

# SoftwareUCM – User Manual

## INTRODUCTION

SoftwareUCM is a software IPPBX solution which allows deployment on bare-metal or a virtualized environment, either on-premise or on the cloud, to achieve a flexible telephony solution which meets the needs from a few users with limited telephony capacity, to a large telephony capacity. Using SoftwareUCM, the user can also benefit from multi-tenancy of the hardware and the solution, which allows an efficient use of the hardware resources and separation of processes and data.

### Info

For more information regarding the SoftwareUCM PBX license fees, please refer to the following link:  
<https://cloud.grandstream.com/softucm/plans>

## TECHNICAL SPECIFICATIONS

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

Voice/Video Capabilities	
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711, NetEQ, FEC 2.0, jitter resilience up to 50% audio packet loss
Voice and Fax Codecs	Opus, G.711 A-law/U-law, G.722, G722.1 G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38
Video Codecs	H.264, H.263, H263+, VP8
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Signaling and Control	
DTMF Methods	Inband, RFC4733, and SIP INFO
Provisioning Protocol and Plug-and-Play	Mass provisioning using AES encrypted XML configuration file, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66 multicast SIP SUBSCRIBE mDNS), eventlist between the local and remote trunk
Network Protocols	SIP, TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay (pending), IPv6, OpenVPN®
API	Full API available for third-party platform and application integration
Security	
Media Encryption	SRTP, TLS1.2, HTTPS, SSH, 802.1x
Additional Features	

<b>Multi-language Support</b>	<ul style="list-style-type: none"><li>• Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech, Turkish</li><li>• Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Polish, Portuguese, Russian, Swedish, Turkish, Ukrainian, Hebrew, Arabic, Netherlands</li><li>• Customizable language pack for voice prompt to support any other languages</li></ul>
<b>Call Center</b>	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/workload, in-queue announcement
<b>Customizable Auto Attendant</b>	Up to 5 layers of IVR (Interactive Voice Response) in multiple languages
<b>Telephony Operating System</b>	Based on Asterisk version 16
<b>Maximum Call Capacity</b>	<ul style="list-style-type: none"><li>• Up to 5000 extension users</li><li>• Up to 1000 concurrent calls</li></ul>
<b>Call Features</b>	Call park, call forward, call transfer, call waiting, caller ID, call record, call history, ringtone, IVR, music on hold, call routes, DID, DOD, DND, DISA, ring group, ring simultaneously, time schedule, PIN groups, call queue, pickup group, paging/intercom, voicemail, call wakeup, SCA, BLF, voicemail to email, fax to email, speed dial, call back, dial by name, emergency call, call follow me, blacklist/whitelist, voice conference, video conference, eventlist, feature codes, busy camp-on/ call completion, voice control, post-meeting reports, virtual fax sending/receiving.
<b>Wave App</b>	Free; Available for desktop (Windows 10+, Mac OS 10+), web (Firefox and Chrome Browsers) and mobile (Android & iOS), allows users to join UCM-hosted meetings, communicate with other users/solutions and make/receive calls using SIP accounts registered to the SoftwareUCM.
<b>Firmware Upgrade</b>	Supported by Grandstream Device Management System (GDMS), a zero-touch cloud provisioning and management system, It provides a centralized interface to provision, manage, monitor, and troubleshoot Grandstream products
<b>Internet Protocol Standards</b>	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028. RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 4582, RFC 4583, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550

# GETTING STARTED

## Installing SoftwareUCM

SoftwareUCM is designed to run in a Linux environment using the AlmaLinux distribution. It can be installed on either physical or virtual machines, offering flexibility based on the user’s requirements.

For instructions on installing SoftwareUCM on a physical machine, please refer to the guide linked below.

<https://documentation.grandstream.com/knowledge-base/softwareucm-installation-guide-usb-drive/>

SoftwareUCM also supports installation on various hypervisors. For detailed installation instructions, please refer to the corresponding guides listed in the table below:

Hypervisor	Installation Guide Link
------------	-------------------------



VMware Workstation	<a href="#">SoftwareUCM Installation Guide – VMware Workstation</a>
Oracle VirtualBox	<a href="#">SoftwareUCM Installation Guide – VirtualBox</a>
Kernel-based Virtual Machine	<a href="#">SoftwareUCM Installation Guide – KVM</a>
Hyper-V	<a href="#">SoftwareUCM Installation Guide – Hyper-V</a>
AWS	<a href="#">SoftwareUCM Installation Guide – AWS</a>

## Managing SoftwareUCM

Once SoftwareUCM is successfully installed, users can start utilizing its features and functionalities by accessing the console menu, which offers an interface that allows users to navigate through different options and commands.

For more information regarding managing softwareUCM through the console menu, please refer to the guide below:

<https://documentation.grandstream.com/knowledge-base/softwareucm-console-user-guide/>

## Accessing SoftwareUCM

To access SoftwareUCM, users need to retrieve the login information from the console by using the “List SoftwareUCMs” option.

```
Please enter select:
[1] List SoftwareUCMs
[2] Create SoftwareUCM.
[3] Delete SoftwareUCM.
[4] Restart SoftwareUCM.
[5] Network Settings.
[6] Show Resource Usage.
[7] Change Resource Limit.
[8] Reset Factory Password.
[9] Factory Reset.
[0] Exit.
1

Current Mode: Single Tenant

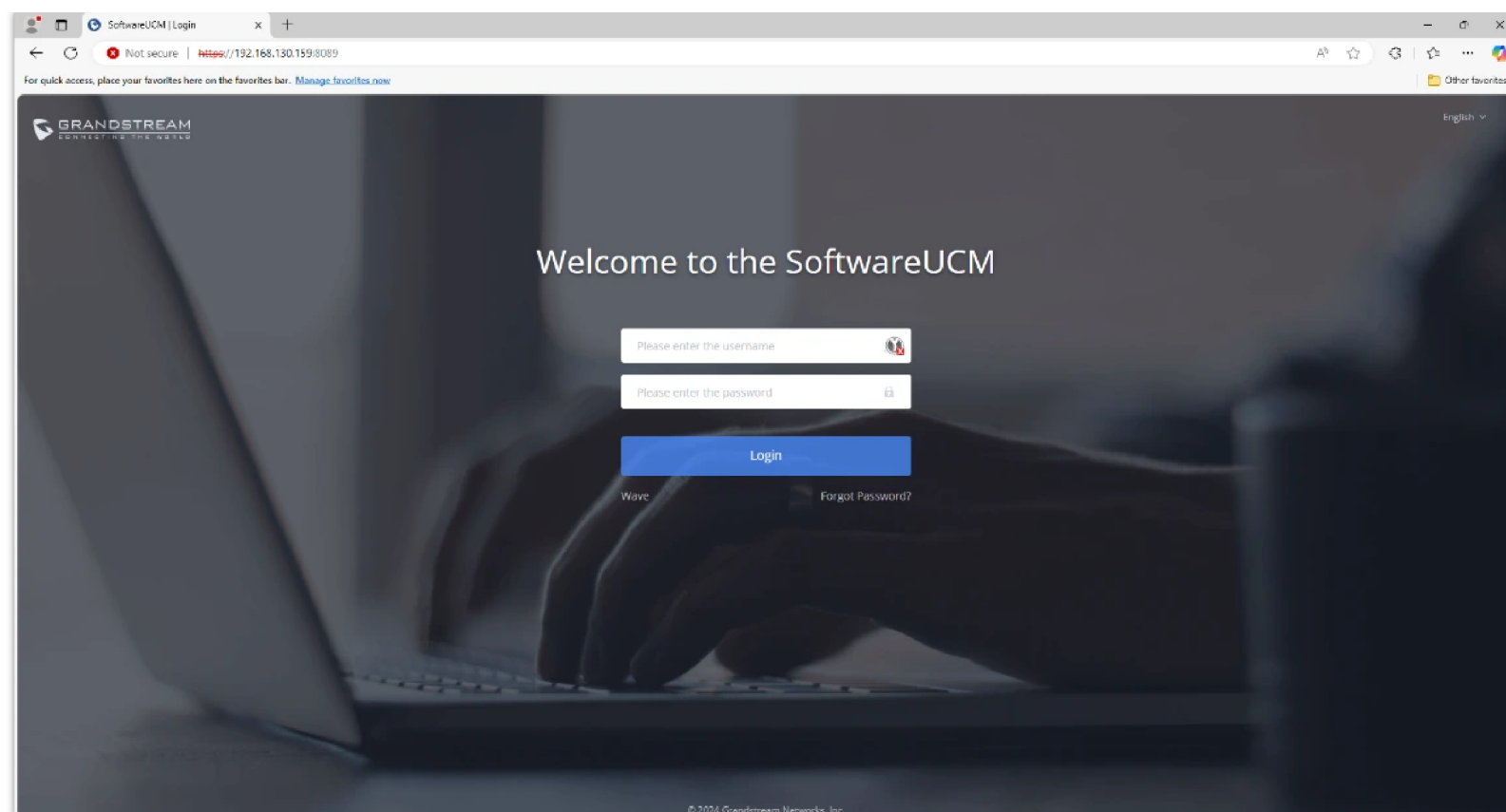
SoftwareUCM Information:
  Instance Name: ucml
  Status: running
  Version: 1.0.27.15
  Admin Portal: https://192.168.130.159:8089
  Initial Username: admin
  Initial Password: SoftUCM@admin
```

List SoftwareUCM Information

Users can enter the IP address, and login to the SoftwareUCM instance using the **initial username** and **password** displayed in the console.

**Note:**

If the instance did not get assigned an IP address, “**Admin Portal**” will appear blank.



SoftwareUCM Login Page

## Trial Period Activation

The steps below outline the process of applying for a trial period for the SoftwareUCM. The trial period is available for the base package which offers 50 user extensions and a maximum of 24 concurrent calls.

### Note

Applying for a trial period can only be done through online activation.

1. Log into the SoftwareUCM. Read the license agreement and makes sure you understand all the terms and conditions of using SoftwareUCM. To proceed, the user should agree to the terms and conditions of use.

## GRANDSTREAM SoftwareUCM LICENSE AGREEMENT

THIS Software UCM LICENSE AGREEMENT AND ALL DOCUMENTS INCORPORATED BY REFERENCE (COLLECTIVELY, THE "**AGREEMENT**") IS A LEGAL CONTRACT BETWEEN YOU ("**YOU**" OR "**CUSTOMER**," EITHER AN INDIVIDUAL OR THE ENTITY ON WHOSE BEHALF YOU ARE EXECUTING THIS AGREEMENT) AND GRANDSTREAM NETWORKS, INC. ("**WE**", "**US**", "**GRANDSTREAM**") WHICH GOVERNS THE DOWNLOAD, INSTALLATION AND USE OF THE GRANDSTREAM SOFTWARE (THE "**SOFTWARE**") AS DESCRIBED HEREIN. YOU AND US ARE ALSO COLLECTIVELY REFERRED TO AS THE PARTIES. BY DOWNLOADING, INSTALLING, USING OR BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THIS AGREEMENT. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SOFTWARE. THIS AGREEMENT IS EFFECTIVE AS OF THE DATE OF YOUR ACCEPTANCE OF THIS AGREEMENT.

THIS SOFTWARE IS BEING LICENSED AND NOT SOLD TO YOU. GRANDSTREAM PERMITS YOU TO DOWNLOAD, INSTALL AND USE THE SOFTWARE ONLY IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT.

**1. DEFINITIONS.** Capitalized terms not otherwise defined herein have the meanings set forth below:

**"Affiliate"** means, with respect to any person or entity, any other person or entity that directly or indirectly Controls or is Controlled by or under common control with such person or entity, from time to time, but only for so long as such Control exists. "Control" and its grammatical variants means (i) a general partnership interest in a partnership, or (ii) the beneficial ownership of a majority of the outstanding equity entitled to vote for directors.

**"Authorized User"** means any individual (employees, agents and contractors) of Customer acting on Customer's behalf in the operation of Customer's own business to whom Grandstream has issued a password, license key or other authorization to create a user account to access and use the Software. All Authorized Users from You and/or Your Affiliates who have identifiers listed as users of the Software are included in aggregate in the total number of Authorized Users.

**"Documentation"** means all manuals and end user documentation regarding the proper installation and use of the Software that Grandstream makes available either in paper or electronic form or on its website. Documentation may include the **"Grandstream API"** which refers to the documentation, set of instructions and functionality included with the Software which may enable the interaction between the Software and Customer's applications or data.

**"Evaluation License"** means the right to use the Licensed Products in accordance with Section 3.1.

**"Licensed Product"** means the Software and Documentation.

**"License Term"** means the term of the license for a specific Licensed Product, as set forth on an Order Form and as further described in Section 6.

SoftwareUCM License Agreement

2. Click on “free trial” to access the trial application page.

SoftwareUCM

admin

Learn about SoftwareUCM

SoftwareUCM Service Plan Activation

Online

Offline

ⓘ Make sure the device has access to the public network.

1

📄 Obtain license file from equipment agent/reseller or apply for a [free trial](#)

2

📁 Upload license file

📁 Upload

3

🕒 Waiting for the system to validate online

4

✅ Complete activation

© 2025 Grandstream Networks, Inc.

SoftwareUCM Service Plan Activation

3. Fill the necessary information in the trial application form.

GDMS

Apply for SoftwareUCM Free Trial Package

Firmware version: 1.0.27.17

Plan Information

Trial Plan ⓘ

Trial Duration

30 Days

\* Email


Used to receive device license files

Superior Channel

Company name of the parent channel

Purpose of Apply Trial

\* Captcha



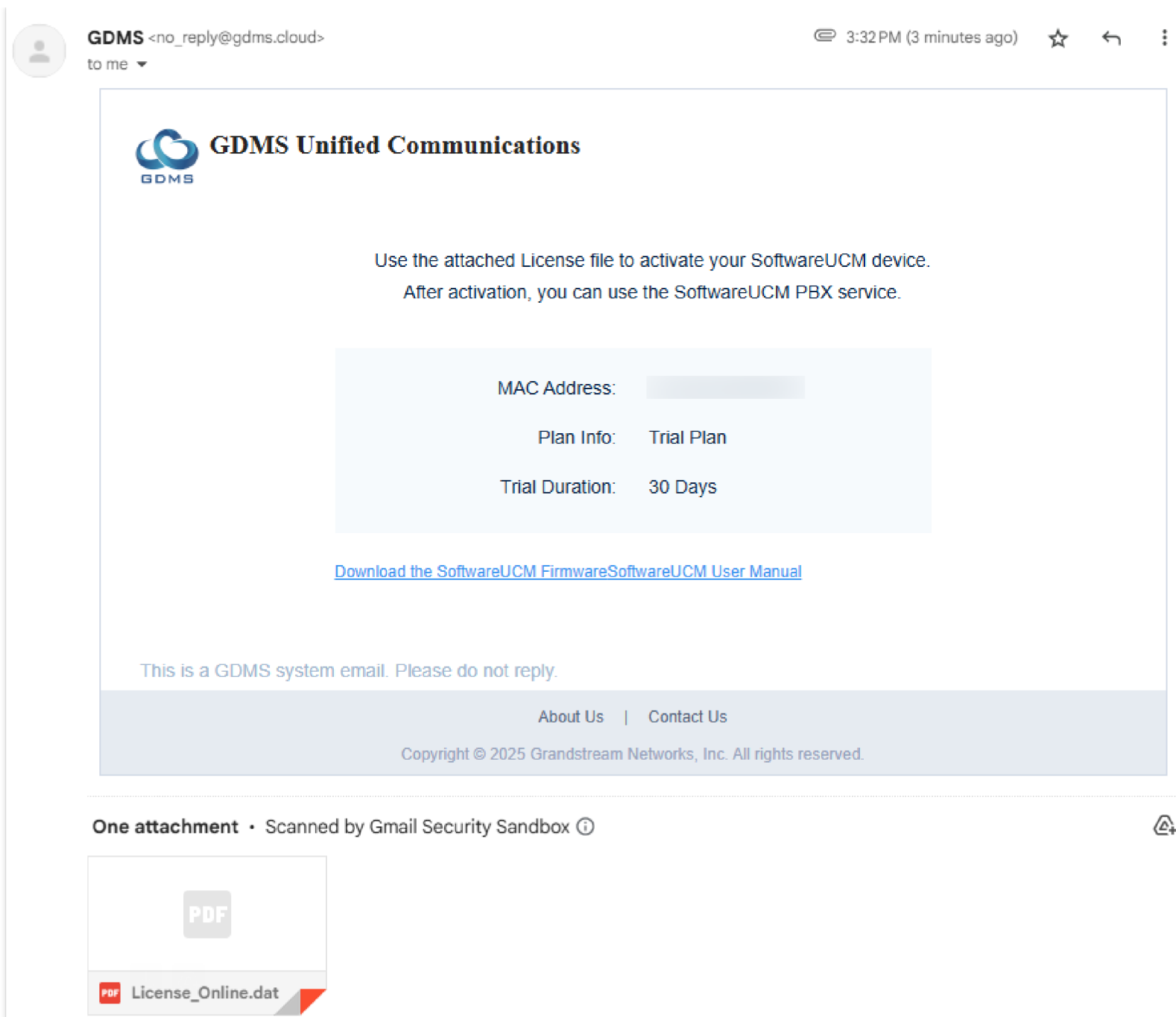
Apply

© 2025 Grandstream Networks, Inc. | English

Privacy Statement | Terms of Service | Cookies

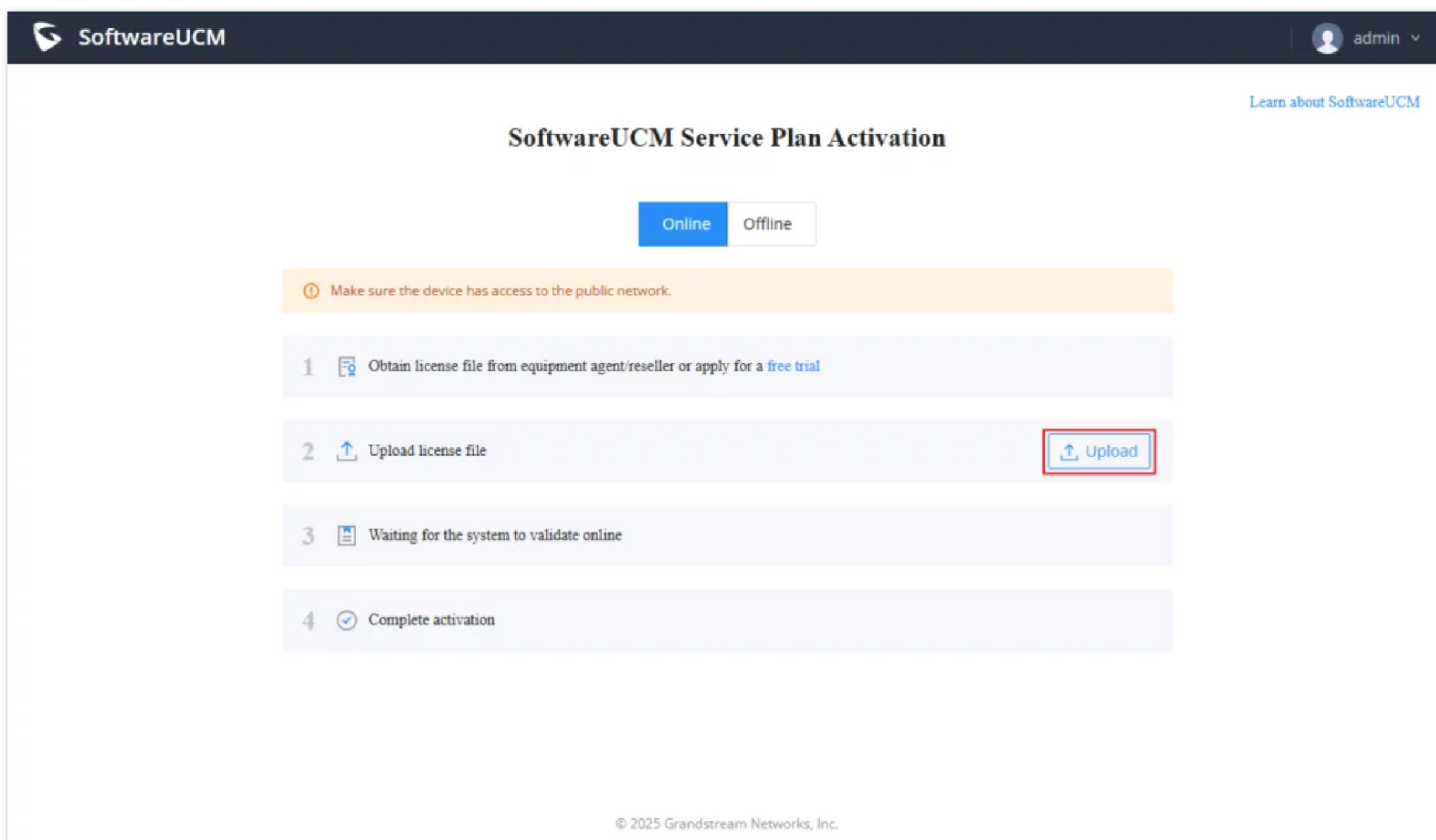
Trial Period Form

4. Access your email inbox and find the email which contains the license file. Once found, download the file from the attachment.



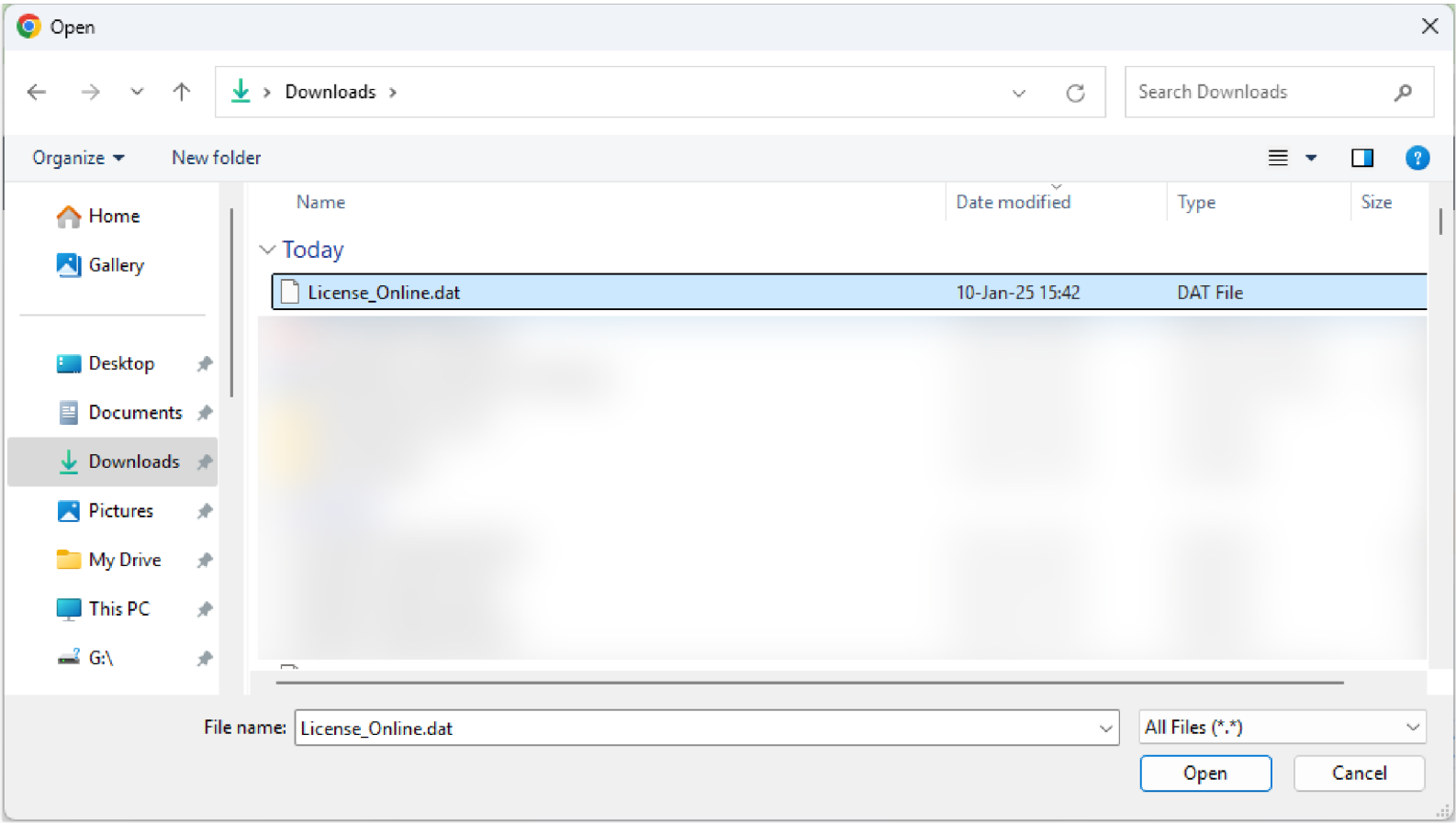
License Email

5. On the SoftwareUCM interface, click on “Upload” to add the license file.



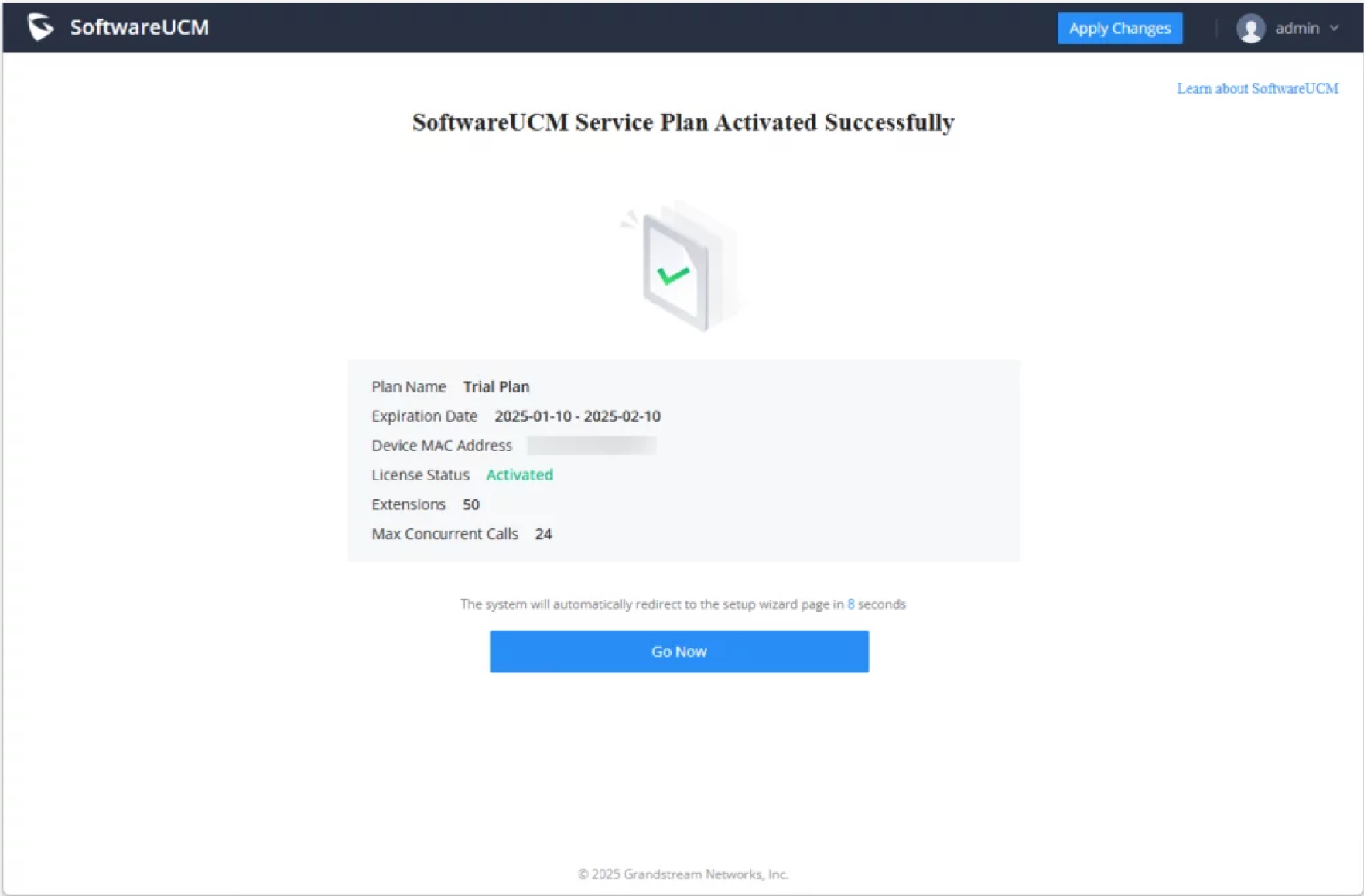
Upload Trial License

6. On the file browser, select the location where the license file is stored then upload it to the SoftwareUCM.



File Explorer

7. When the license file is added, the following page will be displayed showing information regarding the SoftwareUCM, the activation date and the expiration date of the trial, in addition to the package information.

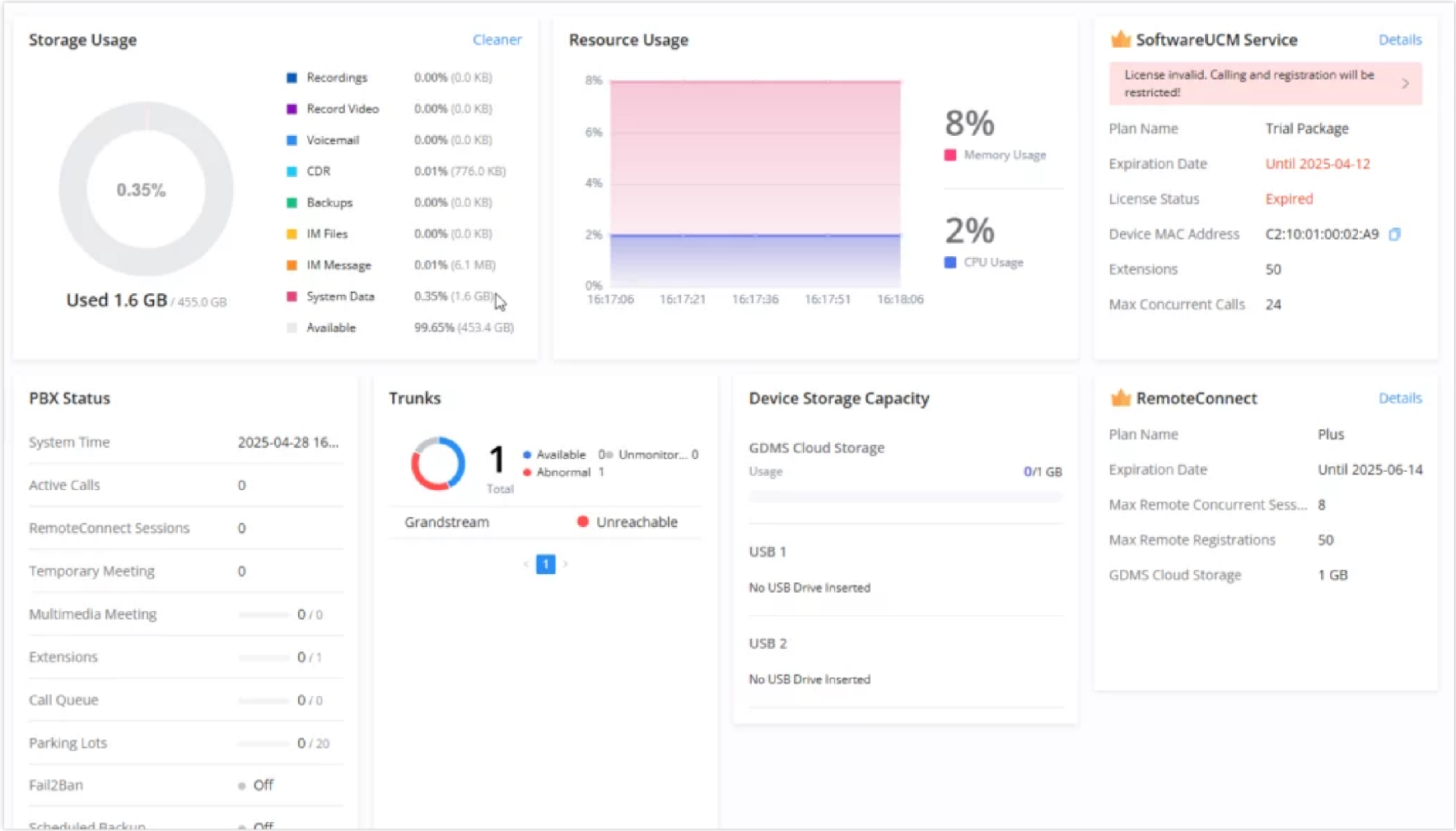


Trial Period Activated

# SYSTEM STATUS

## Dashboard

- Storage Usage
- Resource Usage
- SoftwareUCM Service
- PBX Status
- Trunks



SoftwareUCM Dashboard

System Information

Under this section, the user can view the information related to the system’s hardware and software.

System Information	
General	Network    Remark
System Information	
Model	SoftwareUCM
Device MAC Address	
Serial Number	
System Time	2024-12-23 17:38:59 UTC+01:00
Up Time	08:04:19
Version Information	
Wave Web	1.0.27.10
Program	1.0.27.13

System Information – General



System Information

General

Network

Remark

LAN

MAC Address

IPv4 Address

192.168.6.186

Gateway

192.168.6.1

Subnet Mask

255.255.255.0

DNS Server

192.168.6.1,8.8.8.8

Duplex Mode

Full Duplex

Speed

1000Mbps

System Information – Network

System Information

General

Network

Remark

Remark

SoftwareUCM\_MA

Cancel

Save

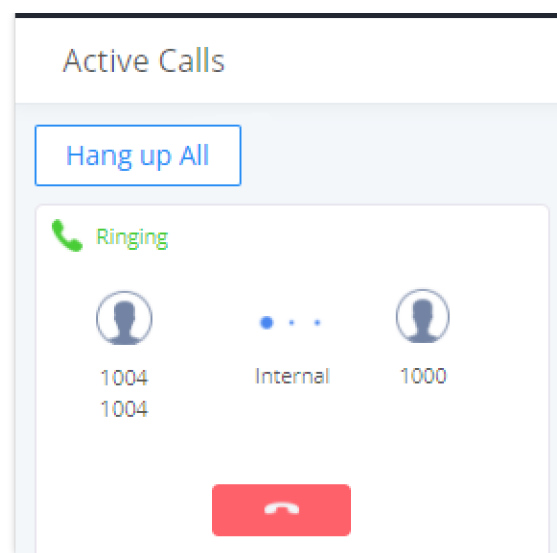
Remark

Active Calls

The active calls on the SoftwareUCM 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.

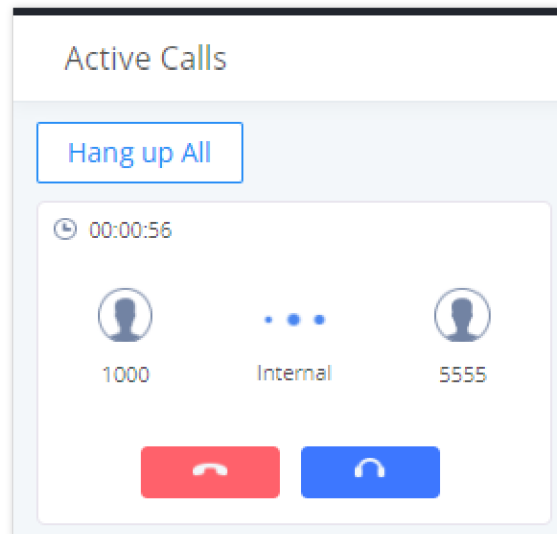
Active Calls Status

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.



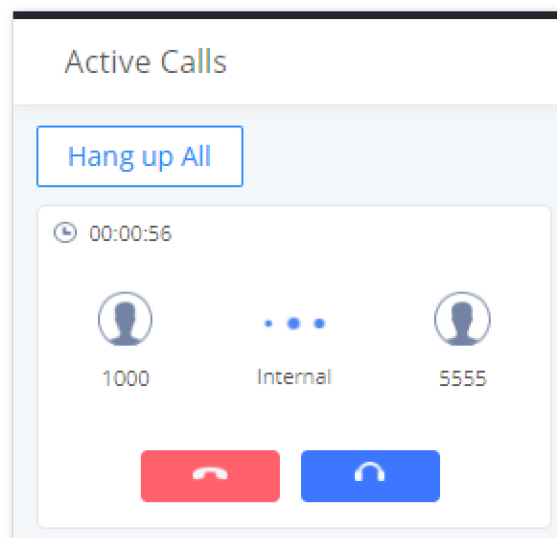
*Active Calls – Ringing Status*

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



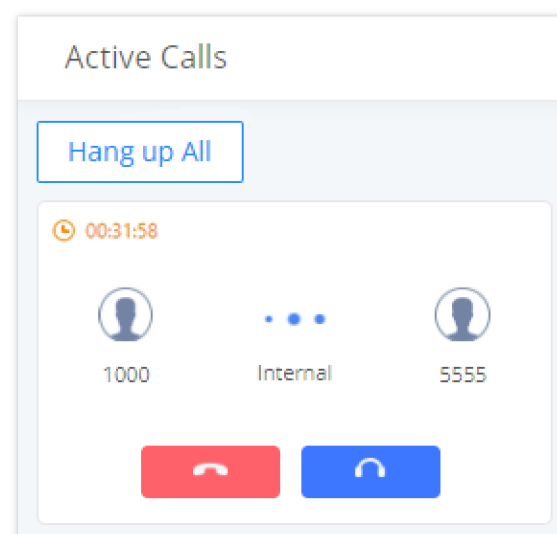
*Active Call – Established Status*

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



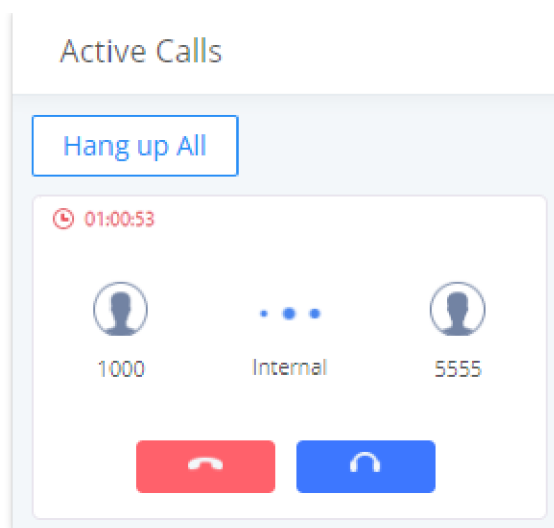
*Active Short-length Call*

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



*Active Medium-length Call*

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



Active Long-length Call

## Setup Wizard

When you log in to the SoftwareUCM 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. The setup wizard cannot be skipped and needs to be completed to access the configuration page of the SoftwareUCM.

The first step of the setup wizard is to configure the user settings, in this step, it's mandatory to configure a new password for the super administrator, and to configure an email address.

The user can also enable file encryption per type of file.

The screenshot shows the "Setup Wizard" interface. At the top, there is a progress bar with six steps: 1. User Settings (active), 2. Network Settings, 3. Time/Prompt Language, 4. Extensions, 5. Trunks/Routes, and 6. Summary. Below the progress bar, the "User Settings" section contains four input fields: "Enter New Username", "Enter New Password" (marked with a red asterisk), "Re-enter New Password" (marked with a red asterisk), and "Email Address" (marked with a red asterisk). Below these fields is the "Security Settings" section, which includes a "Data/File Encryption" label and several checkboxes: "All", "Config File" (checked), "IM Files" (checked), "IM Message", "Recording Files", "Video Recording Files", and "Voicemail". At the bottom left of the form, there is a blue "Next" button.

Setup Wizard

On the second step, the user can configure the networking settings of the device. This includes the Maximum Transmission Unit (MTU) and the IP acquisition method.

Setup Wizard

✓ User Settings

2 Network Settings

3 Time/Prompt Language

4 Extensions

5 Trunks/Routes

6 Summary

Network Settings

ⓘ

Modifying network settings will reboot the device so please be mindful. If the device's IP address was changed, please access the device using the new IP address after reboot.

MTU

1500

Preferred DNS Server

LAN

IP Method

DHCP

Previous

Next

Reset

Network Settings

In the third step, the user can configure the time zone, date format, time format, and prompt language.

Setup Wizard

✓ User Settings

✓ Network Settings

3 Time/Prompt Language

4 Extensions

5 Trunks/Routes

6 Summary

Time/Prompt Language

★ Time Zone

( UTC+01:00 ) Etc/GMT-1

Date Format

yyyy-mm-dd

Time Format

Use 24-hour Format

Prompt Language

English : en

中文 : zh

British English : en\_GB

Deutsch : de

Español : es

Español(Català) : es\_ca

Previous

Next

© 2024 Grandstream Networks, Inc.

Time/Prompt Language

On the fourth step, the user can create a batch of extensions. The user can also configure a SIP password and a user/Wave password which can be initially used to register, or to log into the extension, respectively.

SoftwareUCM

admin

Setup Wizard

✓ User Settings

✓ Network Settings

✓ Time/Prompt Language

4 Extensions

5 Trunks/Routes

6 Summary

Extensions

Can only set SIP extensions.

Enable Extension Range ☒

To modify the extension number range 1000-6299, go to the **PBX Settings** -> **General Settings** page to modify the "User Extensions" range after completing the Setup Wizard.

Start Extension

1000

Create Number

5

SIP Password

☒ Use Random Password

☐ Use Password

User/Wave Password

TLsRuoQ\*e5

Previous

Next

Skip

Extensions

On the fifth step, the user can configure and create initial trunk and route configuration.

Setup Wizard

✓ User Settings

✓ Network Settings

✓ Time/Prompt Language

✓ Extensions

5 Trunks/Routes

6 Summary

Trunks/Routes

+ Add

Trunk Type	Trunks	Outbound Rule	Inbound Rule	Options
<div><div></div><div>No data</div></div>				

Previous

Next

Skip

Trunks/Routes

On the sixth step, the user can view a summary of all the configuration which has been set in the previous steps.

Setup Wizard

✓

User Settings

✓

Network Settings

✓

Time/Prompt Language

✓

Extensions

✓

Trunks/Routes

6

Summary

Summary

User Settings

New Username

Email Address

Network Settings

ⓘ

Modifying network settings will reboot the device so please be mindful. If the device's IP address was changed, please access the device using the new IP address after reboot.

MTU1500

Preferred DNS Server

LAN

Previous

Save

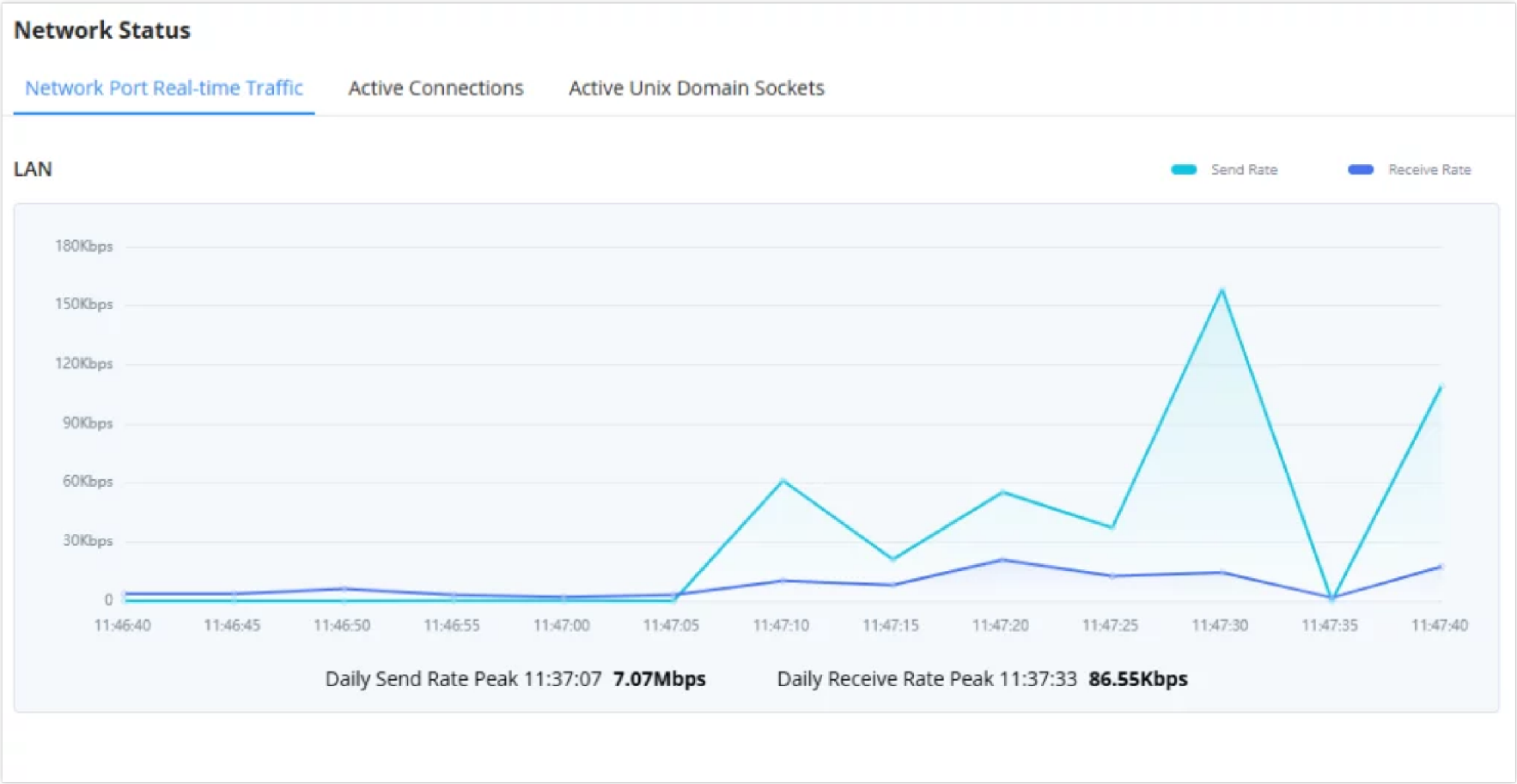
Summary

Network Status

In this page, the user can view information regarding the network status of the SoftwareUCM such as the network interfaces of the SoftwareUCM, the network traffic activity in each network interface.

Network Port Real-time Traffic

In Network Port Real-time Traffic page, the user can view the volume of the traffic exchanges in the SoftwareUCM. The volume of the traffic depends on the number of calls, the codecs used, and the services configured on the SoftwareUCM.





Network Status					
Network Port	Real-time Traffic	Active Connections	Active Unix Domain Sockets		
Proto	Recv-Q	Send-Q	Local-Address	Foreign-Address	State
tcp	0	0	0.0.0.0:3510	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:123	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:7777	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8440	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8441	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8439	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:1999	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:2001	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:2002	0.0.0.0:*	LISTEN
Total: 65 < 1 2 3 4 5 6 7 > 10 / page Goto					

Active Connections

Active Unix Domain Sockets

In this page, the user can view the active unix domain socket connections. These connections are related only to internal process communication.

Network Status					
Network Port	Real-time Traffic	Active Connections	Active Unix Domain Sockets		
Proto	RefCnt	Flags	Type	State	I-Node
unix	2	[ACC]	STREAM	LISTENING	110727
unix	2	[ACC]	STREAM	LISTENING	110730
unix	2	[ACC]	STREAM	LISTENING	110730
unix	2	[ACC]	STREAM	LISTENING	110730
unix	2	[ACC]	STREAM	LISTENING	110731
unix	2	[ACC]	STREAM	LISTENING	110725
unix	2	[ACC]	STREAM	LISTENING	110731
unix	2	[ACC]	STREAM	LISTENING	110731
unix	2	[ACC]	STREAM	LISTENING	110725
unix	3	[]	DGRAM	CONNECTED	14735
Total: 244 < 1 2 3 4 5 ... 25 > 10 / page Goto					

Active Unix Domain Sockets

EXTENSION/TRUNK

Extensions

Create a New SIP Extension

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

Extensions > Edit Extension: 1000

Basic Settings

Media

Features

Voicemail

Specific Time

Wave Client

Follow Me

Advanced Settings

General

\* Extension

1000

CallerID Number

\* Call Privileges

Local

\* SIP Password

\*\*\*\*\*

AuthID

\* Concurrent Registrations

3

Disable This Extension

☐

User Settings

First Name

Last Name

Email Address

\* User Portal/Wave Privileges

Default

\* User/Wave Password

\*\*\*\*\*

Add / Edit Privileges

Mobile Number

+1

Department

---

Job Title

Contact Privileges

Cancel

Save

Create New Extension

Extension options are divided into five categories:

- Basic Settings
- Media
- Features
- Voicemail
- Custom Time
- 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”. <b>Note:</b> Users need to have the same level as or higher level than an outbound rule’s privilege to make outbound calls using this rule.
SIP Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purposes.

<b>Concurrent Registrations</b>	The maximum endpoints which can be registered into this extension. For security concerns, the default value is 3. <b>Note:</b> When this option is set to “1(seize)”
<b>Auth ID</b>	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
<b>Disable This Extension</b>	If selected, this extension will be disabled on SoftwareUCM. <b>Note:</b> The disabled extension still exists on the PBX but cannot be used on the end device.
<b>User Settings</b>	
<b>First Name</b>	Configure the first name of the user. The first name can contain characters, letters, digits, and _.
<b>Last Name</b>	Configure the last name of the user. The last name can contain characters, letters, digits, and _.
<b>Email Address</b>	Fill in the Email address for the user. Voicemail will be sent to this Email address.
<b>User/Wave Password</b>	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purposes.
<b>Mobile Number</b>	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.
<b>Department</b>	Configure the user’s department. The department can be configured in User Management->Address Book Management->Department Management. <b>Job Title:</b> The user’s department position.
<b>Job Title</b>	Enter the job title of the user of the extension.
<b>Contact Privileges</b>	
<b>Same as Department Contact Privileges</b>	When enabled, The extension will inherit the same privilege attributed to the department it belongs to.
<b>Contact View Privileges</b>	Select the privileges regarding the contact view in SIP endpoints and Wave.
<b>Sync Contact</b>	If enabled, this extension will be displayed in SoftwareUCM 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*

<b>General</b>	
<b>NAT</b>	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is a one-way audio issue, usually it is related to NAT configuration or the Firewall's support of SIP and RTP ports. The default setting is enabled.
<b>Enable Direct Media</b>	By default, the PBX will route the media streams from SIP endpoints through itself. If this option is enabled, the PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. <b>Note:</b> It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing.
<b>DTMF Mode</b>	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

	<p>selected, RFC4733 will be used if offered, otherwise "Inband" will be used.</p> <p><b>Note:</b> The default DTMF mode selected is RFC4733.</p>
<b>TEL URI</b>	<p>If the phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. The “User=Phone” parameter will be attached to the Request-Line and “TO” header in the SIP request to indicate the E.164 number. If set to “Enable”, “Tel” will be used instead of “SIP” in the SIP request.</p>
<b>Alert-Info</b>	<p>When present in an INVITE request, the alert-Info header field specifies an alternative ring tone to the UAS.</p>
<b>Enable T.38 UDPTL</b>	<p>Enable or disable T.38 UDPTL support.</p>
<b>TURN Relay</b>	<p>Enable this option if the following are true:</p> <ol style="list-style-type: none"><li>1. PBX is deployed on a private network.</li><li>2. There are remote endpoints outside the PBX's network registering to it via its public IP address.</li><li>3. The network's firewall is not configured for media port forwarding.</li><li>4. Media NAT penetration is required.</li></ol> <p>Once a TURN server is configured, media will be forwarded to it. This configuration does not affect endpoints that are registered via the PBX's RemoteConnect address.</p>
<b>Codec Preference</b>	<p>Select audio and video codec for the extension. The available codecs are: <b>PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p, RTX and VP8.</b></p>
<b>QoS</b>	
<b>Jitter Buffer</b>	<p>Select the jitter buffer method.</p> <ul style="list-style-type: none"><li>● <b>Disable:</b> Jitter buffer will not be used.</li><li>● <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of "jitter buffer size")</li><li>● <b>Adaptive:</b> Jitter buffer with an adaptive size (no more than the value of "max jitter buffer").</li><li>● <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.</li></ul>
<b>Packet Loss Retransmission</b>	<p>Configure to enable Packet Loss Retransmission.</p> <ul style="list-style-type: none"><li>● <b>NACK</b></li><li>● <b>NACK+RTX(SSRC-GROUP)</b></li><li>● <b>OFF</b></li></ul>
<b>Video FEC</b>	<p>Check to enable Forward Error Correction (FEC) for Video.</p>
<b>Audio FEC</b>	<p>Check to enable Forward Error Correction (FEC) for Audio.</p>
<b>Silence Suppression</b>	<p>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.</p>
<b>FECC</b>	<p>Configure to enable Remote Camera Management.</p>
<b>RTP Encryption</b>	
<b>SRTP</b>	<p>Enable SRTP for the call. The default setting is disabled.</p> <ul style="list-style-type: none"><li>● <b>Disabled</b></li><li>● <b>Enabled and Enforced:</b> SRTP will be necessary to transmit media traffic. If the IP phone of this extension has SRTP disabled, calls cannot be established.</li><li>● <b>Optional:</b> The PBX will negotiate whether to use SRTP or not. If the SIP endpoint has SRTP enabled, SRTP will be used. If it is disabled, SRTP will not be used.</li></ul>

<b>SRTP Crypto Suite</b>	<p>SRTP encryption suite used by the PBX for outbound calls. Priority is based on order of configuration. The following encryption alogrithms can be used to encrypt an RTP stream.</p> <ul style="list-style-type: none"><li>• AES_CM_128_HMAC_SHA1_80 (This is the default algorithm used)</li><li>• AES_256_CM_HMAC_SHA1_80</li><li>• AEAD_AES_128_GCM</li><li>• AEAD_AES_256_GCM</li></ul>
<b>ZRTP Encryption Mode</b>	<p>ZRTP, also known as Media Path Key Agreement for Secure RTP, is an encryption protocol which allows negotiating the encryption key for RTP traffic. ZRTP uses Diffie-Hellman exchange to establish an encrypted and secure connection between the PBX and the SIP endpoint.</p> <p>If the SIP endpoint has both SRTP and ZRTP enabled, ZRTP will always be prioritized.</p>

*SIP Extension Configuration Parameters > Media*

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

	<p>‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period.</li><li>• Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li><li>• Office Time and Holiday could be configured on page <b>System Settings</b>»<b>Time Settings</b>»<b>Office Time/Holiday</b> page.</li></ul>
<b>Call Forward Busy</b>	<p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"><li>• <b>“None”</b>: Call forward deactivated.</li><li>• <b>“Extension”</b>: Select an extension from the dropdown list as CFB target.</li><li>• <b>“Custom Number”</b>: Enter a customer number as a target. For example: *97</li><li>• <b>“Voicemail”</b>: Select an extension from the dropdown list. Incoming calls will be forwarded to the voicemail of the selected extension.</li><li>• <b>“Ring Group”</b>: Select a ring group from the dropdown list as CFB target.</li><li>• <b>“Queues”</b>: Select a queue from the dropdown list as CFB target.</li><li>• <b>“Voicemail Group”</b>: Select a voicemail group from dropdown list as CFB target.</li><li>• <b>Custom Prompt</b>:</li></ul> <p>The default setting is <b>“None”</b>.</p>
<b>CFB Time Condition</b>	<p>Select time condition for Call Forward Busy. The available time conditions ‘All’, ‘Office Time’, ‘Out of Office Time’, ‘Holiday’, ‘Out of Holiday’, ‘Out of Office Time or Holiday’, ‘Office Time and Out of Holiday’, ‘Specific Time’, ‘Out of Specific Time’, ‘Out of Specific Time or Holiday’, ‘Specific Time and Out of Holiday’.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period.</li><li>• Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li><li>• Office Time and Holiday could be configured on page System Settings»Time Settings»Office Time/Holiday page.</li></ul>
<b>Do Not Disturb</b>	<p>If Do Not Disturb is enabled, all incoming calls will be dropped. All call forward settings will be ignored.</p>
<b>DND Time Condition</b>	<p>Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday”, and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"><li>• “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period.</li><li>• Specific time can be configured under the Specific Time section. Scroll down the add Time Condition for a specific time.</li></ul> <p>Office Time and Holiday could be configured on page <b>System Settings</b>»<b>Time Settings</b>»<b>Office Time/Holiday</b> page.</p>
<b>DND Whitelist</b>	<p>If DND is enabled, calls from the whitelisted numbers will not be rejected. Multiple numbers are supported and must be separated by new lines. Pattern matching is supported.</p> <ul style="list-style-type: none"><li>• <b>Z</b> match any digit from 1-9.</li><li>• <b>N</b> match any digit from 2-9.</li><li>• <b>X</b> match any digit from 0-9.</li></ul>
<b>FWD Whitelist</b>	<p>Calls from users in the forward whitelist will not be forwarded. Pattern matching is supported.</p> <ul style="list-style-type: none"><li>• <b>Z</b> match any digit from 1-9.</li><li>• <b>N</b> match any digit from 2-9.</li><li>• <b>X</b> match any digit from 0-9.</li></ul>
<b>CC Settings</b>	
<b>Enable CC</b>	<p>If enabled, SoftwareUCM will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, it is disabled.</p>
<b>CC Mode</b>	<p>Two modes for Call Completion are supported:</p>



	<ul style="list-style-type: none"> <li>● <b>Normal:</b> This extension is used as an ordinary extension.</li> <li>● <b>For Trunk:</b> This extension is registered from a PBX.</li> </ul> <p>The default setting is “Normal”.</p>
<b>CC Max Agents</b>	<p>Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel can make.</p> <p>The minimum value is 1.</p>
<b>CC Max Monitors</b>	<p>Configure the maximum number of monitor structures that may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time.</p> <p>The minimum value is 1.</p>
<b>Ring Simultaneously</b>	
<b>Ring Simultaneously</b>	<p>Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as the caller ID number.</p>
<b>External Number</b>	<p>Set the external number to ring simultaneously. ‘-’ is the connection character that will be ignored.</p> <p>This field accepts only letters, numbers, and special characters + = * #.</p>
<b>Time Condition for Ring Simultaneously</b>	<p>Ring the external number simultaneously along with the extension based on this time condition.</p>
<b>Use callee DOD on FWD or RS</b>	<p>Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.</p>
<b>Monitor Privilege Control</b>	
<b>Call Monitoring Whitelist</b>	<p>Add members from “Available Extensions” to “Selected Extensions” so that the selected extensions can spy on the used extension using feature code.</p>
<b>Allow Operator Panel Monitoring</b>	<p>Configure whether this extension can be monitored by the Operator Panel administrator.</p>
<b>Seamless Transfer Privilege Control</b>	
<b>Allowed Seamless Transfer</b>	<p>Any extensions on SoftwareUCM 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.</p>
<b>PMS Remote Wakeup Whitelist</b>	
<b>Select the extensions that can set wakeup service for other extensions</b>	<p>Selected extensions can set a PMS wakeup service for this extension via feature code.</p>
<b>Other Settings</b>	
<b>Ring Timeout</b>	<p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on SoftwareUCM. The valid range is between 5 seconds and 600 seconds.</p> <p><b>Note:</b> If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
<b>Auto Record</b>	<p>Enable automatic recording for the calls using this extension. The default setting is disabled. The recordings can be accessed under <b>Web GUI</b>→<b>CDR</b>→<b>Recording Files</b>.</p>
<b>Skip Trunk Auth</b>	<ul style="list-style-type: none"> <li>● If set to “yes”, users can skip entering the password when making outbound calls.</li> <li>● If set to “By Time”, users can skip entering the password when making outbound calls during the selected time condition.</li> <li>● If set to “No”, users will be asked to enter the password when making outbound calls.</li> </ul>
<b>Time Condition for Skip Trunk Auth</b>	<p>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.</p>
<b>Dial Trunk Password</b>	<p>Configure personal password when making outbound calls via the trunk.</p>
<b>Support Hot-Desking Mode</b>	<p>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</p>

	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 valide tange is from 1 to 20. The default value is 5.
Enable Auto-Answer Support	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
Call Waiting	Allows calls to the extension even when it is already in a call. This only works if the caller is directly dialing the extension. If disabled, the CC service will take effect only for unanswered and timeout calls.
Stop Ringing	If enabled, when the extension has concurrent registrations on multiple devices, upon incoming call or meeting invite ringing, if one end device rejects the call, the rest of the devices will also stop ringing. By default, it’s disabled.
Email Missed Call Log	If enabled, the log of missed calls will be sent to the extension’s configured email address.
Missed Call Type	If <b>Email Missed Calls</b> enabled, users can select the type of missed calls to be sent via email, the available types are: <ul style="list-style-type: none"><li>● <b>Default:</b> All missed calls will be sent in email notifications.</li><li>● <b>Missed Internal Call:</b> Only missed local extension-to-extension calls will be sent in email notifications.</li><li>● <b>Missed External Call:</b> Only missed calls from trunks will be sent in email notifications.</li></ul>
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

Voicemail	<p>Choose whether to enable or disable the voicemail feature. Using this option, the user can select the location of the storage of the voicemail.</p> <ul style="list-style-type: none"><li>● <b>Disable:</b> Disables voicemail entirely.</li><li>● <b>Local Voicemail:</b> Enable local voicemail.</li></ul>
-----------	---

	<ul style="list-style-type: none"><li>● <b>Informatec Remote Voicemail:</b> Send NOTIFY message from the remote voicemail system to the user. Cannot be used alongside local voicemail. <b>Note:</b> This option can be only used with Informatec remote voicemail.</li></ul> <p><b>Note:</b> The default option is Local Voicemail.</p>
<b>Voicemail Password</b>	Configure the password for voicemail access. <b>Note:</b> The password must contain at least 4 characters. It can consist of only digits. Letters and special characters are not accepted.
<b>Skip Voicemail Password Verification</b>	If this option is enabled when the user dials the feature code of the voicemail, the system will not require the user to enter the voicemail password.
<b>Send Voicemail Email Notification</b>	Configures whether to send an email notification when a new voicemail is received. <ul style="list-style-type: none"><li>● Default</li><li>● Yes</li><li>● No</li></ul>
<b>Attach Voicemail to Email</b>	Configures whether to send the voicemail file attached in the email. <ul style="list-style-type: none"><li>● Default</li><li>● Yes</li><li>● No</li></ul>
<b>Keep Voicemail After Emailing</b>	When “Attach Voicemail to Email” is enabled, the user can configure whether to keep the voicemail file stored in the PBX or not. <ul style="list-style-type: none"><li>● Default</li><li>● Yes</li><li>● No</li></ul>

SIP Extension Configuration Parameters > Voicemail

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

SIP Extension Configuration Parameters > Custom Time

<b>Normal</b>	
<b>Enable Wave</b>	Enable Wave for the specific extension.
<b>Allow Concurrent Logins from the Same Client Type</b>	Enables/disables the ability to login to Wave from different sessions on the same type of client. <b>Note:</b> This option is disabled by default.
<b>Wave Welcome Email</b>	Wave Welcome Email template.
<b>Wave Permission Settings</b>	Clicking the path will direct you to Wave Permission configuration.
<b>Wave</b>	
<b>Download Link</b>	<a href="https://fw.gdms.cloud/wave/download/">https://fw.gdms.cloud/wave/download/</a>

SIP Extension Configuration Parameters > Wave Client

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


























SIP Settings	
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.
Enable Auto-Answer	If enabled, the extension will support auto-answer when indicated by Call-info/Alert-info headers.
Enable Keep-alive	If enabled, the PBX will regularly send SIP OPTIONS to check if host device is online.
Keep-alive Frequency	Configure the keep-alive interval (in seconds) to check if the host is up.
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.
ACL Policy	<p>Access Control List manages the IP addresses that can register to this extension.</p> <ul style="list-style-type: none"><li>● <b>Allow All:</b> Any IP address can register to this extension.</li><li>● <b>Allow Whitelist IP Address:</b> Only whitelisted IP addresses in the configured network segments can register to this extension.</li></ul>

	<ul style="list-style-type: none"><li>● <b>Allow Whitelist IP Address + RemoteConnect:</b> Registrations from whitelisted IP address network segments and RemoteConnect registrations to this extension will be allowed.</li></ul>
<b>Fax</b>	
<b>Fax Mode</b>	Configure fax mode. The following options are available: <ul style="list-style-type: none"><li>● <b>None:</b> Disable fax support. This is the default option.</li><li>● <b>Fax Detect:</b> During a call, the fax signal from the user/trunk will be detected, and the received fax will be sent to the user's configured email address. If the destination does not have a configured email address, the fax will be sent to the <b>Default Email Address</b> configured in the <b>Call Features-&gt;Fax/T.38-&gt;Fax Settings</b> page.</li></ul>
<b>Fax to Email</b>	If set to "Yes", the fax will be sent to the user-configured email address. If no user email address is found, the fax will be sent to the default email address configured in <i>Fax/T.38-&gt;Fax Settings</i> .

