

GDMS Platform – User Guide

Thank you for using Grandstream Device Management System! GDMS is a cloud-based solution that provides the ability to easily manage Grandstream products before, during, and after deployment. GDMS separates subsystems independently based on different product lines: VoIP phone systems, PBX systems, network systems, and gateway systems.

PRODUCT OVERVIEW

Feature Highlights

- Intuitive deployment and management: GDMS’s easy-to-navigate web portal and batch operation support allow users to easily deploy and manage Grandstream devices located on several sites.
- All-in-one solution: GDMS offers a complete package that offers convenient management of devices and SIP server accounts on multiple sites, real-time monitoring and alerts, task scheduling and tracking, and device diagnostics.
- Supports presetting offline devices.
- One-click debugging: Easily collect system logs, network captures, and traceroutes with a click of a button.
- Supports UCM devices’ remote management and synchronizes SIP accounts to the GDMS platform in real time. All devices/SIP account one-stop management.
- Supports value-added services – UCM Remote Management Plan in GDMS platform. Supports remote external network communication for UCM clients.
- Supports value-added services – Cloud Storage Space in GDMS platform. UCM users can store more data and do not need to worry about storage space.
- Channel customer support: Allows automatic association of Grandstream ERP devices, allowing for the establishment of channel relationships and quick device allocation.
- Powerful API integration features: GDMS is compatible with ERP/CRM/OA platforms to improve workflow efficiency.

GDMS Technical Specifications

Functions	<ul style="list-style-type: none">● VoIP Device Management● PBX Device Management● Account Management● Device Configuration● Firmware Upgrade● Device Monitoring● Intelligent Alarm● Statistical Analysis● Channel Management● Task Management● PBX Backup● Plan & Service
Security and Authentication	<ul style="list-style-type: none">● HTTPS protocol and two-way certificate verification to ensure data security between devices and GDMS.

	<ul style="list-style-type: none"> • The key information of devices is encrypted and stored so that the key information cannot be obtained from the data storage. • The account password is encrypted and stored with sha256 algorithm to ensure the security of the account. • Serial number authentication of devices to ensure private rights of devices. • The privileges of the sub-users can be managed on the GDMS platform. • Support Multi-Factor Authentication.
Enterprise Features	<ul style="list-style-type: none"> • No limitations on the number of devices and SIP accounts that can be managed. • Configuration of all supported device parameters is supported, including but not limited to account settings, phone settings, network settings, system settings, maintenance, applications, profiles, and handsets. • Management of sites, group templates, and model templates.
Supported Device Models	<ul style="list-style-type: none"> • GXP series (Supported GXP21XX only, pending for other GXP models) • GXV series (Supported GXV3370/GXV3380/GXV3350) • GRP series • DP series • WP series • GVC series (Supported GVC3210 only, pending for other GVC models) • GWN series (pending to merge the existing GWN.Cloud system into GDMS platform) • UCM series • HT series

GDMS Technical Specifications

GETTING STARTED

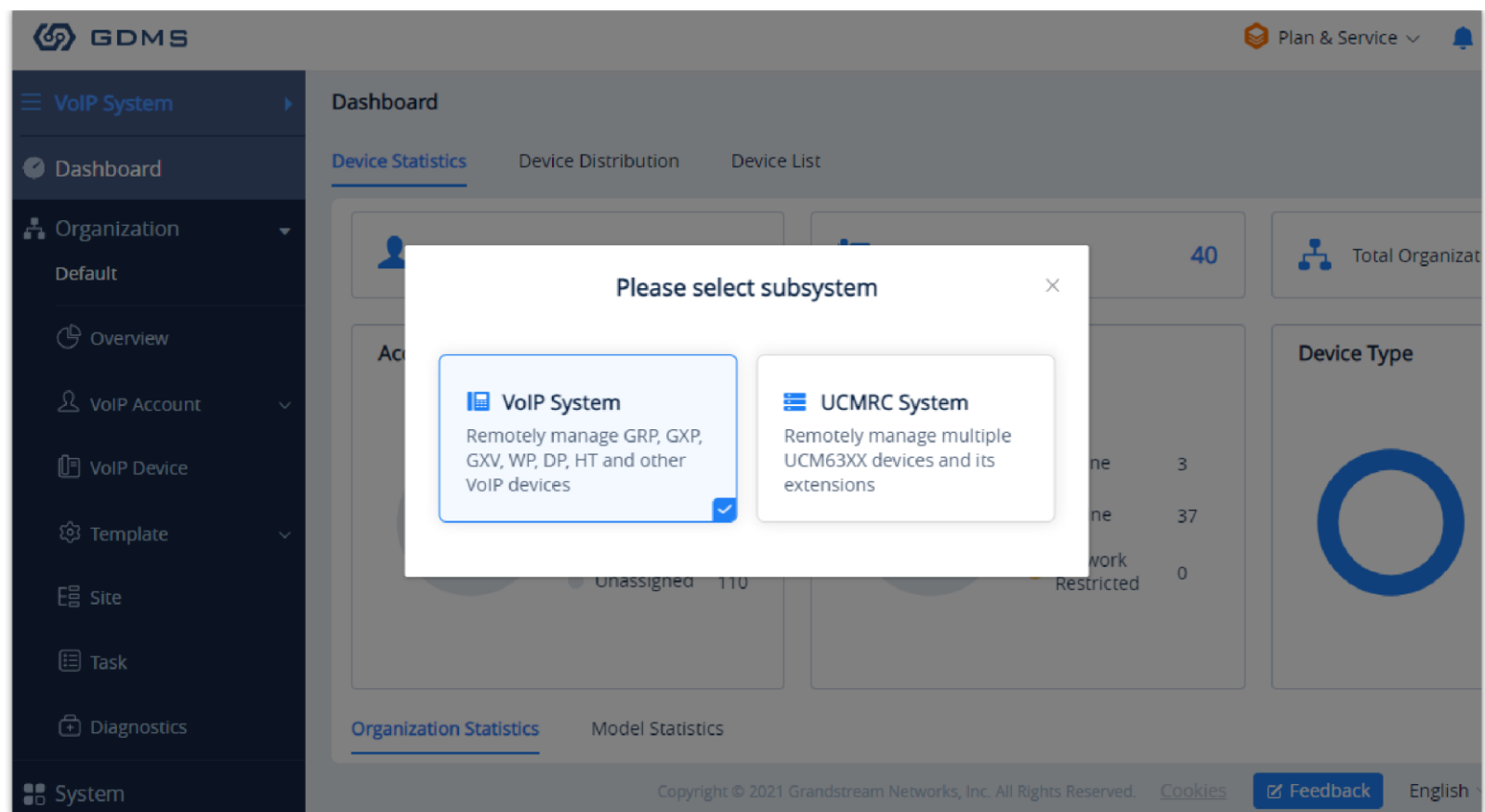
GDMS Overview

Main Functions Overview

For different models, users can select to use different systems in the GDMS platform.

Users can select to access the different sub-systems depending on the different managed devices models by clicking the system selection options in the left upper corner. As the screenshot shows below:

- **VoIP System:** Users can remotely manage IP phones such as GRP, GXP, GXV, WP, and DP models, and the system provides unified configuration, real-time monitoring, scheduling/executing tasks functions, etc.
- **UCMRC System:** Users can remotely manage UCM63xx devices and corresponding extensions, and the system provides remote access, monitoring, upgrade functions, etc. The UCMRC system provides a large cloud storage space, and it allows remote calls through external networks.



Select Sub Systems

Import Devices and Management

Users need to import the devices into the GDMS platform first to view the status and configuration of the devices and monitor the devices on the GDMS platform.

Channel vendors could acquire devices directly through ERP, and the channel vendors need to submit relevant certificates to Grandstream customer support.

Import SIP Accounts and Allocate to Devices

Users could import a batch of SIP accounts with Excel files, and allocate the batch of SIP accounts to devices. Users could complete all accounts configuration for all devices by importing a batch of SIP accounts to a batch of devices.

Configure Devices

- Configure devices by model: Once the device is associated with the GDMS platform, the device will be allocated with the configuration parameters according to the device model and located site.
- Configure devices by group: Manage the devices by certain rules and groups, and the GDMS supports pushing configuration files to all devices under a group.
- Configure a single device: Modify a specific device configuration in the Device list directly.
- Configure devices by configuration file: Users could upload the configuration file of the device into the GDMS platform directly.

Firmware Upgrade

GDMS platform supports upgrading a batch of devices' firmware by device model, site, firmware version range, and other conditions. It also supports upgrading the devices' firmware by a batch of MAC addresses of the devices.

Schedule Tasks

Users could schedule certain tasks for a certain period of time. For example, users could schedule firmware upgrade tasks and execute the task in the early morning, so that the task will not affect the device owners.

Alarm message and diagnostic

In case of malfunction or dangerous operation of the devices, the administrator will be alerted. The GDMS platform supports to allow administrators to diagnose faults of some devices to locate and resolve problems quickly.

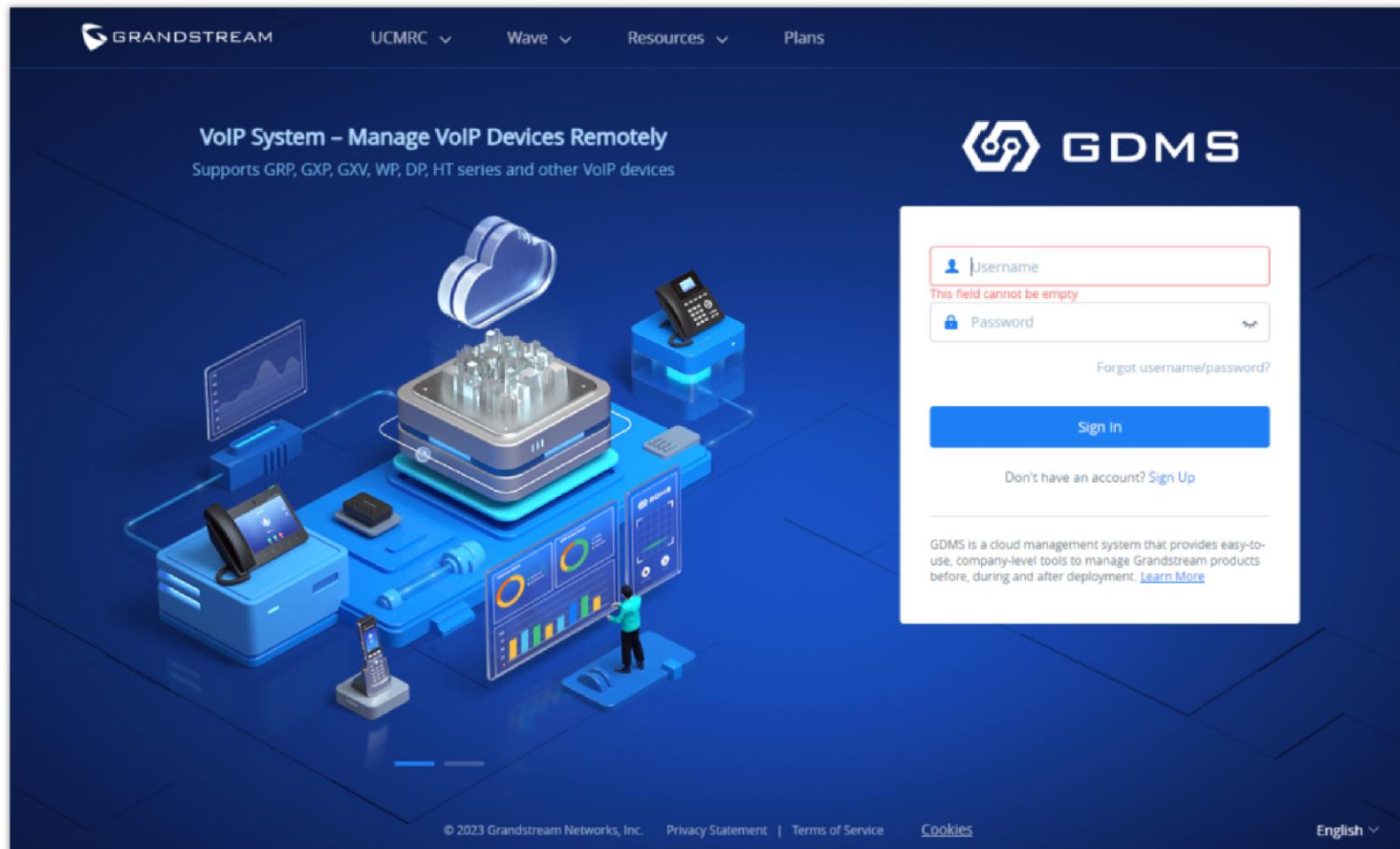
Prerequisites

- TR-069 feature needs to be enabled on the endpoints.
- Working Internet connection to access the GDMS platform.
- Endpoint devices are in the supported device list of the GDMS platform.

GDMS Account Registration

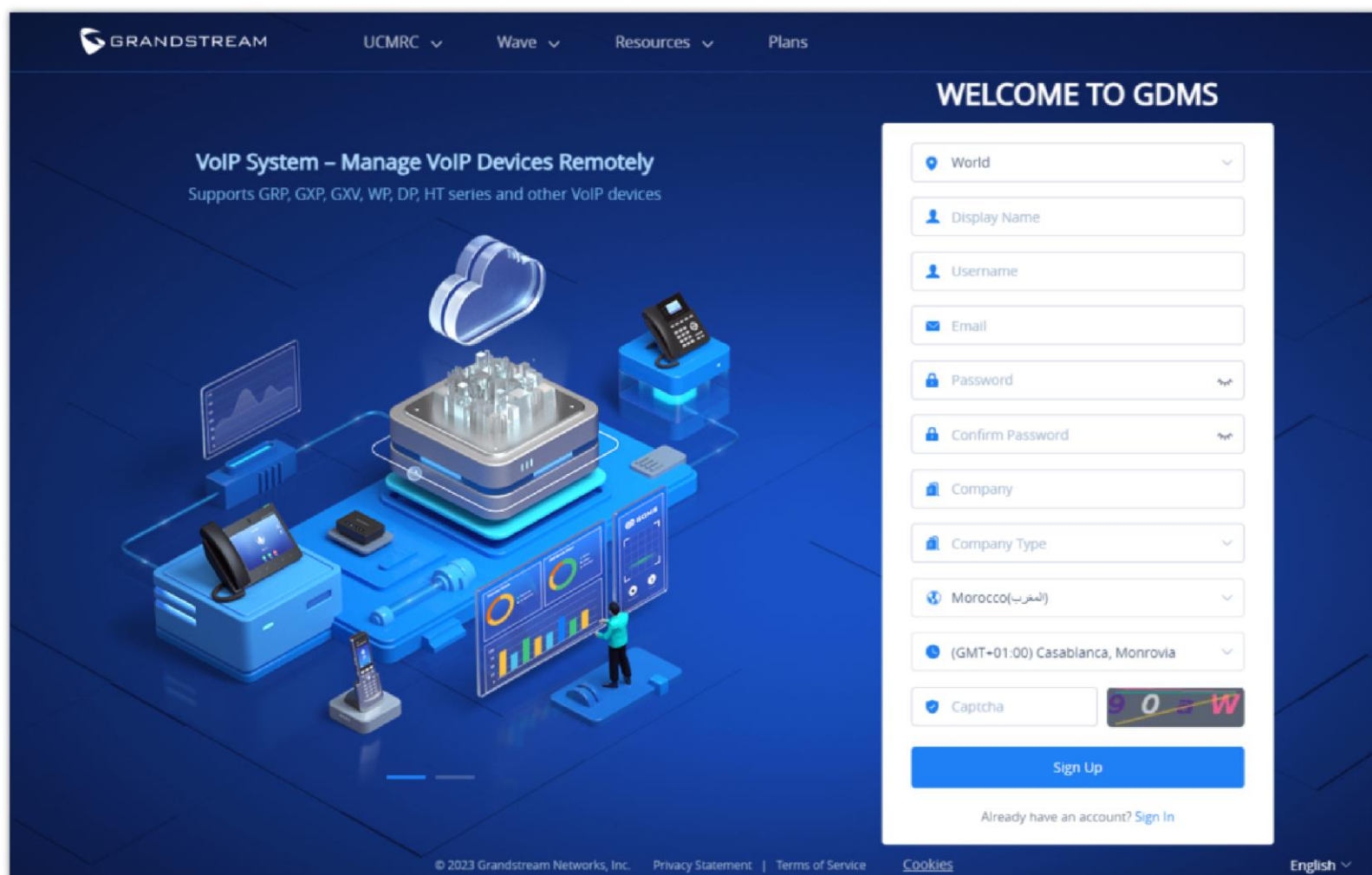
If using GDMS for the first time, an administrator will need to register for a GDMS account using the following steps:

1. Open the GDMS platform URL on the browser: <https://www.gdms.cloud>



Welcome to GDMS

2. Click on the **Sign Up** option to enter the registration page, and then fill in the following information:



Register GDMS Account

Customer Type	Select the customer type of the user. Available options are Provider, Reseller, System Integrator, and Enterprise User.
Email	Enter the email address that will be associated with the account. Account activation and password reset emails will be sent to this address.
Display Name	Enter the user's name
Username	Enter the login name of the GDMS platform
Password	Enter the password that will be used to log into GDMS
Confirm Password	Re-enter the password that will be used to log into GDMS
Company	Enter the user's company name
Country	Enter the located country of the user's company
Time Zone	Set up the current time zone
Verification Code	Enter the captcha displayed on the right of this field.

