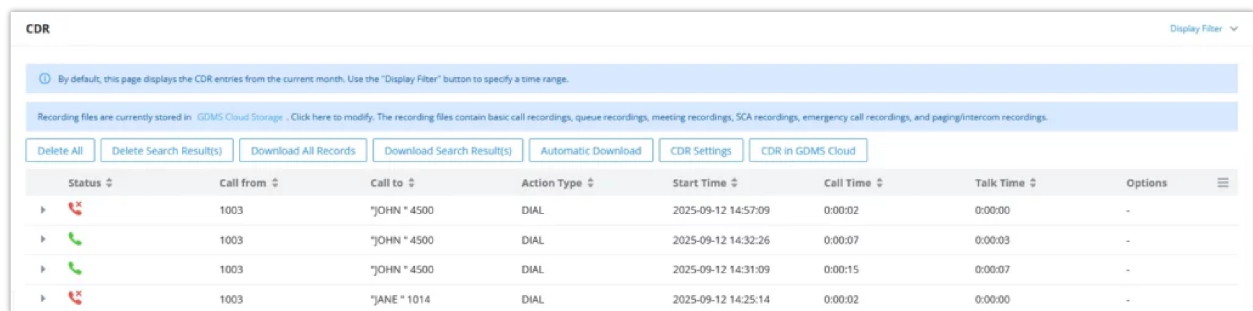
CDR Filter

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

	● Follow Me ● IVR ● Page ● Parked Call ● Queue ● Ring Group ● Transfer ● VM ● VMG ● Video Conference ● VQ_Callback ● Wakeup ● Emergency Call ● Emergency Notify ● SCA
Extension Group	Specify the Extension Group name to filter with.
Export File Data	Select the fields that will be exported, the following fields are available: ● Account Code ● Session ● Premier caller ● Action type ● Source trunk name ● Destination trunk name ● Caller number ● Caller ID ● Caller name ● Callee number ● Answer by ● Context ● Start time ● Answer time ● End time ● Call time ● Talk time ● Source channel ● Dest channel ● Call status ● Dest channel extension ● Last app ● Last data ● Ama Flags ● Unique ID ● Call type ● NAT ● Cost
Account Code	Select the account Code to filter with. If pin group CDR is enabled, the call with pin group information will be displayed as part of the CDR under Account Code Field.
Start Time	Specify the start time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
End Time	Specify the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.

Caller Number	Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out. User could specify a particular caller number or enter a pattern. ‘.’ matches zero or more characters, only appears in the end. ‘X’ matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end. For example: 3XXX: It will filter out CDR that having caller number with leading digit 3 and of 4 digits’ length. 3.: It will filter out CDR that having caller number with leading digit 3 and of any length.
Caller Name	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
Callee Number	Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out. Note: The “Callee Number” filter field supports specifying Pattern (example: 3XXX) or using Leading digits (example: 3.) as filtering options.

The call report will display as the following figure shows.



Status	Call from	Call to	Action Type	Start Time	Call Time	Talk Time	Options
Failed	1003	*JOHN * 4500	DIAL	2025-09-12 14:57:09	0:00:02	0:00:00	-
Answered	1003	*JOHN * 4500	DIAL	2025-09-12 14:32:26	0:00:07	0:00:03	-
Answered	1003	*JOHN * 4500	DIAL	2025-09-12 14:31:09	0:00:15	0:00:07	-
Failed	1003	*JANE * 1014	DIAL	2025-09-12 14:25:14	0:00:02	0:00:00	-

Call Report

The CDR report has the following data fields:

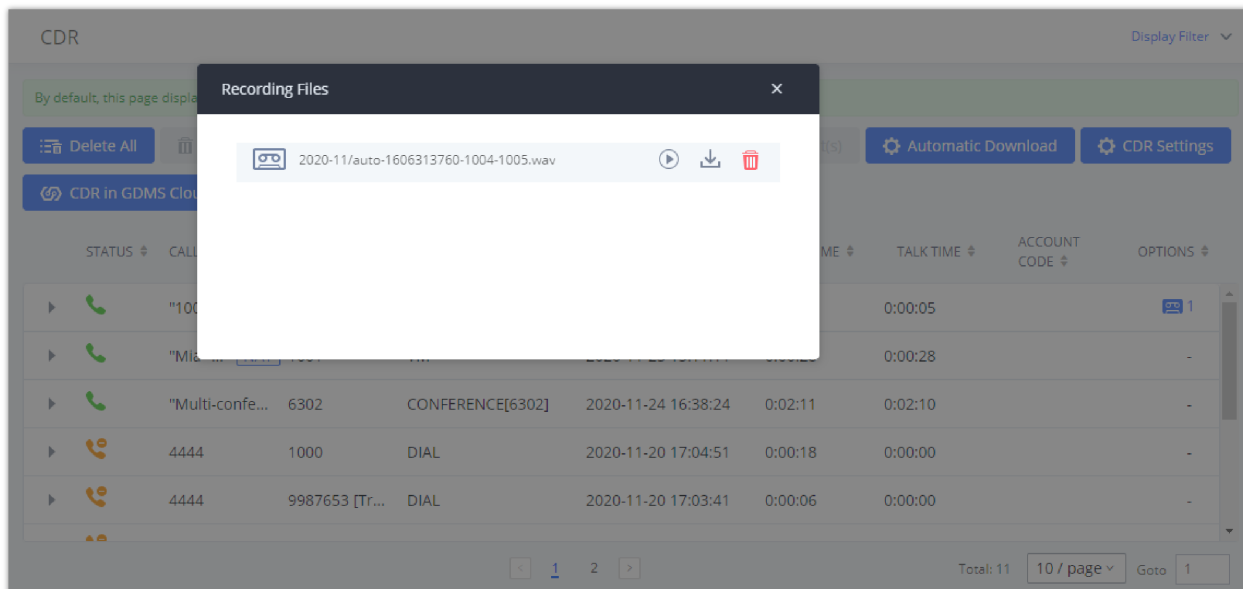
- **Start Time:** Format: 2019-12-11 09:53:03
- **Action Type:** IVR, DIAL, WAKEUP, etc...
- **Call From:** Example format: 5555
- **Call To:** Example format: "John" 1000
- **Call Time:** Format: 0:00:11
- **Talk Time:** Format: 0:00:06
- **Account Code:** Example format: Grandstream/Test
- **Status:** Answered, Busy, No answer, or Failed.
- **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 or .xlsx file.
- **Download All Records:** Click on "Download All Records" to export all the records to a .csv or .xlsx file.
- **Delete All:** Click on "Delete All" button to remove all the call report information.
- **Delete Search Result:** On the bottom of the page, click on "Delete Search Result(s)" button to remove CDR records that appear on search results.
- **Play/Download/Delete Recording File (per entry)**

Note:

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

If the entry has audio recording file for the call, the three icons on the rightest column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

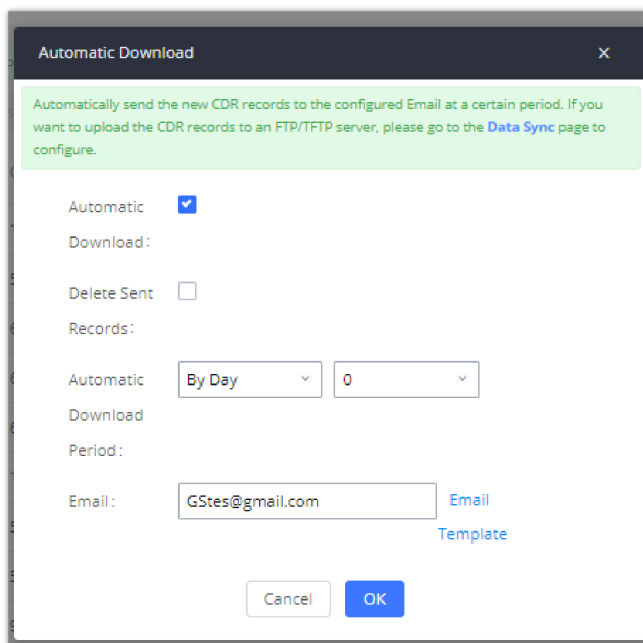
Click on  to play the recording file; click on  to download the recording file in .wav format; click on  to delete the recording file (the call record entry will not be deleted).



Call Report Entry with Audio Recording File

Automatic Download CDR Records

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



Automatic Download Settings

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

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

The user can click on the option icon for a specific call log entry to view details about this entry, such as premier caller and transferred call information.

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

CDR Report

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

Detailed CDR Information

Downloaded CDR File

The downloaded CDR (.csv/.xlsx 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.

caller number	callee number	context	calerid	source channel	dest channel	lastapp
	2009	from-internal	"Wake Up Call" <WakeUp>	Local/2009@from-internal-00000001;2	PJSIP/2009-00000013	Dial
2007	31100	from-internal	" " <2007>	PJSIP/2007-00000014	DAHDI/1-1	Dial
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial
1100	2014	from-did-direct	"1100" <1100>	DAHDI/1-1	PJSIP/2014-00000017	Dial

Downloaded CDR File Sample

Context

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.

ext-did-XXXXX: inbound calls. It starts with "ext-did", and "XXXXX" content varies case by case, which also relate to the order when the trunk is created.

ext-local: internal calls between local extensions.

Source Channel, Dest Channel

Example:

caller number	callee number	context	calerid	source channel	dest channel	lastapp
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial

Downloaded CDR File Sample Source Channel and Dest Channel 2

"SIP" means it is a SIP call. There are three format:

(a) **PJSIP/NUM-XXXXXX**, where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.

(c) **PJSIP/trunk_X/NUM**, where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.

(c) **PJSIP/trunk_X-XXXXXX**, where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

There are some other values, but these values are the application name which are used by the dialplan.

Local/@from-internal-XXXXX: it is used internally to do some special feature procedure. We can simply ignore it.

Hangup: the call is hung up from the dialplan. This indicates there are some errors or it has run into abnormal cases.

Playback: play some prompts to you, such as 183 response or run into an IVR.

ReadExten: collect numbers from user. It may occur when you input PIN codes or run into DISA

Note

The language of column titles in exported CDR reports and statistics reports will be based on the UCM's display language.

CDR Export Customization

Users can select the data they want to see in exported CDR reports by first clicking on the *Filter* button on the CDR page under **CDR > CDR** and selecting the desired information in the *Export File Data* field.

The screenshot displays the CDR Export customization interface. It includes several filter fields: 'End Time' with a date picker, 'Caller Name', 'Account Code', and 'Destination Trunk Name'. Below these are checkboxes for 'Outbound Calls', 'Internal Calls', 'No Answer', and 'Busy'. A green banner提示用户使用“Filter”按钮指定时间范围。 At the bottom, there are buttons for 'All Records' and 'Download Search Result (s)'. The 'Export File Data' field is open, showing a dropdown menu with the following options: ACCOUNT CODE, SESSION, ACTION OWNER, ACTION TYPE, SOURCE TRUNK NAME, DEST TRUNK NAME, CALLER NUMBER, and CALLERID. The background shows a table with columns: type, Start Time, Call Time, Talk Time, Account Code, and Recording File.

CDR Export File data

Call Rate

In Call Rate, the user can set call billing for outbound calls. The user can choose to include the call rate configured in **Carrier** or configure rates for calls which are identified through a prefix.

Note

If *Using Carrier Call Rates* has not been enabled, CloudUCM will fall back to the **Other Call Rates** table.

Call Rate

Carrier Call Rates

Using Carrier Call Rates

Carrier

When enabled, the outgoing trunk carrier rate table will be used for call cost calculation if available. Otherwise, the general rates will be used.

Cancel

Save

Q Name/Match Prefix/Rate

Name	Match Prefix	Starting Cost	Starting Time (seconds)	Rate	Billing Unit (sec)	Valid Time	Options
No data							

Other Call Rates

The system matches rates based on the prefix of the caller's number. After matching, the rates in the table below will be used to calculate the cost of the call. When more than one rate can be matched, the rate with the highest priority will be used.

Add Rate

Delete Selected Rate

Import

Export v

Q Name/Match Prefix/Rate

Priority	Status	Name	Match Prefix	Starting Cost	Starting Time (seconds)	Rate	Billing Unit (sec)	Valid Time	Options	
☐	1	Available	RateA	+212	3	30	0.1	60	2025-06-01 00:00:00~2025-07-31 11:27:57	
☐	2	Available	PMS-9	9			0.5	60	2025-06-24 15:07:21~2099-12-31 23:59:59	
☐	3	Available	RateB	+213	0.2	60	0.1	60	2025-06-01 00:00:00~2025-07-31 11:29:15	
☐	4	Available	RateD	+21	10	30	0.1	60	2025-06-01 00:00:00~2025-07-31 14:40:28	

Call Rate

To add specific rates, click on "Add Rate".

Call Rate > Add Other Call Rates

Call Charge = Starting Cost + Rate x Number of Billing Units Exceeding Start Time

* Name

Match Prefix

Starting Cost

Starting Time (seconds)

* Rate

* Billing Unit (sec)

60

Start Time

Date

Time

End Time

Date

Time

Disable the rate

☐

Cancel

Save

Adding a New Call Rate

The following table describes the configuration parameters for call rates:

Parameter	Description
Name	Enter the name of the call rate.
Match Prefix	Enter the matching prefix of the outgoing number dialed to match the corresponding rate. The prefix entered must match the outgoing mode of the outgoing route. Leave this field blank if you want to calculate every call using this rate. The matching will be done before any digit stripping or prepending is done.
Starting Cost	Configure the starting flat fee to charge for calls. If the length of the external call does not exceed the start time, only this fee will be charged.

Starting Time (seconds)	Sets the starting time period for call billing. If the length of an external call does not exceed the starting time, only the starting cost amount will be charged. ● Example 1: If the starting cost is set to 0.2, and the starting time is set to 60, the first 60 seconds of a call will be charged a flat amount of 0.20 dollars (or other currency). If the starting cost is set to 0 instead, the first 60 seconds will be free. ● Example 2: If the starting cost is set to 0.2 and the starting time is set to 0, the call billing will start upon dialing with an initial cost of 0.2 currency unit. ● Example 3: If the starting cost is set to 0 and the billing time is set to 0, the billing will start upon dialing with no initial cost.
Rate	Sets the billing rate of a call after the starting time period has ended. This is used with Billing Unit (sec) to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time).
Billing Unit (sec)	Sets the billing unit used after the starting time period has ended. This is used with Rate to calculate the cost of a call (Call Charge = Starting Cost + Rate x Amount of Time Exceeding Start Time). Partial units are rounded up (e.g., If the billing unit is set to 60 seconds, and the call lasted 90 seconds (1.5 units), the guest will be billed for 120 seconds (2 units)).
Start Time	Define the starting time. After this time, this rate will be applied.
End Time	Define the end time. After this time, this rate will not be applied.
Disable the rate	Ticking this box will disable this rate. Unticking this box means that this rate will apply.

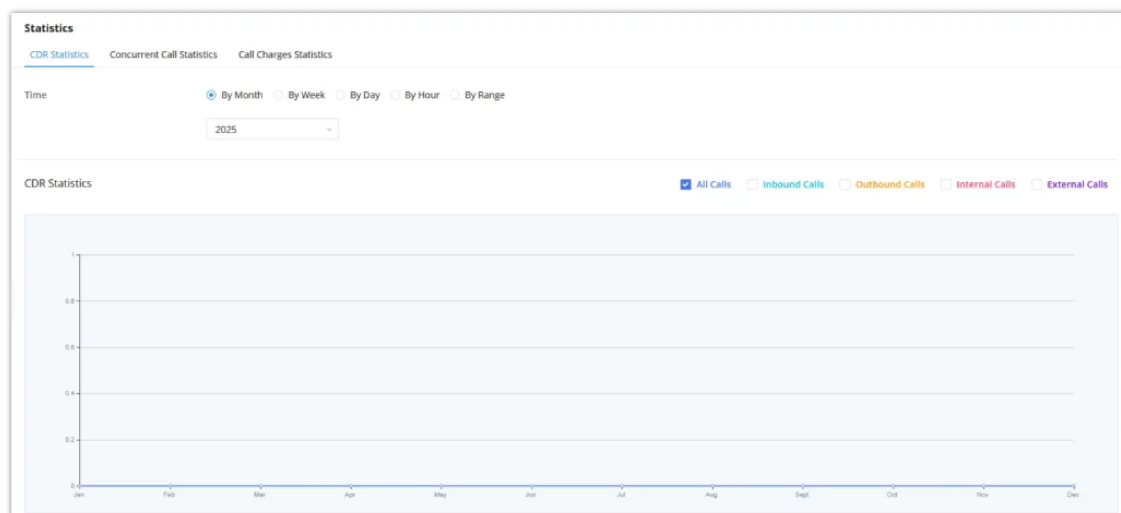
Note:

For more information on the CloudUCM built-in billing feature, please refer to the [Grandstream Billing System Guide](#).

Statistics

CDR Statistics

CloudUCM supports CDR (Call Detail Record) statistics. This function provides users with detailed reports and analytics on call activity across all VoIP trunks. Users can set custom search criteria, such as date ranges, to generate tailored charts and reports.



CDR Statistics

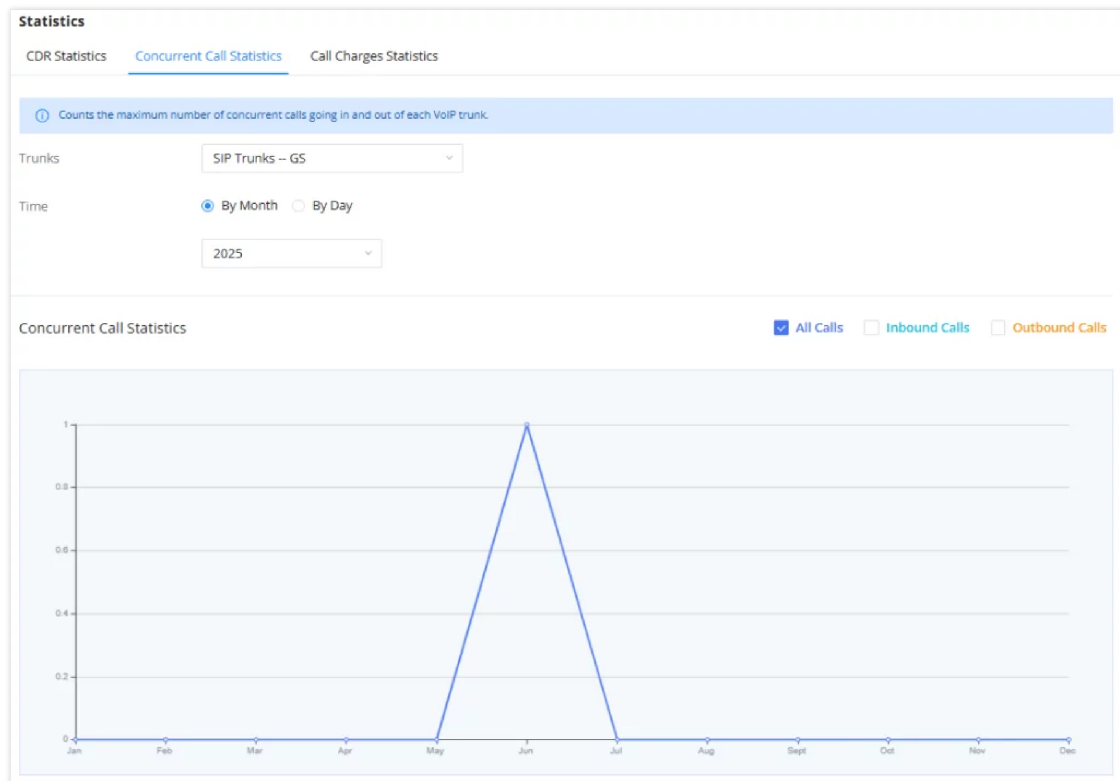
The table below describes the filtering options available for CDR statistics:

Time Range	Select the time period to use for filtering ● By month (of the selected year) ● By week (of the selected year) ● By day (of the specified month for the year) ● By hour (of the specified date) ● By range. Example: 2016-01 to 2016-03
-------------------	--

Call Type	Select one or more in the following checkboxes. ● All Calls ● Inbound Calls ● Outbound Calls ● Internal Calls ● External Calls
------------------	---

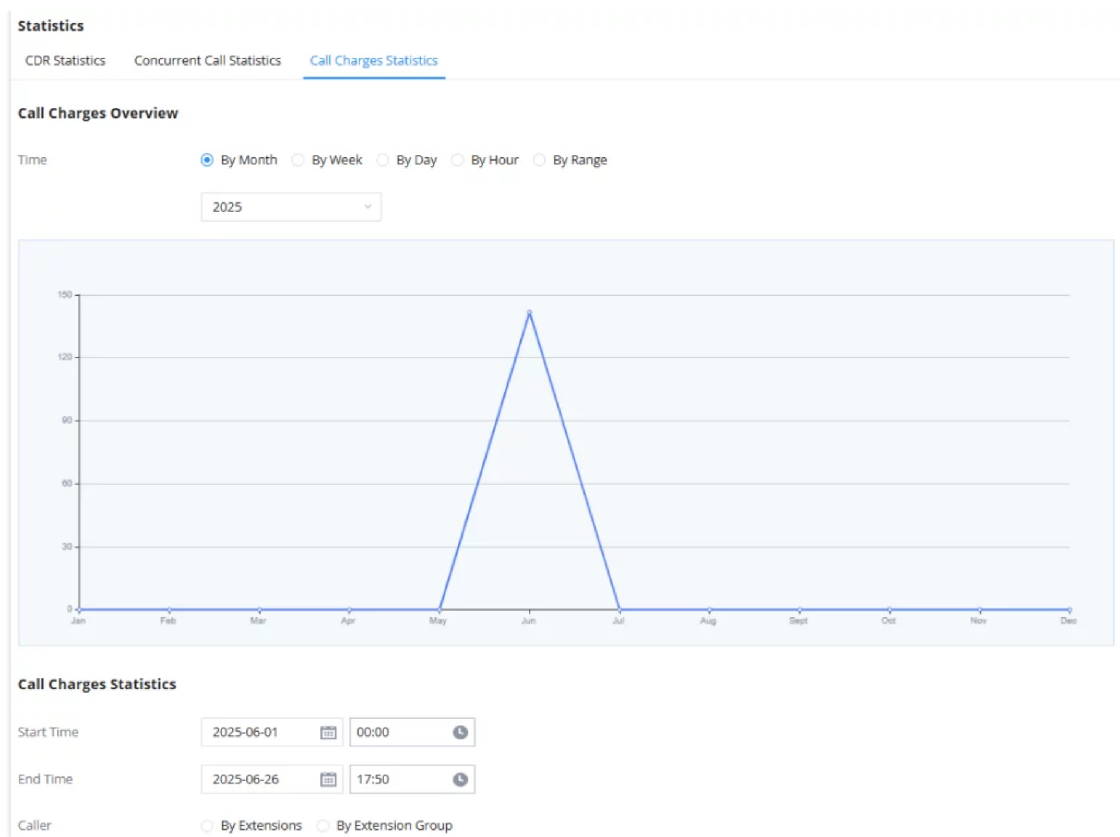
Concurrent Call Statistics

In this tab, the administrator can view the statistics regarding the concurrent calls. The administrator can choose to view the statistics per day, month, and year. The user can also view all calls, inbound calls, or outbound calls; or a combination of all of them together.



