Grandstream Networks

CloudUCM

Endpoint Configuration Guide

Table of Contents

Overview

CloudUCM is a cloud PBX that integrates audio and video calls and collaborative work. Users can register extensions on terminals for communication, including using Grandstream IP phones, Wave Desktop applications, Wave Web clients, and Wave mobile applications for calls/meetings, chats, remotely managing and synchronizing extensions, cloud storage, alerts, statistics reports, etc.

This document describes how to configure CloudUCM services on IP phones so that users can register with CloudUCM on external and internal networks.

Configuring SIP Accounts on End Devices

IP phones can be registered to CloudUCM in external and internal network environment for internal communication and remote communication.

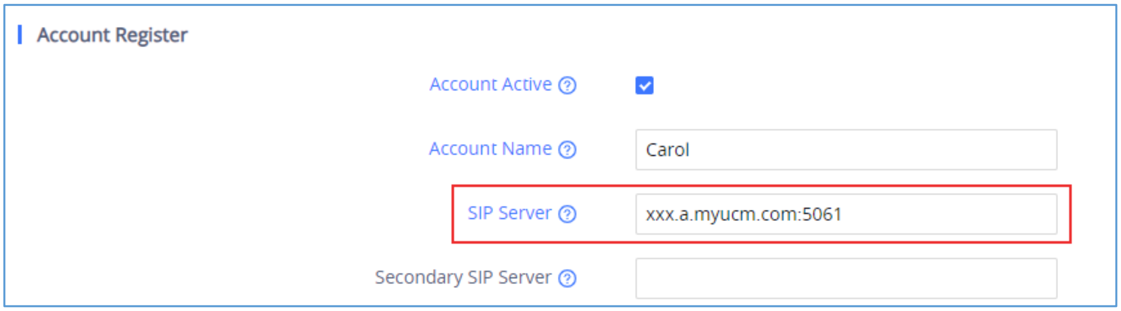
Method 1: Configure SIP Account from End Device Web User Interface

In this method, the user needs to configure the SIP server on the end device web GUI using the CloudUCM SIP Server Address and configure NAT to STUN. For SIP transport protocol, it must be set to TLS using TLS version 1.2 or 1.3.

Please refer to the below configuration example on GRP2604P.

Step 1: Log in GRP2604P web UI as admin, navigate to **Account → Basic Settings** page and configure the following:

- **SIP Server**: Enter the CloudUCM SIP Server Address. This information can be found under UCM **Web GUI → CloudUCM Plan** page.
- **DNS Mode:** Set to “SRV” (this parameter is recommended)
    - **DNS SRV Failover Mode:** Set to “Saved one until no response”
- **NAT Traversal**: STUN