Register GDMS Account

- Once registration is complete, an account activation email will be sent to the configured email address. Follow the instructions in the email to activate the account and complete registration.

Supported Devices and Requirements

The current GDMS platform version supports the following device models.

Supported Device Models	
Audio Device	GXP21XX
	DP7XX
	GRP26XX
	WP8XX
	GHP6XX
	GSC36XX, GSC35XX
Video Device	GXV33XX, GXV34XX

Conference Device	GVC3210, GVC3220
Facility Access Device	GDS37XX
Video Surveillance Device	GSC3610, GSC3615, GSC3620
ATA Device	HT80X, HT81X
Gateway Device	GXW45XX
PBX Device	UCM63XX/A

Supported Devices

Connect with GDMS

The devices must be upgraded to firmware versions that are compatible with the GDMS platform. Otherwise, the devices will not be able to connect to GDMS. When the devices connect to the Internet, and the user has added this device to the GDMS account, the device will connect to GDMS automatically.

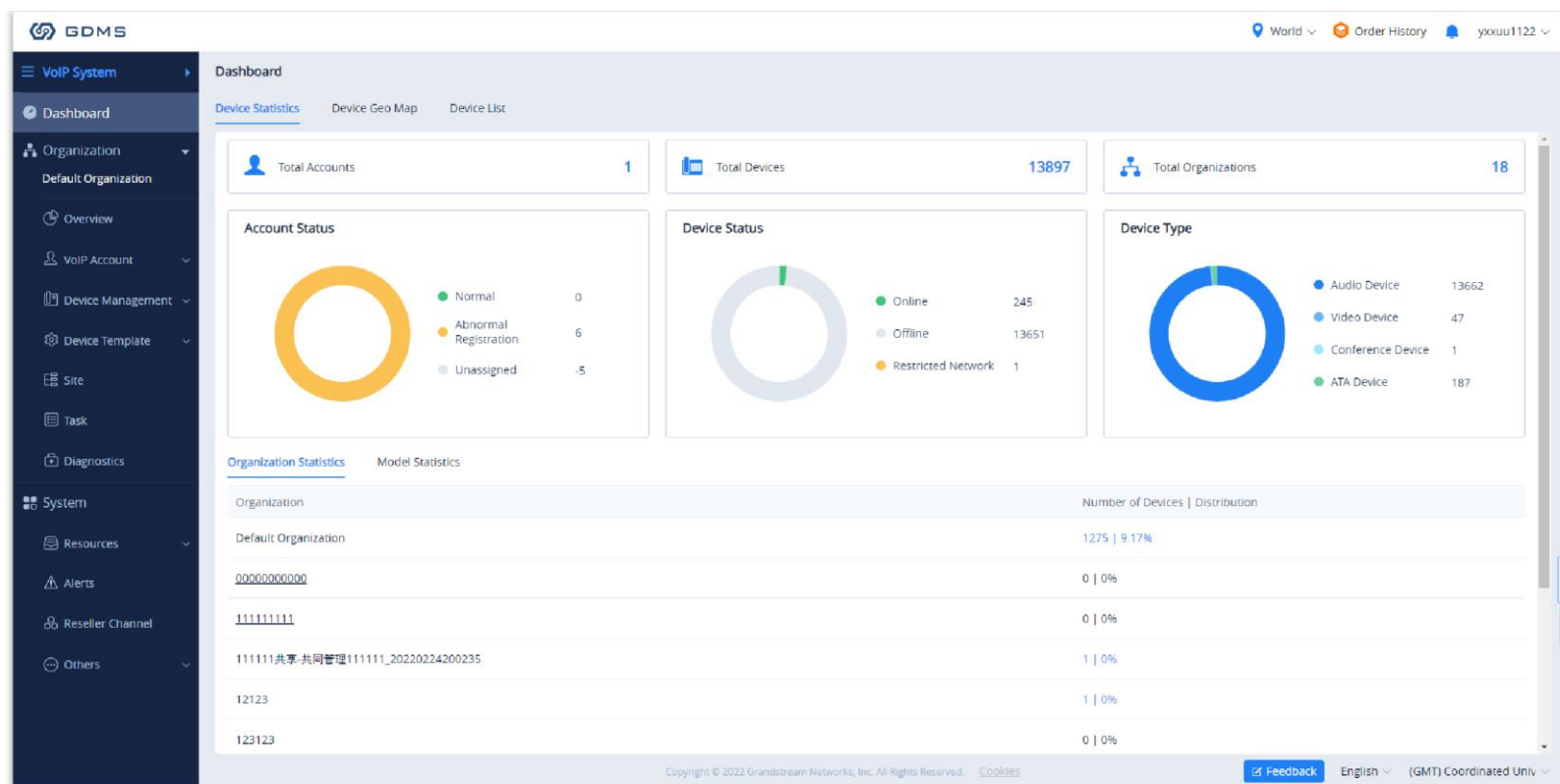
VOIP SYSTEM

Overview

Device Statistics

The Dashboard page provides an overview of the following information:

- Total Accounts
- Total Devices
- Total Sites
- Accounts Status
- Device status
- Device Type
- Site Statistics
- Model statistics



Overview

Module	Description
Total Accounts	Displays the total number of SIP accounts configured on GDMS.
Total Devices	Displays the total number of devices configured on GDMS.
Total Sites	Displays the total number of sites configured on GDMS.
Account Status	<p>Displays the total number of accounts currently registered, unregistered, and unallocated.</p> <ul style="list-style-type: none"> ◊ Normal: All devices which use this account are registered successfully. ◊ Abnormal: The account is unregistered on a device. ◊ Unallocated: This account is not allocated to any device.
Devices Status	<p>Displays the total number of devices currently online and offline.</p> <ul style="list-style-type: none"> ◊ Online: Device and GDMS platform network connection is normal. ◊ Offline: Device and GDMS platform lose network connection.
Device type	<p>Displays the total number of devices in each category: audio, video, and conferencing.</p> <ul style="list-style-type: none"> ◊ Audio devices: GRP series, DP series, GXP series, and WP series ◊ Video devices: GXV series ◊ Conference devices: GVC series
Site Statistics	Displays the total number of devices assigned to each site and the allocation of devices per site.
Model Statistics	Displays the total number of each device model, the percentage of total devices that each model makes up, and the distribution of different firmware per model.


Table 4: Overview Labels

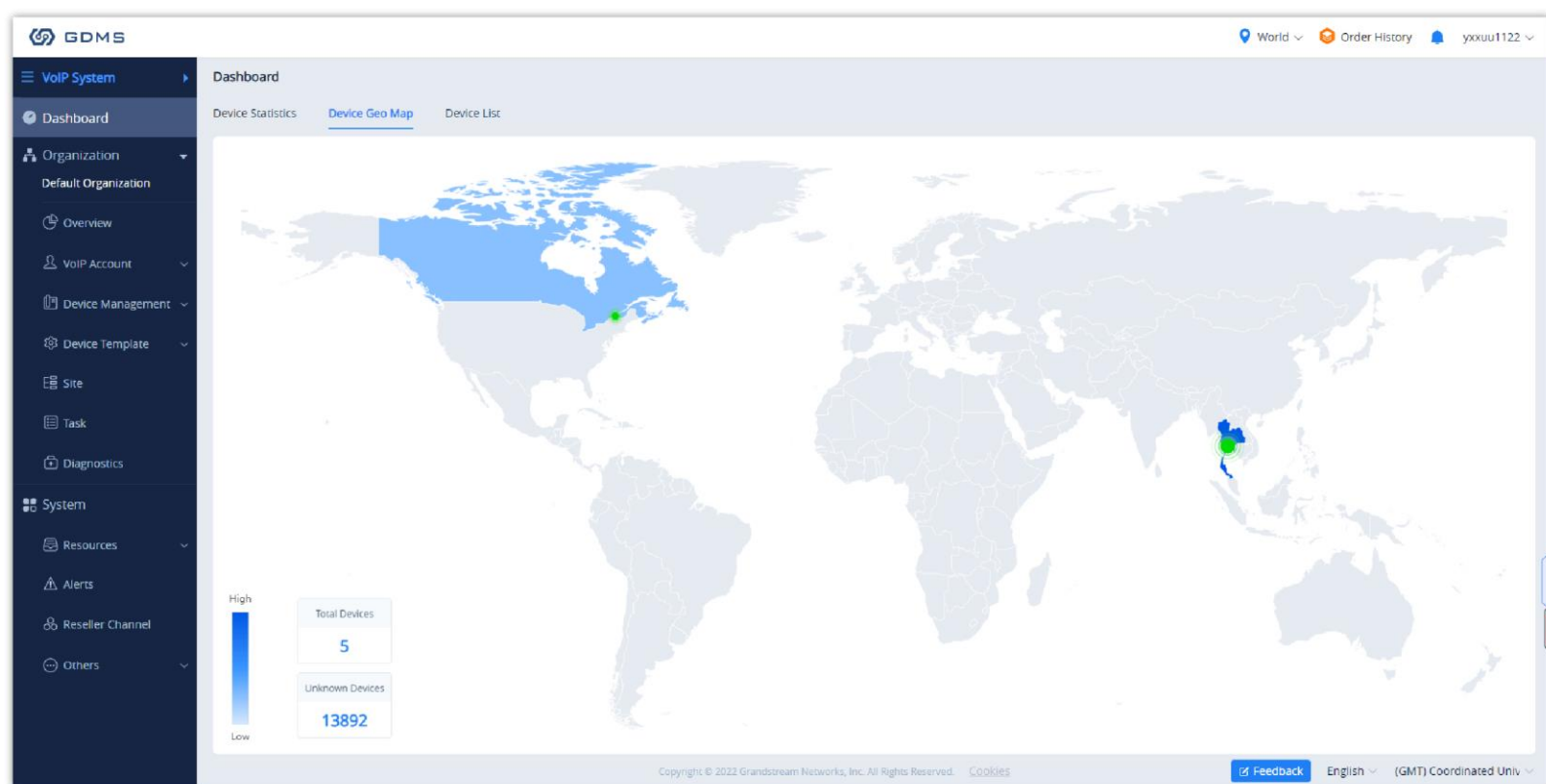
Model	Type	Number of Devices Distribution	Version Statistics
DP750	Audio Device	2 50%	
GRP2614	Audio Device	1 25%	
GV3370	Video Device	1 25%	
Total 3			

Model Statistics

Device Distribution

This menu will show the distribution map of the devices which have been associated with the enterprise.

- The dark blue area on the map shows that area has more associated devices, and the light blue area shows the area has fewer devices.
- Users could leave the cursor on the area to check the number of devices in that area.
- If a certain city has the devices, it will be marked with a green dot , and users could leave the cursor on the city to check the number of devices in that city. The user can click on the dot to see the devices list in this city.



Device Distribution

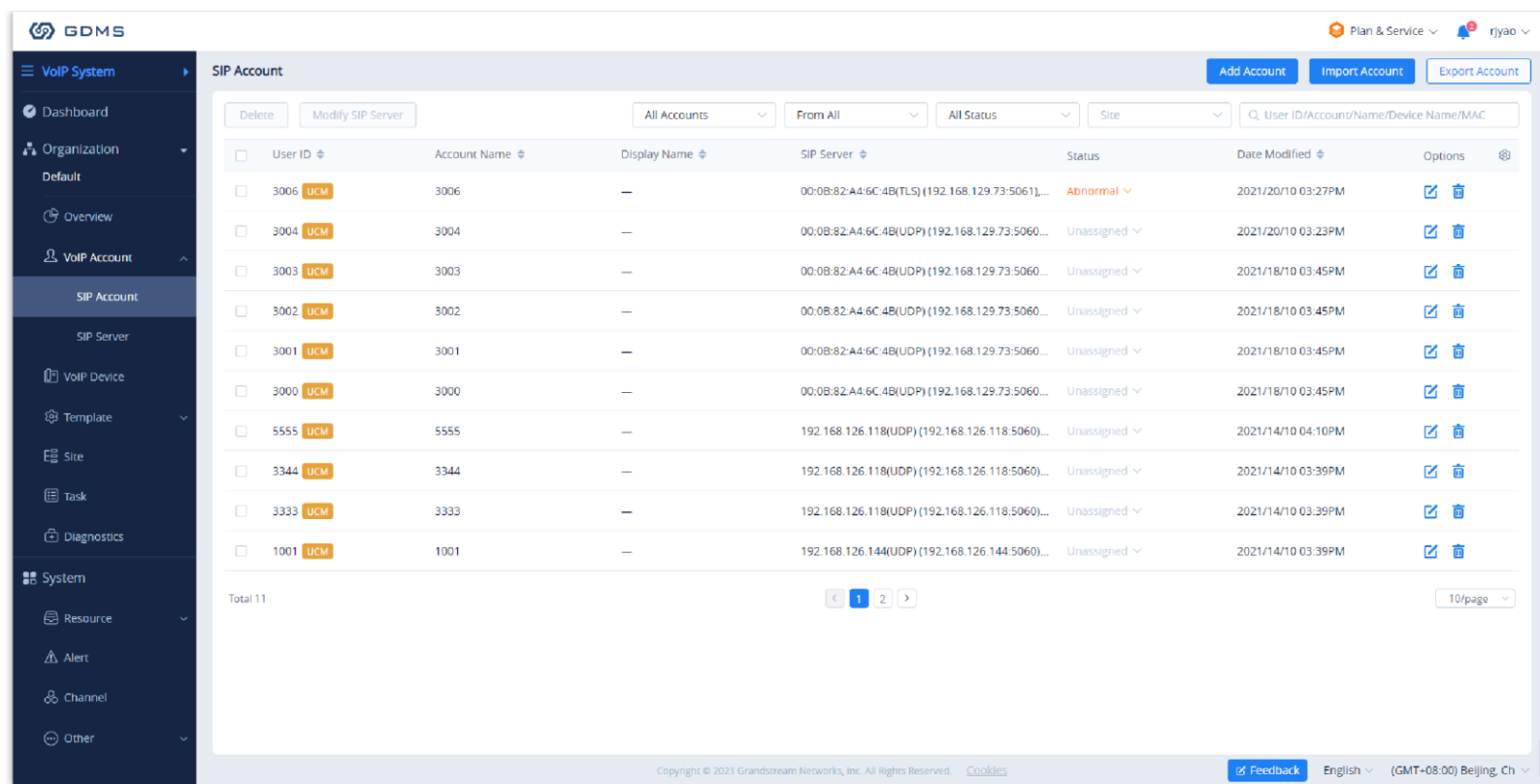
Overview

The Overview page displays all VoIP devices statistics information in the current organization.

Account Management

Overview

On the **SIP Account** page, users can manage SIP accounts across all configured SIP servers in GDMS, import a list of accounts for quick setup, and export a list of all accounts configured on GDMS.