Call Charges Statistics

In the Call Charges Statistics tab, the administrator can view the charges applied to the calls represented in a graph. The administrator can search by time interval, and they can also filter by extension, extension group, or department. Once the administrator sets the intended parameters in the filter, they can display and download the filtered statistics.



Call Reports

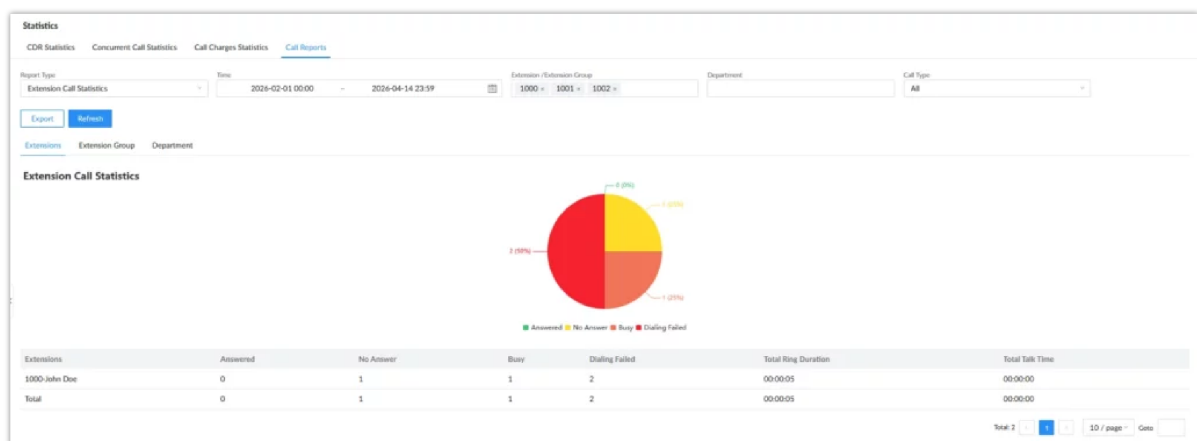
The Call Reports section provides analytics based on different operations within the PBX. These reports allow administrators to analyze how calls are distributed, handled, and processed across extensions, trunks, and system components.

Extension Call Statistics

This report displays insights into call volume associated with selected:

- Extensions
- Extension groups
- Departments

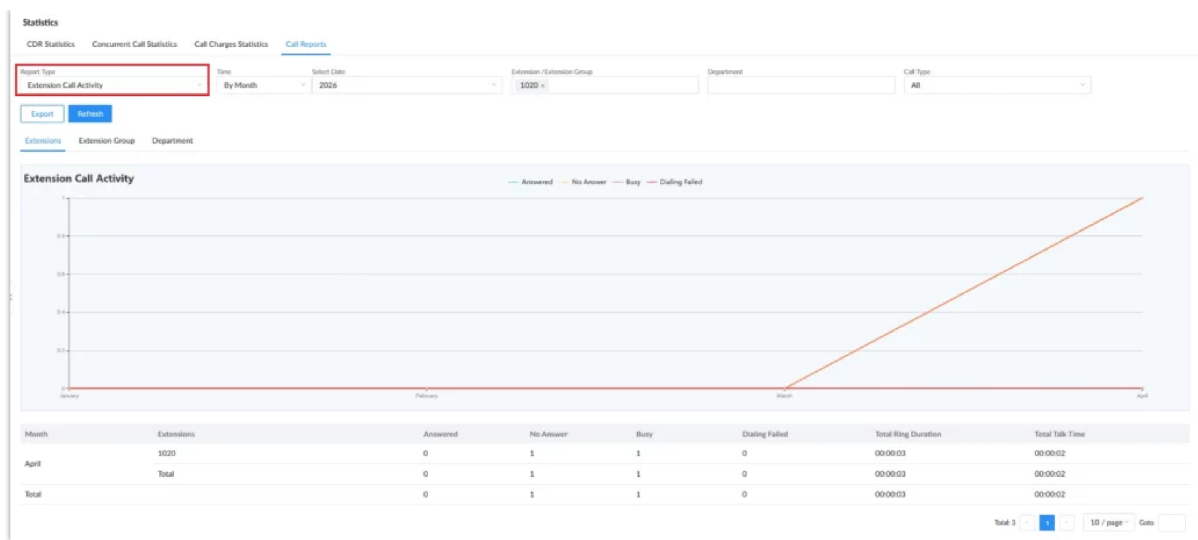
Administrators can filter by time period and call type (inbound, outbound, internal, etc.) to analyze how traffic is distributed across users or organizational units.



Extension Call Statistics

Extension Call Activity

This report focuses on how calls and selected call types were handled by the specified extensions/extension groups/departments over the specified time periods.

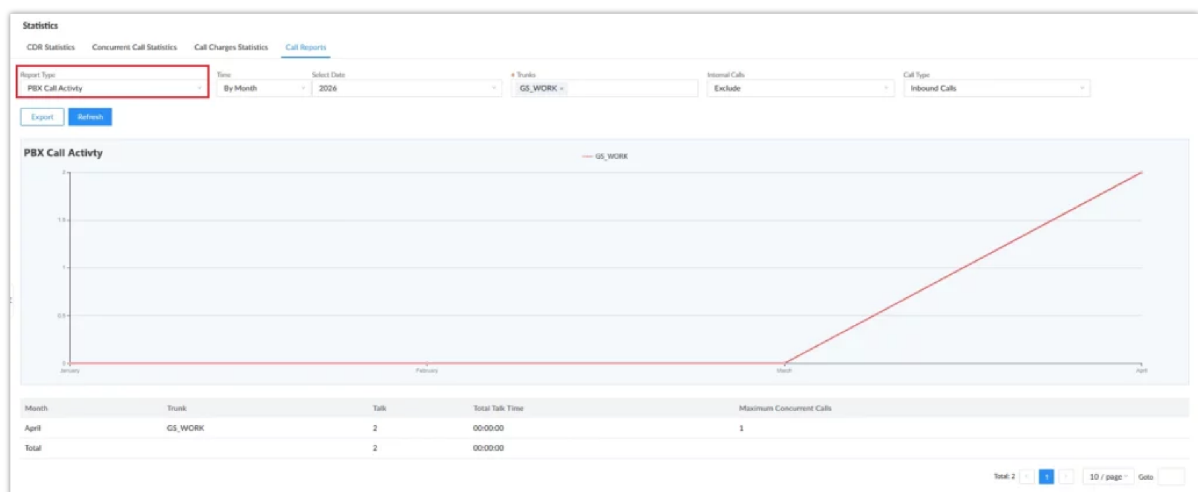


Extension Call Activity

PBX Call Activity

This report provides a system-wide view of call activity across selected trunks, which include or exclude internal calls (extension-to-extension) and can be filtered by call direction.

This enables comparison between internal PBX traffic and external trunk usage, helping identify overall system load distribution and trunk utilization patterns.



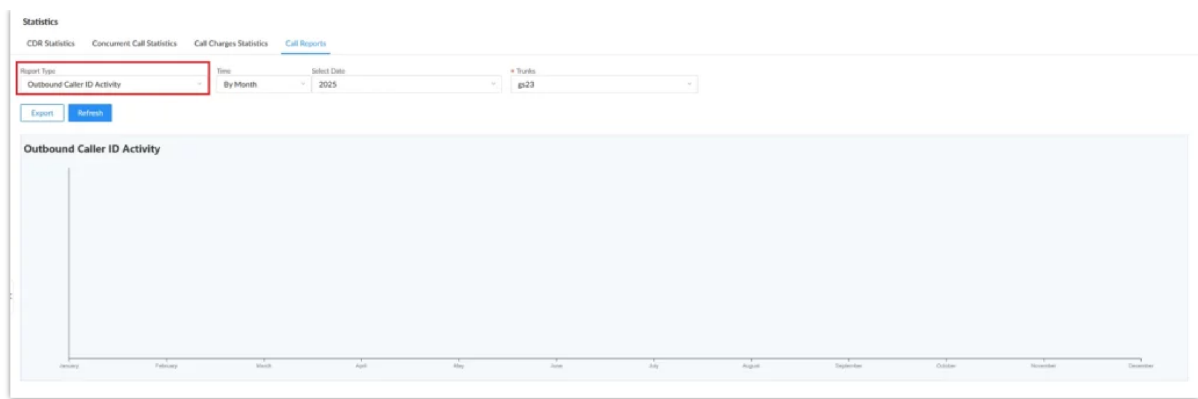
PBX Call Activity

Outbound Caller ID Activity

This report provides visibility into outbound call usage based on the selected trunk and caller ID configuration.

It displays how outbound calls are distributed across:

- Trunks
- Caller IDs



Outbound Caller ID Activity

IVR Report

This option provides analysis of IVR interactions over a selected time period and supports two reporting modes:

- **Standard Mode:** Captures key press events (0–9, *, #), including invalid inputs and timeout events, providing detailed per-key interaction statistics.
- **Custom Mode:** Supports multi-digit or combined key inputs. Reports aggregate IVR activity, including total call entries, invalid inputs, and timeouts.

Statistics

CDR StatisticsConcurrent Call StatisticsCall Charges StatisticsCall Reports

Report Type
IVR Report

Time
2026-03-01 00:00:00 - 2026-05-08 23:59:59

Type
Standard

IVR
7000-70001

Export

Refresh

IVR	Press 0	Press 1	Press 2	Press 3	Press 4	Press 5	Press 6	Press 7	Press 8	Press 9	Press #	Press *	Response Timeout	Invalid Input	Destination	Details
7000	1	3	1	9	1	1	1	1	1	2	0	1	1095	6		

Total: 1

<

1

>

10 / page

Goto

Standard IVR Report

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Report Type

IVR Report

Time

2026-03-01 00:00:00 ~ 2026-05-08 23:59:59

Type

Custom

IVR

7000-70001

Export

Refresh

Key	Count	Details
Overall IVR	1115	i
Response Timeout	1095	i
Invalid Input Destination	6	i
1	1	i
3	6	i
9	1	i
911	3	i
9911	3	i

Total: 8

<

1

>

10 / page

Goto

Custom IVR Report

The report can be exported in two formats:

- **Basic List:** Lists all IVRs and the trigger counts of their key press events.
- **Detailed List:** Includes the caller information, triggered key press events, the time of the events, and how long the callers were in the IVRs. In addition to the information in the Basic report

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Report Type

IVR Report

Time

2026-04-14 00:00

2026-04-14 23:59

Export

Refresh

Export (Basic List)

Export (Detailed List)

Press 1

Press 2

Press 3

Press 4

Press 5

Press 6

IVR Report Export Types

Ring Group Statistics

This report provides performance metrics for ring groups, including total calls received, answered calls, and answer rate.

It enables evaluation of call distribution efficiency and group responsiveness across configured ring groups.

Statistics

CDR Statistics

Concurrent Call Statistics

Call Charges Statistics

Call Reports

Report Type

Ring Group Statistics

Time

2026-04-14 00:00

2026-04-14 23:59

Export

Refresh

Ring Groups

Answered

Received

Answered Rate

6400

0

1

0.00%

6401

1

1

100.00%

Total

1

2

50.00%

Ring Group Statistics

Recordings

This page lists all the audio/video recording files recorded by "Auto Record" per extension/ring group/call queue/trunk, or via feature code "Start/Stop Call Recording".

Recordings

Recording Files

Video Recording Files

Download

Download All

Delete

Delete Search Results

Basic Call Recordin...

2025-09

Display Filter

Caller

Callee

Call Time

Size

Play

Options

No data

CDR Recording Files

The list of recording files is:

- Basic Call Recordings.
- Queue Recordings.
- Record Recordings.
- SCA Recordings.
- Emergency Recordings.
- Paging/Intercom Recordings

On this page, users can search for and select specific recordings to delete, download individual files, or perform batch download and deletion operations.

Users can sort the recording files based on "Caller", "Callee", or "Call Time" for the corresponding column. Click on the title to switch the sorting mode between ascending order and descending order.

CLOUDUCM SERVICES

Plan

In this tab, the user can view information about the plan of the CloudUCM and all the related settings.

Service Description

In this section, the user can view all the services related to the CloudUCM plan.

CloudUCM Services

[Plan](#) [Integrated Customer Service](#) [Enterprise UI Customization](#) [Statistics](#)

[Service Description](#) [My Plan](#) [Plan Settings](#)

Current Plan: SOHO (Trial) 

[Renewal/Upgrade](#) [Learn about CloudUCM](#)

CloudUCM is a cloud audio/video communications and collaboration solution with a rich and powerful suite of features such as audio/video calling, conferencing, Live Chat online customer service, and more. Experience official integrations with software such as CRMs, Whatsapp, Office365, etc., or create custom add-ins with Wave API and SDK to suit your own business needs.



Communicate Across The World

CloudUCM is a comprehensive cloud UC solution that any endpoint can seamlessly connect to regardless of physical location or network. Enjoy features like audio/video calling, conferencing, call centers, instant messaging, Live Chat online customer service and more!

[How to configure endpoints](#) [Notify Employees to Use](#)



Wave — Communicate & Collaborate From Anywhere

Available on desktop, web, Android and iOS, Wave gives your team the power to communicate and collaborate from anywhere and anytime on any device. Whether they're in the office, travelling or working from home, Wave provides easy access to voice and video calling, meetings, instant messaging and more.

[Learn more](#) [How to Use Wave](#) [Notify Employees to Use](#)

My Plan

In the “My Plan” tab, the user can view information related to the CloudUCM plan, such as plan name, plan expiration date, plan status, extensions, max concurrent calls, storage space, and admin portal. In addition to the SIP server address.

CloudUCM Services

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

Service Description

My Plan

Plan Settings

Plan Name

SOHO

Plan Expiration Date

5/7/2024

Plan Status

Trial

Extensions

5 / 20

Max Concurrent Calls

8

Storage Space

107.21 MB / 1.00 GB

Cleaner

Admin Portal

https://myucm.cloud:8443

For improved security, it is recommended to prevent direct link access to Cloud UCM by going to GDMS and enabling "Only allow access via GDMS".

SIP Server

myucm.cloud

SIP Server

myucm.cloud:5061

Wave 3rd Party Add-ins

Supported

Record

Supported

Bound Enterprise: Grandstream Networks, Inc.

Service Site: EU

Organization: Default

Plan Settings

In the “Plan Settings” tab, the user can configure SIP extension synchronization between the CloudUCM and the GDMS platform. The user can also set alert events synchronization, configure remote login settings, and passwordless remote access.

CloudUCM Services

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

Service Description

My Plan

Plan Settings

Bound Enterprise: Grandstream Networks, Inc.

Service Site: EU

Organization: Default

General

SIP Extension Sync

Alert Events Sync

Remote Login Settings

Go to Page

Passwordless Remote Access

Enable Passwordless Remote Access

AI Services

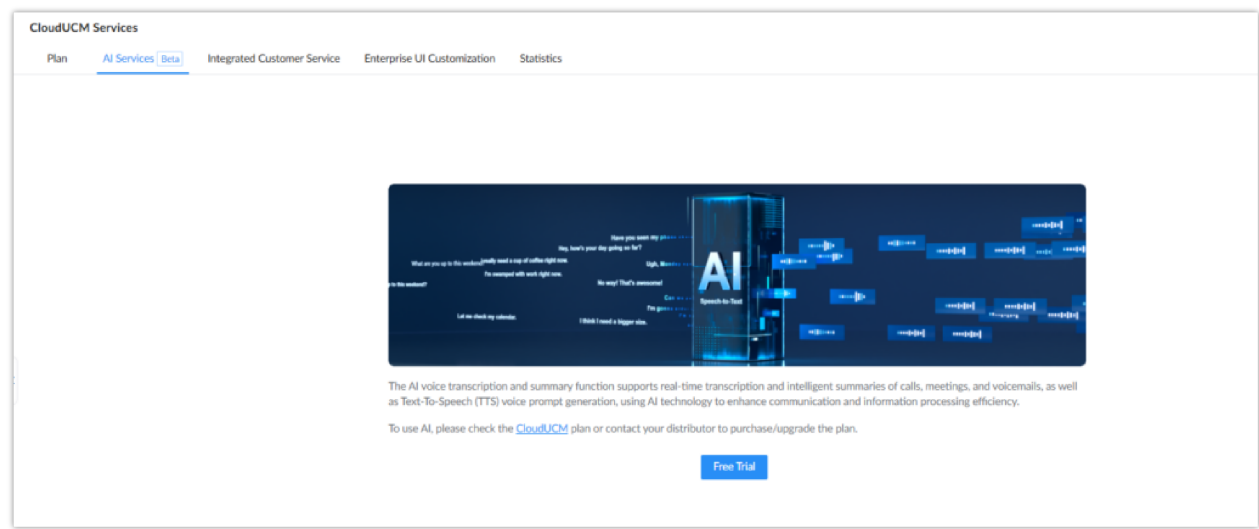
This section displays AI related service status and usage information for the CloudUCM. It provides visibility into the active AI plan, its validity period, and detailed usage statistics. Users can also jump to configure AI Settings from this page.

Supported AI features include:

- AI Voice Message to Text
- AI Generated Speech (Text-to-Speech)

- AI Call Transcription and Summary
- AI Conference Transcription and Summary

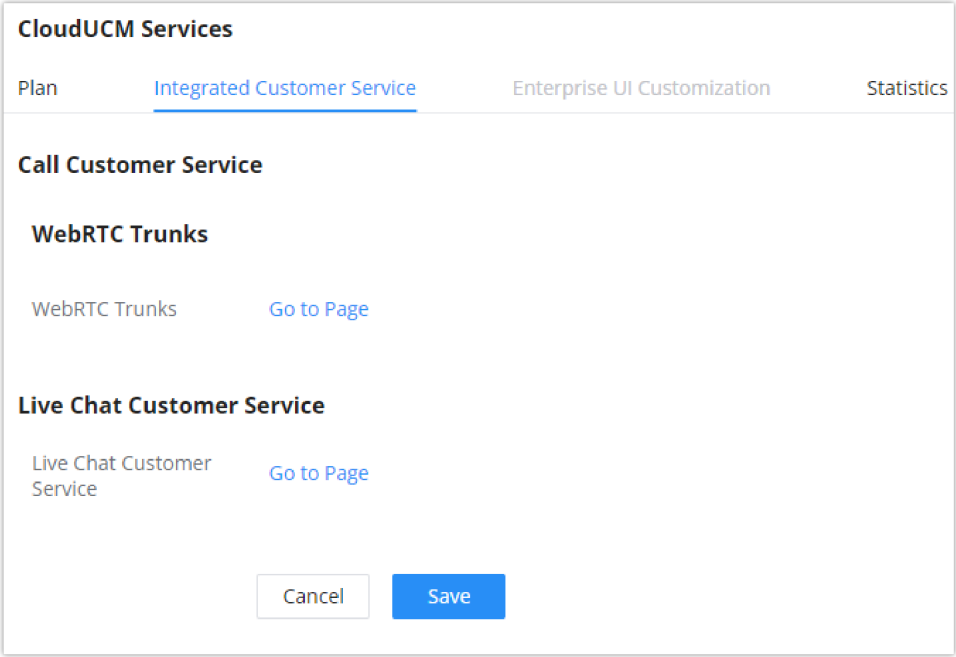
Usage statistics show monthly consumption per feature and total usage versus the available quota, helping administrators monitor AI resource usage.



RemoteConnect AI Services Page

Integrated Customer Service

In "Integrated Customer Service", the user can access the sections for WebRTC Trunks configuration and Live Chat Customer Service.



Enterprise UI Customization

On the **RemoteConnect > Enterprise 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 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.

CloudUCM Services

PlanIntegrated Customer ServiceEnterprise UI CustomizationStatistics

Company Name

Grandstream

Logo

It is recommended to not use blue, black, and white for the logo color.

Logo 1 80x80px

Logo

Upload

Logo 2 256x64px

Logo

Upload

Logo 3 64x64px (.ico)

Logo

Upload

Cancel

Save

Logo1 Preview: UCM

CloudUCM UI Customization

PlanIntegrated Customer ServiceEnterprise UI CustomizationStatistics

Company Name

CompanyABC

Logo

It is recommended to not use blue, black, and white for the logo color.

Logo 1 80x80px

Logo

Upload

Logo 2 256x64px

Logo

Upload

Logo 3 64x64px (.ico)

Logo

Upload

Cancel

Save

Logo1 Preview: Login

Wave UI Customization

PlanIntegrated Customer ServiceEnterprise UI CustomizationStatistics

Company Name

CompanyABC

Logo

It is recommended to not use blue, black, and white for the logo color.