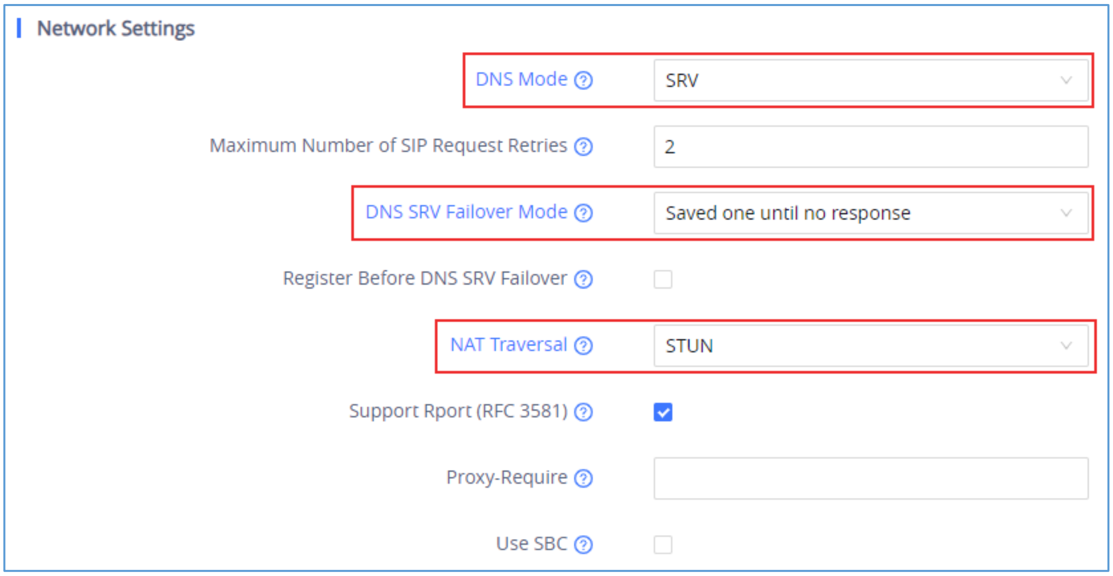
Account Register

Account Active ☑

Account Name: Carol

SIP Server: xxx.a.myucm.com:5061

Secondary SIP Server:



Network Settings

DNS Mode: SRV

Maximum Number of SIP Request Retries: 2

DNS SRV Failover Mode: Saved one until no response

Register Before DNS SRV Failover □

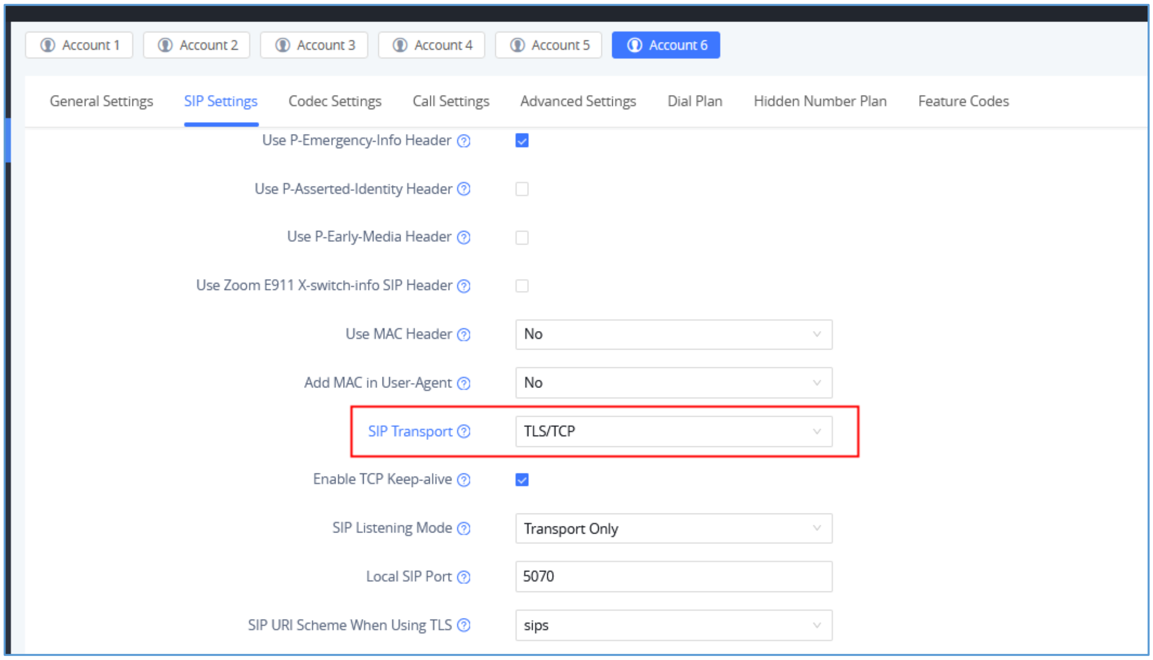
NAT Traversal: STUN

Support Rport (RFC 3581) ☑

Proxy-Require:

Use SBC □

Step2: Go to **Account** → **SIP Settings** and configure SIP transport to “TLS” or “TLS/TCP”.