Account Management

Status	Description
Status	<p>Normal:</p> <p>All devices using the account are registered, and the account is working normally.</p> <p>Abnormal:</p> <p>At least one device using this account is not registered. Possible reasons include:</p> <ul style="list-style-type: none"> The device is unable to register successfully. The account was modified through other means such as through the endpoint device web portal or provisioning. <p>Unassigned:</p> <p>No devices are using this account.</p>
From UCM	<p>UCM</p> <p>This represents the SIP accounts are synchronized from the UCM device. If the user modifies the SIP accounts in UCM device, the updates will be synchronized to GDMS platform.</p> <p>The user can only edit SIP server, assign device, and cannot edit other information.</p>

Table 5: Account Status Description



Operation	Description
Sorting	Click on the  buttons to sort the list in ascending/descending order based on a specific column.
Custom Display Option	Users could customize the displaying options on the list by clicking on option  on the right side of the list to select the displayed/hidden options.
Filter and Search	Filter accounts by status, site, and search for specific accounts by entering their user IDs, account names, or display names.

Table 6: Operation Description

Add SIP Server

The **SIP Server** page shows all of the SIP servers added to GDMS.

Add SIP Server

Server Name	Specifies an identity name for the SIP server. (Required)
SIP Server	This is a necessary option. Specifies the URL or IP address, and port of the SIP server. This should be provided by the VoIP service provider (ITSP).
Outbound Proxy	Configures the IP address or the domain name of the primary outbound proxy, media gateway, or session border controller. It is used by the phone for firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and only an outbound proxy can provide a solution.
Secondary Outbound Proxy	Sets the IP address or domain name of the secondary outbound proxy, media gateway, or session border controller. The phone system will try to connect the Secondary outbound proxy only if the primary outbound proxy fails.
Voice Mail Access Number	Sets if the phone system allows users to access the voice messages by pressing the MESSAGE key on the phone. This ID is usually the VM portal access number. For example, in UCM6xxx IPPBX, *97 could be used.
DNS Mode	<p>Defines which DNS service will be used to look up the IP address for the SIP server's hostname. There are three modes:</p> <ul style="list-style-type: none"> ◦ A Record ◦ SRV ◦ NATPTR/SRV <p>To locate the server by DNS SRV set this option to "SRV" or "NATPTR/SRV".</p>

<p>NAT Traversal</p>	<p>Specifies which NAT traversal mechanism will be enabled on the phone system. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> ◦ NAT NO ◦ STUN ◦ Keep-alive ◦ UPnP ◦ Auto ◦ VPN <p>If the outbound proxy is configured and used, it can be set to “NAT NO”.</p> <p>If set to “STUN” and the STUN server is configured, the phone system will periodically send a STUN message to the STUN server to get the public IP address of its NAT environment and keep the NAT port open. STUN will not work if the NAT is a symmetric type.</p> <p>If set to “Keep-alive”, the phone system will send the STUN packets to maintain the connection that is first established during the registration of the phone. The “Keep-alive” packets will fool the NAT device into keeping the connection open and this allows the host server to send SIP requests directly to the registered phone.</p> <p>If it needs to use OpenVPN to connect to the host server, it needs to set it to “VPN”.</p> <p>If the firewall and the SIP device behind the firewall are both able to use UPnP, it can be set to “UPnP”. Both parties will negotiate to use of which port to allow SIP through.</p>
<p>Proxy-Require</p>	<p>Adds the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server.</p>
<p>Additional Settings</p>	<p>Users could add the custom fields below. Some custom fields are only available for certain device models:</p> <ol style="list-style-type: none"> 1. Secondary SIP Server 2. Failover SIP Server 3. Prefer Primary SIP Server 4. Primary IP 5. Backup IP 1 6. Backup IP 2 7. DNS SRV Failover Mode 8. Use NAT IP 9. SIP Diff-Serv 10. RTP Diff-Serv 11. Tel URI <p>For detailed filling rules, please refer to the User Guide of the devices.</p>

Table 7: Add SIP Server

Upon adding the SIP server, it will appear in the SIP Server list. Entries in the list can be edited or deleted.

Server Name	Server Address	Account Number	Options
Test (unavailable)	192.168.100.100	1	[Edit] [Delete]
192.168.121.22	192.168.121.22	0	[Edit] [Delete]
wll's server	192.168.200.105	20	[Edit] [Delete]
yoxu Server	192.168.120.254	9	[Edit] [Delete]

Finish Adding SIP Server to GDMS

Add SIP Account

The **SIP Account** page shows all of the SIP accounts added to GDMS.

Add SIP Account

Account Active	Activates/deactivates the SIP account.
Account Name	This is a necessary option. Specifies an identity name for the SIP account.
SIP User ID	This is a necessary option. Configures user account information provided by your VoIP service provider (ITSP). It is usually in the form of digits similar to a phone number or actually a phone number.
SIP Authentication ID	This is a necessary option. Configures the SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
Password	This is a necessary option. Configures the account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purposes.
Name	Configure the display name of the SIP account. This option will be used for Caller ID display. The configured content will be included in the From, Contact, and P-Preferred-Identity headers of the SIP INVITE message
Voicemail Access Number	If the SIP Server also configures this item, this configuration will prevail.
SIP Server	This is a necessary option. Users need to select the SIP server for the SIP account. If there is no available SIP server for the current SIP account, users could click on the "Add Server" option to add a new SIP server for the SIP account.

Add Server	If the user needs to configure multiple SIP server addresses for a single SIP account, such as the UDP/TLS protocol server address (The UCM63xx device which purchases UCM RemoteConnect plan can synchronize multiple protocol server addresses to the GDMS platform), the user can configure it and assign to devices separately.
Assign device	This option will allow assigning a specific device to this account.

Allocate to Devices:

To associate devices currently in GDMS with the new SIP account, click on the **Add** button at the bottom of the screen and enter the following information:

Assign Device

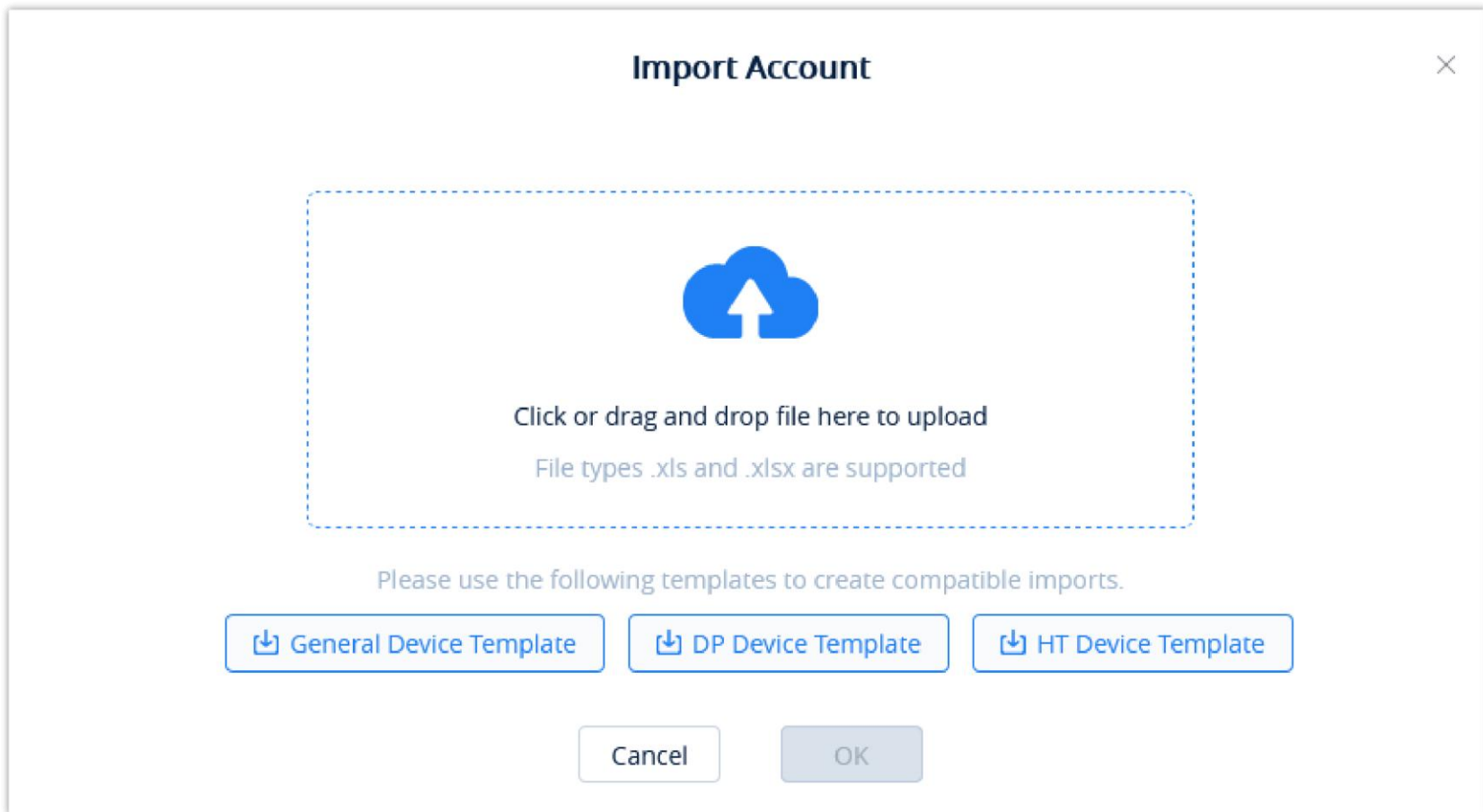
Site	This option is used to set which site this device belongs to.
Select Device Model	This is a necessary option. Users need to select the device model to which the account will be allocated.
Select Device MAC Address	This is a necessary option. Users need to select the device MAC address to which the account will be allocated.
Select Account Index	This is a necessary option. Users need to select the account index to which the account will be allocated to (e.g. Account 1 – Account 16). If the account location has a configured account, the account number will be displayed.
Select Server Address	This is a necessary option. Users can select the SIP Server address for the device, such as the UDP server address or UCM RemoteConnect server address.

- !
 - Assigning accounts to DP devices and HT devices from this page is currently not supported. Please use the account importing feature or the Device Management page to manage SIP accounts on DP devices and HT devices.
 - If a device is not on GDMS, users will be unable to allocate a SIP account.

Batch Import SIP Account

GDMS platform supports to allow users to import a batch of SIP accounts and SIP servers to the system and allocates them to the devices via Excel files.

1. On the **SIP Account** page, click on the **Import Account** button. The following window will appear:



Import SIP Account

2. Click on either the Download **General Device Template** button, Download **DP Device Template**, or Download **HT Device Template** button to get a template that will be used to import account and server information.

Account Name	*SIP Server	*SIP User ID	Authentication ID	Authentication Password	Display Name	Voice Mail Access Number	Outbound Proxy	Device MAC Address	Account Index

Import Account Template – General Device Template

Account Name	*SIP Server	*SIP User ID	Authentication ID	Authentication Password	Display Name	Voice Mail Access Number	Outbound Proxy	DP MAC Address	Account Index	Profile	HS Mode

Import Account Template – DP Device Template

Account Name	*SIP Server	*SIP User ID	Authentication ID	Authentication Password	Display Name	Voice Mail Access Number	Outbound Proxy	HT MAC Address	Port Type(FXS/FXO)	Port Index	Profile

Import Account Template – HT Device Template

Account Name	This is an optional option. Users need to set the identity name for the SIP account.
---------------------	--

SIP Server	This is a necessary option. Users need to input the SIP server address. If the SIP server does not exist in the GDMS platform, the GDMS platform will create the SIP server in the system.
SIP User ID	This is a necessary option. Configures user account information provided by your VoIP service provider (ITSP). It is usually in the form of digits similar to a phone number or actually a phone number.
SIP Authentication ID	This is a necessary option. Configures the SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	This is a necessary option. Configures the account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purposes.
Display Name	Configure the display name of the SIP account. This option will be used for Caller ID display. The configured content will be included in the From, Contact, and P-Preferred-Identity headers of the SIP INVITE message.
Device MAC Address	Input the device MAC address: e.g. 00-15-65-1A-2B-3C; 00:15:65:1a:2b:3c; 0015651a2B3c
Account Index	Users need to select the account index to which the account will be allocated (e.g. Account 1 – Account 16). If the current account location has a configured account, the configured account will be replaced with the new account information.
Profile	For DP devices and HT devices only. Enter the profile that the account will use (e.g. Profile1, Profile2, etc.). If multiple different SIP servers use the same profile, the import will fail.
HS Mode	For DP devices only. Enter the HS mode for the account. Available options are “Circular”, “Linear”, “Parallel”, and “HSx”, where x can be 1 to 5.
HS1-HS5	For DP devices only. Users could configure the Line for each handset from Line 1 to Line 10. Each SIP account can be allocated to different handsets.
Port Type (FXS/FXO)	This option is valid only for HT devices. Input the port type which will be assigned to the device. Users could select FXO port type or FXS port type.
Port Serial Number	This option is valid only for HT devices. Input the port serial number which will be assigned to the device. Users could input the port serial number from Port 1 to Port 10.
Search Group	This option is valid only for HT devices. Users could select the search group between None (default), Active, and other port serial numbers beside their own.

Import Account Template Options

- Once the template is filled out, drag, and drop the file to the upload window or select the file from your PC. Click on the **Import** button to confirm the import.
- When the Excel file is imported into the GDMS platform successfully, the GDMS platform will prompt the execution result. If there is data that failed to be imported, the user could export the failed data and re-edit the Excel file.

Examples:

1. If the user wants to allocate 1 SIP account to multiple devices, the 1st SIP account information will be the correct information to allocate to the devices.

Please see the example below, the SIP account display name “Squuang” will be allocated to the involved devices:

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	Device MAC Address	Account Index
Work Account	192.168.120.100	100	100	123456	Squuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	100	100	123456	Squuang123	00:0B:82:D2:11:22	Account1

Example I

2. For the existing SIP account, if the user wants to allocate this SIP account to another device, here is the example: Account 100 has been allocated to Device 1, and the user wants to allocate the SIP account 100 to Device 2 (00:0b:82:cc:dd:ee).

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	Device MAC Address	Account Index
Work Account	192.168.120.100	100	100	123456	Squuang	00:aa:bb:cc:ee:dd	Account1

Example II

3. If the user wants to allocate multiple SIP accounts to a single device, here is an example:

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	Device MAC Address	Account Index
Work Account	192.168.120.100	100	100	123456	Squuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	200	200	123456	Squuang	00:0B:82:E2:08:D8	Account2
Work Account	192.168.200.100	300	300	123456	Emily	00:0B:82:E2:08:D8	Account3

Example III

4. If the user wants to allocate multiple SIP accounts to a single DP device, here is an example:

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	DP MAC Address	Account Index	Profile	HS Mode	HS1	HS2	HS3	HS4	HS5
Work Account	192.168.120.100	100	100	123456	Squuang	00:0B:82:E2:08:D8	Account1	Profile1	HS1	Line 1				
Work Account	192.168.120.100	200	200	123456	Squuang	00:0B:82:E2:08:D8	Account2	Profile1	Circular	Line 2	Line 1			
Work Account	192.168.200.100	300	300	123456	Squuang	00:0B:82:E2:08:D8	Account3	Profile2	Circular	Line 3	Line 2			

Example IV

Incorrect examples:

1. If the user wants to allocate multiple SIP accounts to a single device, the account index cannot be the same.

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	DP MAC Address	Account Index
Work Account	192.168.120.100	100	100	123456	Squuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	200	200	123456	Squuang	00:0B:82:E2:08:D8	Account1

Example V

2. Different SIP server addresses cannot be allocated to the same Profile in the same DP device.

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	DP MAC Address	Account Index	Profile
Work Account	192.168.120.100	200	200	123456	Squuang	00:0B:82:E2:08:D8	Account2	Profile1
Work Account	192.168.200.200	300	300	123456	Squuang	00:0B:82:E2:08:D8	Account3	Profile1

Example VI

3. If the user wants to allocate the SIP accounts to the same DP device, the different SIP accounts cannot be allocated to the same HS Line.