Logo 1 80x80px

Logo

Upload

Logo 2 256x64px

Logo

Upload

Logo 3 64x64px (.ico)

Logo

Upload

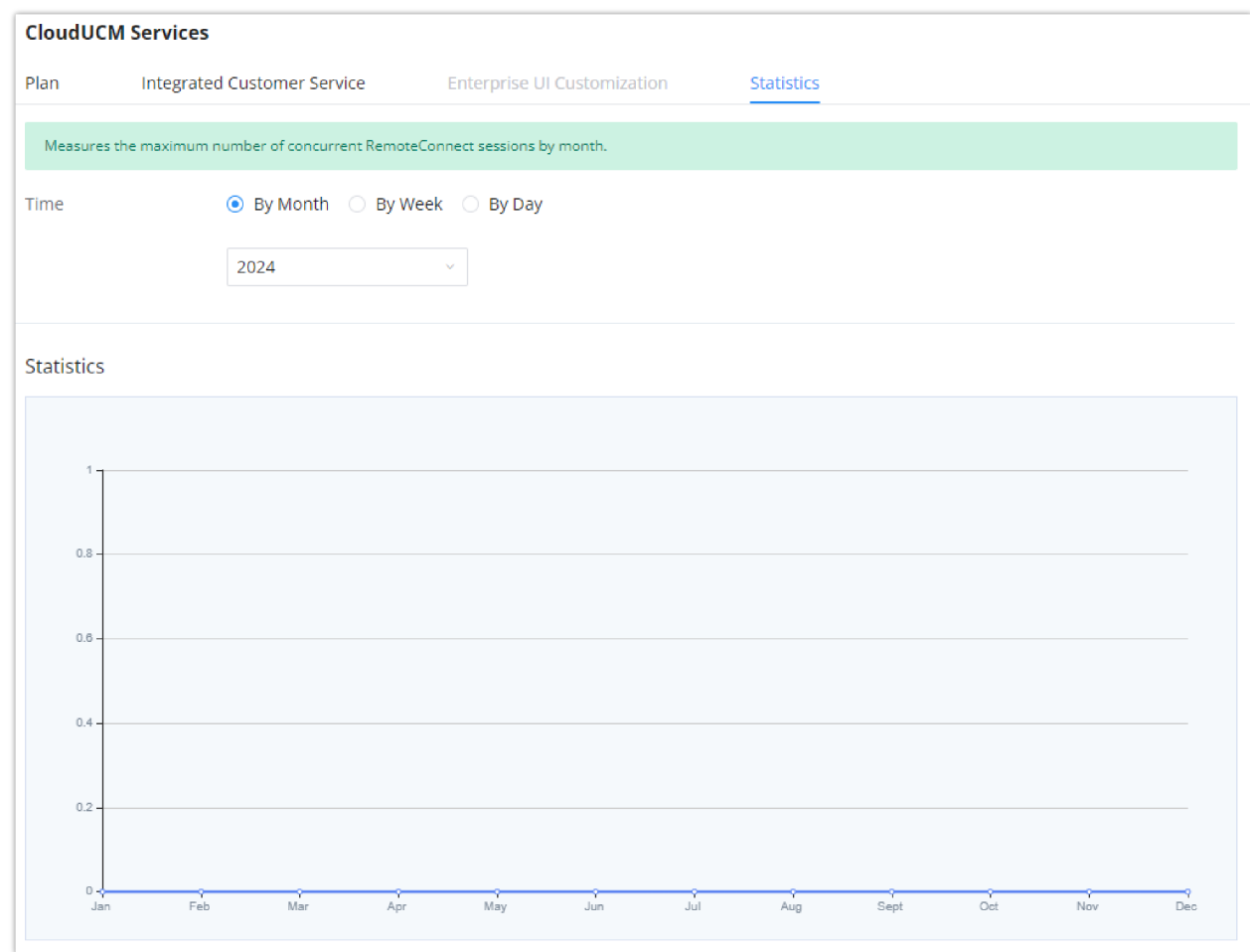
Cancel

Save

Logo2 Preview: Email Template

Email Customization

Statistics



Statistics

Month	Maximum Concurrent RemoteConnect Sessions
Jan	0.0
Feb	0.0
Mar	0.0
Apr	0.0
May	0.0
Jun	0.0
Jul	0.0
Aug	0.0
Sept	0.0
Oct	0.0
Nov	0.0
Dec	0.0

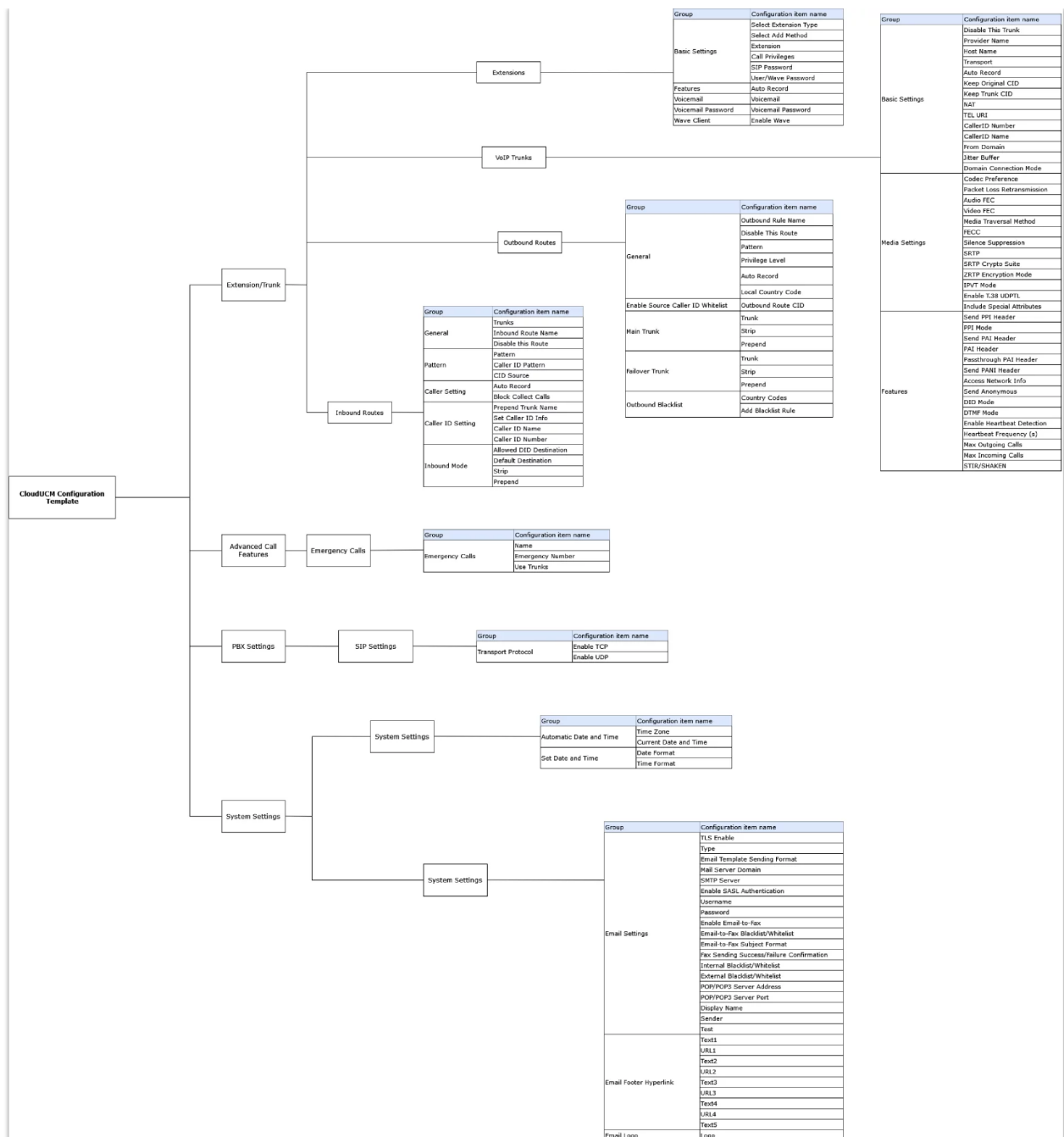
PROVISIONING

CloudUCM supports configuration provisioning via GDMS, enabling users to configure a single CloudUCM instance or perform batch configurations using predefined templates to ensure consistency and increase efficiency.

This section describes in detail how CloudUCM leverages GDMS to facilitate efficient configuration provisioning for both individual devices and large-scale deployments.

Configuration Parameters

To give users a better understanding of the configuration possibilities, the following diagram outlines the key configuration parameters available in CloudUCM through GDMS.



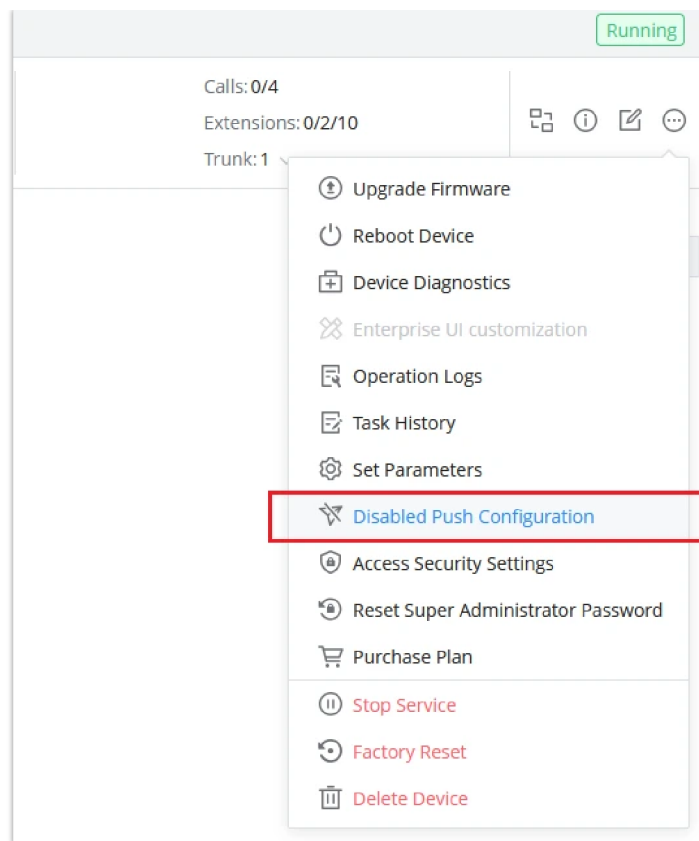
CloudUCM Configuration Template Parameters

Creating CloudUCM Configuration Templates

CloudUCM supports provisioning using two types of templates:

Model Template

After adding a CloudUCM model template, the configuration will be pushed to the selected site automatically, except for CloudUCM instances where push configuration has been disabled. (See image below)



Disable CloudUCM Push Configuration

To add a CloudUCM Model template, please follow these steps:

1. Go to **Organization** → **Device Template** → **By Model** and click on

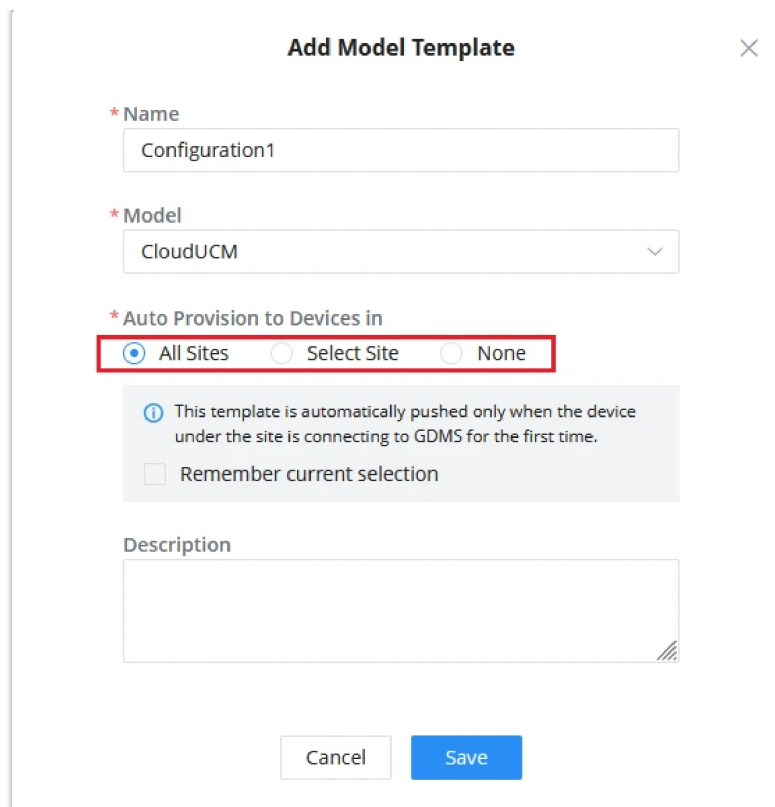
[+ Add Model Template](#)

2. Enter a name for this template and select CloudUCM from the Model list.

 A screenshot of the 'Add Model Template' dialog box. It has a title bar with 'Add Model Template' and a close button (X). Inside, there are two main fields: '* Name' with a text input containing 'Configuration1', and '* Model' with a dropdown menu. The dropdown menu is open, showing a list of models: 'WP810', 'WP816', 'WP820', 'WP822', 'WP825', 'WP826', 'WP836', and 'CloudUCM'. The 'CloudUCM' option is highlighted with a red rectangular box. At the bottom of the dialog, there are 'Cancel' and 'Save' buttons.

Adding New CloudUCM Model Template

3. Choose whether to automatically push this template to a specific site, all sites, or none. Users can also add a description for this template (optional).



Add Model Template

* Name
Configuration1

* Model
CloudUCM

* Auto Provision to Devices in
☒ All Sites ☐ Select Site ☐ None

Info: This template is automatically pushed only when the device under the site is connecting to GDMS for the first time.

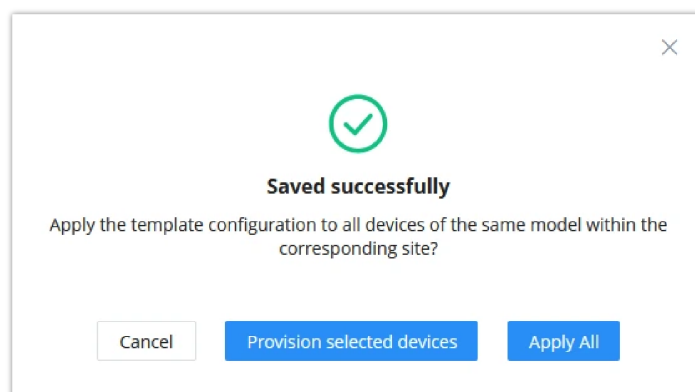
☐ Remember current selection

Description

Cancel Save

CloudUCM Auto Provisioning Sites

- Configure the model template parameters and click **Save**. A prompt will appear, confirming the change and offering the option to push the configuration to the entire site or to specific devices.



Saved successfully

Apply the template configuration to all devices of the same model within the corresponding site?

Cancel Provision selected devices Apply All

Success Prompt

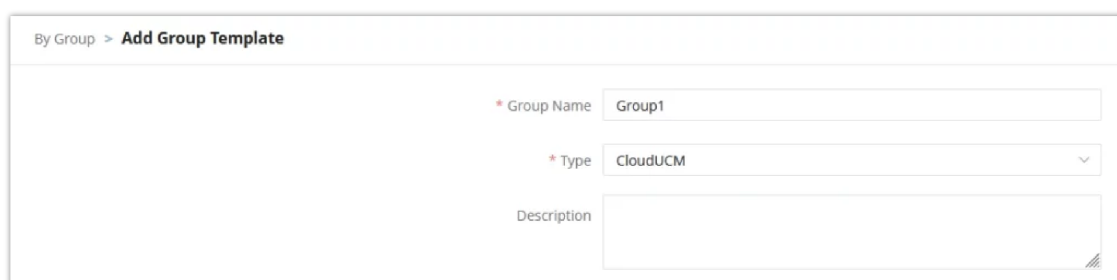
Group Template

Users can configure a group of CloudUCM instances and apply settings to the entire group simultaneously by following the instructions below:

- Under **Organization** → **Device Template** → **By Group**, click on

+ Add Group Template

- Name the group and choose the CloudUCM from the **Type** dropdown list. Writing a description is optional.



By Group > **Add Group Template**

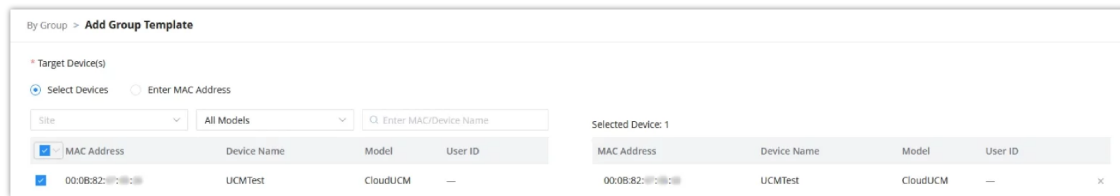
* Group Name Group1

* Type CloudUCM

Description

Add New CloudUCM Group Template

3. Select the target devices by checking the boxes or by entering their MAC addresses.



Select Group CloudUCM Devices

4. Configure the group template parameters and select **Save**. Once this is done, the configuration template will be pushed to all the devices in the group.

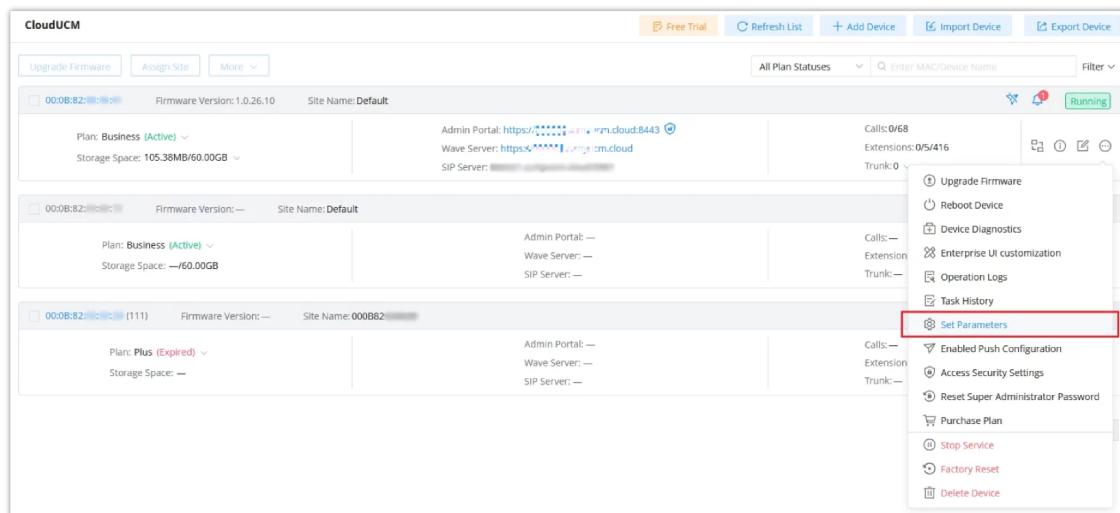
Pushing Configuration for CloudUCM

There are several methods available for users to push configurations to CloudUCM. This section will explain each method in detail, but first, it is important to highlight some important notes.

- All checked parameters on the configuration page will be pushed to the CloudUCM device, overwriting its local configuration.
- If a required configuration parameter fails (e.g., invalid voicemail password), the configuration will be considered unsuccessful.
- If a restart is needed, it will be performed immediately.
- When using a configuration template for a new CloudUCM, the setup wizard will still appear upon the first login and cannot be skipped.

Setting Parameters for a single CloudUCM

Users can edit the configuration for a single CloudUCM by going to **Organization** → **Device Template** → **Options** and selecting **Set Parameters**.



CloudUCM Set Parameters

Automatically Pushing the Configuration

When adding a CloudUCM, if the selected site has an associated CloudUCM model template, a prompt will appear with the option to allow the automatic push configuration.

Add Device ✕

Device Name
Support 1-64 bits

*** Initial Password**

*** Site**

Default
▼

i The configuration template for this device exists in the selected site and can be pushed.

Push Configuration i
☒

Back
Save

CloudUCM Push Configuration Option

As mentioned previously, users can disable/enable push configuration anytime for a specific ClouUCM. The following table includes the icons related to automatic push configuration:

Icon	Description
	Push configuration is prohibited.
	Configuration is being pushed.
	Last push configuration has failed. (Users can click on this icon to try again)

Manually Pushing the Configuration

It is possible to manually push model configuration templates or group configuration templates to multiple CloudUCMs. This can be done by clicking on the **Push Configuration Update** icon that can be found under **Organization** → **Device Template** → **By Model/By Group**.

By Group
+ Add Group Template

Delete Copy Template

All Types Search Group Name

Group Name	MAC Address	Device Name	Model
Test Group			
test_copy			
444			
123213			
111			
test			

Push Configuration Update ✕

Automatically add selected devices to group ☐

* Target Device(s)

Site

All Models

Enter MAC/Device ID

Selected Device: 2

MAC Address	Device Name	Model
00:0B:82:...	—	CloudUCM
00:0B:82:...	—	CloudUCM

Total 3 10/page

< 1 >

Cancel

Apply Now

Schedule Config Update

CloudUCM Push Configuration Update

Users can also manually create tasks to push model or group configuration templates. These tasks can be applied immediately, scheduled for a later time, or set at specific intervals.