Use P-Emergency-Info Header ☑

Use P-Asserted-Identity Header □

Use P-Early-Media Header □

Use Zoom E911 X-switch-info SIP Header □

Use MAC Header: No

Add MAC in User-Agent: No

SIP Transport: TLS/TCP

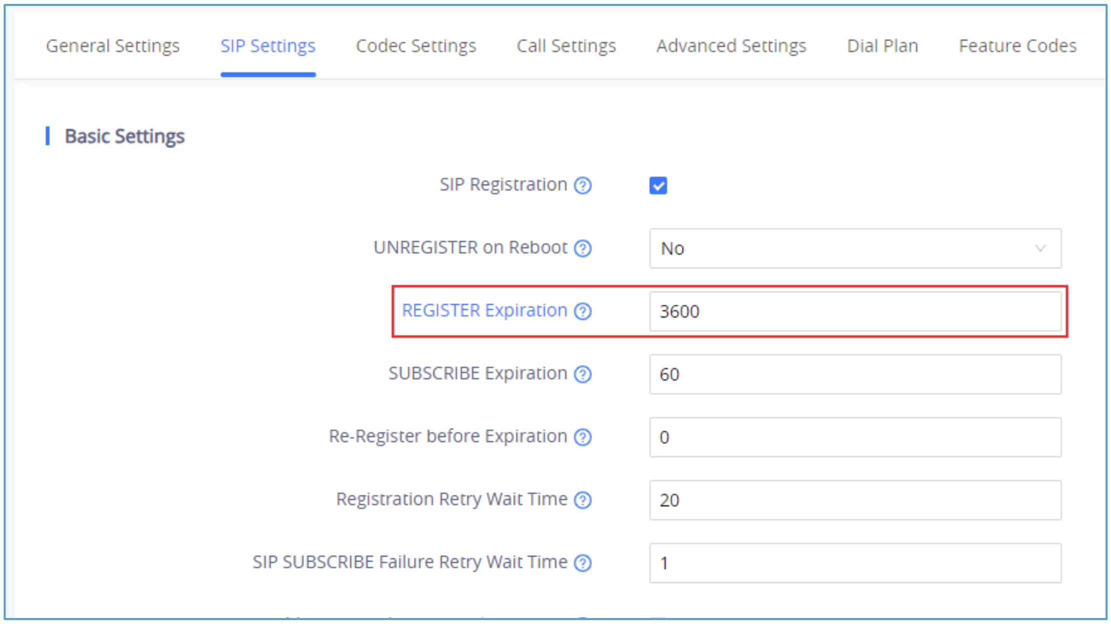
Enable TCP Keep-alive ☑

SIP Listening Mode: Transport Only

Local SIP Port: 5070

SIP URI Scheme When Using TLS: sips

Step3: Go to **Account → SIP Settings** page, you can configure REGISTER Expiration and Session Timer following the configurations below. The configurations are not required, but if your network is unstable, it is recommended to configure those settings, so that the CloudUCM services will be more stable.