Account Name	*SIP Server	*SIP User ID	*Authentication ID	*Authentication Password	Display Name	DP MAC Address	Account Index	Profile	HS Mode	HS1	HS2	HS3	HS4	HS5
Work Account	192.168.120.100	200	200	123456	Squuang	00:0B:82:E2:08:D8	Account2	Profile1	Circular	Line 1	Line 1			
Work Account	192.168.200.200	300	300	123456	Squuang	00:0B:82:E2:08:D8	Account3	Profile2	Circular	Line 1	Line 2			

Example VII

Allocate Device

Users could allocate the SIP accounts to the devices during adding SIP accounts, editing SIP accounts, or importing a batch of SIP accounts to the GDMS platform. Each SIP account can be allocated to multiple devices.

Edit Account

Users could edit the SIP account information and allocated devices on the **Edit Account** configuration page.

1. Click on the button for the SIP account you want to modify.

Edit Account

2. Click on the **Save** button to finalize changes. All associated devices will receive the updated account information.
3. Click on the button to unallocated devices from the account. The SIP account will be removed from unassigned devices.



- If the device is offline at the time, its SIP account information will be updated when it is online again.
- If the SIP server is synchronized from the UCM server, it cannot be edited, and it can only be assigned to the device.

Batch Modify SIP Server of SIP Accounts

Users can batch modify the SIP server of the SIP accounts, e.g. Modify the SIP protocol of the SIP server from UDP to TCP.

1. On the “**SIP Account**” interface, select the SIP accounts that need to be modified.

- The user can select the SIP accounts by searching the items. E.g. If the user wants to modify the SIP server for 250 SIP accounts, the user can set the page to display 250 SIP accounts at once from 10 SIP accounts per page and select all SIP accounts on the page.


2. Click on the “**Modify SIP Server**” button at the top of the interface.
3. Select the target SIP server, which can be searched by the server name.

Modify SIP Server

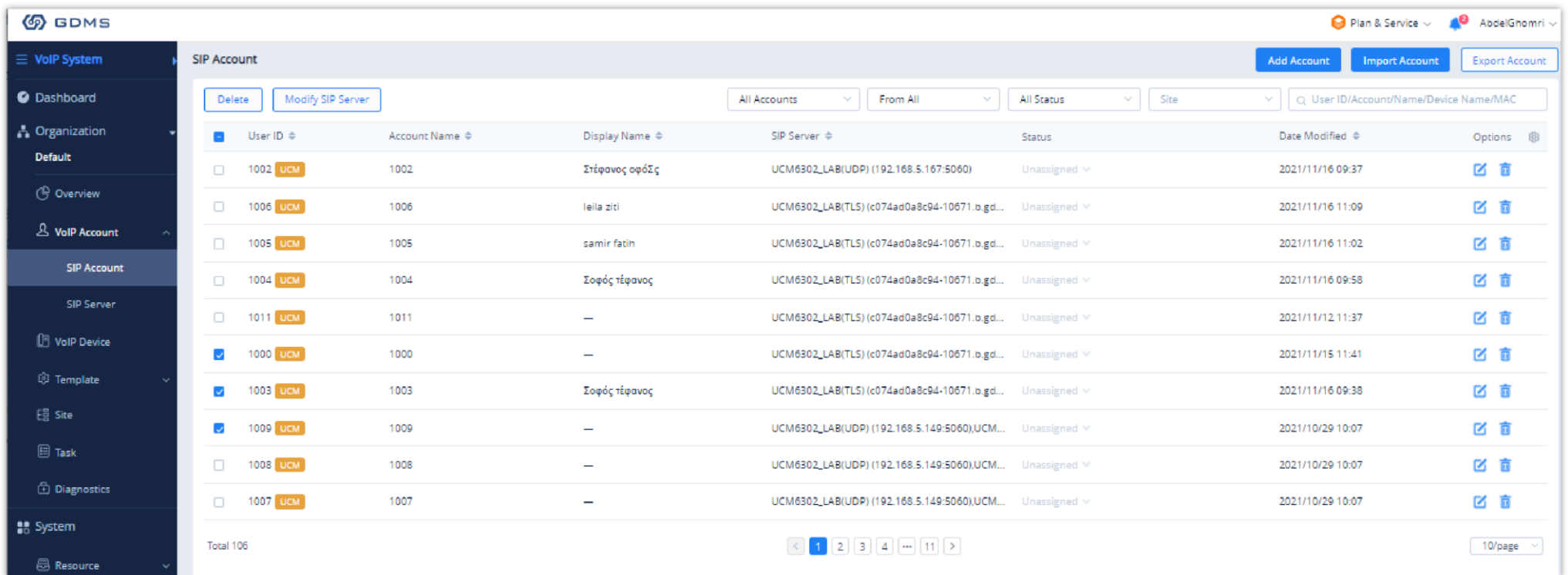
4. After clicking the “OK” button, the SIP server corresponding to the SIP accounts will be modified immediately. Then, the updated account information will be assigned to the corresponding VOIP devices.





















✔ If the SIP accounts are synchronized from UCM device, the SIP accounts information will be synchronized after the SIP server is modified.

Delete Account

To delete SIP accounts on GDMS, click on the  button for a single account or the **Delete** button in the top-left corner for multiple accounts. Associated devices will automatically remove deleted SIP account information.

Users could delete 1 single SIP account or a batch of SIP accounts on the GDMS platform:



User ID	Account Name	Display Name	SIP Server	Status	Date Modified	Options	
<input type="checkbox"/> 1002	UCM	1002	Στέφανος σφόδς	UCM6302_LAB(UDP) (192.168.5.167:5060)	Unassigned	2021/11/16 09:37	 
<input type="checkbox"/> 1006	UCM	1006	leila ziti	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/16 11:09	 
<input type="checkbox"/> 1005	UCM	1005	samir fatin	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/16 11:02	 
<input type="checkbox"/> 1004	UCM	1004	Σοφός τέφανος	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/16 09:58	 
<input type="checkbox"/> 1011	UCM	1011	—	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/12 11:37	 
<input checked="" type="checkbox"/> 1000	UCM	1000	—	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/15 11:41	 
<input checked="" type="checkbox"/> 1003	UCM	1003	Σοφός τέφανος	UCM6302_LAB(TLS) (c074ad0a8c94-10671.b.gd...	Unassigned	2021/11/16 09:38	 
<input checked="" type="checkbox"/> 1009	UCM	1009	—	UCM6302_LAB(UDP) (192.168.5.149:5060),UCM...	Unassigned	2021/10/29 10:07	 
<input type="checkbox"/> 1008	UCM	1008	—	UCM6302_LAB(UDP) (192.168.5.149:5060),UCM...	Unassigned	2021/10/29 10:07	 
<input type="checkbox"/> 1007	UCM	1007	—	UCM6302_LAB(UDP) (192.168.5.149:5060),UCM...	Unassigned	2021/10/29 10:07	 

Delete Account

❗ If the SIP account is synchronized from UCM server, this will only delete the data in GDMS platform, and the data in UCM server will not be deleted.

Export Account

Users can export all existing SIP accounts in GDMS to a file by clicking on the **Export Account** button in the top-right corner of the **SIP Account** page.

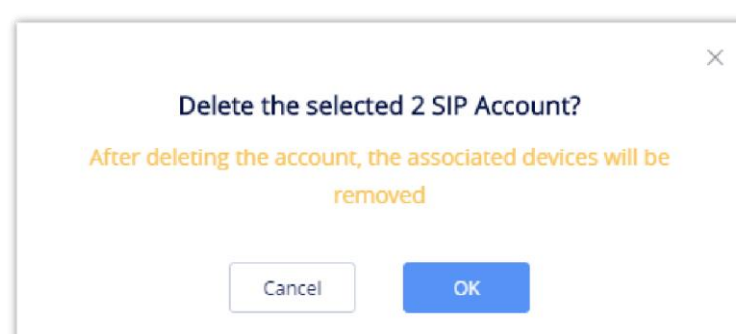
Edit SIP Server

Users can edit SIP server information by clicking on the  button for the desired SIP server. Changes to the server will affect all associated SIP accounts.

❗ If the SIP server is synchronized from UCM server, it cannot be edited.

Delete SIP Server

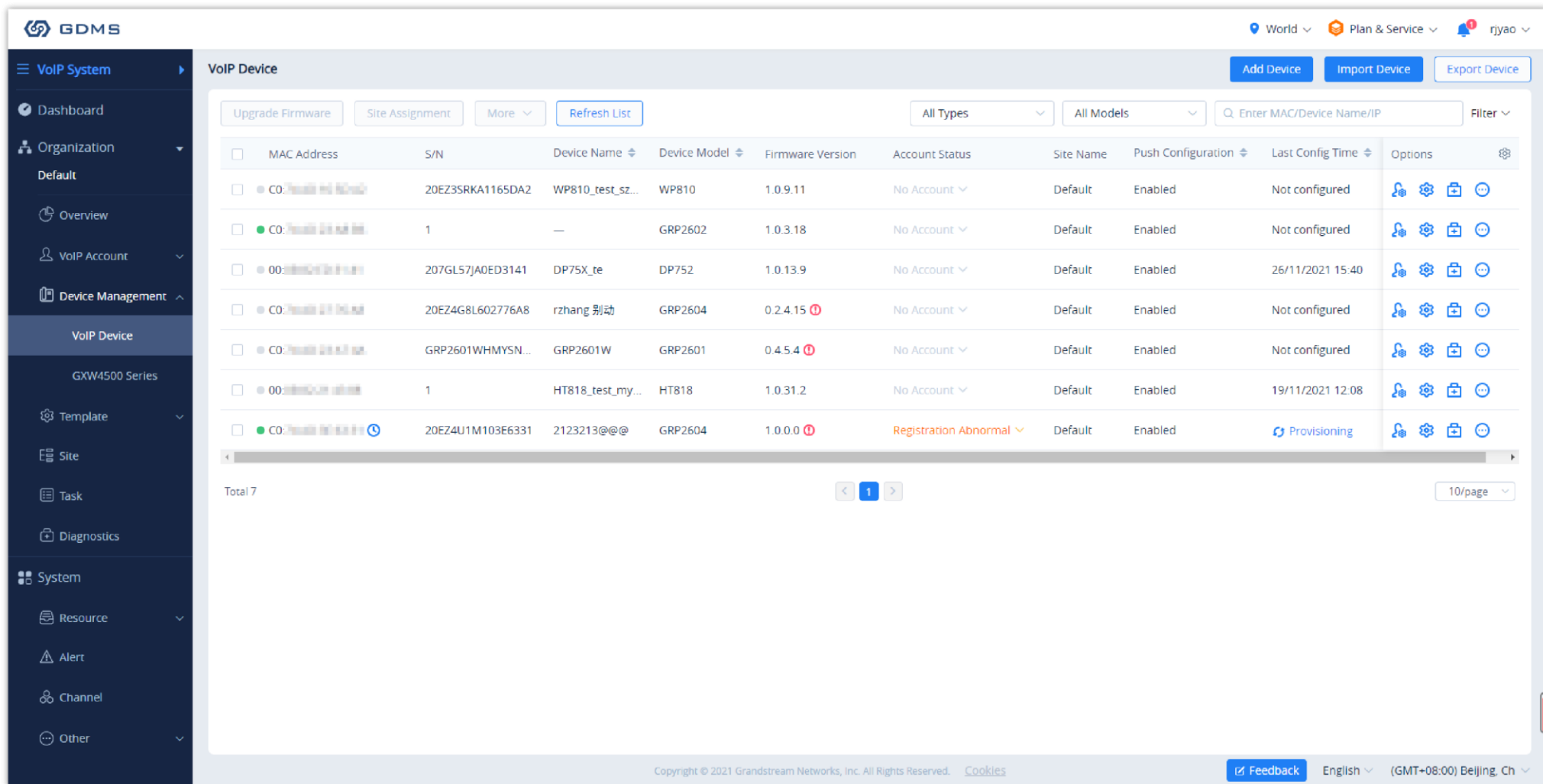
Users can delete selected SIP servers by selecting them in the SIP server list and clicking on the **Delete** button in the top left corner of the **SIP Server** page.



i If the SIP server is synchronized from UCM server, this will only delete the data in GDMS platform, and the data in UCM server will not be deleted.

VoIP Device Management

The Device page shows all the associated VOIP devices. Users can view the information and status of the devices, the allocated account information, etc. GDMS platform supports to allow users to configure parameters, upgrade firmware, reboot/factory reset devices, view device details, device diagnostics, and other operations.





VoIP Device Management

Status	Description
<p>Status Indicator</p>	<ul style="list-style-type: none"> The device is offline. The current account status is the last reported status before the device is offline. The device is online. The device network penetration (NAT) is abnormal, the GDMS server cannot connect to the device, but the device can periodically obtain the configuration.
<p>Account Status</p>	<p>Normal: The allocated accounts from the GDMS platform to the devices are registered successfully, and all accounts can be used normally.</p> <p>When an account is registered normally, the extension number will be displayed.</p> <p>Abnormal: Some of the device’s allocated accounts are unregistered. This may be due to the following reasons:</p> <ul style="list-style-type: none"> The account is not activated. The account registration credentials are incorrect. The account was modified on the device. <p>No Account: GDMS platform does not allocate any account to the device.</p>

Status	Description
Last Config Time	<p>Synchronizing: If the account and device parameters were modified, the changes will immediately be pushed to the device. This status will be shown while this is happening.</p> <p>Date/Time: The date and time of the last successful provisioning.</p>
Call Status	<p>Idle: The SIP account is in an idle state.</p> <p>Busy: The SIP account is on a call.</p>
HS Status	<ul style="list-style-type: none"> ✓ The SIP account is configured on the handset. ✓ The SIP account is not configured on the handset.

VoIP Device Management

Operation	Description
Sorting	Click on the sorting buttons  to sort the list by various columns in ascending/descending order.
Custom Display Option	Click on the  button on the top right corner of the list to select the columns to show and/or hide.
Search	In addition to being able to search for devices with the search bar near the top-right corner of the page, users can further refine search results by clicking on the Filter button by specifying account status, device status, site, city, and firmware version.

Operation Instructions

Upgrade Firmware
Site Assignment
More ▾
Refresh List

All Models ▾

Filter ^

All Cities ▾
All Account Status ▾
All Device Status ▾
Site ▾
All Firmware Version ▾

Search Devices

Add VoIP Device

To add a new device to GDMS, click on the **Add Device** button. The following window will appear:

Add Device ×

Device Name

* MAC Address : : : : :

* S/N

* Site

Sync Configuration If enabled, when the 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](#)

Add VoIP Device

Device Name	(Optional) This option is used to set the name of the device so that the users could identify this device. The maximum number of the input characters is up to 64.
MAC	(Required) This option is used to enter the MAC address of the device. (Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package)
Serial Number	(Required) This option is used to enter the serial number of the device. (Locate the Serial Number on the MAC tag of the unit, which is on the underside of the device, or on the package)
Select Site	(Required) This option is used to set which site this device belongs to. The default setting is “Default” site.
Sync Configuration	If enabled, when the device goes online, its local configuration and SIP accounts will be synced to GDMS.