Task > Add Task

* Task Name: test CloudUCM

* Task Type: Update Config: Group, Group Template (CloudUCM)

* Task Time: ☒ Immediate ☐ Scheduled ☐ Interval

* Target Device(s): ☒ Select Devices ☐ Enter MAC Address

MAC Address	Device Name	Model
00:0E:00:00:00:00	—	CloudUCM
00:0E:00:00:00:00	—	CloudUCM
00:0E:00:00:00:00 2D	111	CloudUCM

Total: 3 10/page

Selected Device: 0

MAC Address	Device Name	Model
-------------	-------------	-------

No Data

Cancel Save

© 2024 Grandstream Networks, Inc. CloudUCM

CloudUCM Provisioning Task

INTEGRATIONS

AI Settings (Beta)

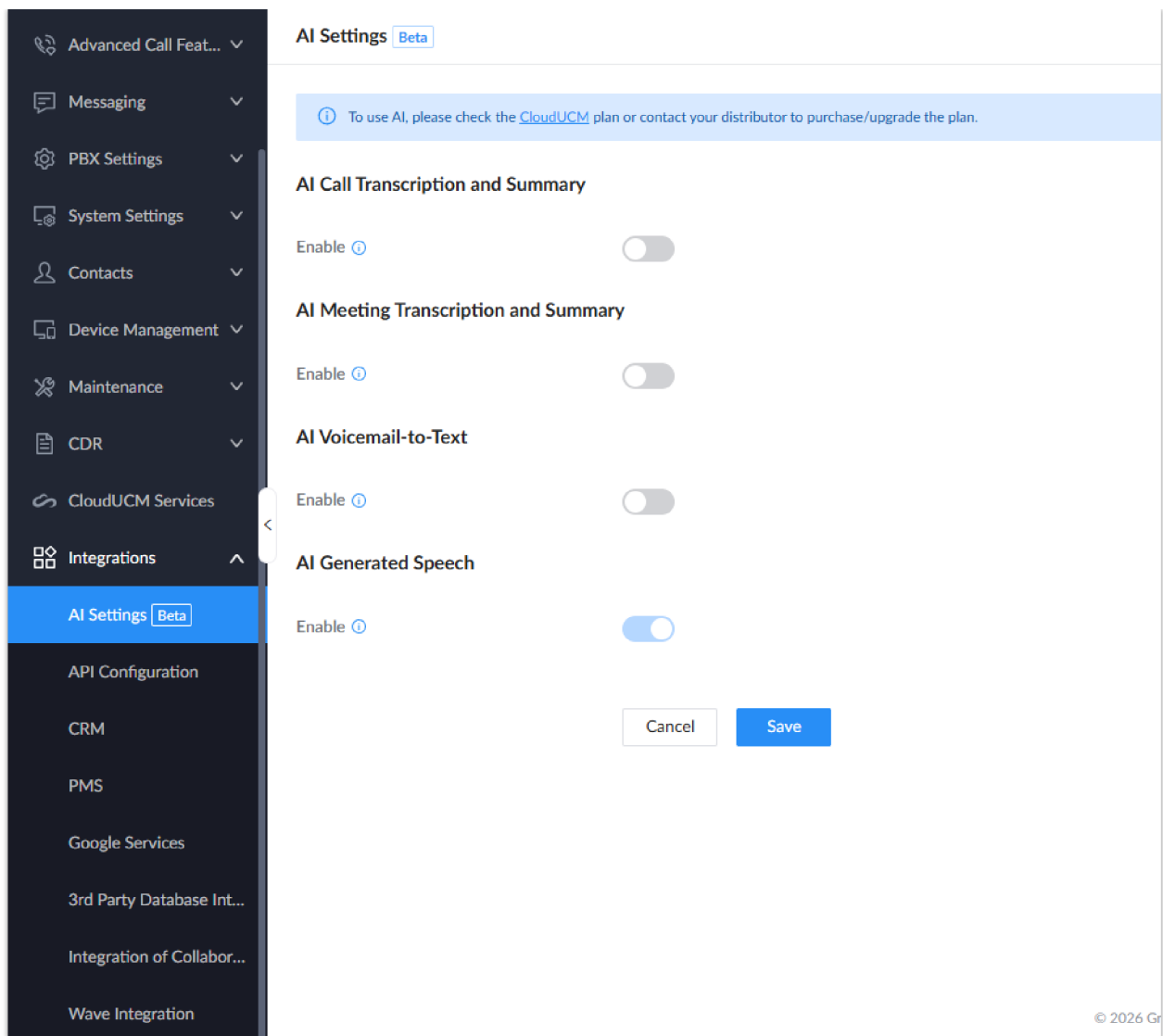
The AI Settings page allows administrators to configure the usage of AI services provided through the RemoteConnect AI service. These features enable automatic speech recognition, transcription, summarization, and text-to-speech processing for calls, conferences, and voice messages.

AI services are a purchaseable add-on and subject to usage limits defined by the active RemoteConnect plan. The administrator can enable each AI feature independently and define whether it applies to all extensions or only selected extensions.

For more information, please refer to the RemoteConnect pricing page: <https://cloud.grandstream.com/plans>

The following AI capabilities are supported on the CloudUCM:

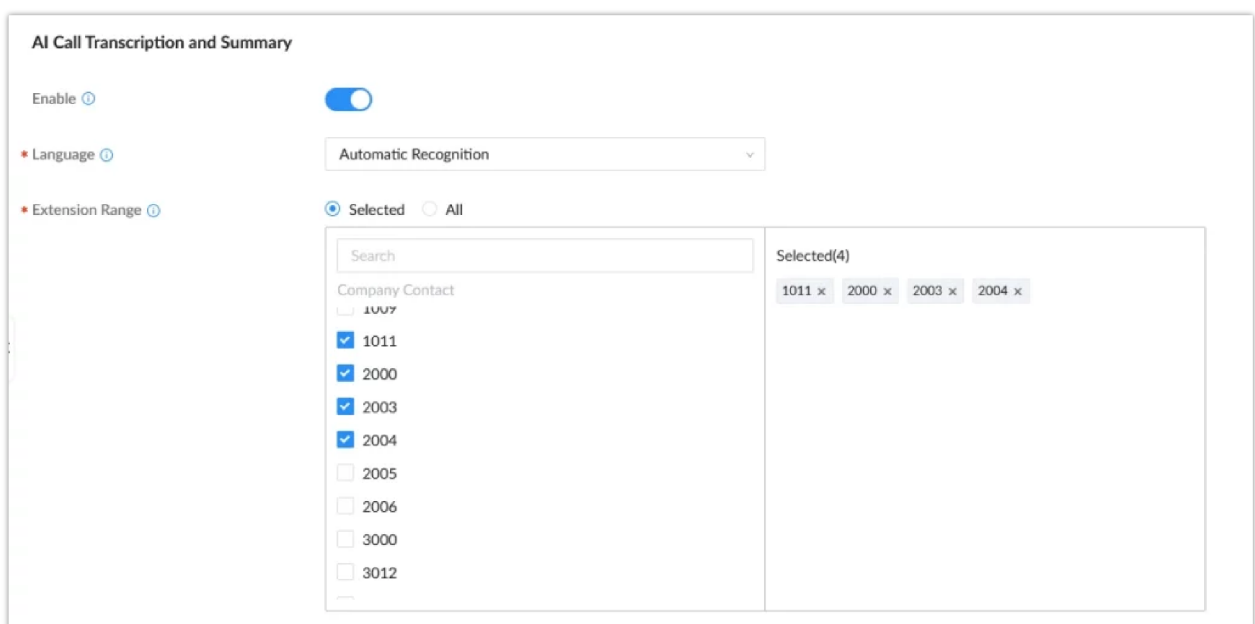
- **AI Call Transcription and Summary**
- **AI Conference Transcription and Summary**
- **AI Voice Message to Text**
- **AI Generated Speech**



AI Settings Page

AI Call Transcription and Summary

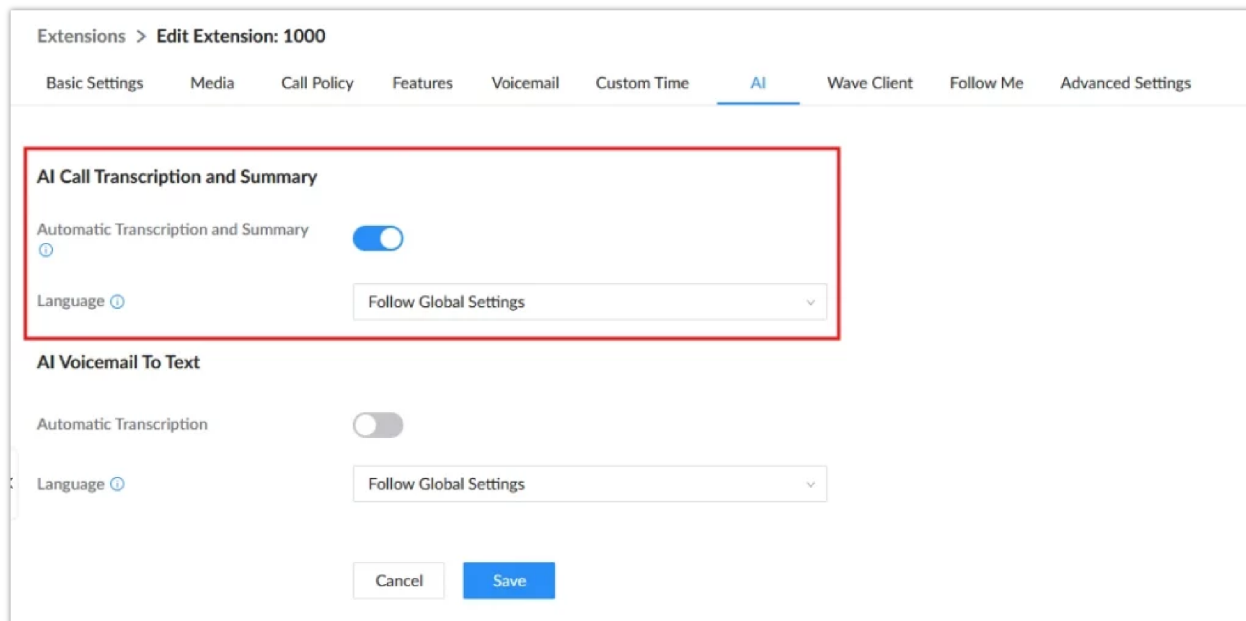
This feature enables AI-based transcription and summarization for one-to-one calls. When enabled globally, the administrator defines whether the feature applies to all extensions or only selected extensions. Only extensions included in this scope are eligible for call transcription and summarization.



AI Call Transcription and Summary General Setting

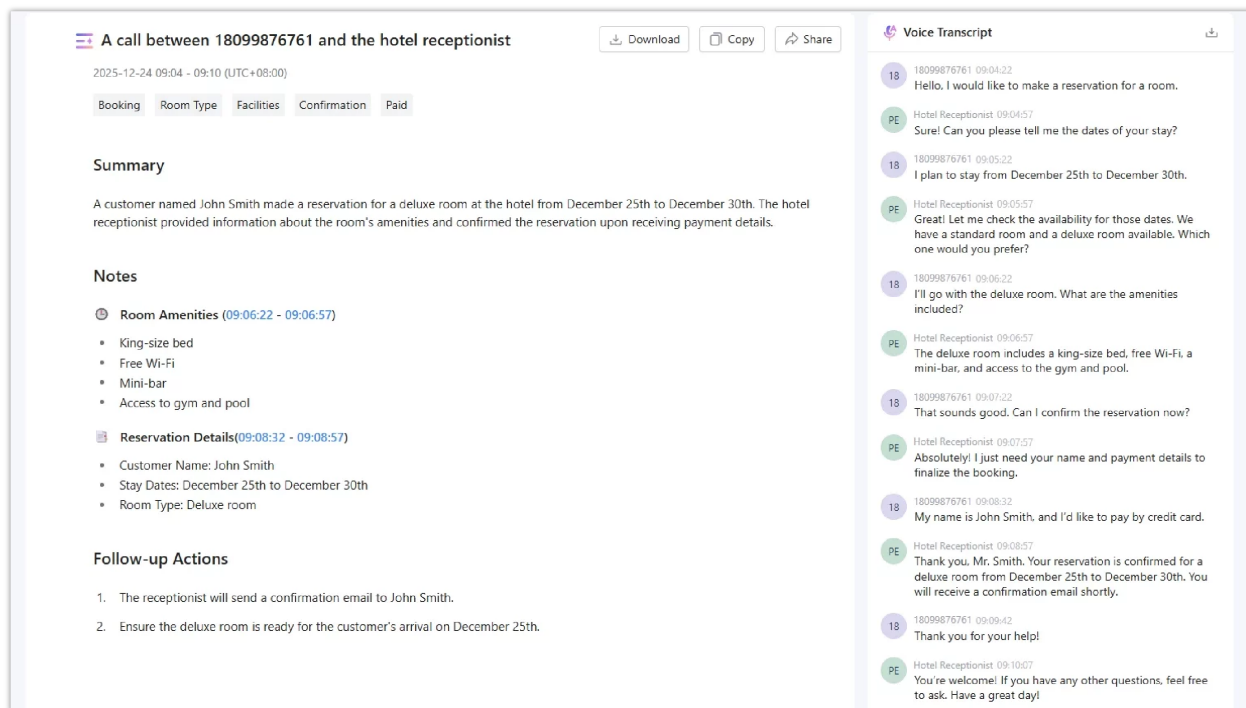
At the extension level, the *Automatic Transcribing and Summarizing* option determines whether calls for that extension are processed automatically. When enabled, all calls made or received by the extension are automatically transcribed and summarized.

The recognition language can be configured globally under **AI Settings (Beta)**→**AI Call Transcription and Summary** and followed by the extension, or explicitly set per extension.



Extension Automatic Call Transcription

Generated transcripts and summaries can be viewed by users through the **Wave client**, as shown below.



Call Transcript on Wave

AI Meeting Transcription and Summary

This feature enables AI-based transcription and summarization for conference calls and meetings. When enabled, meeting audio is processed by the AI service and a transcript and summary are generated after the meeting ends. The administrator can define whether the feature applies to all extensions or only selected extensions participating in conferences.

AI Meeting Transcription and Summary

Enable ⓘ

☒

Extension Range ⓘ

Selected
All

Search

Company Contact

☒ All
☐ Sales
☐ Quality Control
☐ Finance
☒ Marketing
☐ Technical Support
☐ IT
☐ Human Resources
☐ Logistics

Selected(1)

Marketing x

AI Meeting Transcription and Summary Setting

When scheduling a meeting, the meeting organizer can explicitly choose whether the conference will be transcribed or not. This selection applies only to the scheduled meeting and does not affect global or extension-level AI settings.

System Status

Extension/Trunk

Basic Call Features

Multimedia Meeting

IVR

Voicemail

Ring Groups

Paging/Intercom

Call Queue

Speed Dial

Event List

Feature Codes

Parking Lot

Advanced Call Feat...

Messaging

Multimedia Meeting > Schedule Meeting

resource-intensive codec.

Batch Add

Allow User Invite ⓘ ☒

Advanced

Email Reminder (m) ⓘ ☒ 60 Range 5 - 120

Call Participants ⓘ ☒

Allowed to Override Host Mute ⓘ ☐

Play Joining/Leaving Meeting Announcement ⓘ ☒

Auto Record ⓘ None

Sync to Google Calendar ⓘ ☐ Google Services

Support AI transcription ☒

Language ⓘ Automatic Recognition

Automatic AI Transcription ⓘ ☐

AI Transcription Support for Scheduled Meeting

Meeting transcripts and summaries can be accessed by participants through supported Wave clients and user portals.

Hotel Weekly Meeting

2025-12-24 10:04 - 10:24 (UTC+08:00)

Participants: Jianhua Zhao, Peter, Kevin, Lucy, Daniel, James

Hotel OperationsOccupancy RateGuest SatisfactionF&B ServicesMaintenanceRevenue GrowthUpcoming EventsSustainability

Summary

The meeting focused on reviewing last week's operational performance, discussing guest feedback, operational issues, and strategies for the upcoming peak season. Each department provided updates on their progress and outlined plans for future work.

Notes

Operations Management (Front Office & Facilities)(10:04:22 - 10:08:32)

- Front Office Operations: 85% occupancy rate last week; 40% of guests used the online check-in feature, significantly reducing front desk wait times.
- Facility Maintenance: Resolved Sunday's key card encoder glitch and inconsistent HVAC temperatures on floors 5-7; pending investigation of slow-draining showers in some rooms. Cleaning Progress: Completed deep cleaning of floors 1-4 (next floors scheduled for next week).

Food & Beverage Services(10:08:52 - 10:24:37)

- Performance & Feedback: 10% growth in dinner revenue, with the new seafood platter and vegetarian risotto receiving positive reviews. Long-stay guests noted repetitive breakfast buffets, prompting plans for a rotating menu.
- Cost & Planning: Food costs remained within budget, while beverage costs exceeded projections slightly due to a special event.

Follow-up Actions

1. Coordinate a dedicated check-in area for the "Global Innovators" group.

2. Collaborate with James on the banquet menu for the corporate client.

3. Test A/V equipment in all conference rooms and ensure HVAC systems are monitored.

Voice Transcript

JHJianhua Zhao 10:04:22

Let's start with a quick overview of last week's performance, then we'll dive into guest feedback, operational issues, and the upcoming peak season strategy.

Peter, let's start with front office. How were last week's check-ins and check-outs?

PEPeter 10:06:57

Morning, Jianhua. Last week was fairly busy. We saw a steady 85% occupancy rate. The new online check-in feature has been a huge success, with about 40% of guests using it. We've seen a corresponding decrease in wait times at the front desk. The main issue was a small technical glitch with the key card encoder on Sunday afternoon, which Kevin's team resolved quickly.

KEKevin 10:10:07

Yes, Peter. It was a software-related issue. We've updated the driver and it should be stable now. We'll be doing a full diagnostic on all the key card machines this week to prevent a recurrence.

JHJianhua Zhao 10:12:12

Good, Kevin, what's the status of the HVAC system on floors 5 through 7? We had a few complaints about inconsistent temperatures.

KEKevin 10:15:27

We've replaced the main thermostat controllers for that entire section. The new units are more precise and energy-efficient. We'll be monitoring them closely over the next few days. We're also starting the preventative maintenance schedule on all guest room AC units this week.

LLLucy 10:16:02

Speaking of that, Kevin, my team reported a couple of rooms with slow-draining showers. Could you have your maintenance crew take a look?

KEKevin 10:19:55

Lucy, yes, of course. I've already got two on the list. I'll have a team up there this afternoon.

Meeting Transcript on Wave

AI Voicemail to Text

This feature converts voice messages (voicemail) into text using AI speech recognition. When enabled globally, voice messages left for eligible extensions can be transcribed.

AI Voicemail To Text

Enable

* Language

Automatic Recognition

* Extension Range

Selected

All

Search

Company Contact

All

Sales

Quality Control

Finance

Marketing

Technical Support

IT

Human Resources

Logistics

Selected(1)

Technical Support x

AI Voice Message to Text General Setting

At the extension level, the Automatic Transcription option determines whether voice messages for that extension are automatically converted into text.

The recognition language can follow the global configuration or be explicitly specified for the extension.

Extensions > Edit Extension: 1000

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

AI Call Transcription and Summary

Automatic Transcription and Summary ☐

Language ⓘ Follow Global Settings

AI Voicemail To Text

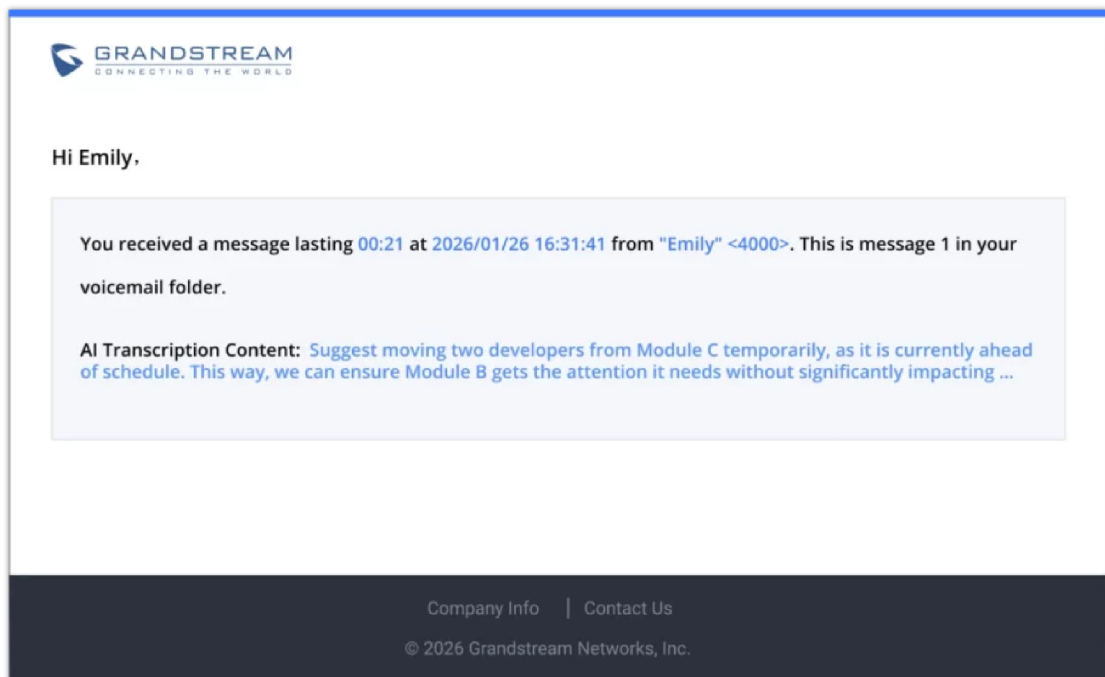
Automatic Transcription ☒

Language ⓘ Follow Global Settings

Cancel Save

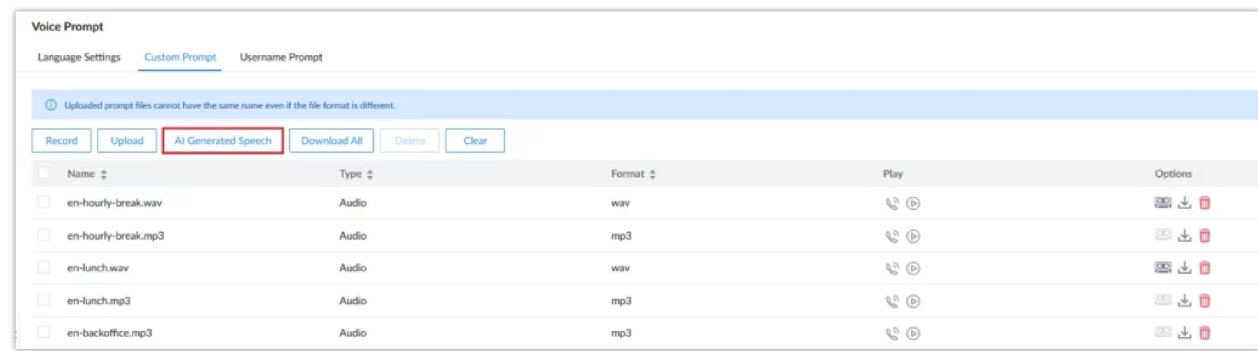
Extension Automatic Voicemail Transcription

Transcribed voicemail content can be viewed in supported Wave clients and may also be included in voicemail notifications, depending on system configuration.