SIP Extension Configuration Parameters > Advanced Settings

Search and Edit Extension

All the SoftwareUCM 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										
<div><div><div>Add</div><div>Edit</div><div>Delete</div><div>Edit All SIP</div><div>Email Notification</div><div>More</div></div><div><div>All</div><div>Extension Number or Name</div><div></div></div></div>										
<input type="checkbox"/>	Status	Presence S...	Extension	Name	Message	Type	IP and Port	Sync to Co...	Extension ...	Options
<input type="checkbox"/>	Unregistered	Available	1000		0/0/0	SIP(WebRTC)	--	Synced		   
<input type="checkbox"/>	Unregistered	Available	1001		0/0/0	SIP(WebRTC)	--	Synced		   
<input type="checkbox"/>	Unregistered	Available	1002		0/0/0	SIP(WebRTC)	--	Synced		   
<input type="checkbox"/>	Unregistered	Available	1003		0/0/0	SIP(WebRTC)	--	Synced		   
<input type="checkbox"/>	Unregistered	Available	1004		0/0/0	SIP(WebRTC)	--	Synced		   
Total: 5 < 1 > 30 / page Goto										


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

Click on  to send NOTIFY reboot event to the device that has a SoftwareUCM 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**

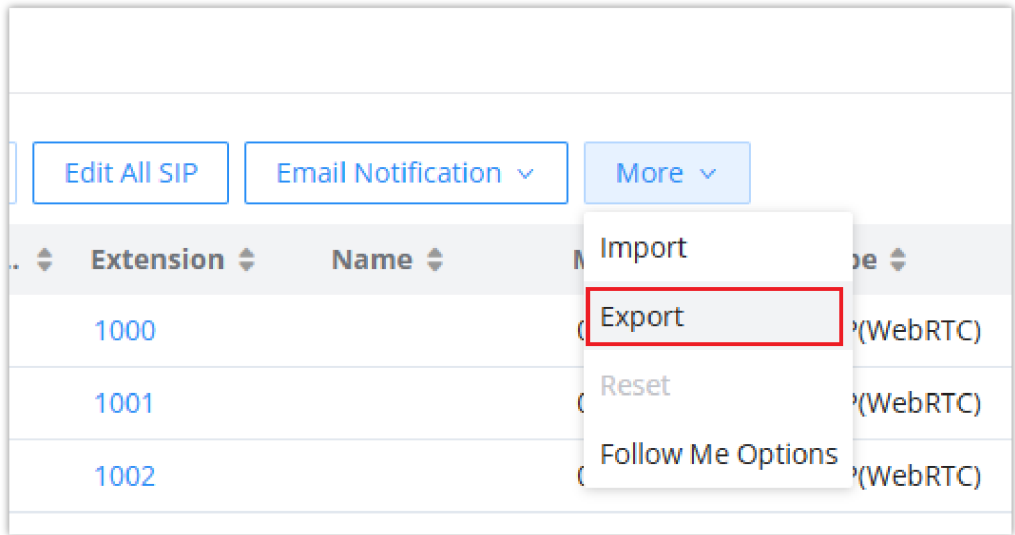
Select the checkbox for the extension(s). Then click on “Edit” to edit the extensions in a batch.

- **Delete selected extensions**

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

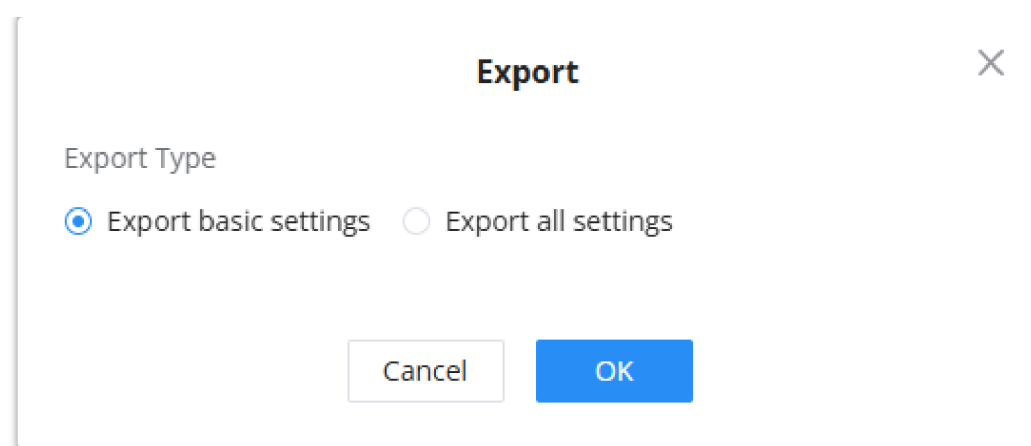
**Export Extensions**

The extensions configured on the SoftwareUCM can be exported to a CSV format file. Click on the “Export Extensions” button and select technology in the prompt below.



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 file can serve as a template for users to fill in desired extension information to be imported to the SoftwareUCM.

## Import Extensions

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

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

Import

Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.  
If an extension import does not contain a column for a setting, the following will occur:  
- If importing a new extension or replacing an existing extension, the default value for the setting will be used.  
- If updating an extension, the extension's current setting will be retained.

On Duplicate Extension

Skip

Extension File

Choose File to Upload

Cancel

Upload

Import Extensions

4. Select the option in “On Duplicate Extension” to define how the duplicate extension(s) in the imported CSV file should be treated by the PBX.
- Skip:** Duplicate extensions in the CSV file will be skipped. The PBX will keep the current extension information as previously configured without change.

**Delete and Recreate:** The current extension previously configured will be deleted and the duplicate extension in the CSV file will be loaded to the PBX.

**Update Information:** The current extension previously configured in the PBX will be kept. However, if the duplicate extension in the CSV file has 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 file from a local directory on the PC.

6. Click on “Apply Changes” to apply the imported file on the SoftwareUCM.
- 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 Voic | Ring Time | Auto Reco | SRTP | Fax Mode | Strategy  | Local Sub | Local Sub | Local Sub | Local Sub | Local Sub | Local Sub | Local Sub | Local Sub | Local |
| 2  | 1000      | Bonnie    | MacFarla | 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       |            | rY3\$z\$j | 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       |            | tW8%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                  |

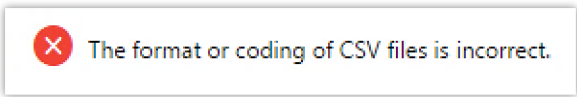
Field	Supported Values
<b>Skip Voicemail Password Verification</b>	yes/no
<b>Ring Timeout</b>	Empty/ 3 to 600 (in second)
<b>SRTP</b>	yes/no
<b>Skip Trunk Auth</b>	yes/no/bytime
<b>Codec Preference</b>	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
<b>Permission</b>	Internal/Local/National/International
<b>DTMF Mode</b>	RFC4733/info/inband/auto
<b>Insecure</b>	Port
<b>Enable Keep-alive</b>	Yes/no
<b>Keep-alive Frequency</b>	Value from 1-3600
<b>AuthID</b>	Alphanumeric value without special characters
<b>TEL URI</b>	Disabled/user=phone/enabled
<b>Call Forward Busy</b>	Digits
<b>Call Forward No Answer</b>	Digits
<b>Call Forward Unconditional</b>	Digits
<b>Support Hot-Desking Mode</b>	Yes/no
<b>Dial Trunk Password</b>	Digits
<b>Disable This Extension</b>	Yes/no
<b>CFU Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFN Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>CFB Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Music On Hold</b>	Default/ringbacktone_default

Field	Supported Values
<b>CC Agent Policy</b>	If CC is disabled use: never
	If CC is set to normal use: generic
	If CC is set to trunk use: native
<b>CC Monitor Policy</b>	Generic/never
<b>CCBS Available Timer</b>	3600/4800
<b>CCNR Available Timer</b>	3600/7200
<b>CC Offer Timer</b>	60/120
<b>CC Max Agents</b>	Value from 1-999
<b>CC Max Monitors</b>	Value from 1-999
<b>Ring simultaneously</b>	Yes/no
<b>External Number</b>	Digits
<b>Time Condition for Ring Simultaneously</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Time Condition for Skip Trunk Auth</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Enable LDAP</b>	Yes/no
<b>Enable T.38 UDPTL</b>	Yes/no
<b>Max Contacts</b>	Values from 1-10
<b>Enable Wave</b>	Yes/no
<b>Alert-Info</b>	None/Ring 1/Ring2/Ring3/Ring 4/Ring 5/Ring 6/Ring 7/ Ring 8/Ring 9/Ring 10/bellcore-dr1/bellcore-dr2/ bellcore-dr3/ bellcore-dr4/ bellcore-dr5/custom
<b>Do Not Disturb</b>	Yes/no
<b>DND Time Condition</b>	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
<b>Custom Auto answer</b>	Yes/no
<b>Do Not Disturb Whitelist</b>	Empty/digits
<b>User Password</b>	Alphanumeric characters.
<b>First Name</b>	Alphanumeric without special characters.
<b>Last Name</b>	Alphanumeric without special characters.

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

SIP extensions Imported File Example

The CSV file should contain all the above fields, if one of them is missing or empty, the SoftwareUCM 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.

More

Options	Value
Extension	1000
Status	<div><div></div>Unregistered</div>
Presence Status	Available
Endpoint Type	SIP(WebRTC)
CallerID Name	
Message	0/0/0
IP and Port	--
Extension Info Notification Status	Extension info email has not been 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 SoftwareUCM 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.

Please make sure that selected extensions have been configured with email addresses to ensure successful email delivery. View Email Template

Send the Extension Information email to the selected extensions?

If no extension is selected, account information emails will be sent to all extensions.

Cancel

Send

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:

## Welcome to the Wave Client

Wave offers an easy-to-use platform to remotely join, schedule and hold meetings, calls and conferences from anywhere. Through Wave, you can:

- Start face-to-face video calls and meetings anywhere.
- Schedule and start meetings from the app.
- Chat and share files with your colleagues.
- Compatible with UCM RemoteConnect cloud service for secure remote connections.

### Wave Settings (A communication and collaboration solution integrating IM, telephone and office)

Please Visit <https://000000.e.myucm.cloud>

Login Name 1001

Login Password P@ssw0rd

Use Wave App to scan qr code and log in

Use Wave App to scan qr code and log in

### Download Wave PC or APP client

Wave offers an easy-to-use platform to chat and collaboration features, remotely join, schedule and hold meetings, calls and conferences from anywhere

Download Wave

[Company Info](#) | [Contact Us](#)

© 2024 Grandstream Networks, Inc.

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 SoftwareUCM admin can also send "Extension Information" mail and "Wave Welcome" mail as the figure below shows.

Extensions

Add

Edit

Delete

Edit All SIP

Email Notification ▾

More ▾

<div>▾</div>	Status ▴ ▾	Prese... ▴ ▾	Exten... ▴ ▾	Name	Extension Information ▴ ▾	IP and
<div>✓</div>	<div>●</div> Unregis...	Available	1000		Remote Registration	webR... --
<div>✓</div>	<div>●</div> Unregis...	Available	1001		Wave Welcome	webR... --
<div>✓</div>	<div>●</div> Unregis...	Available	1002		0/0/0	SIP(WebR... --
<div>✓</div>	<div>●</div> Unregis...	Available	1003		0/0/0	SIP(WebR... --

Send Email Notification

## Multiple Registrations per Extension



SoftwareUCM 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 10. 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.

General

\* Extension

1000

\* Call Privileges

Local

AuthID

Disable This Extension

☐

CallerID Number

\* SIP Password

.....

\* Concurrent Registrations

3

Extension – Concurrent Registration

### SMS Message Support

The SoftwareUCM provides built-in SIP SMS message support. For SIP end devices such as Grandstream GXP or GXV phones that support SIP messages, after a SoftwareUCM 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.

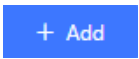
### Extension Groups

The SoftwareUCM extension group feature allows users to assign and categorize extensions in different groups to better manage the configurations on the SoftwareUCM. 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.

Create New Extension Group

\* Name:

Tech\_Supprot\_Team

Members:

☐

0 item

Available

Search

Q

None

<

>

↑

^

↓

⌵

☐

6 items

Selected

Search

Q





☐ 1000

☐ 4001

☐ 4002

☐ 4003

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.

Outbound Routes > Create New Outbound Rule

General

\* Outbound Rule Name

Rule\_1

\* Pattern

\_9x.

PIN Groups

None

Password

Local Country Code

Disable This Route

☐

Privilege Level

Disable

PIN Groups with Privilege Level

☐

Auto Record

☐

Enable Source Caller ID Whitelist

Enable Source Caller ID Whitelist

☒

Source Caller ID Pattern

Outbound Route CID

Whitelisted Extensions/Extension Groups

Call Duration Limit

Cancel

Save

Select Extension Group in Outbound Route

### VoIP Trunks

#### VoIP Trunk Configuration

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

4000

◦ Click on “Add SIP Trunk” to add a new VoIP trunk.

◦ Click on



to configure detailed parameters for the VoIP trunk.

◦ Click on



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

◦ Click on



to start LDAP Sync.

◦ Click on



to delete the VoIP trunk.

The VoIP trunk options are listed in the table below.

Disable This Trunk	Check this box to disable this trunk.
Type	<p>Select the VoIP trunk type.</p> <ul style="list-style-type: none"><li>● <b>Peer SIP Trunk:</b> A direct IP-to-IP connection between the PBX and another SIP server or device, without requiring registration.</li><li>● <b>Register SIP Trunk:</b> A trunk that requires the PBX to register with the SIP server or provider using credentials (username and password).</li><li>● <b>Account SIP Trunk:</b> A trunk where the PBX acts as the registrar, allowing remote devices or endpoints to register with it.</li></ul>
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	<p>Select the transport protocol to use.</p> <ul style="list-style-type: none"><li>● <b>UDP:</b> if selected, then the option Enabe UDP should be checked, under <b>PBX Settings &gt; SIP Settings &gt; Transport Protocol</b>.</li><li>● <b>TCP:</b> If selected, then the option TCP Enable should be checked under <b>PBX Settings &gt; SIP Settings &gt; Transport Protocol</b>.</li><li>● <b>TLS:</b> The default Transport protocol.</li></ul>
Trunk Mode	<p>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.</p> <ul style="list-style-type: none"><li>● <b>DID Access:</b> When a domain is not included in “To” SIP header, the user can configure a DID which will be used to verify incoming calls.</li><li>● <b>Port Access:</b> 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</li></ul>

	<p><b>Note:</b> This option is available only for Register Trunk and Peer Trunk when using UDP as transport protocol.</p>
<b>DID Number</b>	<p>Enter the DID number which will be included in the “To” SIP header. This option is mandatory when <b>Trunk Mode</b> is set to <i>DID Access</i>.</p>
<b>Server Address</b>	<p>Use the indicated address to register/peer trunks when configuring other PBXs with the CloudUCM.</p>
<b>Keep Original CID</b>	<p>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.</p>
<b>Keep Trunk CID</b>	<p>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”.</p>
<b>NAT</b>	<p>Enable this setting if the PBX is using public IP and communicating with devices behind NAT.  <b>Note 1:</b> 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 <b>PBX Settings &gt; SIP Settings &gt; NAT</b> instead.  <b>Note 2:</b> If one is experiencing one-way audio issues, please check the NAT configuration and SIP/RTP ports in the firewall.</p>
<b>TEL URI</b>	<p>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.</p>
<b>Need Registration</b>	<p>Defines Whether to register the trunk on the external server. Enabled by default.  <b>Note:</b> This option appears when the Type is set to Register Trunk.</p>
<b>Allow outgoing calls if registration fails</b>	<p>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.  <b>Note:</b> This option appears when the Type is set to Register Trunk.</p>
<b>Caller ID Number</b>	<p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>Important Note: When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call:  From the user (Register Trunk Only) → CID from inbound call (Keep Original CID Enabled) → Trunk Username/CallerID (Keep Trunk CID Enabled) → DOD → Extension CallerID Number → Trunk Username/CallerID (Keep Trunk CID Disabled) → Global Outbound CID.</p>
<b>CallerID Name</b>	<p>Configure the new name of the caller when the extension has no CallerID Name configured.</p>
<b>Username</b>	<p>The number or username used for registration and authentication with the service provider.  <b>Note:</b> You can configure this option for “Account SIP Trunk” and “Register SIP Trunk only”</p>
<b>Password</b>	<p>The password used for registration and authentication with the service provider.  <b>Note:</b> You can configure this option for “Account SIP Trunk” and “Register SIP Trunk only”</p>
<b>Auth ID</b>	<p>Enter the Authentication ID for the “Register SIP Trunk” type.</p>
<b>AuthTrunk</b>	<p>If enabled, the PBX will send a 401 response to the incoming call to authenticate the trunk.</p>

<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded. <b>Note:</b> the recording functionality is not available on the startup plan.
<b>Direct Callback</b>	Allows external numbers the option to get directed to the extension that last called them. For Example, User 2002 has dialed external number 061234575 but they were not reachable, once they have received missed call notification on their phone, they would mostly call back the number, if the option “Direct Callback” is enabled then they will be directly bridged to user 2002 regardless of the configured inbound destination.
<b>Domain Connection Mode</b>	If enabled, the following options will be automatically configured: <b>TLS</b> transport, <b>From Domain, Enable Heartbeat Detection</b> and <b>ICE Support</b> . Please ensure that the trunk host name is a GDMS-assigned address and supports TLS.
<b>Monitor Concurrent Calls</b>	If enabled and when the number of concurrent calls exceeds any trunk’s configured concurrent call thresholds, an alarm notification will be generated. Note: Please make sure the system alert event “Trunk Concurrent Calls” is enabled.
<b>Concurrent Call Threshold</b>	Threshold of all incoming and outgoing concurrent calls through this trunk.
<b>Outgoing Concurrent Calls Threshold</b>	Threshold of all outgoing concurrent calls passing through this trunk.
<b>Incoming Concurrent Calls Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.
<b>Total Time Limit For Outbound Calls</b>	
<b>Enable Total Time Limit For Outgoing Calls</b>	When this setting is activated, the user can set a time limit before calls cannot be initiated through this trunk
<b>Period</b>	This setting defines how long until the time allowed for outgoing calls is reset.  <ul style="list-style-type: none"> <li>● <b>Monthly:</b> The time allowed will reset every month.</li> <li>● <b>Quarterly:</b> The time allowed will reset every 3 months.</li> </ul> <b>Example:</b> If the time limit has been set to 4320 minutes, the allowed time will always revert back to 4320 after a month or 3 month based on the period configured.
<b>Total Time</b>	Total time allowed in minutes.
<b>Advanced Settings</b>	
<b>Codec Preference</b>	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, iLBC, ADPCM, H.264, H.263, H.263p and VP8.
<b>Packet Loss Retransmission</b>	Configure to enable Packet Loss Retransmission.
<b>Audio FEC</b>	Configure to enable Forward Error Correction (FEC) for audio.
<b>Video FEC</b>	Configure to enable Forward Error Correction (FEC) for video.
<b>ICE Support</b>	Toggles ICE support. For peer trunks, ICE support will need to be enabled on the other end.
<b>FECC</b>	Configure to enable Far-end Camera Control
<b>Silence Suppression</b>	If enabled, the PBX will send CN packets for silence suppression after a successful CN negotiation in the SIP SDP. If the client endpoint’s OPUS codec supports the reception of DTX

	packets, the PBX will send DTX packets instead.
<b>SRTP</b>	Enable SRTP for the VoIP trunk. The default setting is “No”.
<b>SRTP Crypto Suite</b>	SRTP encryption suite used by PBX for outbound calls. Priority is based on order of configuration.
<b>ZRTP Encryption Mode</b>	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.
<b>IPVT Mode</b>	Similar to Enable Direct Media. The PBX will attempt to redirect the RTP media streams to bypass the PBX and to go directly between caller and callee. Primarily for use with trunks to IPVT.
<b>Enable T.38 UDPTL</b>	Enable or disable T.38 UDPTL support.
<b>Include Special Attributes</b>	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.
<b>Send PPI Header</b>	If checked, the invite message sent to trunks will contain PPI (P-Preferred-Identity) Header.
<b>Send PAI Header</b>	<p>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:</p> <ol style="list-style-type: none"> <li>1. On incoming calls, the Passthrough PAI Header value will be preferred for this PBX’s 18x and 200 SIP messages to the caller.</li> <li>2. On outbound calls, the Send PAI Header value will be preferred for this PBX’s INVITE SIP message to the callee.</li> </ol>
<b>Passthrough PAI Header</b>	If enabled and “Send PAI Header” is disabled, PAI headers will be preserved as calls pass through the PBX.
<b>Send PANI Header</b>	If checked, the INVITE sent to the trunk will contain P-Access-Network-Info header.
<b>Send Anonymous</b>	If checked, the “From” header in outgoing INVITE message will be set to anonymous.
<b>DID Mode</b>	Configure to obtain the destination ID of an incoming SIP call from SIP Request-line or To header.
<b>DTMF Mode</b>	<p>Configures the mode for sending DTMF.</p> <ul style="list-style-type: none"> <li>● <b>RFC4733</b> (default): DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream. Backward-compatible with RFC2833.</li> <li>● <b>Inband</b>: DTMF is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs.</li> <li>● <b>Info</b>: DTMF is transmitted separately from the media streams. RFC4733_info: DTMF is transmitted through both RFC4733 and SIP INFO.</li> <li>● <b>Auto</b>: DTMF mode will be negotiated with the remote peer, only supports RFC4733 and inband. RFC4733 will be used by default unless the remote peer does not indicate support.</li> </ul>
<b>Enable Heartbeat Detection</b>	If enabled, the PBX will regularly send SIP OPTIONS to check if the device is online.
<b>Max Outgoing Calls</b>	The number of current outgoing calls over the trunk at the same time. The default value 0 means no limit.
<b>Max Incoming Calls</b>	The max allowed number of concurrent incoming calls through the trunk. Default is 0 (no limit).





<b>Disable This Trunk</b>	Check this box to disable this trunk
<b>Type</b>	Register Trunk
<b>Provider Name</b>	Configure a unique label to identify the trunk when listed in outbound rules and incoming rules.
<b>Host Name</b>	Enter the IP address or hostname of the VoIP provider's server.
<b>Transport</b>	Configure the SIP Transport method. Only TLS is supported, and TLS service must be enabled on the other end.
<b>Keep Original CID</b>	Keep CID from the inbound call when dialing out even if option "Keep Trunk CID" is enabled. Please make sure the peer PBX at the other end supports matching user entry using the "username" field from the authentication line.
<b>Keep Trunk CID</b>	Always use trunk CID if specified even if extension has DOD number or CID configured.
<b>TEL URI</b>	if "Enabled" option is selected, TEL URI and remove OBP from Route cannot be enabled at the same time. If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". A "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request.
<b>Need Registration</b>	Whether to register on the external server.
<b>Allow outgoing calls if registration fails</b>	Uncheck to block outgoing calls if registration fails. If "Need Registration" option is unchecked, this setting will be ignored.
<b>CallerID Name</b>	To display the caller ID name of the trunk, you must configure the caller ID number of the trunk.
<b>Trunk Registration Number</b>	The number used to register with the provider server, and the VoIP provider will authenticate the number based on the trunk registration number.
<b>Line Selection Strategy</b>	<ul style="list-style-type: none"> <li>● <b>Linear:</b> Use lines in the list order for outbound calls.</li> <li>● <b>Round Robin:</b> Use lines based on rotary line selection for outbound calls. Previously used lines will be remembered.</li> </ul>
<b>AuthTrunk</b>	If enabled, the UCM will send a 401 response to the incoming call to authenticate the trunk.
<b>Auto Record</b>	If enabled, calls handled with this extension/trunk will automatically be recorded.
<b>Direct Callback</b>	Allows external numbers the option to get directed to the extension that last called them.
<b>Monitor Concurrent Calls</b>	If enabled, the number of concurrent calls on this trunk will be monitored. If the "Trunk Concurrent Calls" system alert is enabled, alert notifications will be generated if the number of concurrent calls exceeds this trunk's configured concurrent call thresholds.
<b>Concurrent Call Threshold</b>	Threshold of all incoming and outgoing concurrent calls in this trunk.
<b>Outgoing Concurrent Call Threshold</b>	Threshold of all outgoing concurrent calls passing through this trunk.
<b>Incoming Concurrent Call Threshold</b>	Threshold of all incoming concurrent calls passing through this trunk.

<b>Enable Total Time Limit For Outbound Calls</b>	If enabled, a limit will be placed on the cumulative duration of outbound calls within a specific period. Once this limit has been reached, further outbound calls from this trunk will not be allowed.
---	---

Direct Outward Dialing (DOD)

The SoftwareUCM 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's 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 SoftwareUCM:

- 1. To setup DOD go to SoftwareUCM 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.

Create DOD

\* DOD Number

DOD Name

Add Extension

☐

☐ 6

Available

Search

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ VFAX

<

>

☐ 0

Selected

Search

None

Cancel

Save

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
05365840000	DOD1	1000100110021003...	<div><div></div><div></div></div>

Total: 1

<

1

>

10 / page

Goto

Edit DOD

- Add DOD

: Add a DOD.
- Import

: Import DODs using a csv file.
- Export

: Export the DODs using a csv 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

When importing a DOD list, if identical DOD numbers are already configured on the IPPBX, the user can choose either to skip them or update them, by selecting the action from "On Duplicate DOD". Please see the screenshot below.

Import

Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.  
If a DOD import does not contain a column for a setting, the default value for that setting will be used.

On Duplicate DOD

Skip

Upload File

Choose File to Upload

Cancel

Upload

Import DOD Numbers

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 SoftwareUCM 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. <b>Disable:</b> Jitter buffer will not be used. <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of “Jitter Buffer Size”) <b>Adaptive:</b> Jitter buffer with a adaptive size that will not exceed the value of “Max Jitter Buffer”). <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.
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

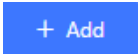
In the following sections, we will discuss the steps and parameters used to configure and manage outbound rules in SoftwareUCM, these rules are the regulating points for all external outgoing calls initiated by the UCM through the SIP trunks.

Configuring Outbound Routes


In the SoftwareUCM, an outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks. Users can also set up a fail-over trunk to be used when the primary trunk fails.

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

- Click on



to add a new outbound route.

- Click the “Import” button to upload the outgoing route in .CSV format.
- Click the “Export” button to generate outgoing routes in .CSV format.
- 

Click to edit the outbound route.

- 

Click to delete the outbound route.

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

Outbound Rule Name	Configure the name of the calling rule (e.g., local, long_distance, etc.). Letters, digits, _ and – are allowed.
Pattern	<p>All patterns are prefixed by the “_” character, but please do not enter more than one “_” at the beginning. All patterns can add comments, such as “_pattern /* comment */”. In patterns, some characters have special meanings:</p> <ul style="list-style-type: none"><li>● [12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 is allowed.</li><li>● N ... Any digit from 2-9.</li><li>● . ... Wildcard, matching one or more characters.</li><li>● ! ... Wildcard, matching zero or more characters immediately.</li><li>● X ... Any digit from 0-9.</li><li>● Z ... Any digit from 1-9.</li><li>● – ... Hyphen is to connect characters and it will be ignored</li><li>● [] Contain special characters ([x], [n], [z]) represent letters x, n, z.</li></ul>
Disable This Route	After creating the outbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in UCM. Users can enable it again when it is needed.
Password	Configure the password for users to use this rule when making outbound calls.
Local Country Code	If your local country code is affected by the outbound blacklist, please enter it here to bypass the blacklist.
Call Duration Limit	Enable to configure the maximum duration for the call using this outbound route.
Maximum Call Duration	Configure the maximum duration of the call (in seconds). The default setting is 0, which means no limit.
Warning Time	Configure the warning time for the call using this outbound route. If set to x seconds, the warning tone will be played to the caller when x seconds are left to end the call.
Auto Record	If enabled, calls using this route will automatically be recorded.
Warning Repeat Interval	Configure the warning repeat interval for the call using this outbound route. If set to X seconds, the warning tone will be played every x seconds after the first warning.
PIN Groups	Select a PIN Group
PIN Groups with Privilege Level	If enabled and PIN Groups are used, Privilege Levels and Filter on Source Caller ID will also be applied.

<b>Privilege Level</b>	<p>Select the privilege level for the outbound rule.</p> <ul style="list-style-type: none"><li>● <b>Internal:</b> The lowest level required. All users can use this rule.</li><li>● <b>Local:</b> Users with Local, National, or International levels can use this rule.</li><li>● <b>National:</b> Users with National or International levels can use this rule.</li><li>● <b>International:</b> The highest level required. Only users with the international level can use this rule.</li><li>● <b>Disable:</b> The default setting is “Disable”. If selected, only the matched source caller ID will be allowed to use this outbound route.</li></ul> <p>Please be aware of the potential security risks when using the “Internal” level, which means all users can use this outbound rule to dial out from the trunk.</p>
<b>Enable Filter on Source Caller ID</b>	<p>When enabled, users could specify extensions allowed to use this outbound route. “Privilege Level” is automatically disabled if using “Enable Source Caller ID Allowlist”.</p> <p>The following two methods can be used at the same time to define the extensions as the source caller ID.</p> <ol style="list-style-type: none"><li>1. Select available extensions/extension groups from the list. This allows users to specify arbitrary single extensions available in the PBX.</li><li>2. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one.</li></ol> <ul style="list-style-type: none"><li>● All patterns are prefixed with the “_”.</li><li>● Special characters</li></ul> <p>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.</p> <p><b>Note:</b> Multiple patterns can be used. Patterns should be separated by a comma “,”. Example: _X, _NNXXNXXXXX, _818X.</p>
<b>Outbound Route CID</b>	<p>Attempt to use the configured outbound route CID. This CID will not be used if DOD is configured.</p>
<b>Send This Call Through Trunk</b>	
<b>Trunk</b>	<p>Select the trunk for this outbound rule.</p>
<b>Strip</b>	<p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p>Example: 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.</p>
<b>Prepend</b>	<p>Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.</p>
<b>Use Failover Trunk</b>	
<b>Failover Trunk</b>	<p>Failover trunks can be used to make sure that a call goes through an alternate route when the primary trunk is busy or down. If “Use Failover Trunk” is enabled and “Failover trunk” is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through. 10 failover trunks are supported.</p>
<b>Strip</b>	<p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p>Example: 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.</p>



<b>Prepend</b>	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
<b>Time Condition</b>	
<b>Time Condition Mode</b>	<p>Use Main Trunk or Failover Trunk: Use the Main Trunk and its settings during the configured time conditions. If the main trunk is unavailable, the Failover Trunk and its settings will be used instead.</p> <p>Use Specific Trunks: Use specific trunks during the configured time conditions. The Strip and Prepend settings of the Main Trunk will be used. If a trunk is unavailable during its time condition, no failover trunks will be used.</p>

Failover Trunk Toggles

Outbound Routes

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

Add

Scheduled Sync

Outbound Blocklist

PIN Groups

Failover Trunk Toggles

Import

Export

Sequence

Name

Pattern

Privilege Level

Options

Inbound Routes

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

Outbound Routes > Failover Trunk Toggles

No-Failover Response Codes

6Available

Search

Q

403

404

408

480

503

603

1Selected

Search

Q

486

<

>

Cancel

Save

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

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

Import

Export

Sequence	Name	Pattern	Privilege Level	Options
1	Rule_1	_x.	Internal	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>
2	Rule_2	_9x.	Internal	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>

Total: 2

<1>

10 / page

Goto

Outbound Routes Page

Outbound Routes > DOD: Rule\_1

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
054865879	DOD1	10001001	<div><div></div><div></div></div>

Total: 1

<1>

10 / page

Goto

DOD Outbound Rule 1

Outbound Routes > DOD: Rule\_2

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
059875478	DOD2	10031004	<div><div></div><div></div></div>

Total: 1

<1>

10 / page

Goto

DOD Outbound Rule 2

Outbound Blocklist

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

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

Outbound Routes > Outbound Blacklist

Blocklist Manage

Don't Call Me Blocklist Integration

The blocklist (based on CalleelD) 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

Blocklist Manage

Add Blocklist Rule

Add

Clear

Delete

Import

Export

Q Please enter blocklist nu...

Continent

Countries & Regions

Blocklist 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.

Import

Blocklist File

Choose File to Upload

Cancel

Upload

Blacklist Import/Export

## Don't Call Me Blacklist Integration

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

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

Outbound Routes > Outbound Blacklist

Blacklist Manage

Integrate Don't Call Me Blacklist

Integrate Don't Call Me Blacklist

☒

\* Authorization Token

This field is required

\* Query Timeout Time (s)

This field is required

Query Timeout Handling

Allow Dialing

Test Connection

Start

Cancel

Save

Don't Call Me Database Integration

Parameter	Description
Integrate Don't Call Me Blacklist	Enable or disable Don't Call Me integration
Authorization Token	Enter the authorization token generated by the Don't Call Me database.
Query Timeout 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. <b>Allow Dialing:</b> If the query times out, the call will be allowed. <b>Prohibit Dialing:</b> 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. <b>Note:</b> If the database or Internet access is momentarily down, this test will fail.

PIN Groups

The SoftwareUCM 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 to configure the new PIN.

Outbound Routes > PIN Groups > Create New PIN Group

\* Name

Store\_Staff

Record in CDR

☒

Members

\* PIN Number

1695

\* PIN Name

Morgan

✓ Save

✕ Cancel

Create a New PIN Group

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

Outbound Routes > PIN Groups

AddUpload

Name	Record in CDR	Options
Store_Staff	yes	<div><div></div><div></div><div></div></div>
<div><div>PIN Number</div><div>1695</div></div>	<div><div>PIN Name</div><div>Morgan</div></div>	

Total: 1

<

1

>

10 / page

Goto

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.

General

\* Calling Rule Name:

GStest

\* Pattern:

\_9.

PIN Groups:

GSEMEA

Password:

Disable This Route:

☐

Privilege Level:

Disable

PIN Groups with Privilege Level:

☐

Outbound PIN

Importing PIN Groups from CSV files:

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

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

2. Select the CSV file to upload.

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.

Outbound Routes > PIN Groups

AddUpload

Name	Record in CDR	Options
Store_Staff	yes	<div><div></div><div></div><div></div></div>
<div><div>PIN NumberPIN Name</div><div>1695Morgan</div></div>		

Total: 1

<1>

10 / pageGoto

CSV File Successful Upload

Inbound Routes

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

- Click onto add a new inbound route.
- Click on “Blacklist” to configure the blacklist for all inbound routes.
- Click onto edit the inbound route.
- Click onto delete the inbound route.

Inbound Route Configuration

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 “_”.

	<p>Special characters:</p> <p><b>X:</b> Any Digit from 0-9. <b>Z:</b> Any Digit from 1-9. <b>N:</b> Any Digit from 2-9. <b>“.”:</b> Wildcard. Match one or more characters. <b>“!”:</b> Wildcard. Match zero or more characters immediately. Example: [12345-9] – Any digit from 1 to 9.</p> <p><b>Notes:</b></p> <p>Multiple patterns can be used. Each pattern should be entered in a new line.</p> <p><b>Example:</b></p> <p>_X.</p> <p>_ NNXXNXXXXX /* 10-digit long distance */</p>
<b>Disable This Route</b>	<p>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.</p>
<b>CID Source</b>	<p>Configures the source of the CID to match with the configured CallerID Pattern.</p> <p><b>None:</b> CID is not obtained from any source. Only applicable if no CallerID Pattern is configured.</p> <p><b>DiversionID:</b> CID is obtained from the Diversion header. Only applicable to SIP trunks.</p> <p><b>CallerID:</b> If the call is from a SIP trunk, the CID is obtained from the From header. Otherwise, the CID will be obtained from other related signaling.</p>
<b>Seamless Transfer Whitelist</b>	<p>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.</p>
<b>Ringback tone</b>	<p>Choose the custom ringback tone to play when the caller reaches the route.</p>
<b>Auto Record</b>	<p>If enabled, calls using this route will automatically be recorded.</p>
<b>Block Collect Call</b>	<p>If enabled, collect calls will be blocked.</p> <p><b>Note:</b> Collect calls are indicated by the header “P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call”.</p>
<b>Alert-Info</b>	<p>Configure the Alert-Info, when UCM receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.</p>
<b>Fax Detection</b>	<p>If enabled, fax signals from the trunk during a call will be detected.</p>
<b>Fax Destination</b>	<p>Configures the destination of faxes.</p> <ul style="list-style-type: none"> <li>● <b>Extension:</b> send the fax to the designated FAX extension.</li> <li>● <b>Fax to Email:</b> send the fax as an email attachment to the designated extension’s email address. If the selected extension does not have an associated email address, it will be sent to the default email address configured in the Call Features-&gt;Fax/T.38-&gt;Fax Settings page.</li> </ul> <p><b>Note:</b> please make sure the sending email address is correctly configured in <b>System Settings-&gt;Email Settings</b>.</p>
<b>Auto Answer</b>	<p>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.</p>
<b>Block Collect Calls</b>	<p>If enabled, collect calls will be <b>blocked</b>.</p> <p><b>Note:</b> Collect calls are indicated by the header “P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect <b>Call</b>”.</p> <p><b>Note:</b> This is affected by Block Set Calls on the SIP Settings -&gt; General Settings page.</p>
<b>Prepend Trunk Name</b>	<p>If enabled, the trunk name will be added to the caller id name as the displayed caller id name.</p>



<b>Set Caller ID Info</b>	Manipulates Caller ID (CID) name and/or number within the call flow to help identify who is calling. When enabled two fields will show allowing to manipulate the CallerID Number and the Caller ID Name.
<b>CallerID Number</b>	<p>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.</p> <ul style="list-style-type: none"><li>• <b>\${CALLERID(num)}</b>: Default value which indicates the number of an incoming caller (CID). The CID will not be modified.</li><li>• <b>\${CALLERID(num):n}</b>: Skips the first n characters of a CID number, where n is a number.</li><li>• <b>\${CALLERID(num):-n}</b>: Takes the last n characters of a CID number, where n is a number.</li><li>• <b>\${CALLERID(num):s:n}</b>: Takes n characters of a CID number starting from s+1, where n is a number and s is a character position (e.g. \${CALLERID(num):2:7} takes 7 characters after the second character of a CID number).</li><li>• <b>n\${CALLERID(num)}</b>: Prepends n to a CID number, where n is a number.</li></ul>
<b>CallerID Name</b>	<p>The default string is <b>\${CALLERID(name)}</b>, which means the name of an incoming caller, it is a pattern-matching syntax format.</p> <p><b>A\${CALLERID(name)}B</b> means Prepend a character ‘A’ and suffix a character ‘B’ to <b>\${CALLERID(name)}</b>.</p> <p>Not using pattern-matching syntax means setting a fixed name to the incoming caller.</p>
<b>Enable Custom Inbound Mode</b>	<p>Gives users the ability to configure inbound mode per individual route. When enabled two fields will show allowing to set the Inbound mode and the Inbound mode Suffix.</p> <p><b>Note:</b> Global inbound mode must be enabled before users can configure custom inbound mode.</p>
<b>Inbound Mode</b>	<p>Choose the inbound mode for this route.</p> <p><b>Note:</b> Toggling the global inbound mode will not affect routes that have Custom Inbound Mode enabled. If all routes have the option enabled, toggling the global inbound mode via BLF will trigger a voice prompt indicating that none of the routes will be affected by the global inbound mode change.</p>
<b>Inbound Mode Suffix</b>	<p>Dial “Global Inbound Mode feature code + Inbound Mode Suffix” or a route’s assigned suffix to toggle the route’s inbound mode.</p> <p>The BLF subscribed to the inbound mode suffix can monitor the current inbound mode.</p>
<b>Inbound Multi-Mode</b>	<p>Multi-mode allows users to switch between destinations of the inbound rule by feature codes. Configure related feature codes as described in [Inbound Route: Multi-Mode]. If this option is enabled, the user can use feature code to switch between different modes/destinations.</p>
<b>CallerID Name Lookup</b>	<p>If enabled, the callerID will be resolved to a name through local LDAP. Note, if a matched name is found, the original callerID name will be replaced. The name lookup is performed before other callerID or callerID name modifiers (e.g., Inbound Route’s Set CallerID Info or Prepend Trunk Name).</p> <p><b>Note:</b> Name lookup may impact system performance.</p>
<b>Dial Trunk</b>	<p>This option shows up only when “By DID” is selected. If enabled, the external users dialing into the trunk via this inbound route can dial outbound calls using the UCM’s trunk.</p>
<b>Privilege Level</b>	<p>This option shows up only when “By DID” is selected.</p> <ul style="list-style-type: none"><li>• <b>Disable:</b> Only the selected Extensions or Extension Groups are allowed to use this rule when enabled Filter on Source Caller ID.</li><li>• <b>Internal:</b> The lowest level required. All users are allowed to use this rule, checking this level might be risky for security purposes.</li><li>• <b>Local:</b> Users with Local level, National or International level are allowed to use this rule.</li><li>• <b>National:</b> Users with National or International Level are allowed to use this rule.</li><li>• <b>International:</b> The highest level required. Only users with an international level are allowed to use this rule.</li></ul>
<b>Allowed DID Destination</b>	<p>This option shows up only when “By DID” is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination is:</p>



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

	<p>groups as configured in “DID destination”. If the dialed number matches the DID pattern, the call will be allowed to go through.</p> <p>Configure the number of digits to be stripped in the “Strip” option.</p> <ul style="list-style-type: none"><li>• Dial By Name</li><li>• External Number</li><li>• Callback</li></ul>
--	---

Inbound Route: Prepend Example

SoftwareUCM 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.

Inbound Routes > Edit Inbound Rule

\* Pattern

\_18005251163

CallerID Pattern

CID Source

None

Seamless Transfer Allowlist

Dial Trunk

☐

Call Setting

Ringback Tone

None

Alert-info

None

Auto Record

☐

Fax Detection

☐

Block Collect Calls

☐

CallerID Setting

Prepend Trunk Name

☐

Set CallerID Info

☐

CallerID Name Lookup

☐

Inbound Mode

Inbound Multi-Mode

☐

Allowed DID Destination

Extension \*

Default Mode

\* Default Destination

By DID

Strip

8

Prepend

2

Cancel

Save

Inbound Route feature: Prepend

Inbound Route: Inbound Multi-Mode

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

**Inbound Mode**

Inbound Multi-Mode☒

Custom Inbound Mode☐

Default Mode

Mode 1

\* Default Destination

Extension

1000


**Time Condition**

Add

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

This feature can be used to change inbound modes either through the web UI or feature code. You can also configure each mode.

Global Inbound Multi-Mode

☒

Global Inbound Mode

Default Mode

BLF Subscription Number

Inbound Mode Toggle Feature Code

\* Default Mode ⓘ

\*61

\* Mode 1 ⓘ

\*62

Add Mode +

Cancel

Save

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

### Inbound Route: Custom Inbound Mode

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

Inbound Mode

Inbound Multi-Mode☒

Inbound ModeDefault Mode▼

Allowed DID DestinationExtension ×

Custom Inbound Mode☒

\* Inbound Mode Feature Code33

The global inbound mode must be enabled before configuring Custom Inbound Mode. Additionally, Mode 1 must be configured as well.

When Custom 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 Feature Code" and the current inbound route can be monitored by subscribing a BLF to the Inbound Mode Feature Code.

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

### Note

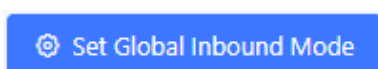
Toggling the global inbound mode will not affect routes that have *Inbound Multi-Mode* enabled. If all routes have the option enabled, toggling the global inbound mode via BLF will trigger a voice prompt indicating that none of the routes will be affected by the global inbound mode change.

## Inbound Route: Inbound Mode BLF Monitoring

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

To do this, please refer to the following steps:

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



button and enable Inbound Multi-Mode.

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

Inbound Routes > Set Global Inbound Mode

This feature can be used to change inbound modes either through the web UI or feature codes.

Global Inbound Multi-Mode☒

Global Inbound ModeDefault Mode

BLF Subscription Number777

Inbound Mode Toggle Feature Code

\* Default Mode ⓘ

\* Mode 1 ⓘ

Add Mode +

CancelSave

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



Inbound Mode – Default Mode

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



Inbound Mode – Mode 1

Inbound Route: Third-party Database Search

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

Important Note

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

Inbound Routes

Add

Blacklist

Set Global Inbound Mode

Third-party Database Search

Import

Export

Filter

SIP Trunks -- Grandstrea

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

Inbound Routes

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

Inbound Routes > Third-party Database Search

Third-party Database Search

\*

MySQL Host

\*

Database

\*

Username

\*

MySQL Password

\*

Character Set

\*

Query Key

Table

Caller Name

Number

phonebook

name

number

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

Test Connection

Start

Cancel

Save

Third-party Database Search

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

Inbound Route: Import/Export Inbound Route

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

Inbound Routes

Add

Blocklist

Set Global Inbound Mode

3rd Party Database Search

Import

Export

Filter

SIP Trunks -- 123Cloud

Inbound Route Name	Pattern	CallerID Pattern	Inbound Mode	Inbound Mode Feature Code	Time Condition	Time	Destination	Options
--------------------	---------	------------------	--------------	---------------------------	----------------	------	-------------	---------

Import/Export Inbound Route

The imported file should be in CSV 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 Multi-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

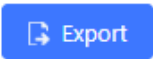
In the UCM, Blocklist is supported for all inbound routes. Users could enable the Blocklist feature and manage the blocklist by clicking on “Blocklist”.

- 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 to the list. Anonymous can also be added as a Blocklist Number by typing “Anonymous” in Add Blacklist 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.



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

All ×

Add

Blocklist list

Clear

Delete

Import

Export

Q Please enter blocklist nu...

Q

☐

Number ↕

Apply to

Options

Cancel

Save

Blocklist Configuration Parameters

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

Paste					
Format Painter					
Clipboard			Font		
F8					
	A	B	C	D	E
1	13238680006	12135958547	12136268547	6262357999	
2					
3					
4					
5					

Blacklist CSV File

Users could also add a number to the Blacklist or remove a number from the Blacklist by dialing the feature code for "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 room allowing multiple rooms 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 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, 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	<p>Meeting audio and video can be automatically recorded. These reconrdings can be found under the Meeting Recording or Meeting Video Recordings Page.</p> <ul style="list-style-type: none"><li>● <b>None:</b> Auto record is disabled.</li><li>● <b>Record Audio:</b> Record only the meeting Audio.</li><li>● <b>Record video (Focus Mode):</b> 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.</li></ul>
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 the **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 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		--	<div><div></div><div></div></div>

Multimedia Meeting

Meetings Settings

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

Meeting Max Concurrent Audio	Maximum number of partipants that can be heard simultaenously 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.
<b>Silence Suppression</b>	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.
<b>Enable Talk Detection</b>	If enabled, the AMI will send the corresponding event when a user starts or stops talking.
<b>DSP Talking Threshold (ms)</b>	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.
<b>DSP Silence Threshold (ms)</b>	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.
<b>Max Number of Video Feeds</b>	Set the maximum number of video feeds supported per meeting room.
<b>Audio Codec Preference</b>	Configures the preferred codecs for temporary accounts such as meeting participants who joined via link.
<b>Packet Loss Retransmission</b>	Packet Loss Retransmission configuration for temporary accounts (meeting participants without registered extensions who entered the meeting via link).
<b>Jitter Buffer</b>	<p>Select the jitter buffer method for temporary accounts such as meeting participants who joined via link.</p> <ul style="list-style-type: none"><li>● <b>Disabled:</b> Jitter buffer will not be used.</li><li>● <b>Fixed:</b> Jitter buffer with a fixed size (equal to the value of "Jitter Buffer Size")</li><li>● <b>Adaptive:</b> Jitter buffer with an adaptive size that will not exceed the value of "Max Jitter Buffer").</li><li>● <b>NetEQ:</b> Dynamic jitter buffer via NetEQ.</li></ul>

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 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 Web GUI or IVR.

o 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.

o 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. <ul style="list-style-type: none"><li>1: List all users currently in the conference call.</li><li>2: Kick all non-administrator participants from the conference call.</li><li>3: Mute/Unmute all non-administrator participants from the conference call.</li><li>4: Record the conference call.</li><li>8: Exit the caller menu and return to the conference.</li></ul>
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.

Meeting Caller IVR Menu

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

Google Service Settings Support

SoftwareUCM supports Google OAuth 2.0 authentication. This feature is used for supporting the SoftwareUCM meeting scheduling system. Once OAuth 2.0 is enabled, the SoftwareUCM conference system can access Google Calendar to schedule or update 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:

Save

Reset

Google Service Settings→OAuth2.0 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 SoftwareUCM to access 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.

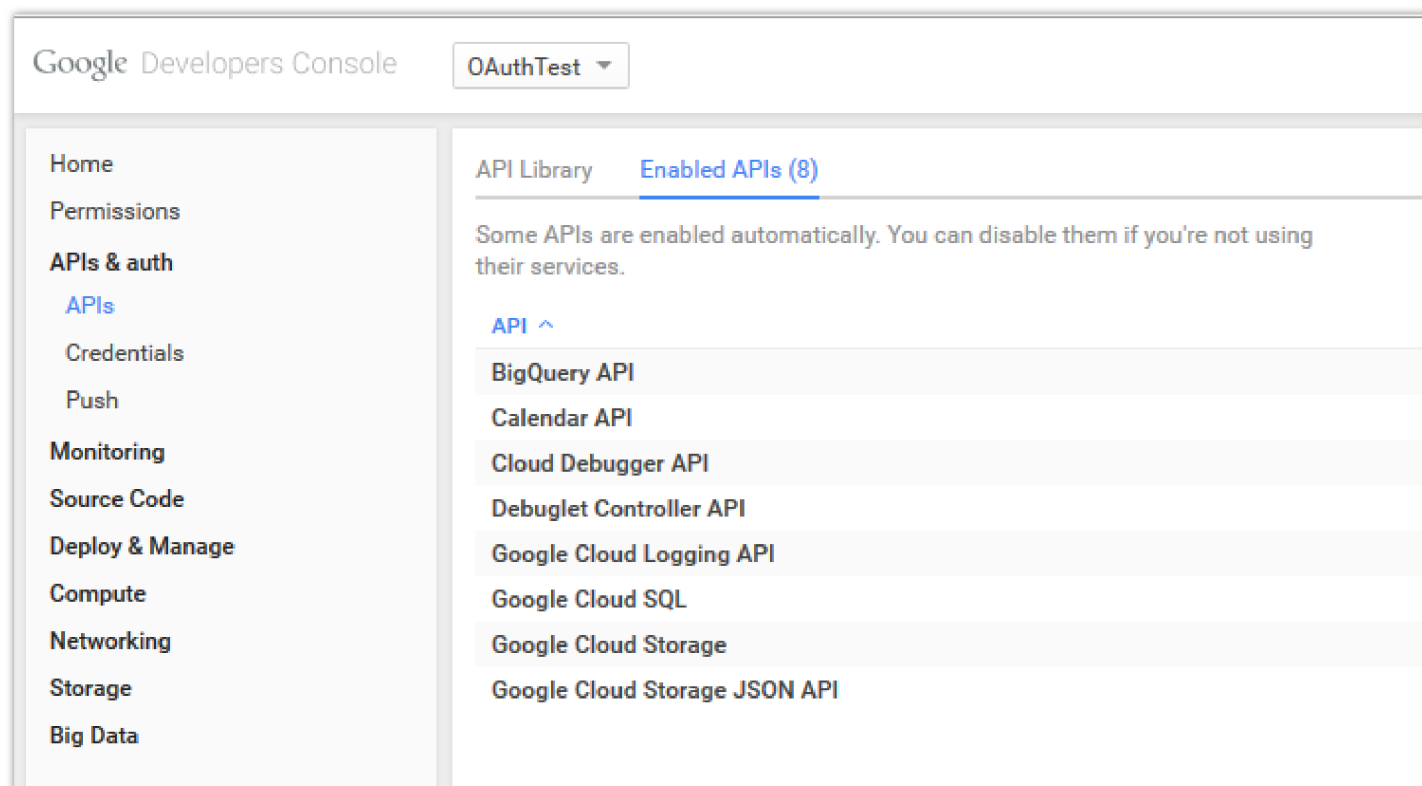
☒ Yes ☐ No

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

CreateCancel

Google Service → New Project

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



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 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 → OAuth2.0 Login

6. Once this has been done, the SoftwareUCM 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 disable.

## Schedule Meeting

Log in to the UCM Web GUI, open the **Basic Call Features → Multimedia Meeting → Meeting** page, and you can manage the reservation management of the meeting room. Users can create, edit, view, and delete conference room reservation records. The following is a set meeting room reservation, which shows the ongoing and pending reservations. Once the conference room is reserved, all users will be removed from the conference room at the start time, and extensions will no longer be allowed to enter the conference room. At the scheduled meeting time, UCM will send invitations to the extensions that have been selected to participate in the meeting. At the same time, it supports users to enter the meeting 10 minutes in advance. If the current meeting is occupied, enter the waiting room and wait (members joining the meeting in advance occupy global member resources, but it will be released after the scheduled meeting starts); otherwise, you can join the meeting directly and the meeting will be held in advance. After the meeting ends, the reservation record is transferred to the historical meeting list. History meeting displays the information of the ended and expired meetings.

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

Multimedia Meeting > Schedule Meeting

\* Meeting Subject

\* Time

2025-01-13

Password

\* Host

Allow User Invite

☒

Email Reminder (m)

☒ 60

Sync to Google Calendar

☐ [Google Services](#)

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.

Cancel

Save

Meeting Room

☐ Public Meeting Room

\* Time Zone

( UTC+01:00 ) Etc/GMT-1

\* Host Password

6940

Repeat

No Repeat

Call Participants

☒

Allowed to Override Host Mute

☐

\* Auto Record

None

Meeting Agenda

Schedule meeting Interface

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

	<ul style="list-style-type: none"><li>● Press ‘0’ to invite others to join the meeting with invited party’s permission</li><li>● Press ‘1’ to invite without invited party’s permission</li><li>● Press ‘2’ to create a multi-meeting room to another meeting room</li><li>● Press ‘3’ to drop all current multi-meeting rooms.</li></ul> <p><b>Note:</b> Meeting host is always allowed to access this menu.</p>
Call Participant	If enabled, the invited participants will be called upon meeting start time.
Allowed to Override Host Mute	If enabled, participants will be able to unmute themselves if they have been muted by the host.
Email Reminder (m)	Email reminders will be sent out x minutes prior to the start of the meeting. Valid range is 5-1440. 60 is the default value. 0 indicates not to send out email reminders for the meeting. <b>Note:</b> After editing the time of a single recurrence of a scheduled meeting, a cancelation email will now be sent out followed by a meeting update email.
Auto Record	If selected, the meeting will be recorded and saved as either a .WAV or .MKV file. The default filename is meeting-`\${Meeting Number}-\${UNIQUEID}`. Recordings can be downloaded from either the Meeting Recordings or the Meeting Video Recordings page. Video recordings require external storage to be available. When recording a screen share, only the screen share and meeting audio will be recorded.
Enable Google Calendar	Select this option to sync scheduled meeting with Google Calendar. <b>Note:</b> Google Service Setting OAuth2.0 must be configured on the PBX. Please refer to Google Services configuration section.
Meeting Agenda	Enter information about the meeting, e.g., the purpose of the meeting or the subjects that will be discussed in the meeting.
Invitees	Local extensions, remote extensions, and special extensions are supported.

Once the Meeting Schedule is configured, the scheduled meeting will be displayed as the below figure.

Multimedia Meeting

Room

Meeting

Meeting Recordings

Meeting Video Recordings

Pending Meeting

Meeting 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	<div></div> <div></div> <div></div>

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 Subject

Weekly\_Meeting

Room Number

70709021

Session state

Not started

Start Time

2025-01-15 10:00

Time Zone

Etc/GMT-1

Meeting Owner

admin

Password

Host Password

9283

Sync to Google Calendar

No

Repeat

No 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, SoftwareUCM will send INVITE to the extensions that have been selected for the conference.

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

Multimedia Meeting

Room

Meeting

Meeting Recordings

Meeting Video Recordings

Pending Meeting

Meeting 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	<div></div> <div></div> <div></div>

Total: 1

<

1

>

10 / page

Meeting Scheduled – Ongoing

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

Multimedia Meeting

RoomMeetingMeeting RecordingsMeeting Video Recordings

Pending MeetingMeeting History

Clear

Meeting Su...

Time:2025-01-01to2025-01-13

Search

Reset

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 he/she 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:

Multimedia Meeting

RoomMeetingMeeting RecordingsMeeting Video Recordings

Pending MeetingMeeting History

Clear

Meeting Su...

Time:2025-01-01to2025-01-13

Search

Reset

Meeting Subject

Meeting Room

Meeting Owner

Start Time

Meeting Duration

Repeat

Options

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

## Meeting Recordings

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

To record the Meeting call, when the meeting room is 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

RoomMeetingMeeting RecordingsMeeting Video Recordings

DownloadDownload AllDeleteClear

Local2025-01

Name

Room

Date

Size



Options

Meeting Recordings

Meeting Video Recordings

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

To record the Meeting call, when the meeting room is 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.

Call Statistics

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

1000

Call In

Answered

Name

Number

Admission Mode

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			

Meeting Report on CSV

IVR

Configure IVR

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

- Click on “Add” to add a new IVR.
- Click on



to edit the IVR configuration.

- Click on



to delete the IVR.

Create New IVR

Basic Settings

Key Pressing Events

Name :

GStest

Extension :

7000

Dial Trunk :

☐

Auto Record :

☐

Dial Other Extensions :

☐ All ☒ Extension ☐ Audio Conference ☐ Video Conference ☐ Call Queue

☐ Ring Group ☐ Paging/Intercom Groups ☐ Voicemail Groups ☐ Fax Extension

☐ Dial By Name

IVR Black/Whitelist :

Disable

Replace Display Name :

☐

Return to IVR Menu :

☐

Alert-info :

None

Prompt :

welcome

Upload Audio File

Add Prompt

Digit Timeout (s) :

3

Response Timeout :

10

Response Timeout Prompt :

ivr-create-timeout

Upload Audio File

Invalid Input Prompt :

invalid

Upload Audio File

Response Timeout Prompt Repeats :

3

Invalid Input Prompt Repeats :

3

Language :

Default

Create 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	



<b>IVR Webhook</b>	If enabled, call event notification and call control can be achieved via URL.
<b>Target URL</b>	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.
<b>Username</b>	Enter the username used to connect to the target URL.
<b>Password</b>	Enter the password used to connect to the target URL.
<b>Call Event</b>	<p>Select the call events to notify the IVR about.</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Notify IVR of Incoming Calls</li> <li>• Notify IVR of Answer</li> <li>• Notify IVR of DTMF Events</li> <li>• Notify IVR of End</li> </ul>
<b>Call Control</b>	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.
<b>Timeout Time (s)</b>	Configure the timeout time for receiving call control, default 2 seconds, the system tries up to three times after the timeout.
<b>Timeout/Invalid Settings</b>	
<b>Digit Timeout (s)</b>	Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, the UCM630X will consider the entries complete. The default timeout is 3s.
<b>Response Timeout (s)</b>	After playing the prompts in the IVR, the UCM630X will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout prompt will be played. The default setting is 10 seconds.
<b>Response Timeout Prompt</b>	Select the prompt message to be played when timeout occurs.
<b>Response Timeout Prompt Repeats</b>	Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3.
<b>Invalid Input Prompt</b>	Select the prompt message to be played when an invalid extension is pressed.
<b>Invalid Input Prompt Repeats</b>	Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3.
<b>PMS Wake-Up Call Service Mode</b>	
<b>PMS Wake-Up Call Service</b>	<p>If enabled, this IVR can be used with Wakeup Service to send notifications to specified destinations based on caller key presses.</p> <p>If enabled, key events will only be supported in standard mode. Time conditions will not be supported.</p>
<b>Other Settings</b>	
<b>Replace Display Name</b>	If enabled, the UCM will replace the caller display name with IVR name.
<b>Return IVR Menu</b>	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
<b>Alert-info</b>	When present in an INVITE request, the Alert-info header field specifies an alternative ringtone to the UAS.
<b>IVR Black/Whitelist</b>	If enabled only numbers inside of the Whitelist or outside of the Blacklist can be called from IVR.
<b>Internal Black/Whitelist</b>	Contain numbers, either of Blacklist or Whitelist.