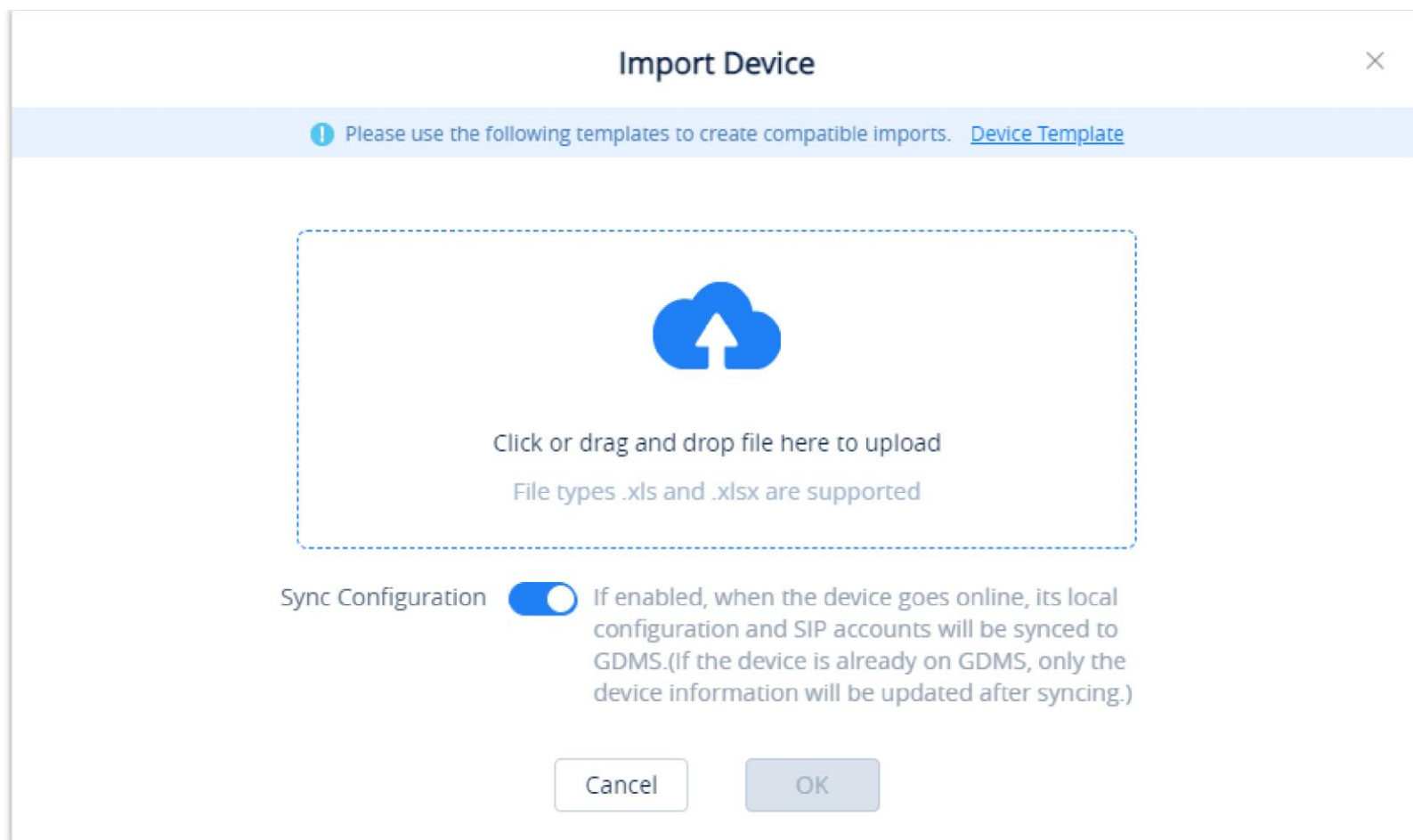
Add VoIP Device



- Users could click on the “Save” button to save the configuration.
- Each device can only be associated with only one GDMS account.
- Users can use the search bar on the Device page to find added devices via device name, MAC address, and sites.

Batch Import VoIP Devices

Users can import multiple devices by uploading a file. Click on the **Import Devices** button on the **Device** page to get started. The following window will appear:



Import VOIP Device

1. Click on the [Device Template](#) button to download the template. Users must follow the instructions to enter the required information.

Instructions:

- Fields marked with * are required and cannot be empty.
- MAC Address: Valid characters are 0-9, A-Z, hyphens (-), and colons (:) (e.g. 00-15-65-1A-2B-3C, 00:15:65:1a:2b:3c, 0015651a2B3c, etc.). If users want to assign accounts to multiple devices, they must enter the MAC addresses in multiple lines.
- Serial Number: Required if users want to add new devices to GDMS. Only alphanumeric characters allowed.
- Device Name: The maximum allowed number of characters is 64 characters.
- Site Name format: 1st Level Site/2nd Level Site/.../New Site. Users must enter the names starting from the 1st Level Site. If the higher level sites do not exist, they will be created automatically. If no higher level site name is entered, this site name will be used by default to fill in missing site names. The maximum allowed number of characters is 64 characters.

*MAC address	*SN	Device Name	Site Name

Import VoIP Device Template

2. The template will have the following fields:

MAC Address	Users need to fill in the MAC address of the device in this field (Required). For instance, 000B82E21234, and it supports to fill “:” and “-” characters in this field.
SN	Users need to fill in the serial number of the device in this field (Required).
Device Name	This option is used to set the name of the device so that the users could identify this device (Optional). The maximum number of the input characters is up to 64.
Site Name	Enter the site to assign this device to (Required). If the site is under more than one level, all site levels must be included in the site name (e.g. first_level/second_level/.../new_site). If the site level does not exist, it will be automatically created. Maximum character limit is 64.

Import VoIP Device Template

3. Users can drag the file to the pop-up window, or they can click the upload button to select a file from their PC to import.

4. Once the file is imported into GDMS, the result window will appear. If any data failed to import successfully, users can export the problematic data, re-edit, and attempt to import them into GDMS again.


5. The user can choose to sync the devices' configuration by enabling "Sync Configuration". Once that is enabled, the local configuration and SIP accounts will be synchronized to the GDMS.

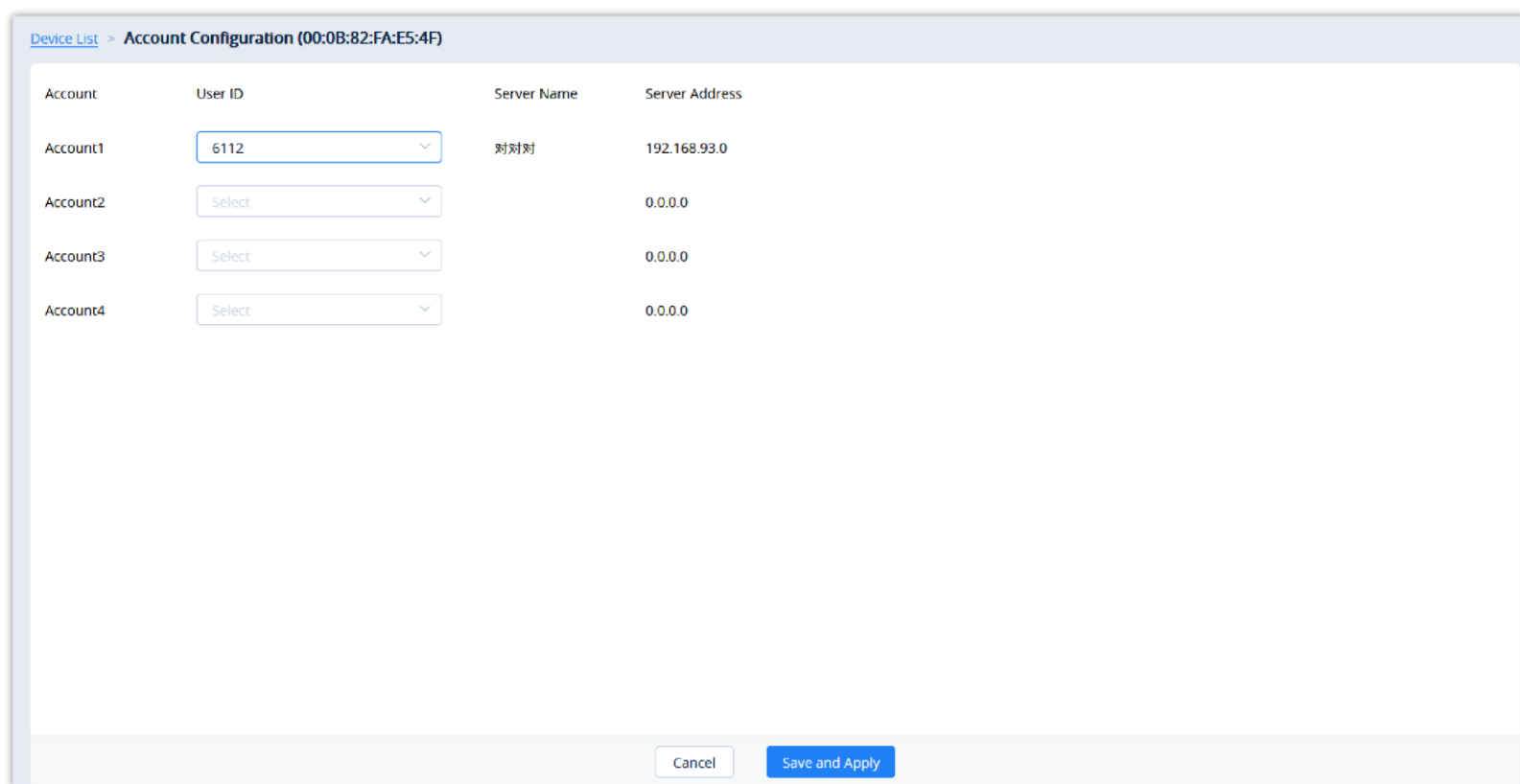


- If an existing device on GDMS is imported, the device's existing information will be replaced with the newly imported information.
- If a device's MAC address and serial number are invalid, the import will fail.

Configure SIP Account (Non-DP Devices)

Users can configure SIP accounts for each device from the **Device** page.

1. In the devices list, click on the icon  corresponding to the account to access the Account configuration page.
2. After clicking the button, users will see the Account configuration page as the figure shows below:



Account	User ID	Server Name	Server Address
Account1	6112	对对对	192.168.93.0
Account2	Select		0.0.0.0
Account3	Select		0.0.0.0
Account4	Select		0.0.0.0

Configure SIP Account


3. On this **Account Configuration** page, users can select the SIP accounts created on the **SIP Account** page to assign to the device.
4. Users could also select to replace the existing SIP account with a specific account or delete the existing accounts.
5. Click on the **Save and Apply** button. The accounts will then be assigned to the device.



- If a device is offline during the account assignment, GDMS will synchronize any changes to it the next time it goes online.
- Settings configured via other means (e.g. endpoint device web portals, Zero Config provisioning, etc.) will not be synchronized to GDMS.

Configure SIP Account/Line (DP Devices)

Users could configure SIP accounts and lines for DP devices. GDMS platform supports to allow users to view the existing SIP accounts for current devices and edit/delete the accounts.

1. In the devices list, click on the icon  corresponding to the account to access the Account configuration page.
2. After clicking the button, users will see the figure as shown below:

Configure SIP Account for DP Devices

User ID	Allocated: This SIP account has already been allocated to other devices; Unallocated: This SIP account has not been allocated to any device.
Profile	Different SIP servers cannot be set to the same profile.
HS Mode	If this field is not filled, the default setting is “Circular” mode.

Configure SIP Account for DP Devices

3. To configure the lines for each HS mode, click on the **Line Configuration** tab.

Line Configuration

i Set up a line account for each handset and select the SIP accounts from the configured accounts in the device

4. Select the desired SIP accounts to use for each line and handset.

5. Click on the button **Save and Apply** to allocate the SIP accounts or lines to the devices.

i

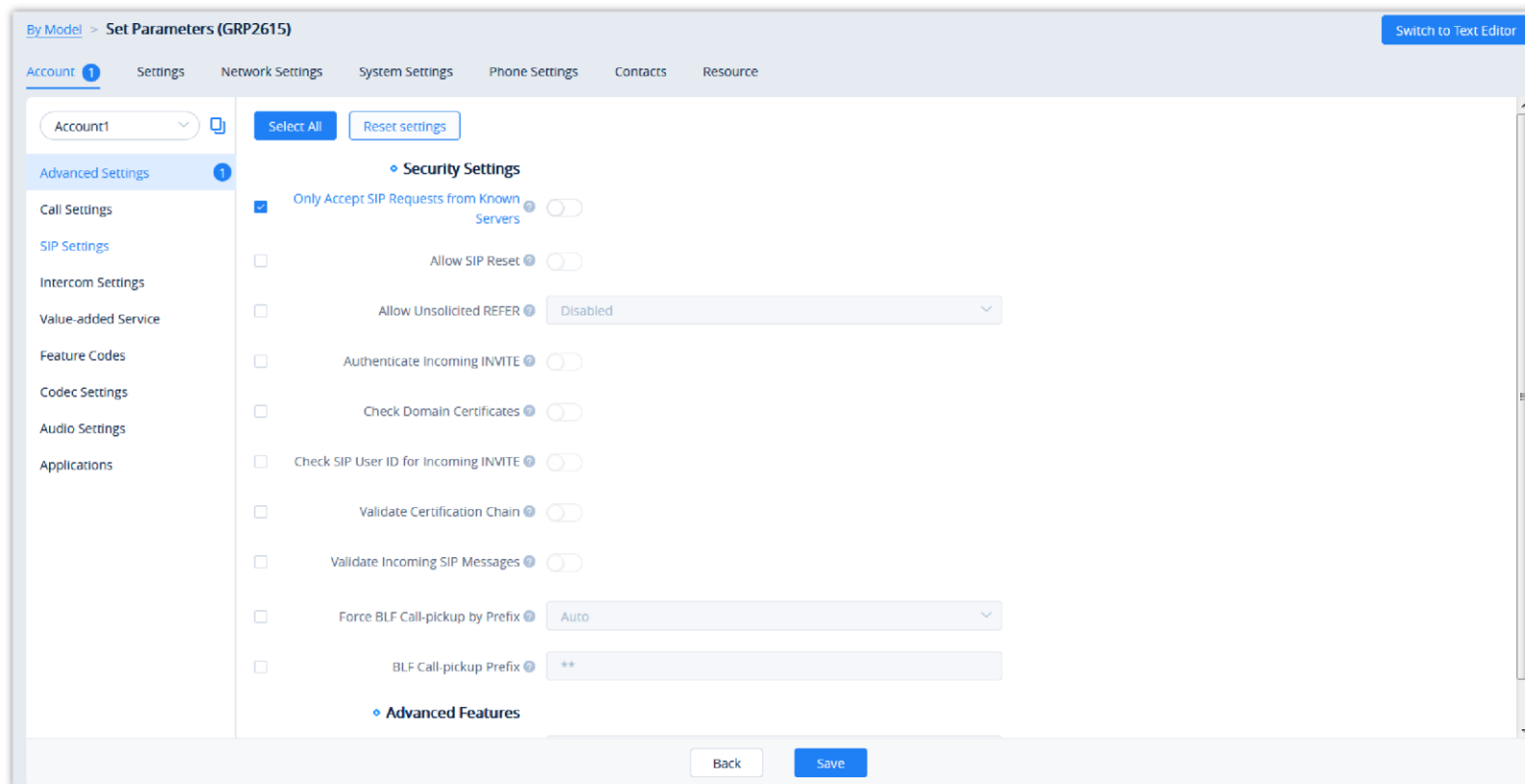
- If a device is offline during the account assignment, GDMS will synchronize any changes to it the next time it goes online.

- Settings configured via other means (e.g. endpoint device web portals, Zero Config provisioning, etc.) will not be synchronized to GDMS.
- For device-specific configuration rules, please refer to the DP device user guide.


Device Parameters Configuration

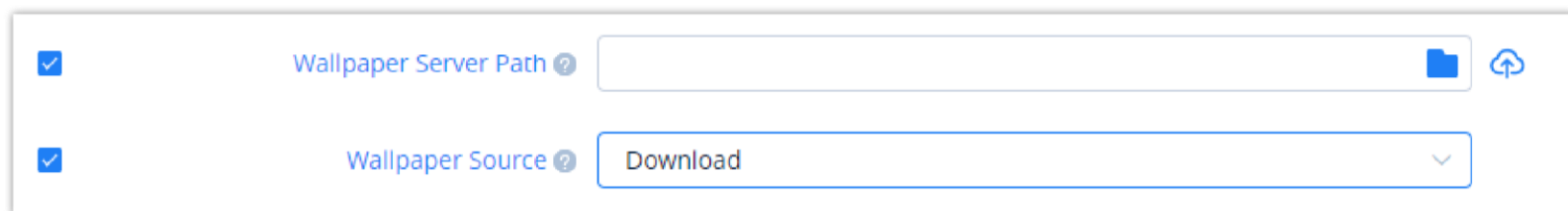
Users can modify the configuration parameters for a single device.