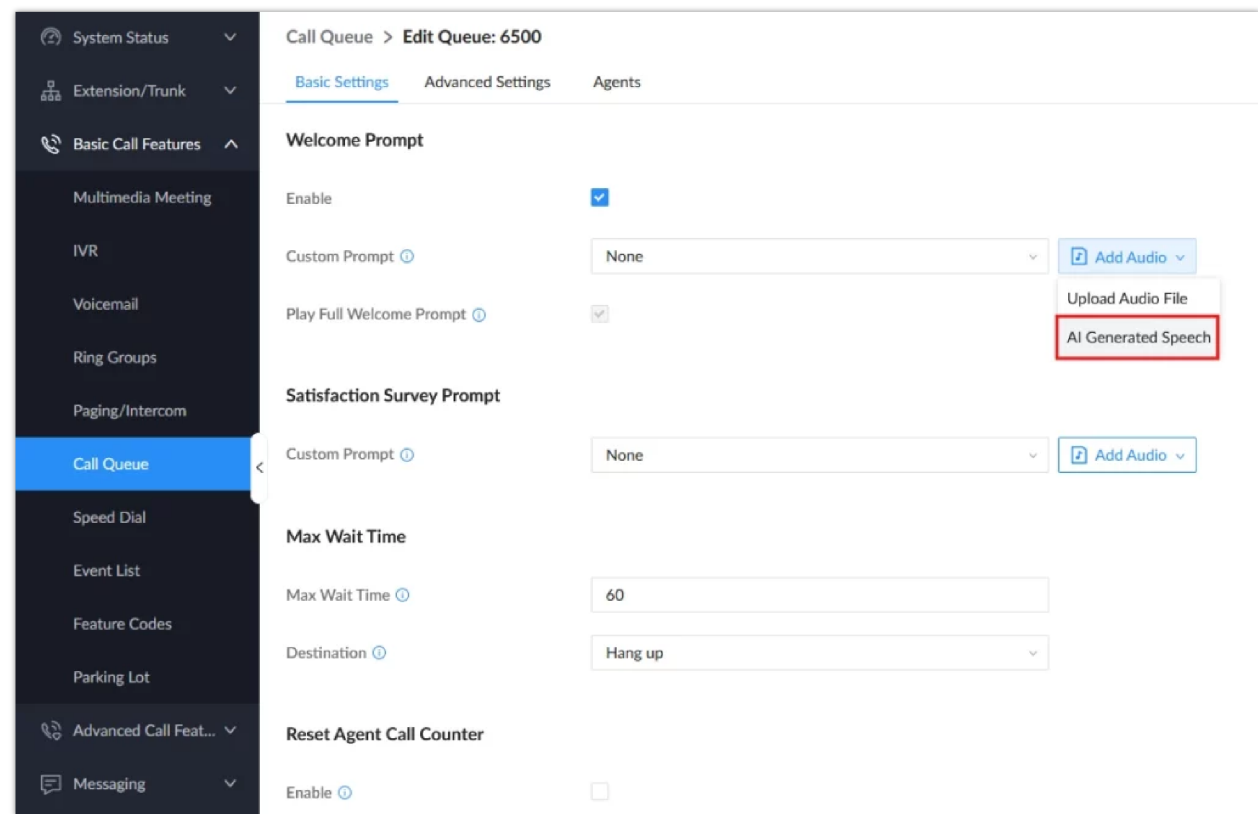
Voicemail Transcript Email

The feature can be accessed from **PBX Settings**→**Voice Prompt**→**Custom Prompt** by clicking the *AI Generated Speech* button, which opens the AI generation window.



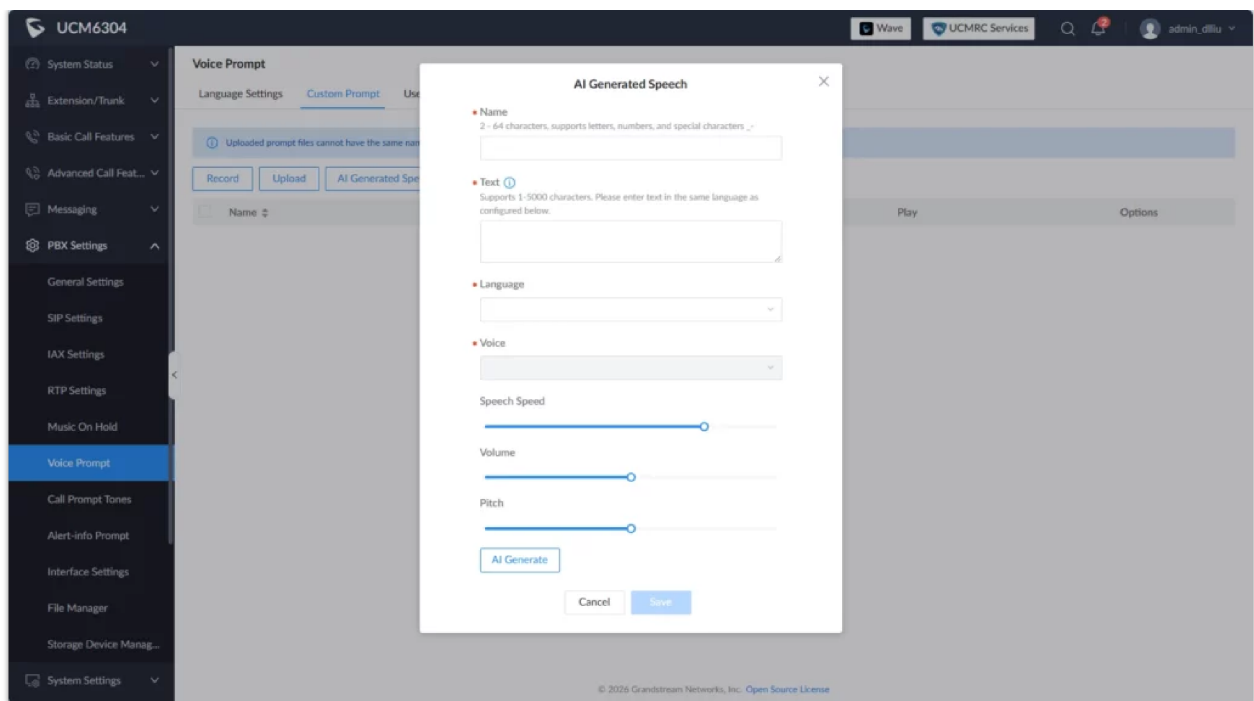
AI Generated Speech Option in Custom Prompt

It is also accessible while configuring features that require voice prompts (such as call queues). In those cases, selecting *AI Generated Speech* from the prompt selection dropdown redirects the user to the same AI generation window used in the Voice Prompt page.



Call Queue AI Generated Prompt Option

When creating an AI-generated voice prompt, the following settings are available:



AI Generated Speech Configuration Options

Name	Defines the name of the generated voice prompt. This name is used to identify the prompt in the system and must be unique. The field supports 2–64 characters, including letters, numbers, and special characters.
Text	Specifies the text content that will be converted into speech. The text length supports up to 5,000 characters.
Language	Specifies the language used for text-to-speech processing.
Voice	Selects the voice profile used to generate the speech. Different voice options may be available depending on the selected language. A preview option is provided, allowing administrators to listen to the voice style before generating the prompt.
Speech Speed	Controls the playback speed of the generated speech. The speed can be adjusted from slower to faster relative to normal speaking speed.
Volume	Adjusts the output volume level of the generated audio. The value can be set from 0 to 100 to accommodate different playback environments.
Pitch	Controls the pitch of the generated voice. Higher values produce a higher-frequency voice, while lower values produce a deeper tone. The pitch range can be set from 0 to 100.

After configuring the parameters, clicking *AI Generate* produces the audio preview. Once satisfied, the generated prompt can be saved and reused like any other system voice prompt.

API Configuration

CloudUCM API allows creating an interface between the UCM and an application to send HTTP requests to the UCM, either to configure the UCM or to get information from it.

API Settings

Before accessing the API, the administrators need to enable the API and configure the access/authentication information on the CloudUCM first under **Integrations** → **API Configuration**. The API configuration parameters are listed in the tables below.

Username	The username for API Authentication.
Password	The password for API Authentication.
IP Address Allowlist	If enabled, only addresses in the list below will be allowed access. If disabled, geo-ip access control will be used instead.
API Interface Permissions	Select the API interface permissions. The permissions which can be selected with their respective parameters are listed below. ● Call Control ● CDR ● Contacts ● Device Management ● Extensions ● Extension Group ● Files ● Inbound Routes ● IVR ● Multimedia Meeting ● Outbound Rules ● Paging/Intercom ● PIN Groups ● PMS ● Queues ● Recordings ● Status ● Trunk ● User Information

Note

You can create multiple users with different login credentials to access to the HTTPS API.

API Queries Supported

The new API supports new queries listed below, which will accomplish certain requests and get data about different modules on CloudUCM.

Queries Supported
getSystemStatus
getSystemGeneralStatus
listAccount
getSIPAccount
updateSIPAccount

listVoIPTrunk
addSIPTrunk
getSIPTrunk
updateSIPTrunk
deleteSIPTrunk
listOutboundRoute
addOutboundRoute
getOutboundRoute
updateOutboundRoute
deleteOutboundRoute
listInboundRoute
addInboundRoute
getInboundRoute
updateInboundRoute
deleteInboundRoute
playPromptByOrg
listBridgedChannels
listUnBridgedChannels
Hangup
callbarge
listQueue
getQueue
updateQueue
addQueue
deleteQueue
loginLogoffQueueAgent
pauseUnpauseQueueAgent
listPaginggroup
addPaginggroup
getPaginggroup
updatePaginggroup
deletePaginggroup
listIVR
addIVR
getIVR
updateIVR
deleteIVR
cdrapi
recapi
pmsapi
queueapiget
getPinSets
addPinSets
updatePinSets
deletePinSets

cleanTerminalChatInformation
getSIPAccountQR
getCallQueuesMemberMessage
getQueueCalling

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.

API Configuration Parameters

Upload Voice Prompt via API

Customers 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 follows:

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 as the HTTP/HTTPS requester and download the prompt file from the FTP server.

The steps and conditions to upload the voice prompt via API are listed below:

1. Configure the prompt User under **Integrations** → **API Configuration** → **Upload Prompts User Configuration**. By default, the username and password for the voice prompt user are "Username: uploader; Password: uploader123".

API Configuration

API Settings (New)
CDR Real-time Output Settings
Upload Prompts User Configuration

Upload Prompts User Configuration

Enable
☐

Username

Password

Cancel
Save

Upload Prompt User Configuration

2. Hash the password of the user configured in an MD5 hash format.
3. Set the permission on the FTP server to Anonymous on the local computer hosting the FTP server, and make sure that the default FTP port 21 is used.
4. Send an HTTP/HTTPS command to trigger the Prompt file upload on the UCM. If UCM's HTTP server is set to HTTPS, the example of the request sent to the UCM is:

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

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

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

Note

If the File name on the HTTP/HTTPS request exists already on the UCM's Custom voice prompts list, the existing file will be overwritten by the new file downloaded from the FTP server.

For more details on CDR API (Access to Call Detail Records) and REC API (Access to Call Recording Files), please refer to the document in the link here:

<https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>

CRM

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 CloudUCM supports the following CRMs: SugarCRM, VtigerCRM, 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 the CRM page, and saves the call information in the contact's history.

Sugar CRM

The configuration page of SugarCRM can be accessed via admin login, on the UCM WebGUI **Features**→**CRM**.

CRM

CRM System: SugarCRM

* CRM Server Address: https://exasandbox.sugaropencloud.eu

* Add Unknown Number: Leads

Contact Lookups:

1 item	Available	2 items	Selected
☐	Look up in Accounts table	☐	Look up in Contacts table
		☐	Look up in Leads table

SugarCRM Basic Settings

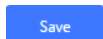
1. Select "SugarCRM" from the CRM System Dropdown to use SugarCRM.

CRM System	Select a CRM system from the dropdown menu.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	Select from the “ Available ” list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

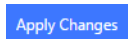
SugarCRM Settings

Once settings on admin access are configured:

2. Click on

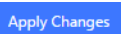


and



3. Log out of admin access.

4. Log in to the UCM as a user and navigate to “**User Portal→Other Feature→CRM User Settings**”.

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

CRM User Settings

Enable CRM :
☒

* Username :

* Password :

Login Status :

CRM User Settings

Vtiger CRM

The configuration page of the VtigerCRM can be accessed via admin login. On the UCM WebGUI, go to **Integrations > CRM**.

CRM

CRM System :

VtigerCRM

* CRM Server Address :

http://vtiger.mydomain.com

* Add Unknown Number :

Organizations

Contact Lookups :

0 item

Available

None

<

>

↑

↓

3 items

Selected

Look up in Organizatio...

Look up in Leads table

Look up in Contacts ta...

VtigerCRM Basic Settings

1. Select "Vtiger CRM" from the CRM System Dropdown to use Vtiger CRM.

CRM System	Select a CRM system from the dropdown menu.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it cannot be found in the selected module.
Contact Lookups	Select from the " Available " list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.

VtigerCRM Settings

Once settings on admin access are configured:

2. Click on

Save

and

Apply Changes

3. Log out of admin access.

4. Log in to the UCM as a user and navigate to "**Other Features > CRM User Settings**".

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

CRM User Settings

Enable CRM: ☒

* Username:

* Password:

Login Status:

CRM User Settings

Bitrix24 CRM

CloudUCM supports integration with Bitrix24 CRM, allowing the system to query CRM records during calls, display contact information, and automatically create CRM records for unknown numbers based on configuration.

For detailed step-by-step instructions on preparing the Bitrix24 account, generating webhooks, and completing the integration, refer to the [Bitrix24 CRM Configuration Guide](#).

CRM

CRM System: Bitrix24CRM

* CRM Server Region

* Add Unknown Number

Contact Lookups

Available: 3 items

- ☐ Look up in Contacts table
- ☐ Look up in Leads table
- ☐ Look up in Organizations table

Selected: 0 items

None

Bitrix24 CRM Settings

The table below describes the configurable parameters for this integration.

CRM System	Select "Bitrix24CRM" from the CRM System dropdown menu to enable Bitrix24 integration.
CRM Server Region	Specify the Bitrix24 server region or domain associated with the Bitrix24 account. This value must match the region or URL used when configuring the Bitrix24 webhook.
Add Unknown Number	Specifies how the CloudUCM handles incoming or outgoing calls from phone numbers that do not exist in Bitrix24 CRM. • None: No CRM record is created when an unknown number is detected. • Contacts: Automatically creates a new Contact record in Bitrix24 when the number is not found in existing CRM records. • Leads: Automatically creates a new Lead record in Bitrix24 when the number is not found.

	● Accounts: Automatically creates a new Account record in Bitrix24 when the number is not found.
Contact Lookups	Select from the “Available” list and move items to the “Selected” list to define where the CloudUCM performs contact lookups in Bitrix24. Supported lookup tables include Contacts, Leads, and Organizations. When multiple tables are selected, the lookup order determines the priority of the search.

Once the Bitrix24 CRM settings on the admin interface are configured:

1. Click Save and Apply Changes.
2. Log out from the admin account.
3. Log in to the CloudUCM as a user and navigate to **User Portal→Other Features→CRM User Settings**.
4. Enable CRM and enter the Bitrix24 account credentials information as required.
5. Click Save to complete the login process.

After successful login, the CRM status will change from *Logged Out* to *Logged In*, and the user can start using Bitrix24 CRM features during calls.

Salesforce CRM

The configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI **Integrations > CRM**.

Salesforce Basic Settings

1. Select “Salesforce” from the CRM System Dropdown to use Salesforce CRM.

CRM System	Select a CRM system from the dropdown menu. Four CRM systems are available: SugarCRM, VtigerCRM, 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.

Salesforce Settings

Once settings on admin access are configured:

2. Click on

Save

and

Apply Changes

3. Log out of admin access.

4. Log in to the UCM as a user and navigate to “**Other Features > CRM User Settings**”.

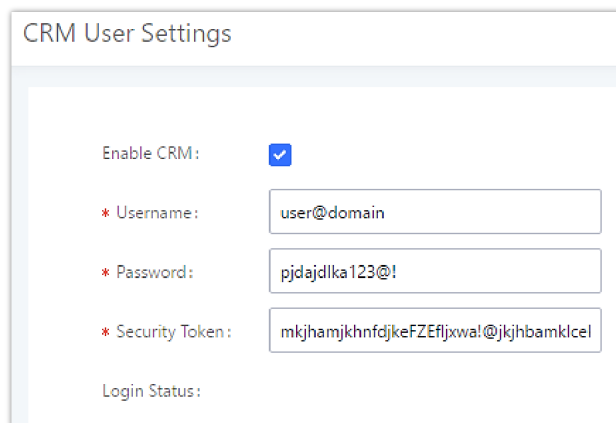
Click on “**Enable CRM**” and enter the **username**, **password**, and Security Token associated with the CRM account, then click on

Save

 and

Apply Changes

. The status will change from “Logged Out” to “Logged In”. User can start then using Salesforce CRM features.



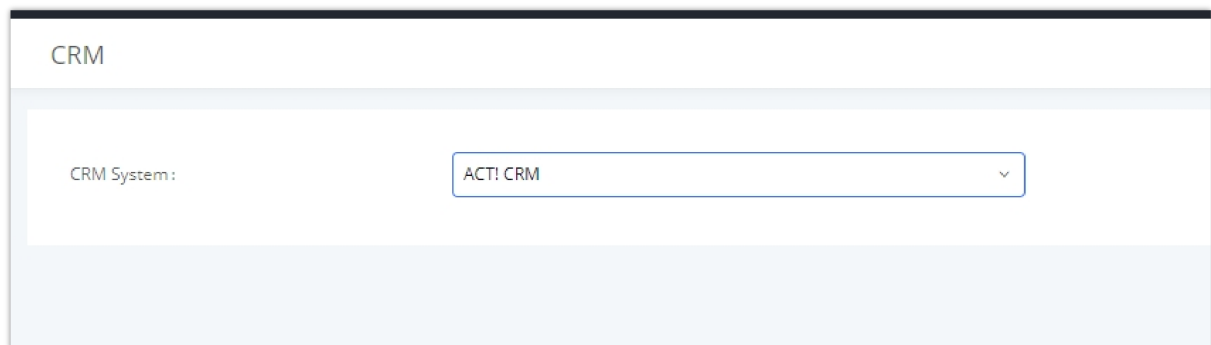
Salesforce User Settings

ACT! CRM

Configuration page of the ACT! CRM can be accessed via admin login, on the UCM Web GUI under **Integrations > CRM**

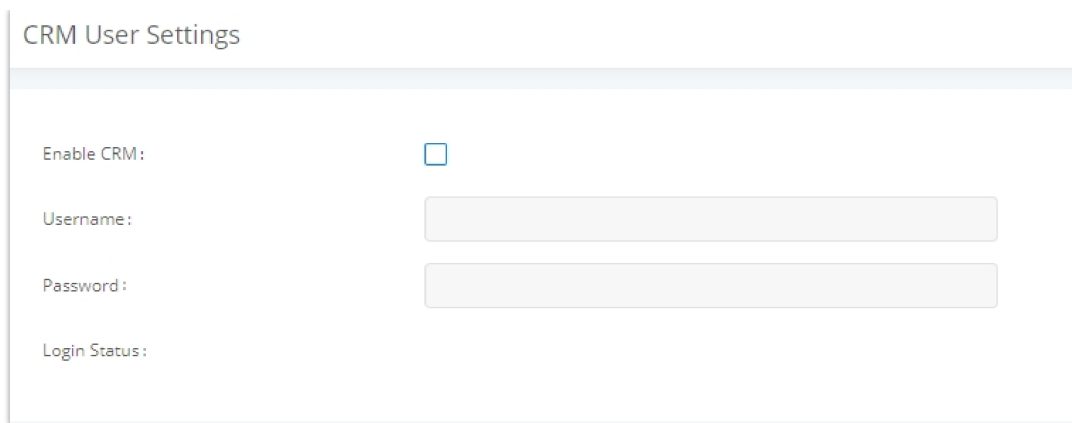
The configuration steps of the ACT! CRM is as follows:

1. Navigate to **Integrations > CRM** and select the “ACT! CRM” option.



Enabling ACT CRM

2. Log in to the UCM as a regular user and navigate to Other Features > CRM User Settings and check the “Enable CRM” option and enter the username and password, which will be the ACT! CRM account’s **API Key** and **Developer Key**, respectively. To obtain these, please refer to the ACT! CRM API developer’s guide here: <https://www.act.com/>

A screenshot of the 'CRM User Settings' form. It has a title bar 'CRM User Settings'. Below it, there are four labels with corresponding input fields: 'Enable CRM:' with an unchecked checkbox, 'Username:' with a text input field, 'Password:' with a text input field, and 'Login Status:' with a text input field.

CRM User Settings

Enable CRM: ☐

Username:

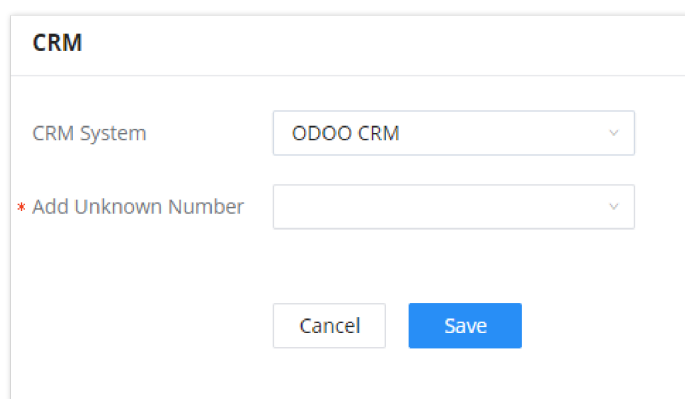
Password:

Login Status:

Enabling CRM on the User Portal

Odoo CRM

The CloudUCM supports integration with Odoo CRM. To enable Odoo CRM, please access the UCM's web UI and then navigate to **Integration > CRM**.