<b>External Black/Whitelist</b>	This feature can be used only when Dial Trunk is enabled, it contains external numbers allowed or denied calling from the IVR, the allowed format is the following: Number1, number2, number3...
<b>Replace Display Name</b>	If enabled, the UCM will replace the caller display name with IVR name.
<b>Return to IVR Menu</b>	If enabled and if a call to an extension fails, the caller will be redirected to the IVR menu.
<b>Alert Info</b>	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.
<b>Timeout</b>	When exceeding the number of defined answer timeout, IVR will enter the configured event when timeout. If not configured, then it will Hangup.
<b>Invalid</b>	Configure the destination when the Invalid Repeat Loop is done.
<b>Time Condition</b>	Configure the time condition for each key press event, so that it goes to the corresponding destination within a specified time.

Edit IVR: test

Basic Settings

Key Pressing Events

Cancel

Save

Press 0

Destination: 

Extension

3001

Time Condition: 

Specific Time

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

[Add](#)

Press 1

Destination: 

Select an Option

Time Condition: 

All Time

[Add](#)

Press 2

Destination: 

Select an Option

Time Condition: 

All Time

[Add](#)

Press 3

Destination: 

Select an Option

Time Condition: 

All Time

[Add](#)

Press 4

Destination: 

Select an Option

Time Condition: 

All Time

[Add](#)

Key Pressing Events

## Black/Whitelist in IVR

In some scenarios, the IPPBX administrator needs to restrict the extensions that can be reached from IVR. For example, the company CEO and directors prefer only receiving calls transferred by the secretary, and some special extensions are used on IP surveillance endpoints which should not be reached from external calls via IVR for privacy reasons. SoftwareUCM has now added blacklist and whitelist in IVR settings for users to manage this.

Up to 500 extensions are allowed on the back/whitelist.

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

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

*Black/Whitelist*

## Create Custom Prompt

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

*Click on Prompt to Create IVR Prompt*

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

## Key Pressing Events

### Standard Key Event

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

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

Edit IVR: IVR-DISA

Basic Settings

Key Pressing Events

Cancel

Save

Press 0

Destination:

Select an Option

Time Condition:

Office Time

Destination:

Select an Option

Time Condition:

Holiday

All Time

Office Time

Out of Office Time

Holiday

Out of Holiday

Out of Office Time or Holiday

Office Time and Out of Holiday

Press 1

Destination:

Select an Option

Time Condition:

Key Pressing Events

## Note

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

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

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

## Custom Key Event

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

IVR > Create New IVR

Basic Settings

Key Pressing Events

Key Event Type

Standard

Custom

Key Events

Add

Delete

Clear

Key

12

Destination

Extension

1000

Time Condition

All Time

This new feature supports the following:

- Up to 100 custom key press events
- Each key combination can contain up to 8 characters (numbers and star (\*) only)

- Supports Time Conditions
- Different custom keys can have the same Destination and Time Condition

**Note**

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

**Voicemail**

**Configure Voicemail**

If the voicemail is enabled for SoftwareUCM 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

<b>Max Greeting Time (s)</b>	Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds.
<b>Dial ‘0’ For Operator</b>	If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator’s extension.
<b>Operator Type</b>	Configure the operator type; either an extension or a ring group.
<b>Operator Extension</b>	Select the operator extension, which will be dialed when users press 0 to exit the voicemail application. The operator extension can also be used in IVR.
<b>Max Messages Per Folder</b>	Configure the maximum number of messages per folder in users’ voicemail. The valid range is 10 to 1000. The default setting is 50.

<b>Max Message Time</b>	<p>Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the maximum message time. The default setting is 15 minutes. The available options are:</p> <ul style="list-style-type: none"><li>○ 1 minute</li><li>○ 2 minutes</li><li>○ 5 minutes</li><li>○ 15 minutes</li><li>○ 30 minutes</li><li>○ Unlimited</li></ul>
<b>Min Effective Message Time</b>	<p>Configure the minimum duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Message Time. The default setting is 3 seconds. The available options are:</p> <ul style="list-style-type: none"><li>○ No minimum</li><li>○ 1 second</li><li>○ 2 seconds</li><li>○ 3 seconds</li><li>○ 4 seconds</li><li>○ 5 seconds</li></ul> <p><b>Note:</b> Silence and noise duration are not counted in message time.</p>
<b>Announce Message Caller-ID</b>	<p>If enabled, the caller ID of the user who has left the message will be announced at the beginning of the voicemail message. The default setting is “No”.</p>
<b>Announce Message Duration</b>	<p>If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is “No”.</p>
<b>Play Envelope</b>	<p>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”.</p>
<b>Play Most Recent First</b>	<p>If enabled, it will play the most recent message first.</p>
<b>Allow User Review</b>	<p>If enabled, users can review the message following the IVR before sending.</p>
<b>Voicemail Remote Access</b>	<p>If enabled, external callers routed by DID and reaching VM will be prompted by the SoftwareUCM with 2 options:</p> <ul style="list-style-type: none"><li>○ <b><i>Press 1 to leave a message.</i></b></li></ul> <p>To leave a message for the extension reached by DID.</p> <ul style="list-style-type: none"><li>○ <b>Press 2 to access the voicemail management system.</b></li></ul> <p>This will allow the caller to access any extension VM after entering the extension number and its VM password. <b>Note:</b> This option applies to inbound calls routed by DID only. The default setting is “Disabled”.</p>

<b>Forward Voicemail to Peered UCMs</b>	<p>Enables the forwarding of voicemail to remote extensions on peered SIP trunks.</p> <p>The default setting is “Disabled”.</p>
<b>Voicemail Password</b>	<p>Configures the default voicemail password that will be used when an extension is reset.</p>
<b>Format</b>	<p>Warning: WAV files take up significantly more storage space than GSM files.</p>

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

Otherwise, the user can dial the voicemail access code (by default \*98) followed by the extension number and password 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 which case they can press # to submit the message.

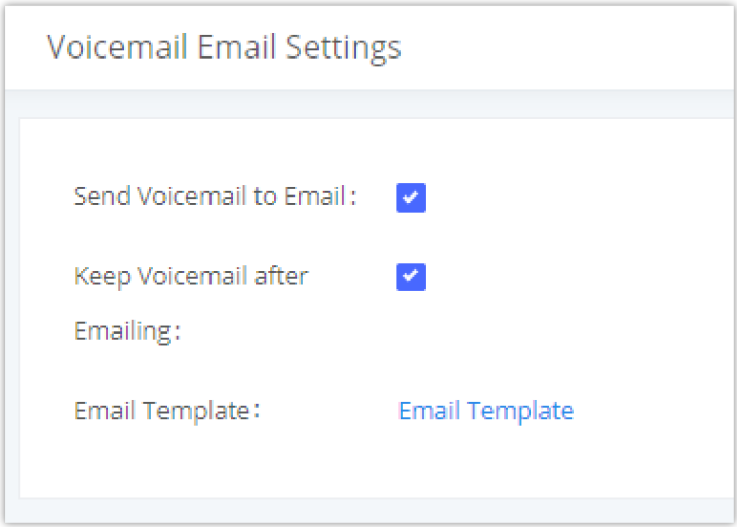
In case the caller is calling from an internal extension, they will be directly forwarded to the extension’s voicemail box. But if the caller is calling from outside the system and the incoming call is routed by DID to the destination extension, then the caller will be prompted with the choice to either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

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

Voicemail Email Settings



Voicemail Email Settings

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

Configure Voicemail Group

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

Voicemail > Create New Voicemail Groups

\* Extension

6600

\* Name

Name

\* Method

Forwarded

Shared

Voicemail Password

Voicemail Password

Email Address

Email Address

Shared Voicemail Status

Members

498

Available

Search

1000 " "

1003 "Johnny Doe"

1004 "John Marston"

1005 "Abigail Roberts"

1006 "Mary-Beth Gaskill"

1007 "Hosea Matthews"

<

>

0

Selected

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	<div>Select the preference for receiving and managing group voicemail.</div> <div><div><div>Forwarded:</div>Voicemail will be stored in the group voicemail box, and each voicemail group member will be forwarded a copy of it.</div><div><div>Shared:</div>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.</div></div>

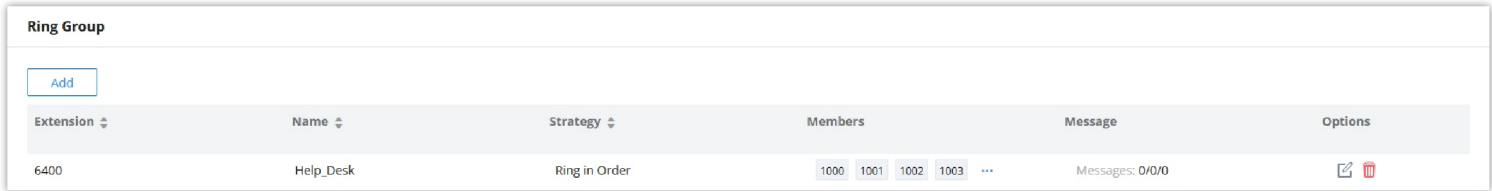
<b>Shared Voicemail Status</b>	If enabled, voicemail group status can be monitored via BLF. Green indicates no unread voicemail, and red indicates existing unread voicemail.
<b>Members</b>	Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list.
<b>Greet Prompt</b>	<p>This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Temporary Prompt</b>	<p>This voicemail prompt will be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Unavailable Prompt</b>	<p>This voicemail prompt will be played when user enters voicemail. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>

Ring Groups

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

Configure Ring Group

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



Ring Group

- Click on



to add ring group.

- Click on



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

- Click on



to delete the ring group.

Ring Groups > Create New Ring Groups

\* Ring Group Name

RingGroup1

\* Extension

6401

Local Members

11

Available

Search

Q

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ 1005

<

>

0

Selected

Search

Q

None

⤴

⤶

⤷

⤵

LDAP Members

0

Available

Search

Q

None

<

>

0

Selected

Search

Q

None

⤴

⤶

⤷

⤵

Ring Group Options

Ring Strategy

Ring in Order

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	<div>Select the ring strategy. The default setting is “Ring in order”.</div> <div><div><div>● Ring Simultaneously:</div><div>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.</div></div><div><div>● Ring in Order:</div><div>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.</div></div></div>
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	<div>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.</div> <div><b>Note:</b> Users can also refer to the page <b>PBX Settings</b>☒ <b>Voice Prompt</b>☒ <b>Custom Prompt</b>, where they could record new prompt or upload prompt files.</div>

<b>Ring Timeout on Each Member</b>	<p>Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 60 seconds.</p> <p><b>Note:</b> The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.</p>
<b>Auto Record</b>	<p>If enabled, calls on this ring group will be automatically recorded. The default setting is No. The recording files can be accessed from WebGUI <b>CDR</b> <b>Recording Files</b>.</p>
<b>Endpoint Call Forwarding Support</b>	<p>This allows the UCM to work with endpoint-configured call forwarding settings to redirect calls to ring group. For example, if a member wants to receive calls to the ring group on his mobile phone, he will have to set his endpoint's call forwarding settings to his mobile number. By default, it is disabled. However, this feature has the following limitations:</p> <ul style="list-style-type: none"> <li>• This feature will work only when call forwarding is configured on endpoints, not on the UCM.</li> <li>• If the outbound route is PIN-protected and requires authentication, the other ring group members will no longer receive the call after it is forwarded.</li> <li>• If the forwarded call hits voicemail, the other ring group members will no longer receive the call.</li> </ul>
<b>Replace Display Name</b>	<p>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.</p>
<b>Skip Busy Agent</b>	<p>If enabled, skip busy agents regardless of call waiting settings.</p>
<b>Enable Destination</b>	<p>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.</p>
<b>Default Destination</b>	<p>The call would be routed to this destination if no one in this ring group answers the call.</p> <p><b>Note:</b> Users can now set the voicemail of ring groups as routing destinations and IVR key press event destinations and to do so ring group must have their Default Destination set to Voicemail with Ring Group Extensions.</p>
<b>Voicemail</b>	<p>Whether to enable the voicemail for the ring group or not.</p>
<b>Voicemail Password</b>	<p>Configure the voicemail password (only numbers).</p>
<b>Email Address</b>	<p>Fill in the user's Email address (s), the voice message will be sent to this address (s).</p>
<b>Busy Prompt</b>	<p>This voicemail prompt will be played when the callee is in another call or is in DND mode. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Greet Prompt</b>	<p>This voicemail prompt will be played when the callee does not answer within their ring timeout period. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Temporary Prompt</b>	<p>This voicemail prompt well be played in all scenarios when it is configured (unregistered, unanswered/ring timeout, busy, DND). Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p> <p>Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.</p>
<b>Unavailable Prompt</b>	<p>This voicemail prompt will only be played when the callee's extension is unregistered. Priority: Temporary Prompt &gt; Busy Prompt/Unavailable Prompt &gt; Greet Prompt</p>

	Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .mp3/.wav/.ulaw/.alaw/.gsm suffix. The file size must be less than 5MB.
--	--

## 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 Ring Group with peer extensions is presented in the following:

1. Creating SIP Peer Trunk between both 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 edit button in the menu



, and check if **Sync LDAP Enable** is selected, this option will allow UCM\_A update remote LDAP server automatically from peer UCM\_B. In addition, **Sync LDAP Password** must match for UCM\_A and UCM\_B to sync LDAP contact automatically. Port number can be anything between 0~65535, and use the outbound rule created in step 1 for the **LDAP Outbound Rule** option.

Sync LDAP Enable

☒

\* Sync LDAP Password

.....

LDAP Outbound Rule

None

LDAP Dialed Prefix

LDAP Sync Method




wget

LDAP Last Sync Date

Unknown

Sync LDAP Server Options

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

VoIP Trunks						
VoIP Trunks    Trunk Group						
Add SIP Trunk						
Provider Name	Endpoint Type	Type	Hostname/IP	Username	Total Time for Outbound Calls (m)	Options
test	SIP	peer	192.168.1.1		Unlimited	  

Manually Sync LDAP Server

4. Under **Ring Groups** setting page, click “Add”. **Ring Groups** can be found under Web GUI→**Basic Call Features**→**Ring Groups**.
5. If LDAP server is synced correctly, **Available LDAP Numbers** box will display available remote extensions that can be included in the current ring group. Please also make sure the extensions in the peer UCM can be included into that UCM’s LDAP contact.



Ring Groups > Create New Ring Groups

\* Ring Group Name

Ring Group Name

\* Extension

6401

Local Members

☐ 11

Available

Search

Q

☐ 1005  
☐ 1006  
☐ 1007  
☐ 1008  
☐ 1009  
☐ 5002

<

>

Selected

0

Selected

Search

Q

None

✖

⬆

⬇

⬆

LDAP Members

☐ 4

Available

Search

Q

☐ test--1000 "John"  
☐ test--1001 "Anne"  
☐ test--1002 "David"  
☐ test--1003 "Bob"

<

>

Selected

0

Selected

Search

Q

None

✖

⬆

⬇

⬆

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 speaker. The SoftwareUCM paging and intercom can be used via feature code to a single extension or a paging/intercom group. This section describes the configuration of paging/intercom group under Web GUI→**Basic Call Features**→**Paging/Intercom**.

## Paging/Intercom Groups

### 2-way Intercom

Paging/Intercom > Create New Paging/Intercom Group

Disable

☐

\* Name

Name

\* Strategy

2-way Intercom

▼

\* Extension

Extension

Private Intercom

☐

Auto Record

☐

Replace Display Name

☐

\* Maximum Call Duration (s)

0

Custom Prompt

None

▼

Upload Audio File

Play Prompt to Caller

☐

\* Members

☐ 5 items Available

Search

Q

☐ 1000

☐ 1001

☐ 1002

<

>

☐ 0 item Selected

Search

Q

None

Cancel

Save

2-way Intercom

Parameter	Description
Disable	If disabled, the real-time and scheduled intercom will not be triggered.
Name	Configure intercom group name.
Strategy	Select “2-way Intercom”.
Extension	Configure the intercom group extension.
Private Intercom	If enabled, members can only hear the voice of the initiator and cannot hear the voice of other members. The initiator can hear the voice of all members.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the PBX will replace the caller display name with Intercom name.
First Answer Termination	Enabling this option will result in halting other phones from ringing once the intercom is answered.
Maximum Call Duration	Specify the maximum call duration in seconds. The default value 0 means no limit.
Custom Prompt	<p>This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on 'Upload Audio File', it will direct the users to upload the customized voice prompts.</p> <p><b>Note:</b> Users can also refer to the page <b>PBX Settings</b>→<b>Voice Prompt</b>→<b>Custom Prompt</b>, where they could record new prompt or upload prompt files.</p>
Play Prompt to Caller	Play the prompt to the caller.

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

Private Intercom

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

Paging/Intercom > Create New Paging/Intercom Group

Disable

☐

\* Name

2-Way\_Intercom

\* Strategy

2-way Intercom

\* Extension

Extension

Private Intercom

☒

Auto Record

☐

Replace Display Name

☐

\* Maximum Call Duration (s)

0

Custom Prompt

None

Play Prompt to Caller

☐

\* Members

☐ 5 items

Available

Search

☐ 0 item

Search

Upload Audio File

Private Intercom

Parameter	Configuration
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Name	Enter a name for the intercom
Type	Choose “Private Intercom”.
Extension	Configure the intercom group extension.
Auto Record	Enable this option to record in WAV format.
Replace Display Name	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
Maximum Call Duration (s)	The maximum allowed duration of a call in seconds. Default value is 0 (no limit).

<b>Custom Prompt</b>	This option sets a custom prompt to be used as an announcement to the person receiving a paging/intercom call. The file can be uploaded from the page “Custom Prompt”. Click “Upload Audio File” to add additional record.
<b>Members</b>	Selected members will receive paging/intercom calls to this paging/intercom group.
<b>Paging/Intercom Whitelist</b>	Only selected extensions will be able to use this paging /intercom group. If none is selected, all extensions will be able to use this paging/intercom group.

### 1-way Paging

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

Paging/Intercom > Create New Paging/Intercom Group

Disable

☐

\* Name

Page\_1

\* Strategy

1-way Paging

\* Extension

Extension

Video Broadcast

☐

Auto Record

☐

Replace Display Name

☐

Delayed Paging

☐

\* Maximum Call Duration (s)

0

Announcement File

None

Upload Audio File

Play Prompt to Caller

☐

\* Members

☐ 5 items

Available

Search

☐ 0 item

Search

1-way Paging

Parameter	Description
<b>Disable</b>	If disabled, the real-time and scheduled paging/intercom will not be triggered.
<b>Name</b>	Configure paging/intercom group name.
<b>Strategy</b>	Select “1-way Paging”.
<b>Extension</b>	Configure the paging/intercom group extension.
<b>Video Broadcast</b>	If checked, video paging will be supported. If the caller sends a video page, the paging group members will be able to receive and view the video.
<b>Auto Record</b>	Enable this option to record in WAV format (audio) and MKV format (video).

<b>Replace Display Name</b>	If enabled, the PBX will replace the caller display name with Paging/Intercom name.
<b>First Answer Termination</b>	Enabling this option will result in halting other phones from ringing once the intercom is answered.
<b>Delayed Paging</b>	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the prerecorded message will be played, and the call will end after it is finished playing.
<b>Maximum Call Duration</b>	Specify the maximum call duration in seconds. The default value 0 means no limit.
<b>Announcement File</b>	Configures an audio/video file to play to the paging members. This can be used to play preconfigured audio/video at the beginning of paging calls or to simply notify members that it is a paging/intercom call.
<b>Play Prompt to Caller</b>	Play the prompt to the caller.
<b>Members</b>	Select available users from the left side to the paging/intercom group member list on the right.
<b>Paging/Intercom Whitelist</b>	Select which extensions are allowed to use the paging/intercom feature for this paging group.

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

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

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

Video Broadcast

Using this feature, the user can send a video to the SIP endpoints which 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

Disable

☐

\* 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.

Replace Display Name

☐

Delayed Paging

☐

\* Maximum Call Duration (s)

0

Announcement File

None

Upload Video

Play Prompt to Caller

☐

\* Members

☐ 12 Available

Search

☐ 2001

☐ 2002

☐ 0 Selected

Search

Cancel

Save

Upload Announcement File

Multicast Paging

Paging/Intercom > Create New Paging/Intercom Group

Disable

☐

\* Name

Name

\* Strategy

Multicast Paging

\* Extension

Extension

Delayed Paging

☐

\* Maximum Call Duration (s)

0

Custom Prompt

None

Upload Audio File

Play Prompt to Caller

☐

\* Prompt Playback Count

1

\* Multicast Address/Port

Multicast IP Address

Port

Add Multicast IP Address

Paging/Intercom Allowlist

☐ Selected

☒ All

☐ 0 item Available

Search

☐ 5 items Selected

Search

1000

Cancel

Save

Multicast Paging

Parameter	Description
Disable	If disabled, the real-time and scheduled paging/intercom will not be triggered.
Name	Configure paging/intercom group name.
Strategy	Select “Multicast Paging”.

<b>Extension</b>	Configure the paging/intercom group extension.
<b>Delayed Paging</b>	If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the recorded message will be played, and the call will end after it is finished playing.
<b>Delay (s)</b>	Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds.
<b>Maximum Call Duration</b>	Specify the maximum call duration in seconds. The default value 0 means no limit.
<b>Custom Prompt</b>	This option is to set a custom prompt for a paging/intercom group to announce to caller. Click on ‘Prompt’, it will direct the users to upload the customized voice prompts. <b>Note:</b> Users can also refer to the page <b>PBX Settings</b> → <b>Voice Prompt</b> → <b>Custom Prompt</b> , where they could record new prompt or upload prompt files.
<b>Play Prompt to Caller</b>	Play the prompt to the caller.
<b>Prompt Playback Count</b>	Sets the number of times the prompt is played during the page/intercom. To ensure the prompt is played the specified number of times, please set an appropriate max call duration.
<b>Multicast IP Address/Port</b>	The allowed multicast IP address range is 224.0.1.0 – 238.255.255.255. <b>Note:</b> You can add up to 30 multicast addresses.
<b>Paging/Intercom Whitelist</b>	Select the extension which can initiate this paging. If none is selected, all extensions will be able to use this paging/intercom group.

**Multicast Community**

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



Paging/Intercom > Create New Multicast Community

\*

Name

Name

\*

Extension

Extension

Delayed Paging

\*

Maximum Call Duration (s)

0

Custom Prompt

None

Upload Audio File

Play Prompt to Caller

\*

Prompt Playback Count

1

\*

Multicast Paging Group

0

Available

Search

None

<

>

0

Selected

Search

None

Paging/Intercom

Selected

All

Cancel

Save

Multicast Community Parameter

Name	Enter the name of the multicast community.
Extension	Configure the extension number for the paging/intercom group. When this number is dialed, the paging/intercom will be initiated.
Delayed Paging	<p>If enabled, a caller can enter *82 before the paging group extension to start a delayed paging call. In a delayed paging call, the system will prompt the caller to record a message. Once the messaging is recorded and saved, and the configured delay has passed, the paging call will be sent out. When a paging group member answers the call, the precoded message will be played, and the call will end after it is finished playing.</p> <ul style="list-style-type: none"><li><b>Delay (s):</b> Configure the amount of delay in seconds after a message is recorded to send out the delayed paging call. Default is 5 seconds.</li></ul>
Maximum Call Duration (s)	<p>The maximum allowed duration of a call in seconds. Default value is 0 (no limit).</p> <p><b>Note:</b> Please note that the call duration that can be configured can be within the range 0 – 86400.</p>
Custom Prompt	<p>Choose the custom prompt to play for the callees at the beginning of the paging. The user can also directly upload a prompt file directly on this page.</p> <p><b>Note:</b> When uploading the custom prompt file, please make sure it respects the following requirements:</p> <ul style="list-style-type: none"><li>The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.</li><li>If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB.</li></ul> <p>File name can only contain alphanumeric characters and special characters -_</p>
Play Prompt to Caller	When this option is enabled, the prompt will be played back on the caller’s phone.

Prompt Playback Count	<p>Sets the number of times the prompt is played during the page/intercom. To ensure the prompt is played the specified number of times, please set an appropriate max call duration.</p> <p><b>Note:</b> The minimum number of playcounts which can be configured is 1 and the maximum is 10.</p>
Multicast Paging Group	<p>Configures multicast paging groups within a community. When dialing the extension number of the community, users may simultaneously initiate paging to linked multicast paging groups.</p>
Paging/Intercom Whitelist	<ul style="list-style-type: none"> <li>• <b>Selected:</b> Only selected extension will be allowed to initiate paging/intercom.</li> <li>• <b>All:</b> Allow all extensions and configured services to initiate paging/intercom.</li> </ul>

## Scheduled Paging/Intercom

### Pending Paging/Intercom

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

Paging/Intercom > Create New Scheduled Paging/Intercom

\* Paging/Intercom

\* Name

\* Caller

\* Start Date

2024-03-07

\* Start Time

Select time

Add Start Time

Repeat

No Repeat

Sync to Google Calendar

Google Services

Cancel

Save

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

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

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 which have been scheduled. The user can choose to display per day, week, or per month.

Paging/Intercom Groups

Paging/Intercom Groups

Multicast Community

Scheduled Paging/Intercom

Pending Paging/Intercom

Paging/Intercom Schedule

2024

Mar

Today

<

>

Mar 1 – 31, 2024

Day

Week

Month

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

Scheduled Paging/Intercom

Call Queue

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

Add Call Queue









Call queue settings can be accessed via **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	100010011002	 
6501	Sales	Ring All	1005	1003100410051002	 
6502	Marketing	Ring All	4005	40004001400240034004	 
6503	Support	Ring All	5009	50015002500350045006	 

Total: 4

<1>

10 / page

Goto

Call Queue Page

- Click on “Add” to add call queue.
- Click on



to edit the call queue.

- Click on



to delete the call queue.

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

Static and Dynamic Agents

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

Static Agents

SoftwareUCM allows a specific number of static agents based on the SoftwareUCM Plans and Add-On Options. This number follows this logic:

- If the number of supported extensions is **fewer than 100**, the maximum number of static agents will be equal to that number.
- If the number of extensions **exceeds 100**, the maximum number of static agents will be limited to 100.

Static agents can be configured on **Basic Call Features→Call Queue→Edit Queue→Agents**.

Important Notes:

The static number of agents limitation here refers to the entirety of the SoftwareUCM system, including all queues, not just a specific queue.

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 Setting** as shown below:

Call Queue > Global Queue Settings

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

Dynamic Agent Login Settings

Agent Login Code Suffix

Agent Logout Code Suffix

Example

If 6500 is the queue extension,

Agent Login Extension Suffix is \*,

Agent Logout Extension Suffix is \*\*,

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

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

Dynamic Agent Login Settings

**Note:**

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

Call Queue Feature Codes

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

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

**Note:**

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

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

Queue Recordings

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

Call Queue						
Call Queue Queue Recordings Queue Switchboard Call Queue Statistics						
Recording files are currently stored in <a href="#">GDM5</a> . 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.						
<div>DownloadDownload AllDeleteClear</div> <div>Local2024-10</div>						
<input type="checkbox"/>	Name	Caller	Call Queue	Date	Size	Options
<input type="checkbox"/>	q6502-4000-20241023-171020-1729 699819.28-5009.wav	4000	6502	2024-10-23 17:10:19	9.57 MB	10:27 <div></div> <div></div> <div></div>
<input type="checkbox"/>	q6503-1002-20241023-170556-1729 699555.15-5009.wav	1002	6503	2024-10-23 17:05:55	248.54 KB	00:16 <div></div> <div></div> <div></div>
<input type="checkbox"/>	q6500-5007-20241023-170358-1729 699436.10-5009.wav	5007	6500	2024-10-23 17:03:56	604.63 KB	00:54 <div></div> <div></div> <div></div>

Queue Recordings Page

- Click on



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



to delete the recording file.

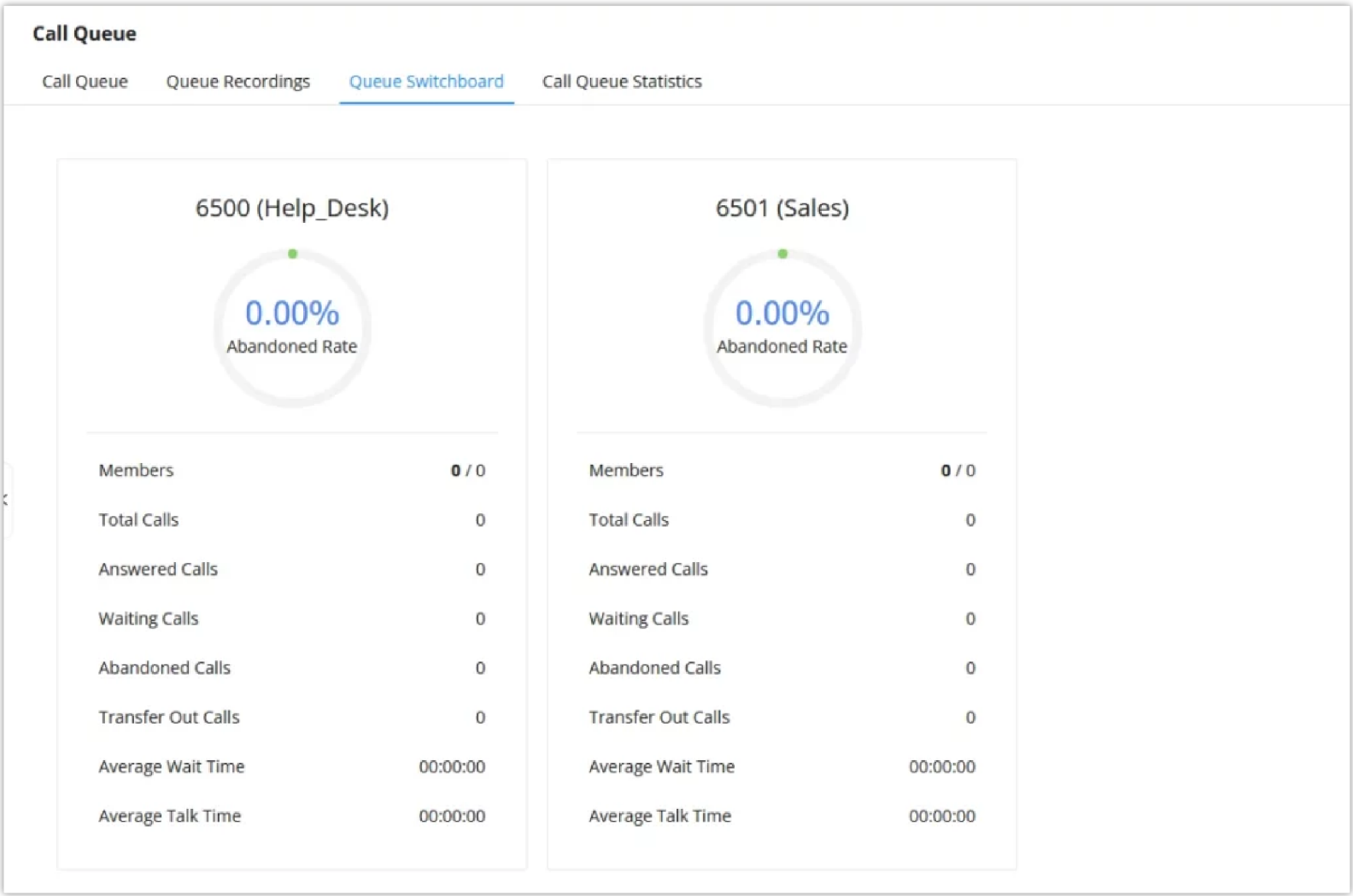
**Note:**

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**

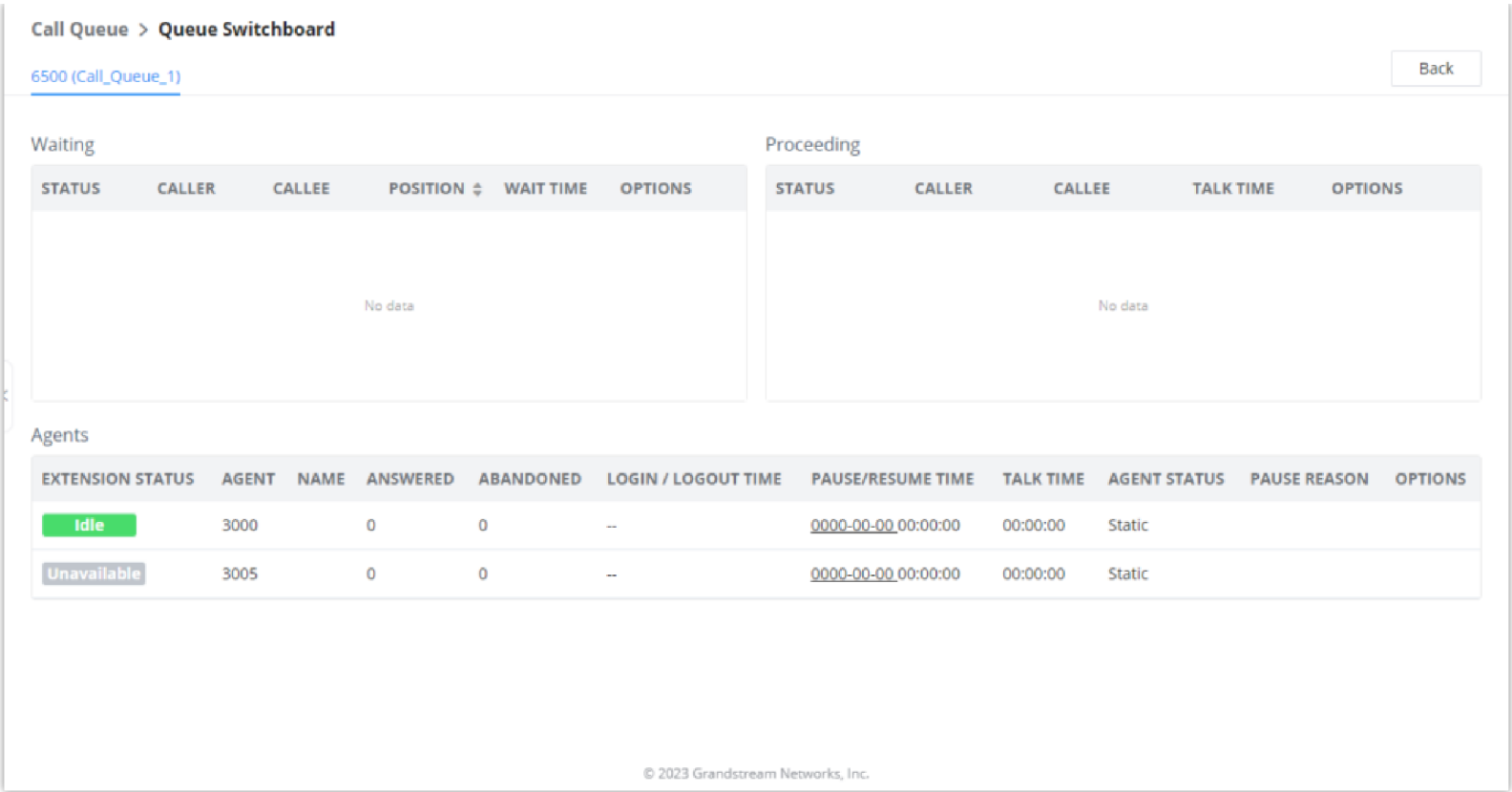
Switchboard is a Web GUI tool for call queue monitoring and management, admin can access to it from the menu **Basic Call Features**→**Call Queue** then press “Switchboard”.

Following page will be displayed:



Switchboard Summary

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



Call Queue Switchboard

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

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

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

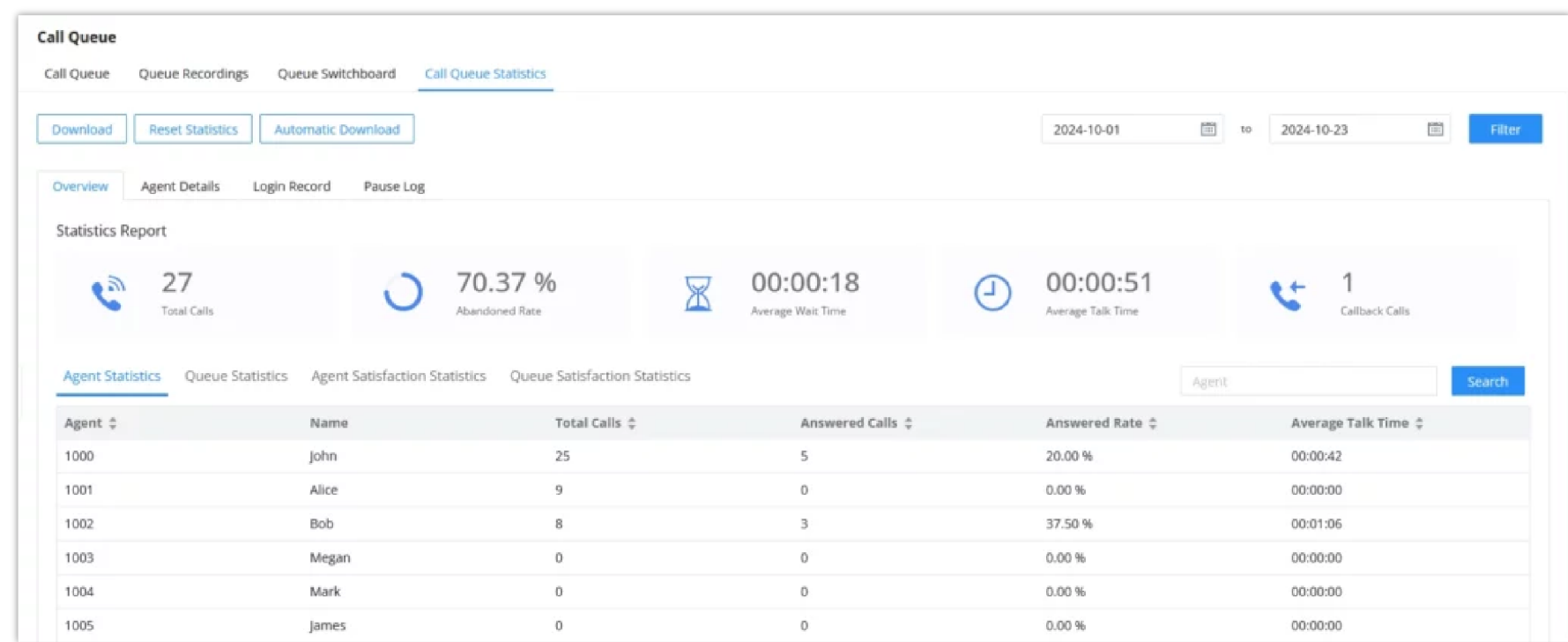


Queue Agent	User appointed by Super Admin to be a member of a queue extension. A queue agent can log into the UCM user portal with their extension number and assigned user password to manage their calls only.
-------------	---

Call Queue Statistics

Along with call center features, users can also gather detailed call queue statistics allowing them to make better changes/decision to manage better 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 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

By Week

Mon

23

Email

james@company.com

Email Template

Cancel

Save

Call Queue Statistics Automatic Download

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

Overview Tab

The overview page shows shows the following information:

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

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

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

Details

Queue

6500

Total Calls

29

Answered Calls

10

Abandoned Calls

19

Answered Rate

34.48 %

Abandoned Rate

65.52 %

Transfer Out Calls

2

Transfer Out Rate

6.90 %

Average Wait Time

00:00:16

Average Talk Time

00:00:46

Callback Calls

1

SLA

0.00 %

Callback SLA

0.00 %

Total Calls

Answered Calls

Abandoned Calls

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

Queue Statistics Details

Agent Details Tab

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

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

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

▼

Search

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

Agent details

Login Record Tab

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

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

Call QueueQueue RecordingsQueue SwitchboardCall Queue Statistics

DownloadReset StatisticsAutomatic Download

2024-10-01to2024-10-24Filter

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

▼

Search

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

Total: 3

<1>

10 / page

Login Record

Pause Log Tab

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

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

Call QueueQueue RecordingsQueue SwitchboardCall Queue Statistics

DownloadReset StatisticsAutomatic Download

2024-10-01to2024-10-24Filter

OverviewAgent DetailsLogin RecordPause Log

Statistics Report

Agent

▼

Search

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

Total: 4

<1>

10 / page

Pause Log

Global Queue Settings

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

Call Queue > Global Queue Settings

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

Dynamic Agent Login Settings

Agent Login Code Suffix

Agent Logout Code Suffix

Example

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

Agent Pause Reason

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

Agent Pause Reason Settings

Default

CancelSave

Global Queue Settings

Dynamic Agent Login Settings	
Agent Login Code Suffix	Configure the code to dial after the queue extension to log into the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log in.
Agent Logout Code Suffix	Configure the code to dial after the queue extension to log out of the queue (i.e. queue extension + suffix). If no suffix is configured, dynamic agents will not be able to log out.
Agent Pause Reason	
Agent Pause Reason Settings	Select the agent pause reason settings. <ul style="list-style-type: none"><li>Default: Use the default settings for the agent pause reason.</li><li>Custom: User the custom settings. These settings should be configured using they corresponding key for each status. The user can upload a custom prompt which will be played for the agent once they set the pause reason.</li></ul>
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 SoftwareUCM supports Speed Dial feature that allows users to call a certain destination by pressing one or four digits on the keypad. This creates a system-wide speed dial access for all the extensions on the SoftwareUCM.

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

User should first click on 

+ Add

 . Then decide from one digit up to four digits combination used for Speed Dial and select a dial destination from “Default Destination”. The supported destinations include extension, voicemail, conference room, voicemail group, IVR, ring group, call queue, page group, DISA, Dial by Name and external number.

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

Default Destination

Extension

▼

1000

▼

Cancel

Save







Speed Dial Destinations

Speed Dial

Add

Import

Export

Speed Dial Extension	Speed Dial	Default Destination	Default Destination	Options
7	Enable	Extension	1000	 
8	Enable	Extension	1001	 
9	Enable	Voicemail	1004	 

List of Speed Dial

Import Speed Dial







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

Speed Dial

Add

Import

Export

Speed Dial Extension	Speed Dial	Default Destination	Default Destination	Options
7	Enable	Extension	1000	 
8	Enable	Extension	1001	 
9	Enable	Voicemail	1004	 

Import Dial Speed

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

Import

Important

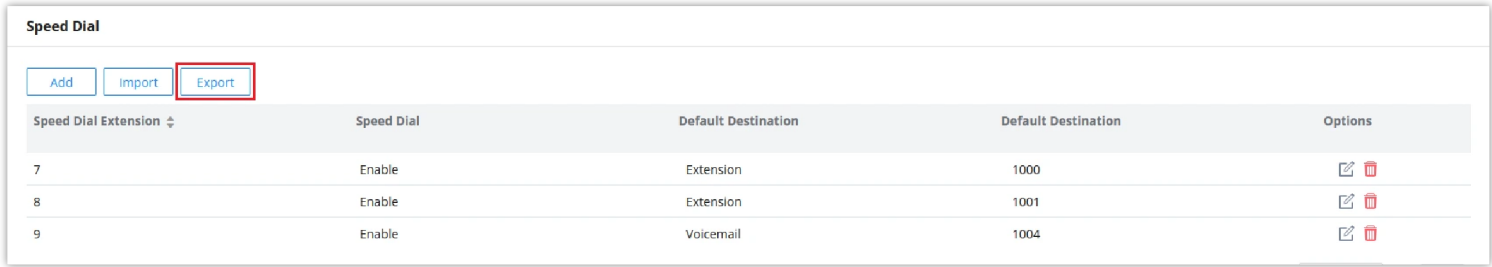
Please use UTF-8 encoding when importing a CSV file. CSV files can be opened using programs such as Notepad and saved as a UTF-8 encoded file.

**Alert**

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

## Export Speed Dial

To export speed dial entries, please click on export as the screenshot below shows, then choose the location where to save the csv file.



Export Dial Speed

## Event List

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

- Click on “Add” to add a new event list.
- Sort selected extensions manually in the Eventlist
- Click on



to edit the event list configuration.

- Click on



to delete the event list.

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



*Create New Event List*

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 remote BLF feature. Please note the SIP end points need support event list BLF in order to monitor remote extensions.

When an event list is created on the 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 end points register and subscribe to the local UCM event list, it can obtain the remote extension status from this event list. Once successfully configured, the event list page will show the status of total extension and subscribers for each event list. Users can also select the event URI to check the monitored extension's status and the subscribers' details.

- To configure LDAP sync, please go to SoftwareUCM Web GUI→Extension/Trunk→VoIP Trunk. You will see "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, LDAP Dialed Prefix will also be required. Both PBXs need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM PBX. However, it might not work the other way around depending on whether the non-UCM PBX supports event list BLF or remote monitoring feature.

## Feature Codes


Feature Codes allow the use to perform certain actions using the IP phone keypad. The user may enter the corresponding action they want to perform, the action will either be immediately performed by the UCM, or the user will follow the voice prompt to enter additional parameters for the option.



SoftwareUCM is by default configured with feature codes for different use cases, but users can change these codes manually by accessing **Basic Call Features → Feature codes**.


### Notes:






- When manually configuring feature codes, please make sure there is no conflict between the values.
- In order to avoid incompatibility, some feature codes do not support being nested by other numbers. (e.g. if a feature code is \*44, another feature code cannot be \*441). This is important because there are a few codes that can be used in conjunction with a series of digits.
- For example, users can dial \*72 (Call Forward Always Enable) followed by 1000 (\*721000) to set the forwarding destination as extension 1000. However, if there is another feature code configured as \*7210, it is impossible for SoftwareUCM to determine whether the user wants to use this code or to enable call forward always with extension 10 as the destination.








Feature Maps	
Blind Transfer	<ul style="list-style-type: none"><li>– Default code: #1</li><li>– 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.</li><li>– Options:<ul style="list-style-type: none"><li>• Disable</li><li>• Allow Caller: Enable the feature code on caller side only.</li><li>• Allow Callee: Enable the feature code on callee side only.</li><li>• Allow Both: Enable the feature code on both caller and callee.</li></ul></li></ul>
Attended Transfer	<ul style="list-style-type: none"><li>– Default code: *2</li><li>– Enter the code during active call. After hearing “Transfer”, you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. In case of the called party does not answer, users could press *0 to cancel the call and retrieve the first call leg.</li><li>– Options:<ul style="list-style-type: none"><li>• <b>Disable</b></li><li>• <b>Allow Caller:</b> Enable the feature code on caller side only.</li><li>• <b>Allow Callee:</b> Enable the feature code on callee side only.</li><li>• <b>Allow Both:</b> Enable the feature code on both caller and callee.</li></ul></li></ul>
Transfer Dialing Timeout Period (s)	Configures the dial timeout period of blind and attended transfers.
Seamless Transfer 	<ul style="list-style-type: none"><li>• Default code: *44 (Disabled by default).</li><li>• Seamless Transfer allows user to perform blind transfer using PBX feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple.</li><li>• During an active call use the feature code (*44 by default) followed by the number you want to transfer to in order to perform the seamless transfer.</li></ul> <p>(This feature code cannot be nested by other feature codes)</p>
Disconnect	<ul style="list-style-type: none"><li>– Default code: *0</li><li>– Enter the code during active call. It will disconnect the call.</li><li>– Options:<ul style="list-style-type: none"><li>• <b>Disable</b></li><li>• <b>Allow Caller:</b> Enable the feature code on caller side only.</li><li>• <b>Allow Callee:</b> Enable the feature code on callee side only.</li><li>• <b>Allow Both:</b> Enable the feature code on both caller and callee.</li></ul></li></ul>
Call Park	<ul style="list-style-type: none"><li>– Default code: #72</li><li>– Enter the code during active call to park the call.</li><li>– Options:<ul style="list-style-type: none"><li>• <b>Disable</b></li><li>• <b>Allow Caller:</b> Enable the feature code on caller side only.</li><li>• <b>Allow Callee:</b> Enable the feature code on callee side only.</li><li>• <b>Allow Both:</b> Enable the feature code on both caller and callee.</li></ul></li></ul>
Feature Code Input Timeout (ms)	Configure the maximum interval (ms) between digits for feature code activation.
Start/Stop Call Recording	<p>-Default code: *3</p> <ul style="list-style-type: none"><li>– Enter the code followed by # or SEND to start recording the audio call and the PBX will mix the streams natively on the fly as the call is in progress.</li></ul>

	<div>– Options:</div> <div><div><div>●</div><div>Disable</div></div><div><div>●</div><div>Allow Caller:</div><div>Enable the feature code on caller side only.</div></div><div><div>●</div><div>Allow Callee:</div><div>Enable the feature code on callee side only.</div></div><div><div>●</div><div>Allow Both:</div><div>Enable the feature code on both caller and callee.</div></div></div>
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	<div><div><div>●</div><div>Basic</div></div><div><div>●</div><div>Advanced</div></div></div> <div>If <b>Advanced</b> is selected, call forwarding can be set for all calls, internal calls and external calls. To do this, users can dial one of the feature codes below and then dial <b>0</b>, <b>1</b> or <b>2</b>.</div> <div>The feature code modifiers are as follow:</div> <div><div>☒ <b>0</b> corresponds to “<b>All calls</b>”.</div><div>☒ <b>1</b> refers to “<b>Internal calls</b>”. (calls that came within the PBX)</div><div>☒ <b>2</b> is used for “<b>External calls</b>”. (calls from outside the PBX)</div></div>
Do Not Disturb (DND) Activate	<div>Default code: <b>*77</b></div> <div>Activate DND feature to ignore any incoming calls.</div>
Do Not Disturb (DND) Deactivate	<div>Default code: <b>*78</b></div> <div>Deactivate DND Feature.</div>
Call Forward Busy Enable <div></div>	<div>Default Code: <b>*90</b></div> <div>Enables Call Forward Busy (CFB) for the dialing extension.</div> <div>Assuming feature code is xxx, the following call forward setting methods are available :</div> <div><b>Method 1:</b> Dial xxx and follow the system prompts.</div> <div><b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000).</div> <div><b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000).</div> <div>Methods 1 and 2 are supported in <b>Basic</b>.</div> <div>Methods 1 and 3 are supported in <b>Advanced</b>.</div> <div>(This feature code cannot be nested by other feature codes)</div>
Call Forward Busy Disable	<div>Default Code: <b>*91</b></div> <div>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:</div> <div><b>Basic:</b> Dial xxx.</div> <div><b>Advanced:</b> Dial xxx + 0/1/2.</div>
Call Forward No Answer Enable <div></div>	<div>Default Code: <b>*92</b></div> <div>Enables Call Forward No Answer (CFNA) for the dialing extension.</div> <div>Assuming feature code is xxx, the following call forward setting methods are available :</div> <div><b>Method 1:</b> Dial xxx and follow the system prompts.</div> <div><b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000).</div> <div><b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000).</div> <div>Methods 1 and 2 are supported in <b>Basic</b>.</div> <div>Methods 1 and 3 are supported in <b>Advanced</b>.</div> <div>(This feature code cannot be nested by other feature codes)</div>

<b>Call Forward No Answer Disable</b>	Default Code: <b>*93</b> Disables Call Forward No Answer (CFNA) for the dialing extension.Assuming feature code is xxx, use one of the following methods based on your Call Forward Setting Type: <b>Basic:</b> Dial xxx. <b>Advanced:</b> Dial xxx + 0/1/2.
<b>Call Forward Always Enable</b> 	Default Code: <b>*72</b> Enables Call Forward Always (CFA) for the dialing extension. Assuming feature code is xxx, the following call forward setting methods are available : <b>Method 1:</b> Dial xxx and follow the system prompts. <b>Method 2:</b> Dial xxx + target extension (e.g., xxx6000). <b>Method 3:</b> Dial xxx + 0/1/2 + target extension (e.g., xxx16000). Methods 1 and 2 are supported in <b>Basic</b> . Methods 1 and 3 are supported in <b>Advanced</b> . (This feature code cannot be nested by other feature codes)
<b>Call Forward Always Disable</b>	Default Code: <b>*73</b> 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: <b>Basic:</b> Dial xxx. <b>Advanced:</b> Dial xxx + 0/1/2.
<b>Remote Call Forward Enable</b>	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.
<b>Remote DND / Call Forward Settings</b>	
<b>Enable</b>	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.
<b>Remote Call Forward Busy Enable</b>	Default code: <b>*65</b> Configures and enables CFB for any extension.
<b>Remote Call Forward No Answer Enable</b>	Default code: <b>*66</b> Configures and enables CFNA for any extension.
<b>Remote Call Forward Always Enable</b>	Default code: <b>*67</b> Configures and enables CFU for any extension.
<b>Remote DND Enable</b>	Default code: <b>*68</b> Enables Do Not Disturb for any extension.
<b>Remote Call Forward Busy Disable</b>	Default code: <b>*651</b> Disables CFB for any extension.
<b>Remote Call Forward No Answer Disable</b>	Default code: <b>*661</b> Disables CFNA for any extension.
<b>Remote Call Forward Always Disable</b>	Default code: <b>*671</b> Disables CFU for any extension.
<b>Remote DND Disable</b>	Default code: <b>*681</b> Disables Do Not Disturb for any extension.
<b>Whitelist</b>	Extensions in this whitelist can configure DND or call forwarding for any extension via feature codes.

Feature Codes	
Voicemail	
<b>Voicemail Access Code</b> 	<ul style="list-style-type: none"><li>– Default code: <b>*98</b></li><li>– Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension’s voicemail box.</li></ul> (This feature code cannot be nested by other feature codes)
<b>My Voicemail</b>	<ul style="list-style-type: none"><li>– Default code: <b>*97</b></li><li>– Press *97 to access the voicemail box.</li></ul>
<b>Voicemail Group Access Code</b>	Default code: <b>*99</b> Dial this code to access group voicemail. If password is required, enter password followed by the pound (#) key.
<b>Direct Dial Voicemail Prefix</b>	Prefix used to dial directly to voicemail.
Call Queue	
<b>Agent Pause</b> 	Default code: <b>*83</b> Pause the agent in all call queues. (This feature code cannot be nested by other feature codes)
<b>Agent Unpause</b>	Default code: <b>*84</b> Unpause the agent in all call queues.
<b>Dynamic Agent Logout</b>	Default code: <b>*85</b> Log the dynamic agent out of all queues.
Call Pickup	
<b>Pickup on Ringing Prefix</b> 	Picks up a ringing call for another extension. Example: If the prefix is **, and there is a call ringing ext 1008, dial **1008 from a different extension to pick up the call to 1008. (This feature code cannot be nested by other feature codes)
<b>Pickup In-call Prefix</b>	Picks up an ongoing call for another extension. Example: If the feature code is *45, and ext 1008 is in a call, dialing *45 and then 1008 following the prompt will take that call. Note: The feature code user must be in the extension’s Allowed to seamless transfer list to pick up calls for it.
<b>Pickup Extension</b>	This is the feature code to pick up incoming calls for other extensions in the same pickup group. The default setting is *8.
Call Barging	
<b>Enable Spy</b>	Check this box to enable spy feature codes.
<b>Listen Spy</b> 	This is the feature code to listen in on a call to monitor performance. Your line will be muted, and neither party will hear you. The default setting is *54. (This feature code cannot be nested by other feature codes)
<b>Barge Spy</b> 	This is the feature code to join in on the call to assist both parties. The default setting is *56. (This feature code cannot be nested by other feature codes)

<b>Whisper Spy</b> 	<p>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.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>PMS</b>	
<b>PMS Wakeup Service</b>	Dial this feature code to access PMS Wakeup Service. You can add, update, activate or deactivate PMS Wakeup Service.
<b>PMS Remote Wakeup Service</b>	Dial this code to add, update, activate, and deactivate PMS wakeup service for other extensions.
<b>Update PMS Room Status</b> 	<p>2 methods are available:</p> <p>1. Dial the room status feature code + housekeeper code, listen to the prompt and then the dial the appropriate key for the desired room status. Example: The housekeeper with housekeeper code 0001 dials *230001, listens to the room status options prompt, and then dials 1 to change room status to Available.</p> <p>2. Dial room status feature code*housekeeper code*desired room status option key to quickly change the room status without needing to go through the system voice prompts. Example: Housekeeper with Housekeeper code 0001 dials *23*0001*1 to change room status Available.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>Misc</b>	
<b>Paging Prefix</b> 	<p>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.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>Intercom Prefix</b> 	<p>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.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>Blacklist Add</b>	Follow the voice prompt to add a caller ID to blacklist.
<b>Blacklist Last Caller</b>	Add the last inbound caller ID number to blacklist.
<b>Blacklist Remove</b>	Follow the voice prompt to remove a caller ID from blacklist.
<b>Direct Dial Mobile Phone Prefix</b> 	<p>If calling mobile phone numbers is permitted, use this prefix plus the extension number to dial the mobile phone number of this extension directly.</p> <p>(This feature code cannot be nested by other feature codes)</p>
<b>Call Completion Request</b>	If the caller wants to use CC to complete a call, he/she can dial this code. After the CC has been registered successfully, the system will start to monitor the status of the callee. The system will call back the caller when the callee's extension is available.
<b>Call Completion Cancel</b>	If the caller has requested CC successfully, and he/she doesn't need to call back anymore, he/she can dial this code to cancel the request.
<b>Presence Status</b>	Dial this feature code to set the presence status of the extension.
<b>Call Flip</b>	<p>– Default code: <b>*46</b></p> <p>– Dial this code to move the call of this extension from another device to the current device.</p>






Feature Codes

Feature Maps

DND / Call Forward

Feature Codes

Feature codes marked with  do not support being nested by other numbers (e.g., When \*90 is used as a feature code, another number cannot start with that same \*90 such as \*901).

Default All

Call Forward Setting Type

Basic

Advanced


If **Advanced** is selected, users will be able to set call forwardings for all calls, internal calls and external calls individually with their own unique feature code modifiers, allowing for greater control over call forwardings. To do this, dial one of the feature codes below and then dial 0, 1 or 2 afterwards to specify setting the call forwarding for all calls, internal calls or external calls respectively.

\*

Do Not Disturb (DND) Activate


\*77

\*

Call Forward Busy Enable 


\*90

\*

Call Forward No Answer Enable 

\*92

\*

Call Forward Always Enable 

\*72

\*

Do Not Disturb (DND) Deactivate

\*78

\*

Call Forward Busy Disable

\*91

\*

Call Forward No Answer Disable

\*93

\*

Call Forward Always Disable

\*73

Remote DND / Call Forward Settings

Enable

Cancel

Save


DND / Call Forward

Feature Codes

Feature Maps


DND / Call Forward

Feature Codes

Feature codes marked with  do not support being nested by other numbers (e.g., When \*90 is used as a feature code, another number cannot start with that same \*90 such as \*901).

Default All

\*

Voicemail Access Code 

\*98

\*

Voicemail Group Access Code

\*99

\*

My Voicemail


\*97

\*

Direct Dial Voicemail Prefix

\*

\*

Agent Pause 

\*83

\*

Dynamic Agent Logout


\*85

\*

Agent Unpause

\*84

\*

Pickup on Ringing Prefix 

\*\*

\*

Pickup Extension

\*8

\*





Pickup In-call Prefix

\*45

Enable/Disable Feature codes

## Parking Lot

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	
<div>Add</div>			
Extension ↕	Name ↕	Slots ↕	Options
700	DefaultLot	701-720	 
800	Sales	801-820	 

Parking Lot

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



Parking Lot > Create New Parking Lot

\* Parking Lot Extension

\* Parking Slots

\* Parking Timeout (s)

300

Forward to Destination on Timeout

☐

Ring-All Callback on Timeout

☐

Cancel

Save

\* Parking Lot Name

Use Parking Slot as Extension

☐

Music on Hold Playlists

Default

Fallover Destination

Parking Lot Timeout Alert-Info

None

New Parking Lot

<b>Parking Lot Extension</b>	<ul style="list-style-type: none"><li>Default Extension: <b>700</b></li><li>During an active call, initiate blind transfer and then enter this code to park the call.</li></ul>
<b>Parking Lot Name</b>	<ul style="list-style-type: none"><li>Set a name to the parking lot</li></ul>
<b>Parked Slots</b>	<ul style="list-style-type: none"><li>Default Extension: <b>701-720</b></li><li>These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.</li></ul>
<b>Use Parklot as Extension</b>	<ul style="list-style-type: none"><li>If checked, the parking lot number can be used as extension. The user can transfer the call to the parking lot number to park the call. Please note this parking lot number range might conflict with extension range.</li></ul>
<b>Parking Timeout (s)</b>	<ul style="list-style-type: none"><li>Default setting is <b>300</b> seconds, and the maximum limit is <b>99.999</b> seconds.</li><li>This is the timeout allowed for a call to be parked. After the timeout, if the call is not picked up, the extension who parks the call will be called back.</li></ul>
<b>Music On Hold Classes</b>	Select the Music on Hold Class.
<b>Fallover Destination</b>	Configures a callback failover destination when the extension that is called back is busy. The call will be routed to the destination number and this reduces the chance of dropping parked calls.
<b>Ring All Callback on Timeout</b>	If enabled, all registered endpoints of the extension will ring when callback occurs. Otherwise, only the original endpoint will be called back.
<b>Forward to destination on timeout</b>	If enabled, the call will be routed to the configured destination upon timeout. Otherwise, the call will be routed back to the original caller.
<b>Timeout Destination</b>	This option appears once Forward to Destination on Timeout is enabled. Upon park timeout, the call will be routed to the configured destination.
<b>Parking Lot Timeout Alert-Info</b>	Adds an Alert-Info header to parking lot callbacks after the Parking Timeout has been reached.

Parking Lot

Call Park

The SoftwareUCM provides call park and call pickup features via feature code.

Park a Call

There are two feature codes that can be used to park the call.

- **Feature Maps→Call Park (Default code #72)**

During an active call, press #72 and the call will be parked. Parking lot number (default range 701 to 720) will be announced after parking the call.

- **Feature Misc→Call Park (Default code 700)**

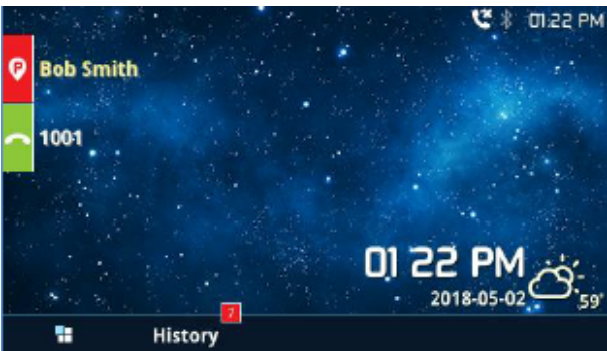
During an active call, initiate blind transfer (default code #1) and then dial 700 to park the call. Parking lot number (default range 701 to 720) will be announced after parking the call.

**Retrieve Parked Call**

To retrieve the parked call, simply dial the parking lot number and the call will be established. If a parked call is not retrieved after the timeout, the original extension who parks the call will be called back.