1. In the device list, click on the  button to go to the **Device Parameters Configuration** page, as shown in the figure below:



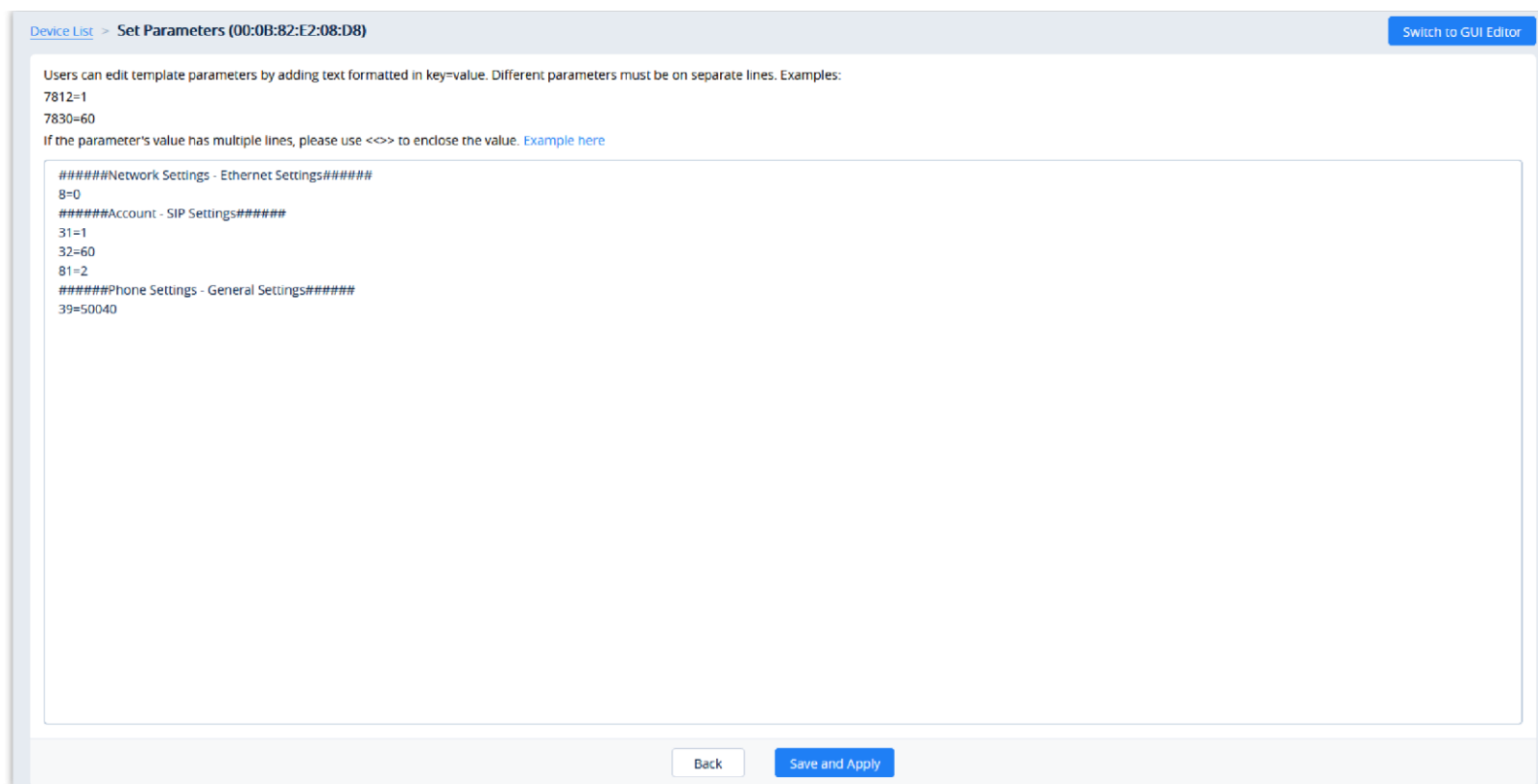
Device Parameter Configuration

- Clicking on the **Select All** button will select every option on the current page. Clicking on it again will deselect all the options.
- Clicking on the **Reset Settings** button will restore all settings on the current page to default values.
- Clicking on the button  following the account, users can copy and paste the current account configuration to other accounts.
- When users try to configure the device wallpaper or screensaver image, users can select a picture from the resources list, or upload the local picture to GDMS and configure it to the device.



Ringtone Configuration

2. Modify the desired settings on the page or click on the **Switch to GUI Editor** to configure device settings via text editing (i.e. p-values).



Edit Configuration File

- The format requirement is key=value. The key can be either a P-value or an alias.
- Users can enter the latest parameters and values of a device in the text editor even if the GDMS configuration page does not display the configuration options.

3. Click on the **Save and Apply** button to finalize changes. Only settings that are checked will be pushed to the device.

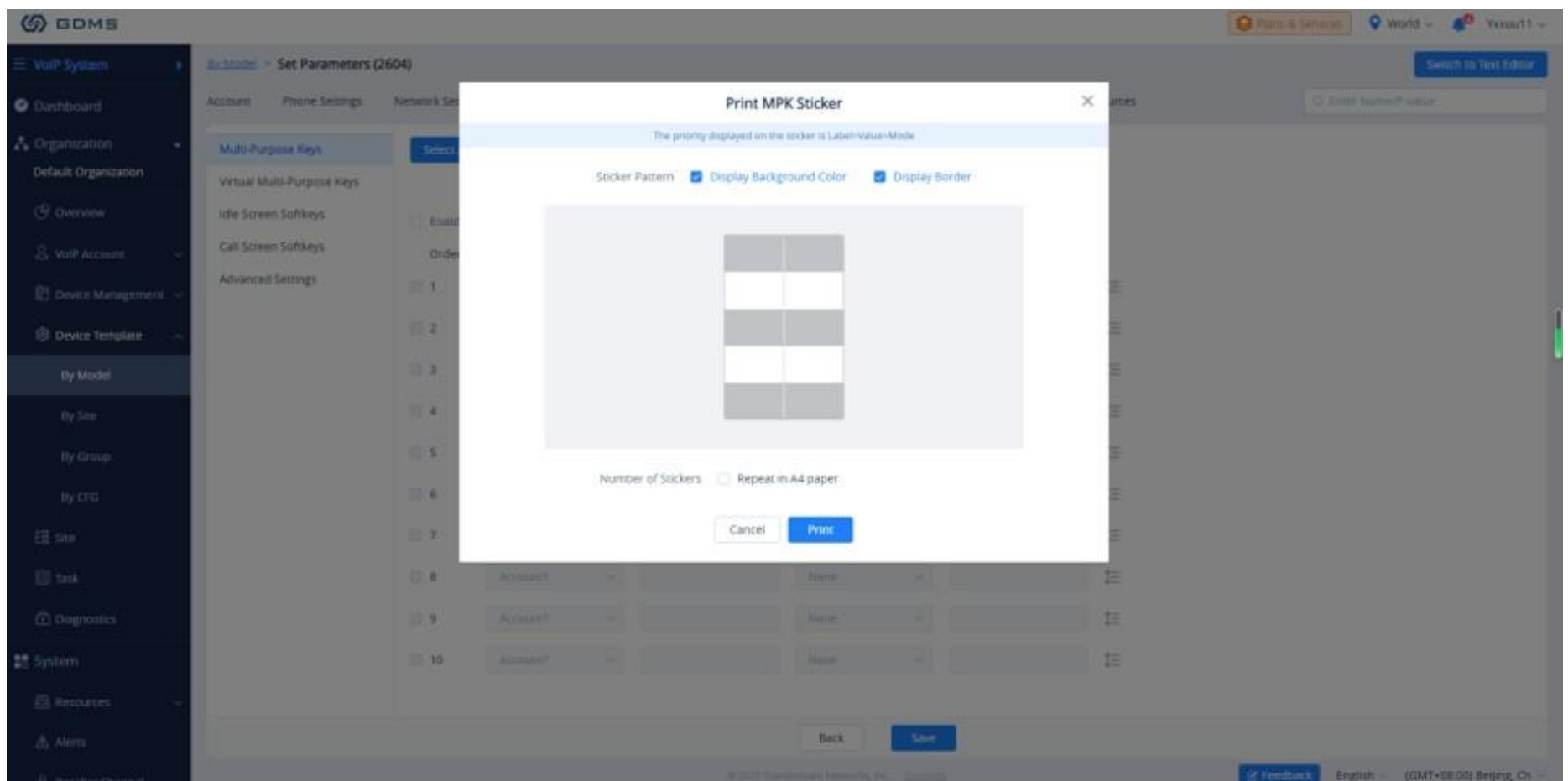


- If the device is not connected to the GDMS platform currently, the device cannot be synchronized with the GDMS platform.
- When the device is connected to the GDMS platform, the allocated accounts will be synchronized on the device immediately.
- The SIP accounts which are configured manually on the device will not be synchronized to the GDMS platform. For the configuration rules, please refer to the User Guide of the devices.

MPK Stickers Printing

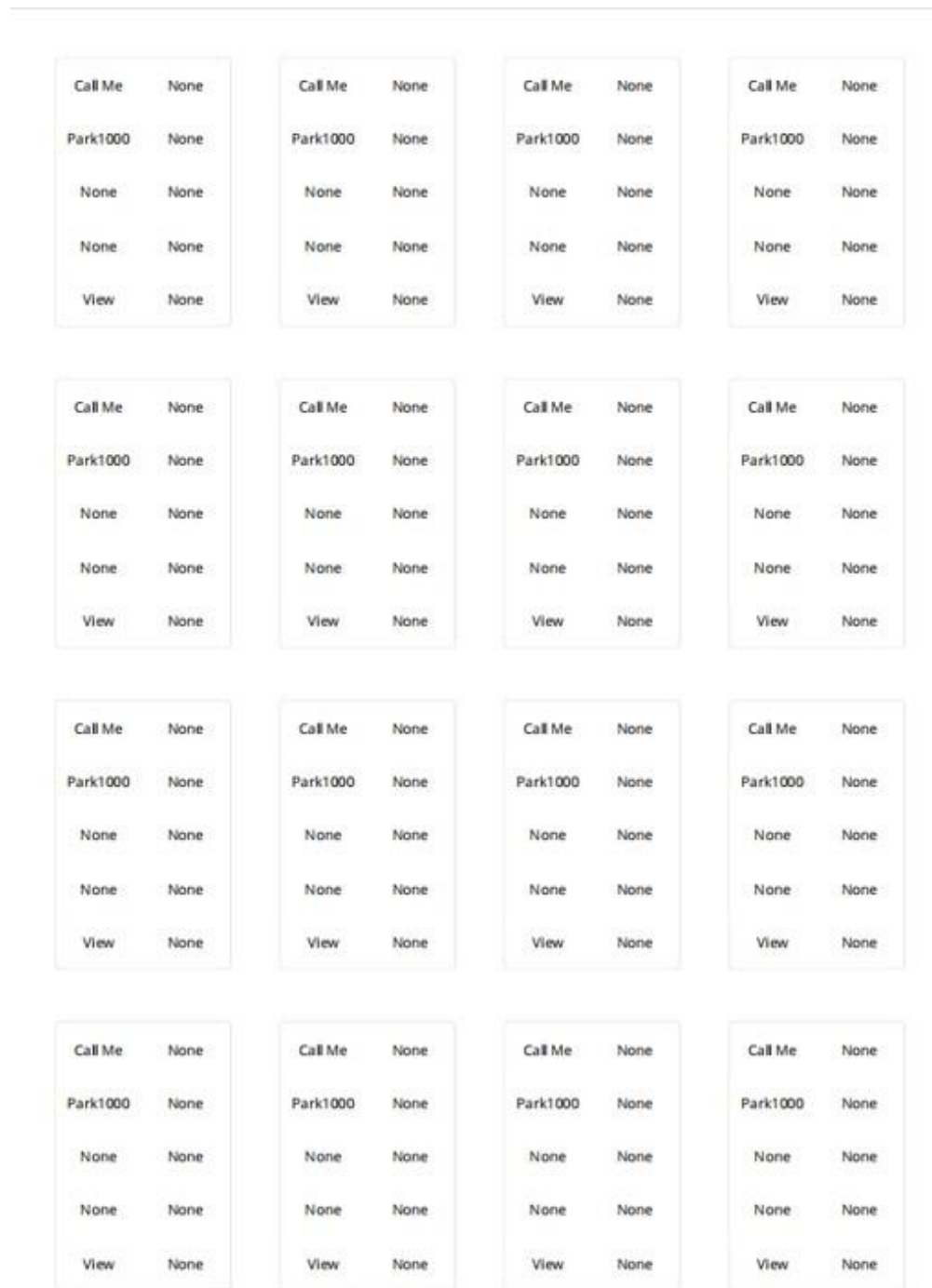
Certain Grandstream IP phones have a MPK sticker placement (GRP2604, GRP2634, GRP2636, GXP2130, GXP2160) to label the MPKs as the user desires. GDMS offers a way to print the stickers when configuring the devices.

You can select whether to print the background color, whether to display the border, or whether to print repeatedly on the A4 paper.



Print MPK Sticker

When the user prints MPK sticker repeatedly on an A4 paper, it will be displayed as following.



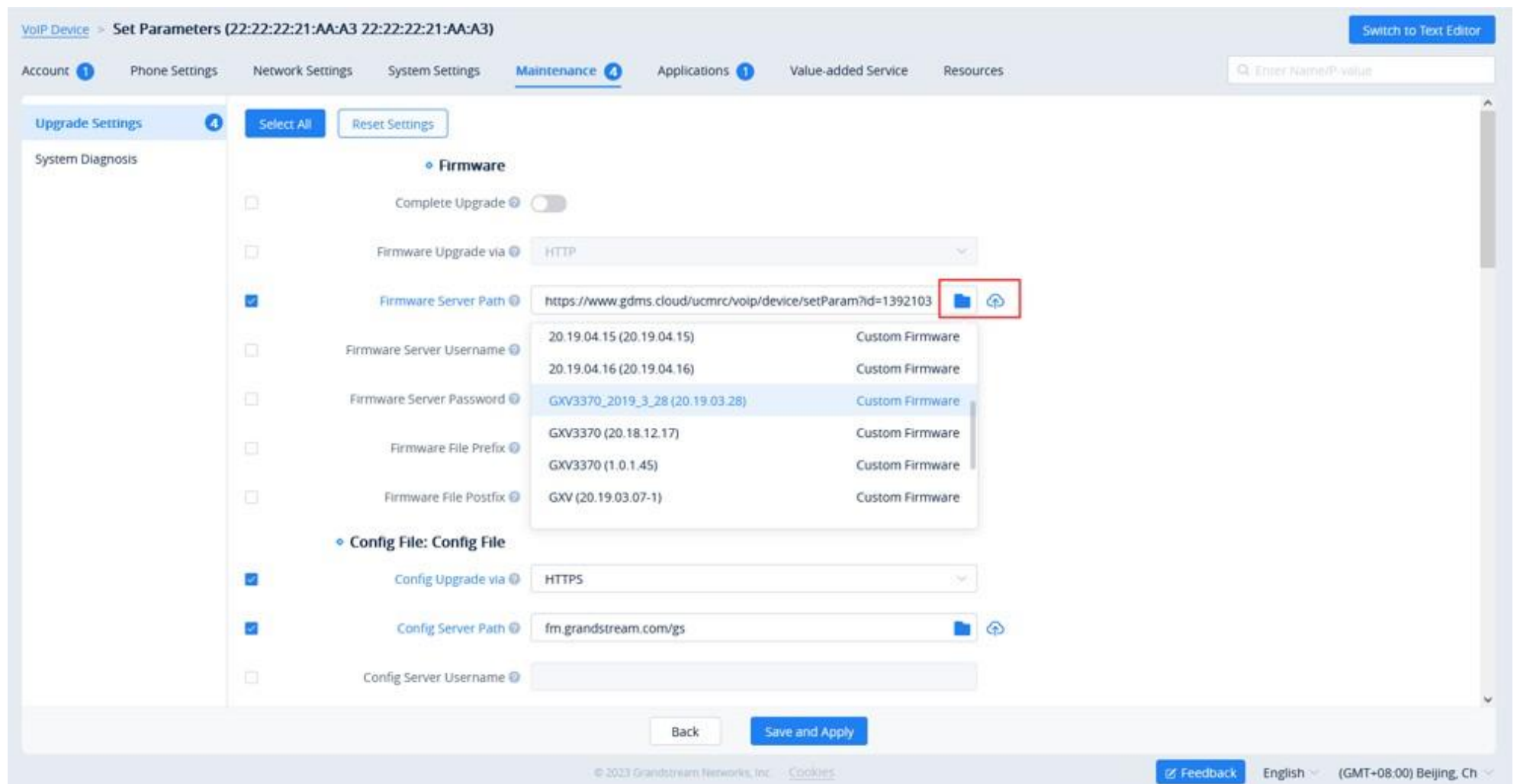
Multiple MPK Stickers

If you want to print on the native sticker provided with the IP phone unit. Please refer to the following video:

https://v.youku.com/v_show/id_XNDc3MDczOTIwOA==.html

Upgrade The Firmware

You can select the firmware path from the existing firmware resource list or directly upload your firmware file by clicking the “Upload” button following the option. Please refer to the screenshot below.