A screenshot of the 'CRM' configuration form. It has a title bar 'CRM'. Below it, there are two dropdown menus: 'CRM System' with 'ODOO CRM' selected, and '* Add Unknown Number' with a dropdown arrow. At the bottom, there are 'Cancel' and 'Save' buttons.

CRM

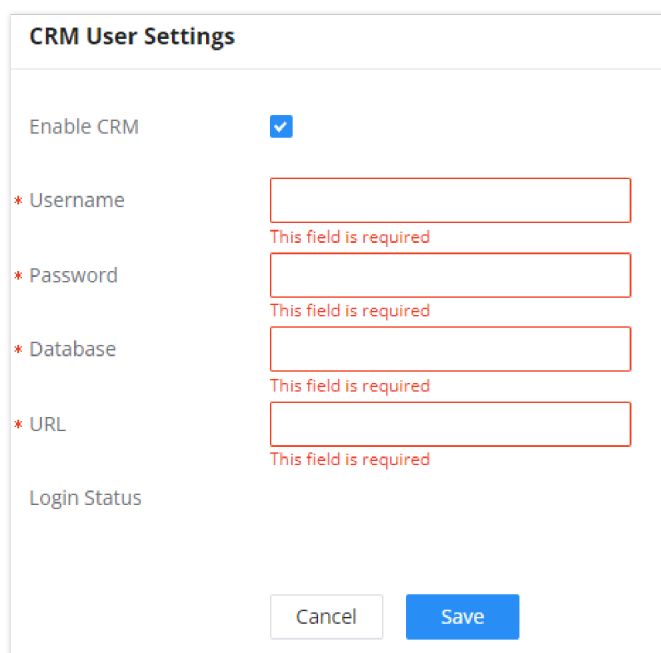
CRM System

* Add Unknown Number

Odoo CRM

Click "Save" then "Apply Changes".

Once Odoo CRM is enabled, the user can log into the user portal by accessing the UCM web UI and entering their username and password. Then, they can navigate to Other Features > CRM User Settings, and then they configure their account using the username and password created on the Odoo platform.

A screenshot of the 'CRM User Settings' form. It has a title bar 'CRM User Settings'. Below it, there are five labels with corresponding input fields: 'Enable CRM' with a checked checkbox, '* Username' with a text input field and a red error message 'This field is required', '* Password' with a text input field and a red error message 'This field is required', '* Database' with a text input field and a red error message 'This field is required', and '* URL' with a text input field and a red error message 'This field is required'. At the bottom, there are 'Cancel' and 'Save' buttons.

CRM User Settings

Enable CRM ☒

* Username
This field is required

* Password
This field is required

* Database
This field is required

* URL
This field is required

Login Status

CRM User Settings

PMS (Property Management System)

CloudUCM supports Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI→**Integrations**→**PMS**.

The PMS integration on CloudUCM is currently supported only with one of the five following solutions.

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

Feature	Mitel	char pmslink	HSC	IDS	Oracle OPERA
Check-In	Yes	Yes	No	Yes	Yes
Check-out	Yes	Yes	No	Yes	Yes
Wake-up Call	Yes	Yes	No	Yes	Yes
Name Change	Yes	No	No	No	Yes
Update	No	Yes	No	Yes	Yes
Set Credit	Yes	No	No	No	No
Set Station Restriction	Yes	No	No	No	No
Room Status	No	Yes	No	Yes	Yes
Room Move	No	Yes	No	Yes	Yes
Do Not Disturb	No	Yes	Yes	No	Yes
Mini Bar	No	Yes	No	Yes	Yes
MSG	No	Yes	No	No	No
MWI	No	No	Yes	No	No
Unconditional Call Forward	No	No	Yes	No	No

Char pmslink Integration

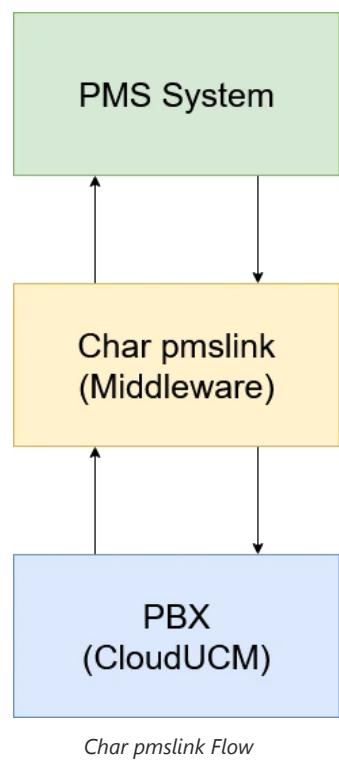
In this mode, the system leverages the **char pmslink** cloud middleware to integrate the CloudUCM with a wide variety of Property Management System (PMS) software.

The communication flow is divided into three parts:

1. **PMS (Property Management System):** Your hotel's management software.
2. **charpmslink (Middleware):** Acts as the universal interface, translating messages between the PMS and the PBX.
3. **PBX (CloudUCM):** The Grandstream CloudUCM, which receives commands from the PMS via charpmslink to execute hospitality features.

This integration enables hotel features such as: Automatic Room Status (Check-in/Check-out) and Wake-up Calls.

The following figure illustrates the communication flow:



For a complete list of supported PMS software and equipment, please visit: <https://www.charpmslink.com>

The table below describes the settings available for char pmslink:

PMS

Basic Settings

Room Management

Room Status

Wakeup Service

Mini Bar

Housekeeper

General

PMS Module

char pmslink (formerly Hmbile)

PMS URL

Server Address

Username

Password

Site

Prompt

Wakeup Prompt

Wake Call

Upload Audio File

Room Status Update Prompt

Default Room Status Update Prompt

Upload Audio File

Automatically Clear/Reset

Automatically Clear Phone Call History

None

Char pmslink Settings

General	
PMS Module	Select the “char pmslink (formerly Hmbile)” option.
PMS URL	Enter the URL of the Oracle Hospitality Opera server.
Server Address	Displays the server address that char pmslink must configure to connect to this CloudUCM.
Username	The authentication username for charpmslink.

Password	The authentication password for charpmslink.
Site	A unique identifier for this specific hotel or property.
Prompt	
Wakeup Prompt	Upload the prompt to play when a wakeup call is answered, or used the default prompt. The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate. Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size. File name can only contain alphanumeric characters and special characters - _ Mp3 and WAV formats are supported. If the user uploads an mp3 recording, it will be converted to WAV.
Room Status Update Prompt	Select the prompt to play when the room status is updated, or use the default prompt. The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate. Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size. File name can only contain alphanumeric characters and special characters - _
Automatically Clear/Reset	
Automatically Clear Phone Call History	Select when to clear phone call history. • None: The phone call history will not be cleared. • Check Out: The phone call history of the guest will cleared upon checking-in. • Check In: The phone call history will be cleared when checking-in a new guest.
Automatically Clear Wake Up Calls	Select when to clear scheduled Wakeup calls. • None: The wake-up call configuration will not be cleared. • Check In/Out: The wake-up call configuration will cleared upon either checking-in or checking-out. • Check Out: The wake-up call configuration will cleared upon checking-out. • Check In: The wake-up call configuration will cleared upon checking-in.
Automatically Clear Wave Chat History	Select when to clear Wave chat history. • None: Wave chat history will not be cleared. • Check Out: Wave chat history will cleared upon checking-out. • Check In: Wave chat history will cleared when checking-in a new guest.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.

PMS API

The PMS API allows users to use their own middleware to work with PMS systems instead of the currently supported integrations.

Additionally, this API allows access to read and modify certain CloudUCM parameters that the current supported PMS integrations cannot. To use this, users must first enable and configure the HTTPS API settings.

For more details, please refer to the online <https://documentation.grandstream.com/knowledge-base/https-api/>, Pmsapi section.

Oracle Hospitality OPERA

CloudUCM integrates directly with Oracle Hospitality OPERA PMS to manage room statuses and extensions from within the OPERA interface. This connection is established using the IFC_PBX interfacing protocol.

To configure the integration, first select the pre-built interface, “Oracle Hospitality OPERA TMS Interface for UCM Series PBX by Grandstream Networks,” within the OPERA software. Once enabled, you can complete the setup from the CloudUCM admin portal.

Data exchange between CloudUCM and the OPERA server is handled by the Fidelio Interface Application Specification (FIAS) protocol. FIAS uses specific attributes to define the data being transmitted. For example:

- o “**RN**” represents the Room Number.
- o “**RS**” represents the Room Status.
- o “**RU**” is used as an update indicator to initiate a room status change.

A typical FIAS message to update a room’s status would be formatted as follows: **RU|RN211|RS3**

In this example, room 211 is updated to status code 3.

In addition, CloudUCM supports Oracle OPERA’s Youth Hostel Mode. This feature allows a single room to be partitioned into multiple independent units, enabling management of separate groups with distinct extensions and individual billing records within the same physical room.

The screenshot shows the 'Basic Settings' tab for the PMS. Under the 'General' section, the 'PMS Module' is set to 'Oracle Hospitality OPERA'. The 'PMS URL' is '192.168.6.32' and the 'PMS Port' is '50001'. The 'Protocol Type' is set to 'tcp'. In the 'Prompt' section, the 'Wakeup Prompt' is 'Wake Call' and the 'Room Status Update Prompt' is 'Default Room Status Update Prompt'. Both prompts have an 'Upload Audio File' button. In the 'Automatically Clear/Reset' section, three options are listed: 'Automatically Clear Phone Call History', 'Automatically Clear Wakeup Calls', and 'Automatically Clear Wave Chat History', all of which are set to 'None'.

The table below describes the settings available for Oracle Hospitality OPERA:

General	
PMS Module	Select “Oracle Hospitality OPERA”
PMS URL	Enter the URL of the Oracle Hospitality Opera server.
PMS Port	Enter the PMS server port. Note: The allowed range 1 – 65535.
Protocol Type	Select the transport protocol to use. • TCP: The connection is established using only TCP handshake. • Simple SSL: Authentication is required to establish the connection. The identity is verified only on the Oracle OPERA Hospitality server. • Mutual SSL: Authentication is required to establish the connection. The identity of both parties is verified by having both parties exchanging their certificates. This reinforces the security by ensuring that only the authorized parties are allowed to contact the server.

Prompt	
Wakeup Prompt	Upload the prompt to play when a wakeup call is answered, or used the default prompt. The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate. Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size. File name can only contain alphanumeric characters and special characters - _ Mp3 and WAV formats are supported. If the user uploads an mp3 recording, it will be converted to WAV.
Room Status Update Prompt	Select the prompt to play when the room status is updated, or use the default prompt. The audio file must be less than 30 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz. For better audio quality, it is recommended to upload mp3 files with 44.1kHz/48kHz sampling rate. Compressed files must be .tar/.tgz/.tar.gz format and cannot exceed 50 MB in file size. File name can only contain alphanumeric characters and special characters - _
Automatically Clear/Reset	
Automatically Clear Phone Call History	Select when to clear phone call history. • None: The phone call history will not be cleared. • Check Out: The phone call history of the guest will cleared upon checking-in. • Check In: The phone call history will be cleared when checking-in a new guest.
Automatically Clear Wake Up Calls	Select when to clear scheduled Wakeup calls. • None: The wake-up call configuration will not be cleared. • Check In/Out: The wake-up call configuration will cleared upon either checking-in or checking-out. • Check Out: The wake-up call configuration will cleared upon checking-out. • Check In: The wake-up call configuration will cleared upon checking-in.
Automatically Clear Wave Chat History	Select when to clear Wave chat history. • None: Wave chat history will not be cleared. • Check Out: Wave chat history will cleared upon checking-out. • Check In: Wave chat history will cleared when checking-in a new guest.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
Billing	
Type of Call Billing	Select the type of billing the call fees for the guests. • Send to Oracle PMS: The call details will be sent and calculated on Oracle Opera. • PBX Direct Billing: The billing will be calculated by CloudUCM and synchronized with Oracle Opera.
Mini Bar Billing Type	Select the type of billing the mini bar • Send to Oracle PMS: The consumed mini bar goods will be pushed to Oracle Opera where they will be processed for the billing. • PBX Direct Billing: The consumed mini bar goods will be processed for billing on CloudUCM, and the bill will be synchronized with Oracle Opera.

The CloudUCM includes an integrated on-premise Property Management System, providing essential hotel management capabilities without the need for a separate software purchase. This local PMS solution allows users to perform core operations such as Room Management, check-in/check-out procedures, Wake-up Services, and Housekeeper management directly from the web interface.

In addition, the CloudUCM local PMS automates important check-out tasks, including backing up guest voicemail recordings, automatically clearing wake-up calls and Wave chat history, and resetting Wave passwords.

For detailed descriptions of PMS features, workflows, and configuration steps, refer to the [Local PMS Guide](#).

PMS

[Basic Settings](#)
Room Management
Check-in Management
Wakeup Service
Mini Bar
Housekeeper

General

PMS Module

Local PMS

Prompt

Wakeup Prompt ⓘ

Wake Call

Add Audio ▾

Room Status Update Prompt ⓘ

Default Room Status Update Prompt

Add Audio ▾

Automatically Clear/Reset

Automatically Clear Phone Call History ⓘ

None

Automatically Clear Wakeup Calls ⓘ

None

Automatically Clear Wave Chat History ⓘ

None

Automatically Reset User/Wave Password ⓘ

☐

Self-Service Settings

ⓘ To ensure successful email delivery, please set the email addresses for both the booker and the guest in advance.

Self Check-in via Email ⓘ

☐

Check-in Email Template

Self Check-out via Email ⓘ

☐

Check-out Email Template

Local PMS Page

The configuration parameters available on the local PMS basic settings are explained in the table below:

Parameter	Description
<i>Prompt</i>	
Wakeup Prompt	A customized prompts that can be played when the wakeup call is answered. To customize it please navigate to PBX Settings→Voice Prompt→Custom Prompt
Room Status Update Prompt	Choose a previously uploaded prompt or upload the prompt which will be played when the room status is changed. If the room status codes have been change, please update the Room Status accordingly.
<i>Automatically Clear/Reset</i>	
Automatically Clear Phone Call History	Configures whether or not the call history of phones will be automatically cleared upon check-in or check-out. Currently only supported on Grandstream phones. • None: Call history will not be deleted after checking-in or checking-out. • Check Out: Call history will be delete when the guest checks-out. • Check In: Call history will be delete when a new guest checks-in.

Automatically Clear Wakeup Calls	Scheduled wakeup calls for rooms can be cleared upon checking in or checking out. ● None: The wakeup calls won't be automatically cleared. ● Check out: The wake up calls assigned to the guest will be cleared when they check out. ● Check In: The wake up calls assigned to a guest will be cleared when a new client checks in.
Automatically Clear Wave Chat History	If enabled, room Wave chat history will be automatically cleared upon check-in or check-out.
Automatically Reset User/Wave Password	If enabled, the User/Wave password of the room extension will be automatically reset to a random password upon check-out.
<i>Self-service Settings</i>	
Self-Check-In Via Email	Enables the system to automatically send a self check-in email with a link prior to the guest's arrival.
Send in Advance (hrs)	Defines how many hours before the scheduled check-in time the self check-in email will be sent.
Self-Check-Out Via Email	Allows the system to automatically send a self check-out email with a link prior to departure.
Send in Advance (hrs)	Defines how many hours before the scheduled check-out time the email will be delivered.
Allow Check-out with Unsettled Bill	Controls whether guests are allowed to complete self check-out even if their bill is not fully paid. ● Enabled: The guest may check out before completing the payment ● Disabled: Payment must be settled before self-check-out is allowed. This option is disabled by default.
Sync Guest Name to Phone	Provisions the name of the checked-in guests to endpoints via Zero Config. Requires endpoints to be discoverable and provisable by Zero Config.
Review Bill at Check-Out	If enabled, a pop-up window with all the charges will appear during guest check-out for reviewing purposes.
Currency Unit	The currency unit for the call rate. These are the supported options which you can choose from: ● American Dollar ● Euro ● Sterling Pound ● Yen ● Won ● Hong Kong Dollar ● Australian Dollar ● Canadian Dollar ● Baht ● Singapore Dollar ● Swiss Franc ● Swedish Krona ● Danish Krone ● Norwegian Krone ● New Zealand Dollar ● South African Rand ● Brazilian Rial ● Indian Rupee ● Russian Ruble ● Vietnamese Dong ● Polish Zloty ● Czech Koruna ● Turkish Lira ● Custom: Enter the currency unit.
Periodically Email Recordings	If enabled, new recordings will be automatically sent to the specified email inbox periodically at the specified intervals.
Type	Configures the type of recordings that should be sent periodically

	• Wakeup Service • Check-in/Check-out History • CDR Records
Period	Specifies the automatic download period. The default option is “By Day”. At the specific time of each day, week or month, the last cycle of new records will be sent to the user. • By Day • By Week • By Month
Email	Specifies the automatic download period. The default option is “By Day”. At the specific time of each day, week or month, the last cycle of new records will be sent to the user.
Customer Email	Enables the system to send automated emails to guests. This includes reservation updates and billing information. Note: Email notifications will not be sent if the customer’s email address is missing.
Reservation Notification	When enabled, the guest will automatically receive an email whenever a reservation is created, modified, or cancelled.
Billing Notification	If enabled, billing-related emails will be sent automatically to the guest.

Google Services

Google Services integration allows integrating the CloudUCM with Google Calendar to automatically synchronize the created Multimedia and Onsite Meetings schedule with the Google Calendar of the host and the participants. In order to use this integration, the user needs to enable API on Google Cloud Console and obtain the Client ID and the Client Secret, then enter the authorized redirect URIs.

Google Calendar Authorization

In the Google Calendar Authorization configuration page, please enter the generated OAuth2.0 Client ID, OAuth2.0 Client Secret, and Authorized redirect URIs to integrate the CloudUCM with Google Calendar.

Google Services

[Google Calendar Authorization](#)

Google Calendar Settings

OAuth2.0 Authentication

* OAuth2.0 Client ID	
* OAuth2.0 Client Secret	
Authorized redirect URIs	
Reset Save	

Google Calendar Authorization

1. Click "Get Authorization Code".
2. Enter the Google account and password (Note: Please make sure that the account information on the authorization page is correct. If you are not logged into the correct account, please log out and log back into the correct one.).
3. Click "Accept" on authorization page.
4. Copy the string to the Authorization Code input box, then click the "Authorize" button.

* Authorization Code		Authorization
----------------------	----------------------	--

Google Calendar Settings

On the Google Calendar Settings configuration page, the user can enable "Google Calendar Auto Refresh Synchronization" to synchronize the meetings created automatically with Google Calendar. The user can also create a calendar label to mark different events on the calendar with customized labels.

To learn more about labels, please refer to the following link: <https://support.google.com/calendar/answer/12377581>

Google Services

Google Calendar Authorization

Google Calendar Settings

Google Calendar Auto Refresh Synchronization

☐

Calendar Label

+ Add

Name	Description	Options
No data		

Cancel

Save

3rd Party Database Integration

The Third-Party Database Integration feature allows the CloudUCM to connect to external databases (such as MySQL) to query contact information when calls are received. When a matching record is found, the caller name is displayed. Optionally, contacts can be synchronized into the CloudUCM LDAP phonebook for centralized management.

Note:

LDAP phonebooks synced from third-party databases support up to 500,000 contacts.

This feature is configured under **Integrations→3rd Party Database Integration**.

3rd Party Database Integration

Basic Settings

Contacts Sync

Connection success

3rd Party Database Integration

☒

Database Type

MySQL

Server Address

192.168.6.36

IPv4 Address

Port

3306

Range 1 - 65535

Database Name

phonebook

Connection Timeout (s)

5

Username

phonebook_user

1 - 64 characters

Password

Phonebook123!

At least 4 characters

Character Set

UTF8MB4

Test Connection

Start

Cancel

Save

3rd Party Database Integration Basic Settings

The Basic Settings tab is used to configure and enable the database connection. The table below describes the parameters on this page:

3rd Party Database Integration	Enable or disable 3rd party database integration. When enabled, the CloudUCM queries the configured database for contact information.
Database Type	Select the database engine: • SQL Server • MySQL
Server Address	Enter the IPv4 address of the database server.
Port	Enter the port used by the database service. Valid range: 1–65535
Database Name	Enter the name of the database used for establishing the connection.
Connection Timeout (s)	Set the time (in seconds) to wait before a connection attempt times out. Please enter a value between 1 and 300. The default value is 5.
Username	Enter the username used to connect to the database.
Password	Enter the password for the specified username.
Character Set	Specifies the character set for MySQL connections. • ASCII • UTF-8 • GBK • GB2312 • UTF8MB4
Test Connection	Click to test connectivity and authentication to the configured database.

After the database connection is successfully established, an additional Contact Synchronization tab becomes available, which enables synchronization of database contacts into the CloudUCM LDAP phonebook.

3rd Party Database Integration

Basic Settings

Contacts Sync

Sync successful

Contacts Sync ⓘ

Table

contacts

Phonebook Name ⓘ

PhonebookSQL

1 - 32 characters, supports alphanumeric characters, chinese characters, and underscore (.)