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

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



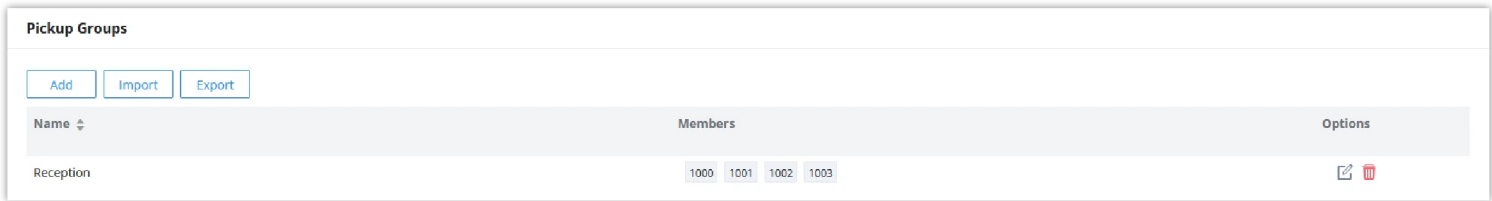
Monitored Call Park CID name

**ADVANCED CALL FEATURES**

**Pickup Groups**

The SoftwareUCM 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



to create a new pickup group.

- Click the



button to upload the pickup group information in CSV format.

- Export

Click on



- Click on



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

**Pickup Groups > Edit Pickup Groups: Reception**

---

\* Name

\* Members

<input type="checkbox"/> 7 Available	<input type="checkbox"/> 4 Selected
Search <input type="text"/>	Search <input type="text"/>
<input type="checkbox"/> 1004	<input type="checkbox"/> 1000
<input type="checkbox"/> 1005	<input type="checkbox"/> 1001
<input type="checkbox"/> 1006	<input type="checkbox"/> 1002
<input type="checkbox"/> 1007	<input type="checkbox"/> 1003
<input type="checkbox"/> 1008	
<input type="checkbox"/> 1009	

## Configure Pickup Feature Code

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

Call Pickup

\* Pickup on Ringing Prefix ⓘ

☒

\* Pickup Extension

☒

\* Pickup In-call Prefix

☐

Call Barging

Enable Spy

☐

\* Barge Spy ⓘ

\* Listen Spy ⓘ

\* Whisper Spy ⓘ

PMS

\* PMS Wakeup Service

☒

\* Update PMS Room Status ⓘ

☒

\* PMS Remote Wakeup Service

☒

Misc

### Edit Pickup Feature Code

## Dial By Name

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

## Dial by Name Configuration

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

Dial By Name > Create New Dial By Name

\* Name

Name

\* Extension

7101

Custom Prompt

None

Upload Audio File

Local Members

11 Available

Search

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ 1005

<

>

0 Selected

Search

None

LDAP Phonebook

1 Available

Search

☐ ou=test,dc=pbx,dc=co...

<

>

0 Selected

Search

None

### Create Dial by Name Group

Extensions > Edit Extension: 1000

Basic Settings

Media

Features

Voicemail

Custom Time

Wave Client

Follow Me

Advanced Settings

General

\* Extension

1000

CallerID Number

\* Call Privileges

Local

\* SIP Password

AuthID

\* Concurrent Registrations

3

Disable This Extension

User Settings

First Name

Last Name

Email Address

\* User/Wave Password

\* User Portal/Wave Privileges

Default

Mobile Number

+1

Add / Edit Privileges

Configure Extension First Name and Last Name

## 1. Name

Enter a Name to identify the Dial by Name group.

## 2. Extension

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

## 3. Custom Prompt

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

## 4. Available Extensions/Selected Extensions

Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have a valid first name and last name configured under Web GUI→**Extension/Trunk**→**Extensions** in order to be searchable in Dial By Name directory through IVR. By specifying the extensions here, the administrators can make sure unscreened calls will not reach the company employee if he/she does not want to receive them directly.

## 5. Prompt Wait Time

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

## 6. Query Type

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

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

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

## 7. Select Type

Specify the select type on the searching result. The IVR will confirm the name/number for the party the caller would like to reach before dialing out.

By Order: After the caller enters the digits, the IVR will announce the first matching party's name and number. The caller can confirm and dial out if it is the destination party, or press \* to listen to the next matching result if it is not the desired party to call.

By Menu: After the caller enters the digits, the IVR will announce 8 matching results. The caller can press number 1 to 8 to select and call or press 9 for results in next page.

The Dial by Name group can be used as the destination for inbound route and key pressing event for IVR. The group name defined here will show up in the destination list when configuring IVR and inbound route. If Dial by Name is set as a key pressing event for IVR, user could use ‘\*’ to exit from Dial by Name, then re-enter IVR and start a new event. The following example shows how to use this option.

IVR > Create New IVR

Basic Settings

Key Pressing Events

Key Event Type

☒ Standard

☐ Custom

Key Events

Key0

Destination

Dial By Name

Test

Time Condition

All Time

Key1

Destination

Extension

1000

Time Condition

All Time

Key2

Destination

Voicemail

1007

Time Condition

All Time

Dial By Name Group In IVR Key Pressing Events

Inbound Routes > Create New Inbound Rule

Auto Record

☐

Fax Detection

☐

Block Collect Calls

☐

CallerID Setting

Prepend Trunk Name

☐

Set CallerID Info

☐

CallerID Name Lookup

☐

Inbound Mode

Inbound Multi-Mode

☐

Default Mode

\* Default Destination

Dial By Name

Test

Time Condition

Add

Time Condition	Time	Week	Month	Day	Destination	Options
----------------	------	------	-------	-----	-------------	---------

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 SoftwareUCM, the user can then dial out via the SIP trunk connected to the SoftwareUCM as it is an internal extension.

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

- Click on



to add a new DISA.

- Click on



to edit the DISA configuration.

- Click on



to delete the DISA.

DISA > Create New DISA

\* Name

\* Password

Privilege

Internal

▼

\* Response Timeout (s)

\* Digit Timeout (s)

Allow Hang-up

☐

Replace Display Name

☐

Create New DISA

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

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.



<b>Digit Timeout</b>	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
<b>Allow Hangup</b>	If enabled, during an active call, users can enter the 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”.
<b>Replace Display Name</b>	If enabled, the UCM will replace the caller display name with the DISA name.

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

### Callback

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

The callback feature works as follows:

1. Configure a new callback on the SoftwareUCM.
2. On the SoftwareUCM, configure destination of the inbound route for callback.
3. Save and apply the settings.
4. The user calls number of the SoftwareUCM using the mobile phone, which goes to callback destination as specified in the inbound route.
5. Once the user hears the ringback tone from the mobile phone, hang up the call on the mobile phone.
6. The SoftwareUCM 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 SoftwareUCM instead of to the mobile phone directly. Therefore, the user will not be charged on mobile phone services for long distance or international calls.

To configure callback on the SoftwareUCM, go to Web GUI > **Advanced Call Features** > **Callback** page and click on 

Add

 . Configuration parameters are listed in the following table.

<b>Name</b>	Configure a name to identify the Callback. (Enter at least two characters)
<b>CallerID Pattern</b>	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the CallerID match this pattern so that the caller can get callback after hanging up the call. Note: If leaving as blank, all numbers are allowed to use this callback.
<b>Outbound Prepend</b>	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.
<b>Delay Before Callback</b>	Configure the number of seconds to be delayed before calling back the user.
<b>Destination</b>	Configure the destination which the callback will direct the caller to. Two destinations are available: <ul style="list-style-type: none"><li>• <b>IVR</b></li><li>• <b>DISA</b></li></ul>

	The caller can then enter the desired number to dial out via IPPBX trunk.
--	---

Scheduled Call

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 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

Scheduled Call

Upload Audio File

Custom Date

☐

\* Date

Select date

\* Time

Select time

\* Members

☐ 5 Available

Search

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

<

>

☐ 0 Selected

Search

None

Cancel

Save

Scheduled Call

Fax Sending

The SoftwareUCM supports sending Fax via 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 uploade the pdf file that you wish to send as a fax.

Fax Sending

It is recommended to use A4 vertical size PDF files to accommodate most printer formats. Otherwise, sending may fail due to the printer not supporting the sent format.

\* External Fax Number

Fax File

Test\_Fax.pdf

Send

File Send Progress

Delete

Clear

Fax Sending in Web GUI

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

Fax Sending

It is recommended to use A4 vertical size PDF files to accommodate most printer formats. Otherwise, sending may fail due to the printer not supporting the sent format.

\* External Fax Number

Fax File

Choose File to Upload

Send

File Send Progress

Delete

Clear

Q External Fax Number

Q

<input type="checkbox"/>	Name	Date	Sender	External Fax Number	Current Progress	Options
<input type="checkbox"/>	Test_Fax.pdf	2025-01-13 12:27:01 UTC-01:00	admin	0123456789	<div>Sending... 5%</div>	<div></div>

Fax Send Progress

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

Fax/T.38

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

to edit the Fax extension.

- Click on

to delete the Fax extension.

Fax/T.38 > 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













<b>Enable Error Correction Mode</b>	<p>Configure to enable Error Correction Mode (ECM) for the Fax.</p> <p>The default setting is “Yes”.</p>
<b>Maximum Transfer Rate</b>	<p>Configure the maximum transfer rate during the Fax rate negotiation.</p> <p>The possible values are 2400, 4800, 7200, 9600, 12000, and 14400.</p> <p>The default setting is 14400.</p>
<b>Minimum Transfer Rate</b>	<p>Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000, and 14000. The default setting is 2400.</p>
<b>Max Concurrent Sending Fax</b>	<p>Configure the concurrent fax that can be sent by SoftwareUCM. Two modes “Only” and “More” are supported.</p> <ul style="list-style-type: none"> <li>○ <b>Only</b></li> </ul> <p>Under this mode, the SoftwareUCM allows only a single user to send a fax at a time.</p> <ul style="list-style-type: none"> <li>○ <b>More</b></li> </ul> <p>Under this mode, the SoftwareUCM supports multiple concurrent faxes sending by the users. By default, this option is set to “only”.</p>
<b>Fax Queue Length</b>	<p>Configure the maximum length of Fax Queue from 6 to 10.</p> <p>The default setting is 6.</p>

<b>User Information in Fax Header</b>	If enabled, this will give users the option to send a special header in SIP fax messages.
<b>Fax Header Information</b>	Adds fax header into the fax file.
<b>Default Email Address</b>	<p>Configure the Email address to send the received Fax to if the user’s Email address cannot be found.</p> <p><b>Note:</b></p> <p>The extension’s Email address or the Fax’s default Email address needs to be configured to receive Fax from Email. If neither of them is configured, Fax will not be received from email.</p>
<b>Template Variables</b>	<p>Fill in the “Subject:” and “Message:” content, to be used in the Email when sending the Fax to the users. The template variables are:</p> <ul style="list-style-type: none"><li>○ \${CALLERIDNUM} : Caller ID Number</li><li>○ \${CALLERIDNAME} : Caller ID Name</li><li>○ \${RECEIVEEXTEN} : The extension to receive the Fax</li><li>○ \${FAXPAGES} : Number of pages in the Fax</li><li>○ \${VM_DATE} : The date and time when the Fax is received. (Format: MM/dd/yyyy hh:mm:ss )</li></ul>
<b>Send PDF Files Only</b>	If enabled, fax emails will no longer attach TIFF files. Only PDF files will be attached.
<b>Enable Fax Resend</b>	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 &gt; Fax Sending</i> to allow manual resending.
<b>Max Resend Attempts</b>	<p>Configures the number of the maximum attempts to resend the fax.</p> <p>The default value is set to 5.</p>
<b>Fax Resend Frequency</b>	<p>Configures the Fax Resend Frequency.</p> <p>The default value is set to 50.</p>

FAX/T.38 Settings

Announcement Center

The SoftwareUCM supports Announcement Center feature which allows users to pre-record and store voice message into the SoftwareUCM 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			
<a href="#">Add Announcement Center</a>			
Code ↕	Name ↕	Options	
33	Announcement_A	 	
Total: 1		  	10 / page  Goto <input type="text"/>
<a href="#">Add Group</a>			
Number ↕	Name ↕	Members	Options
66	Group_A	<div>100010011002</div>	 
Total: 1		  	10 / page  Goto <input type="text"/>

Announcement Center

Announcement Center Settings

Announcement Center > Create New Announcement Center

\* Name

\* Code

\* Custom Prompt

Upload Audio File

\* Ring Timeout (s)

30

\* Auto Answer

No

Announce Message Caller-ID

☐

Cancel

Save

Create 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. <b>Note:</b> The combination number must not conflict with any number in the system such as extension number or conference number.
Custom Prompt	<p>This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page ‘Custom Prompt’. Click ‘Prompt’ to add additional record.</p> <p><b>Note:</b> When uploading a custom, please ensure that the custom prompt file respect the following requirements.</p> <ul style="list-style-type: none"><li>• The audio file must be less than 5 MB in file size with a file extension of .mp3/. wav/. ulaw/. alaw/. gsm. WAV files must be PCM encoded, 16 bit mono, and 8000Hz.</li><li>• If uploading a compressed file, the file extension must be .tar/.tgz/.tar.gz, and the file size must not exceed 50MB.</li></ul> <p>File name can only contain alphanumeric characters and special characters -_</p>
Ring Timeout	Configure the ring timeout for the group members. The default value is 30 seconds.
Auto Answer	If set to <b>Yes</b> , the Auto answer will be enabled by the members.
Call Privileges	Please select the permission level for outgoing calls.

<b>Announce Message Caller-ID</b>	If enabled, the caller’s CID number will be announced before playing the uploaded prompt. This CID will also be used as the displayed CID of the call.
-----------------------------------	--

Group Settings

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



to add new group.

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

Announcement Center > Create New Group

\* Name

Group\_B

\* Number

77

Local Members

☐ 8

Available

Search

Q

☐ 1003

☐ 1004

☐ 1005

☐ 1006

☐ 1007

☐ 1008

<

>

☐ 3

Selected

Search

Q

☐ 1000

☐ 1001

☐ 1002

☐ 4

Available

Search

Q

☐ test--1000 "John"

☐ test--1001 "Anne"

☐ test--1002 "David"

☐ test--1003 "Bob"

<

>

☐ 0

Selected

Search

Q

None

Announcement Center Group Configuration

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

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

5. Click



[Add Announcement Center](#)

to create a new Announcement Center.

- 6. Give a name to the newly created Announcement Center.
- 7. Specify the code which will be used with group number to send the voice message to.
- 8. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click "Prompt" link and follow the instructions in that page.

Announcement Center > Create New Announcement Center

\* Name

\* Code

\* Custom Prompt

Upload Audio File

\* Ring Timeout (s)

30

\* Auto Answer

No

Announce Message Caller-ID

Cancel

Save

Announcement Center Code Configuration

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the SoftwareUCM. All the members in group 666 which are extension 1000, 1001 and 1002 will receive this voice message after they pick up the call.

Announcement Center

Add Announcement Center

Code	Name	Options
33	Announcement_A	<div></div>

Total: 1

<1>

10 / pageGoto

Add Group

Number	Name	Members	Options
66	Group_A	100010011002	<div></div>

Total: 1

<1>

10 / pageGoto

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 below steps:

- 1. Navigate on the web GUI under "Advanced Call Features > Announcement"
- 2. Click on

[Add](#)

to add a new Announcement.

- 3. Configure the required fields Name, Prompt, Default Destination to be used for the announcement.

Save and apply the configuration.

Announcement > Create New Announcement

\* Name

Test

\* Prompt

ringback.wav

Upload Audio File

\* Default Destination

Extension

1001

Announcement settings

The table below gives more description of the configuration parameters when creating 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 SoftwareUCM. With SCA, users can assign multiple devices to one extension, configure endpoints to monitor that extension, make actions on behalf of that extension such as viewing call status and placing and receiving calls, and even barging into existing calls. To configure the SCA functionality, please follow the steps below:

1. Users can enable SCA by navigating to the Extensions page, editing the desired extension, and enabling the option SCA under the "Feature" tab, and in "Other Settings" category.

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

Other Settings

Ring Timeout (s)

\* Skip Trunk Auth

No

Support Hot-desking Mode

Use MOH as IVR ringback tone.

Call Waiting

Email Missed Call Log

Emergency CID

Auto Record

OFF

Dial Trunk Password

Enable LDAP

\* Music On Hold

Default

Stop Ringing

Enable SCA

\* Language

Default

Enabling 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
Unregistered	1000	shared	--	no	<div>+ </div>

SCA Number Configuration

3. Configure the private number as desired.

Add Private Number

\* Private Number

Related Shared Line

1000

Enable This Number

☒

Allow Origination from This Number

☒

Allow Termination to This Number

☒

Cancel

Save

SCA Private Number Configuration

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

SCA > Edit SCA Number Group:

\* Shared Line Number

1000

Allow Call Retrieve from Another Location

☒

Alert All Appearances for Group Paging Calls

☐

Multiple Call Arrangement

☐

Allow Bridging between Locations

☐

Bridge Warning Tone

Barge-In only

SCA Options

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

The following table describe the SCA Number configuration setting:

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.
--------------------	---

<b>Allow Call Retrieve from Another Location</b>	Allows remote call retrieval. Must be enabled in public hold. By default, it is enabled.
<b>Alert All Appearances for Group Paging Calls</b>	Allows all SCA group members to ring when the SCA shared number is paged. If disabled, only the SCA shared number will ring when paged. By default, it is disabled.
<b>Multiple Call Arrangement</b>	Allows simultaneous calls in an SCA group. By default, it is disabled.
<b>Allow Bridging between Locations</b>	Allows location bridging for SCA group. Must be enabled when using the Barge-In feature. By default, it is disabled.
<b>Bridge Warning Tone</b>	<p>Configures the notification in the bridge when another party join.</p> <ul style="list-style-type: none"><li>◦ <b>None:</b> No notification sound.</li><li>◦ <b>Barge-In only:</b> Notification sound will play when another party join.</li><li>◦ <b>Barge-In and Repeat:</b> Notification sound will play when another party joins and repeat every 30 seconds.</li></ul> <p>By default, it is set to “Barge-In Only”.</p>

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 SoftwareUCM 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 be sent to the configured email address(es).

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

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

1. Navigate on the web GUI under “**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.

Emergency Calls > Create New Emergency Call

\* Name

911

\* Emergency Number

911

Emergency Level

1 - Not Urgent

Disable Hunt on Busy

☐

Custom Prompt

None

Upload Audio File

\* Use Trunks

Members Notified

☐ 11 Available

Search

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ 1005

<

>

☐ 0 Selected

Search

None

Strip

Prepend

### Emergency Number Configuration

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

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


<b>Auto Record</b>	When enabled, emergency call will be automatically recorded.
<b>Send Recording File</b>	When enabled recording files will be sent to the configured email address.
<b>Email Address</b>	The email address to where the recording files will be sent.

Emergency Calls				
<a href="#">Emergency Calls</a> <a href="#">Emergency Recordings</a> <a href="#">Emergency Location Mapping</a>				
<a href="#">Add</a>				
Name ↕	Emergency Number ↕	Emergency Level ↕	Disable Hunt on Busy ↕	Options
911	911	1	No	<a href="#">✎</a> <a href="#">✖</a>

911 Emergency Sample

Emergency Recordings

The SoftwareUCM allows recording emergency calls and they can be found under WebUI → **Call Feature** → **Emergency Calls** → **Emergency Recordings**

Emergency Calls					
<a href="#">Emergency Calls</a> <a href="#">Emergency Recordings</a> <a href="#">Emergency Location Mapping</a>					
Recording files are currently stored in <a href="#">GDMS</a> . 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.					
<a href="#">Download</a> <a href="#">Download All</a> <a href="#">Delete</a> <a href="#">Clear</a> <span>Local</span> <span>2025-01</span> <a href="#">📅</a>					
<input type="checkbox"/>	Name ↕	Emergency Calls ↕	Caller Number ↕	Date ↕	Size ↕
Options					
					

Emergency Recordings

Emergency Location Mapping

In compliance with Kari’s Law and Ray Baum’s Act, UCM’s Emergency Calls feature supports emergency location mapping. This will allow users to associate subnets with emergency location identification numbers (ELINs), which can then be used by E911 service providers for example to determine the exact location of callers. The new options can be found under **Advanced Call Features**→**Emergency Calls**→**Emergency Location Mapping**.

Emergency Calls > Create New Emergency Location Mapping

\* ELIN

\* Subnet

\* Location

Geolocation Routing

No

CancelSave

Emergency Location Mapping

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

Important Note

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

## 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 > Create New Restrict Calls

\* Name

Tech\_Support

Restrict Calls between Extension

☒

\* Members

☐ 11

Available

Search

Q

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ 1005

☐ 0

Selected

Search

Q

None

☐ 11

Available

Search

Q

☐ 1000

☐ 1001

☐ 1002

☐ 1003

☐ 1004

☐ 0

Selected

Search

Q


None

Allowed List


Restrict Calls

## Configure Restrict Calls

- Click on “Add” to add a rule for restrict calls.
- Click on

 to edit the rule of restrict calls.

- Click on

 to delete the rule of restrict calls.

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

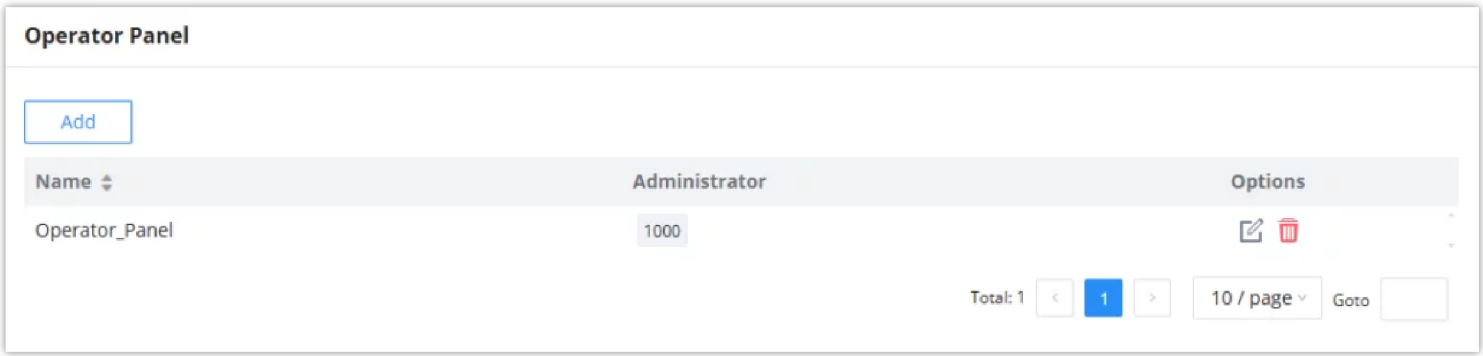
## Operator Panel

## Configure Operator Panel



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

The SoftwareUCM 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.

<b>Name</b>	The Operator panel name.
<b>Administrator</b>	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.
<b>Management Module</b>	
<b>Extension</b>	The selected extensions will be supervised by the administrator, and you can choose extensions, extension groups, and departments. For the selected extension groups and departments, subsequent extensions will be automatically supervised by the administrator.
<b>Ring Groups</b>	The checked Ring Groups will be supervised by the administrator. Select “All”, all Ring Groups and subsequent updates will be automatically supervised by the administrator.
<b>Voicemail Groups</b>	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.
<b>Call Queue</b>	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.
<b>Parking Lot</b>	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

## 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	<div>1. Configures whether Wave users can see the read status of sent messages when using local IM.</div> <div>2. If using Cloud IM, read receipts must be configured on the IM server (GDMS or custom IM server) being used. To configure this on GDMS, navigate to the top right corner of the GDMS page <b>Plan &amp; Services-&gt;My Plans-&gt;Edit Cloud IM</b> page.</div>
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)	<div>1. Configures whether Wave users can see the maximum chat file size when using local IM.</div> <div>2. If using Cloud IM, maximum chat file size must be configured on the IM server (GDMS or custom IM server) being used.</div> <div>To configure this on GDMS, navigate to the top right corner of the GDMS page <b>Plan &amp; Services-&gt;My Plans-&gt;Edit Cloud IM</b> page</div>

Cloud IM Service

IM Settings

IM SettingsCloud IM Service

Enable Cloud IM

☒

Local Proxy

☐

\* Cloud IM Server Address

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

\* Service ID

\* Key

\* Site Name

Trusted User

Prefix

Sync Local Chat Data

☐

To sync this SoftUCM's local chat data to the cloud server, please check "Sync Local Chat Data". Otherwise, when the Cloud IM service is enabled, previous local chat data will not be available.

Cancel

Save

Cloud IM Service

Enable CloudIM	If the user already purchased the SoftwareUCM CloudIM plan, the user can configure this option. If not, the setting will not be applied. The user can only use the IM service in the PBX locally.
Local Proxy	If a SoftwareUCM is used as the IM Server, it is recommended to check this option to ensure normal Wave operation.
CloudIM Server Address	<div><div>The user can configure the CloudIM server domain or IP address. The user can view the CloudIM plan information in the GDMS platform or on a SoftwareUCM which has had “IM Server” mode enabled.</div><div><div><div>My Plans &gt; Plan Details</div><div><div>Service Domain: 192.168.126.101Service ID: 45924e547962456ea0e06b9debb89e49</div><div>Service Key: d0ab3bc58c1c46a38e0ec40d7b3587a4Plan Storage: Chat file and picture (0B Used — 0%)</div></div><div><div>Order ID</div><div>Plan</div><div>Price(USD)</div><div>Type</div><div>Subscription Time ↕</div><div>Expiration Time ↕</div><div>Status</div><div>Options ⚙</div></div></div></div></div>
Service ID	The user needs to configure the service ID for the CloudIM plan PBX IM server.
Key	The user needs to configure the service Key for the CloudIM plan or PBX IM server.
Site Name	Enter the site name of this specific PBX.

Trusted User	If the PBX is used as the IM Server, and the IM server address is configured with an IP address, please enter it here.
Prefix	Enter the call prefix. <b>Note:</b> Call prefix should have a length of minimum 1 digit and maximum 20 digits.
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.

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.

<b>Visitor Information</b>	
<b>Require Visitor Info</b>	Configure the visitor information required to start a live chat session.
<b>Privacy Control</b>	If enabled, visitors must consent to allow the processing of personal data and cookies before entering Live Chat.
<b>Call Settings</b>	
<b>Allow Visitor To Call</b>	If enabled, visitors will have the option to call the configured destination from this Live Chat.
<b>Customer Service Agent Information</b>	
<b>Avatar</b>	Upload the avatar of the agent. Please select a png, jpg, or jpeg format file.
<b>Name</b>	Enter the name of the agent.
<b>Show Agent's Real Name</b>	Enable this option to show the agent's real name in the live chat.
<b>Chat Settings</b>	
<b>Welcome Message</b>	Configure the initial message to display to visitors when they first enter the live chat session.
<b>Reply to First Message</b>	Configure the message to send to visitors in response to their first message.
<b>Visitor Chat Log Retention Time (days)</b>	This value determines how long a visitor's chat history will be kept before it's deleted automatically. <b>Note:</b>
<b>Live Chat Link Address</b>	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

Enterprise Administrator

\* Message Content

\* Recipients

Search

Company Contact

☐ All

☐ Technical Support

☐ Quality Control

☐ Sales

☐ IT

☐ Marketing

☐ Human Resources

☐ Finance

☐ 1000 " "

Selected(0)

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 SoftwareUCM 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

+1

Test

SMS Settings

Enable SMS	Tick this box to enable SMS service.
SMS Carrier	Choose the SMS carrier: <ul style="list-style-type: none"><li>Amazon</li><li>Twilio</li></ul>
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 Settings

SMS Settings

SMS Template

SMS Delivery Log

①

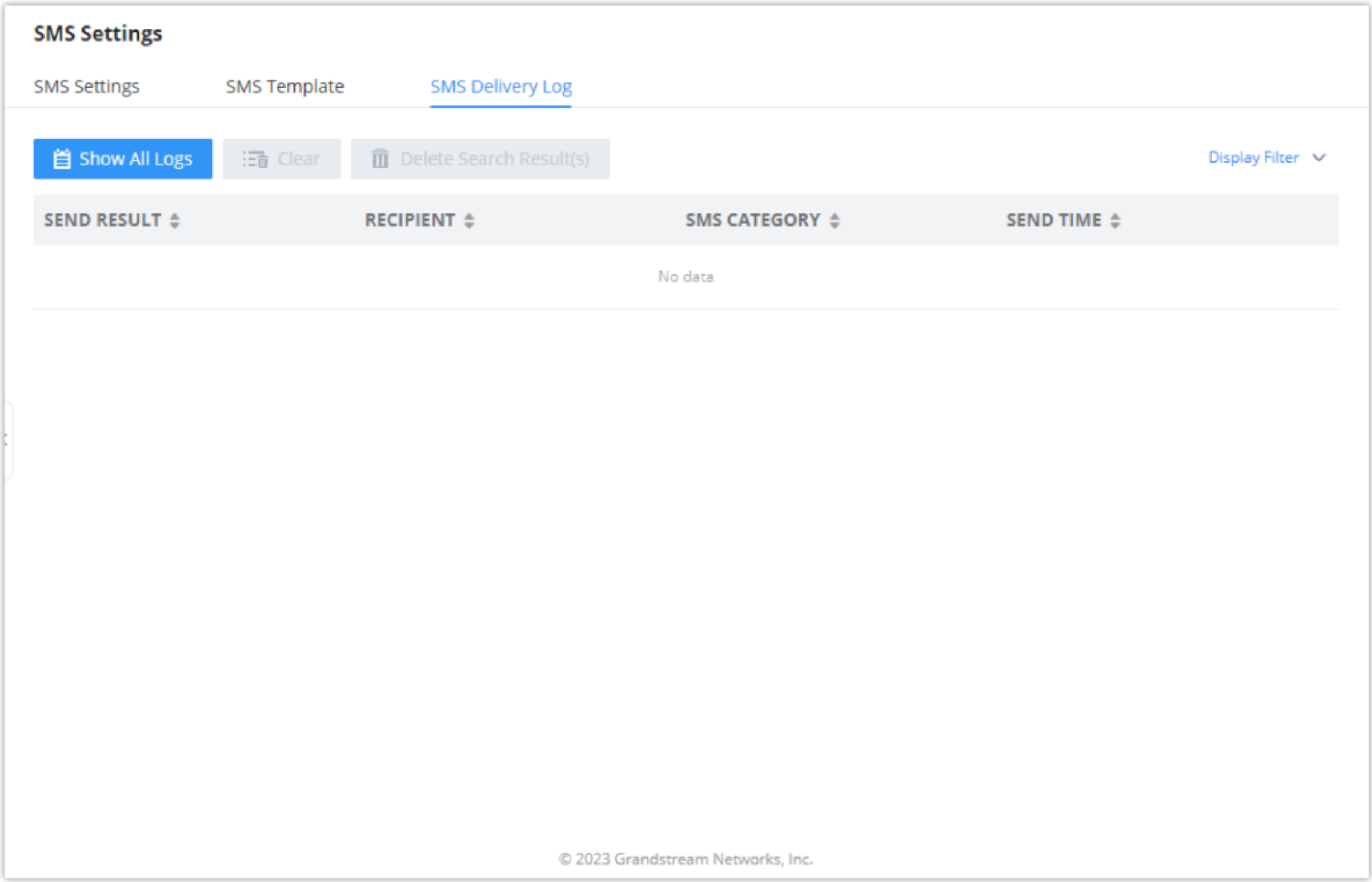
SMS templates are subject to carrier specifications, and carriers may require senders to pre-register templates for each type of message they plan to send. Please follow the default templates to apply for the corresponding templates on the SMS Cloud Platform, subject to the operator's requirements. More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

Type	Template Content	Options
Verification Code	[SoftUCM] Your verification code is <span style="color: #FF9900;">\${code}</span> . It will expire in 10 minutes.	
Alarm Notification	[SoftUCM] <span style="color: #FF9900;">\${hostName}</span> ( <span style="color: #FF9900;">\${macAddr}</span> ) system event: <span style="color: #FF9900;">\${content}</span>	

SMS Templates

## SMS Delivery Log

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



SMS Delivery Log

## PBX SETTINGS

### General Settings

General Preferences	
Global Outbound CID	Configure the global CallerID used for all outbound calls when no other CallerID is defined with higher priority. If no CallerID is defined for extension or trunk, the global outbound CID will be used as CallerID.
Global Outbound CID Name	Configure the global CallerID Name used for all outbound calls. If configured, all outbound calls will have the CallerID Name set to this name. If not, the extension's CallerID Name will be used.
Ring Timeout	Configure the number of seconds to ring an extension before the call goes to the user's voicemail box. The default setting is <b>60</b> . <b>Note:</b> This is the global value used for each extension if "Ring Timeout" field is left empty on the extension configuration page.
Call Duration Limit	Block calls for the configured duration. If Extensions->Features->Call Duration Limit and Outbound Routes->Call Duration Limit are not configured, General Settings->Call Duration Limit will be used.
Record Prompt	If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the 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.

<b>Merge Same Call Recordings</b>	If enabled, the system will merge all recordings created during a call regardless of how many times a user starts and stops recording during a call.
<b>Stereo Recording</b>	If enabled, the caller and callee’s audio will be split into two channels during call recording. Not applicable to calls with more than 2 parties.
<b>Calling Channel</b>	Configure the audio channels for the calling party and the called party. If the caller is selected as the right channel, the callee will be used for the left channel, and vice-versa. <b>Note:</b> This option will be available when “Stereo Recording” is enabled.
<b>International Call Prefix</b>	When this configuration is empty, International Call Prefix can be empty or +.
<b>Extension Preferences</b>	
<b>Enforce Strong Password</b>	If enabled, a strong password policy will be enforced. This does not affect user login passwords, which must be strong.
<b>Enable Random Password</b>	If enabled, the extension will created with a randomly generated password.
<b>Send Extension Update Emails</b>	If enabled, an email will be sent to an extension’s configured email address after creating it or modifying that extension’s settings.
<b>Disable Extension Range</b>	If set to “Yes”, users could disable the extension range pre-configured/configured on the IPPBX. The default setting is “No”.Note: It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.
<b>Extension Ranges</b>	<p>The default extension range assignment is:</p> <ul style="list-style-type: none"><li>● <b>User Extensions:</b> 1000-6299 User Extensions is referring to the extensions created under Web GUI→Extension/Trunk→Extensions page.</li><li>● <b>Meeting Extensions:</b> 6300-6399 This extension range is used for creating meeting rooms.</li><li>● <b>Ring Group Extensions:</b> 6400-6499 This extension range is used for ring groups</li><li>● <b>Queue Extensions:</b> 6500-6599 This range of extensions is used for queueing</li><li>● <b>Voicemail Group Extensions:</b> 6600-6699 This extension range is used for voicemail groups.</li><li>● <b>IVR Extensions:</b> 7000-7100 This extension range is used for</li><li>● <b>Dial By Name Extensions:</b> 7101-7199 This extension range is used for Dial by Name feature</li><li>● <b>FAX Extension:</b> 7200-8200 This extension range is used for T.38 Fax.</li></ul>
<div>Default Extension Segment</div>	Clicking this button will reset the extension range to their default values.

SIP Settings

General

<b>Realm For Digest Authentication</b>	Configure this as the host name or domain name of the PBX. Realms MUST be globally unique according to RFC3261.
<b>MWI From Header</b>	If disabled, the server will not transfer the Diversion Header
<b>Enable Diversion Header</b>	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”.

<b>Send Deflection Diversion</b>	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.
<b>Block Collect Calls</b>	If enabled, collect calls will be blocked. <b>Note:</b> Collect calls are indicated by the header "P-Asserted-Service-Info: service-code=Backward Collect Call, P-Asserted-Service-Info: service-code=Collect Call".
<b>Unavailable Extension Cause</b>	Sets the cause code to respond with when calling an unavailable extension.

### Session Timer

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

### TCP/TLS

Choose the supported transport protocol used for SIP packets.

<b>Enable TCP</b>	Configure to allow incoming TCP connections with the SoftwareUCM. The default setting is “No”.
<b>TCP Bind IPv4 Address</b>	Configure the IP address for the TCP server to bind to. “0.0.0.0” means binding to all interfaces. The port number is optional, and the default port number is 5060. For example, 192.168.1.1:5062.
<b>Enable TLS</b>	Configure to allow incoming TLS connections with the SoftwareUCM. The default setting is “Yes”.
<b>TLS Bind IPv4 Address</b>	Configure the IPv4 address for TLS server to bind to. “0.0.0.0” means binding to all interfaces. The port number is optional, and the default port number is 5061. For example, 192.168.1.1:5063. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket will not bind to multiple IP addresses.
<b>Server Certificate Verification</b>	Toggles whether the SoftwareUCM validates server certificates when acting as a client. <b>Note:</b> This option is disabled by default.
<b>TLS CA Cert</b>	Upload certification authority certificate. Note: CA certificate file size must be under 2MB.
<b>Private Certificate and Key</b>	
<b>TLS Cert</b>	This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as “TLS.pem” automatically. <b>Note:</b> The size of the uploaded certificate file must be under 2MB.
<b>TLS Key</b>	This file must be named with the CA subject name hash value. It contains CA’s (Certificate Authority) public key, which is used to verify the accessed servers. <b>Note:</b> The size of the uploaded CA certificate file must be under 2MB.
<b>Cipher Suite</b>	

<b>Restrict Cipher List</b>	By default, all SIP TLS encryption suites are in effect on the system, and when turned on, you can configure the encryption suites allowed to be used.
<b>Cipher Suite</b>	Select the encryption suites that are allowed to be used for SIP TLS connections, in the order of priority as configured.

NAT

<b>External Host</b>	Configure a static IP address and port (optional) used in outbound SIP messages if the UCM630X is behind NAT. If it is a host name, it will only be looked up once.
<b>Use IP address in SDP</b>	If enabled, the SDP connection will use the IP address resolved from the external host.
<b>External UDP Port</b>	Configure externally mapped UDP port when the PBX is behind a static NAT or PAT.
<b>External TCP Port</b>	Configure the externally mapped TCP port when the UCM630X is behind a static NAT or PAT.
<b>External TLS Port</b>	Configures the externally mapped TLS port when UCM630X is behind a static NAT or PAT.
<b>Local Network Address</b>	<p>Specify a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly.</p> <p>A sample configuration could be as follows:</p> <p>192.168.0.0/16</p>

ToS

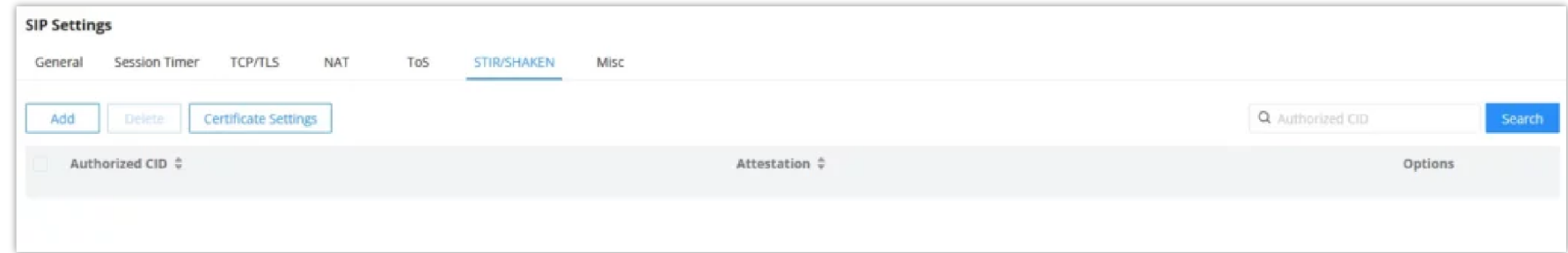
<b>ToS for SIP</b>	Configure Type of Service for SIP packets.
<b>ToS for RTP Audio</b>	Configure Type of Service for RTP audio packets.
<b>ToS for RTP Video</b>	Configure Type of Service for RTP video packets.
<b>Default Incoming/Outgoing Registration Time</b>	Configure the default duration (in seconds) of incoming and outgoing registration.
<b>Max Registration/Subscription Time</b>	Configure the maximum duration (in seconds) of incoming registrations and subscriptions allowed on the PBX. The default setting is 28800 seconds (8 hours).
<b>Min Registration/Subscription Time</b>	Configure the minimum duration (in seconds) of incoming registration and subscription allowed on the PBX. The default setting is 90 seconds.

DTMF Mode	<p>Configures the mode for sending DTMF.</p> <p>RFC4733 (default): DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream. Backward-compatible with RFC2833.</p> <ul style="list-style-type: none"><li>• <b>Inband:</b> DTMF is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs.</li><li>• <b>Info:</b> DTMF is transmitted separately from the media streams.</li><li>• <b>RFC4733_info:</b> DTMF is transmitted through both RFC4733 and SIP INFO.</li><li>• <b>Auto:</b> DTMF mode will be negotiated with the remote peer, only supports RFC4733 and inband. RFC4733 will be used by default unless the remote peer does not indicate support.</li></ul>
RTP Timeout	Configure the timeout in seconds. When the call is in talking status, if there is no RTP activity after the timeout, the call will be terminated. If configured as 0 or left blank, there will be no timeout.
RTP Hold Timeout	Configures the timeout in seconds. When a call is on hold, if there is no RTP activity within the timeout period, the call will be terminated. This value must be larger than “RTP Timeout”. If configured as 0 or left blank, there will be no timeout.
RTP Keep-alive (s)	The interval (in seconds) that a RTP Keepalive packet will be sent on an SDP connection. Default 0 (no RTP Keepalive).
100rel	Configure the 100relNo: Unsupported. Yes: Supported. Required: Forced to support.
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted or not.
Send Remote Party ID	Configure to enable or disable sending Remote-Party-ID.
Generate In-band Ringing	Configure whether or not to generate in-band ringing. <ul style="list-style-type: none"><li>• <b>Yes:</b> PBX will send 183 to ring back the caller after receiving the called party’s 180.</li><li>• <b>No:</b> PBX will directly forward the called 180 response to the caller.</li></ul>
Server User Agent	Configure the user agent field.
Send Compact SIP Headers	Configure to enable or disable sending compact SIP headers. This change requires a system reboot to take effect.
Passthrough PAI Header	Configures whether to preserve PAI headers from calling parties.

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:



STIR/SHAKEN

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

Certificate Settings

\* Certificate Download Timeout (s)

5

\* Signature Valid Time (s)

15

\* Public Key (Cert)

public.crt

\* Private Key

private.key

Cancel

Save

STIR/SHAKEN – Certificate Settings

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

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 SoftwareUCM ceases to attempt the registration. The default setting is 0, which means the SoftwareUCM 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	



<b>Reject Non-Matching INVITE</b>	If enabled, when rejecting an incoming INVITE or REGISTER request, the SoftwareUCM will always reject with “401 Unauthorized” instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. Default setting is “No”.
<b>SDP Attribute Passthrough</b>	
<b>Enable Attribute Passthrough</b>	If enable, and if the service does not know the attribute of FEC/FECC/BFCP, then the attribute will be passthrough.
<b>Early Media</b>	
<b>Enable Use Final SDP</b>	If enabled, call negotiation will use final response SDP.
<b>Ignore 180 Response</b>	If enabled, ringing indication after 183 response will be ignored.
<b>Blind Transfer</b>	
<b>Allow callback when blind transfer fails</b>	If enabled, the SoftwareUCM will call back to the transferrer when blind transfer fails (reason of failure includes busy and no answer). <b>Note:</b> This feature takes effect only on internal calls.
<b>Blind transfer timeout</b>	Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s.
<b>Hold</b>	
<b>Forward HOLD Requests</b>	Configure the SoftwareUCM to forward HOLD requests instead of processing holds internally. This serves to meet the standards set by some providers that require HOLD requests to be passed along from endpoint to endpoint. This option is disabled by default. <b>Note:</b> Enabling this option may cause hold retrieval issues and MOH to not be heard.

RTP Settings

RTP Settings

<b>RTP Start</b>	Configure the RTP port starting number. The default setting is 10000.
<b>RTP End</b>	Configure the RTP port ending address. The default setting is 20000.
<b>Strict RTP</b>	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is “Disable”.
<b>RTP Checksums</b>	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is “Disable”.
<b>ICE Support</b>	Configure whether to support ICE. The default setting is enabled. ICE is the integrated use of STUN and TURN structure to provide reliable VoIP or video calls and media transmission, via a SIP request/ response model or multiple candidate endpoints exchanging IP addresses and ports, such as private addresses and TURN server address.
<b>STUN Server</b>	Configure STUN server address. STUN protocol is a Client/Server and also a Request/Response protocol. It is used to check the connectivity between the two terminals, such as maintaining a NAT binding entries keep-alive agreement. The default STUN Server is stun.ipvideotalk.com. Valid format:

	[(hostname   IP-address) [':' port] The default port number is 3478 if not specified.
BFCP UDP Start	Configure BFCP UDP port starting number. The default setting is 50000.
BFCP UDP End	Configure BFCP UDP port ending number. The default setting is 52999.
BFCP TCP Start	Configure BFCP TCP port starting number. The default setting is 53000.
BFCP TCP End	Configure BFCP TCP port ending number. The default setting is 55999.
TURN Server	Configure TURN server address. TURN is an enhanced version of the STUN protocol and is dedicated to the processing of symmetric NAT problems.
TURN Server Name	Configure turn server account name
TURN Server Password	Configure turn server account password.
Connection Protocol	Protocol used to connect to the TURN server.
Number of ICE Candidates	This configures the number of pre-collected ICE candidates to gather and send to remote peers. The higher the number, the greater the network traffic consumption.

## Payload Type Settings

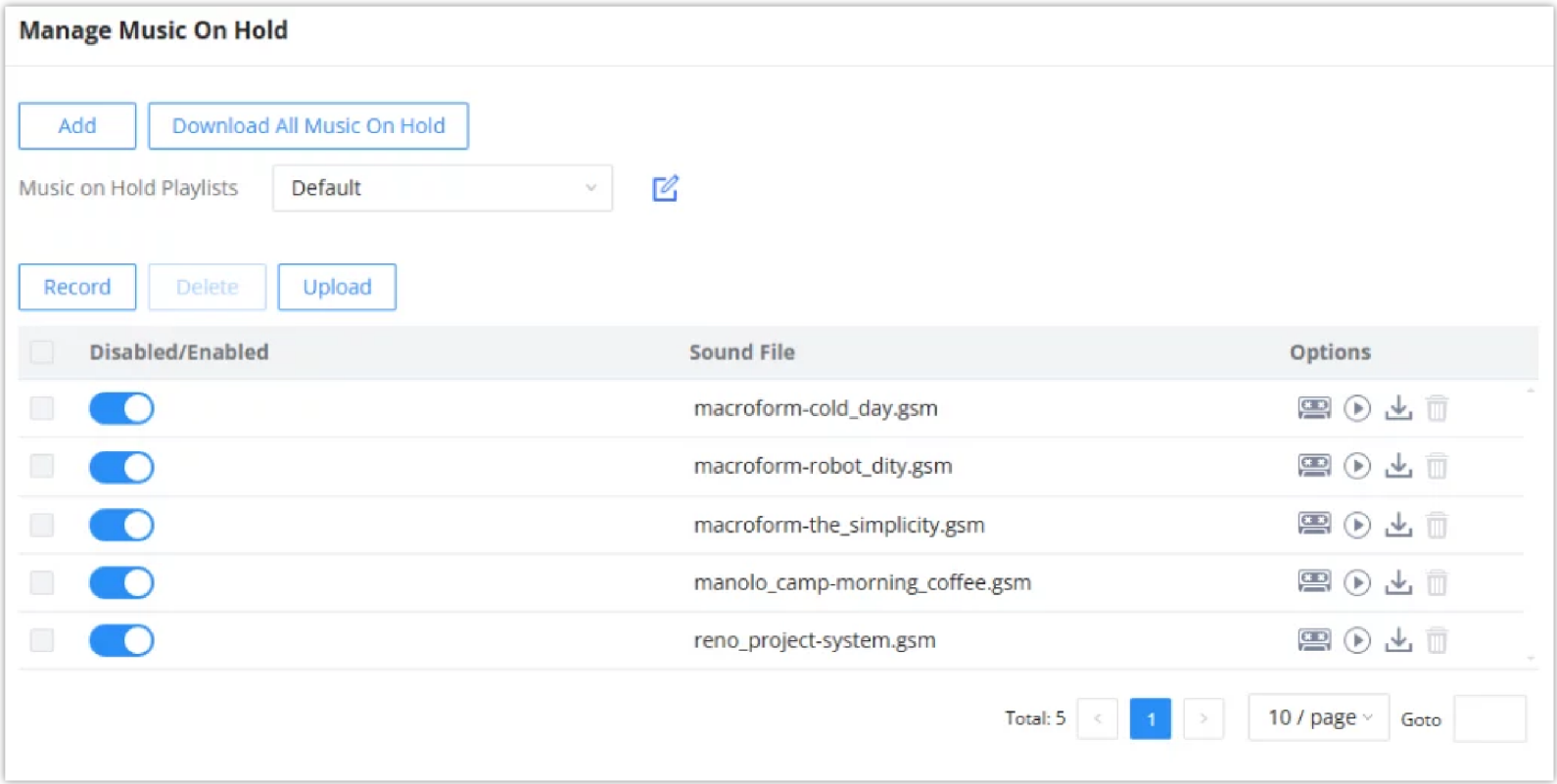
The SoftwareUCM payload type for audio codecs and video codes can be configured here.

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.

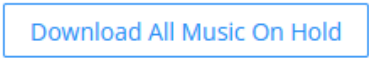
- Click on  next to the selected Music On Hold class to delete this Music On Hold class.

- 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 SoftwareUCM allows Users to select the Music On Hold file from WebGUI to play it. The SoftwareUCM 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

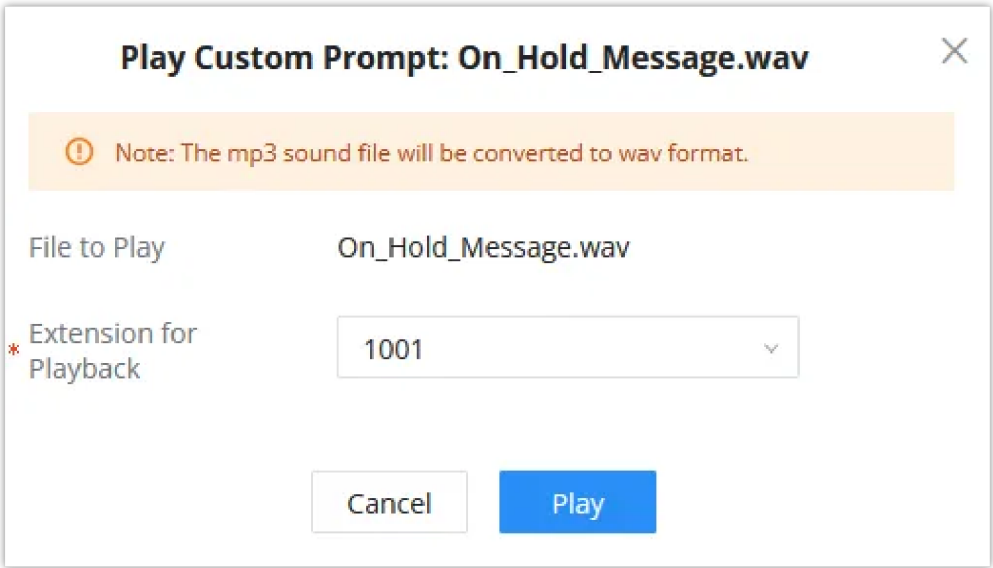


button for the Music On Hold file.

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



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



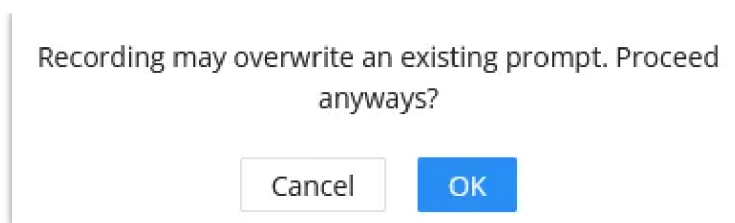
Play Custom Prompt

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

1. Click on

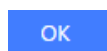


2. A message of confirmation will pop up, as shown below.

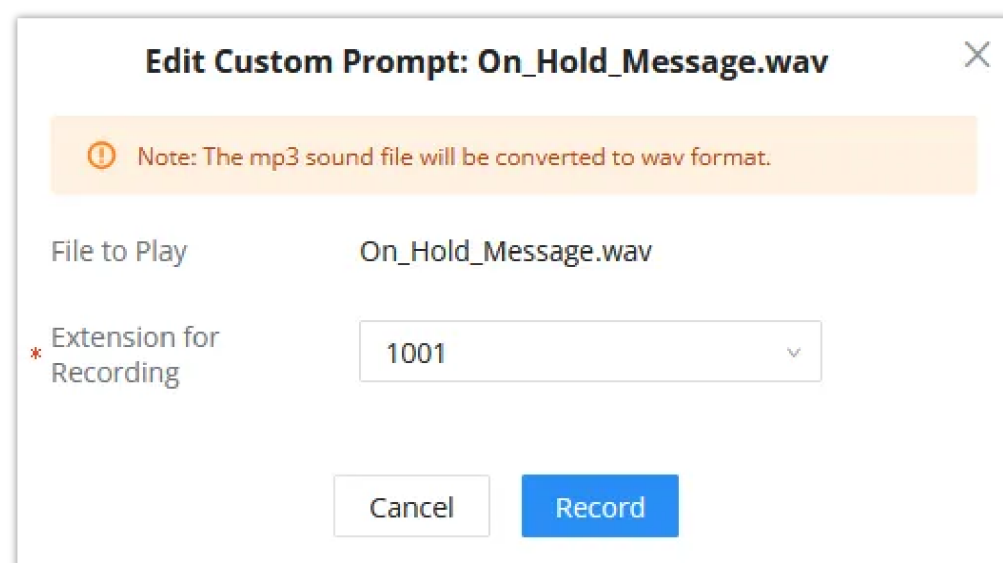


*Information Prompt*

3. Click



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



*Record Custom Prompt*

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

6. 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: <https://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 SoftwareUCM 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 SoftwareUCM already. The other languages provided by Grandstream can be downloaded and installed from the SoftwareUCM Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the SoftwareUCM.

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 SoftwareUCM Web GUI, click on "Add Voice Prompt Package" button.

Voice Prompt

Language Settings

Custom Prompt

Username Prompt

Add Voice Prompt Package

Upload

Voice Prompt Package List

LANGUAGE	OPTIONS
<input checked="" type="radio"/> English : en	
<input type="radio"/> 中文 : zh	

Cancel

Save

Language Settings for Voice Prompt

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

Details

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

Voice Prompt Package List

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





## 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 30MB.
  - 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.

Call Prompt Tones

SIP Trunk Prompt Tone

General Call Prompt Tones

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

Reset All

Default All

400	<div>sip-trunk-out-busy</div>	401	<div>sip-trunk-out-busy</div>
402	<div>sip-trunk-out-busy</div>	403	<div>sip-trunk-out-rejected</div>
404	<div>sip-trunk-out-wrong-nu...</div>	405	<div>sip-trunk-out-busy</div>
406	<div>sip-trunk-out-busy</div>	407	<div>sip-trunk-out-busy</div>
408	<div>sip-trunk-out-busy</div>	410	<div>sip-trunk-out-busy</div>
413	<div>sip-trunk-out-busy</div>	414	<div>sip-trunk-out-busy</div>
415	<div>sip-trunk-out-busy</div>	416	<div>sip-trunk-out-busy</div>
420	<div>sip-trunk-out-busy</div>	421	<div>sip-trunk-out-busy</div>
423	<div>sip-trunk-out-busy</div>	480	<div>sip-trunk-out-busy</div>
481	<div>sip-trunk-out-busy</div>	482	<div>sip-trunk-out-busy</div>
483	<div>sip-trunk-out-busy</div>	484	<div>sip-trunk-out-busy</div>
485	<div>sip-trunk-out-busy</div>	486	<div>sip-trunk-out-busy</div>
487	<div>sip-trunk-out-busy</div>	488	<div>sip-trunk-out-busy</div>

Cancel

Save

SIP Trunk Prompt Tone

General Call Prompt Tones

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

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

Call Prompt Tones

SIP Trunk Prompt Tone

General Call Prompt Tones

Specify the tones to play for various general call scenarios.

Reset All

Default All

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

Cancel

Save

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

<input type="checkbox"/>	Name	Type	Format	Options
<input type="checkbox"/>	Ring-IVR.wav	Audio	wav	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Ring-Queue.wav	Audio	wav	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Ring-Extension.wav	Audio	wav	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Ring-External.wav	Audio	wav	<div><div></div><div></div><div></div></div>

Total: 4

<

1

>

10 / page

Goto

Alert-info Prompt

## File Manager

UCM supports automatic or manual recording of calls and storage of IM chat files. Only recording files and IM files can be stored locally or on the GDMS.

File Manager

After configuring the storage path, please navigate to the Maintenance->System Events->Alert Events List page to enable the External Disk Usage alert notifications to ensure that storage space is sufficient.

Recording Files

Enable Auto Change

☒

Storage Path Priority

GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > Local (In Use) Custom

Video Recording Files

Enable Auto Change

☒

Video recordings can only be stored in NAS.

Storage Path Priority

NAS (Unavailable) Custom

IM Files

Enable Auto Change

☒

Storage Path Priority

GDMS Cloud Storage (Unavailable) > NAS (Unavailable) > Local (In Use) Custom

Save

File Manager

- If “**Enable Auto Change**” is selected, the files will be automatically saved in the available storage location.
- If “**Local**” is selected, the files will be stored in the storage space allocated to the SoftwareUCM.
- If “**GDMS Cloud Storage**” is selected, data will no longer be stored locally and if you need to listen to the recording, download the file to the computer side and play it offline.

### Note

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

On the SoftwareUCM, users have the following options when select the categories to copy the files to the external device:

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

Storage Device Manager

In Storage Device Manager, the user can configure the SoftwareUCM as a client of NAS (Network Attached Storage) and SFTP (Secure File Transfert Protocol) servers.

While SFTP is used to back up the PBX data and configuration, either manually or automatically. The user can also use the SFTP integration to synchronize CDR data, recording files, voicemail, and fax in real-time to the SFTP server.

NAS

NAS is used to store call recording files, video recording files, and the files exchanged in Wave.

Storage Device Management

NAS

SFTP

Please make sure that the NAS is connected and writeable if using it as storage for recordings.

NOTE: NAS will not be available if the local disk usage exceeds the set threshold.

Enable

☒

\* Host

\* Folder Path

Example: folder1/subfolder2

Username

Password

Security Mode

ntlmssp

Status

Unavailable

Cancel

Save

NAS Integration

Enable	Enabled / Disable the NAS recording functionality.
Host	Configure the Domain or IP address of the NAS server. <b>Note:</b> Currently, only IP addresses are supported in the Host/IP field.
Folder Path	Specify the name of the shared folder. <b>Example:</b> folder1/subfolder2
Username	Specify the account username to access the NAS server.

Password	Configure the account password to access the NAS server. The password can include letters, number, and special characters.
Security Mode	Select a security mode based on the server settings to ensure proper connection establishment. The default value is ntlmssp. <ul style="list-style-type: none"><li>• None</li><li>• krb5</li><li>• krb5i</li><li>• ntlmv2</li><li>• ntlmv2i</li><li>• ntlmssp</li><li>• ntlmsspi</li></ul>
Status	If configured correctly, the Status field will show “Mounted”, and the newly added NAS server will be shown on the Mounted Netdisk List. Additionally, the NAS will appear as a selectable storage option in the <b>PBX Settings</b> → <b>Recording Storage</b> page and <b>CDR</b> → <b>Recording Files</b> page.

SFTP

While SFTP is used to back up the PBX data and configuration, either manually or automatically. The user can also use the SFTP integration to synchronize CDR data, recording files, voicemail, and fax in real-time to the SFTP server.

Storage Device Management

NAS

SFTP

Please enter the SFTP server information. The SFTP server can be used for regular backups, data sync, packet capture storage, PMS and other data syncing services.

Enable

☒

\* Account

Password

\* Server Address

Test Connection

Start

Cancel

Save

SFTP Integration

Enable	Tick this box to enable SFTP integration.
Account	Enter the account of the SFTP server.
Password	Enter the password of the account of the SFTP server.
Server Address	Enter the address of the SFTP server.

USB Disk File Management

USB Disk File Management allows the user to browse the files and directories created on a USB drive, the user can plug-in a USB flash drive, a USB solid state drive, a USB hard disk drive, or any storage drive with a USB interface. The user can download and the delete the files and the directories directly from the webUI of the SoftwareUCM.

Storage Device Management

NAS

SFTP

USB Disk File Management

EXT4 is the recommended file system for external storage devices.

USB 1 (EXT4)

Delete

<input type="checkbox"/>	Name	Type	Date	Size	Options
<input type="checkbox"/>	PBX_Paging_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Conferences_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_IM_ShareFiles_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Queue_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_SCA_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Conferences_Videoing_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Paging_Videoing_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Emergency_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>
<input type="checkbox"/>	PBX_Recordings_C210010002AA	Directory	2025-03-13 14:02:13 UTC+01:00	0	<div><div></div><div></div></div>

Total: 9

<1>

10 / page

Goto

USB Disk File Management

Note

For optimal reading/writing time, the user may use EXT4 file system.

# SYSTEM SETTINGS

This section will explain the available system-wide parameters and configuration options on the SoftwareUCM. 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:

Enable CPU Flow Control:

☒

CPU Flow Control

90%

Threshold:

Data Partition Write

90%

Threshold:


SoftwareUCM General Settings

Device Name	Name of the UCM
Enable CPU Usage Call Control	Enable CPU usage call control.

<b>CPU Usage Call Control Threshold</b>	Configures the CPU usage threshold. Upon exceeding this threshold, new calls can no longer be made or received. The default value is 90%.
<b>Data Partition Usage Threshold</b>	Configures the data partition usage threshold. Upon exceeding this threshold, the UCM will no longer be able to write data to the data partition. The default value 90%.

HTTP Server

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

 For a stable and secure automatic NAT penetration solution, please check out Grandstream's [RemoteConnect](#) service and contact your equipment agent about available plans.

HTTP Server

SoftUCM Web Settings

Redirect from Port 80

Enable

External Host

\* Port

8089

Enable IP Address Allowlist

☐

Permitted IP (s)

IP Address

/

Subnet Mask

Add IP Address

Wave Settings

Cross-origin Address Allowlist

https://wave.gdms.cloud

External Host

\* Port

8090

Certificate Settings

Default Certificate Auto Renewal

☒

Options

Upload Certificate

HTTP Server Settings

<b>Redirect From Port 80</b>	Toggles automatic redirection to UCM’s web portal from port 80. If disabled, users will need to manually add the UCM’s configured HTTPS port to the server address when accessing the UCM web portal via browser. Default is “Enabled”.
<b>External Host</b>	Configure a URL and port (optional) used to access the UCM web portal if the UCM is behind NAT.
<b>Port</b>	Specifies the port number used to access the UCM HTTP server. Default is “8089”.
<b>Enable IP Address Allowlist</b>	IP Allowlist restricts all IP addresses except for those in the allowlist from accessing the device via HTTP(S) (i.e., web portal, ZeroConfig, CTI apps).