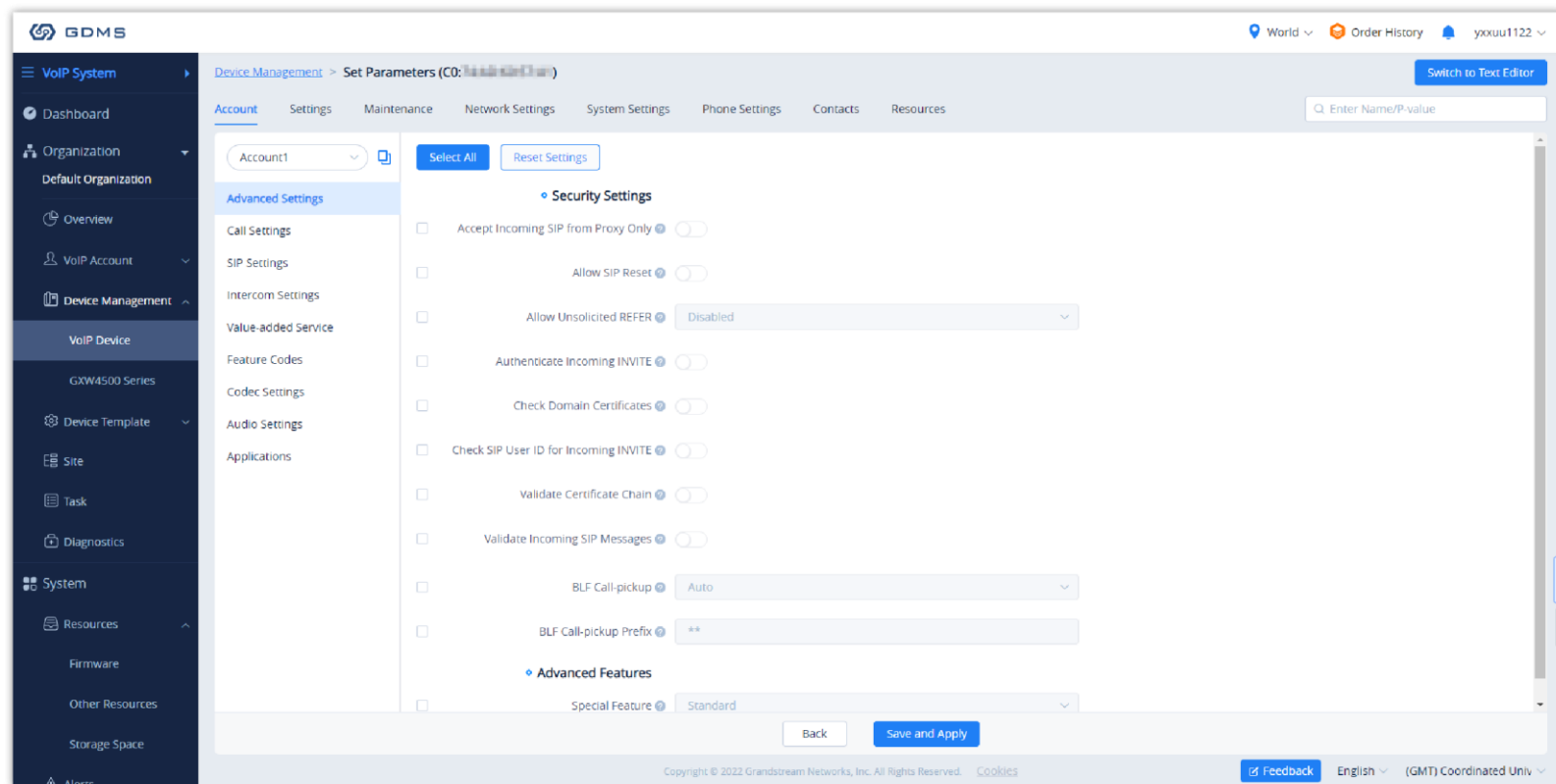


Upgrade Settings – Firmware

Configure Resource Files


Users can configure custom ringtones and languages for devices (Supported models: GXP/DP series).

1. On the Device list, click on the  button to go to the **Device Parameters Configuration → Resource Configuration** page, as shown in the figure below:




Resource Configuration


2. On the “Custom Ringtone” page, for Ringtone 1 to Ringtone N, select a ringtone file from the resources for each ringtone index.
3. On the “Language Configuration” page, select a language pack from the resources for the device.
4. Click on the “Save and Apply” button, the device will download the selected resources from the firmware path.

-  For each device model, the size and duration of each ringtone are different. If the duration and size exceed the limit, the system will intercept the resource file to the maximum limit automatically.

Synchronize Device Local Configuration


Before the device is configured, the user can synchronize the device's local configuration to the GDMS server.


1. Select a specific device, click icon  and select the option “**Synchronize Device Local Configuration**”.
2. Click “**OK**” to confirm synchronization on the pop-up window. Then, the GDMS server will synchronize all the account configurations and parameters of the current device to the GDMS server.
3. Enable Sync SIP Account if you wish to have your SIP accounts synchronized to the GDMS.

- 
 - If the device's parameter configuration conflicts with the server's configuration, the device's local configuration prevails.
 - If the account on the device does not exist on the GDMS server, the SIP account and server are automatically created on the GDMS server.
 - This option can be turned on only for the devices which are online.

Disable Push Configuration

If the user does not want to push any configuration to the device through the GDMS server, please follow the steps below:

1. Select a specific device, click icon  and select the option “**Disable Push Configuration**”.
2. Click “**OK**” to confirm the operation, the account configuration or parameters will not be pushed to the device through the GDMS server anymore, including the scheduled tasks. The configuration that has not been pushed to the device will not be pushed to the device anymore.

-  If the user wants to resume pushing the configuration or parameters to the device, the user can click “Enable Push Configuration” option to operate in the GDMS server.

View VoIP Device Details

Click on the  button to view a specific device's system information and account status.

Device Model	Firmware Version	Account Status	Site Name	Push Configuration	Last Config Time	Options
GRP2603	1.0.3.83	No Account	Default	Enabled	Not configured	
GXV3450	1.0.1.13	No Account	Default	Enabled	Not	<ul style="list-style-type: none"> Device Details Operation Logs Task History Edit Device Authorization Management Transfer Device Disabled Push Configuration Sync Device Local Configuration Remote Access to Web UI Remote Access to Device Interface Reboot Device Factory Reset
WP825	1.0.11.22	No Account	Default	Enabled	Not	
HT801	1.0.43.6	No Account	Default	Enabled	Not	
GRP2601	1.0.3.57	No Account	Default	Enabled	202	
GRP2613	1.0.5.93	No Account	Default	Enabled	Not	

View VoIP Device Details

System Information

The device details include System information, Network information, Account status, etc.

VoIP Device > Device Details (C074AD224D32 C0:74:AD:22:4D:32)

System Information Account Status

Last Restart Time 07/12/2021 01:26AM (Reboot via device)

Hardware Version GRP2601PV1.3A

Software Version 0.4.4.14

MAC Address C0:74:AD:22:4D:32

S/N 20EZ41KL30224D32

OpenVPN® IP 10.10.1.6

• IPv4

Address Type Static

IPv4 Address 192.168.126.192

Subnet 255.255.255.0

Default Gateway 192.168.126.1

DNS Server 1 192.168.121.118

DNS Server 2

• IPv6

IPv6 Address Type

VoIP Device Details

The information in this page is obtained from the device in real-time. If the device is offline, the details page will be inaccessible.

Account Status

Account	User ID	Server Name	Server Address	Account Status
Account1 Local	1008	192.168.5.142	192.168.5.142	Unregistered

Device Details

Energy Saving Inform (GRP Series Only)

If you are viewing the detail of a GRP series IP phone, an additional tab will appear **Energy Saving Inform**. This tab contains information about your GRP device power usage. It provides information about which Energy Saving Mode has been configured on your device, the percentage of the energy saved, whether Deep Energy Saving has been enabled, and information about when the Energy Saving has been enabled with all the related information of how much energy has been saved and how long the phone has been operational under energy saving mode.

[VoIP Device](#) > **Device Details (C0:74:AD:27:76:65)**

System Information Account Status Energy Saving Inform

Energy Saving Mode Optimized

Energy Saving Percentage 32.00%

Deep Energy Saving Status Yes

Last Energy Saving Info 2022/12/30 15:51

Energy Saving Amount 1540mWh

■ Phone Usage Duration 18906s

■ Deep Energy Saving Duration 18252s

Copyright © 2023 Grandstream Networks, Inc. All Rights Reserved. [Cookies](#) [Feedback](#) English ▾ (GMT+01:00) Casablanca ▾

Energy Saving Inform









































Edit VoIP Device

Users could edit the Device name and which site the device belongs to.

1. In the device list, click on the button  which is following the device, and select **Edit Device** to access the device editing page.

Device List [Add Device](#) [Import Device](#) [Export Device](#)

[Upgrade Firmware](#) [Site Assignment](#) [More ▾](#) [Refresh List](#) All Models ▾ Filter ▾

<input type="checkbox"/>	MAC Address	Device Name	Model	Firmware Version	Public IP	Private IP	Account Status	Site Name	Last Config Time	Options
<input type="checkbox"/>	00:0B:82:9A:8F:2C	000B829A8F2C	GXV3370	20.19.8.1	192.168.126.215	192.168.126.215	Abnormal ▾	default	2019/11/07 14:21	   
<input type="checkbox"/>	C0:74:AD:01:B4:80	—	GRP2614	—	—	—	Abnormal ▾	default	Provisioning	   
<input type="checkbox"/>	C0:74:AD:05:C6:6C	—	GRP2614	—	—	—	No Account ▾	default	Provisioning	   
<input type="checkbox"/>	C0:74:AD:05:D4:82	—	GRP2614	—	—	—	No Account ▾	default	Provisioning	   
<input type="checkbox"/>	C0:74:AD:01:B5:00	—	GRP2614	—	—	—	No Account ▾	default	Provisioning	   
<input type="checkbox"/>	C0:74:AD:05:C4:C0	—	GRP2614	—	—	—	No Account ▾	default	Provisioning	   
<input type="checkbox"/>	00:0B:82:E5:8C:CD	00:0B:82:E5:8C...	DP750	0.1.11.2	192.168.200.27	192.168.200.27	Abnormal ▾	o-oo	2019/11/01 09:09	   
<input type="checkbox"/>	00:0B:82:FA:E5:4F	—	GXP2140	—	—	—	No Account ▾	default	Not configured	   
<input type="checkbox"/>	00:0B:82:FA:E5:50	—	GXP2140	—	—	—	Normal ▾	default	Not configured	   
<input type="checkbox"/>	00:0B:82:FA:E5:52	—	GXP2140	—	—	—	No Account ▾	default	Not configured	   

Total 260 [1](#) [2](#) [3](#) [4](#) ... [26](#) > 10/page ▾

Edit VoIP Device Option

2. Users will see the device editing page as the figure shows below:

✕

Edit Device

MAC Address 00:0B:82:E5:8C:C9

Device Name

* S/N

* Site

Edit VoIP Device

3. Click on the **Save** button to apply the changes on the GDMS platform.

View VoIP Device Operation Logs

Users could view all operation logs for a specific device on the GDMS platform.

1. On the Device List, select the menu button following the specific device, and click on the “Operation Log” button.
2. Access to the Operation Log menu of the device, the menu includes the operation logs of device SIP account configuration, updating configuration parameters, device rebooting, device upgrading/downgrading, device factory reset, device diagnostics, etc.

Note:

Users could only view the device operation logs for the last 30 days.

Device List > Operation Logs (000B829A8F2C 00:0B:82:9A:8F:2C)

All Levels
All Operations

Filter

Username	Log Contents	Level	Operating Time
Grandstream	Configure Account	High	2019/11/07 14:20
Grandstream	Reboot Device (Immediate Task)	High	2019/11/07 14:20
Grandstream	Ping/Traceroute	High	2019/11/07 14:01
Grandstream	Ping/Traceroute	High	2019/11/07 13:59
Grandstream	Configure Account	High	2019/11/07 13:59
Grandstream	Configure Account	High	2019/11/07 13:57
Grandstream	Configure Account	High	2019/11/07 13:56
Grandstream	Configure Account	High	2019/11/07 13:55
Grandstream	Configure Account	High	2019/11/07 13:52
Grandstream	Configure Account	High	2019/11/07 13:50

Total 224

< 1 2 3 4 ... 23 >

10/page

View VoIP Device Operation Logs

View VoIP Device Task History

Users could view all task histories in the sub-system for a specific device on the GDMS platform, including immediate tasks and timed tasks.

1. On the Device List, select the menu button following the specific device, and click on the “Task History” button.
2. Access the Task management page, and search for all tasks of the specific device.

Task Name	Task Type	Task Time	Creator	Status	Run Time	Options
—	Upgrade Firmware	Immediate (09/05/2022 10:16AM)	yxxuu1122	Timeout	—	ⓘ
—	Update Config: CFG	Immediate (29/04/2022 06:36AM)	yxxuu1122	Timeout	—	ⓘ
—	Update Config: Group	Immediate (29/04/2022 06:35AM)	yxxuu1122	Timeout	29/04/2022 06:36AM	ⓘ
—	Update Config: Model	Immediate (29/04/2022 06:31AM)	yxxuu1122	Timeout	29/04/2022 06:31AM	ⓘ
—	Update Config: Group	Immediate (29/04/2022 02:21AM)	yxxuu1122	Timeout	—	ⓘ
—	Update Config: Model	Immediate (29/04/2022 02:20AM)	yxxuu1122	Timeout	—	ⓘ
5454	Update Config: Model	27/04/2022 04:00PM ~ 29/04/2022 03:59PM	yxxuu11	Ongoing	—	ⓘ ⓘ
111	Upgrade Firmware	24/04/2022 10:41AM ~ 25/04/2022 02:59AM	yxxuu1122	Timeout	—	ⓘ
—	Update Config: Model	Immediate (18/04/2022 02:19AM)	yxxuu1122	Timeout	—	ⓘ
重现bug	Reboot Device	30/12/2021 12:00AM ~ 31/12/2021 11:59PM	yxxuu	Timeout	—	ⓘ

View VoIP Device Task History

Firmware Upgrade

Users could upgrade firmware for a batch of devices to a specific firmware version.

1. In the device list, check multiple devices, and then click on the button **Upgrade Firmware** on the top of the Device page.

Upgrade Firmware

2. Users need to select the firmware version to upgrade to.
3. **Task Time:** Select when to start the firmware upgrade. Users can choose to upgrade immediately or to schedule the firmware upgrade for a specific time.
4. Click on the **Save** button to create the task. Users can check the status of the upgrade by navigating to the **Task Management** page.