Attribute Mapping ⓘ

display_name

→

CallerIDName

✖

phone

→

AccountNumber

✖

email

→

Email

✖

Add

Scheduled Sync

By Day

00:00

Cancel

Save and Sync

3rd Party Database Integration Contacts Sync

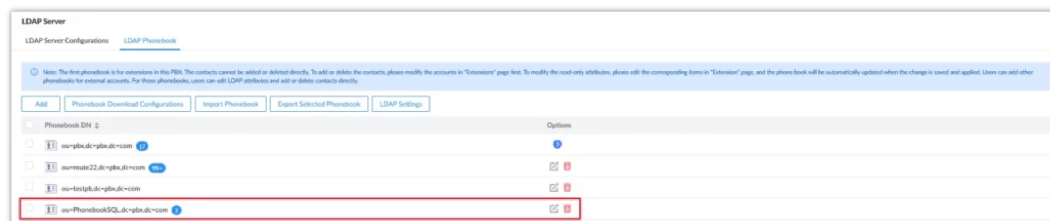
The configurable parameters on this page are described in the table below:

Contacts Sync	Enables synchronization of database contacts into the CloudUCM LDAP phone book. When disabled, real-time caller lookup remains available, but contacts are not synchronized.
---------------	--

Table	Enter the database table containing contact records.
Phonebook Name	Choose the display name of the LDAP phone book created on CloudUCM.
Attribute Mapping	Maps the 3rd party database fields to CloudUCM LDAP attributes (max 10).
Scheduled Sync	Defines automatic synchronization schedule.

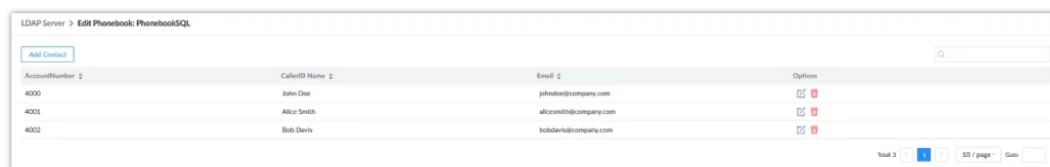
To verify the synced LDAP Phonebook:

1. Navigate to **System Settings→LDAP Server→LDAP Phonebook**.
2. Confirm a new phonebook with the configured name is present.



3rd Party Database Synced Phonebook

3. Verify that the 3rd party database synced contacts are listed and searchable.



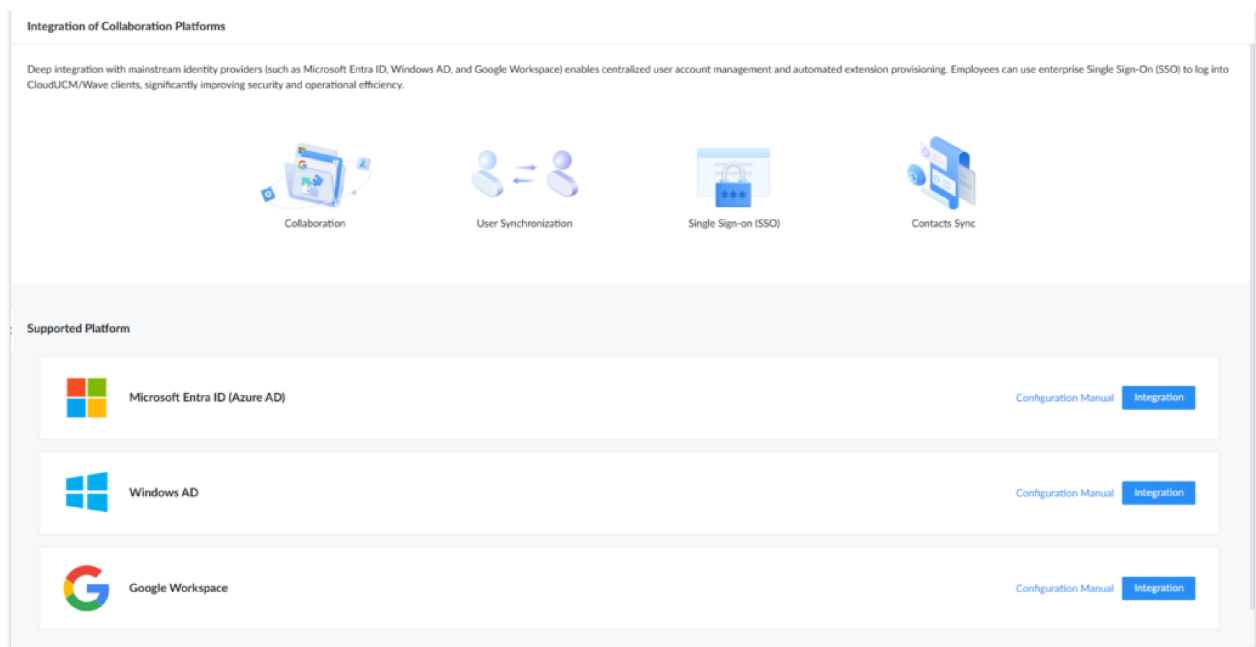
Synced Phonebook Contacts

Integration of Collaboration Platforms

CloudUCM supports integration with enterprise collaboration and identity platforms to centralize user management, authentication, and directory synchronization. These integrations allow administrators to synchronize user identity information from external platforms into the CloudUCM, associate users with extensions or system accounts, and enable Single Sign-On for simplified and secure access to the web interface.

Supported platforms include:

- **Microsoft Entra ID (Azure AD)**
- **Windows Active Directory**
- **Google Workspace**



Integration of Collaboration Platforms Page

Each integration provides configurable options for user synchronization scope, user linking behavior, LDAP directory integration, and authentication methods. The following sections describe the configuration and usage of each platform.

Microsoft Entra ID (Azure AD)

Microsoft Entra (formerly Azure Active Directory) is a cloud platform which provides access management and identity provision. When integrated with CloudUCM, it allows synchronizing the identity information which can be used to log into the CloudUCM's user interface.

Note

For step-by-step configuration guide for Microsoft Entra, please refer to the following link:
<https://documentation.grandstream.com/knowledge-base/microsoft-entra-id-azure-ad-configuration-guide/>

The Microsoft Entra ID configuration page consists of the following tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-On (SSO)**

Each tab is described below.

Basic Settings

This tab defines the connection between the CloudUCM and Microsoft Entra ID.

Integration of Collaboration Platforms > Microsoft Entra ID (Azure AD)

Basic Settings User Settings Single Sign-on (SSO)


Authorized Account: [redacted]@onmicrosoft.com

For more information about Microsoft Entra ID (Azure AD), see [Microsoft Entra ID \(Azure AD\) Configuration Manual](#).

Microsoft Entra ID Authorization ☒

ⓘ Enter your Microsoft Azure app details below.

* Redirect URIs ⓘ

* Application (Client) ID

* Client Password ⓘ ⓘ

* Tenant ID

Cancel

Save and Authorize

Google Workspace Basic Settings Tab

Parameter	Description
Microsoft Entra ID Authorization	Enable Microsoft Entra ID
Redirect URIs	Enter a URI to return Microsoft tokens.
Application (Client) ID	Enter the application ID
Client Password	Enter the client password. If the client's password expires, this will interrupt Microsoft user synchronization. Ensure that the password is updated in a timely manner.
Tenant ID	Enter the tenant ID provided by Microsoft. This can be found in the admin center of Microsoft Entra ID.

User Settings

This tab controls how Microsoft users are synchronized to the CloudUCM.

Integration of Collaboration Platforms > Microsoft Entra ID (Azure AD)

Basic Settings User Settings Single Sign-on (SSO)

Microsoft User

Get Microsoft User

When enabled, Microsoft users can be associated one-to-one with system users/extensions in CloudUCM.

User Range ⓘ

All Users

Add User to LDAP ⓘ

☐

Linked User Settings

Linked CloudUCM

If enabled, the linked CloudUCM user's information (first name, last name, email, mobile number, job title) will be overwritten by the Microsoft user's information.

Linking Method ⓘ

☒ Automatic Link
 ☐ Manual Link

Linked User Range

All Users

Link Policy ⓘ

Automatic Allocation

★ Starting Extension

Cancel

Save

Google Workspace User Settings Tab

The table below describes the parameters available on this tab.

Get Microsoft User	
Get Microsoft User	Enable to retrieve users from Microsoft Entra ID. When enabled, Microsoft users can be associated with CloudUCM users/extensions. When disabled, synchronization is stopped.
User Range	Defines the scope of Microsoft users to retrieve. Options include retrieving all users or specifying user types.
User Type	Available when “Specify Type User” is selected. Defines which Entra user types (e.g., Members, Guest) will be retrieved. Only selected types are synchronized.
Add User to LDAP	When enabled, synchronized Microsoft users are added to the CloudUCM LDAP directory, allowing them to appear in LDAP searches and dialing features.
Linked User Settings	
Linked CloudUCM	Enable to associate Microsoft Entra users with existing CloudUCM users/extensions. When enabled, the linked CloudUCM user's information will be overwritten by the Microsoft user's information.
Linking Method	Defines how Microsoft users are linked to CloudUCM users. Automatic Link: The system automatically matches Microsoft users to CloudUCM users based on defined matching rules.

	● Manual Link: Administrator must manually associate users.
Linked User Range	Specifies which CloudUCM users are eligible for linking. Options include linking all users or only selected user types.
Linked User Type	Available when “Specify Type User” is selected. Defines the Entra user categories (e.g., Members) that are eligible for linking.
Link Policy	Defines how the extension number is assigned during automatic linking. Available options are: ● Automatic Allocation: assigns extensions sequentially, starting from a specified number. ● Read Attribute Value: The extension number is taken from a specified Microsoft Entra user attribute.
Starting Extension	Specifies the initial extension number used when Automatic Allocation is enabled under the linking policy.
Attribute Name	Available when <i>Read Attribute Value</i> is selected. Specifies which Microsoft Entra attribute will be used to determine the extension number.
<i>Microsoft User</i>	
Sync Now	Manually triggers immediate synchronization with Microsoft Entra ID based on the defined User Range.
Sync Settings	Opens synchronization configuration options.
Microsoft User List	Displays all retrieved Microsoft Entra users with the following fields: 1. Microsoft Entra username (typically UPN). 2. Display Name 3. First Name 4. Last Name 5. Job Title 6. Email (Entra ID Contact Email) 7. Mobile Number 8. Business Phone 9. Link CloudUCM User

Single Sign-on (SSO)

The SSO tab allows users to log into the CloudUCM Web UI and Wave using Microsoft Entra authentication.

Integration of Collaboration Platforms > Microsoft Entra ID (Azure AD)

Basic Settings
User Settings
Single Sign-on (SSO)

Single Sign-on (SSO)
☒

i If enabled, users will be able to log into the webUI and Wave with their linked Microsoft account.

Cancel
Save

Google Workspace Single Sign on SSO Tab

Windows AD

Integrating AD with CloudUCM allows the system to fetch and manage user data directly from the AD server, making it easier to maintain consistent user information across platforms.

Contacts can be imported into the CloudUCM’s LDAP phonebook, and AD users can be linked to CloudUCM extensions or system accounts for unified user administration. The integration also supports automatic and scheduled synchronization, reducing manual workload and keeping user records up to date.

Additionally, enabling Single Sign-On (SSO) allows AD users to log in to the CloudUCM web interface using their domain credentials, enhancing security and simplifying password management.

Note

For step-by-step configuration guide for Windows AD, please refer to the following link:
<https://documentation.grandstream.com/knowledge-base/windows-ad-configuration-guide/>

Integration of Collaboration Platforms > Windows AD

Basic Settings

Windows

Unconnected

For more information about Windows AD, see [Windows AD Configuration Manual](#).

Windows AD

* Server Address

192.168.1.1

IPv4 Address

* Domain

* Port

389

Range 1 - 65535

* Username

1 - 64 characters

* Password

At least 4 characters

* Filter

(objectClass=*)

* Base DN

dc=pbx,dc=com

1 - 128 characters, supports alphanumeric characters, chinese characters, and underscore (_)

* Phonebook Name

LdapClient

* AD properties

☐ All

☒ telephoneNumber

☐ mail

☐ displayName

☐ givenName

☐ sn

☐ mobile

☐ homePhone

☐ facsimileTelephoneNumber

☒ userPrincipalName

☐ department

☐ title

Windows AD Integration

The table below describes the parameters available during the Windows AD integration setup.

Parameter	Description
Windows AD	Toggle on/off the Windows AD integration
Server Address	Enter the AD server address.
Domain	Enter the domain
Port	Enter the port to use. The port number must be within the range 1 – 65535
Username	Enter the username.
Password	Enter the password.
Filter	Enter the filter which can be an object class.
Base DN	Information about the AD node to be pulled, for example,dc= pbx,dc=com.
Phonebook Name	Enter the phonebook name.

AD Properties	Select the AD properties which can be used by the CloudUCM.
---------------	---

Google Workspace Integration

The Google Workspace Integration allows the CloudUCM Series to connect with a Google Workspace domain to synchronize user identity information and enable Single Sign-On (SSO).

When enabled, Google users can be associated with CloudUCM system users or extensions, optionally synchronized into the LDAP directory, and used for authentication when accessing the web interface.

This feature is configured under **Integrations→Integration of Collaborative Office Platforms→Google Workspace**.

The Google Workspace integration module consists of three tabs:

- **Basic Settings**
- **User Settings**
- **Single Sign-on (SSO)**

For detailed configuration procedures refer to the [Google Workspace Integration Guide](#).

Basic Settings

The Basic Settings tab is used to configure OAuth authorization between the CloudUCM and Google Workspace. This step is mandatory before any user synchronization or SSO functionality can be enabled.

Google Workspace Basic Settings Tab

The table below describes the parameters of this page:

Parameter	Description
Google Workspace Authorization	Enables or disables Google Workspace integration on the CloudUCM.
Redirect URIs	OAuth redirect URI used to receive authorization tokens from Google. This value must exactly match the redirect URI configured in the Google Cloud Console application.

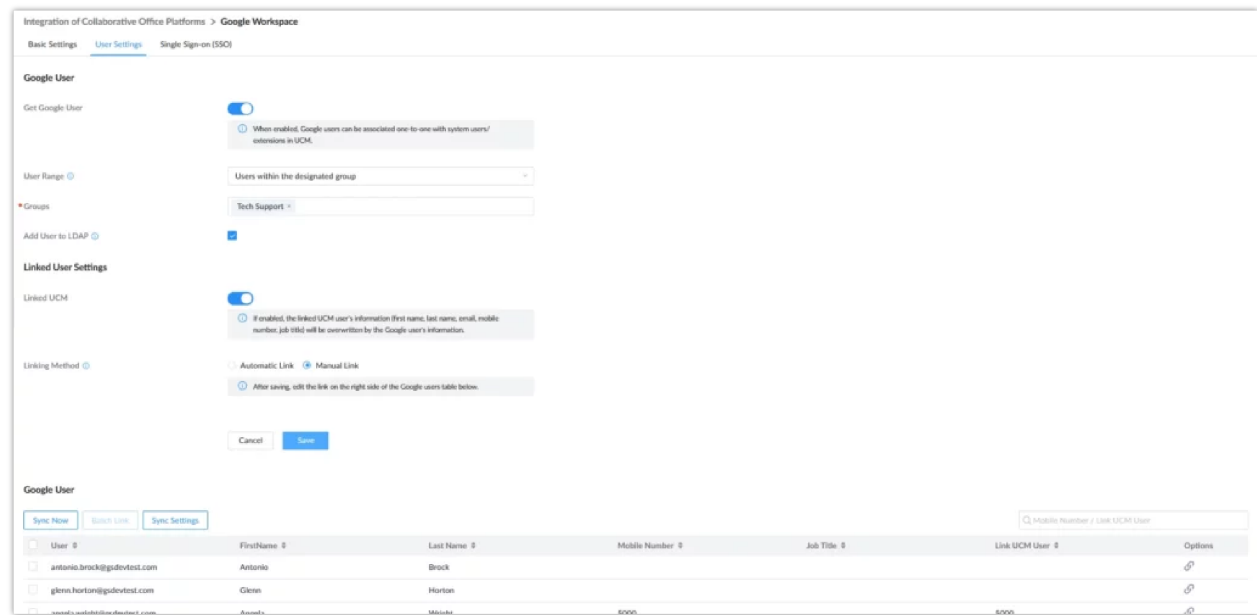
Application (Client) ID	OAuth Client ID generated in Google Cloud Console for the Workspace application.
Client Password	OAuth Client Secret associated with the Client ID. If the client secret expires or is regenerated, it must be updated here to avoid authorization failure.

User Settings

The User Settings tab controls how Google Workspace users are retrieved, synchronized, and linked to CloudUCM users or extensions. The settings on this page are grouped into three categories:

- 1. Google User
- 2. Linked User Settings
- 3. Google User Management

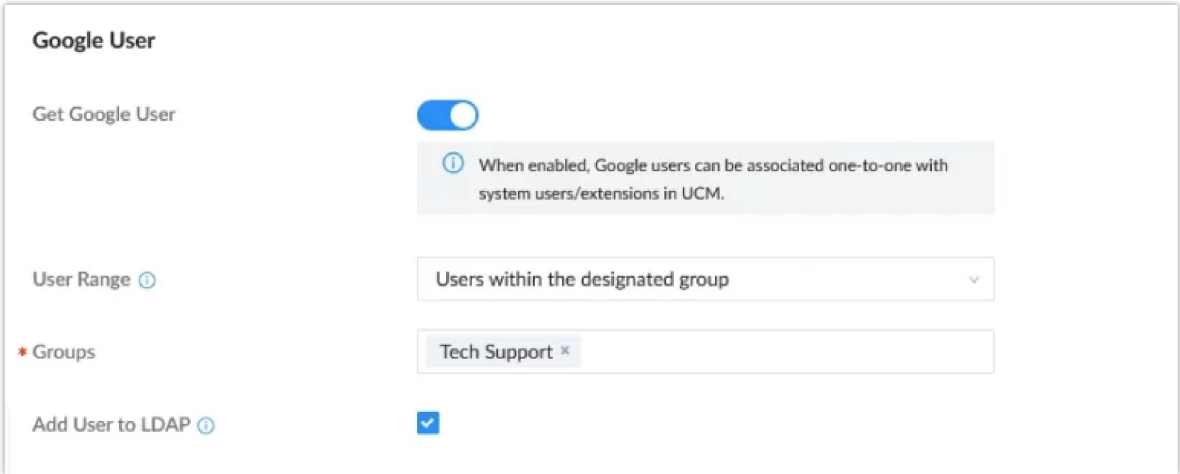
The sections below describe each of the Google Workspace user settings tab categories.



Google Workspace User Settings Tab

Google User

This section defines how Google Workspace users are retrieved from the domain and whether they are synchronized into the CloudUCM system.



User Settings Google User

Parameter	Description
Get Google User	Enables/disables retrieval of users from the connected Google Workspace domain. When enabled, Google users can be listed and managed on the CloudUCM.
User Range	Specifies the scope of Google Workspace users to retrieve. The available options are: • All Users: Retrieves all users from the Google Workspace domain. • Users within the designated organizational unit: Retrieves users from a specific Google Workspace organizational unit. • Users within the designated group: Retrieves only users who belong to one or more specified Google Workspace groups.
Organizational Unit	Specify the Google Workspace Organizational Units whose users will be retrieved.
Groups	Specify the Google Workspace Groups whose users will be retrieved.
Add User to LDAP	When enabled, retrieved Google Workspace users are synchronized into the CloudUCM LDAP directory under the "ou=google,dc=pbx,dc=com" phone book.

Linked User Settings

This section controls how Google Workspace users are associated with CloudUCM users or extensions.

Linked User Settings

Linked UCM ☒

ⓘ If enabled, the linked UCM user's information (first name, last name, email, mobile number, job title) will be overwritten by the Google user's information.

Linking Method ⓘ

☒ Automatic Link
☐ Manual Link

Link Policy ⓘ

Read Attribute Value

Attribute Name

phones

User Settings Linked User Settings

Parameter	Description
Linked CloudUCM	Enables linking between Google Workspace users and CloudUCM system users or extensions. When enabled, selected Google user attributes (such as first name, last name, email address, mobile number, and job title) can be applied to the linked CloudUCM user.
Linking Method	Defines how the association between Google users and CloudUCM users is performed: • Automatic Link: The CloudUCM automatically links Google users to existing users or extensions based on the selected link policy.

	• Manual Link: Administrators manually associate Google users with CloudUCM users or extensions from the Google User list.
Link Policy	Defines how the CloudUCM determines the target user or extension when <i>Automatic Link</i> is selected. Available options include: • Automatic Allocation: The CloudUCM automatically assigns available users or extensions to Google users. • Read Attribute Value: The CloudUCM reads a specific Google user attribute (such as extension number or mobile number) and uses it to match an existing CloudUCM user or extension.
Starting Extension	This field is displayed when <i>Link Policy</i> is set to <i>Automatic Allocation</i>. It defines the starting extension number that the CloudUCM uses when automatically assigning extensions to Google Workspace users.
Attribute Name	Displayed when <i>Read Attribute Value</i> is selected. Specifies the Google Workspace user attribute that the CloudUCM will use for automatic matching. Note: When Read Attribute Value is used for automatic linking, the CloudUCM only evaluates the <i>Work Number</i> attribute from Google Workspace users. Mobile and Home numbers are ignored for automatic binding.

Google User List

This section displays the list of retrieved Google Workspace users and provides controls for synchronization and user linking.

The screenshot displays the 'Google User' interface. At the top, there are three buttons: 'Sync Now', 'Batch Link', and 'Sync Settings'. To the right is a search bar labeled 'Mobile Number / Link UCM User'. Below these is a table with the following columns: 'User', 'First Name', 'Last Name', 'Mobile Number', 'Job Title', 'Link UCM User', and 'Options'. The table contains three rows of data:

User	First Name	Last Name	Mobile Number	Job Title	Link UCM User	Options
☐ antonio.brock@gsdevtest.com	Antonio	Brock				Link
☐ glenn.horton@gsdevtest.com	Glenn	Horton				Link
☐ angela.wright@gsdevtest.com	Angela	Wright	5000		5000	Link

At the bottom right, there is a pagination control showing 'Total: 3', a page selector with '1' selected, and '10 / page'.

User Settings Google User List

Parameter	Description
Sync Now	Immediately retrieves the latest user information from Google Workspace based on the current User Settings configuration.
Sync Settings	Opens the Google Workspace Sync Settings page, which allows configuration of automatic extension deletion policies (for deleted, paused, or unlinked Google users), scheduled synchronization, and provides visibility into synchronization history.
Batch Link	Available when Manual Link is selected. Allows multiple Google users to be linked to CloudUCM users or extensions in a single operation.
Google User List	Displays the synced google users with the following fields: 1. User (email address) 2. First Name 3. Last Name 4. Mobile Number 5. Job Title 6. Linked CloudUCM User

Note: For manually linked users, the *Options* column provides controls to link, modify, or remove the association with a CloudUCM user or extension.