Basic Settings

SIP Registration ☑

UNREGISTER on Reboot: No

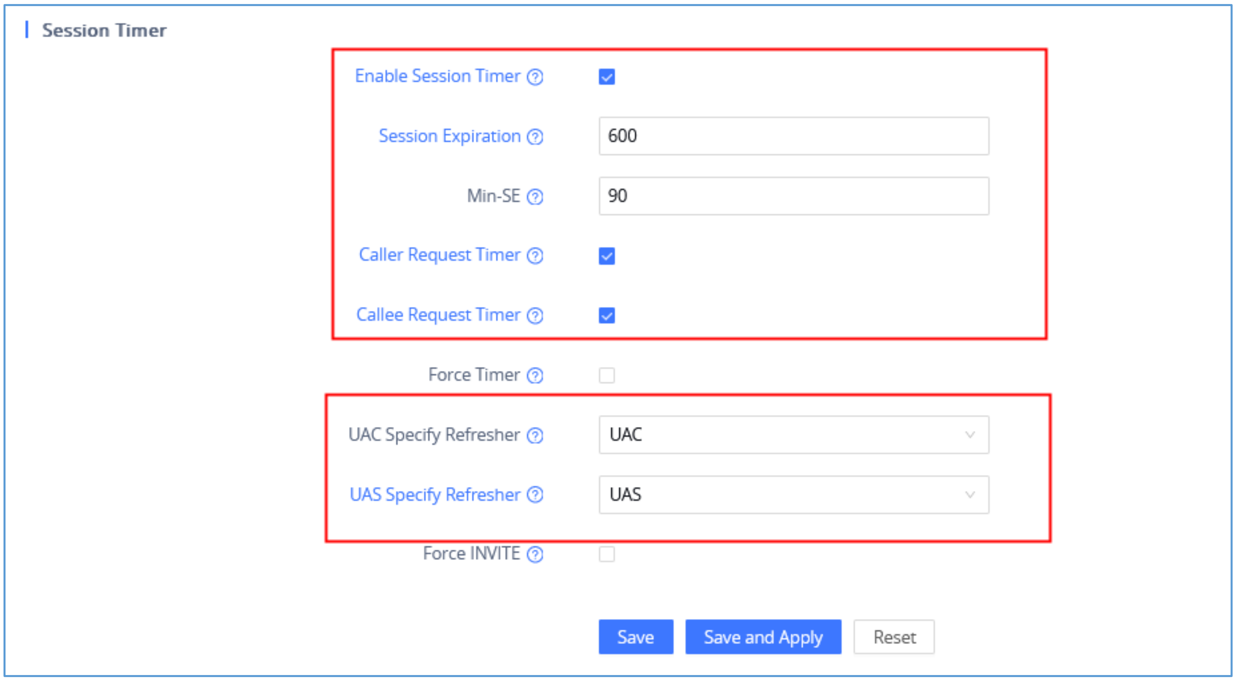
REGISTER Expiration: 3600

SUBSCRIBE Expiration: 60

Re-Register before Expiration: 0

Registration Retry Wait Time: 20

SIP SUBSCRIBE Failure Retry Wait Time: 1



Session Timer

Enable Session Timer ☑

Session Expiration: 600

Min-SE: 90

Caller Request Timer ☑

Callee Request Timer ☑

Force Timer □

UAC Specify Refresher: UAC

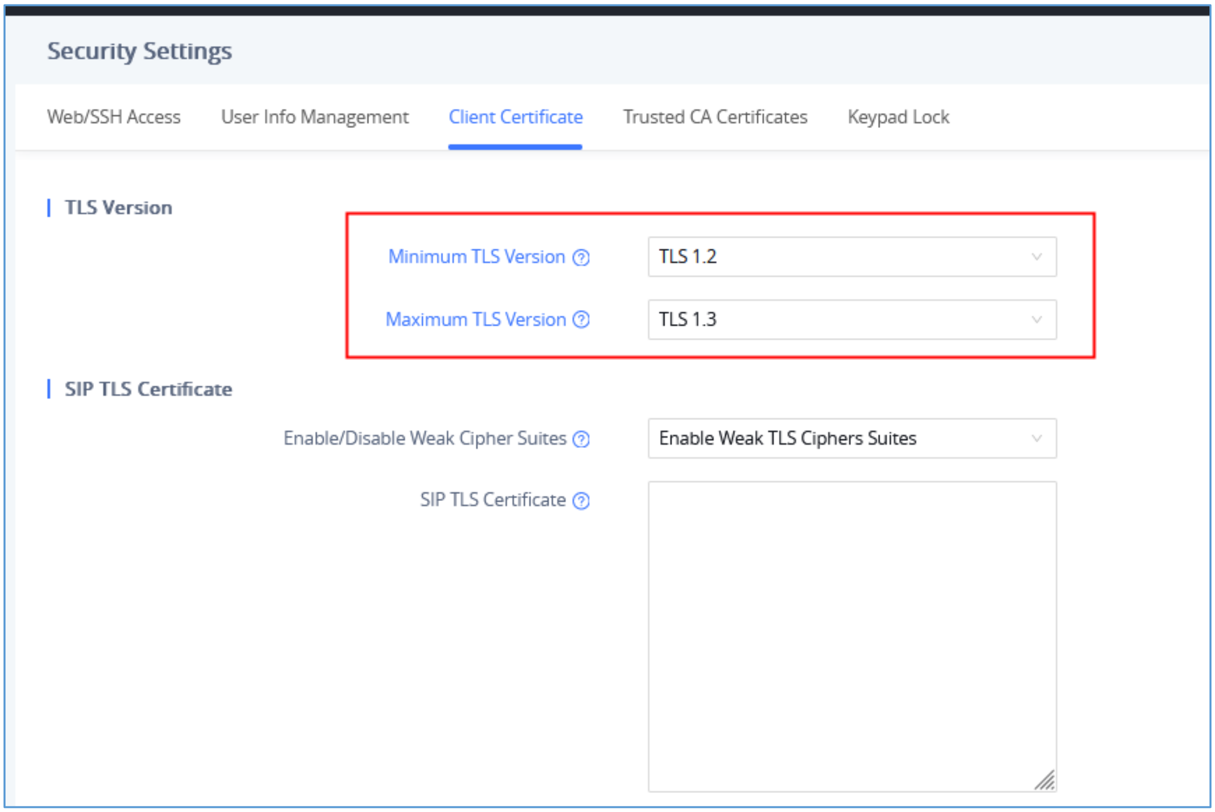
UAS Specify Refresher: UAS

Force INVITE □

REGISTER Expiration	3600
Enable Session Timer	Yes
Session Expiration	600

Min-SE	90
Caller Request Timer	Yes
Callee Request Timer	Yes
UAC Specify Refresher	UAC
UAS Specify Refresher	UAS

Step 4: Go to the phone's web **UI** → **System Settings** → **Security Setting** → **TLS** page, configure "Minimum TLS Version" and "Maximum TLS Version" to be 1.2 or 1.3.


Security Settings

Web/SSH Access | User Info Management | Client Certificate | Trusted CA Certificates | Keypad Lock