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

Network Settings

In the network settings, the user can configure the settings related to the network card of the SoftwareUCM such as the MTU, IP address acquisition method, etc... the user can also configure network authentication, static routes, and ARP table settings.

Basic Settings

Basic settings allows the configuration of the essential network settings of the SoftwareUCM, like the MTU and IP address configuration.

Network Settings

Basic Settings

802.1X Settings

Static Routes

ⓘ

Modifying network settings will reboot the device so please be mindful. If the device's IP address was changed, please access the device using the new IP address after reboot.

MTU

1500

IPv4 Address

Network Port Traffic Control

Preferred DNS Server

LAN

IP Method

DHCP

Cancel

Save

Network Settings – Basic Settings

Please refer to the following table for basic network configuration parameters on SoftwareUCM.

MTU	<p>Specify the size of the MTU.</p> <p>The default value is 1492.</p> <p>The user can enter a value in the range 1280 – 1492 bytes.</p> <p>It is recommended that you keep the MTU in the default value.</p>
IPv4 Address	
Preferred DNS Server	Enter the IP address of the preferred DNS server
LAN	
IP Method	<p>Select the IP address acquisition method.</p> <ul style="list-style-type: none"><li>● <b>DHCP</b>: The IP address is assigned using a DHCP server</li><li>● <b>Static</b>: Enter the network configuration manually</li></ul>
IP Address	<p>This option appears when the IP method is set to Static.</p> <p>Enter the IP address.</p>
Subnet Mask	<p>This option appears when the IP method is set to Static.</p> <p>Enter the subnet mask.</p>
Gateway IP	<p>This option appears when the IP method is set to Static.</p> <p>Enter the IP address of the gateway.</p>
DNS Server 1	<p>This option appears when the IP method is set to Static.</p> <p>Enter the IP address of the DNS server.</p>
DNS Server 2	<p>This option appears when the IP method is set to Static.</p> <p>Enter the IP address of the DNS server.</p>

Network Port Traffic Control allows the user to enable measures which prevent the SoftwareUCM from being overloaded with a network storm. In this tab, the user can enable the Network Port Traffic Storm Alert, so when a network storms occurs, the SoftwareUCM will alert the user to take the necessary actions.

In Network Port Incoming Traffic Control, the user can enter the threshold for the bandwidth, if the bandwidth is exceeded, it will trigger an alert.

Network Settings

Basic Settings

802.1X Settings

Static Routes

ⓘ

Modifying network settings will reboot the device so please be mindful. If the device's IP address was changed, please access the device using the new IP address after reboot.

MTU

1500

IPv4 Address

Network Port Traffic Control

Enable Network Port Traffic Storm Alert

After checking the box, if you need email or HTTP notification, please go to [Maintenance - System Events](#)

LAN

Network Port Incoming Traffic Control

Please enter digits from 1 to 1024000

Kbps

Cancel

Save

Network Port Traffic Control

802.1X Settings

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to a device before the device can access the Internet or other LAN resources. The SoftwareUCM supports 802.1X as a supplicant/client to be authenticated.

Network Settings

Basic Settings

802.1X Settings

Static Routes

802.1X Mode

EAP-PEAPv0/MSCHAPv2

\* Identity

\* MD5 Password

802.1X CA Certificate

Choose File to Upload

Delete

802.1X Client Certificate

Choose File to Upload

Delete

Cancel

Save

802.1X Settings

The table below describes the settings related to 802.1X

802.1X Mode	Select 802.1X mode. The default setting is “Disable”. The supported 802.1X modes are: <ul style="list-style-type: none"><li>EAP-MD5</li><li>EAP-TLS</li><li>EAP-PEAPv0/MSCHAPv2</li></ul>
Identity	Enter 802.1X mode Identity information.
MD5 Password	Enter 802.1X mode MD5 password information.

<b>802.1X CA Certificate</b>	Select 802.1X certificate from local PC and then upload. <b>Note:</b> This option appears when selecting either EAP-TLS or EAP-PEAPv0/MSCHAPv2 security protocols.
<b>802.1X Client Certificate</b>	Select 802.1X client certificate from local PC and then upload. <b>Note:</b> This option appears when selecting either EAP-TLS or EAP-PEAPv0/MSCHAPv2 security protocols.

Static Routes

The SoftwareUCM provides the possibility to users to set static routing that allows the device to use manually configured routes, rather than information only from dynamic routing or gateway configured in the SoftwareUCM Web GUI→**System Settings**→**Network Settings**→**Basic Settings** to forward traffic. It can be used to define a route when no other routes are available or necessary or used in complementary with existing routing on the SoftwareUCM as a failover backup, etc.

- Click on “**Add IPv4 Static Route**” to create a new IPv4 static route. The configuration parameters are listed in the table below.
- Once added, users can select



to edit the static route.

- Select



to delete the static route.

OpenVPN®

OpenVPN® settings allow the users to configure SoftwareUCM to use VPN features, the following table gives details about the various options to configure the PBX as OpenVPN Client.

**OpenVPN®**

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

OpenVPN® Enable

☒

Configuration Method

Manual Configuration

\*

OpenVPN® Server Address

OpenVPN® Server Protocol

UDP

OpenVPN® Device Mode

Dev TUN

OpenVPN® Use Compression

☐

Allow Weak SSL Ciphers

☐

OpenVPN® Encryption Algorithm

BF-CBC(Blowfish)

User Authentication

☐

\*

OpenVPN® CA Cert

Choose File to Upload

Delete

**Private Certificate and Key**

\*

OpenVPN® Client Cert

Choose File to Upload

\*

OpenVPN® Client Private Key

Choose File to Upload

Certificate & Private Key

Delete

Cancel

Save

OpenVPN® Enable	Enable / Disable the OpenVPN® feature.
Configuration Method	Select the OpenVPN® configuration method. <b>Manual Configuration:</b> Allows to configure OpenVPN® settings manually. <b>Upload Configuration File:</b> Allows to upload .ovpn and .conf files to the UCM and to automatically configure OpenVPN® settings.
OpenVPN® Server Address	Configures the hostname/IP and port of the server. For example 192.168.1.2:22
OpenVPN® Server Protocol	Specify the protocol user, user should use the same settings as used on the server
OpenVPN® Device mode	Use the same setting as used on the server. <ul style="list-style-type: none"><li>• <b>Dev TUN:</b> Create a routed IP tunnel.</li><li>• <b>Dev TAP:</b> Create an Ethernet tunnel.</li></ul>
OpenVPN® Use Compression	Compress tunnel packets using the LZO algorithm on the VPN link. Do not enable this unless it is also enabled in the server config file.
Enable Weak SSL Ciphers	Either to enable the Weak SSL ciphers or not.

<b>OpenVPN® Encryption Algorithm</b>	Specify the cryptographic cipher. Users should make sure to use the same setting that they are using on the OpenVPN server.
<b>OpenVPN® CA Cert</b>	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
<b>OpenVPN® Client Cert</b>	Upload a client certificate. This file will be renamed as 'client.crt' automatically.
<b>OpenVPN® Client Key</b>	Upload a client private key. This file will be renamed as 'client.key' automatically.
<b>Username</b>	Username used to authenticate into the server.
<b>Password</b>	Password used to authenticate into the server.

## DDNS Settings

DDNS setting allows users to access SoftwareUCM via domain name instead of IP address.

The SoftwareUCM supports DDNS service from the following DDNS provider:

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

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

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

Hostname Information

Hostname:

haograndstream.ddns.net

Host Type:

☒ DNS Host (A)
☐ DNS Host (Round Robin)
☐ DNS Alias (CNAME)

☐ Port 80 Redirect
☐ Web Redirect

IP Address:

1.2.3.4

Last Update: 2015-01-07 17:29:20 PST

Assign to Group:

- No Group -

Configure Groups

Enable Wildcard:

Wildcards are a Plus / Enhanced feature. [Upgrade Now!](#)

Advanced Records:

TXT, SPF, and SRV records and the use of some special clients are Plus / Enhanced features. [Upgrade now](#) to use them.

*Register Domain Name on noip.com*

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

DDNS Settings

DDNS Server

no-ip.com

Enable DDNS

☒

\* Username

user\_no\_ip

\* Password

.....

\* Host Name

MyGSPBX.ddns.net

Cancel

Save

DDNS Settings

Security Settings

The SoftwareUCM provides users firewall security configurations to prevent certain malicious attacks to the SoftwareUCM system. Users could configure to allow, restrict, or reject specific traffic through the device for security and bandwidth purpose. The SoftwareUCM also provides the Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. To configure firewall settings in the SoftwareUCM, go to Web GUI→**System Settings**→**Security Settings** page.

Static Defense

Under Web GUI→**System Settings**→**Security Settings**→**Static Defense** page, users will see the following information:

- Current service information with port, process, and type.
- Typical firewall settings.
- Custom firewall settings.

The following table shows a sample current service status running on the SoftwareUCM.

Port	Process	Type	Protocol or Service
7777	Asterisk	TCP/IPv4	SIP
389	Slapd	TCP/IPv4	LDAP
6060	zero_config	UDP/IPv4	UCM zero_config service
5060	Asterisk	UDP/IPv4	SIP
4569	Asterisk	UDP/IPv4	IAX
38563	Asterisk	udp/ipv4	SIP
10000	gs_avs	udp/ipv4	gs_avs
10001	gs_avs	udp/ipv4	gs_avs
10002	gs_avs	udp/ipv4	gs_avs



10003	gs_avs	udp/ipv4	gs_avs
10004	gs_avs	udp/ipv4	gs_avs
10005	gs_avs	udp/ipv4	gs_avs
10006	gs_avs	udp/ipv4	gs_avs
10007	gs_avs	udp/ipv4	gs_avs
10010	gs_avs	udp/ipv4	gs_avs
10012	gs_avs	udp/ipv4	gs_avs
10013	gs_avs	udp/ipv4	gs_avs
10014	gs_avs	udp/ipv4	gs_avs
10015	gs_avs	udp/ipv4	gs_avs
10018	gs_avs	udp/ipv4	gs_avs
10019	gs_avs	udp/ipv4	gs_avs
10020	gs_avs	udp/ipv4	gs_avs
6066	Python	udp/ipv4	python
3306	Mysqld	tcp/ipv4	mysqld
45678	Python	udp/ipv4	python
8439	Lighttpd	tcp/ipv4	HTTP
8088	asterisk	tcp/ipv4	SIP
8888	Pbxmid	tcp/ipv4	pbxmid
25	Master	tcp/ipv4	master
636	Slapd	tcp/ipv4	SLDAP
4569	asterisk	udp/ipv6	SIP
42050	asterisk	udp/ipv6	SIP
7681	Pbxmid	tcp/ipv4	pbxmid

SoftwareUCM Firewall →Static Defense →Current Service

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

<b>Ping Defense Enable</b>	If enabled, ICMP response will not be allowed for Ping requests. The default setting is disabled. To enable or disable it, click on the check box for the LAN or (SoftwareUCM) interface.
----------------------------	---

<b>SYN-Flood Defense Enable</b>	<p>Allows the SoftwareUCM to handle excessive amounts of SYN packets from one source and keep the web portal accessible. There are two options available and only one of these options may be enabled at one time.</p> <ul style="list-style-type: none"><li>◦ eth(0)LAN defends against attacks directed to the LAN IP address of the SoftwareUCM.</li><li>◦ eth(1)WAN defends against attacks directed to the WAN IP address of the SoftwareUCM.</li></ul> <p>SYN Flood Defense will limit the amount of SYN packets accepted by the UCM from one source to 10 packets per second. Any excess packets from that source will be discarded.</p>
<b>Ping-of-Death Defense Enable</b>	<p>Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (SoftwareUCM) interface.</p>

Typical Firewall Settings

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

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

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

Security Settings > Create New Firewall Rule

\* Rule Name

Reject\_SSH\_WAN

\* Action

Reject

\* Type

IN

\* Interface

LAN

\* Service

SSH

Cancel

Save

Create New Firewall Rule

<b>Rule Name</b>	Specify the Firewall rule name to identify the firewall rule.
<b>Action</b>	<p>Select the action for the Firewall to perform.</p> <ul style="list-style-type: none"><li>◦ ACCEPT</li><li>◦ REJECT</li><li>◦ DROP</li></ul>

<b>Type</b>	<p>Select the traffic type.</p> <ul style="list-style-type: none"><li>◦ <b>IN</b></li></ul> <p>If selected, users will need to specify the network interface “LAN” or “WAN” (for SoftwareUCM) for the incoming traffic.</p> <ul style="list-style-type: none"><li>◦ <b>OUT</b></li></ul>
<b>Interface</b>	Select the interface to use the Firewall rule.
<b>Service</b>	<p>Select the service type.</p> <ul style="list-style-type: none"><li>◦ <b>FTP</b></li><li>◦ <b>SSH</b></li><li>◦ <b>Telnet</b></li><li>◦ <b>HTTP</b></li><li>◦ <b>LDAP</b></li><li>◦ <b>Custom</b></li></ul> <p>If “Custom” is selected, users will need to specify Source (IP and port), Destination (IP and port), and Protocol (TCP, UDP, or Both) for the service. Please note if the source or the destination field is left blank, it will be used as “Anywhere”.</p>
<b>Source IP Address and Port</b>	Configure a source subnet and port. If set to “Anywhere” or left empty, traffic from all addresses and ports will be accepted. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
<b>Destination IP Address and Port</b>	Configure a destination subnet and port. If set to “Anywhere” or left empty, traffic can be sent to all addresses and ports. A single port or a range of ports can be specified (e.g., 10000, 10000-20000).
<b>Protocol</b>	Select the protocol for the rule to be used.

Firewall Rule Settings

Save the change and click on the “Apply” button. Then submit the configuration by clicking on “Apply Changes” on the upper right of the web page. The new rule will be listed at the bottom of the page with sequence number, rule name, action, protocol, type, source, destination, and operation. More operations are below:

- Click on



to edit the rule.

- Click on



to delete the rule.

Dynamic Defense

Dynamic defense is supported on the SoftwareUCM. It can blacklist hosts dynamically when the LAN mode is set to “Route” under Web GUI→**System Settings**→**Network Settings**→**Basic Settings** page. If enabled, the traffic coming into the SoftwareUCM can be monitored, which helps prevent massive connection attempts or brute force attacks to the device. The blacklist can be created and updated by the SoftwareUCM firewall, which will then be displayed on the web page. Please refer to the following table for dynamic defense options on the SoftwareUCM.

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

SoftwareUCM Firewall Dynamic Defense

The following figure shows a configuration example like this:

- If a host at IP address 192.168.5.7 initiates more than 20 TCP connections to the SoftwareUCM it will be added to the SoftwareUCM blacklist.
- This host 192.168.5.7 will be blocked by the SoftwareUCM for 500 seconds.
- Since IP range 192.168.5.100-192.168.5.200 is in the whitelist if a host initiates more than 20 TCP connections to the SoftwareUCM it will not be added to the SoftwareUCM blacklist. It can still establish a TCP connection with the SoftwareUCM.

Security Settings

Static Defense

Dynamic Defense

Fail2Ban

Dynamic Defense

Dynamic Defense Enable

☒

\* Blocklist Update Interval (s)

120

\* Connection Threshold

100

Dynamic Defense Allowlist

192.168.5.100-192.168.5.200 1500:2000

Configure Dynamic Defense

Fail2ban

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

Security Settings

Static DefenseDynamic DefenseFail2Ban

Basic Protection

SIP Defense

Login Attack Defense

Customer Service Protection

Customer Service System Call Defense

Live Chat Protection

Global Protection Settings

Banned Duration (s)

600

Fail2ban Allowlist

Fail2ban Allowlist

Description / Comment

Add Fail2ban Allowlist

Blocklist

Banned

All

Search

Fail2ban Settings

SIP Defense	If enabled, the UCM will monitor failed SIP registration attempts and heartbeat timeouts based on the UCM’s 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 banned for the amount of time configured in the <i>Banned Duration</i> field.
Login Attack Defense	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 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 Max Retries value configured for this defense, the IP address will banned for the amount of time configured in the Banned Duration field.
Live Chat Protection	Once the number of chat attempts from an IP address has reached the Max Retries value configured for this defense, the IP address will banned for the amount of time configured in the Banned Duration field.
Banned Duration (s)	Configure the duration (in seconds) that an IP address is banned. 0 indicates a permanent ban.
Fail2ban Allowlist	Configure IP address, CIDR mask or DNS host in the allowlist. Fail2ban will not ban the host with matching address in this list.
Blocklist	Users will be able to view the IPs that have been blocked by UCM.

LDAP Server

The SoftwareUCM 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 SoftwareUCM 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 SoftwareUCM 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 SoftwareUCM, 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 SoftwareUCM. If the SoftwareUCM 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 SoftwareUCM 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 SoftwareUCM.

LDAP Server

LDAP Server Configurations

LDAP Phonebook

Enable LDAP Server

☒

\* Base DN

dc=pbx,dc=com

PBX DN

ou=pbx

,dc=pbx,dc=com

Root DN

cn=admin

,dc=pbx,dc=com

\* Root Password

••••••••

\* Confirm Root Password

••••••••

LDAP CA Cert

server.ca

Reset

Private Certificate and Key

LDAP Cert

server.crt

LDAP Private Key

private.key

Certificate & Private Key

Reset

Cancel

Save

LDAP Server Configurations

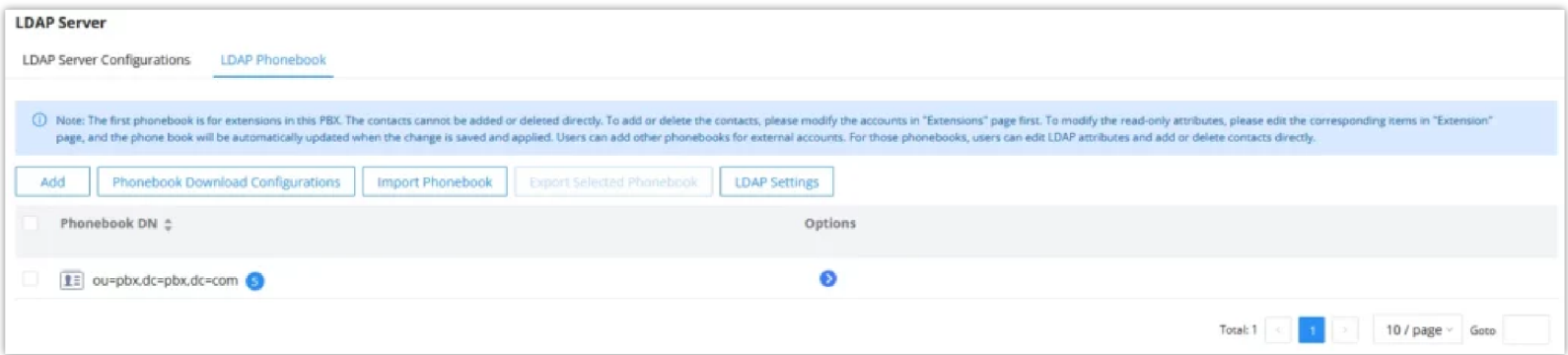
Enable LDAP Server	Enable LDAP Server
LDAP Server Address	LDAP server address is predefined by the datacenter chosen for the IPPBX. The user cannot modify this option.

<b>LDAPS Server Port</b>	LDAPS server port is predefined and cannot be set by the user. The port number is 636.
<b>Base DN</b>	Specifies the location in the directory where the search is requested to begin. It is predefined and cannot be modified.
<b>PBX DN</b>	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.
<b>Root DN</b>	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.
<b>Root Password</b>	Defines the root password for authentication.
<b>Confirm Root Password</b>	Confirms the root password for authentication.

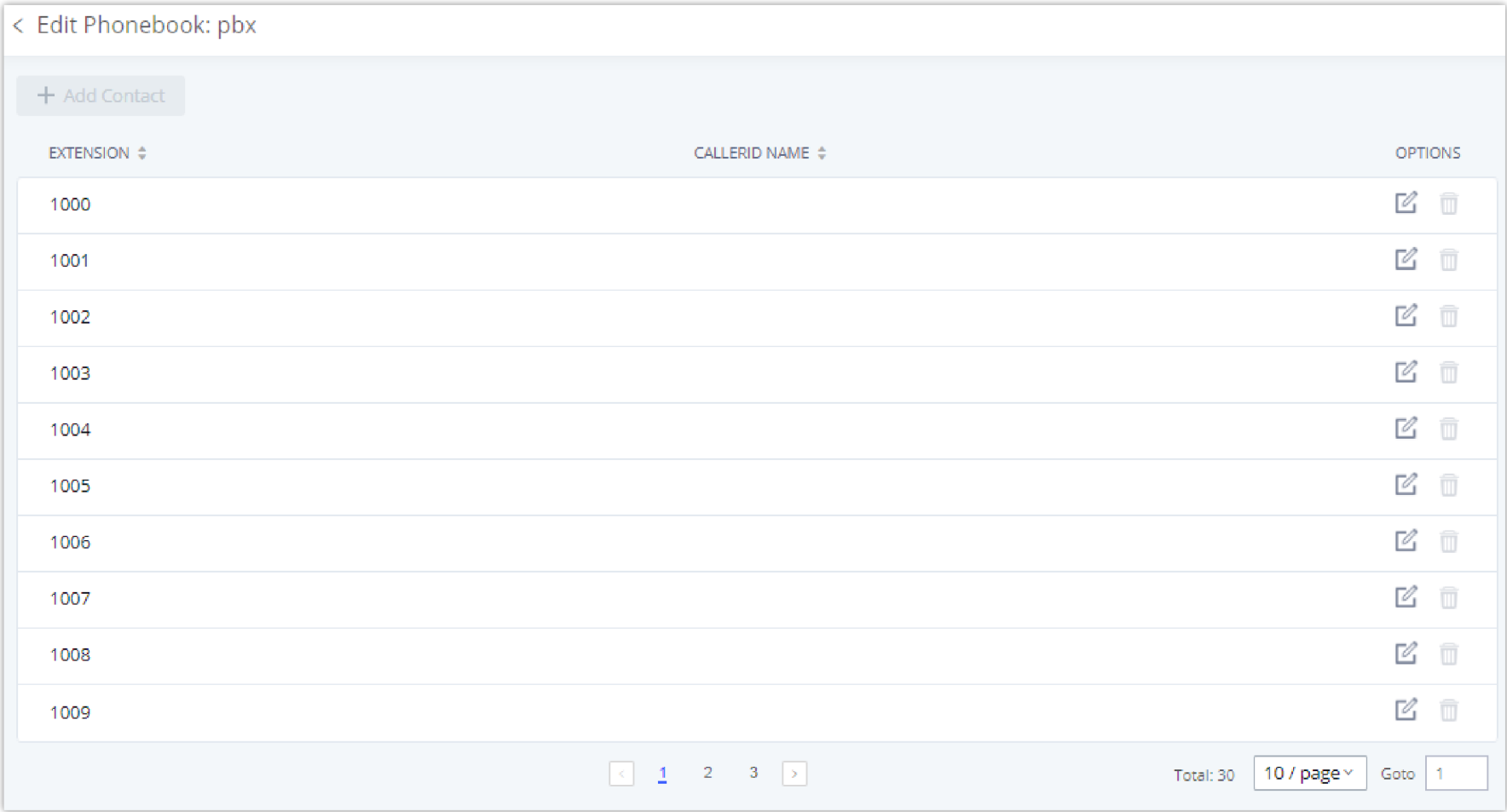
The SoftwareUCM LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client does not have to configure a username and password to access the phonebook directory. The “Root DN” and “Root Password” here are for LDAP management and configuration where users will need to provide 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 SoftwareUCM support secure LDAP (LDAPS) where the communication is encrypted and secure.



Default LDAP Phonebook DN

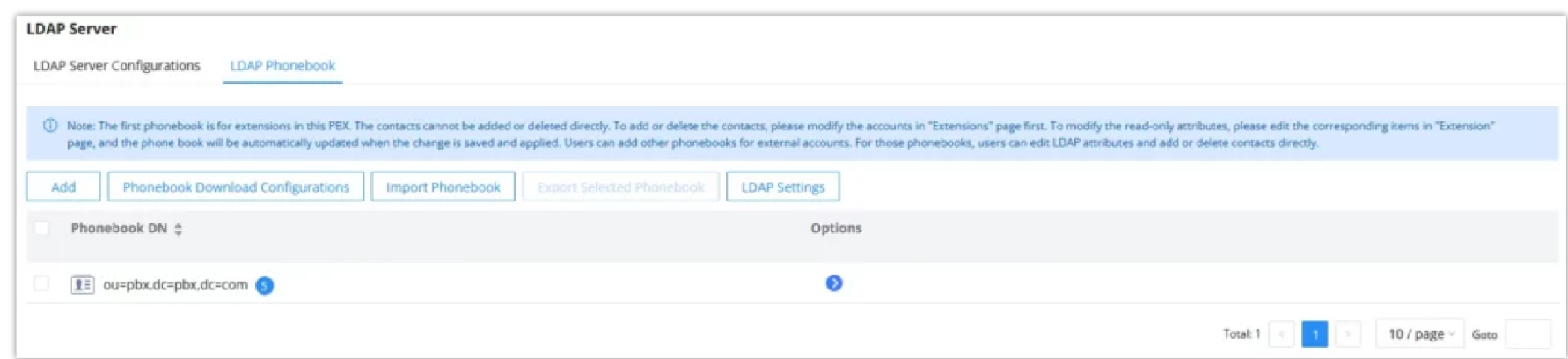


Default LDAP Phonebook Attributes

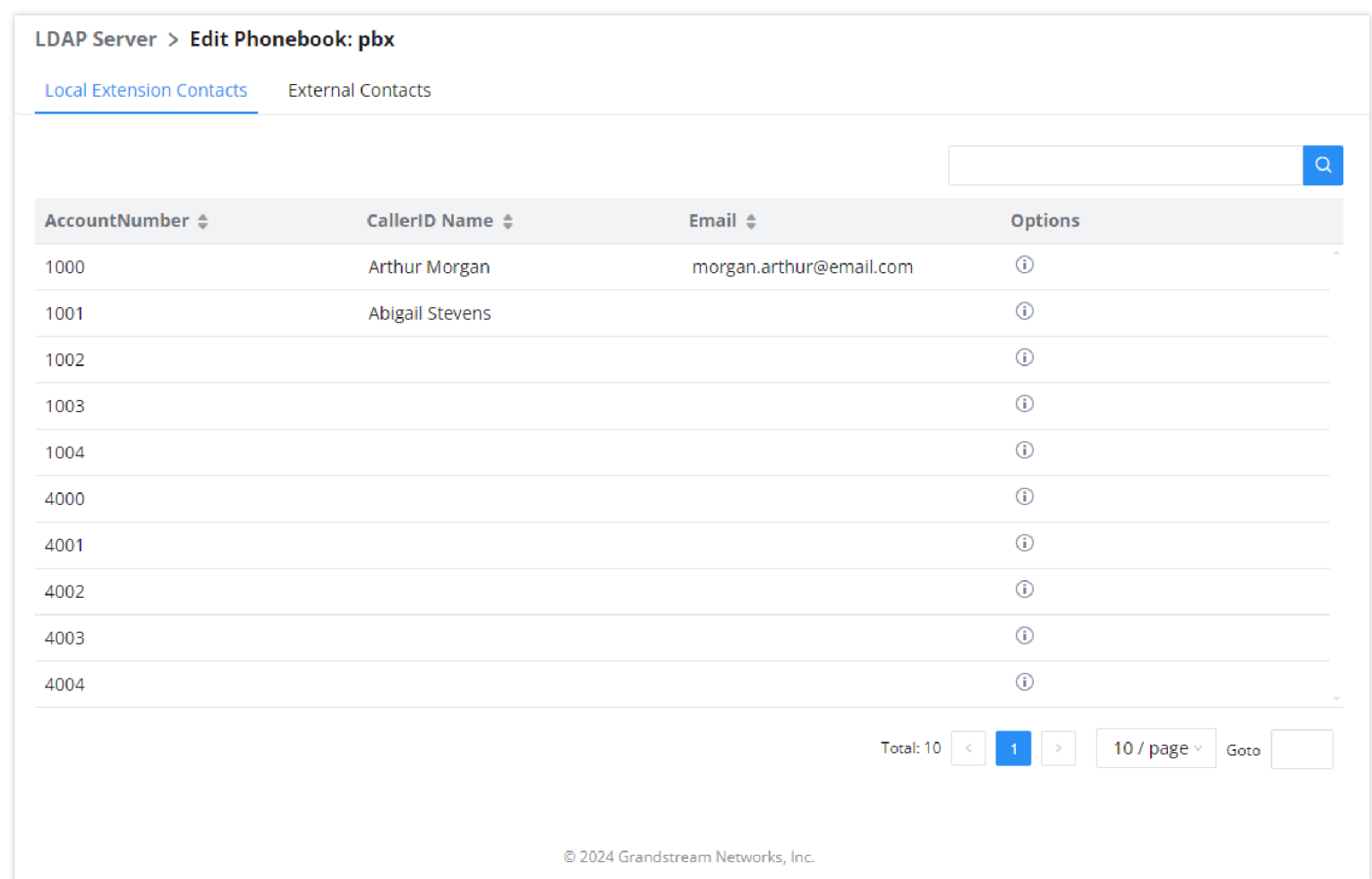
LDAP Phonebook



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.



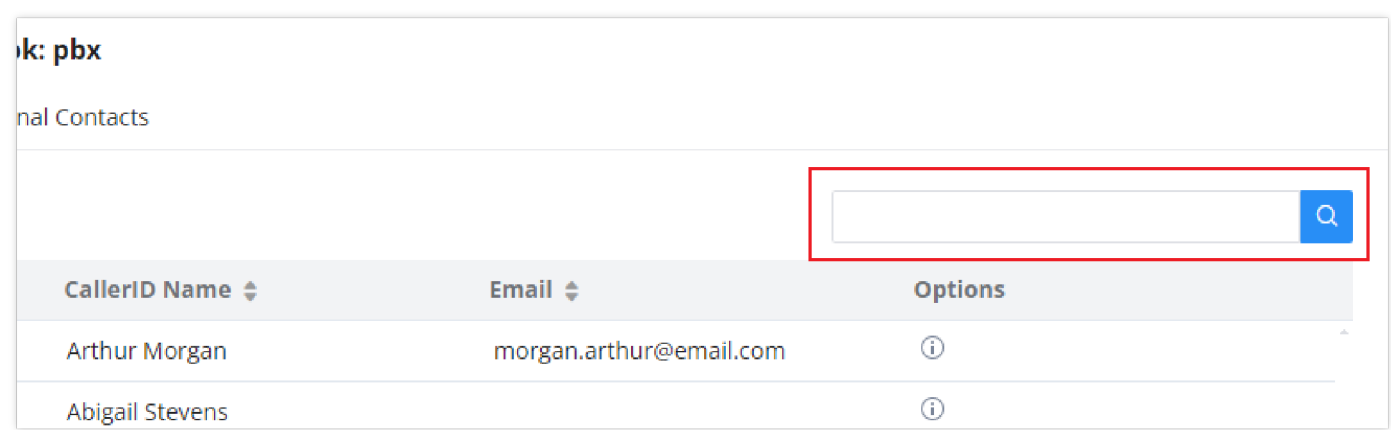
LDAP Phonebook



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 Search Bar

○ **Add new phonebook**

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

Add Phonebook

\* Phonebook Prefix



Phonebook DN

Cancel

Save

Add LDAP Phonebook

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

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

LDAP Server > Edit Phonebook: gtest

Add Contact

AccountNumber



CallerID Name

Email

Options

55555555

Dr.Smith



Total: 1

1

10 / page

Goto

Edit LDAP Phonebook

- Import phonebook from your computer to LDAP server

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

Import Phonebook

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

File Type

CSV

File

Choose File to Upload

Import Phonebook

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

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

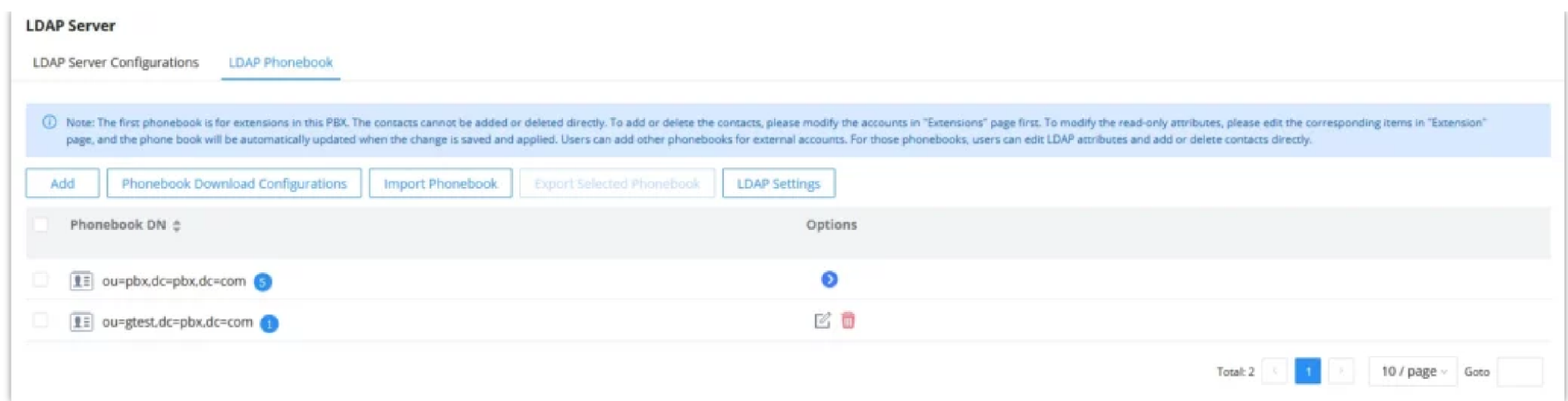
	A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	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 SoftwareUCM 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 SoftwareUCM LDAP Phonebook, the contacts in the CSV file will be added into the existing phonebook. If the phonebook DN does not exist on the SoftwareUCM LDAP Phonebook, a new phonebook with this phonebook DN will be created.

The samle phonebook CSV file in above picture will result in the following LDAP phonebook in the SoftwareUCM.

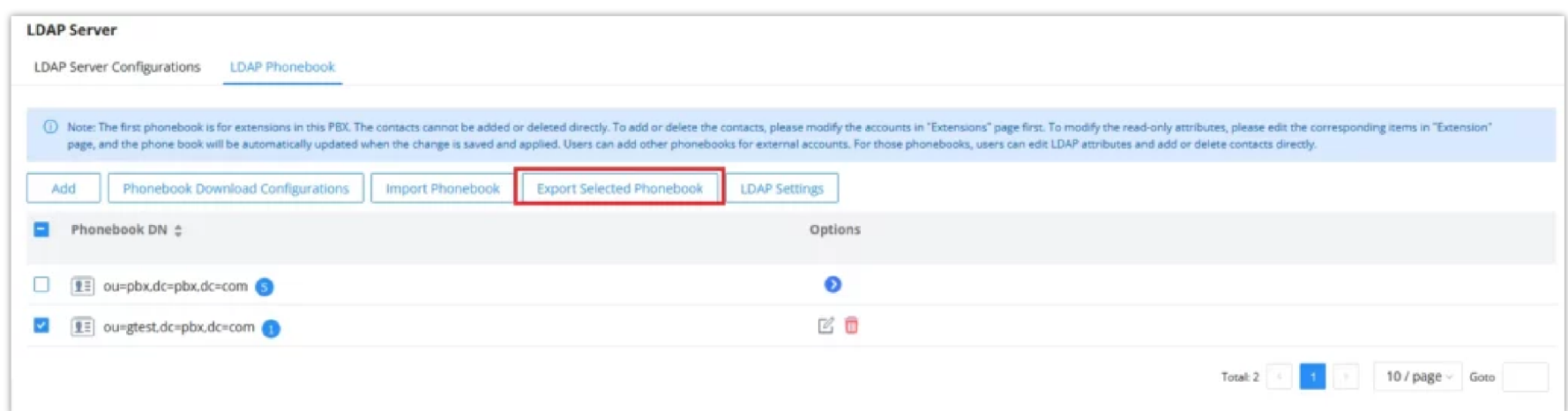


LDAP Phonebook After Import

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 SoftwareUCM LDAP server

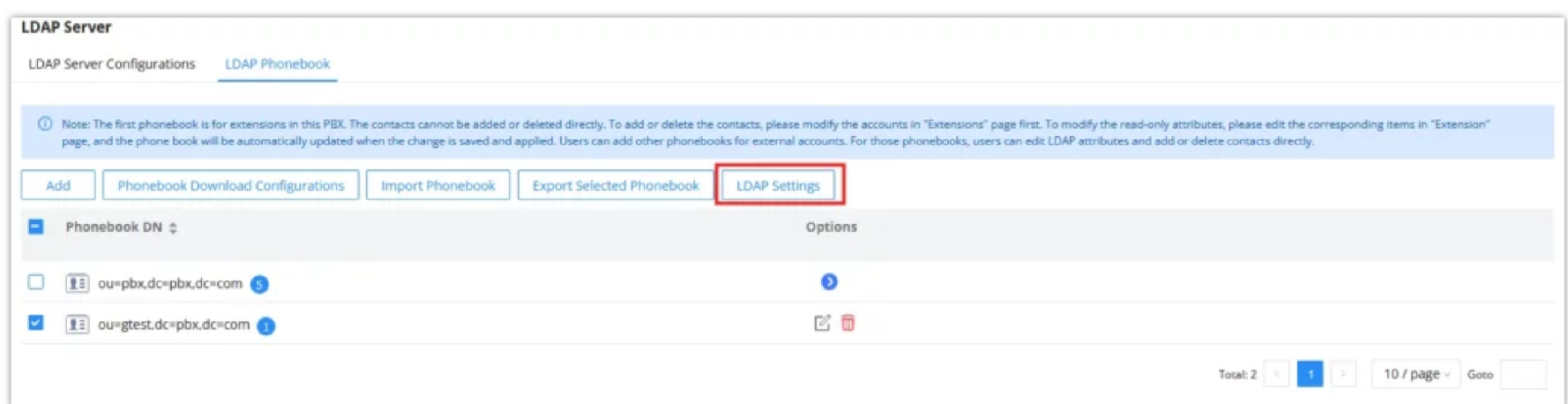
Select the checkbox for the LDAP phonebook and then click on "Export Selected Phonebook" to export the selected phonebook. The exported phonebook can be used as a record or a sample CSV, VFC or XML file for the users to add more contacts in it and import to the SoftwareUCM again.



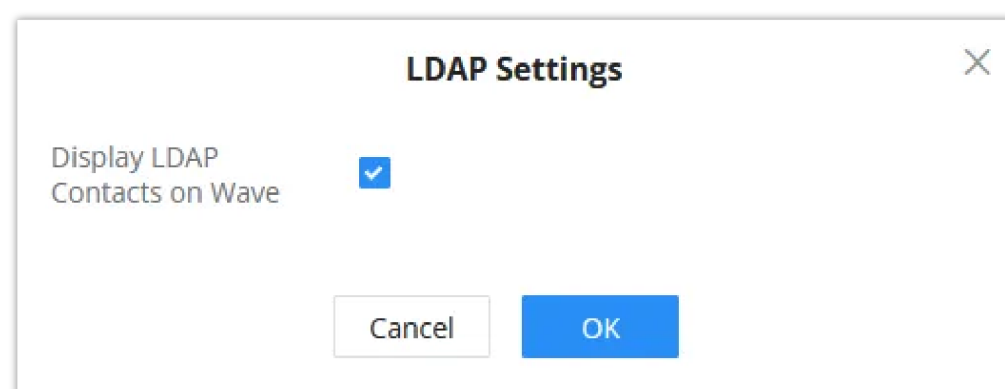
Export Selected LDAP Phonebook

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

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

LDAP Client Type

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

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

LDAP Server > Phonebook Download Configurations

Server Type

LDAP

AD

\* Server Address

192.168.1.1

\* Username

cn=admin,dc=pbx,dc=com

\* Filter

(objectClass=\*)

\* LDAP Number Attributes

AccountNumber MobileNumber HomeN

LDAP Name Attributes

CallerIDName Email Department FirstNa

\* Phonebook Name

LdapClient

\* Base DN

dc=pbx,dc=com

\* Password

\* Port

389

Automatic Update Cycle

None

Client Type

LDAP

Example

1. Client Configuration Examples

2. LDAP Configurations examples on Grandstream IP Phones

3. Examples of Endpoint Phonebook Download Configuration

Cancel

Save

LDAP Client Configurations

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

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

- **Server Address:** The IP address or domain name of the UCM
- **Base DN:** dc=pbx,dc=com
- **Username:** 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 CallerIDName

Max. Hits

50

Search Timeout

30

Sort Results

No

Yes

LDAP Lookup

Incoming Calls

Outgoing Calls

Lookup Display Name

Save

Save and Apply

Reset

GXP2170 LDAP Phonebook Configuration

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

AD Client Type

LDAP Server > Phonebook Download Configurations

Server Type

LDAP

AD

\* Server Address

192.168.1.1

\* Username

AD domain username

\* Filter

(objectClass=\*)

\* AD Attributes

telephoneNumber mail displayNa...

\* Host Name

\* Phonebook Name

LdapClient

\* Base DN

dc=pbx,dc=com

\* Password

\* Port

389

Automatic Update Cycle

None

Example

1. Client Configuration Examples

2. LDAP Configurations examples on Grandstream IP Phones

3. Examples of Endpoint Phonebook Download Configuration

Cancel

Save

AD Phonebook Server Type

Phonebook Name	Enter a name for the phonebook
Server Address	The IP address of the AD server
Base DN	Enter the base domain name.
Username	Enter the username used to authenticate into the LDAP server, if authentication is required.
Password	Enter the password used to authenticate into the LDAP server, if authentication is required.
Filter	Enter the filter. Ex: (&((CallerIDName=*)(AccountNumber=*))
Port	Enter the port number. Default port is 389
AD Attributes	AccountNumber must be included if the default configuration is used.
Automatic Update Cycle	If “None” is selected, LDAP phonebooks will not automatically update. Otherwise, LDAP phonebooks will automatically update at 00:00 / 12:00 AM with the selected frequency.
Host Name	Enter the host name of the remote AD server.

Time Settings

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

Time Zone Settings

To configure the SoftwareUCM to update time automatically, 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+01:00 ) Etc/GMT-1

Update Time Zone List

Cancel

Save

Automatic Date and Time

Important

The configurations under **Web GUI > Settings > Time Settings > Automatic Date** and Time page require reboot to take effect. Please consider configuring auto time updating related changes when setting up the SoftwareUCM for the first time to avoid service interrupt after installation and deployment in production.

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

Set Date and Time

To manually set the time on the SoftwareUCM, 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

Custom Time Groups

Date Format

yyyy-mm-dd

Time Format

Use 24-hour Format

Cancel

Save

Set Date and Time

Office Time

On the SoftwareUCM, 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

Custom Time Groups

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

Add

Delete

Import

Export

<input type="checkbox"/> Index	Time	Week	Month	Day	Options
<div><div></div><div>No data</div></div>					

Office Time

Time Settings > Create New Office Time

Time

00:00

-

23:59

Week

Sun	Mon	Tue	Wed
Thu	Fri	Sat	

Show Advanced Options

☐

Cancel

Save

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 files.

Time Settings

Time Zone Settings

Set Date and Time

Office Time

Holiday

Custom Time Groups

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

Add

Delete

Import

Export

<input type="checkbox"/> Index	Time	Week	Month	Day	Options
<input type="checkbox"/> 1	08:00-17:00	Mon Fri	Default	Default	<div><div></div><div></div></div>

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 UCM, the system administrator can define “holidays” 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→Holiday**, and click the “Add” button to see the following configuration page.

Time Settings > Create New Holiday

\* Name

Description

Year

2025

Month

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug

Sept

Oct

Nov

Dec

Day

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

Show Advanced Options

☒

Week

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Time

00:00

-

23:59

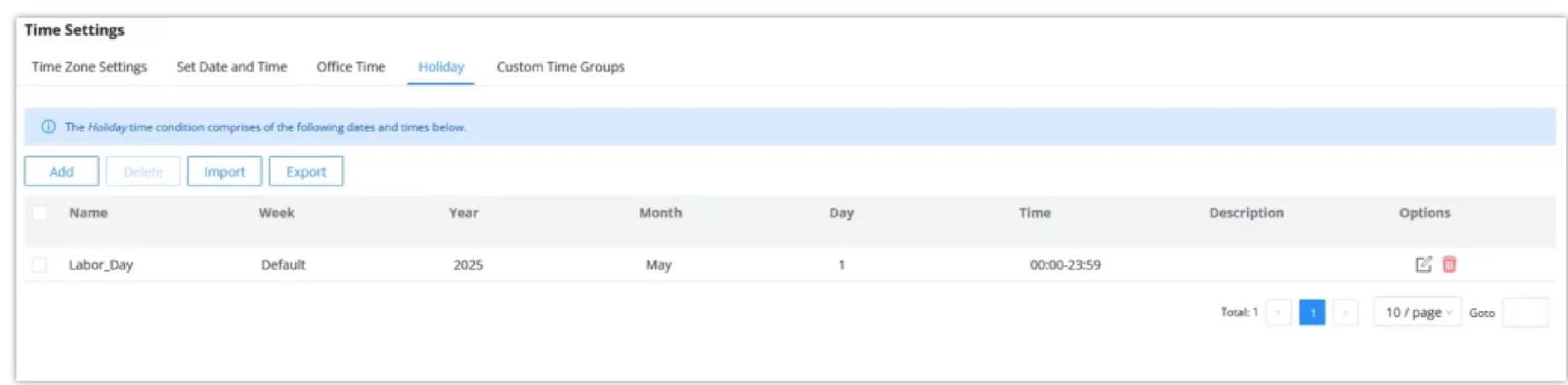
Create New Holiday

<b>Name</b>	Specify the holiday name to identify this holiday.
<b>Holiday Memo</b>	Create a note for the holiday.
<b>Month</b>	Select the month for the holiday.
<b>Year</b>	Select the Year for the holiday. <b>Note:</b> In the “Year” option, select “All” to set annual fixed holiday information.
<b>Day</b>	Select the day for the holiday.

Show Advanced Options	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
Week	Select the days as holiday in one week.
Time	Select the time on which the holiday starts.

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

The Holiday feature support import/export CSV files.



Settings→Time Settings→Holiday

○

Click on



to edit the holiday.

○

Click on



to delete the holiday.

○

Click on “**Delete**” to delete multiple selected holidays at once.

### Custom Time Groups

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

**Note**

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

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

Time Settings > Create New Custom Time Groups

\* Name

Description

Time Groups

Time

Start Time

-

End Time

Frequency

☒ By Week

☐ By Month

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Add

Time	Week	Month	Day	Options
<div></div>				

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 feature on the SoftwareUCM 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**.

Email Settings

Email Settings

Email Template

Email Footer Hyperlink

Email Send Log

Mail Server Providers

Common

TLS Enable

☒

Type

Client

Email Template Sending Format

HTML

\* Mail Server Domain

example.com

\* SMTP Server

Example: smtp.mydomain.com:25

Enable SASL Authentication

☒

\* Username

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

\* Password

Enable Email-to-Fax

☐

\* Display Name

PBX

\* Sender

PBX@example.com

Cancel

Save

Email Settings

Parameter	Description
Mail Server Providers	<p>Defines the mail service porvider category, the two availalble options are:</p> <ul style="list-style-type: none"><li><b>Common:</b> The Common category supports standard email protocols like SMTP, IMAP, and POP3, allowing integration with widely used email services such as Gmail, Yahoo Mail, or custom mail servers. It offers a flexible setup for sending and receiving emails without being tied to a specific provider.</li><li><b>Microsoft:</b> The Microsoft category is designed for Microsoft’s email services, including Microsoft 365, Exchange Server, and Outlook.com. It supports advanced features like OAuth authentication with Azure Active Directory and integration with Microsoft Graph API for seamless access to emails, calendars, and contacts.</li></ul>
TLS Enable	If enabled, TLS will be used when forwarding emails to the SMTP server.
Domain	Configures the domain of the UCM’s internal email server. This should not be the name of known and existing email servers (e.g. Gmail, Outlook, etc.).
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.
Domain	Specifies the domain of the mail server used to send emails for functions like voicemail to email and system notifications. This ensures proper routing and delivery of all outgoing emails.

<b>SMTP Server</b>	Enter the SMTP server. For example, smtp.mydomain.com:465. Port number cannot be 25.
<b>Enable SASL Authentication</b>	Toggles SASL authentication. If disabled, UCM will not use the username and password for email client authentication. Most email servers require login authentication while private email servers may allow anonymous login. If using Microsoft Exchange Server or if credentials are not required, please disable this option.
<b>Username</b>	Enter the username of the email account.
<b>Password</b>	Enter the password of the email account. It is highly recommended to use HTTPS when saving and applying password changes.
<b>Enable Email-to-Fax</b>	Monitors the inbox of the configured email address for the specified subject. If detected, the UCM will get a copy of the attachment from the email and send it to the XXX extension by fax. The attachment must be in PDF/TIF/TIFF format.
<b>Email-to-Fax Blacklist/Whitelist</b>	<ul style="list-style-type: none"><li>• <b>Disable:</b> This option is disabled.</li><li>• <b>Enable Blacklist:</b> Select the blacklist to apply.</li><li>• <b>Enable Whitelist:</b> Select the whitelist to apply.</li></ul> <b>Note:</b> This option only appears when “Enable Email-to-Fax” is enabled.
<b>Email-to-Fax Subject Format</b>	Select the email subject format to use for emails to fax. XXX refers to the extension that the fax will be sent to. This extension can only contain numbers. <b>Note:</b> This option only appears when “Enable Email-to-Fax” is enabled.
<b>Fax Sending Success/Failure Confirmation</b>	If enabled, the UCM will send an email notification to the sender about the fax sending result. <b>Note:</b> This option only appears when “Enable Email-to-Fax” is enabled.
<b>POP/POP3 Server Address</b>	Enter the IP address of the POP/POP3 server. <b>Note:</b> This option only appears when “Enable Email-to-Fax” is enabled.
<b>POP/POP3 Server Port</b>	Enter the port of the POP/POP3 server. <b>Note:</b> This option only appears when “Enable Email-to-Fax” is enabled.
<b>Display Name</b>	Enter the name of the PBX that will be displayed in sent emails.
<b>Sender</b>	Enter the email used to send the emails.

The following figure shows a sample Email setting on the SoftwareUCM

Once the configuration is finished, click on “Test”. The test page directly returns the result, clearly indicating that the task has been submitted or the email sent failed with the reason.

In the prompt, fill in a valid Email address to send a test email to verify the Email settings on the SoftwareUCM.

### Email Template

The Email templates on the SoftwareUCM 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 Settings	Email Template	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 SoftwareUCM 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 SettingsEmail TemplateEmail Footer HyperlinkEmail Send Log

Text

Company Info

Text

Contact Us

URL

https://www.grandstream.com

URL

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

Cancel

Save

Add

Email Footer Hyperlink

### Email Send Log

Under SoftwareUCM 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 Settings	Email Template	Email Footer Hyperlink	Email Send Log		
<div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div> <div><div>Show All Logs</div><div>Clear</div><div>Delete Search Result(s)</div></div> <div><div>Display Filter</div></div>					
Send Result	Recipient	Email Send Module	Email Generated Time	Last Send Time	Details

Email Send Log

Start Time

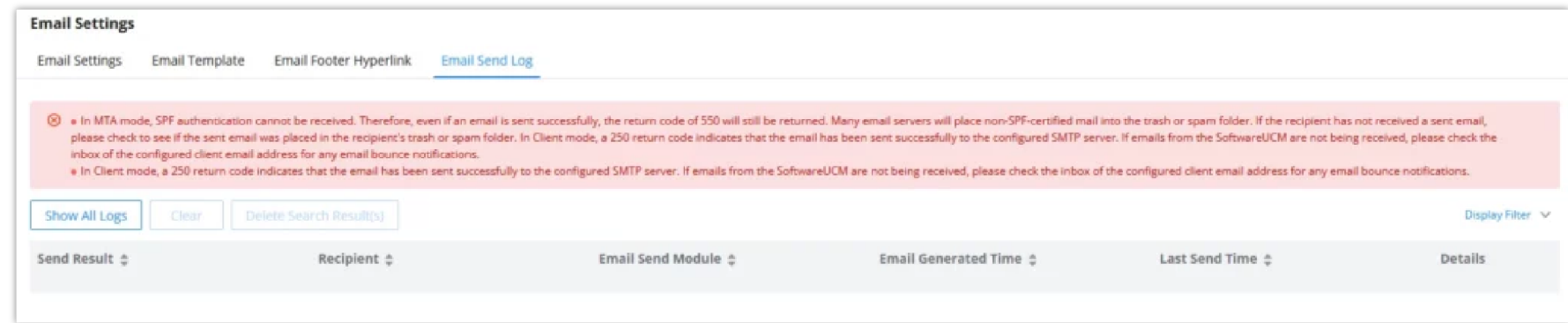
Enter the start time for the filter



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	<div>Select the email module to filter with from the drop-down list, which contains:</div> <div><div></div><div><div>All Modules</div><div>Extension</div><div>Voicemail</div><div>Conference Schedule</div><div>User Password</div><div>Alert Events</div><div>CDR</div><div>Test</div></div></div>

Email Log – Display Filter

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



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.
535	The username and password verification in the client mode is incorrect. Please check whether the username and password are configured correctly.

Code	Description
550	<p>Possible reasons:</p> <ol style="list-style-type: none"><li>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.</li><li>2. The number of destination addresses sent by the sender exceeds the maximum limit per day and is temporarily blacklisted. Please reduce the sending frequency or try again the next day.</li><li>3. The sender’s IP does not pass the SPF permission test of the sending domain. Emails sent in MTA mode may return this error code even if they are sent.</li></ol>
552	The sent email is too large or the email attachment type is prohibited
553	The sender and the email account are inconsistent, please configure the sender as your email account correctly.
554	The email was identified as spam. Please reduce the sending frequency or try again the next day
none	<p>This indicates that there is no return code.</p> <p>If the sending result is “deferred”, the general reason is that the mail service area is configured incorrectly. Please check whether the server configuration is correct.</p> <p>If the sending result is “bounced”, the general reason is that the receiving email address domain name is wrong, please check whether the email recipient is the correct email address. If it is in MTA mode, please check whether the “domain” is configured to be in the same domain name as the “recipient”.</p>

# 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 Na...

<input type="checkbox"/>	Extension	Name	Department	Email Addresses	Contact Privileges	Options
<input type="checkbox"/>	1000		Enterprise Root Directory		All Contacts (Same as Department)	
<input type="checkbox"/>	1001		Enterprise Root Directory		All Contacts (Same as Department)	
<input type="checkbox"/>	1002		Enterprise Root Directory		All Contacts (Same as Department)	
<input type="checkbox"/>	1003		Enterprise Root Directory		All Contacts (Same as Department)	
<input type="checkbox"/>	1004		Enterprise Root Directory		All Contacts (Same as Department)	

Total: 5

<

1

>

10 / page

Goto

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.

Contact Management > Edit Extension Contacts: 1000

\* Extension

1000

First Name

John

Last Name

Doe

Department

Enterprise Root Directory

Job Title

Support Engineer

Email Address

Mobile Number

+1

Home Number

Fax

Contact Privileges

Same as Department Contact Privileges

☒

\* Contact View Privileges

All Contacts

Add / Edit Privileges

Cancel

Save

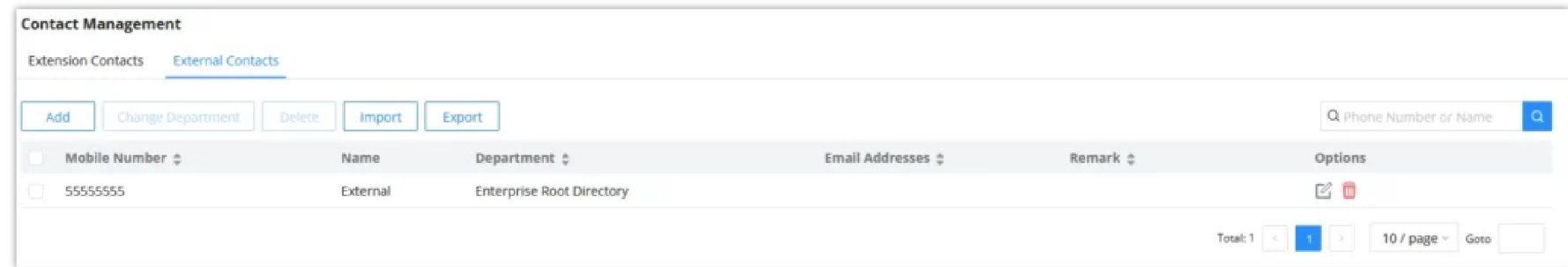
Edit Extension Contact

Extension	Displays extension number.
First Name	Configure first name for the extension contact.

<b>Last Name</b>	Configure last name for the extension contact.
<b>Department</b>	Select department for the extension contact. Department can be created in “Department Management” page.
<b>Department Title</b>	Configure the job title for the extension contact.
<b>Email Address</b>	Configure email address for the extension contact.
<b>Mobile Phone Number</b>	Configure mobile phone number for the extension contact.
<b>Home Number</b>	Configure home number for the extension contact
<b>Fax</b>	Configure Fax for the extension contact.
<b>Same as Department Contact Privileges</b>	When this option is enabled, the contact extension will inherit the same privilege as the department it belongs to.
<b>Contact View Privileges</b>	This option allows configuring privileges for the contact extension. <b>Note:</b> This option will be disabled if “ <b>Same as Department Contact Privileges</b> ” has been enabled.

- External contacts

On external contacts page, the admin can create single external contact, import contacts in batch, edit contacts, delete contacts and export contacts.

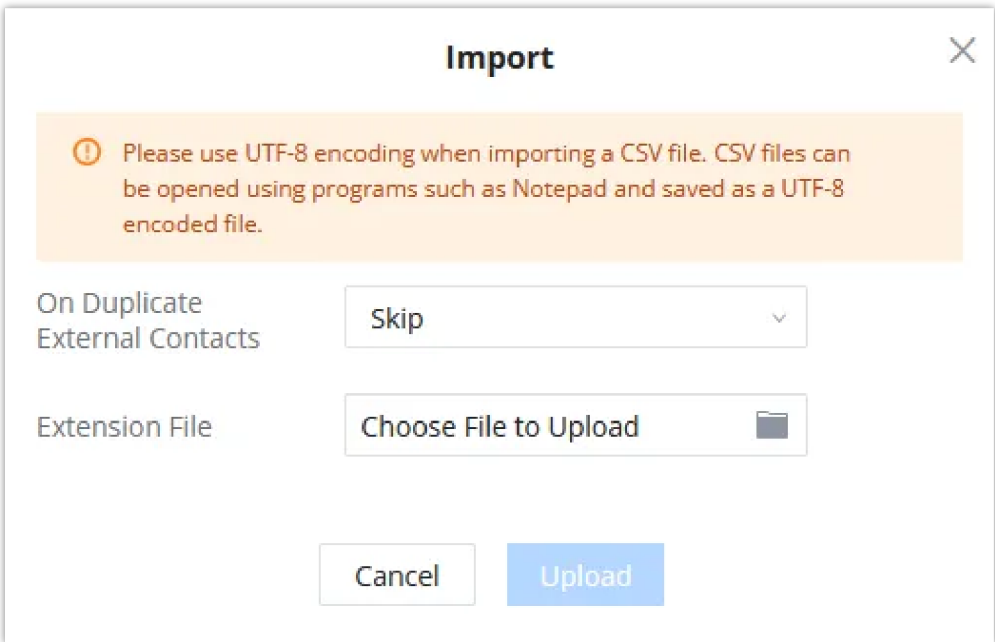


External Contacts

Click on “Export” icon, a CSV format file will be generated with the current external contacts.

Click on “import” icon, then follow the steps below to add external contacts in batch:

- Step 1:** For option “On Duplicate External Contacts”, select whether to skip duplicate contact on the imported CSV file or update the duplicate UCM contact with the information in the CSV.
- Step 2:** Choose file from local PC to upload.
- Step 3:** Click on “Upload”.
- Step 4:** Click on “Apply” to complete importing external contacts.