The **Sync Settings** page is used to define how Google Workspace user data is synchronized with the CloudUCM and how linked extensions are handled during synchronization events. This page is accessed by clicking Sync Settings from the Google User List section.

Integration of Collaborative Office Platforms > Google Workspace > Sync Settings

Extensions

Automatically Delete Extensions of ⓘ

- ☐ Deleted Google Workspace users
- ☐ Paused Google Workspace users
- ☐ Unlinked Users

Google User Data Sync

ⓘ Data synchronization includes obtaining the latest Google users and updating the association between Google users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours.

Scheduled Sync ☐

Sync History

Sync Time	Sync Mode	Results	Options
2026-02-09 14:10:04	Manual sync	Success	ⓘ
2026-02-09 14:09:56	Manual sync	Success	ⓘ
2026-02-05 16:59:40	Manual sync	Success	ⓘ
2026-02-05 15:11:11	Manual sync	Success	ⓘ

Google Workspace Sync Settings

The **Extensions** section controls automatic cleanup behavior for CloudUCM extensions based on Google Workspace user status:

- **Deleted Google Workspace users:** Automatically deletes the linked CloudUCM extension when the corresponding Google Workspace user is deleted.
- **Paused Google Workspace users:** Automatically deletes the linked CloudUCM extension when the corresponding Google Workspace user is suspended or paused.
- **Unlinked Users:** Automatically deletes CloudUCM extensions that are no longer linked to any Google Workspace user.

Extensions

Automatically Delete Extensions of ⓘ

- ☐ Deleted Google Workspace users
- ☐ Paused Google Workspace users
- ☐ Unlinked Users

Extensions Sync Settings

The **Google User Data Sync** section controls how and when Google Workspace user data is synchronized. When **Scheduled Sync** is enabled, CloudUCM automatically retrieves the latest Google Workspace users and updates the association between Google users and CloudUCM users or extensions according to the current configuration.

Note:

Data synchronization may temporarily impact system performance. It is recommended to perform synchronization during non-office hours.

Google User Data Sync

 Data synchronization includes obtaining the latest Google users and updating the association between Google users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours.

Scheduled Sync:



Sync Time

By Day

04:00

Cancel

Save

Google User Data Sync Settings

The **Sync History** section displays historical records of Google Workspace synchronization activities. The following information is shown for each synchronization event:

- **Sync Time:** Date and time when the synchronization was executed.
- **Sync Mode:** Indicates whether the sync was triggered manually or by schedule.
- **Results:** Displays the synchronization result (Success, Partial Success, or Failed).
- **Options:** Provides access to detailed synchronization logs for troubleshooting purposes.

Sync History			
Sync Time	Sync Mode	Results	Options
2026-02-09 14:10:04	Manual sync	Success	
2026-02-09 14:09:56	Manual sync	Success	
2026-02-05 16:59:40	Manual sync	Success	
2026-02-05 15:11:11	Manual sync	Success	
2026-02-05 15:10:46	Manual sync	Partial Success	
2026-02-05 15:10:34	Manual sync	Success	
2026-02-05 15:10:30	Manual sync	Failed	
2026-02-05 15:08:56	Manual sync	Failed	

Google Workspace Sync History

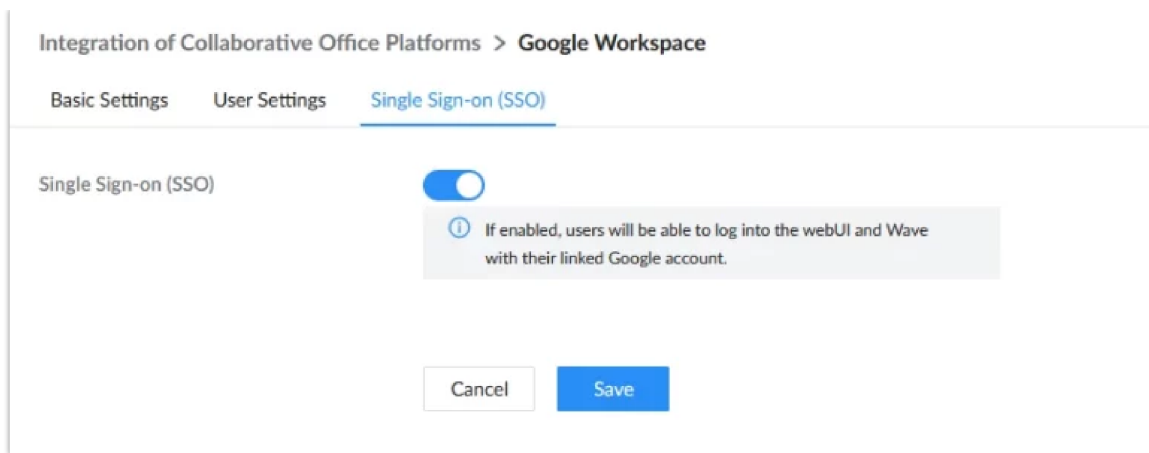
Single Sign-On (SSO)

The Single Sign-On (SSO) tab controls Google-based authentication for accessing the CloudUCM web interface.

This page is used to enable or disable Google Workspace SSO and define how Google-authenticated users are mapped to CloudUCM system users.

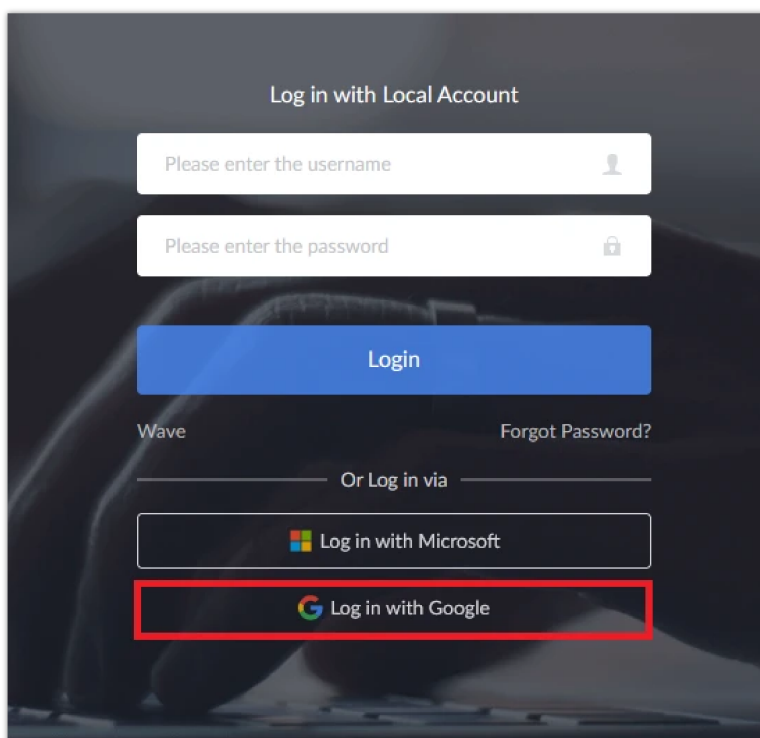
Note:

- For Google Workspace SSO to function, **at least one Google Workspace** user must be successfully linked to a CloudUCM system user. SSO authentication will fail if no linked user exists.
- Google Workspace SSO requires the CloudUCM to be accessed using **a valid domain name (FQDN)**. Accessing via a private IP address is not supported and will trigger a warning during OAuth authorization.



Google Workspace Single Sign on SSO Tab

If SSO is enabled, the Sign in with Google option will appear on the CloudUCM login page.



Log in with Google Option for CloudUCM

Detailed configuration flows, and OAuth authorization steps for Google Workspace SSO are covered in the [Google Workspace Integration Guide](#).

Wave Integration & Expansion

Wave integrations include further expansion of the UC features offered by our solutions. These expansions include integrating popular CRM solutions, like Odoo CRM, Oracle Netsuite, and Salesforce CRM, with Wave to easily manage customer relationships directly through the calls received on Wave. Other add-ins include WhatsApp Business, Office356, Google Drive, and IPVideoTalk.



Wave Add-ins — Connect Your Work

Wave can be integrated with a wide variety of services and applications, including popular CRM platforms, Whatsapp Business, Office365, Wave for Outlook, Microsoft Teams and more.

[View all Wave plugins](#)



Integrate Wave with your applications

Wave provides an SDK that opens up integration with other 3rd party software, allowing for the incorporation of audio/video calling functionality into various types of applications.

[View Wave SDK](#)

CHANGELOG

Firmware 1.0.33.10

- Added AI Generated Speech (TTS) feature for creating voice prompts directly from text. [[AI Generated Speech](#)]
- Added support for AI Voicemail to Text. [[AI Voicemail to Text](#)]
- Added support for AI Meeting Transcription & Summary. [[AI Meeting Transcription and Summary](#)]
- Added support for AI Call Transcription & Summary. [[AI Call Transcription and Summary](#)]
- Added CloudUCM Services page to display AI service status, plan validity, and detailed usage statistics [[AI Services](#)]
- Added scheduled meeting configuration with AI transcription option, allowing organizers to enable or disable AI transcription per meeting. [[Schedule Meeting](#)]
- Added AI configuration tab to SIP extensions, allowing per-extension control of Automatic AI Transcription. [[Create a New SIP Extension](#)]
- Added AI Settings (Beta) page to centrally manage AI services. [[AI Settings \(Beta\)](#)]
- Added support for multi-factor authentication using email for Wave. [[Create a New SIP Extension](#)]
- Added recording file and CDR access permission. [[Administration Privileges](#)]
- Added Wave recording indicator appearance permission. [[Wave Permissions](#)]
- Added support for configuring the pre-installed Wave add-ins. [[Pre-installed Plugins](#)]
- Added option to control Wave app Screenshot and Screen Recording permission. [[Wave Permissions](#)]
- Added ability to modify LDAP phonebooks through API. [[API Queries Supported](#)]
- Added support for proficiency-based routing as a routing strategy in the call queue. [[Add Call Queue](#)]
- Added selecting the dynamic agents which can be added to a specific call queue. [[Add Call Queue](#)]
- Added Cleaner Record and Details [[Cleaner](#)]
- Added the ability to have multiple Scheduled Backup tasks on different storage locations. [[Backup/Restore](#)]
- Added support for inbound and outbound routes batch deletion. [[Configuring Inbound Routes](#)][[Configuring Outbound Routes](#)]
- Added display of trunk status and current call count display on the VoIP Trunk page. [[VoIP Trunks](#)]
- Added outbound route total call duration limit setting. [[Configuring Outbound Routes](#)]
- Added Caller ID Transform feature on outbound routes [[Configuring Outbound Routes](#)]
- Updated the Inbound Routes→3rd Party Database Search page to align with the new third-party SQL database integration feature. [[Inbound Routes: 3rd Party Database Search](#)]

- Added support for third-party SQL database integration for phonebook lookup and synchronization. [[3rd Party Database Integration](#)]
- Added support for Bitrix24 CRM integration. [[Bitrix24 CRM](#)]
- Added configurable room types with support for day-based pricing, holiday pricing, tax rates, and hourly pricing. [[Local PMS](#)]
- Added reservation management. [[Local PMS](#)]
- Added a guest list for centralized customer profile management, including search, import/export. [[Local PMS](#)]
- Added email templates for reservation notifications, cancellation notices, and billing emails. [[Local PMS](#)]
- Added multiple check-in workflows, supporting check-in from reservation list, from room list (immediate check-in), and hourly or full-day room selection. [[Local PMS](#)]
- Added room change (house switch) functionality to move checked-in guests to another available room while preserving guest and billing data. [[Local PMS](#)]
- Added a room availability calendar with visual status indicators, booking and check-in actions, hover-based detail display. [[Local PMS](#)]
- Added bill printing with detailed room charges, minibar costs, call charges, tax breakdowns, and prepayment deductions. [[Local PMS](#)]
- Added wake-up service management with support for room group based scheduling. [[Local PMS](#)]
- Added support for self-service check-in and check-out via email for guests with valid reservations. [[Local PMS](#)]
- Added configurable email delivery timing for self-service check-in and check-out messages relative to arrival and departure times. [[Local PMS](#)]
- Added tracking of check-in and check-out methods, distinguishing between front-desk and self-service operations in history records. [[Local PMS](#)]
- Added automatic room assignment during self-service check-in when reservations are not pre-assigned to specific rooms. [[Local PMS](#)]
- Updated the Local PMS wake-up service prompt to dynamically use the language configured during room check-in. [[Local PMS](#)]
- Optimized Local PMS check-in and check-out actions to take effect immediately without requiring "Apply Changes". [[Local PMS](#)]
- Added support for configuring holidays by date or by week. [[Holiday](#)]
- Added support for Google Workspace integration to synchronize user identity information with Google Workspace. [[Google Workspace Integration](#)]
- Added Google Workspace Single Sign-On (SSO) support for CloudUCM web interface authentication. [[Google Workspace Integration](#)]
- Added support for configuring Microsoft Entra ID user synchronization scope. [[Microsoft Entra ID \(Azure AD\)](#)]
- Added unified integration tab for collaboration and identity platforms. [[Integration of Collaboration Platforms](#)]
- Added Strict Defend Mode option to Geo-IP Access Control [[Geo-IP Access Control](#)]
- Added several new call report types for various call scenarios [[Call Reports](#)]

Firmware 1.0.29.10

- Removed the extension strong password setting. A strong password policy is now enforced. [[Create a New SIP Extension](#)] [[General Settings](#)]
- Increased the maximum number of queue chairman agents to 10. [[Add Call Queue](#)]

Firmware 1.0.29.7

- Added support for data backup and archiving to third-party cloud storage (Amazon S3). [[Storage Device Management](#)]
- Added support for Call Billing. [[Call Rate](#)][[Call Charges Statistics](#)]
- Added Least Cost Routing policy to Outbound Routes. [[Carrier](#)]
- Administrators can now choose either dial plan accuracy or outbound route priority list as the criteria for call routing. [[Outgoing Routing Priority](#)]

- Added country-specific restriction in ACL. [[Geo-IP Access Control](#)]
- Added support for Microsoft Outlook SMTP OAuth2 authentication. [[Email Settings](#)]
- Added support for Microsoft Entra ID integration. [[Microsoft Entra ID \(Azure AD\)](#)]
- Added support for Windows Active Directory integration. [[Windows AD](#)]
- Added Extension Call Policy. [[Create New SIP Extension](#)]
- Added Advanced Messaging page. [[Advanced Messaging](#)]
- Added LDAP Attribute Conversion. [[LDAP Client Configuration](#)]
- Added ability to customize PAI for Emergency Calls based on individual extensions. [[Emergency Location Mapping](#)]
- Added *Premium Code* and *Premium Code Prompt* option to Call Queue settings. [[Add Call Queue](#)]
- Added option to disable RPID in the Call Queue. [[Add Call Queue](#)]
- Added prompt language configuration in Call Queue. [[Add Call Queue](#)]
- Call Queue Chairman can now view the CDR of their queues. [[Queue Switchboard Privilege](#)]
- Added support for triggering webhooks via an IVR. [[Configure IVR](#)]
- Added support for maximum concurrent call limit. [[Alert Events List](#)]
- Added TLS compression for LDAP server. [[LDAP Server Configurations](#)]
- The restore feature now supports TGZ file format. [[Backup/Restore](#)]
- The backup packages now use TGZ format by default instead of TAR. [[Backup/Restore](#)]
- Increased voicemail group members number to 150. [[Configure Voicemail Group](#)]
- Added Call Privilege to Announcement Center. [[Announcement Center Settings](#)]
- Added end time for scheduled meetings. [[Schedule Meeting](#)]
- Added "Play Joining/Leaving Meeting Announcement" which enables/disables the sound played when a user joins/leave. [[Schedule Meeting](#)]
- Meeting will now end when a GDS or GSC extensions are the only ones left in the meeting. [[During The Meeting](#)]
- Added support for automatic update of the timezone list. [[Time Zone Settings](#)]
- Added name configuration in Speed Dial. [[Speed Dial](#)]
- Administrator password, user password, and SIP password now require at least 10 characters [[Create New SIP Extension](#)] [[User Management](#)]
- Add the ability to play/hear the uploaded Prompts directly from the WebGUI. [[Custom Prompt](#)]
- Updated email template for "new messages to inactive user notification". [[Email Template](#)]
- Added "First Answer Termination" in Paging/Intercom configuration. [[Paging/Intercom Groups](#)]
- CDR now displays the name of the callee. [[CDR](#)]
- Added support for batch download of recorded files. [[Recordings](#)]
- Added ability to select the error message to display when the number of maximum concurrent calls is reached. [[VoIP Trunk Configuration](#)]
- Added option to set the maximum concurrent calls allowed by a SIP trunk. [[VoIP Trunk Configuration](#)]
- Added support for enabling/disabling sending the diversion header on a trunk. [[VoIP Trunk Configuration](#)]
- Added support for configuring the allowed API modules when adding a user. [[API Settings](#)]
- Added ability to use key pressing events when receiving a wake up call. [[Wakeup Service](#)]
- Added Oracle Hospitality OPERA PMS integration. [[Oracle Hospitality Opera](#)]
- Added support for Oracle Hospitality OPERA's Youth Hostel Mode. [[Oracle Hospitality OPERA](#)]
- Added option to set prefixes that label different types of calls for call billing purposes (Only applicable for Oracle Hospitality's OPERA PMS). [[PBX Settings](#)]
- SIP Defense and Login Attack Defense are now enabled by default. [[Fail2Ban](#)]
- Added support for manual addition of Fail2Ban blocklist entries. [[Fail2Ban](#)]
- PMS parameters have been added to list of privileges for admins. [[Custom Privilege](#)]

- Added “Allow Simultaneous Logins from the Same Client Type” Wave permission. [[User Portal/Wave Privileges](#)]
- Added “Delete message” Wave permission. [[User Portal/Wave Privileges](#)]
- Added a link to the Open Source Software License Agreement. [[Open Source License](#)]
- Import and export functions now support XLSX file format. [[Export Extensions](#)][[Import Extensions](#)]

Firmware 1.0.27.26

- Added support for Cloud IM Service. [[Cloud IM Service](#)]
- Added support to download a single decrypted recording file via the API (REC API). [[API Queries Supported](#)]

Firmware 1.0.27.22

- No major changes.

Firmware 1.0.27.19

- Added Port Access mode to Register Trunk configuration. [[VoIP Trunk Configuration](#)]
- Users can now change the default extension of the Parking Lot. [[Parking Lot](#)]

Firmware 1.0.27.18

- Added DID Access mode option to peer and register trunks, allowing for calls to be verified via specific DID mapping rather than random port mapping. [[VoIP Trunk Configuration](#)]

Firmware 1.0.27.15

- Added Support for CloudUCM GDMS configuration template. [[Creating CloudUCM Configuration Templates](#)]
- Removed “Download All” and “Batch Download” for Recordings. [[Recordings](#)]
- Added support to check Release Notes from the firmware Upgrade page. [[Upgrade](#)]
- Added support for Data/File encryption. [[Data/File Encryption](#)]
- Added support for FIDO Multi-Factor Authentication. [[Multi-Factor Authentication](#)]
- Added support for limiting the number of call queue agents through CloudUCM packages. [[Static Agents](#)]
- Added support for searching CallerID in a third-party MySQL database. [[Inbound Route: Third-party Database Search](#)]
- Added support for integration with Don't Call Me database. [[Don't Call Me Blacklist Integration](#)]
- Added support for ZRTP on the extensions level. [[Create a New SIP Extension](#)]
- Added support for ZRTP on the trunk level. [[VoIP Trunk Configuration](#)]
- Added support for enabling multiple Wave session on the same platform. [[Create New SIP Extension](#)]
- Added Task Management feature [[Task Management](#)]
- Added support for search function in LDAP server phonebooks [[LDAP Phonebook](#)]
- *Password Visibility Toggle* has been added to the Admin privilege [[Super Administrator](#)]
- Added *Merge Same Call Recordings* setting [[PBX Settings](#)]
- Added support for adding suffix to Call Forward Enable/Disable feature [[Feature Codes](#)]
- Added icons next to feature codes to indicate whether or not they can be nested by other feature codes [[Feature Codes](#)]
- Added support for Time Condition Routing [[Time Condition Routing](#)]
- Added support for Custom Time Groups [[Custom Time Groups](#)]
- Added support for custom announcement for Call Queue [[Call Queue](#)]
- Added number and percentage of transferred calls in the Call Queue Switchboard [[Switchboard](#)]
- Added Call Memory in Call Queue [[Call Queue](#)]
- Updated Wake-up Service by adding call failure notification [[Wakeup Service](#)]
- Added Wakeup Call Service Failure email template. [[Email Template](#)]
- Room status can now be modified using the API. [[API CONFIGURATION](#)]

- Odoo CRM integration has been added [[Odoo CRM](#)]
- Added custom repeating setting when scheduling meetings [[Schedule Meeting](#)]
- Added API support to retrieve recording filename [[API CONFIGURATION](#)]
- Added enable/disable setting for Paging/Intercom [[Paging/Intercom](#)]
- Added support for configuring custom agent pause reason with a custom prompt [[Global Queue Settings](#)]
- Added support for allowing multiple login session from the same platform for Wave [[Create a New SIP Extension](#)]
- UCM reboot event alerts and logs will now contain the reboot reason and the name of the user who initiated the reboot (if applicable) [[Alert Events List](#)]
- Increased members notified for Emergency Calls from 10 to 30 [[Emergency Calls](#)]

Firmware 1.0.25.25

- No major changes

Firmware 1.0.25.24

- No major changes

Firmware 1.0.25.20

- No major changes

Firmware 1.0.25.18

- Add support for UDP SIP trunk over IP addresses with random ports
- Added "Account SIP Trunk" method. [[VoIP Trunk Configuration](#)]
- Added support for downloading capture traces for analysis [[Ethernet Capture](#)]
- Added support for "TLS Key" in the Regular Debugging Module [[Ethernet Capture](#)]

Firmware 1.0.25.13

- This is the initial release