TLS Version

Minimum TLS Version: TLS 1.2

Maximum TLS Version: TLS 1.3

SIP TLS Certificate

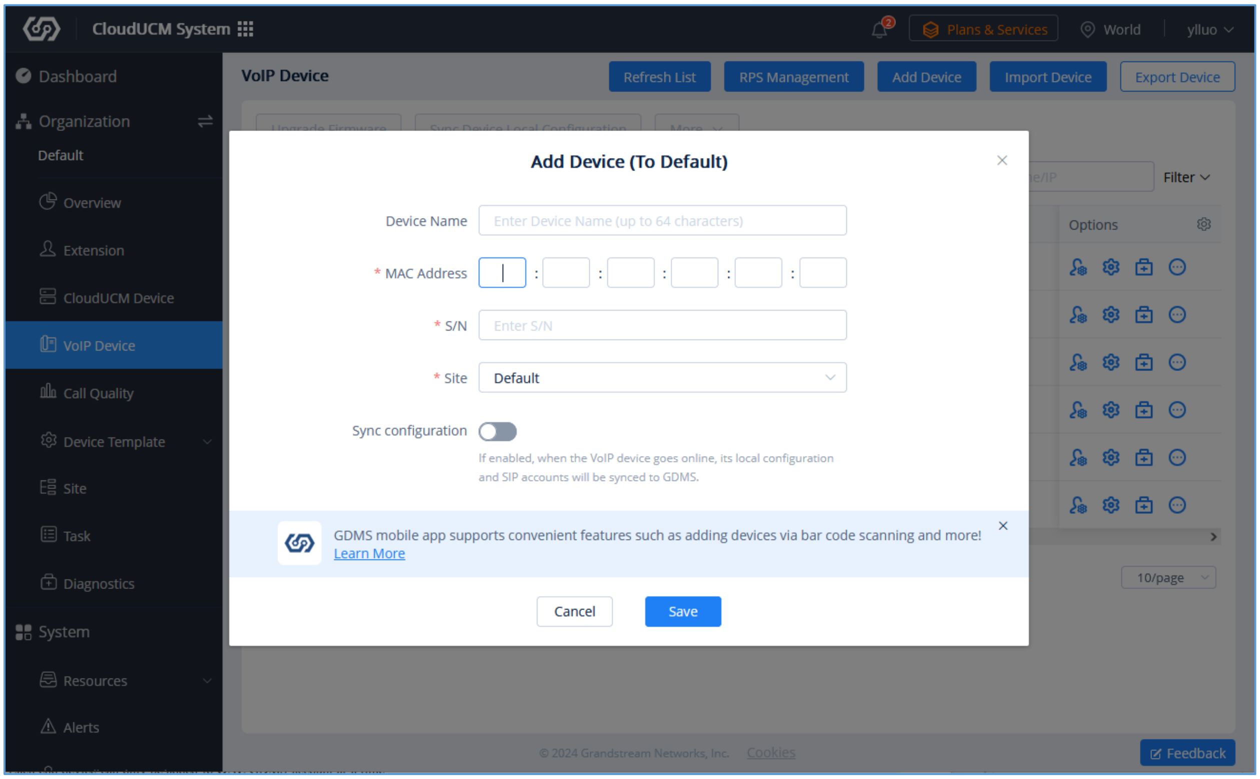
Enable/Disable Weak Cipher Suites: Enable Weak TLS Ciphers Suites

SIP TLS Certificate:

Method 2: Assign SIP Account for End Device from GDMS

In this method, user needs to log in GDMS to assign SIP account to the end device.

Step 1: Add the end device as VOIP Device to GDMS. Click on "Save" to save the configuration.



Add Device (To Default)

Device Name: Enter Device Name (up to 64 characters)

* MAC Address: _ : _ : _ : _ : _ : _

* S/N: Enter S/N

* Site: Default

Sync configuration: ○

If enabled, when the VoIP device goes online, its local configuration and SIP accounts will be synced to GDMS.

GDMS mobile app supports convenient features such as adding devices via bar code scanning and more! Learn More

Cancel | Save

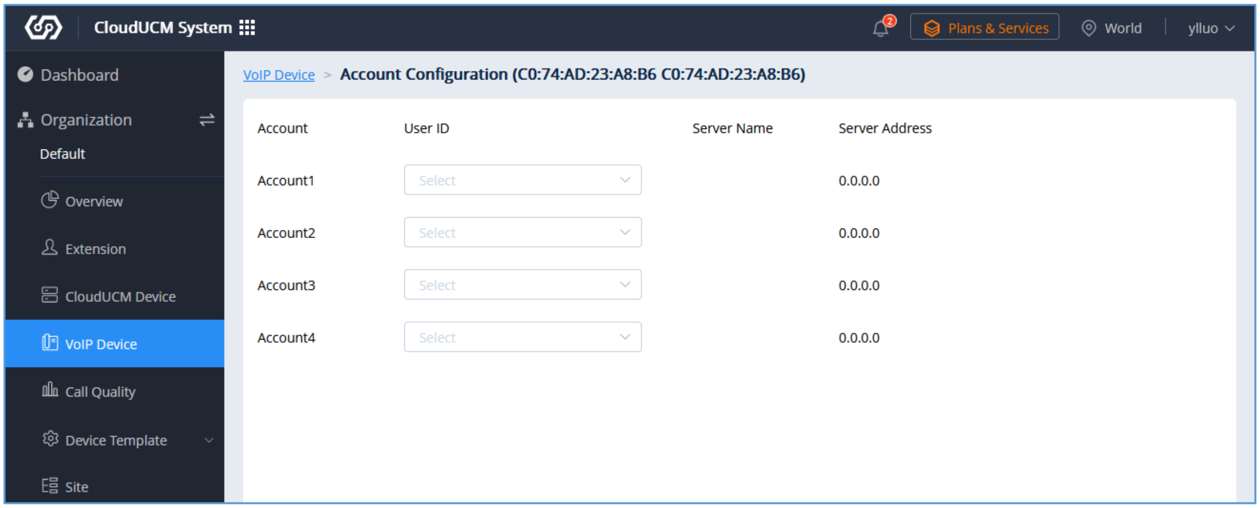
Notes:

- Each end device can only be added to ONE GDMS account at a time.
- Users can use the “Device Name”, “MAC Address”, or “Site Name” to search for the end device.

Step 2: There are two methods to assign the SIP account for the end device on GDMS.

Assign Method (1): Configure SIP Accounts from VoIP Device Page

1. In the VoIP Device Page, click on 👤 to enter the Account Configuration page.
2. In this page, users can choose to deploy the extensions from the Extension page to the device. They can also change the existing extension to another or remove existing extensions.
3. Save and apply the configuration.



VoIP Device > Account Configuration (C0:74:AD:23:A8:B6 C0:74:AD:23:A8:B6)

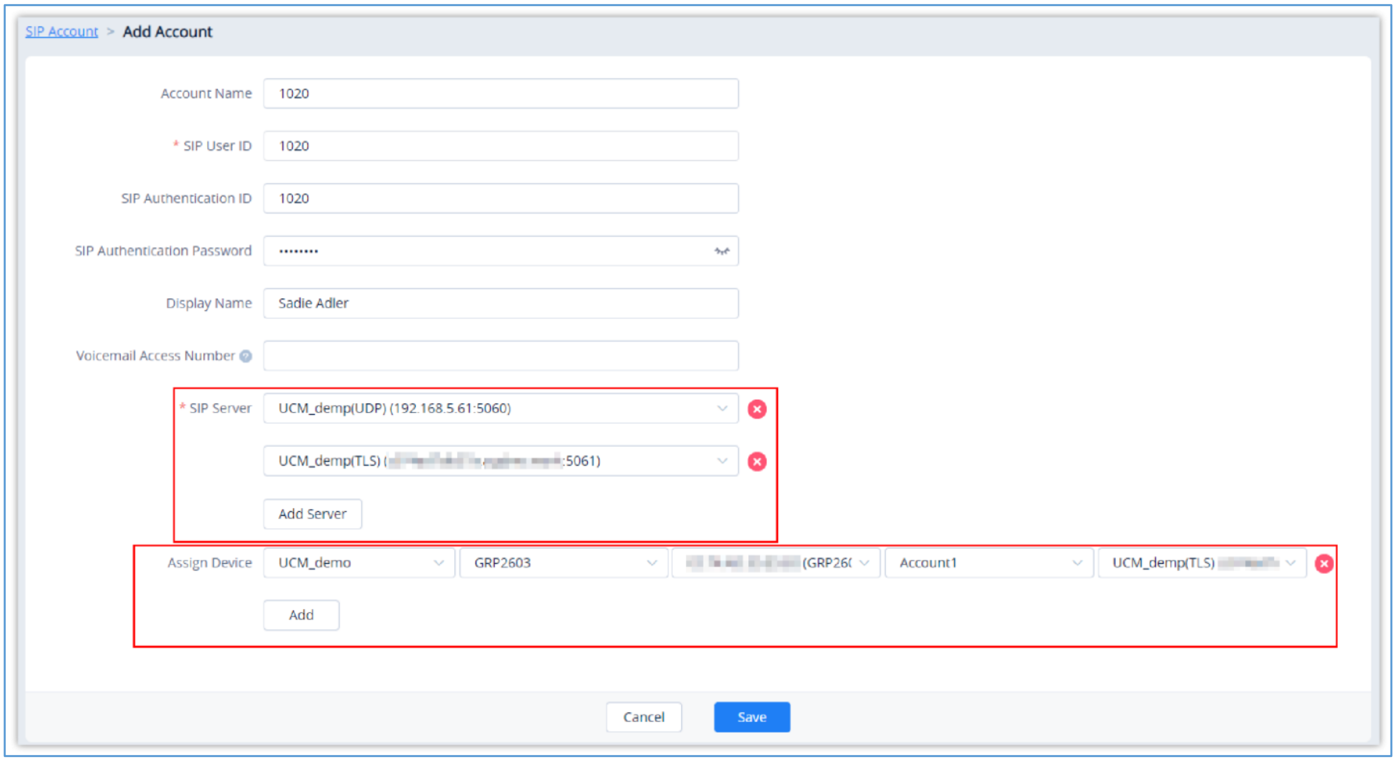
Account	User ID	Server Name	Server Address
Account1	Select		0.0.0.0
Account2	Select		0.0.0.0
Account3	Select		0.0.0.0
Account4	Select		0.0.0.0