Import External Contacts

## Department Management

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

Department Management			
<div>Add</div>			
Department Name	Number of Members	Contact Privileges	Options
Enterprise Root Directory	6	All Contacts	<div><div></div><div></div><div></div><div></div><div></div></div>
IT	2	All Contacts	<div><div></div><div></div><div></div><div></div><div></div></div>
Support	0	All Contacts	<div><div></div><div></div><div></div><div></div><div></div></div>
Marketing	0	All Contacts	<div><div></div><div></div><div></div><div></div><div></div></div>

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

Marketing

Upper Level Department

Enterprise Root Directory

\* Contact View Privileges

All Contacts

Add / Edit Privileges

Privileges Applied To Sub-Level Departments

Cancel

OK

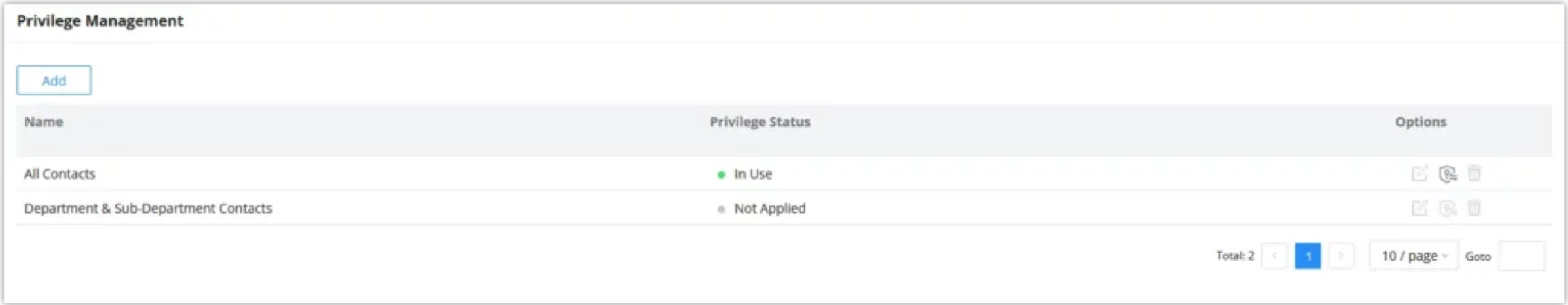
Edit Department

## 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.

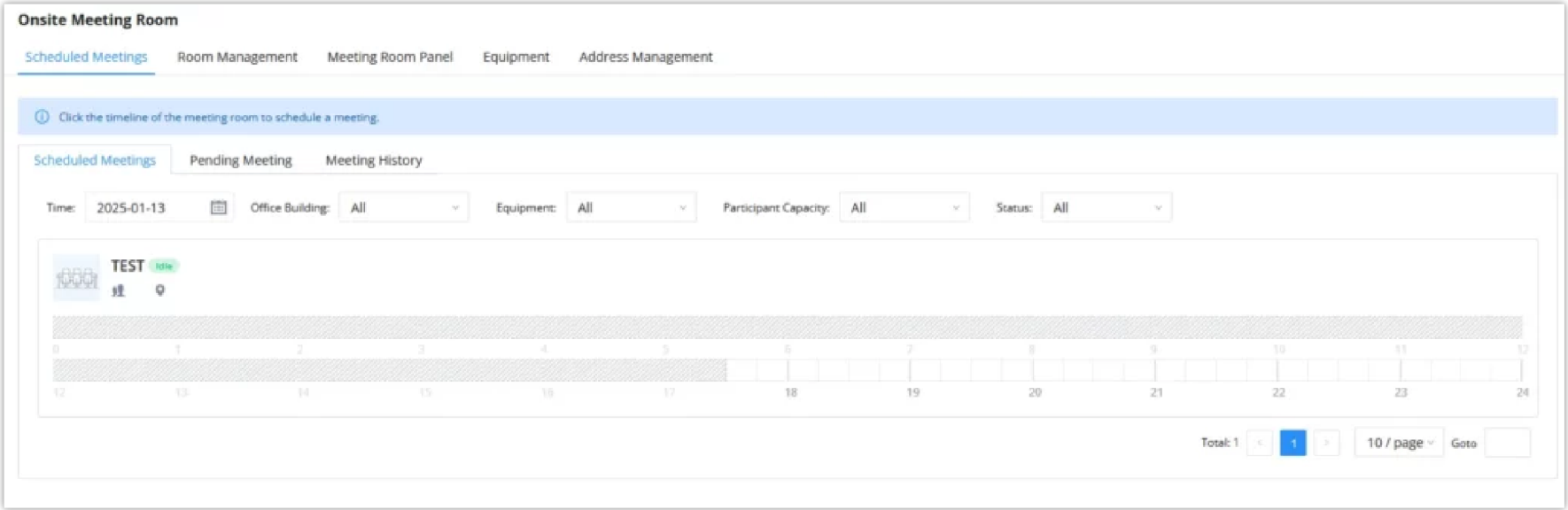


Privilege Management

## DEVICE MANAGEMENT

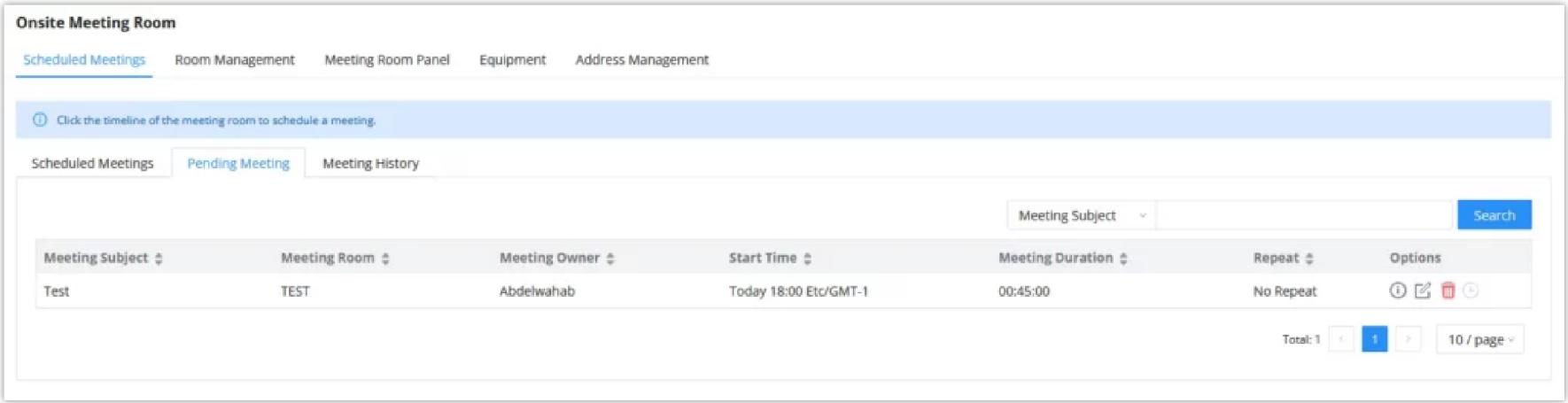
### Onsite Meeting Room

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.



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

Total: 1

Normal: 0

Unmonitored: 1

Abnormal: 0

All

Device-Number / Device Name

Add

Edit Allowed Members

Delete

Import

Export

No.	Device Number	Device Name	URL	Options
1	4001	GSC3620	rtsp://192.168.5.74:554	<div></div> <div></div>

Total: 1

10 / page

Goto

IPC Devices

IP Camera Devices > Create New IP Camera Devices

General

\* Device Number

\* Device Name

\* Protocol

RTSP

\* IP Address

\* Port

554

Channel Path

Username

Password

\* Transport Protocol

UDP

Heartbeat Detection

User Settings

\* Allowed Members

Cancel

Save

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. <div><div>●</div>RTSP</div>
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 if 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.

## Zero Config

### Overview

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

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

### Configuration Architecture for End Point Device

The endpoint device configuration in **Zero Config** is divided into the following three layers with priority from the lowest to the highest:

- Global

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

- Model

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

- Device

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

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

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

After understanding the **Zero Config** configuration architecture, users could configure the available options for endpoint devices to be provisioned by the SoftwareUCM by going through the three layers. This configuration architecture allows users to set up and manage the Grandstream endpoint devices in the same LAN area in a centralized way.

### Auto-Provisioning Settings

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

o SIP SUBSCRIBE

When the phone boots up, it sends out SUBSCRIBE to a multicast IP address in the LAN. The SoftwareUCM discovers it and then sends a NOTIFY with the XML config file URL in the message body. The phone will then use the path to download the config file generated in the SoftwareUCM and take the new configuration.

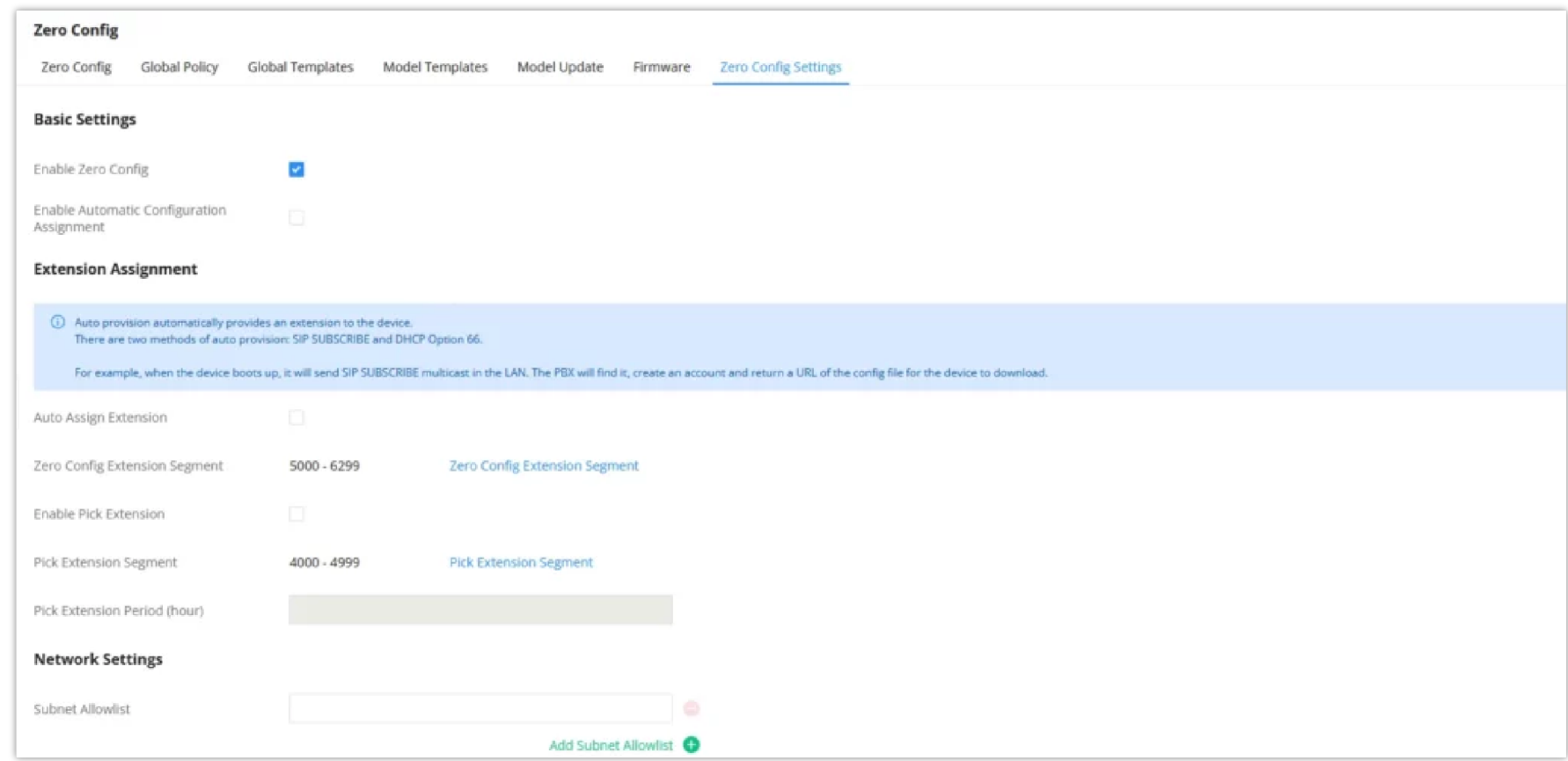
o DHCP OPTION 66

Route mode needs to be set to use this feature. When the phone restarts (by default DHCP Option 66 is turned on), it will send out a DHCP DISCOVER request. The SoftwareUCM receives it and returns the DHCP OFFER with the config server path URL in Option 66, for example, https://192.168.2.1:8089/zccgi/. The phone will then use the path to download the config file generated in the SoftwareUCM.

o mDNS

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

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



Auto Provision Settings

Enable Zero Config	Enable or disable the Zero Config feature on the PBX. The default setting is enabled.
Enable Automatic Configuration Assignment	By default, this is disabled. If disabled, when the SIP device boots up, the SoftwareUCM will not send the SIP device the URL to download the config file, and therefore the SIP device will not be automatically provisioned by the SoftwareUCM. <b>Note:</b> When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the SoftwareUCM which will include the XML config file URL for the SIP device to download.
Auto Assign Extension	If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in the “Zero Config Extension Segment” to the device. The default setting is disabled.
Zero Config Extension Segment	Click on the link “ <b>Zero Config</b> Extension Segment” to specify the extension range to be assigned if “Automatically Assign Extension” is enabled. The default range is 5000-6299. <b>Zero Config</b> Extension Segment range can be defined in Web GUI→ <b>PBX Settings</b> → <b>General Settings</b> → <b>General</b> page→Extension Preference section: “Auto Provision Extensions”.

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

Auto Provision Settings

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

Discovery

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

- PING
- ARP
- SIP Message (NOTIFY)

Click on "Auto Discover" under Web GUI→**Device Management**→**Zero Config**→**Zero Config**, fill in the "Scan Method" and "Scan IP". The IP address segment will be automatically filled in based on the network mask detected on the SoftwareUCM. If users need to scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address. Then click on "Save" to start discovering the devices within the same network.

Auto Discover

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

PBX Network Interface IP Address

192.168.6.186

Network Segment

192.168.6.0 - 192.168.6.255

Broadcast IP

192.168.6.255

Scan Method

Ping

Subnet Allowlist

Local Subnet Only

Scan IP

192

.

168

.

6






.

Cancel

OK

Auto Discover

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

<input type="checkbox"/>	MAC Address ↕	IP Address ↕	Extension	Version ↕	Vendor ↕	Model ↕	Create Config ↕	Options
<input type="checkbox"/>	C074AD75635E	192.168.80.183	--	1.0.11.57	GRANDSTREAM	--	--	    

Total: 1 < 1 > 30 / page Goto

Discovered Devices

Firmware

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




Zero Config

Zero ConfigGlobal PolicyGlobal TemplatesModel TemplatesModel UpdateFirmwareZero Config Settings

Firmware Storage PathLocal

Firmware List

Upload

Name ↕	Model ↕	Firmware Version ↕	Date ↕	Size ↕	Status ↕	Options
wp8x6fw.bin	WP8x6	1.0.1.52	2025-01-15 14:58:12	56.24 MB	Disabled	  

Total: 1 < 1 > 10 / page Goto

CancelSave

Upload Firmware Files to the SoftwareUCM

Upload New Firmware

\* Enable☒

Model

Firmware Version

Remark

Choose File to Upload

CancelUpload

Upload New Firmware

- **Enable:** toggles whether the SoftwareUCM will provision this firmware to endpoints if they are using the SoftwareUCM as the firmware server. If not enabled, the SoftwareUCM will reject requests from endpoints for this firmware.
- **Model:** The device model for which this firmware is intended. Only for self-reference and does not affect provisioning.
- **Firmware:** The firmware version of the file being uploaded. Only for self-reference and does not affect provisioning.
- **Remark:** Add a comment about the uploaded firmware. Only for self-reference and does not affect provisioning.
- **Choose File to Upload:** Select the firmware file to upload from the user’s PC. The file name must match the firmware file name requested by the endpoint.

Uploading Devices List

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

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	===== Device Start =====													
2	config_name	vendor	state	ip	account_secret	file_url	url_parameters	last_access	mac	version	ad_state	model	hot_desking	port
3		Grandstream	1	192.168.5.172		https://192.168.5.147:8080/	#####	000B82495	1.0.7.10	0	GXW4248	no	5060	
4														
5	===== Device Start =====													
6	config_name	vendor	state	ip	account_secret	file_url	url_parameters	last_access	mac	version	ad_state	model	hot_desking	port
7		Grandstream	1	192.168.5.114		https://192.168.5.147:8080/	#####	000B826B3	1.0.3.227	0	GXV3240	no	5060	
8														
9	===== Device Start =====													
10	config_name	vendor	state	ip	account_secret	file_url	url_parameters	last_access	mac	version	ad_state	model	hot_desking	port
11		Grandstream	1	192.168.5.201		https://192.168.5.147:8080/	#####	000B826F5	1.0.1.106	0	--	no	5080	

Device List – CSV file Sample

Note

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

Managing Discovered Devices

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

Filter: 

All

to display corresponding results.

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

Zero Config													
<div>Zero ConfigGlobal PolicyGlobal TemplatesModel TemplatesModel UpdateFirmwareZero Config Settings</div>													
Total: 9Registered: 0Unregistered: 9													
<div>AllAll ModelAll VendorModel / Extension Number / MAC Address / IP Address</div>													
<div>Auto DiscoverAddDeleteEditUpgradeUpdate ConfigRebootMore</div>													
	No.	Model	Extension	Vendor	IP Address	Version	Create Config	Options					
<input type="checkbox"/>	1	GXP2160	--	GRANDSTREAM	192.168.6.33	1.0.11.85	--						
<input type="checkbox"/>	2	DP750	--	GRANDSTREAM	192.168.6.8	1.0.21.19	--						

Managing Discovered Devices

From the main menu of Zero Config, users can perform the following operations:

- Click

Auto Discover

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

- Click

Add

to add a new device to the Zero Config database using its MAC address.

- Click

Delete

to delete selected devices from the Zero Config database.

- Click

Edit

to modify selected devices.

- Click

Update Config

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

- Click

Reboot

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

- Click

More ▾

then reset, to clear all device configurations.

- Click

More ▾

then import, to upload xlsx file containing a list of devices.

- Click

More ▾

the export, to export CSV file containing a list of devices. This file can be imported to another SoftwareUCM to quickly set it up with the original SoftwareUCM devices.

- Click

More ▾

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

All these operations will be detailed in the next sections.

## Global Configuration

The global configuration will apply to all the connected Grandstream SIP endpoint devices in the same LAN with the SoftwareUCM no matter what the Grandstream device model it is. It is divided into two levels:

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

Global Templates configuration has higher priority than Global Policy configuration.

## Global Policy



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

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

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

Zero Config

Zero Config

Global Policy

Global Templates

Model Templates

Model Update

Firmware

Zero Config Settings

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

Import

Export

> Localization

> Phone Settings

> Contact List

> Maintenance

> Network Settings

> Customization

> Communication Settings

Cancel

Save

Global Policy Categories

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

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

Global Policy Parameters – Localization

Default Call Settings
-----------------------



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

*Global Policy Parameters – Phone Settings*

<b>LDAP Phonebook</b>	
<b>Source</b>	<p>Select “Manual” or “PBX” as the LDAP configuration source.</p> <ul style="list-style-type: none"><li>◦ If “Manual” is selected, the LDAP configuration below will be applied to the SIP end device.</li><li>◦ If “PBX” is selected, the LDAP configuration built-in from SoftwareUCM Web GUI→<b>System Settings</b>→<b>LDAP Server</b> will be applied.</li></ul>
<b>Address</b>	Configure the IP address or DNS name of the LDAP server.
<b>Port</b>	Configure the LDAP server port. The default value is 389.
<b>Base DN</b>	<p>This is the location in the directory where the search is requested to begin. Example:</p> <ul style="list-style-type: none"><li>◦ dc=grandstream, dc=com</li><li>◦ ou=Boston, dc=grandstream, dc=com</li></ul>

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

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

Global Policy Parameters – Contact List

Upgrade and Provision	
<b>Firmware Source</b>	<p>Firmware source via Zero Config provisioning could be a URL for an external server address, local UCM directory, or USB media if plugged into the SoftwareUCM. Select a source to get the firmware file: URL, Local UCM Server, Local USB Media, Local SD Card Media</p> <ul style="list-style-type: none"><li>● <b>URL:</b> If selected to use URL to upgrade, complete the configuration for the following four parameters: “Upgrade Via”, “Server Path”, “File Prefix” and “File Postfix”.</li><li>● <b>Local UCM Server:</b> Firmware can be uploaded to the UCM internal storage for firmware upgrade. If selected, click on the “Manage Storage” icon next to the “Directory” option, upload the firmware file, and select a directory for the end device to retrieve the firmware file.</li><li>● <b>Local USB Media:</b> If selected, the USB storage device needs to be plugged into the UCM and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory.</li><li>● <b>Local SD Card Media:</b> If selected, an SD card needs to be plugged into the UCM and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory.</li></ul>
<b>Upgrade via</b>	<p>When the URL is selected as a firmware source, configure upgrade via TFTP, HTTP, or HTTPS.</p>
<b>Server Path</b>	<p>When the URL is selected as a firmware source, configure the firmware upgrading server path.</p>
<b>File Prefix</b>	<p>If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone.</p>
<b>File Postfix</b>	<p>If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.</p>

<b>Config Server Path</b>	When the URL is selected as a firmware source, configure the firmware file postfix. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed onto the phone.
<b>Allow DHCP Option 43/66</b>	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
<b>Automatic Upgrade</b>	<p>If enabled, the endpoint device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week, or by minute. By week Once selected, specify the day of the week to check the HTTP/TFTP server for firmware upgrades or configuration file changes.</p> <ul style="list-style-type: none"><li>• <b>By day:</b> Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration file changes.</li><li>• <b>By minute:</b> Once selected, specify the interval X that the SIP end device will request for new firmware every X minutes.</li></ul>
<b>Firmware Upgrade Rule</b>	Specify how firmware upgrading and provisioning requests are to be sent.
<b>Web Access</b>	
<b>Zero Config</b>	Select either to enable or disable Zero Config
<b>Admin Password</b>	Configure the administrator password for admin-level login.
<b>End-User Password</b>	Configure the end-user password for the end-user-level login.
<b>Web Access Mode</b>	Select HTTP or HTTPS as the web access protocol.
<b>Web Server Port</b>	Configure the port for web access. The valid range is 1 to 65535.
<b>RTSP Port</b>	Configure the RTSP Port.
<b>Enable UPnP Discovery</b>	Select either to enable or disable Enable UPnP Discovery.
<b>User Login Timeout</b>	Configure User Login Timeout.
<b>Maximum Consecutive Failed Login Attempts</b>	Configure Maximum Consecutive Failed Login Attempts.
<b>Login Error Lock Time</b>	Configure Login Error Lock Time.
<b>Security</b>	
<b>Disable Telnet/SSH</b>	<p>Enable Telnet/SSH access for the SIP end device.</p> <ul style="list-style-type: none"><li>• If the SIP end device supports Telnet access, this option controls the Telnet access of the device.</li><li>• if the SIP end device supports SSH access, this option controls the SSH access of the device.</li></ul>
<b>Syslog</b>	
<b>Syslog Server</b>	Configure the URL/IP address for the Syslog server.
<b>Syslog Level</b>	Select the level of logging for Syslog.
<b>Send SIP Log</b>	Configure whether the SIP log will be included in the Syslog message.

<b>Basic Settings</b>	
<b>IP Address</b>	<p>Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected.</p> <ul style="list-style-type: none"> <li>◦ <b>DHCP</b></li> </ul> <p>Once selected, users can specify the Host Name (option 12) of the SIP end device as DHCP client and Vendor Class ID (option 60) used by the client and server to exchange vendor class ID information.</p> <ul style="list-style-type: none"> <li>◦ <b>PPPoE</b></li> </ul> <p>Once selected, users need to specify the Account ID, Password, and Service Name for PPPoE.</p>
<b>Host Name</b>	Specify the name of the client. This field is optional but may be required by Internet Service Providers.
<b>Vendor Class ID</b>	Used by clients and servers to exchange vendor class ID.
<b>Account ID</b>	Enter the PPPoE account ID.
<b>Password</b>	Enter the PPPoE Password.
<b>Service Name</b>	Enter the PPPoE Service Name.
<b>Advanced Setting</b>	
<b>Layer 3 QoS</b>	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv, or MPLS. The valid range is 0-63.
<b>Layer 3 QoS For RTP</b>	<p>Assign the priority value of the Layer 3 QoS for RTP packets.</p> <p>The valid range is 0 -63.</p>
<b>Layer 3 QoS For SIP</b>	<p>Assign the priority value of the Layer 3 QoS for SIP packets.</p> <p>The valid range is 0 -63.</p>
<b>Layer 2 QoS Tag</b>	<p>Assign the VLAN Tag of the Layer 2 QoS packets.</p> <p>The valid range is 0 -4095.</p>
<b>Layer 2 QoS Priority Value</b>	<p>Assign the priority value of the Layer 2 QoS packets.</p> <p>The valid range is 0-7.</p>
<b>STUN Server</b>	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
<b>Keep-Alive</b>	Select either to enable or disable Keep Alive.
<b>Keep Alive Interval</b>	Specify how often the phone will send a blank UDP packet to the SIP server to keep the “ping hole” on the NAT router open. The valid range is 10-160.
<b>Register Expiration</b>	Specify the Register Expiration.

<b>Local SIP Port</b>	Configure Local SIP Port.
<b>Local RTP Port</b>	Configure Local RTP Port.
<b>Auto On-Hook Timer(s)</b>	Configure Auto On-Hook Timer(s).
<b>Ring Timeout</b>	Configure Ring Timeout.
<b>SIP Transport</b>	Select either UDP, TCP, or TLS/TCP as the SIP transport protocol.
<b>Direct IP Call</b>	Select either to disable or enable Direct IP Call support.
<b>SIP Proxy Compatibility Mode</b>	Select either to disable or enable SIP Proxy Compatibility Mode.
<b>Unregister On Reboot</b>	Select either to disable or enable Unregister On Reboot.
<b>Whitelist</b>	
<b>Whitelist</b>	Select either to enable or disable the Whitelist
<b>SIP Phone Number Whitelist</b>	Configure the SIP Phone Number Whitelist.

*Global Policy Parameters – Network Settings*

<b>Wallpaper</b>	
<b>Screen Resolution 1024 x 600</b>	<p>Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"><li>◦ <b>Source</b></li></ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"><li>◦ <b>File</b></li></ul> <p>If “URL” is selected as the source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as the source, click to upload the wallpaper file to the SoftwareUCM.</p>
<b>Screen Resolution 800 x 400</b>	<p>Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"><li>◦ <b>Source</b></li></ul> <p>Configure the location where wallpapers are stored.</p> <ul style="list-style-type: none"><li>◦ <b>File</b></li></ul> <p>If “URL” is selected as the source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as the source, click to upload the wallpaper file to the SoftwareUCM.</p>

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

Global Policy Parameters – Communication Settings

Email Settings	
<b>SMTP Settings</b>	<p>Check this option to configure the email settings that will be sent to the provisioned phones:</p> <ul style="list-style-type: none"><li>◦ <b>Server</b></li></ul> <p>The IP address of the SMTP server</p> <ul style="list-style-type: none"><li>◦ <b>Port</b></li></ul> <p>SMTP server port</p> <ul style="list-style-type: none"><li>◦ <b>From E-Mail address</b></li></ul> <p>Email address</p> <ul style="list-style-type: none"><li>◦ <b>Sender Username</b></li></ul> <p>Username of the sender</p> <ul style="list-style-type: none"><li>◦ <b>Password Recovery Email</b></li></ul> <p>Email where the recovered password will be sent</p> <ul style="list-style-type: none"><li>◦ <b>Alarm receive Email 1</b></li></ul> <p>Email address where alarm notifications will be sent</p> <ul style="list-style-type: none"><li>◦ <b>Alarm receive Email 2</b></li></ul> <p>Email address where alarm notifications will be sent</p> <ul style="list-style-type: none"><li>◦ <b>Enable SSL</b></li></ul> <p>Enable SSL protocol for SMTP</p>
<b>FTP</b>	



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

Global Policy Parameters – Communication Settings

Global Templates

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

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

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

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

Create New Template

o

Click on



to edit the global template.

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

Zero Config > Edit Global Templates: BranchOffice

• Template Name

BranchOffice

Description

Branch Office package

Active

☒

Options

Localization

Localization

Language Settings

• Language

English

Date and Time

Date Format

yyyy-mm-dd

Time Format

12-hour Clock

Enable NTP

Disabled

NTP Server



NTP Update Interval

1440


Cancel

Save

Edit Global Template

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

Click on “Save” to save this global template.

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

## Model Templates

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

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

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

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

Model	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
-------	--

<b>Template Name</b>	Create a name for the model template.
<b>Description</b>	Enter a description for the model template. This is optional.
<b>Default Model Template</b>	Select to assign this model template as the default model template. The value of the option in the default model template will be overridden if another selected model template has a different value for the same option.
<b>Active</b>	Check this option to enable the model template.

Create a New Model Template



o

Click on




to edit the model template.

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

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

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

Zero Config > Edit Model Templates: DP755



Model

GRANDSTREAM DP755

Template Name

DP755

Description

Default Model Template

☐

Active

☒

Options

Global Phonebook Settings

Custom Parameters

Custom Parameters

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

+ Add New Field

Contact List

Global Phonebook Settings

Global Phonebook Settings

Global Phonebook Type

XML

Cancel

Save

Edit Model Template

o Click on Save when done. The model template will be displayed on the Web GUI→**Device Management**→**Zero Config**→**Model Templates** page.

o Click on

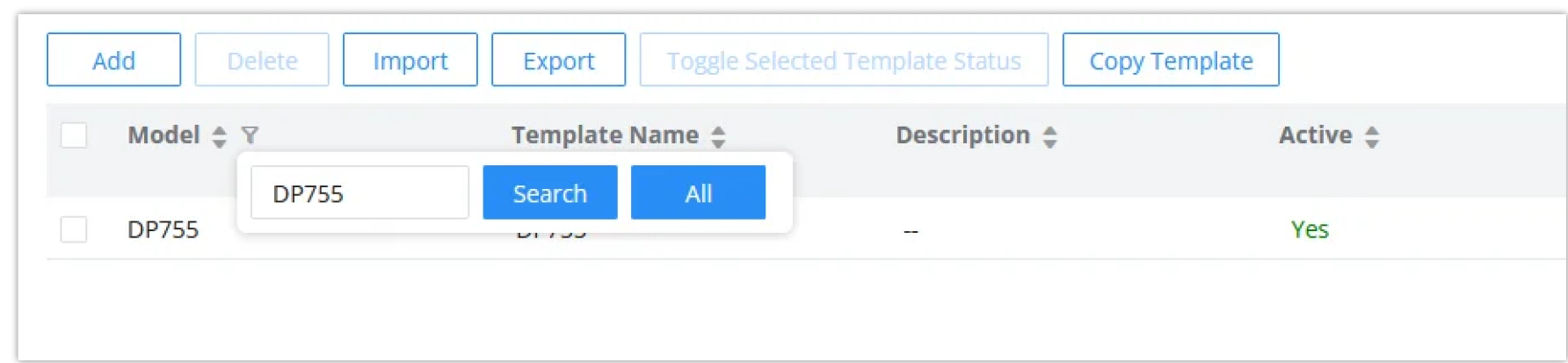


to delete the model template or click on “Delete Selected Templates” to delete multiple selected templates at once.

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

- Click on the “Import/Export” button to upload/export the model template list in .CSV format.

To make it easier for the administrator to search through the templates, a filter button has been added the user interface. Please see the screenshot below:



Filter Model Templates

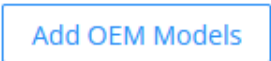
Model Update

Zero Config feature supports provisioning all models of Grandstream SIP end devices including OEM device models.

OEM Models

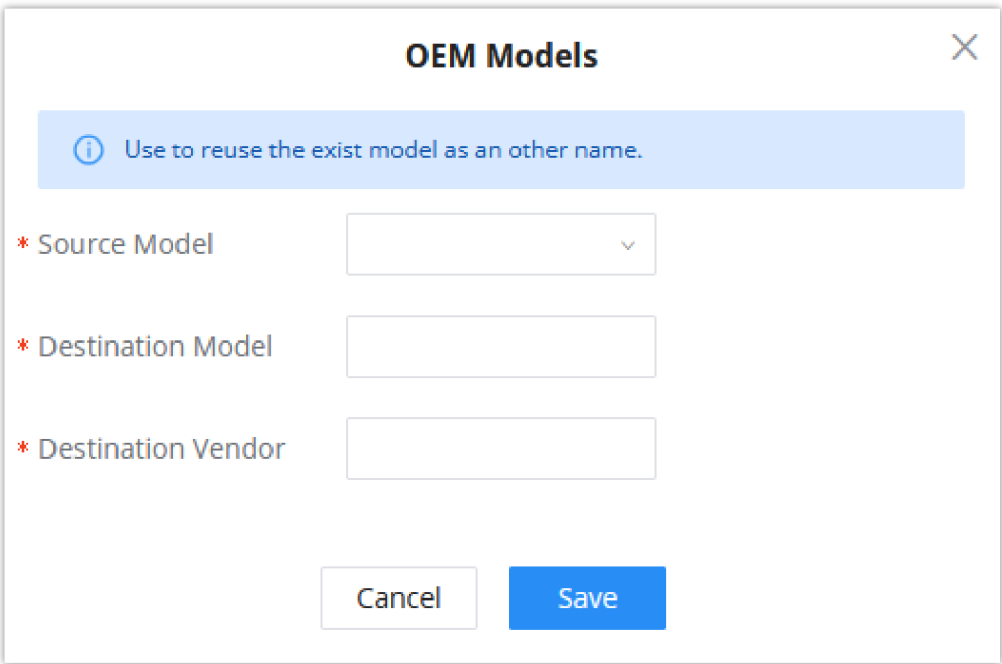
Users can associate OEM device models with their original Grandstream-branded models, allowing these OEM devices to be provisioned appropriately.

- Click on





















button.

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



OEM Models

To make it easier for the users to search for the model templates to download or update, a filter button has been added to the user interface.

Vendor	Model ▾	Version (Remote/Local)	Size	Options
Grandstream	GXV324		27K	 
Grandstream	GXV3275	2.2/2.1	28K	 
Grandstream	GXV3350	1.2/-	36K	 
Grandstream	GXV3370	1.7/-	55K	 
Grandstream	GXV3380	1.4/-	71K	 
Grandstream	GXV3450	1.0/-	94K	 
Grandstream	GXV3470	1.0/-	85K	 
Grandstream	GXV3480	1.0/-	77K	 
Grandstream	GXV3500	1.0/-	28K	 

Filter Endpoint Models

Model Template Package List

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

- Click on



to download the template.

- Click on



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

Model Template Package List				
VENDOR	MODEL	VERSION (REMOTE / LOCAL)	SIZE	OPTIONS
Grandstream	DP750	1.0/-	271K	
Grandstream	DP752	1.2/-	58K	
Grandstream	GAC2500	1.0/-	25K	
Grandstream	GD53705	1.3/-	56K	
Grandstream	GD53710	1.3/-	97K	
Grandstream	GRP2612	1.0/-	495K	
Grandstream	GRP2612P	1.0/-	495K	
Grandstream	GRP2612W	1.0/-	495K	
Grandstream	GRP2613	1.0/-	67K	
Grandstream	GRP2614	1.3/-	52K	

<

1

2

3

4

>

Total: 37

10 / page ▾

Template Management


Upload Model Template Package

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

Upload Model Template Package

Choose Model Package to Upload

Choose File to Upload



Device Configuration

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


Create New Device

Besides configuring the device after the device is discovered, users could also directly create a new device and configure basic settings before the device is discovered by the SoftwareUCM. Once the device is plugged in, it can then be discovered and provisioned. This gives the system administrator adequate time to set up each device beforehand.

Click on “Add” and the following dialog will show. Follow the steps below to create the configurations for the new device.

- 1. Firstly, select a model for the device to be created and enter its MAC address, IP address, and firmware version (optional) in the corresponding field.
- 2. Basic settings will show a list of settings based on the model selected in step 1. Users could assign extensions to accounts, and assign functions to Line Keys and Multiple-Purposed Keys if supported on the selected model.
- 3. Click on “save” to save the configuration for this device.

Zero Config > Edit Device: 000B82836614



\* Model

GRANDSTREAM GXP2160

\* MAC Address

000B82836614

IP Address

192.168.6.33

Version

1.0.11.85

Basic Settings

Advanced Settings

Accounts

☐

Hot Desking

No

☐

Account 1

1000

☐

Account 2

1000

☐

Account 3

1000

☐

Account 4

1000

☐

Account 5

1000

☐

Account 6

1000

Cancel

Update

Save

Create New Device

Manage Devices

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

Zero Config

Zero Config

Global Policy

Global Templates

Model Templates

Model Update

Firmware

Zero Config Settings

Total: 9

Registered: 0

Unregistered: 9

All

All Model

All Vendor

Model / Extension Number / MAC Address / IP Address

Auto Discover

Add

Delete



















Edit

Upgrade

Update Config

Reboot

More

No.	Model	Extension	Vendor	MAC Address	IP Address	Version	Create Config	Options
<input type="checkbox"/> 1	 GXP2160	--	GRANDSTREAM	000B82836614	<a href="#">192.168.6.33</a>	1.0.11.85	--	    
<input type="checkbox"/> 2	 DP750	--	GRANDSTREAM	000B8298E167	<a href="#">192.168.6.8</a>	1.0.21.19	--	    
<input type="checkbox"/> 3	 GRP2614	--	GRANDSTREAM	C074AD05D4FC	<a href="#">192.168.6.200</a>	1.0.11.23	--	    

Manage Devices n Zero Config

- Click on



to access the Web GUI of the phone.

- Click on



to edit the device configuration.

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

*Edit Device*

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

### 1. Global Policy

This is the lowest-level configuration. The global policy configured in Web GUI→**Device Management**→**Zero Config**→**Global Policy** will be applied here. Click on “Modify Global Policy” to redirect to the **Device Management**→**Zero Config**→**Global Policy**.

### 2. Global Templates





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

### 3. Default Model Template

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

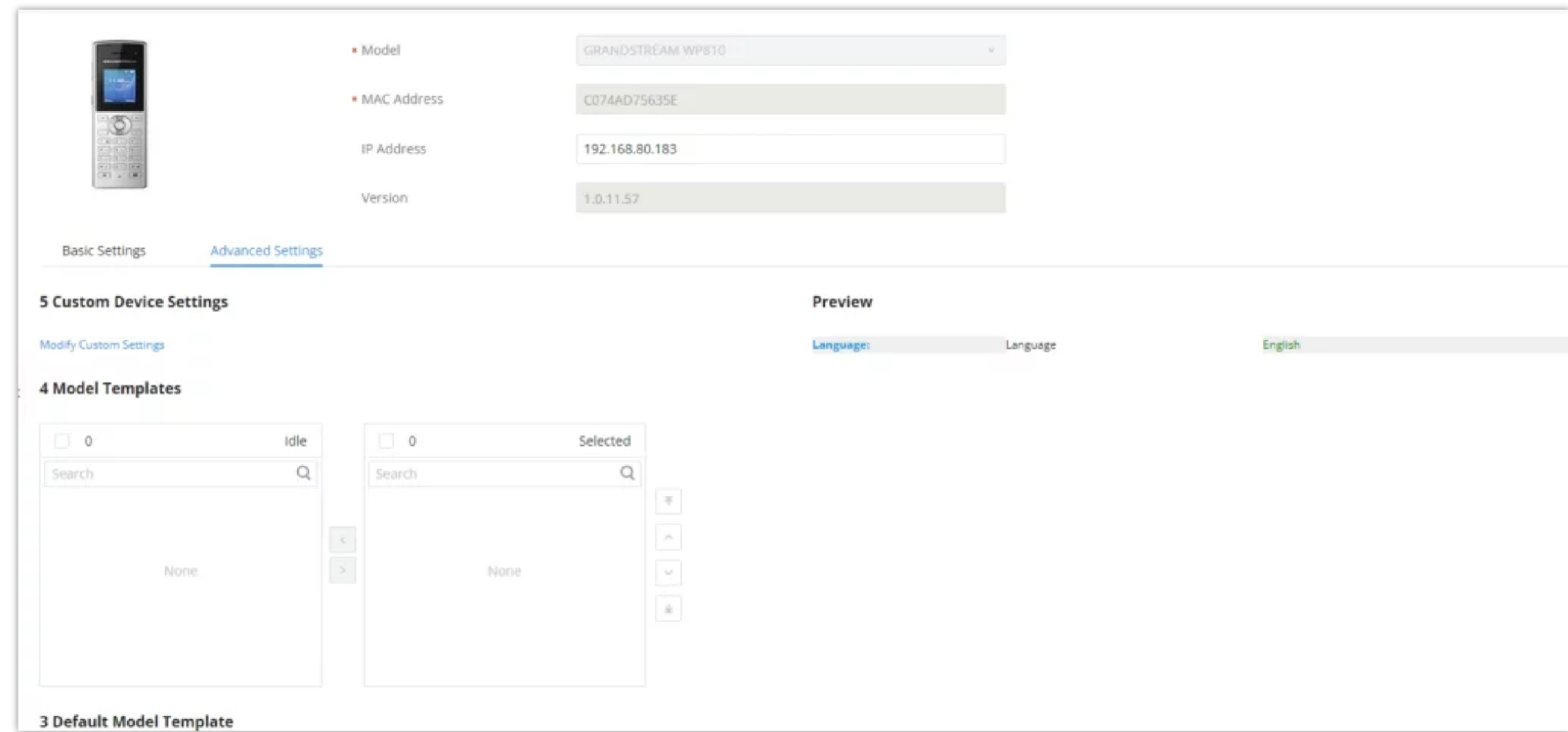
### 4. Model Templates



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

5. Customize Device Settings

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




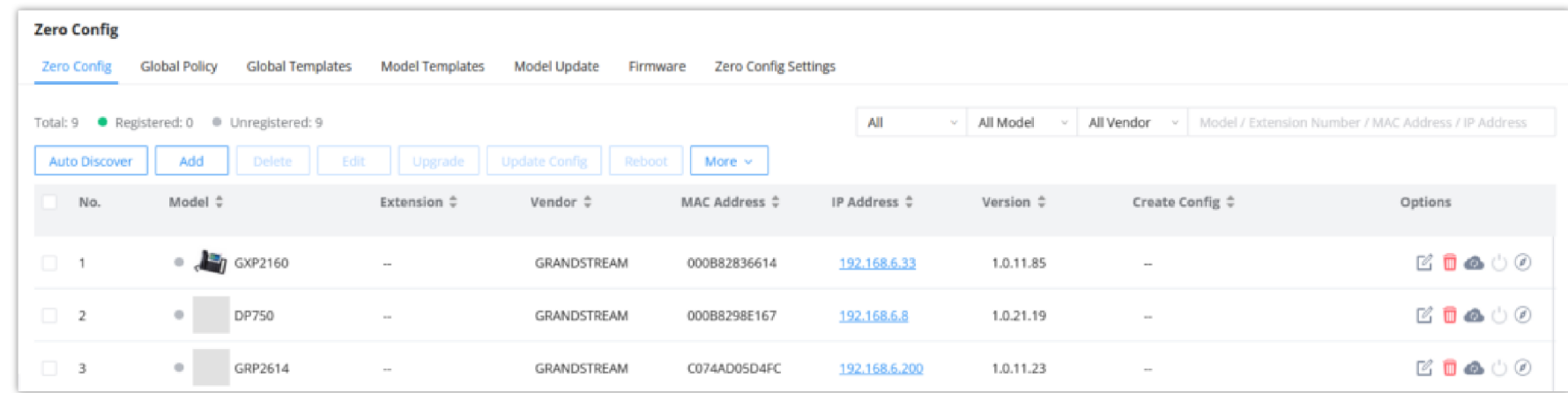
Edit Customize Device Settings

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

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

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

After the above configurations, save the changes and go back to the Web GUI→Device Management→Zero Config. Users could then click on  to send NOTIFY to the SIP endpoint device and trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.



Device List in Zero Config

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

# 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 SoftwareUCM 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

Extension Login Management

User Endpoint Access History

Add

Username	Privilege	Last Operation Time	Options
admin	Super Administrator	2024-11-28 16:41:52	<div><div></div><div></div></div>

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

\* Username

Privilege

Administrator

\* User Password

Email Address

Mobile Number

+1

Multi-Factor Authentication

☐

[Instructions](#)

[Email Settings](#)

Cancel



Save

Create New User

<b>Username</b>	Configure a username to identify the user which will be required in Web GUI login. Letters, digits, and underscore are allowed in the username.
<b>User Password</b>	Configure a password for this user which will be required in Web GUI login. English input is allowed without space,' and ".
<b>Email Address</b>	Configure the email address for the user. This is optional.
<b>Privilege</b>	This is the role of the Web GUI user. When super admin creates new user, "Adminstrator" or customized privilege can be selected.

<b>Multi-Factor Authentication</b>	If enabled, the user account will be required to enter an MFA code in addition to login credentials when logging into the UCM management web portal.
<b>Mobile Number</b>	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.

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.

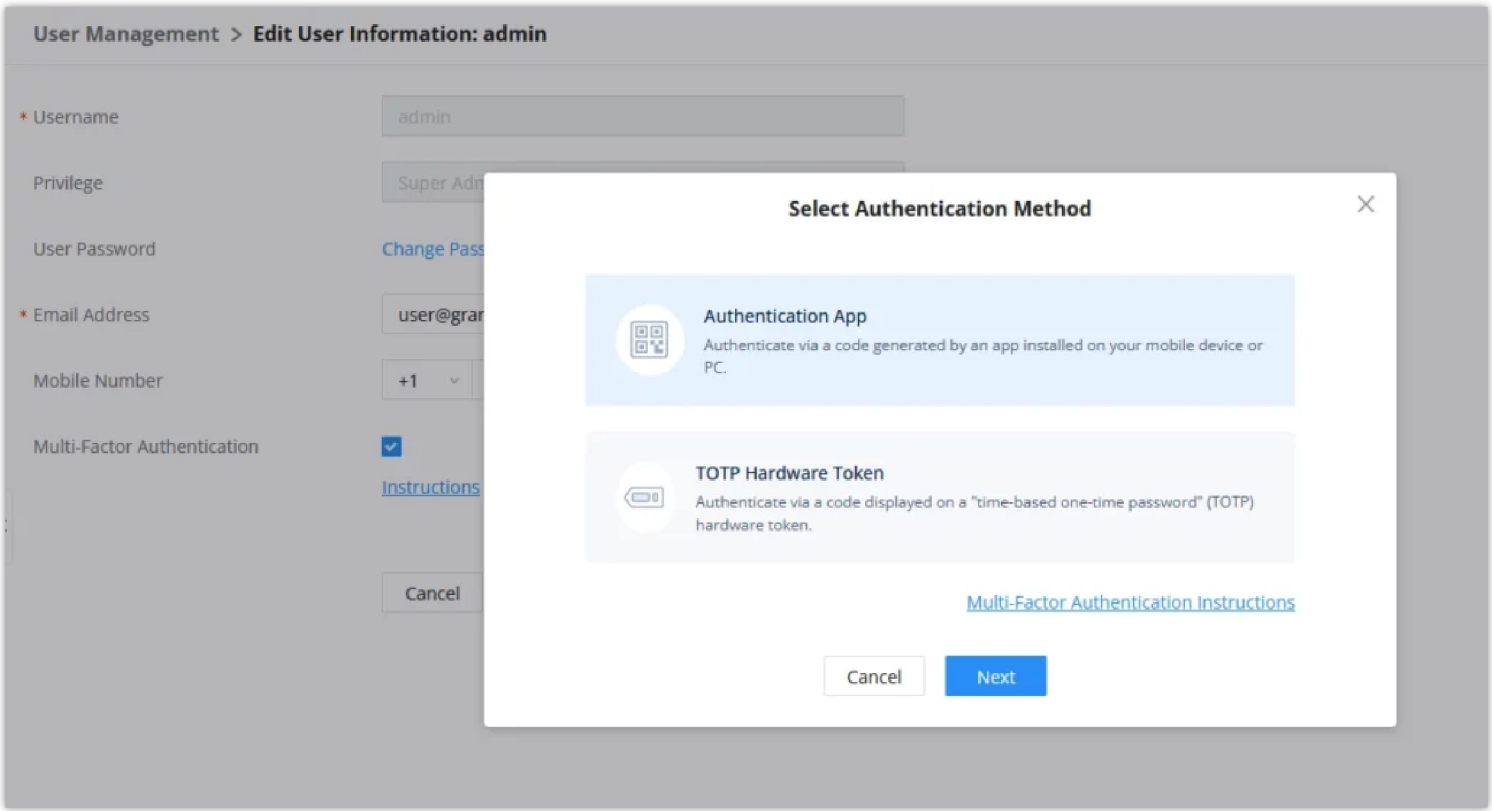
Once created, the Super Admin can edit the users by clicking on  or delete the user by clicking on .

Multi-factor Authentication

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

SoftwareUCM supports two 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 SoftwareUCM.
- **TOTP Hardware Token:** a hardware token that displays a time-sensitive one-time password to allow users to login to SoftwareUCM.



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

User Endpoint Access History

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 SoftwareUCM, 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 SFTP, NAS and Email Account passwords.

User Management > Edit Custom Privilege: Admin

\* Privilege Name

Admin

Password Visibility Toggle

☒ SFTP Password

☒ NAS Password

☒ Email Account Password

\* Custom Privilege

☐ 3 items

Available

Search

☐ Backup

☐ Upgrade

☐ RemoteConnect

<

>

☐ 0 item

Selected

Search

None

Cancel

Save

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

**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

☒ SFTP Password

☒ NAS Password

☒ Email Account Password

\* Custom Privilege

3 items

Available

Search

☐ Backup

☐ Upgrade

☐ RemoteConnect

<

>

0 item

Selected

Search

None

Cancel

Save

Assign Backup permission to "Admin" users

Wave Administrator

- This permission type does not support editing or deletion.
- This includes management of Wave-related function settings only and does not involve access to the UCM module.
- Users can set the Wave Admin privilege for specific extension under **Extension/Trunk → Extensions → Edit Extension**

For more information, please refer to the [Wave Administrator Guide](#) guide.

Extensions > Edit Extension: 1000

Basic Settings

Media

Features

Voicemail

Custom Time

Wave Client

Follow Me

Advanced Settings

AuthID

\* Concurrent Registrations

3

Disable This Extension

☐

User Settings

First Name

Last Name

Email Address

\* User/Wave Password

\*\*\*\*\*

\* User Portal/Wave Privileges

Wave Administrator

Mobile Number

+1

Department

Enterprise Root Directory

Job Title

Contact Privileges

Same as Department Contact Privileges

☒

\* Contact View Privileges

All Contacts

Sync Contact

☒

Cancel

Save

User Portal/Wave Privilege

Add Custom Privilege

User Management

User Information







Custom Privilege

User Portal/Wave Privileges

Extension Login Management

User Endpoint Access History

Add

Privilege Name	Privilege Type	Options
Super_Admin	Super Administrator	 
Admin	Administrator	 
Wave_Admin	Wave Administrator	 

Add New Custom Privilege

The Super Admin user can create users with different privileges. 41 items are available for privilege customization.

API Configuration	Backup	Callback	Call Queue	Queue Statistics
Queue Recordings	CDR Recordings	CDR Records	CDR Statistics	Dial By Name
DISA	Emergency Calls	Event List	Extensions	Extension Groups
Outbound Routes	Inbound Routes	Fax/T.38	Fax Sending	Feature Codes
IVR	Paging/Intercom	Parking Lot	Pickup Groups	PMS – Wakeup Service
Ring Groups	Restrict Calls	SCA	Speed Dial	System Status
System Events	LDAP Server	Time Settings	Multimedia Meeting	Voicemail
Voice Prompt	Schedule Call	Contacts	Zero Config	Announcement
RemoteConnect				

Log into SoftwareUCM as super admin and go to **Maintenance > User Management > Custom Privilege**, create privilege with customized available modules.

When you add CDR Records and CDR Recording Files custom privileges, additional privileges will appear (All Deletion of CDR and Allow Deletion of DCR Recordings, respectively). This offers more flexibility on the privileges that the admin assigns to the user.

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 SoftwareUCM. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on "Apply Changes"), a prompt will pop up as shown in the following figure.

Operating too frequently or other users are doing the same operation. Please retry after 15 seconds.

### 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 user can create customize privileges related to an extension's User Portal and Wave. The created privilege can be affected to the extensions to limit or allow them to use certain functionalities related to Wave and the User Portal.



User Management > Edit User Portal/Wave Privileges: Default

Wave Permissions ?

▼ ☒ Chat ?

☒ Delete Chat ?

☒ Send File ?

☒ Download Chat Logs ?

☒ End-to-End Encrypted Chat ?

☒ Video Call ?

▼ ☒ Meeting ?

☒ Start Video During Meeting ?

☒ Online Status ?

☒ Remote Logout ?

☒ Clear Recent Call History ?

Cancel

Save

User Portal/Wave Privileges

Wave Permissions

- **Chat:** Toggles ability to use the Wave Chat feature.
  - **Delete Chat:** Toggles support for Wave to delete chats and chat history. This data will only be deleted on the Wave client side.
  - **Send File:** Toggles file/image sending support in Wave chat. If disabled, users will still be able to download, view and forward chat files.
  - **Download Chat Logs:** If enabled, chat logs will be downloadable from the Wave client, including chat logs from Wave/WhatsApp/Telegram/LiveChat sessions.
- **End-to-End Encrypted Chat\*:** Toggles ability to use the Wave End-to-End Encrypted Chat feature.
- **Video Call:** Toggles ability to use the Wave Video Call feature.
- **Meeting:** Toggles ability to use the Wave Meeting feature.
  - **Start Video During Meeting:** Toggles ability to use the Wave Start During Meeting feature.
- **Online Status:** Toggles ability to set Wave online status such as "Busy", "Appear Away", "Do Not Disturb", "Appear Offline", etc. If unchecked, the status will be displayed as only either "Online" or "Idle".
- **Remote Logout:** If enabled, Wave users will be able to log out of their accounts from other logged-in devices.
- **Clear Recent Call History:** Toggles ability to delete recent call history entries and entire recent call history on Wave.
- **Application:** Toggles ability to access the "Applications" page under Wave Desktop and Wave Web.
- **Smart Devices:** Toggling off privileges will hide the corresponding pages and options in Wave.
  - **Door System**
  - **Monitor**
  - **Call Device (CTI)**
- **3rd Party Applications**
  - **App Store:** Toggles ability to access the Wave App Store. If unchecked, the App Store will be hidden, but installed apps can still be used.
  - **Pre-installed Apps\*:** Configure Wave pre-installed add-ins and related settings.

User Portal/Wave Privileges

- **Account Settings:** If unchecked, the *User Portal -> Basic Information -> Account Settings* page and the *Wave -> Sidebar -> User -> Account Settings* option will be hidden.
- **Extension Settings:** If unchecked, the extension’s *User Portal->Basic Information->Extensions* page and the *Wave->Sidebar->User->Call Settings* option will be hidden.
  - **Do Not Disturb:** Toggles ability to set DND through the User Portal.
  - **SIP/IAX Password & AuthID:** Toggles ability to access the **SIP/IAX Password** and **AuthID** settings under the *User Portal->Basic Information->Extensions->Basic Settings* page.
  - **Configuration Voicemail**
- **Manage Recordings:** Toggles ability to view recordings through the User Portal and Wave, including the recordings in call logs, meeting details, and Wave application.
  - **Deleting Recordings:** Toggles ability to delete recordings through the User Portal and Wave. For Wave, this includes the ability to delete call logs, meeting details,and recordings.
- **Personal Data:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - CDR
  - Follow Me
  - Voicemail
  - Recordings files
  - Fax Files
  - SCA
- **Other Features:** Toggling off privileges will hide the corresponding pages and options in the User Portal and Wave.
  - Fax Sending
  - Call Queue
  - Schedule Call

\*: Requires a paid RemoteConnect plan.

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	Extension Login Management	<u>User Endpoint Access History</u>	
Extensions ↕	Name ↕	Extension Type ↕		Endpoint Type	Last Operation Time
1000		SIP(WebRTC)			
1001		SIP(WebRTC)			
1002		SIP(WebRTC)			
1003		SIP(WebRTC)			
1004		SIP(WebRTC)			

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 SoftwareUCM 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

s.adler@gmail.com

Email Template

Change Phone Number

Mobile Number

+1

▼

SMS Template

Enter Current Password

\* Enter Current Password

Change Password

Enter Old Password	Enter the Old Password for SoftwareUCM
Change Password	Enable Change Password
Enter New Password	Enter the New Password for SoftwareUCM
Re-enter New Password	Retype the New Password for SoftwareUCM
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

SoftwareUCM allows users to change Super Administrator username.

Change Username

Change Username☒

\* Username

GSadmin

Change Email Address

SoftwareUCM allows user to configure binding email in case login password is lost. SoftwareUCM 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 Email Address

\* Email Address

admin@grandstream.com

Email Template

Change Binding Email


Email Address	Email Address is used to retrieve password when password is lost
---------------	--

Change Binding Email option

Login Security

After the user logs in the SoftwareUCM 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 SoftwareUCM 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 SoftwareUCM 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

Login Settings

\* Login Timeout (m)

0

0 indicates no automatic logout.

SMS OTP Login

☐

Login Security Policy

Enable Login Security

☒

\* Max Login Attempts (IP)

50

\* Maximum number of login attempts

5

\* Ban Period (m)

5

0 indicates a permanent ban after exceeding the max number of failed login attempts.

Login Banned IP/User List

Banned

Ban History

Q Please enter ip address / userna...

Q

IP Address	Username	Banned Time	Estimated Ban Lift Time	Options
<div><div></div></div>				

Cancel

Save

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".

\* Maximum number of login attempts

\* Ban Period (m)

0 indicates a permanent ban after exceeding the max number of failed login attempts.

Login Banned IP/User List

BannedBan History

Please enter ip address / userna...

Delete

<input type="checkbox"/>	IP Address ▴▾	Username ▴▾	Banned Time ▴▾	Ban Lift Time ▴▾	Options
<input type="checkbox"/>	192.168.5.113	admin	2024-11-28 17:23:56	2024-11-28 17:28:56	

Total: 1<1>10 / page ▾Goto

### SoftwareUCM History of Banned IP Addresses

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. <b>Note:</b> 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. <b>Note:</b> The verification code error is not accumulated when the login fails

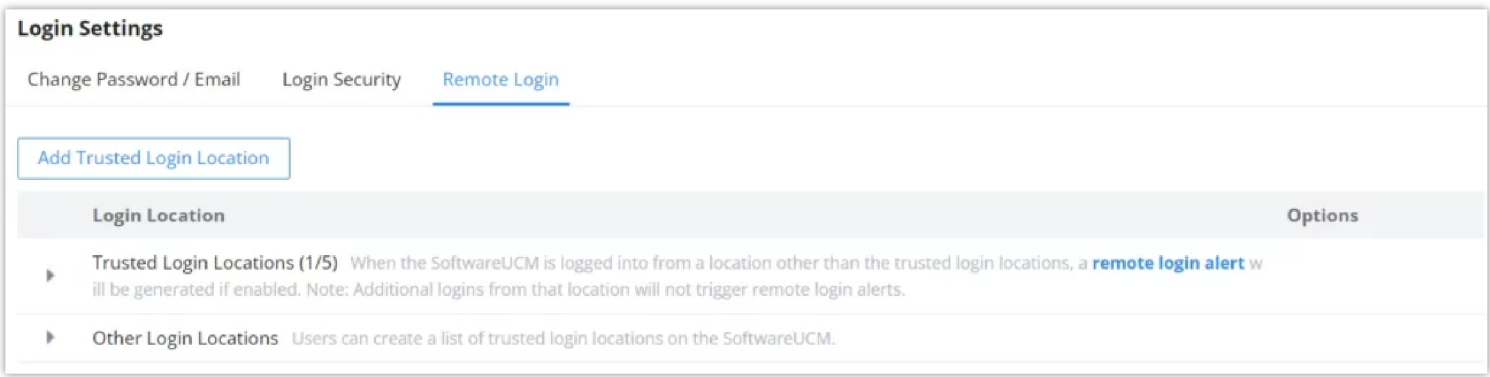
Login Whitelist	List of IP addresses that can make unlimited login attempts, users can define the whitelisted IP Address.
-----------------	---

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 SoftwareUCM 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 enhacing the security of the UCM.

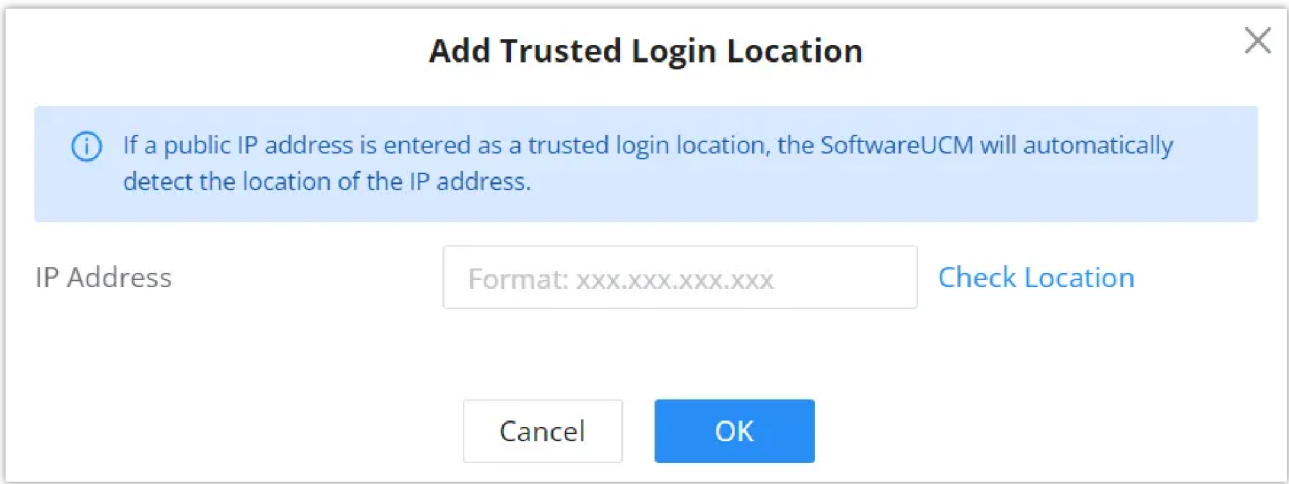
In this tab there are two types of lists of locations:

- 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](#)



add a trusted login location

Then add the public IP address of the location, click on “**Check Location**” to verify if it’s the correct location then click “**OK**”.

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 SoftwareUCM 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”.



Operation Log

Display Filter

Delete Search Result(s)ClearDownload Search Result(s)Download All Log

Date	Username	IP Address	Results	Page Operation	Specific Operation	Remark
2025-01-13 15:30:18	Abdelwahab	192.168.5.248	Operation successful	Apply Changes		<a href="#">Click to modify notes</a>
2025-01-13 15:27:40	Abdelwahab	192.168.5.248 (Tangier, Tanger-Tetouan-Al Hoceim, MA)	Operation successful	Extensions: Login	Username: Abdelwahab.	<a href="#">Click to modify notes</a>
2025-01-13 15:25:39	Abdelwahab	192.168.5.248	Operation successful	deleteMessageCenterNotify	delete_id: all.	<a href="#">Click to modify notes</a>
2025-01-13 15:03:40	admin	192.168.5.247 (Tangier, Tanger-Tetouan-Al Hoceim, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2025-01-13 13:10:34	Abdelwahab	192.168.5.248 (Tangier, Tanger-Tetouan-Al Hoceim, MA)	Operation successful	Extensions: Login	Username: Abdelwahab.	<a href="#">Click to modify notes</a>
2025-01-13 12:29:05	admin	192.168.5.90	Operation successful	Apply Changes		<a href="#">Click to modify notes</a>
2025-01-13 12:29:04	admin	192.168.5.90	Operation successful	Multimedia Meeting: addMultimediaConferenceReservation	Details	<a href="#">Click to modify notes</a>
2025-01-13 12:15:00	admin	192.168.5.90 (Tangier, Tanger-Tetouan-Al Hoceim, MA)	Operation successful	Extensions: Login	Username: admin.	<a href="#">Click to modify notes</a>
2025-01-13 12:14:55	Illas	192.168.5.90	Operation successful	Log out: Log out	Username: Illas.	<a href="#">Click to modify notes</a>
2025-01-13 11:57:45	Illas	192.168.5.90	Operation successful	Apply Changes		<a href="#">Click to modify notes</a>

Total: 51

123456

10 / pageGoto

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 peformed the opertation
IP Address	The IP address and geographical location from which the operation has been made.
Results	The result of the operation.
Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
Specific Operation	Click on the hyperlinked operation detail to reveal more details.
Remark	Allows users to add notes and remarks to each operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on “Display Filter”.

Operation Log

Hide Filter

Start Time

2025-01-0100:00

End Time

2025-01-1315:41

IPv4 Address

Username

admin

Filter

Reset

Delete Search Result(s)ClearDownload Search Result(s)Download All Log

Date	Username	IP Address	Results	Page Operation	Specific Operation	Remark
------	----------	------------	---------	----------------	--------------------	--------

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 

Delete Search Result (s)

 to delete the filtered result of operation logs. Or users can click on 

Clear

 to delete all operation logs at once.

### Syslog

On the SoftwareUCM, 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.

*Syslog*

Some typical modules for SoftwareUCM functions are as follows and users can turn on "NOTICE" and "VERBOSE" levels besides "error" level.

- 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.
- SoftwareUCM retains syslog logs for up to 30 days to automatically manage log storage and prevent running out of space. This extended local retention allows for troubleshooting and auditing even when a remote syslog server is unavailable.

## System Events

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

## Alert Log

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

System Events

Alert Log

Alert Events List

Alert Contact

Delete Search Result(s)

Clear

Display Filter

Time	Event Name	Type	Content
2025-01-10 15:44:36	SoftwareUCM plan	Generate Alert	The license has been updated and is valid until 2025-02-10 00:59. Please be mindful of the plan specifications (e.g., extension limits, agent limits, etc.) to avoid disrupting business operations.

System Events→Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on 

Filter

. Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.

2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

User could filter out alert logs of “Generate Alert” or “Restore to Normal” by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of “Restore to Normal”.

Start Time

2025-01-01

00:00

End Time

2025-01-13

15:45

Event Name

All

Type

All

Reset

Filter

Filter for Alert Log

Alert Events List

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

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.

Alert On

Alert Off

Email Notification On

Email Notification Off

HTTP Notification On

HTTP Notification Off

SMS Notification On


SMS Notification Off

Event Name	Alert	Alert Contact			Options
<div>SoftwareUCM plan</div>	<div>ON</div>	Email <div>ON</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>Fail2ban Blocking</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>Flood Attacks</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>Network Traffic Storm</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>User Login Banned</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>Remote Login</div>	<div></div>	Email <div></div>	SMS <div></div>	HTTP <div></div>	<div></div>
<div>User Login Success</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>User Login Failed</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>System Crash</div>	<div>ON</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>Restore Config</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>System Update</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>System Reboot</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>
<div>CPU Usage Call Control</div>	<div>OFF</div>	Email <div>OFF</div>	SMS <div>OFF</div>	HTTP <div>OFF</div>	<div></div>

Alert Event List

Alert Events
SoftwareUCM Plan
Fail2ban Blocking

User Login Banned
Remote Login
User Login Success
User Login Failed
Restore Config
System Update
System Reboot
Modify Super Admin Password
Data Sync Backup
Local Disk Usage
Emergency Calls
SIP Outgoing Call through Trunk Failure
SIP Internal Call Failure
Excessive Outbound Calls
Outbound Call Duration
Trunk Outbound Call Duration Usage
Trunk Concurrent Calls
Register SIP trunk failed
SIP Peer Trunk Status
Register SIP failed
SIP Lost Registration

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

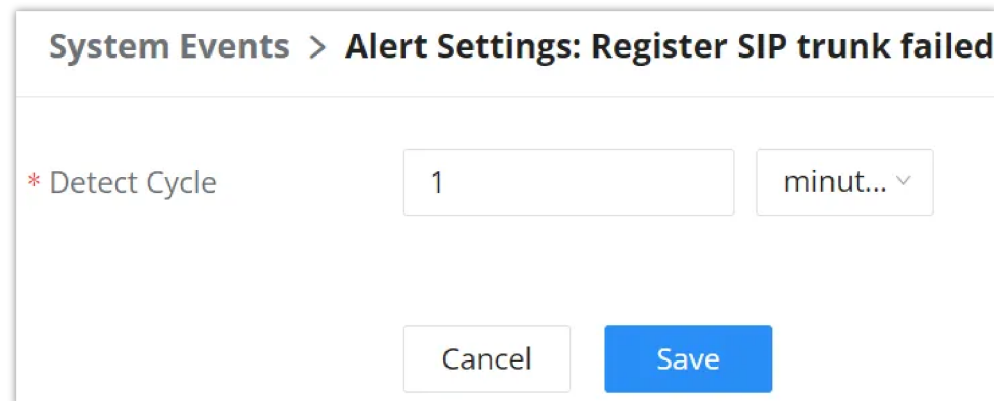
- 1. **Fail2ban blocking:** If the system Fail2ban is blocking, the event will be recorded in the alert log.
- 2. **User login banned:** If user login is blocked, the event will be recorded in the alert log.
- 3. **Remote Login:** An alert will be generated upon a remote login.
- 4. **System Update**
- 5. **Restore Config:** Once the system configuration is restored, the configuration restoration event will be recorded in the alert log.
- 6. **System Update:** Once the system is upgraded, the system upgrade event will be recorded in the alarm log.
- 7. **System Reboot:** UCM will detect the system restart and will send an alert for it. There are two kinds of reboots that the UCM detects, normal and abnormal reboots. Normal reboots are the reboots that are done when you press the restart button on the web UI, reboot that occur after updating the firmware. Abnormal reboots are the reboots that occur due to

a system failure. Normal reboots are registered in the alert log and they are not pushed to GDMS, while abnormal reboots are registered in the alert list and are pushed to GDMS. The alert includes the reason of the reboot.

8. **Modify Super Admin Password:** Once the super administrator password is modified, the system will record the password modification event in the alarm log.

9. **Emergency Calls:** If the system generates an emergency call, the event will be recorded in the alert log.

10. **Register SIP trunk failed**



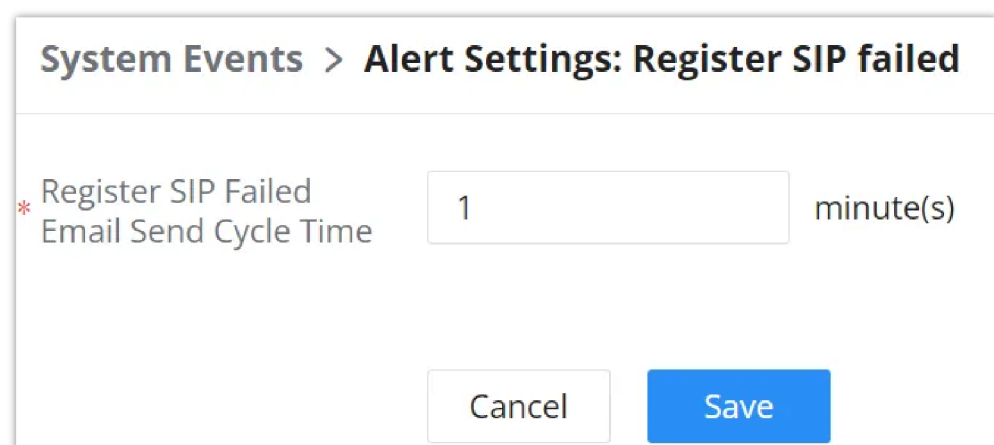
*System Events → Alert Events Lists: Register SIP Trunk Failed*

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

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

14. **SIP Outgoing Call through Trunk Failure:** If the system SIP trunk outgoing call fails, the event will be recorded in the alert log.

15. **Register SIP failed**



*System Events → Alert Events Lists: Register SIP Failed*

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

16. **SIP lost registration:** If System SIP extension registration is lost, 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.

17. **High Frequency Outgoing Call:** When an extension initiates calls frequently, an alert will be logged in the alert log and a notification will be pushed to the GDMS and through email as well.

18. **Remote concurrent calls:** If the remote concurrent call fails, the event will be recorded in the alert log.

19. **Trunk Outbound Call Duration Usage:**

20. **Trunk Concurrent Calls:** When the system detects that the number of concurrent calls of a certain relay exceeds the threshold set by the relay within a certain period of time, the event will be recorded in the alarm log. Calls are not restricted if the threshold is exceeded.

21. **User login success:** Successful user login events will be recorded in the alert log.

22. **User login failed:** User login failure events will be recorded in the alert log.

23. **Data Sync Backup:** If the system performs data synchronization and backup abnormalities, the event will be recorded in the alert log.

## Alert Contact

This feature enables users to receive notifications when the configured alert events occur. Users can add up to 10 email addresses and phone numbers under **Maintenance > System Events > Alert Contacts** to receive these alert notifications.

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.

Email

arthur.morgan@grandstream.com

Add Email

Email Template

Email Template

SMS Notification

Mobile Number

+1

Add Mobile Number

SMS Template

SMS Template

HTTP Notification

Protocol

HTTP

HTTP Server

127.0.0.1

Cancel

Save

Alert Contact

Email Notification	
Email Notification	<div>Alert email notification delivery method:</div> <ul style="list-style-type: none"><li><b>Real-time:</b> Notifications will be sent out as soon as the alerts are generated.</li><li><b>Periodic:</b> Alerts generated within the configured “Notification Interval” time window will be queued up and sent all at once in a single notification.</li></ul>
Notification Interval	<div>When the notification delivery method chosen is <b>Periodic</b>, this option will be available.</div> <div>The sending frequency of alert email notifications. All alert events that have occurred within a send cycle will be sent.</div>
Super Admin Email	<div>Configure the email addresses to send alert notifications to.</div> <div>Up to 10 email addresses can be added.</div>
Admin Email	<div>Configure the email addresses to send alert notifications to.</div> <div>Up to 10 email addresses can be added.</div>
Email Template	<div>Please refer to section <a href="#">Email Templates</a></div>
SMS Notification	







- Scheduled Data Sync
- Scheduled Cleaner (CDR, Reports, IM Data, Files)

Task List

The user can schedule a task in this section to be performed once. The user can schedule 4 possible tasks, Scheduled Paging/Intercom, Scheduled Backup, Scheduled Data Sync, and Scheduled Cleaner.

To schedule a task, please navigate to **Maintenance→Task Management→Task List→Pending Task**, then click on button



Task Management

Task List

Task Schedule

Pending Task

Historical Task

Add

Name

Name	Type	Start Time
------	------	------------

Create New Task

Then select the type of the task from the drop-down menu.

Create New Task

\* Type

Scheduled Paging/Intercom

Cancel

Next

Task Type

Click "Next" and the set the needed parameters accordingly.

Task Management

Task List

Task Schedule

Pending Task

Task History

Add

Name

Time: Start Time to End Time

Search

Reset

Name	Type	Start Time	Repeat	Options
Schedule Cleaning	Scheduled Cleaner (IM Data)	2024-10-10 00:00	Per 30 Days 00:00	

Total: 1

< 1 >

10 / page

Goto

Pending Tasks

The user can check the log of the tasks which have been performed in "Task History"

## Task Management

## Task List

## Task Schedule

### Pending Task

## Task History

Clear

Name

▼

Time: 


2024-09-01

to

2024-09-10

Search

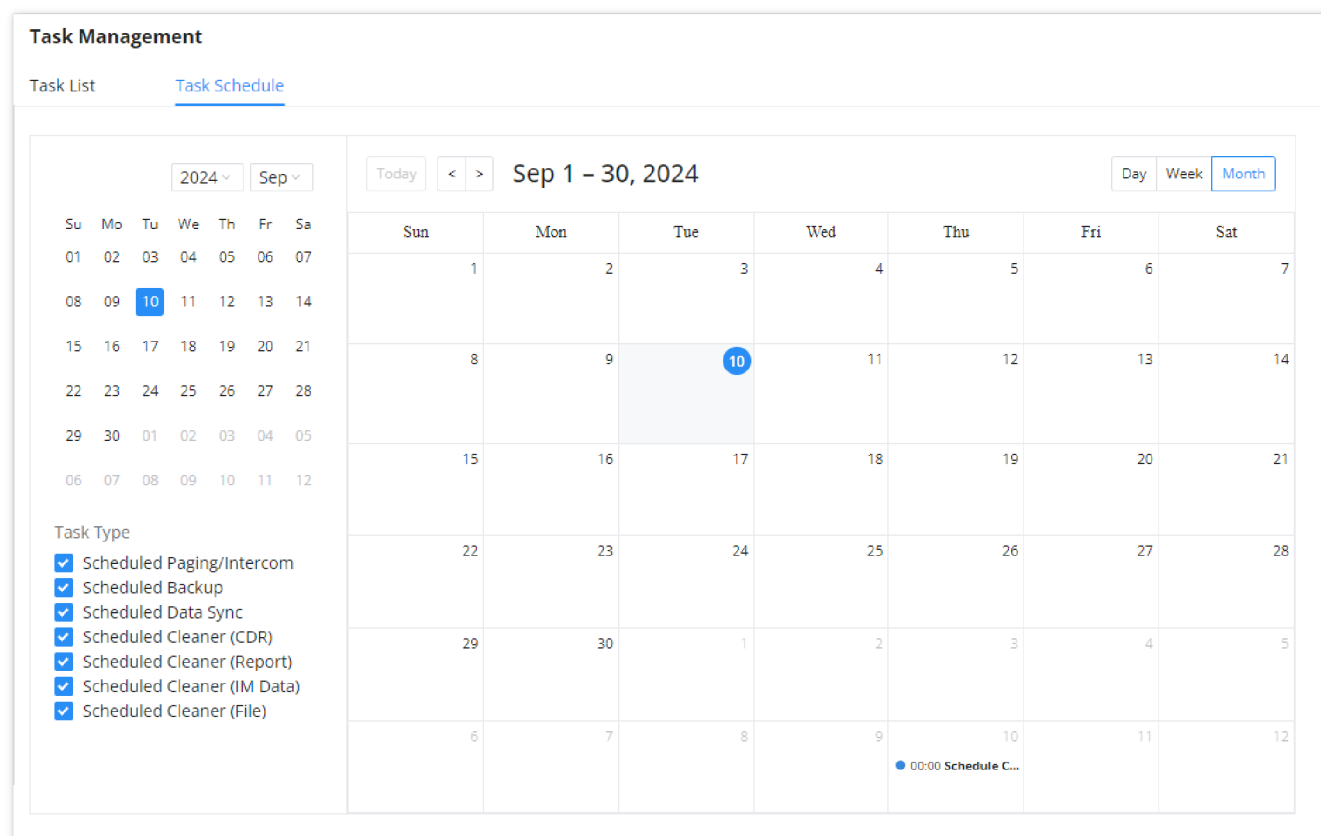
Reset

Name	Type	Action Status	Start Time	Repeat	Options
<div><div><div>No data</div></div></div>					

### 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

The SoftwareUCM receives regular updates. These updates include new features and functionalities, bug fixes, security patches, and general improvements to the security and performance of the device. It is highly recommended that you keep the firmware of your UCM up to date.

Before proceeding with the firmware upgrade, please visit <https://www.grandstream.com/support/firmware> and download the latest firmware available for the UCM. Once the file has been download, please decompress the file, you will get a .bin file, that's the file which will uploaded to the UCM.

To upgrade the firmware of the SoftwareUCM, please access the web UI of the UCM, then navigate to **Maintenance** → **Upgrade**

Upgrade Firmware

It is recommended to back up your current configuration and data before upgrading. [Click here to back up](#)

After downgrading, please factory reset the device to minimize risk of potential issues. It is highly recommended to create and keep backups of earlier firmware versions to restore in these scenarios.

System Firmware (.bin)

Choose File to Upload

Wave Web Firmware (.tgz)

Choose File to Upload

Upgrade

Important

It is highly recommended to back up the data and the configuration before upgrading the software of the SoftwareUCM.

License Management

In this page, the user can view various information regarding the SoftwareUCM license such as the plan type, the date of the activation as well as the date of expiration, the address MAC of the device, the supported number of extensions and maximum concurrent calls.

License Management

License Status

Activated

Update Time

2024-11-22 10:47:26

License

Upload

Plan Name: Demo-Plan

Expiration Date: Valid until 2024-12-22

Device MAC Address: C6:10:01:00:00:02

Extensions: 100

Max Concurrent Calls: 20

Renewal/Upgrade

License Management

Backup

Backup/Restore

Users could backup the SoftwareUCM configurations for restore purpose under Web GUI→Maintenance→Backup→Backup/Restore.

Backup

Backup/Restore

Data Sync

Backup file must be in .tar format and less than 30MB in size. File name can contain alphanumeric characters, dashes (-) and underscores (\_).

Backup

Schedule Backup

Upload

Local Backups

Delete

<input type="checkbox"/>	Name	Date	Size	Options
<input type="checkbox"/>	backup_20241128_180634.tar	2024-11-28 18:06:49 UTC+01:00	15.45 MB	<div><div></div><div></div><div></div></div>

Total: 1

<1>

10 / page

Goto

Task History

Name	Action Status	Start Time	Repeat	Options
<div><div></div><div>No data</div></div>				

Backup/Restore

Click on "Backup" to create a new backup file. Then the following dialog will show.

Backup > Create New Backup

\* File Name

backup\_20240221\_124258

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

☐ Meeting Report




Warning: Backups may take a considerable amount of time if backing up large amounts of data. Selecting "Voicemail" will also back up assigned name announcements.


Cancel

Backup

Create New Backup

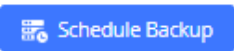
- Choose the type(s) of files to be included in the backup.
- Name the backup file.
- Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download , restore , or delete  it from the SoftwareUCM internal storage or the external device.

Click on  Upload to upload backup file from the local device to SoftwareUCM. The uploaded backup file will also be displayed in the web page and can be used to restore the SoftwareUCM.

Important

In case the back up is restored into a different SoftwareUCM, please ensure that the number of supported extensions and concurrent calls is taken into consideration.

The  option allows UCM to perform automatically backup on the user specified time. User is allowed to set backup time from 0-23 and how frequent the backup will be performed.

Backup > Schedule Backup

Enable Scheduled Backup

☒

\* Backup Time

00:00

\* Backup Frequency

1

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

☐ Meeting Report

Warning: Selecting "Voicemail" will also back up name announcements.

Cancel

Save

Local Backup

### Data Sync

Besides local backup, users could backup the voice records/voice mails/CDR in a daily basis to a remote server via SFTP protocol automatically under Web GUI→Maintenance→Backup→Data Sync.

The client account supports special characters such as @ or "." Allowing the use email address as SFTP accounts. It allows users as well to specify the destination directory on SFTP server for backup file. If the directory does not exist on the destination, SoftwareUCM will create the directory automatically.

Backup

Backup/Restore   Data Sync

- ❗ Use SFTP to automatically sync CDR Records, Recording Files, Voicemail, and Fax every day.
- ❗ SFTP server can be configured in the PBX Settings->Storage Device Management -> SFTP page.

Enable Data Sync

☐

Choose Data Sync Files

☒ CDR Records

☒ Recording Files

☒ Voicemail

☒ Fax

Account

Password

Server Address

Destination Directory

Sync Time

Sync All Data

Task History

Name	Action Status	Start Time	Repeat	Options

Cancel

Save

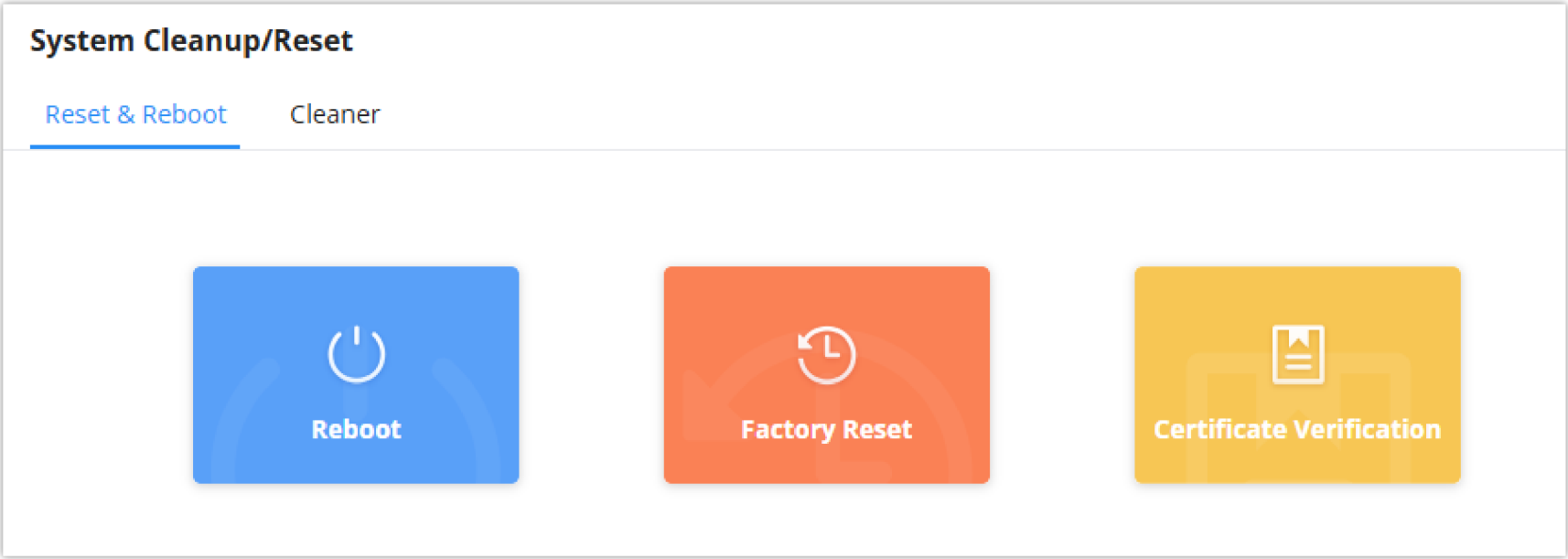
Data Sync

Enable Data Sync	Enable Data Sync by ticking the box. <b>Note:</b> The default setting is disabled.
Choose Data Sync Files	Choose the type of data to sync. <ul style="list-style-type: none"><li>CDR Records</li><li>Recording Files</li><li>Voicemail</li><li>Fax</li></ul>
Account	Enter the account username. <b>Note:</b> This field is mandatory.
Password	Enter the password if set on the SFTP server configuration. <b>Note:</b> This field is optional.
Server Address	Enter the SFTP server address. <b>Note:</b> This field is mandatory.
Destination Directory	Enter ther destination filepath with the folder name. Format: 'xxx/yyy/zzz'. If the directory does not exist, the UCM will create it automatically.
Sync Time	Enter 0-23 to specify the backup hour of the day.

## System Cleanup/Reset

### Reset and Reboot

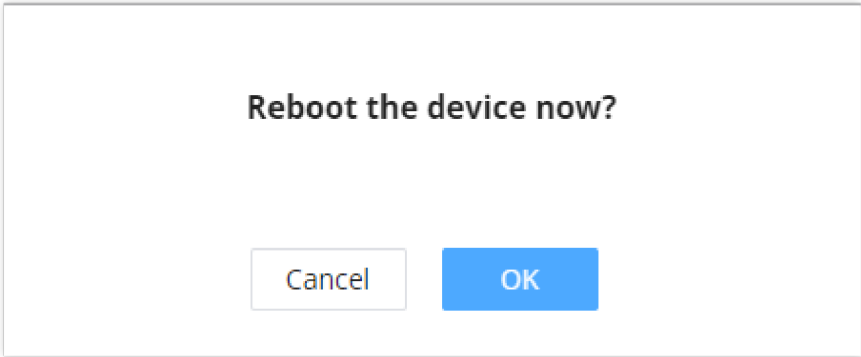
Users could perform reset and reboot under Web GUI→Maintenance→System Cleanup/Reset→Reset and Reboot.



Reset and Reboot

### Reboot

When the user clicks on reboot, a confirmation prompt will appear. To proceed with rebooting the device, please click “OK”.

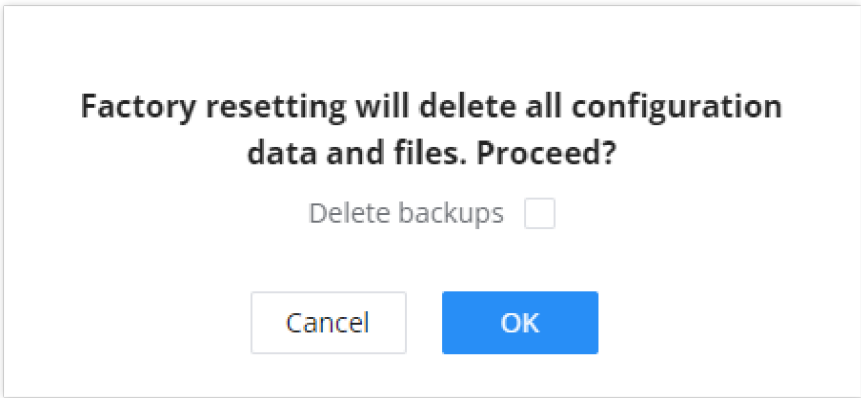


Reboot Confirmation Prompt

### Reset

Reset function will delete all the configuration and data store in the SoftwareUCM 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.



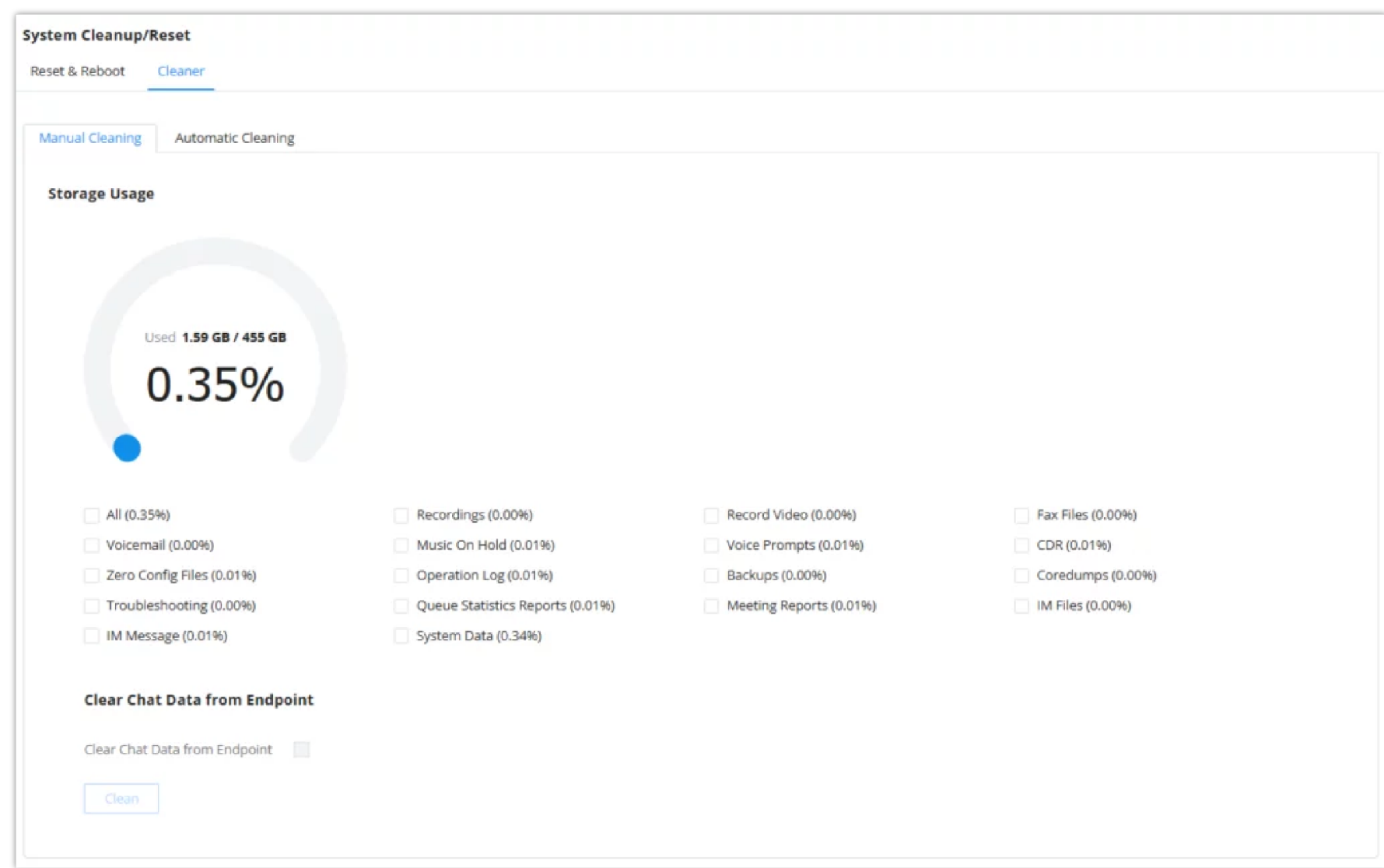
- Ticking the option “Delete Backups” will result in deleting all the backup files store in the device. Please proceed with caution.

## Cleaner

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails etc... manually and automatically under Web GUI→**Maintenance→System Cleanup/Reset→Cleaner**.

### Manual Cleaning

The following screenshot show the settings and parameters to configure the manual cleaner feature on SoftwareUCM.



Manual Cleaning

UCM regularly cleans up CDRs, report data, chat data, recording files, historical appointment meeting records, voice mail, backup files, and fax files. The report data includes queue statistics report and conference room call statistics report; chat data includes chat messages and chat shared files; historical appointment conferences include audio and video conference appointment records. Automatic cleanup is not enabled by default and supports regular cleanup of database data based on dimensions such as cleanup time, cleanup conditions, and cleanup interval.

User can also set an automatic cleaning under **Cleaner > Automatic Cleaning**. The following screenshot show the settings and parameters to configure the cleaner feature on SoftwareUCM.

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

Meeting Call

Report

Statistics Report

Multimedia Meeting

History

Clean Time

Cleaning Conditions

Clean Interval (d)

IM Data Cleaner

Enable Cleaner

Clear Chat Data from  
Fingerprint

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	<ul style="list-style-type: none"><li>● <b>By Schedule:</b> 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.</li><li>● <b>Keep Last X Records:</b> If the max number of CDR has been reached, CDR will be deleted starting with the oldest entry at the configured cleaning time. (Note: The amount of records displayed on the page of call queue statistics is not one-to-one with the actual amount of records in the database.)</li><li>● <b>Keep Last X Days:</b> Delete all entries older than X days.</li></ul>
Clean Interval	Enter 1-30 to specify the day of the month to clean up CDR when <b>By Schedule</b> is selected as <b>Cleaning Conditions</b> .
Max Entries	Set the maximum number of CDR entries to keep when <b>Keep Last X Records</b> is selected as <b>Cleaning Conditions</b> . Default is 50000. Valid range: 10000 – 100000.
Keep Last X Days	Enter the number of days of call log entries to keep when <b>Keep Last X days</b> is selected as <b>Cleaning Conditions</b> . 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.

	<ul style="list-style-type: none"><li>Queue Statistics Report</li><li>Meeting Call Statistics Report</li><li>Multimedia Meeting History</li></ul>
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	<ul style="list-style-type: none"><li><b>By Schedule:</b> If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.</li><li><b>Keep Last X Records:</b> 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.)</li><li><b>Keep Last X Days:</b> Delete all entries older than X days.</li></ul>
Clean Interval	Enter how often (in days) to clean queue logs when <b>By Schedule</b> is selected as <b>Cleaning Conditions</b> . The valid range is 1-30.
Max Entries	Set the maximum number of Queue Statistics Report entries to keep when <b>Keep Last X Records</b> is selected as <b>Cleaning Conditions</b> . Default is 50000. Valid range: 10000 – 100000.
Keep Last X Days	Enter the number of days of Queue Statistics Report entries to keep when <b>Keep Last X days</b> is selected as <b>Cleaning Conditions</b> . Default is 30. Valid range: 1 – 730.
IM Data Cleaner	
Enable Cleaner	Enable IM data cleaner
Data Type	Select a type of file to clean. <ul style="list-style-type: none"><li>IM Files</li><li>IM Messages</li></ul>
Clean time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	<ul style="list-style-type: none"><li><b>By Schedule:</b> If the clean interval is 3, cleaning will be performed every 3 days to remove all records that were generated 3 days ago.</li><li><b>Keep Last X Records:</b> 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.)</li><li><b>Keep Last X Days:</b> Delete all entries older than X days.</li></ul>
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	<div>Select the files for system automatic clean.</div> <div><ul style="list-style-type: none"><li>Basic Call Recording Files</li><li>Meeting Recording Files</li><li>Meeting Video Recordings</li><li>Paging/Intercom Recordings</li><li>Paging/Intercom Video Recordings</li><li>Call Queue Recording Files</li><li>Voicemail Files</li><li>Emergency Calls Recording Files</li><li>Fax</li><li>Backup Files</li><li>SCA Recording Files</li></ul></div>
Clean Time	Enter the hour of the day to start the cleaning. The valid range is 0-23.
Cleaning Conditions	<div><ul style="list-style-type: none"><li><b>By Schedule:</b> If the clean interval is 3, cleaning will be performed every 3 days to delete all files.</li><li><b>By Threshold:</b> Check at the configured cleaning time every day to see if the storage threshold has been exceeded and perform cleaning of all files if it has.</li><li><b>Keep Last X Days:</b> Delete all files older than X days.</li></ul></div>
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.
Cleaner Log	
Cleaner Log	Clicking on the Clean button will clear the cleaner log.

All the cleaner logs will be listed on the bottom of the page.

## Network Troubleshooting

### Ethernet Capture

Ethernet Capture tool allows to capture the ethernet packets from the SoftwareUCM 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.

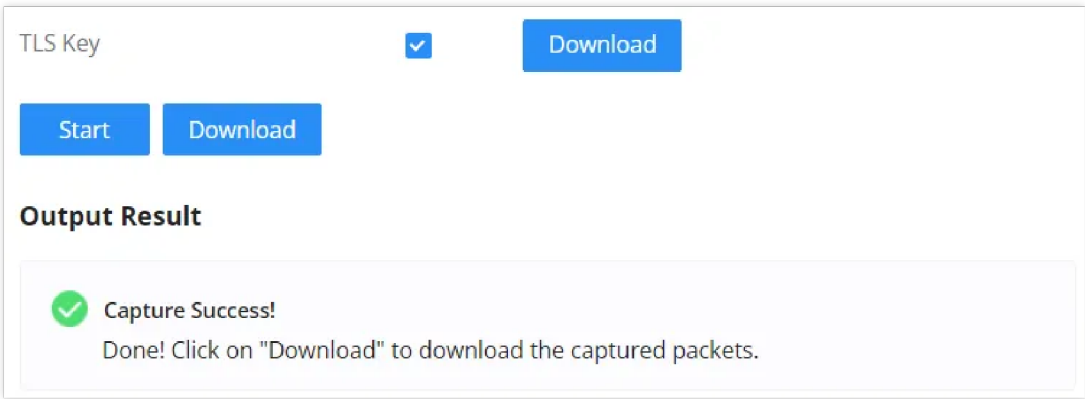
### Enable TLS Key

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 he steps below. In this example, we are using the packet analyzer Wireshark.

**Important**

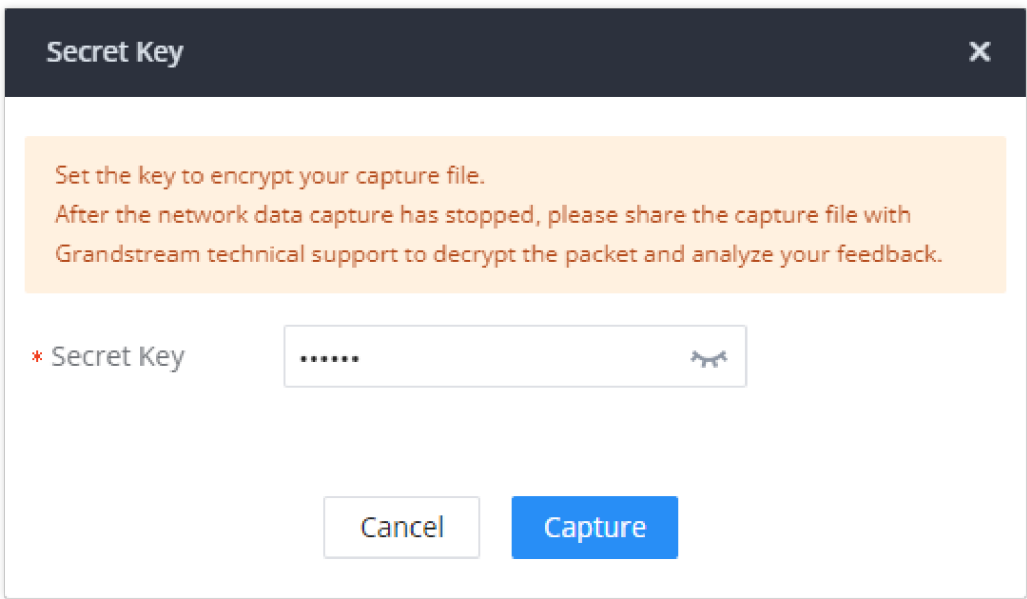
To be able to decrypt the packets captured, they must include the TLS handshake. Otherwise, the packets cannot be decrypted.

1. Before capturing the packet trace, please tick the box “TLS Key”.



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.



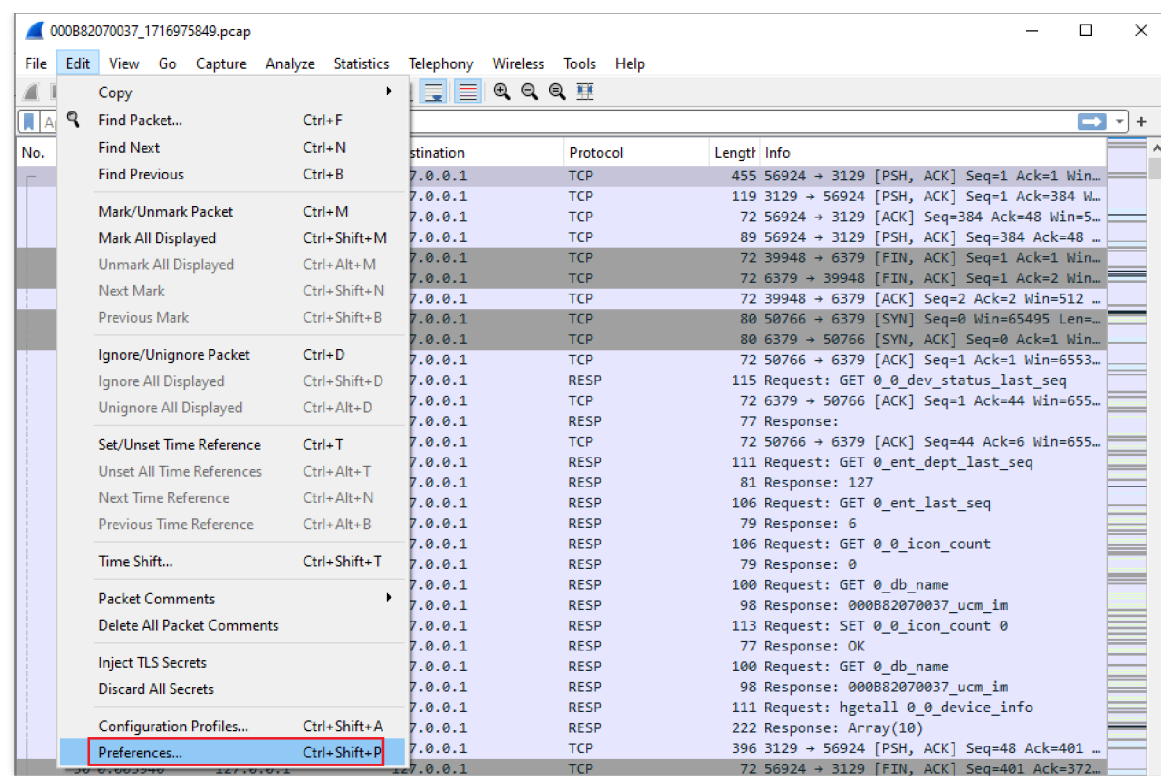
Secret Key

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 SoftwareUCM.

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

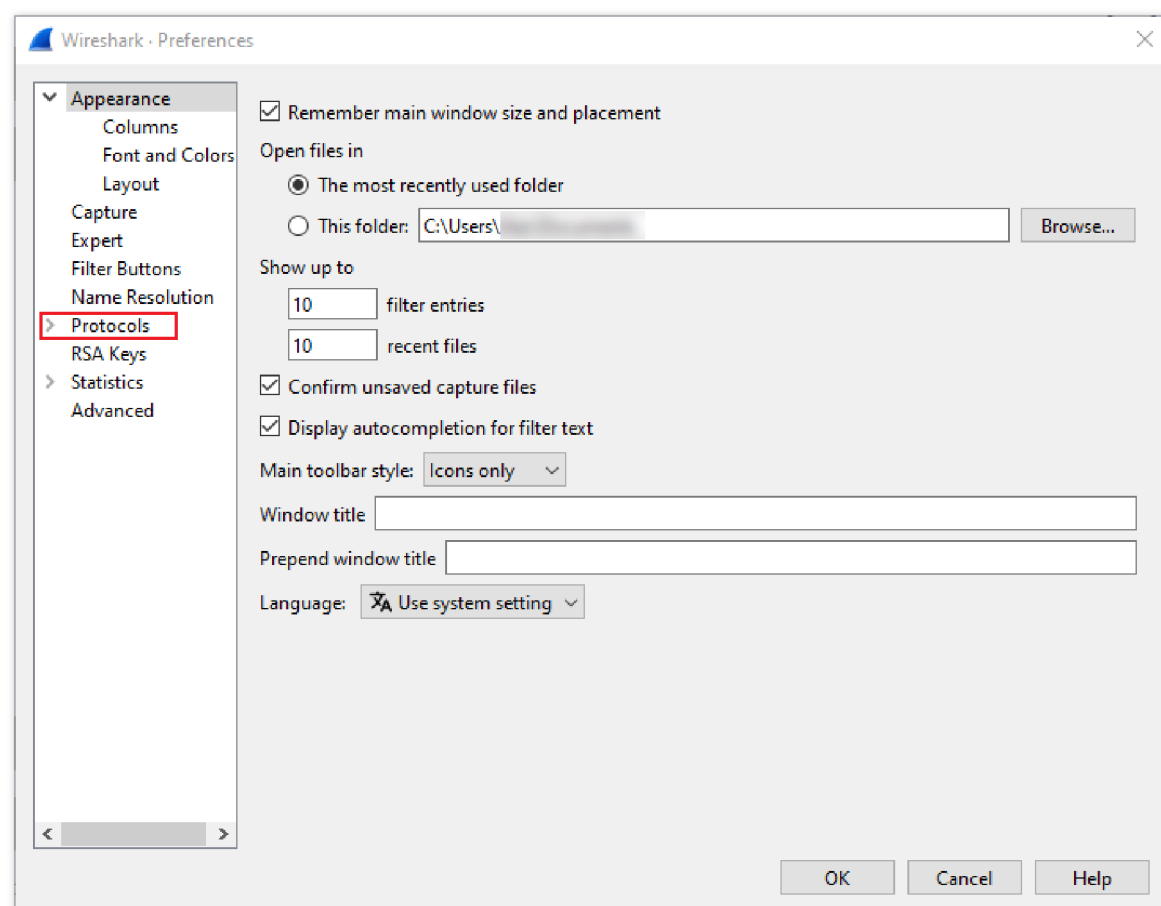
Packet Capture Archive

6. Use Wireshark to open the packet capture file, then select “Edit” Wireshark’s interface. Select “Preferences”



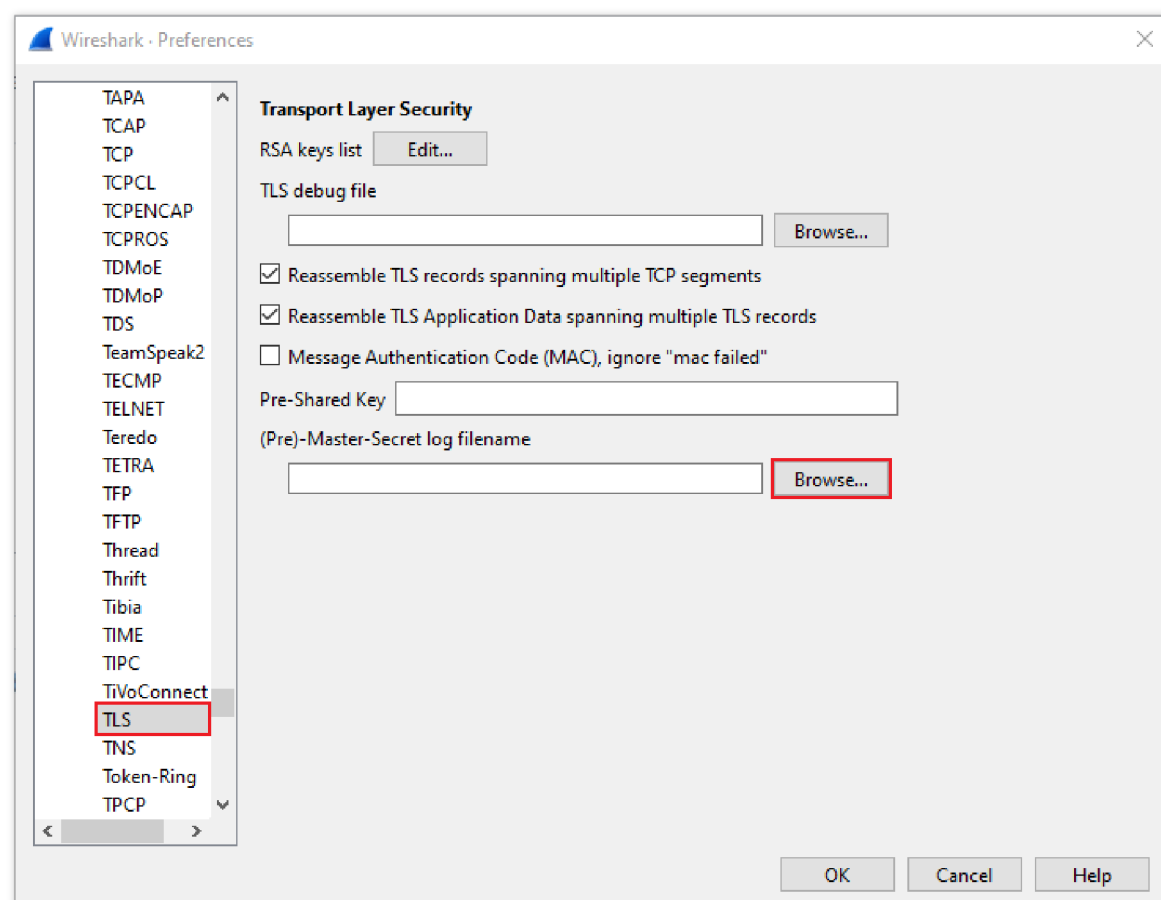
Wireshark

7. Click on “Protocols” to open the list of protocols.

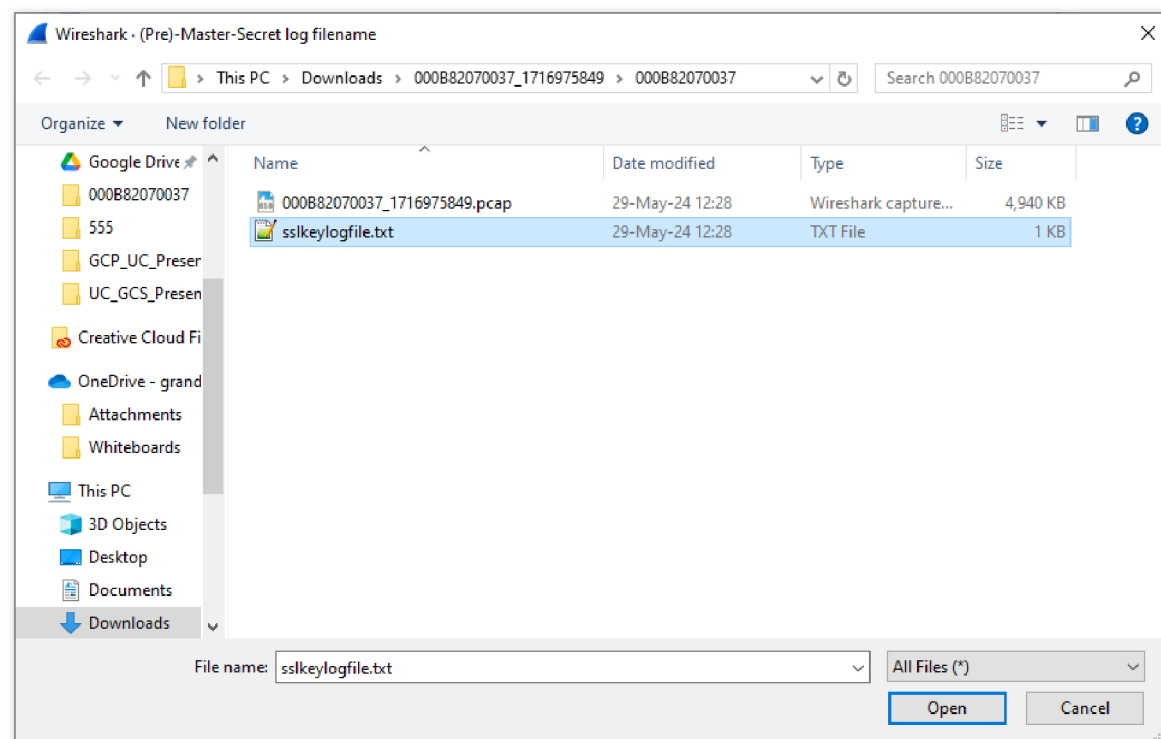


Protocols Preferences

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.



9. Navigate to the folder where the TLS key is stored then select it and click "Open", then click "OK".



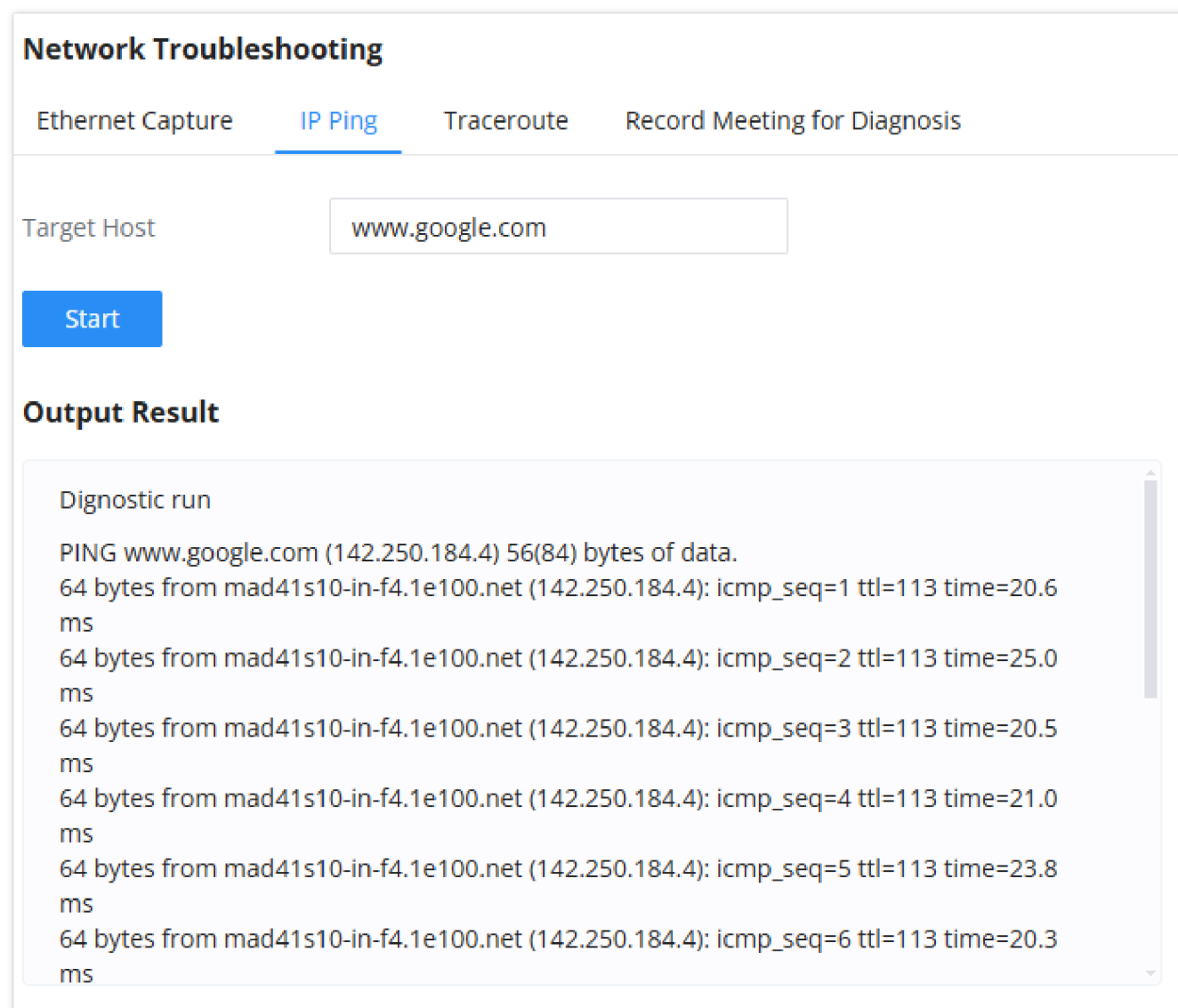
TLS Key File

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.

## IP Ping

Enter the target host's IP address or domain name, then press "Start" button. The ping command will run continuously until it's manually stopped. The output result will dynamically display in the window below.



IP Ping

## Traceroute

Enter the target host's IP address or domain name, then press "Start" button. Once the destination is reached, the traceroute will end.



### Network Troubleshooting

[Ethernet Capture](#)
[IP Ping](#)
[Traceroute](#)
[Record Meeting for Diagnosis](#)

\* Target Host

www.google.com

Start

#### Output Result

Dignostic run

traceroute to www.google.com (142.250.184.4), 30 hops max, 46 byte packets  
 1 192.168.6.1 (192.168.6.1) 0.686 ms 0.715 ms 0.624 ms  
 2 197.247.64.3 (197.247.64.3) 3.796 ms 3.820 ms 3.566 ms  
 3 172.20.1.53 (172.20.1.53) 4.929 ms 5.057 ms 4.815 ms  
 4 10.43.82.206 (10.43.82.206) 4.740 ms 5.280 ms 4.685 ms  
 5 10.43.250.213 (10.43.250.213) 20.427 ms 21.521 ms 20.668 ms  
 6 72.14.211.128 (72.14.211.128) 29.582 ms 20.299 ms 20.289 ms  
 7 108.170.252.215 (108.170.252.215) 21.807 ms 108.170.252.211 (108.170.252.211) 24.703 ms 23.878 ms  
 8 142.250.214.43 (142.250.214.43) 19.970 ms 20.533 ms 20.025 ms  
 9 mad41s10-in-f4.1e100.net (142.250.184.4) 20.147 ms 20.276 ms 21.260 ms

Done

Traceroute

## Record Meeting for Diagnosis

Enter the target meeting, supports the ongoing meeting, and then click the “Start” button to capture the recording diagnosis of the meeting members in progress. The output result will be automatically displayed below, click the “download” button to download to the local storage. After the download is complete, immediately click the “Delete” button to clear the system content.

To capture a meeting recording, make sure that the meeting is ongoing, select it from “Traget Meeting” menu, then click “Start”. The capturing of the meeting will start as shown in the figure below.

### Network Troubleshooting

[Ethernet Capture](#)
[IP Ping](#)
[Traceroute](#)
[Record Meeting for Diagnosis](#)

\* Target Meeting

6300

Stop

Download

Delete

#### Output Result

Capturing...

Meeting Recording Ongoing

When enough data is captured, click on “Stop” to stop the meeting capture. Then click on “Download” to download the capture files.

Network Troubleshooting

Ethernet CaptureIP PingTracerouteRecord Meeting for Diagnosis

Target Meeting

Start

Download

Delete

Output Result

Capture Success!

Done! Click on "Download" to download the captured packets.

Meeting Recording Done

Service Check

Enable Service Check to periodically check SoftwareUCM 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 SoftwareUCM. The default setting is 3. If there is no response from SoftwareUCM after 3 attempts (default) to check, current status will be stored and the internal service in SoftwareUCM will be restarted.

Service Check

Toggle Service Check

\* Check Frequency (s)

60

\* Check Times

3

Cancel

Save

Service Check

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

CDR

Hide Filter

Start Time

2025-01-01

00:00

End Time

2025-01-13

16:12

Caller Number

Caller Name

Original Caller Number

Callee Number

Source Trunk Name

Destination Trunk Name

Action Type

Account Code

Extension Group

Extension

Export File Data

Call Type

☐ Inbound Calls

☐ Outbound Calls

☐ Internal Calls

☐ External Calls

☐ Remote Calls

Status

☐ Answered

☐ No Answer

☐ Busy

☐ Failed

Filter

Reset

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

Delete All

Delete Search Result(s)

Download All Records

Download Search Result(s)

Automatic Download

CDR Settings

CDR in GOMS Cloud

Status	Call from	Call to	Action Type	Start Time	Call Time	Talk Time	Options
	1000	6300	MULTIMEDIA MEETING...	2025-01-13 12:14:36	0:00:31	0:00:31	-

CDR Filter

Call Type	<p>Groups the following:</p> <ul style="list-style-type: none"><li><b>Inbound calls:</b> Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension.</li><li><b>Outbound calls:</b> Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension.</li><li><b>Internal calls:</b> Internal calls are calls from one internal extension to another extension, which are not sent over a trunk.</li><li><b>External calls:</b> External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension.</li></ul>
Status	<p>Filter with the call status, the available statuses are the following:</p> <ul style="list-style-type: none"><li>Answered</li><li>No Answer</li><li>Busy</li><li>Failed</li></ul>
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.

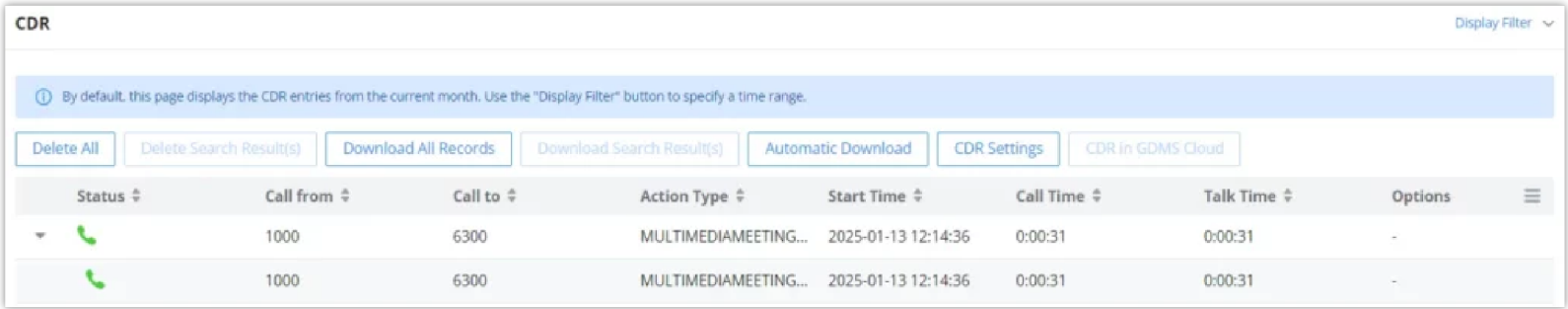
Action Type	<p>Filter calls using the Action Type, the following actions are available:</p> <ul style="list-style-type: none"><li>○ Announce</li><li>○ Announcement page</li><li>○ Dial</li><li>○ Announcements</li><li>○ Callback</li><li>○ Call Forward</li><li>○ Conference</li><li>○ DISA</li><li>○ Follow Me</li><li>○ IVR</li><li>○ Page</li><li>○ Parked Call</li><li>○ Queue</li><li>○ Ring Group</li><li>○ Transfer</li><li>○ VM</li><li>○ VMG</li><li>○ Video Conference</li><li>○ VQ_Callback</li><li>○ Wakeup</li><li>○ Emergency Call</li><li>○ Emergency Notify</li><li>○ SCA</li></ul>
Extension Group	<p>Specify the Extension Group name to filter with.</p>

<b>Export File Data</b>	<p>Select the fields that will be exported, the following fields are available:</p> <ul style="list-style-type: none"><li>○ Account Code</li><li>○ Session</li><li>○ Premier caller</li><li>○ Action type</li><li>○ Source trunk name</li><li>○ Destination trunk name</li><li>○ Caller number</li><li>○ Caller ID</li><li>○ Caller name</li><li>○ Callee number</li><li>○ Answer by</li><li>○ Context</li><li>○ Start time</li><li>○ Answer time</li><li>○ End time</li><li>○ Call time</li><li>○ Talk time</li><li>○ Source channel</li><li>○ Dest channel</li><li>○ Call status</li><li>○ Dest channel extension</li><li>○ Last app</li><li>○ Last data</li><li>○ AMAFLAGS</li><li>○ UIQUEID</li><li>○ Call type</li><li>○ NAT</li></ul>
<b>Account Code</b>	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.
<b>Start Time</b>	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.
<b>End Time</b>	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.
<b>Caller Number</b>	<p>Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out.</p> <p>User could specify a particular caller number or enter a pattern. '.' matches zero or more characters, only appears in the end. 'X' matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end.</p> <p>For example:</p> <p><b>3XXX:</b> It will filter out CDR that having caller number with leading digit 3 and of 4 digits' length.</p> <p><b>3.:</b> It will filter out CDR that having caller number with leading digit 3 and of any length.</p>

<b>Caller Name</b>	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
<b>Callee Number</b>	Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out.  <b>Note:</b> The “Callee Number” filter field supports specifying Pattern (example: 3XXX) or using Leading digits (example: 3.) as filtering options.

CDR Filter Criteria

The call report will display as the following figure shows.



Call Report

The CDR report has the following data fields:

Start Time

Format: 2019-12-11 09:53:03

Action Type

Example:

IVR

DIAL

WAKEUP

Call From

Example format: 5555

Call To

Example format: 1000

Call Time

Format: 0:00:11

Talk Time

Format: 0:00:06

Account Code

Example format:

Grandstream/Test

Status

Answered, Busy, No answer or Failed.

Users could perform the following operations on the call report.

◦ **Sort by “Start Time”**

Click on the header of the column to sort the report by “Start Time”. Clicking on “Start Time” again will reverse the order.


◦ **Download Searched Results**

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


◦ **Download All Records**

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

◦ **Delete All**

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




◦ **Delete Search Result**

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

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

◦ **Play/Download/Delete Recording File (per entry)**

If the entry has audio recording file for the call, the three icons on the rightest column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

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



Call Report Entry with Audio Recording File

◦ **Automatic Download CDR Records**

User could configure the SoftwareUCM 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

Automatically send new CDR entries to the configured email address based on the configured period. To upload CDR records to an SFTP server, please navigate to the [Data Sync](#) page to configure it.