Notes:

- If the device becomes offline during the account deployment, GDMS will push the settings once the device comes back online.
- Configurations from other methods such as via phone’s web UI, ZeroConfig, etc.… will not synchronize to GDMS.

Assign Method (2): Assign SIP Account from Extension Page

Step 1: Select “CloudUCM System” on the upper left page in GDMS and go to the Extension page, select the extension that needs to be assigned to the phone, and click to assign an account.



SIP Account > Add Account

Account Name: 1020

* SIP User ID: 1020

SIP Authentication ID: 1020

SIP Authentication Password: ••••••••

Display Name: Sadie Adler

Voicemail Access Number:

* SIP Server: UCM_demp(UDP) (192.168.5.61:5060)
UCM_demp(TLS) ([redacted]:5061)

Assign Device: UCM_demo | GRP2603 | [redacted](GRP26(| Account1 | UCM_demp(TLS) [redacted]

Step 2: Click the “Add Server” button and select the server address that the user wants to add for the extension.

Step 3: Assign the server to the phone. Select the site, device, MAC address, account location and the CloudUCM server address to assign.

Step 4: Click the “Save” option to complete assigning the extension to the phone.

Notes:

- When configuring the UCMRC server address to the phone, in order to make UCMRC work normally, the system will automatically issue the following configuration to the phone:

1. NAT Traversal: STUN
2. SIP Transport is configured as “TLS”.

3. The Session Timer Settings will be modified following the configurations below:

   - Enable Session Timer: Yes
   - Session Expiration: 600
   - Min-SE: 90
   - Caller Request Timer: Yes
   - Callee Request Timer: Yes
   - UAC Specify Refresher: UAC
   - UAS Specify Refresher: UAS

4. “Minimum TLS Version” and “Maximum TLS Version” to be 1.2 or 1.3.

- After assigning an account to the phone on the GDMS, if the phone cannot be registered or there is a problem with the call after registration, please go to the phone to check whether the configuration is correct according to section [CONFIGURING SIP ACCOUNTS on END DEVICES].
- IP phones which are not supported on GDMS cannot be remotely managed and deployed.
- Clients will not be able to edit SIP UserID, Authentication ID, Authentication Password, Display Name or Voice Mail Access Number from this page.
- The available devices for configuration will be the devices listed in the VoIP Device page.

Make Calls using IP Phones

After configurating the IP phones with CloudUCM service, users can use the phone to make audio/video calls and join GS Wave audio/video conferences.

Note: Presentation on end device IP Phones is currently not supported.