Automatic Download

☒

Delete Sent Records

☒

Automatic Download Period

By Day

0

Email

admi@grandstream.com

Email Template

Cancel

OK

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 C ODE	RECORDING FILE OPTIONS
	5555	1000	DIAL	2019-12-11 09:53:03	0:00:11	0:00:06		-

CDR Report

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

Detailed CDR Information

Downloaded CDR File

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

- Caller number, Callee number

“Caller number”: the caller ID.

“Callee number”: the callee ID.

C	D	E	F	G	H	I	J	K	L
Caller Number	Original Caller Number	Caller NAT	Callee Number	Callee NAT	Context	Caller ID	Source Channel	Dest. Channel	Last app.
1001	1001	no	1000	no	from-internal	"" <1001>	PJSIP/1001-00000001	PJSIP/1000-00000002	Dial
1001	1001	no	1000	no	from-internal	"" <1001>	PJSIP/1001-00000001	PJSIP/1000-00000002	Dial
1000	1000	no	6300		from-internal	"" <1000>	PJSIP/1000-00000000		ConfBridge
1000	1000	no	6300		from-internal	"" <1000>	PJSIP/1000-00000000		ConfBridge

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:

C	D	E	F	G	H	I	J	K	L
Caller Number	Original Caller Number	Caller NAT	Callee Number	Callee NAT	Context	Caller ID	Source Channel	Dest. Channel	Last app.
1001	1001	no	1000	no	from-internal	"" <1001>	PJSIP/1001-00000001	PJSIP/1000-00000002	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.

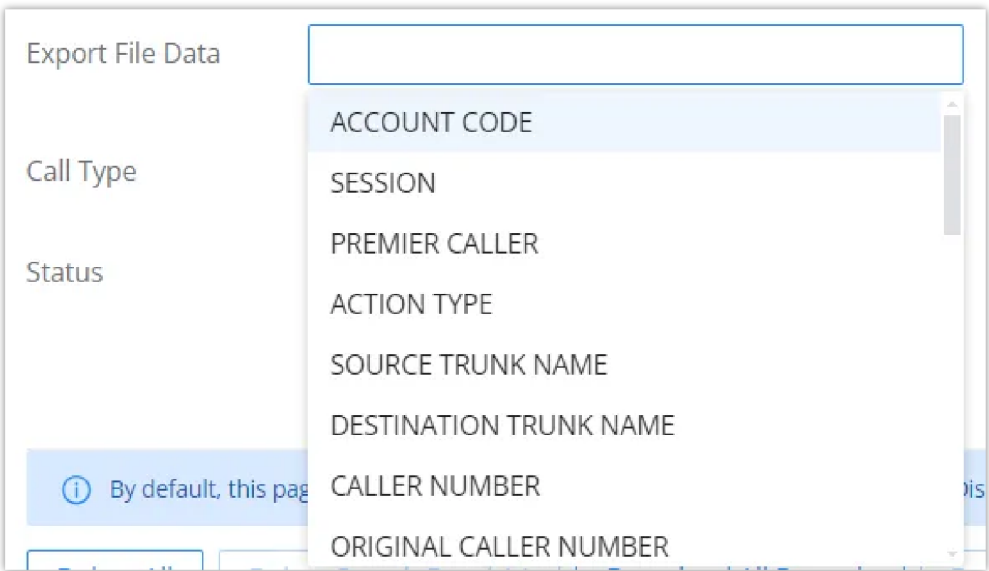
**ReadExten**: collect numbers from user. It may occur when you input PIN codes or run into DISA

**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**

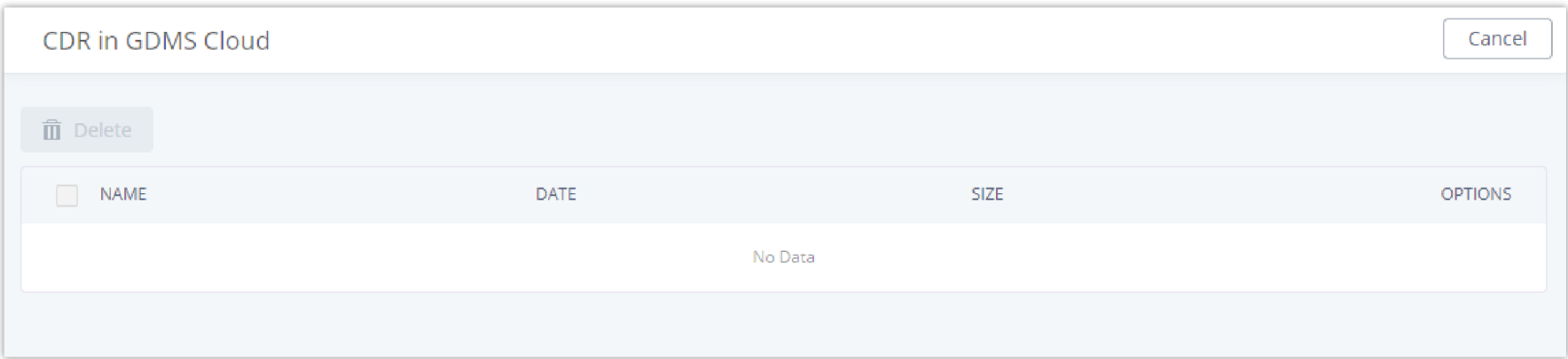
Users can select the data they want to see in exported CDR reports by first clicking on the *Filter* button on the CDR page under **CDR > CDR** and selecting the desired information in the *Export File Data* field.



CDR Export File data

**CDR in GDMS Cloud**

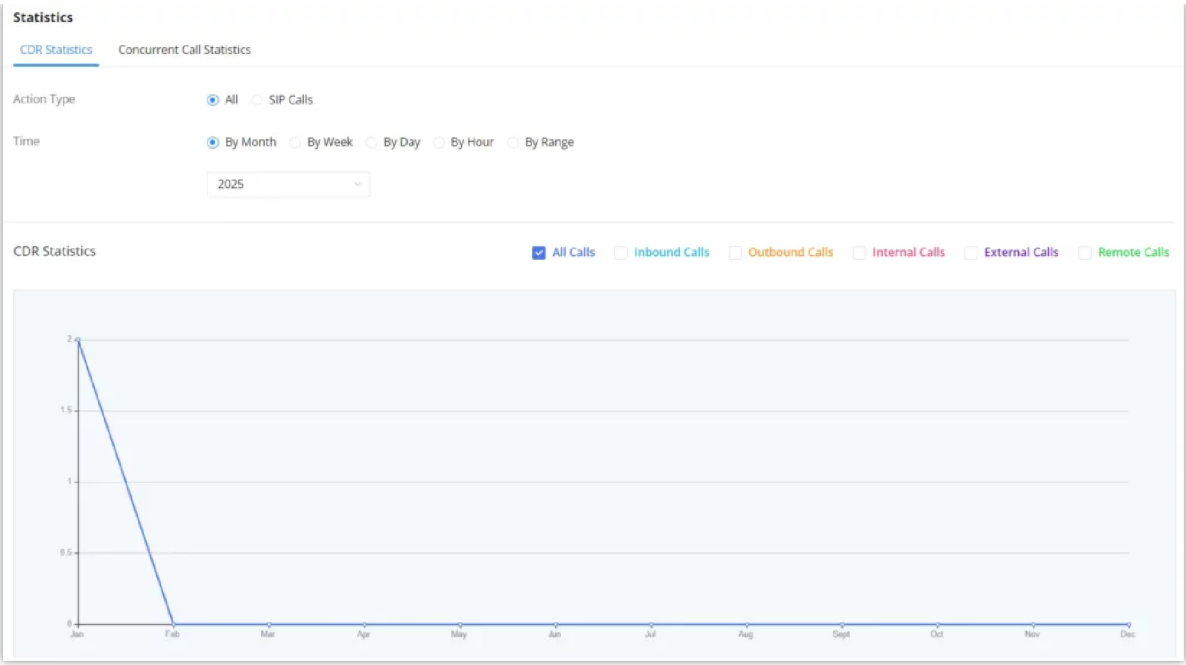
Cloud Storage for CDR Record which can be displayed under **CDR → CDR in GDMS Cloud**.



CDR in GDMS Cloud

**Statistics**

UCM supports the function of concurrent call statistics. This function provides users with statistics on the number of concurrent calls of all VOIP trunks (SIP trunks ). Users can set search criteria to generate custom charts. Select the trunk and time to view the chart of the maximum number of concurrent calls corresponding to the trunk in a certain day or month.



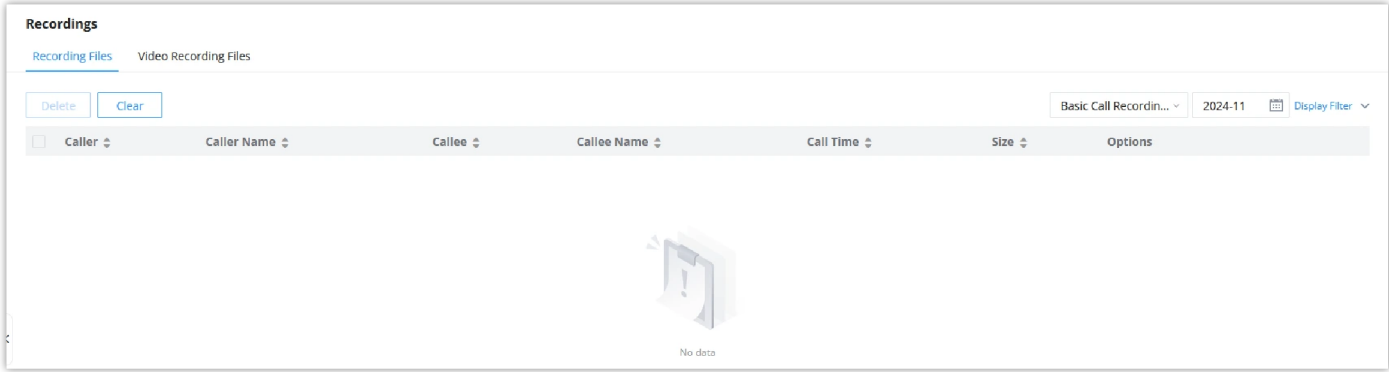
CDR Statistics

Trunk Type	<div>Select one of the following trunk type.</div> <div><div>All</div><div>SIP Calls</div></div>
Call Type	<div>Select one or more in the following checkboxes.</div> <div><div>Inbound calls</div><div>Outbound calls</div><div>Internal calls</div><div>External calls</div><div>All calls</div></div>
Time Range	<div><div>By month (of the selected year).</div><div>By week (of the selected year).</div><div>By day (of the specified month for the year).</div><div>By hour (of the specified date).</div><div>By range. For example, 2016-01 To 2016-03.</div></div>

CDR Statistics Filter Criteria

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”.





CDR – Recording Files

The list of recording files are:

- Basic Call Recordings.
- Queue Recordings.
- Record Recordings.

- SCA Recordings.
- Emergency Recordings.
- Paging/Intercom Recordings

Click on  to download the recording file in .wav format and  to delete the recording file.

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 or descending order.

# REMOTECONNECT

## Plan

In this tab, the user can view information about the plan of the SoftwareUCM all the settings related.

## Service Description

In this section, the user can view all the services related to RemoteConnect.

RemoteConnect

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics



GDMS Cloud Storage Space

Service Description

My Plan

Plan Settings

Current Plan: Plus (Trial)

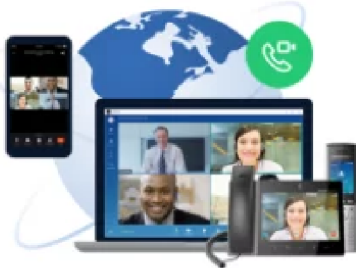


Renewal/Upgrade

[Learn about UCMRC](#)

[UCMRC User Guide](#)

Grandstream has launched the UCM RemoteConnect service, a remote communications solution that offers TURN penetration capabilities to meet the needs of those working in home offices or out on business trips. Additionally, it offers cloud storage space, Cloud IM, add-in integrations and other collaboration features.



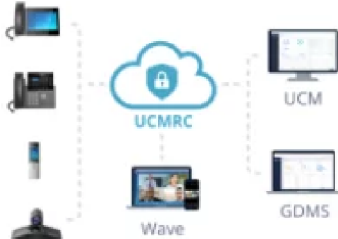
Remote Communication

Use Wave to make/receive calls, schedule and start up meetings with colleagues remotely and easily invite outside parties to join in on meetings for cost-effective communication.

How to configure and use

How to configure endpoints

Notify Employees to Use



Remote Management of UCMs and Endpoints

Use GDMS to deploy, provision, monitor, and diagnose UCM6300 series devices and registered endpoints. The GDMS mobile app is also available to allow users to manage their devices right from their mobile device.

Learn more

How to Manage Remotely

Log into GDMS

## My Plan

In “My Plan” tab, the user can view information related to the SoftwareUCM 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.

RemoteConnect

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics


GDMS Cloud Storage Space

Service Description

My Plan

Plan Settings

Plan Name

Plus(Trial) 

Plan Expiration Date

2/28/2025

Max Remote Concurrent Sessions

8

Max Remote Registrations

50

Max Remote Call Time

Per Call

Unlimited

Per Day

Unlimited

Per Month

Unlimited


GDMS Cloud Storage

1 GB


STUN Address

161.189.44.114

Wave RemoteConnect Address



IP Endpoint/Trunk RemoteConnect Address



Wave 3rd Party Add-ins

[Supported](#)

Cloud IM Server

Not supported by the current plan

## Plan Settings

In “Plan Settings” tab, the user can configure SIP extension synchronization between the SoftwareUCM and the GDMS platform. The user can also set alert events synchronization, configure remote login settings and passwordless remote access.

RemoteConnect

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

GDMS Cloud Storage Space

Service Description

My Plan

Plan Settings

Bound Enterprise: GS

Service Site: US

Organization: Default

General

SIP Extension Sync

☒

Media NAT Traversal Service

☒

Alert Events Sync

☒

Remote Login Settings

[Go to Page](#)

Cloud IM Settings

Not supported by the current plan

Storage & Backup

Enable GDMS Cloud Storage

☒

CDR Stored in GDMS Cloud

☐

Back up to GDMS

[Go to Page](#)

Recordings Stored in GDMS Cloud

[Go to Page](#)

## Integrated Customer Service

In “Integrated Customer Service”, the user can access the sections for WebRTC Trunks configuration and Live Chat Customer Service.

RemoteConnect

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

GDMS Cloud Storage Space

Call Customer Service

WebRTC Trunks

WebRTC Trunks

Go to Page

Enable Click2Call

Enable Click2Call

☐

Live Chat Customer Service

Live Chat Customer Service

Go to Page

Cancel

Save

## Enterprise UI Customization

On the **Web GUI → 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

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

Company Name

Grandstream

Logo

It is recommended to not use blue, black, and white for the logo color.

Logo 1 80\*80px

Logo

Upload

Logo 2 256\*256px

Logo

Upload

Logo 3 64\*64px (.ico)

Logo

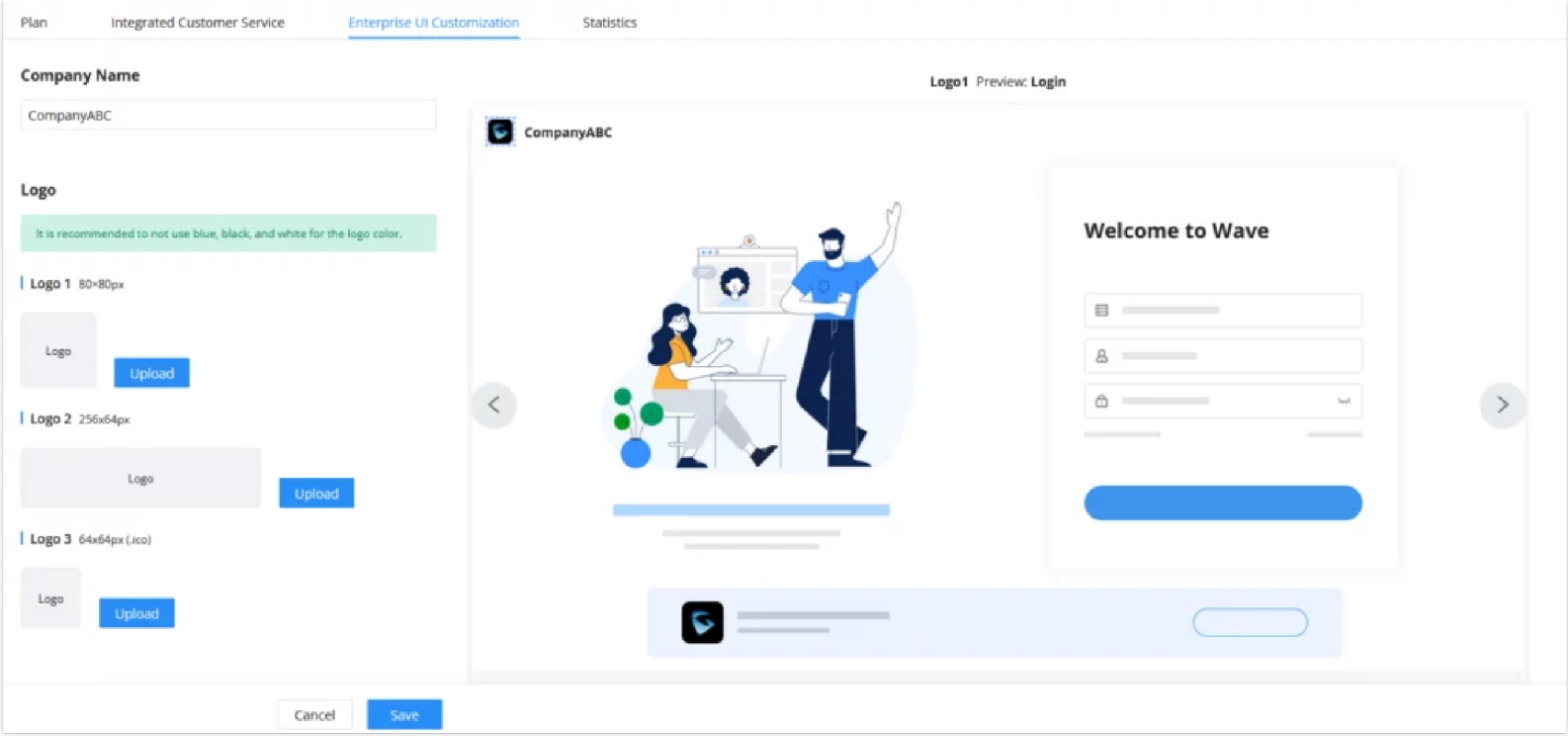
Upload

Logo1 Preview: UCM

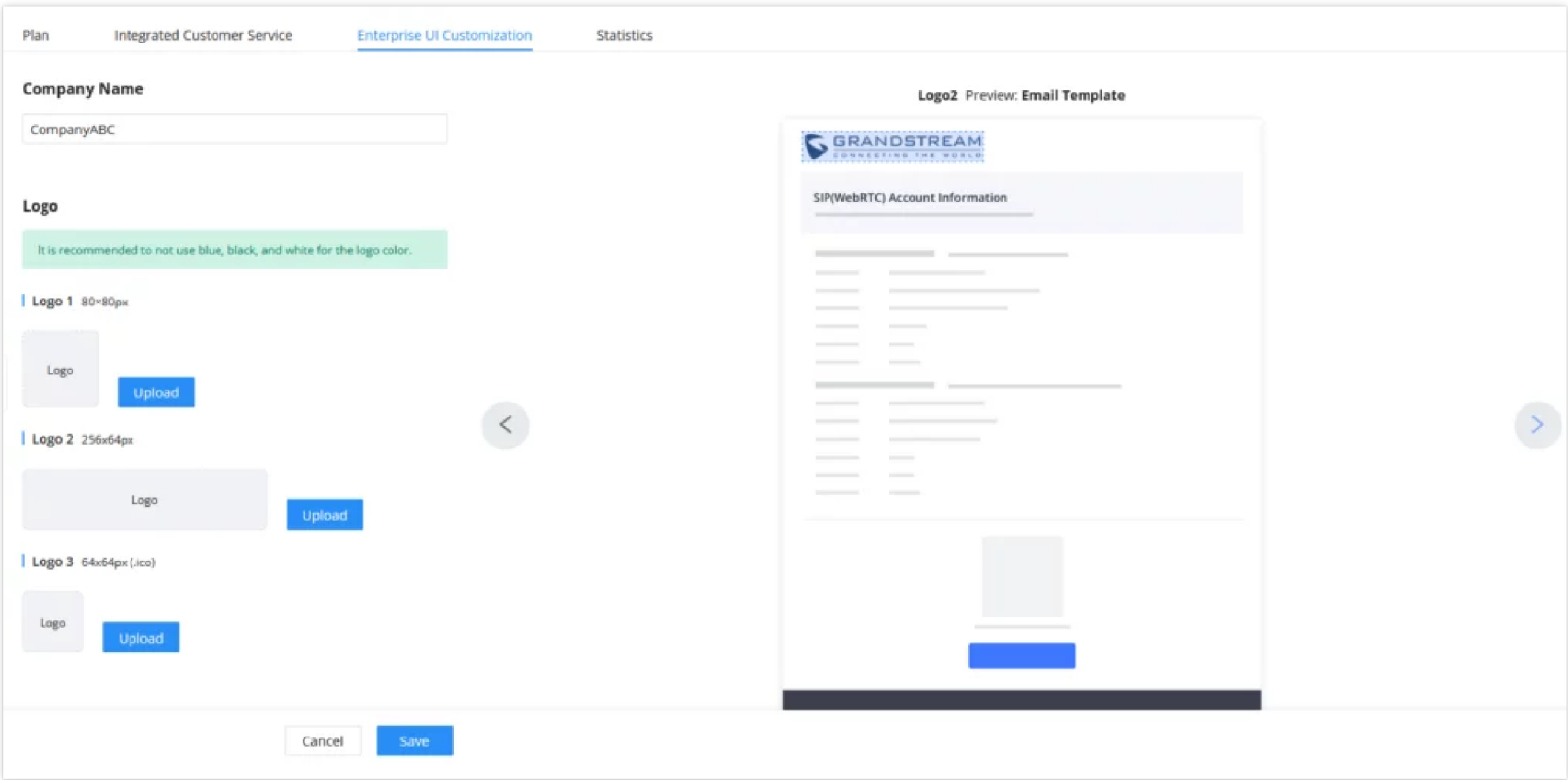
Cancel

Save

SoftwareUCM UI Customization

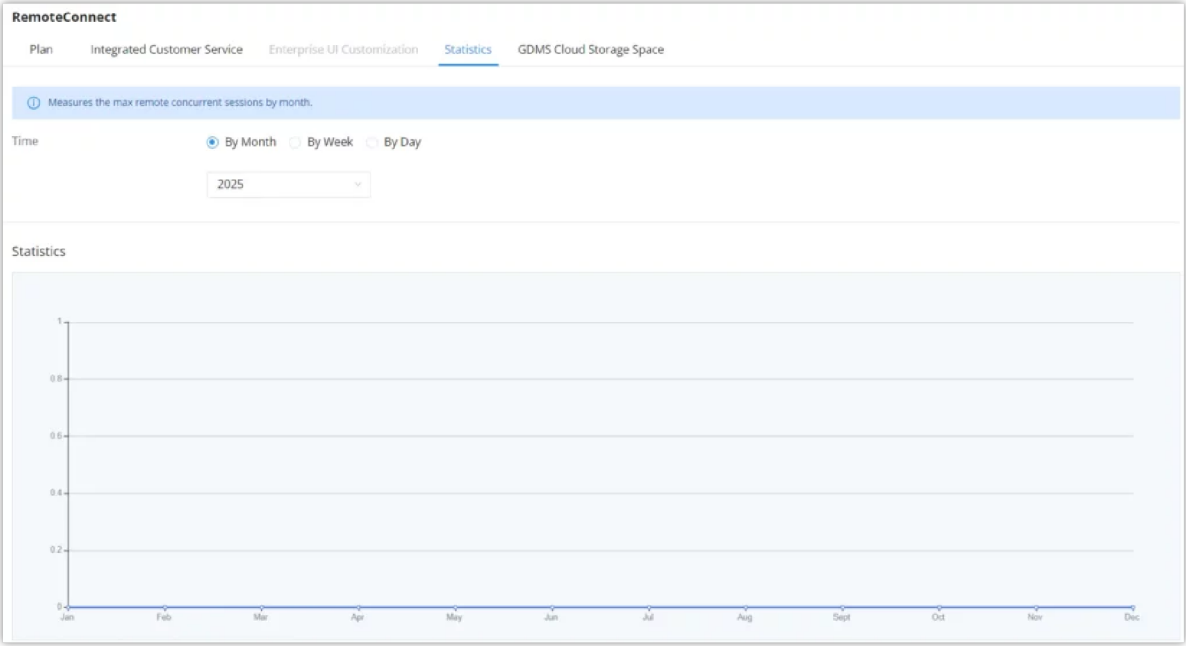


Wave UI Customization



Email Customization

## Statistics

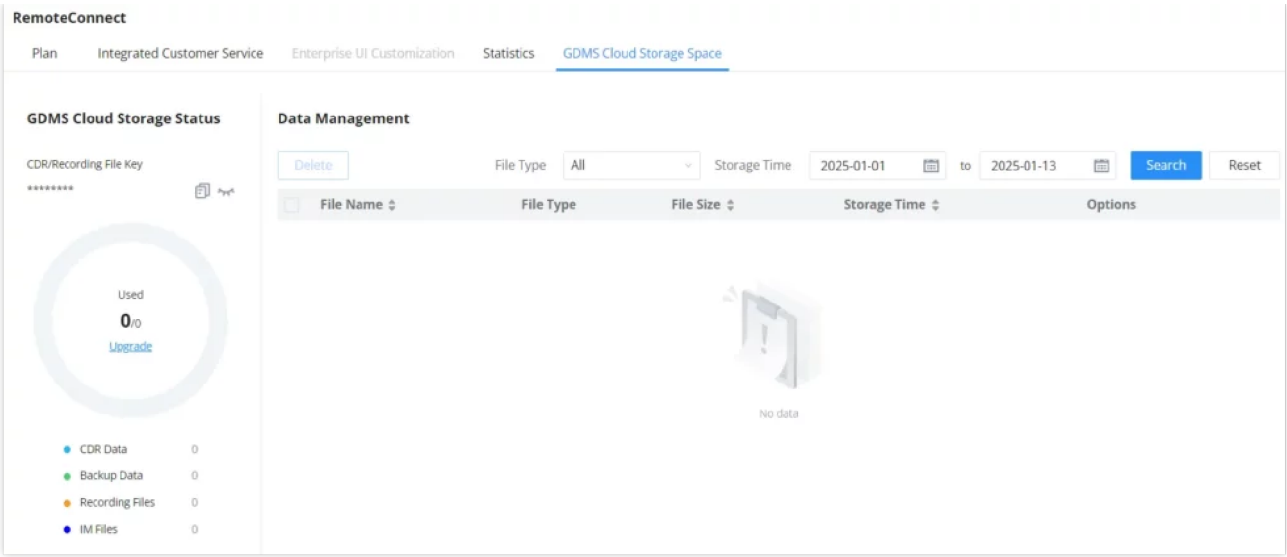


## GDMS Cloud Storage Space

When the correspondent RemoteConnect plan is active, the user can access to a GDMS Cloud Storage Space to get an overview about how the storage space is being used. The data is represented in four categories of file types: CDR Data, Backup Data, Recording Files, and IM Files.

The user is also able to see the names of all the files stored in the GDMS Cloud Storage Space.





GDMs Cloud Storage

# INTEGRATIONS

## API Configuration

SoftwareUCM API allows creating an interface between the UCM and an application to send HTTP requests to the UCM, either to configure the UCM to get information from it.

## API Settings

Before accessing the API, the administrators need to enable API and configure the access/authentication information on the SoftwareUCM first under **Integrations → API Configuration**. The API configuration parameters are listed in the tables below.

<b>Username</b>	The username for API Authentication.
<b>Password</b>	The password for API Authentication.
<b>Call Control</b>	If enabled, 3rd party applications will be able to manage inbound calls via API actions. <b>acceptCall</b> will accept incoming calls while <b>refuseCall</b> will reject them. If no actions are done within 10 seconds, calls will automatically be accepted.
<b>Permitted IP (s)</b>	Sets an IP address Access Control List (ACL) for addresses that are allowed to authenticate and register as this user. By default, this is not configured, allowing all IP addresses to register to this extension. The format is: "xxx.xxx.xxx.xxx/255.255.255.255"

### Note

You can create multiple users with different login credentials to access to the HTTPS API.

## API Queries Supported

The new API supports now new queries listed below which will accomplish certain requests and get data about different modules on SoftwareUCM.

getSystemStatus	addInboundRoute	listPaginggroup
getSystemGeneralStatus	getInboundRoute	addPaginggroup
listAccount	updateInboundRoute	getPaginggroup

getSIPAccount	deleteInboundRoute	updatePaginggroup
updateSIPAccount	playPromptByOrg	deletePaginggroup
listVoIPTrunk	listBridgedChannels	MulticastPaging
addSIPTrunk	listUnBridgedChannels	MulticastPagingHangup
getSIPTrunk	Hangup	listIVR
updateSIPTrunk	Callbarge	addIVR
deleteSIPTrunk	listQueue	getIVR
listOutboundRoute	getQueue	updateIVR
addOutboundRoute	updateQueue	deleteIVR
getOutboundRoute	addQueue	cdrapi
updateOutboundRoute	deleteQueue	recapi
deleteOutboundRoute	loginLogoffQueueAgent	pmsapi
listInboundRoute	pauseUnpauseQueueAgent	queueapi
mute	Unmute	hold
unhold	dialExtension	dialOutbound
callTransfer	transferNumberInbound	transferNumberOutbound
dialIVR	dialIVROutbound	dialQueue
dialRinggroup	dialOutboundTwo	listUser
getUser	updateUser	listExtensionGroup
listPinSets	refuseCall	acceptCall
applyChanges	deleteDigitalTrunk	addDigitalTrunk
getDigitalTrunk	listDigitalTrunk	updateDigitalTrunk
listDepartment	getRecordInfosByCall	addMessageBroadcast

<b>CDR Real-time Output Settings</b>	
<b>Enable</b>	Enables real-time CDR output module. This module connects to selected IP addresses and ports and posts CDR strings as soon as it is available.
<b>Server Address</b>	CDR server IP address

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 now can use the “Upload Prompts User Configuration” to upload/replace voice prompt files as an alternative method to the manual upload method on UCM **PBX Settings→ Voice Prompt→ Custom Prompt.**

The workflow of the prompt file upload goes as:

An HTTP/HTTPS request is sent to the UCM to upload/replace a voice prompt file, the request should include authentication details to the UCM and the name of the file to be uploaded. Then the UCM will contact an FTP server that should be hosted on the same IP address of the HTTP/HTTPS requester and download the prompt file from the FTP server.

The steps and conditions to upload the voice prompt via API are listed below:

1. Configure the prompt User under **Integrations → API Configuration → Upload Prompts User Configuration.** By default, the username and password for voice prompt user are “Username: uploader; Password: uploader123”.

API Configuration

API Settings (New)CDR Real-time Output SettingsUpload Prompts User Configuration

Upload Prompts User Configuration

Enable

☐

Username

uploader

Password

uploader123

Cancel

Save

Upload Prompt User Configuration

2. Hash the password of the user configured to 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 the document in the link here:

<https://documentation.grandstream.com/knowledge-base/cdr-rec-api/>

## AMI (Asterisk Management Interface)

The SoftwareUCM supports Asterisk Manager Interface (AMI) with restricted access. AMI allows a client program to connect to an Asterisk instance commands or read events over a TCP/IP stream. It is particularly useful when the system admin tries to track the state of a telephony client inside Asterisk.

User could configure AMI parameters on **Integrations > AMI**. For details on how to use AMI on the PBX, please refer to the following AMI guide: <https://documentation.grandstream.com/knowledge-base/ami-asterisk-management-interface/>

### Warning

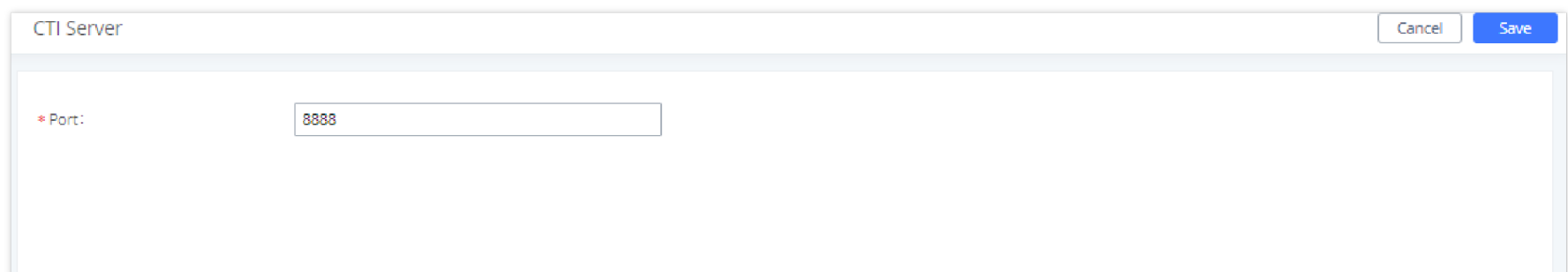
Please do not enable AMI on the SoftwareUCM if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your SoftwareUCM system. Please be cautious when enabling AMI access on the SoftwareUCM and restrict the permission granted to the AMI user. By using AMI on SoftwareUCM, you agree you understand and acknowledge the risks associated with this.

## CTI Server

SoftwareUCM does support CTI server capabilities which are designed to be a part of the CTI solution suite provided by Grandstream, including GXP21XX and GXP17XX enterprise IP phones along with GS Affinity app.

Mainly the Software UCM will, by default, listening on port TCP 8888 for the connections from GS affinity application in order to interact, modify and serve data requests by the application which includes setting call features for the connected extension as call forward and DND.

Users can change the listening port under the menu page, **Integrations > CTI Server** as shown on below screenshot:

A screenshot of a web-based configuration window titled "CTI Server". The window has a title bar with "CTI Server" on the left and "Cancel" and "Save" buttons on the right. The main content area contains a label "\*Port:" followed by a text input field containing the value "8888".

CTI Server

More information about GS affinity and CTI Support on Grandstream products. Please refer to the following link:

<https://documentation.grandstream.com/knowledge-base/gs-affinity-user-guide/>

## 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 SoftwareUCM support the following CRMs: SugarCRM, VtigerCRM, Salesforce CRM and ACT! CRM, and Odoo CRM. Which allows users to look for contact information in the Contacts, Leads and / or Accounts tables, shows the contact record in CRM page, and saves the call information in the contact’s history.

Sugar CRM

Configuration page of the SugarCRM can be accessed via admin login, on the UCM WebGUI **Features > CRM**.

CRM

CRM System

SugarCRM

\* CRM Server Region

https://exasandbox.sugaropencloud.eu

\* Add Unknown Number

None

Contact Lookups

None

Contacts

Leads

Accounts

☐ Look up in Accounts table

1/1

Selected

Search

☒ Look up in Contacts table

<



>

Cancel

Save

SugarCRM Basic Settings

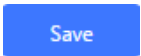
1. Select “SugarCRM” from the CRM System Dropdown in order to use SugarCRM.

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.

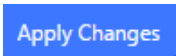
SugarCRM Settings

Once settings on admin access are configured:

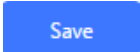
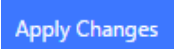
2. Click on



and



3. Logout from admin access.
4. Login to the UCM as user and navigate under “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”. User can start then using SugarCRM features.

CRM User Settings

Enable CRM :

☒

\* Username :

GStest

\* Password :

password@123

Login Status :

CRM User Settings

Vtiger CRM

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 Region

http://vtiger.mydomain.com

\* Add Unknown Number

None

None

Contacts

Leads

Organizations

☐ Look up in Organizations table

<

>

Contact Lookups

☐ 1

Selected

Search

Q

☐ Look up in Contacts table

↕

^

↓



⌵

Cancel

Save

VtigerCRM Basic Settings

1. Select “Vtiger CRM” from the CRM System Dropdown in order 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 “ <b>Available</b> ” list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Organizations, and Contacts.

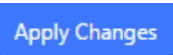
VtigerCRM Settings

Once settings on admin access are configured:

2. Click on



and



- 3. Logout from admin access.
- 4. Login to the UCM as user and navigate under “**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 :

GStest

\* Password :

password@123

Login Status :

CRM User Settings

Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI **Integrations > CRM**.

CRM

CRM System

Salesforce

\* Add Unknown Number

Contacts

Contact Lookups

☐ 2 Available

Search

☐ Look up in Leads table

☐ Look up in Accounts table

☐ 1 Selected

Search

☐ Look up in Contacts table

<

>

↕

↑

↓



✖

Cancel

Save

Salesforce Basic Settings

- 1. Select “Salesforce” from the CRM System Dropdown in order 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 “ <b>Available</b> ” list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Salesforce Settings

Once settings on admin access are configured:

- 2. Click on



Save

and

Apply Changes

.

- 3. Logout from admin access.
- 4. Login to the UCM as user and navigate under “**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.

CRM User Settings

Enable CRM:

☒

\* Username:

user@domain

\* Password:

pjdajdlka123@!

\* Security Token:

mkjhamjkhndjkeFZEfljxwa!@jkjhbamklcel

Login Status:

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 are as follows:

- 1. Navigate to **Integrations > CRM** and select the “ACT! CRM” option.

CRM

CRM System

ACT! CRM

\* Add Unknown Number

Contacts

Cancel

Save

Enabling ACT! CRM

- 2. Log into the UCM as a regular user and navigate to **Other Features > CRM User Settings** and check “Enable CRM” option and enter the username and password, which will be the ACT! CRM account’s **API Key** and **Developer Key**, respectively. To obtain these, please refer to the ACT! CRM API developer’s guide here: <https://www.act.com/>

CRM User Settings

Enable CRM:

☐

Username:

Password:

Login Status:

Enabling CRM on the User Portal

## Odoo CRM

The SoftwareUCM supports integration with Odoo CRM. To enable Odoo CRM, please access the UCM's web UI then navigate to **Integration > CRM**.

CRM

CRM System

ODOO CRM

\* Add Unknown Number

Cancel

Save

Odoo CRM

Click "Save" then "Apply Changes".

Once Odoo CRM is enabled, the user can log into the user portal by access the UCM web UI and entering their username and password, then they can navigate to **Other Features > CRM User Settings**, then they configure their account using username and password created on Odoo platform.

CRM User Settings

Enable CRM

☒

\* Username

This field is required

\* Password

This field is required

\* Database

This field is required

\* URL

This field is required

Login Status

Cancel

Save

CRM User Settings

## PMS

SoftwareUCM supports Hotel Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI→**Integrations**→**PMS**.

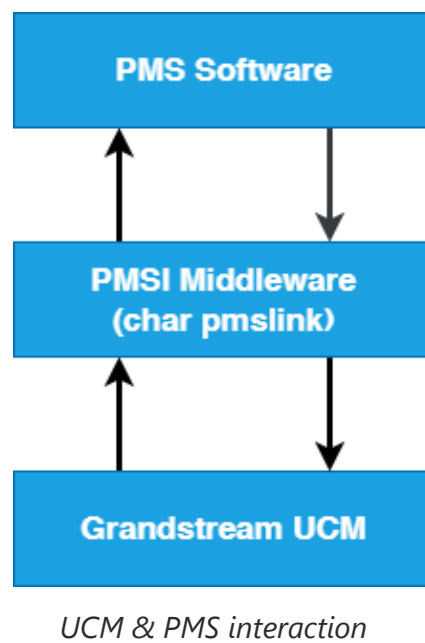
### Char Pmslink Connector

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

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

SoftwareUCM has integrated Char Pmslink which supports a large variety of PMS software providing the following hospitality features: Check-in, Check-out, set Room Status, Wake-up call, and more.

The following figure illustrates the communication flow between the UCM and PMS software, which is done through a middleware system (Char Pmslink) acting as an interface between both parties.



## HSC PMS

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

- PMS (Property Management System)
- PBX

Grandstream SoftwareUCM has integrated HSC PMS providing the following features:

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

Notes:

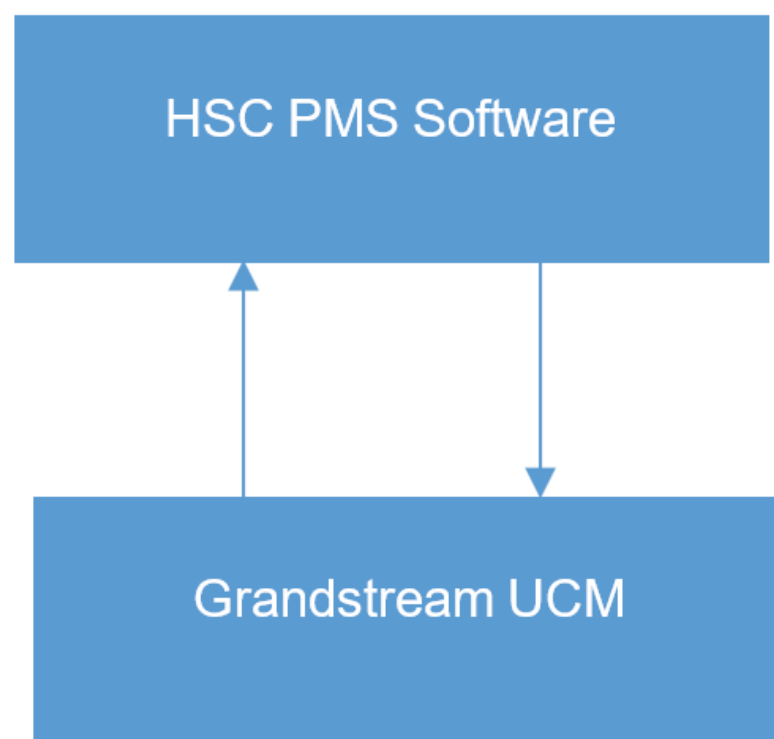
1. Added support for receiving HTTP GET keep-alive messages from HSC PMS. This will allow the PMS to be aware of its connection to the UCM and take the appropriate actions such as raising alarms, sending notifications, etc.
2. Added support for HTTP GET requests from HSC PMS to retrieve UCM extension information. UCM can provide the following information:

- extension – UCM extension number
- name – extension display name / CID name
- mwi – MWI state
- permission – permission level of the extension
- cftw – call forwarding always number
- dnd – DND state
- language – display language of the extension in ISO 639-1 format

The UCM should respond with either 200 OK or 404 responses.

### 3. Added HTTPS support

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



*UCM & HSC PMS interaction*

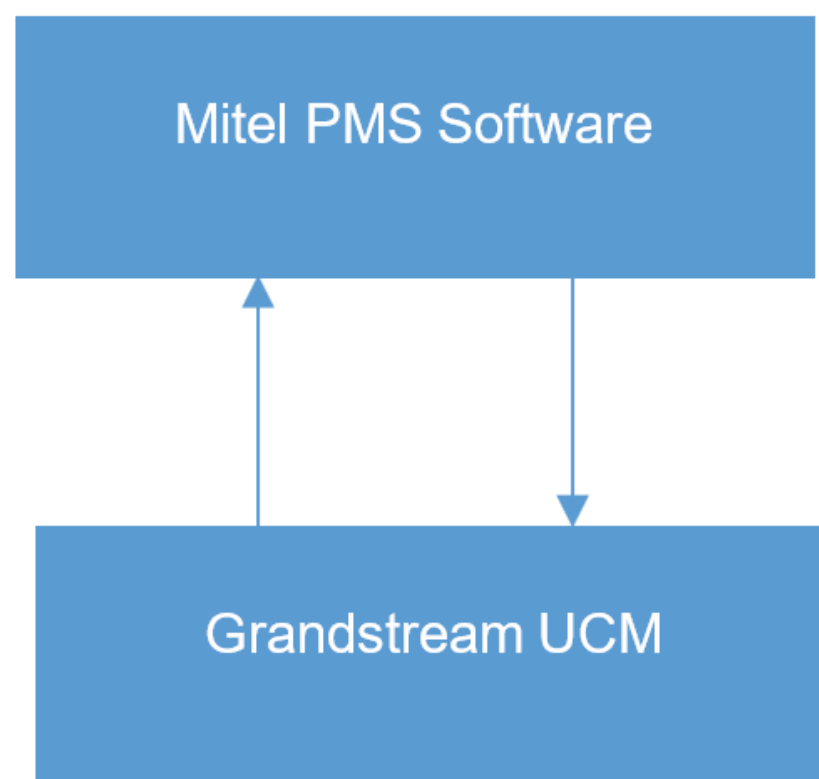
## Mitel PMS

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

- PMS (Property Management System)
- PBX

SoftwareUCM has integrated Mitel PMS providing the following hospitality features: Check-in, Check-out, set Room Status, Wake-up call, and more.

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



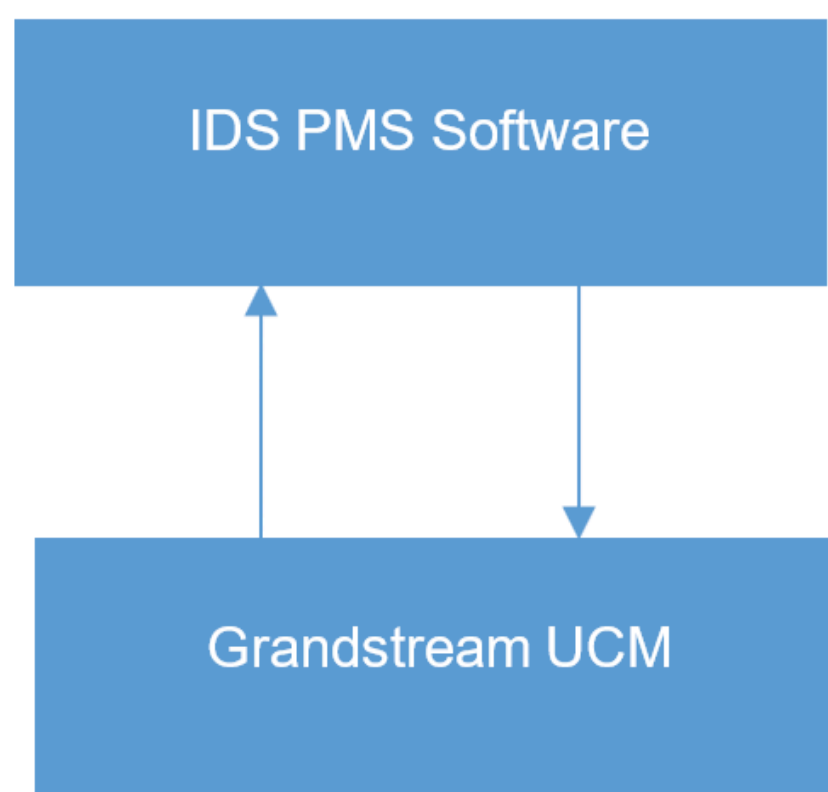
*UCM & Mitel PMS interaction*

## IDS PMS

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

- PMS (Property Management System)
- PBX

SoftwareUCM integrates IDS PMS to set room status, Mini Bar, wake-up calls, activate/deactivate dialing permissions, and more.



*UCM & IDS PMS interaction*

## PMS API

The PMS API allows users to use their own middleware to work with PMS systems instead of currently supported integrations.

Additionally, this API allows access to read and modify certain UCM parameters that current supported PMS integrations cannot. To use this, users must first enable and configure the HTTPS API settings.

For more details, please refer to online <https://documentation.grandstream.com/knowledge-base/https-api/>, Pmsapi section.

## Local PMS

SoftwareUCM offers a local Property Management System to give the user basic management features without having to purchase a PMS for the most basic property management actions. In addition to Room Management, Rooms Status for checking-in and checking-out, Wakeup Service, and Housekeeper functions, the SoftwareUCM allows a number of additional functions upon checking-out, like backing up voicemail recordings, clearing wakeup calls and Wave history automatically, in addition to resetting Wave’s password. The user can use the Local PMS feature to check-in and check-out clients from the web user interface.

- 1. To enable the Local PMS, please navigate to **Integrations > PMS**.
- 2. On the PMS Module menu, select “Local PMS”.

PMS

Basic Settings

PMS Module

Local PMS

Wakeup Prompt

Wake Call

Room Status Update Prompt

Default Room Status Update Prompt

Back Up Voicemail Recordings

☐

Sync Guest Name to Phone

☐

Automatically Clear Phone Call History

None

Automatically Clear Wakeup Calls

None

Automatically Clear Wave Chat History

None

Automatically Reset User/Wave Password

☐

Review Bill at Check-Out

☐

Currency Unit

Dollar: \$

PMS Basic Settings

Room Management

In Room Management tab, the user can create a room and affect up to two extensions to it. This will appear in Room Status tab, and from there the user can change the Check-in/Check-out.

Create New Room

CancelSave

\* Address:

1001

\* Room Number:

1001

\* Extension 1:

1000

\* Extension 2:

None

\* Call Privileges:

Internal

Create New Room

**Call Privileges** allows the administrator to set the level of call privilege of the room.

Room Status

Room Number	<input type="text" value="1000"/>
* Room Status	<input type="text" value="Available"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Guest Account	<input type="text"/>
Guest Category Code	<input type="text"/>
Guest Credit Money	<input type="text"/>
* Arrival Date	<input type="text" value="Select date"/> <input type="text" value="Select time"/>
* Expected Departure Date	<input type="text" value="Select date"/> <input type="text" value="Select time"/>
Language	<input type="text" value="Default"/>
* Call Privileges	<input type="text" value="Internal"/>
	<input type="button" value="Cancel"/> <input type="button" value="OK"/>

Check-in a Client

After clicking "OK" the client entry will be added to the list.

PMS

Basic SettingsRoom ManagementRoom StatusWakeup ServiceMaid

Check-in/Check-out HistoryCustom Room Status Codes

ROOM NUMBER	CHECK-IN STATUS	CHECK IN / CHECK OUT	ROOM STATUS	CUSTOMER NAME	GUEST CATEGORY CODE	ARRIVAL DATE	EXPECTED DEPARTURE DATE	OPTIONS
1000	● Checked in	Check Out	Available					
1001	● Not checked in	Check In	Not checked in	Arthur Morgan				
1002	● Not checked in	Check In	Not checked in	Bonnie MacFarlan				
1003	● Not checked in	Check In	Not checked in	Catherine Braitwaite				
1004	● Not checked in	Check In	Not checked in	John Marston				
1005	● Not checked in	Check In	Not checked in	Abigail Roberts				
1006	● Not checked in	Check In	Not checked in	Mary-Beth Gaskill				
1007	● Not checked in	Check In	Not checked in	Hosea Matthews				
1008	● Not checked in	Check In	Not checked in					
1009	● Not checked in	Check In	Not checked in					

Room Check-in

The user can click on **Check-in/Check-out Records** to view the history of the checked-in and checked-out guests.

## Note

The Call Privilege configured during a guest's check-in will be reset to the room's default call privilege upon guest check-out.

## Custom Room Status Codes

The user can customize the existing room statuses or add more statuses along with the corresponding name. The user can customize the status code to up to 16-digit code. To customize room status, please click on [Custom Room Status Codes](#).



Reset All

Press 1

Status Code

1

Room Status

Available

Press 2

Status Code

2

Room Status

Cleaning

Press 3

Status Code

3

Room Status

Repairing

Press 4

Status Code

4

Room Status

Vacant

Press 5

Status Code

5

Room Status

Dirty

Press 6

Status Code

6

Room Status

Closed

Custom Room Status Codes

Call Rate

In Call Rate page, the user can create different call rates for different call types. For example, the user can create a call rate which applies to national calls. The call rates can be differentiated by the prefix set for each call rate, the prefix corresponds to an outbound route pattern which allows national calls. Thus, the call rate applies accordingly.

PMS

Basic Settings

Room Management

Room Status

Call Rate

Wakeup Service

Mini Bar

Housekeeper

+ Add Rate

Delete Selected Rate

☐

Sequence

Prefix

Starting Cost

Starting Time (seconds)

Rate

Billing Unit (sec)

Options

No data

Add Call Rate

Call Charge = Starting Cost + Rate x Billing Unit

Prefix

Starting Cost

Starting Time (seconds)

\* Rate

\* Billing Unit (sec)

60

Cancel

OK

Add Call Rate

Prefix	Enter the prefix to be used for outgoing calls that should correspond with an outbound route pattern. If left blank, outgoing calls will not require a prefix, and any number can be dialed.
Starting Cost	Configure the device role. When set as a media server, This UCM’s PBX-related features will be disabled.
Starting Time (seconds)	Sets the starting time period for call billing. If the length of a guest’s external call does not exceed the starting time, only the starting cost amount will be charged. Example: If the starting cost is set to 0.2, and the starting time is set to 60, the first 60 seconds of a call will be charged a flat amount of 0.20 dollars (or other currency). If the starting time is set to 0 instead, the first 60 seconds will be free.

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 (Rate x Billing Unit = Telephone Cost).
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 (Rate x Billing Unit = Telephone Cost). Partial units are rounded up (e.g., If the billing unit is set to 60 seconds, and the call lasted 90 seconds (1.5 units), the guest will be billed for 120 seconds (2 units)).

**Note**

The user can create up to 500 call rate entries.

**Wakeup Service**

In some cases, guests will request the hotel staff to wake them up at a specific time, you can do that by configuring a wake-up time related to the room number of the guest, where the specific IP phone on that room will ring the extension related to the room number at that specific time, this option is supported on the integrated local PMS on the SoftwareUCM.

**Pending Wake-up**

The settings can be defined as follows:

- 1. Select the wake-up service tab, click to create a new wake-up schedule.

Add

PMS

Basic Settings

Room Management

Room Status

Call Rate

Wakeup Service

Mini Bar

Housekeeper

Pending Wake-Up

Wake-Up History

Add

Edit

Delete

Wake-Up Call Failure Notification

☐

Room Number

Action Status

Wake Up Date

Start Time

Repeat

Options

No data

Create New Wake Up Service

- 2. The configuration consists of defining some attributes such as :
  - o **Room number:** The room number on which the phone extension will ring at a specific time.
  - o **Start Time:** Define the time and the date of the wake up call
  - o **Repeat:** Select the frequency of the call: Daily, Weekly, Monthly.
  - o **Number of Redials:** Configures the number of times the system will repeat the call attempt after the task has started, but the call is not connected.
  - o **Redial Interval (minute):** The time interval between the end of the last call and the next initiated call when the Wake Up Call is not answered.

PMS > Create New Wakeup Service

\* Room Number

1000 ×

\* Start Time

2024-09-11

10:00

Repeat

No Repeat

\* Number of Redials

3

\* Redial Interval (minutes)

5

Cancel

Save

Create a New Wakeup Service

The newly displayed entry will be displayed as shown in the figure below:

PMS

Basic Settings

Room Management

Room Status

Call Rate

Wakeup Service

Mini Bar

Housekeeper

Pending Wake-Up

Wake-Up History

Add

Edit

Delete

Wake-Up Call Failure Notification

<input type="checkbox"/>	Room Number	Action Status	Wake Up Date	Start Time	Repeat	Options
<input type="checkbox"/>	1000	Pending	2024-09-11	12:00	No Repeat	<div><div></div><div></div></div>

Total: 1

<

1

>

10 / page

Goto

Canceled Wakeup Service

To delete a specific wake-up service, Click the icon and confirm the deletion by Clicking “OK” 

Delete?

Cancel

OK

Delete Wakeup Service

The administrator can configure to send a voicemail or an email notification in case the Wake Up call is not answered.

PMS > Wake-Up Call Failure Notification

Voicemail Notification

☒

Voicemail Destination

Voicemail

Email Notification

☒ Email Template

\* Receive Email

Add Email Address

Delivery Method

Periodic

\* Alert Sending Interval

5

minute(s)

Cancel

Save

Wake-up Call Failure Notification

The parameters of the “Wake-Up Call Failure Notification” page are:

Voicemail Notification	Enable to send a notification to the configured voicemail extension/group when a wake-up call has failed, meaning it has non-answered status. Default settings is “disabled”. <b>Note:</b> No notification will be sent if no failed wake-up call has occurred.
Voicemail Destination	Choose the voicemail/group to receive the failed wake-up call notifications.
Email Notification	Enable to send notifications of failed wake-up calls to the email addresses configured, based on the interval chosen. Any wake-up call that is not marked as “Answered” will be included in these notifications. If there are no failed wake-up calls, no alerts will be sent. Default settings is “disabled”.
Receive Email	Configure the e-mail address to receive failed wake-up call notifications. Maximum number of allowed email addresses is 5.
Delivery Method	Choose the delivery method of the email notifications. <ul style="list-style-type: none"><li>● <b>Real-time:</b> Notifications will be sent out immediately after alerts are generated.</li><li>● <b>Periodic:</b> Notifications will be queued up and sent out all at once every send cycle. The interval between each send cycle can be configured via the “Alert Sending Interval” option.</li></ul> Default setting is “Periodic”.
Alert Sending Interval	The frequency of notification emails for all failed wakeup calls that happen during that cycle in minutes, hours or days. Default setting is 5 minutes.
Key Settings	Set the settings for the key. You can select predefined statuses for a specific key, and you can also enter a custom status which will be sent on the notification email. The user can set a preloaded voice prompt or upload a custom one.

Wake-Up History

The Wake-Up History tab allows users to easily search for past wakeup calls by room number or answer status under a specified period. It is possible to download a CSV file containing the specific search results or a file with all historical wakeup call data.

PMS

Basic Settings

Room Management

Room Status

Call Rate

Wakeup Service

Mini Bar

Housekeeper

Pending Wake-Up

Wake-Up History

Download All Records

Download Search Result(s)

Clear

Room Number

Time:

2024-10-01

to

2024-10-11

Search

Reset

Room Number	Action Status	Answer Status	Wake Up Date	Start Time	Repeat	Options
1003	Executed	Answered	2024-10-11	10:43	No Repeat	
1001	Executed	No Answer	2024-10-11	10:39	No Repeat	

Wake-up History

Mini Bar

The mini bar feature is used to track the goods which have been consumed by the guests during their stay. This feature allows to add the consumed goods to the bill by the housekeeper.

Enable Mini Bar

☒

✖

Increase Mini Bar Usage Code

✖

Decrease Mini Bar Usage Code

✖

Global Tax Rate (%)

0

✖

Prompt

welcome

Upload Audio File

Skip Housekeeper and Password Authentication

☐

Enable Multi-Item Billing

☐

+ Add Purchasable Items

Code	Name	Price (\$)	Tax rate (%)	Options
No data				

Cancel

Save

Mini Bar

Enable Mini Bar	If enabled, feature codes can be used to increase and decrease usage of Mini Bar items.
Increase Mini Bar Usage Code	Dial this code + the item code to increase usage of the Mini Bar item for billing purposes.
Decrease Mini Bar Usage Code	Dial this code + the item code to reduce usage of the Mini Bar item for billing purposes.
Global Tax Rate (%)	Set the tax rate and configure it for an additional tax charge. If no personal tax is configured for a commodity, the global tax rate of the Mini Bar will prevail.
Prompt	This tone will be played when a housekeeper dials a number to enter the Mini Bar and can be used to indicate the corresponding goods code.
Skip Housekeeper and Password Authentication	If enabled, the default housekeeper code is 0000.
Enable Multi-Item Billing	If enabled, users can enter multiple goods in a single call by separating each good code with star ( * ).

Housekeeper

In order to create a new housekeeper, click on 

+ Add

 under UCM WebGUI→Integrations→PMS→Housekeeper.

PMS > Create New Housekeeper

\* Housekeeper Code

\* Password

Cancel

Save

Create New Housekeeper

Housekeeper Code	Enter the Code to use when the houskeeper wants to change the status of the room.
Password	Enter the password associated with the housekeeper.

Create New Housekeeper

Note

Please note that you can dial the **“Update PMS Room Status”** feature code, the **“Housekeeper”** feature code, and the **“Room Status”** feature code all at once to change the room status.

QueueMetrics

The QueueMetrics docking tool provides an interface for UCM system and QM docking. Pass the UCM call queue report to QueueMetrics in a richer form. QueueMetrics is a call center control platform that supports login and logout of frequently used agents in the call center, provides call reports, real-time queue monitoring and other functions.

QueueMetrics

Enable QueueMetrics Integration

☒

\* QueueMetrics URL

\* Username

webqloader

\* Webqloader Password

.....

Partition

Outbound Call Tracking

☒

Cancel

Save

QueueMetrics

Parameter	Description
Enable QueueMetrics Integration	Tick this box to enable QueueMetrics integration module.

QueueMetrics URL	Enter the URL of the QueueMetrics on-premise server you have installed. (i.e. http://xxx.xxx.xxx.xxx:8080/queuemetrics.).
Username	Please enter the username used to interface with QueueMetrics. This is typically the QueueMetrics webqloader user. Please confirm that the user is enabled to avoid connection failure.
Webqloader Password	Please enter the webqloader password.
Partition	Enter the data storage partition identifier
Outbound Call Tracking	If enabled, QueueMetrics will track the outgoing calls of all extensions. <b>Note:</b> Outbound Call Tracking is available only on the PBX.

## Google Services

Google Services integration allows integrating the SoftwareUCM with Google Calendar to automatically synchronize the created Multimedia and Onsite Meetings schedule with 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 Google Calendar Authorization configuration page, please enter the generated OAuth2.0 Client ID, OAuth2.0 Client Secret, and Authorized redirect URIs to integrate the SoftwareUCM 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

1. Click "Get Authorization Code".

Get Authorization Code

2

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

3. Click "Accept" on authorization page.

4

4. Copy the string to the Authorization Code input box, then click the "Authorize" button.

\* Authorization Code

Authorization

## Google Calendar Settings



On 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
<div><div><div></div><div>No data</div></div></div>		

Cancel

Save

For the full configuration guide, kindly follow the steps mentioned in the following how-to guide: <https://documentation.grandstream.com/knowledge-base/google-calendar-api-integration/>

Wave Integration & Expansion

Wave integrations include further expansion of the UC features offered by our solutions. These expansions includes integrating popular CRM solutions, like Odoo CRM, Oracle Netsuite, and Salesforce CRM with Wave to easily manage customer relationship directly through the calls received on Wave. Other add-ins include Whatsapp Business, Office356, Google Drive, and IPVideoTalk.

Wave Integration & Expansion

Outlook

SalesForce

Office 365

ZohoCRM

Whatsapp

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

CRM SYSTEM

ERP System

Project Management

QA SYSTEM

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 1.0.27.25

- Syslog logs will now be retained for up to 30 days. [[Syslog](#)]

## Firmware 1.0.27.18

- This is the initial release.

### Need Support?

Can't find the answer you're looking for? Don't worry we're here to help!

[CONTACT SUPPORT](#)