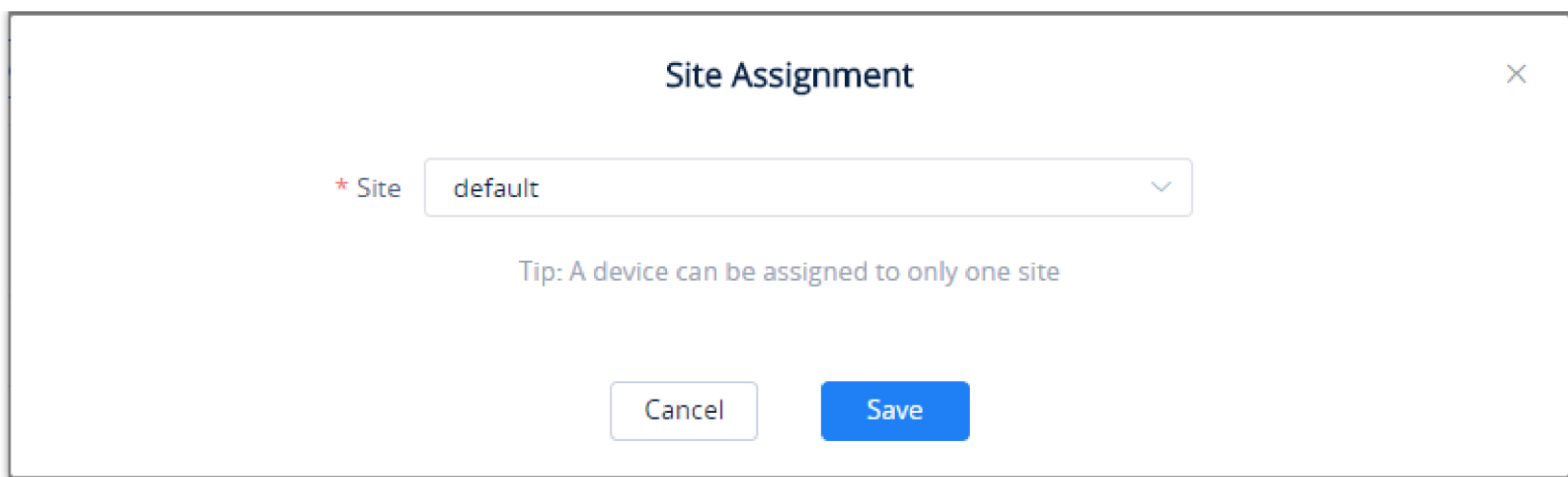


- Users cannot batch upgrade different device models or models on different firmware.
- If the desired firmware is not available, users will need to contact their GDMS administrator.

Site Assignment

Users could edit the site of a batch of devices on the GDMS platform. The default site is “default”.

1. Select the desired devices and click on the **Site Assignment** button.

A dialog box titled "Site Assignment" with a close button (X) in the top right corner. It contains a required field labeled "* Site" with a dropdown menu currently showing "default". Below the dropdown is a tip: "Tip: A device can be assigned to only one site". At the bottom are two buttons: "Cancel" and "Save".

Site Assignment

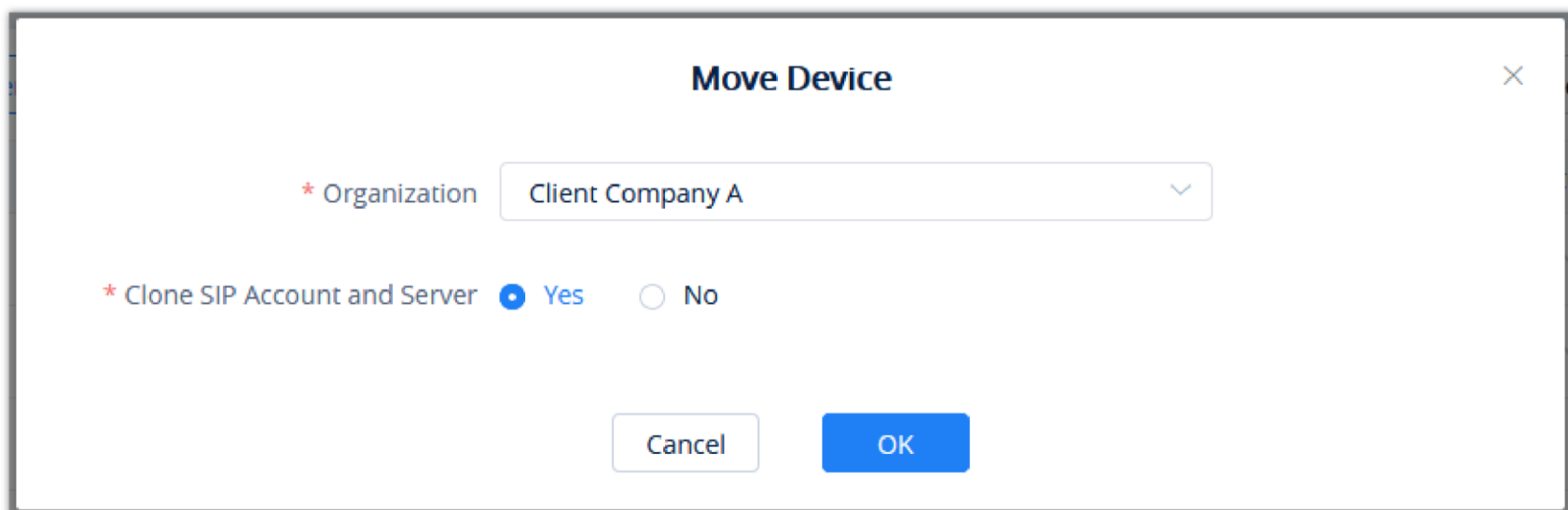
2. Select the site to assign the selected devices.
3. Click on the **Save** button, and all selected devices will be transferred to the selected site.

i Each device can only be allocated to one single site.

Move Device

Users can move devices to other organizations.

1. Select the desired devices and click on **More → Move Device**.

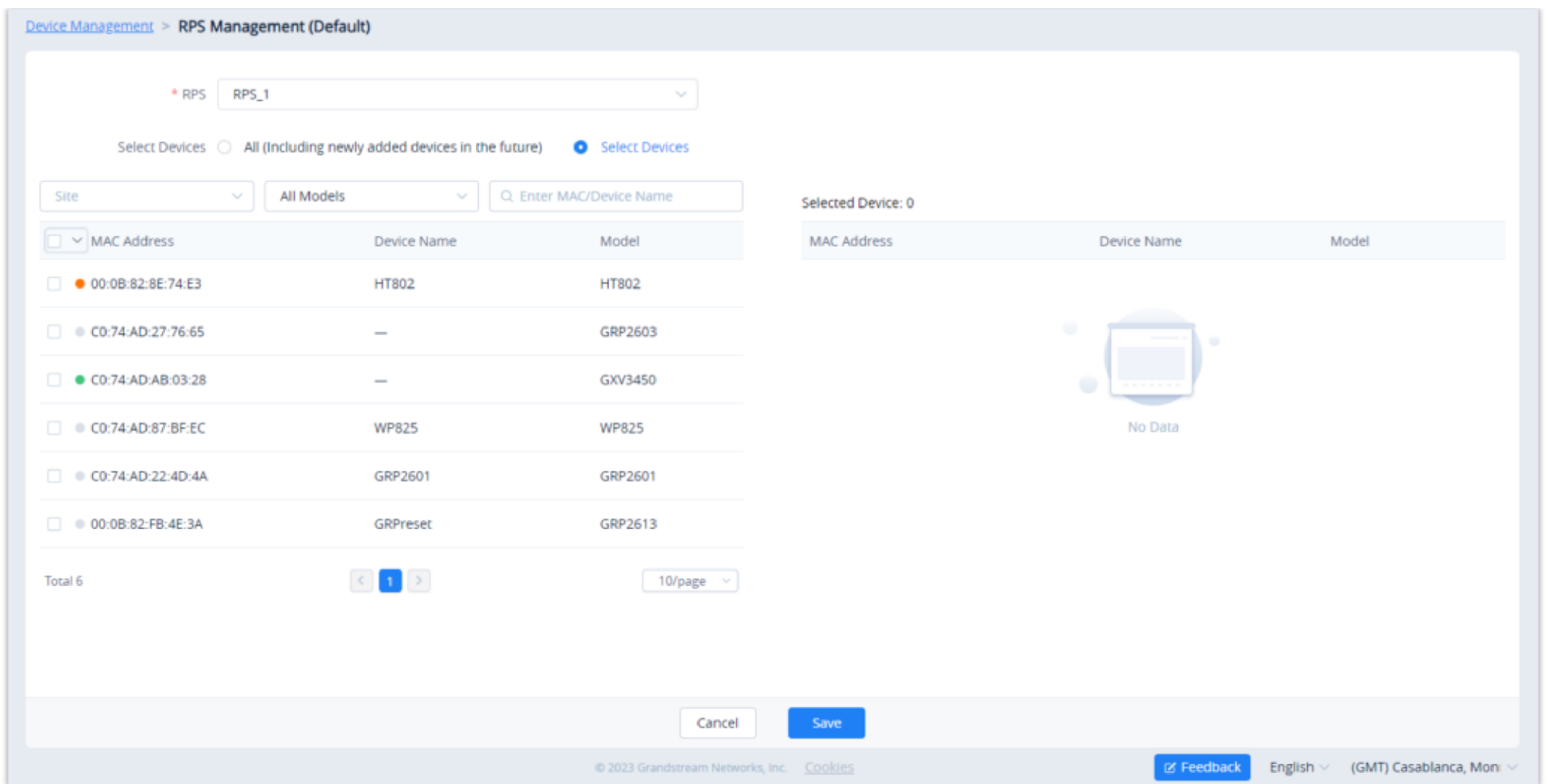
A dialog box titled "Move Device" with a close button (X) in the top right corner. It contains a required field labeled "* Organization" with a dropdown menu currently showing "Client Company A". Below this is a required field labeled "* Clone SIP Account and Server" with two radio buttons: "Yes" (selected) and "No". At the bottom are two buttons: "Cancel" and "OK".

Move Device

2. Select the target organization where to transfer the device.
3. The user needs to select whether to clone the SIP account and server which have been configured in the devices. If the user selects “No”, only the device data are transferred to the new organization, and the configured SIP accounts become empty after moving the devices.

Assign RPS

To assign an RPS to the devices, please click on [RPS Management](#) and pick an RPS from the list, then select the devices to configure with the selected RPS.



Assign RPS

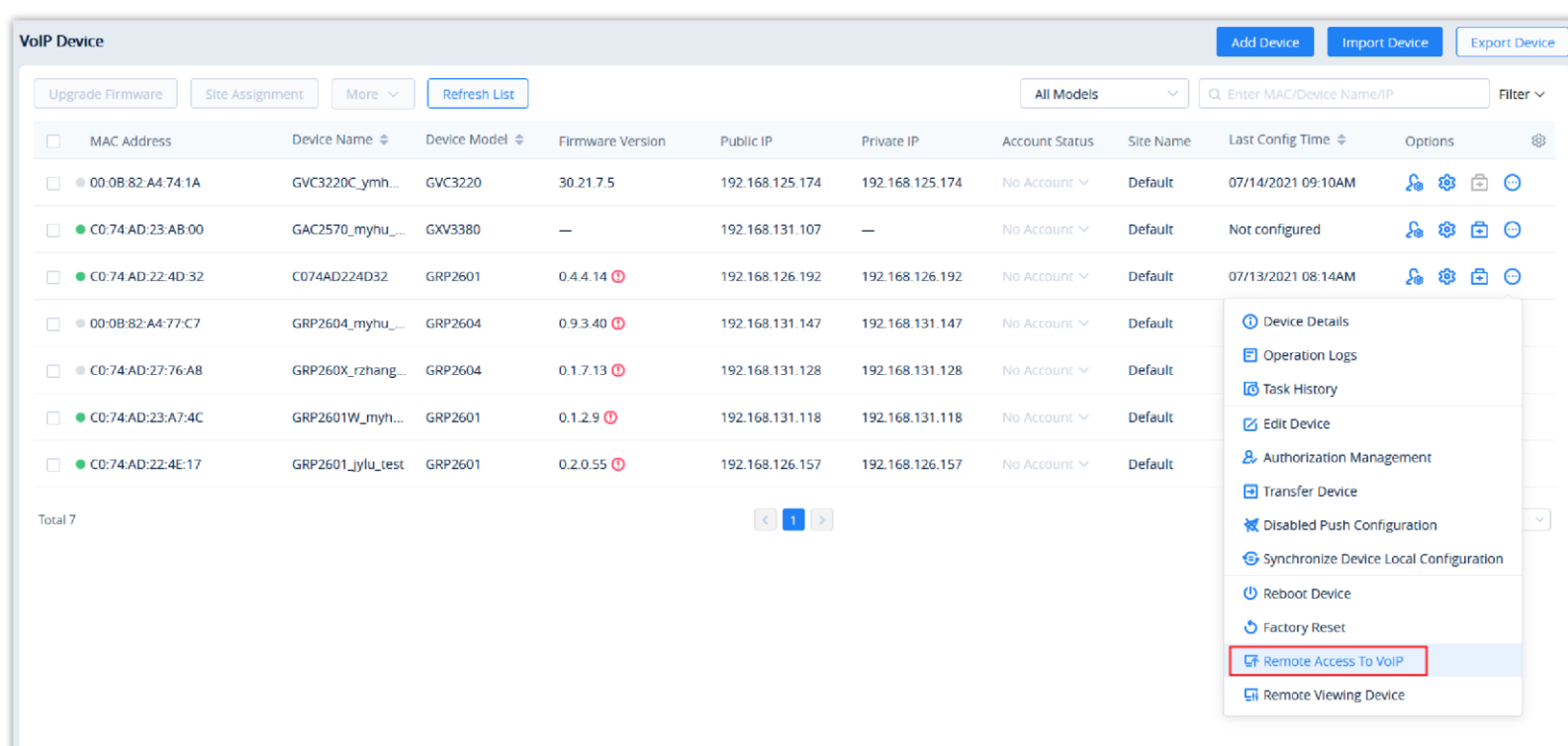
If no RPS has been created, please refer to RPS Management section.

Remote Access to Device Web UI

On the GDMS platform interface, even though the VoIP device is under the internal network, the user can remote access the VOIP device Web UI through the external network for viewing data and configuration.

i This function is only supported in GRP260x starting from firmware version 1.0.3.x and above, GXW450X starting from firmware version 1.0.1.6 and above, and UCM6300 series starting from firmware version 1.0.11.8 and above.

1. Go to the **VoIP Device** interface, click the “**More**” settings for a VoIP device → Remote access to Device Web UI, as the screenshot shows below:



VoIP Device List

2. Go to the Web UI, and log in to the VoIP device through the username and password. As the screenshot shows below:



VoIP Device Web Interface

Remote Access to Device Interface

The user can remote access Grandstream devices using the GDMS. This can be performed even if the device is behind a NAT router, and the user will be able to view the screen of the device.

i This function is only supported in GRP260x firmware version 1.0.3.x and above.

1. Go to **VoIP Device** interface, click the “**More**” settings for a VoIP device → Remote access to Device Interface, as the screenshot shows below:

MAC Address	Device Name	Device Model	Firmware Version	Public IP	Private IP	Account Status	Site Name	Last Config Time	Options
00:0B:82:A4:74:1A	GVC3220C_ymh...	GVC3220	30.21.7.5	192.168.125.174	192.168.125.174	No Account	Default	07/14/2021 09:10AM	[Icons]
C0:74:AD:23:AB:00	GAC2570_myhu...	GXV3380	—	192.168.131.107	—	No Account	Default	Not configured	[Icons]
C0:74:AD:22:4D:32	C074AD224D32	GRP2601	0.4.4.14	192.168.126.192	192.168.126.192	No Account	Default	07/13/2021 08:14AM	[Icons]
00:0B:82:A4:77:C7	GRP2604_myhu...	GRP2604	0.9.3.40	192.168.131.147	192.168.131.147	No Account	Default		[Icons]
C0:74:AD:27:76:A8	GRP260X_rzhang...	GRP2604	0.1.7.13	192.168.131.128	192.168.131.128	No Account	Default		[Icons]
C0:74:AD:23:A7:4C	GRP2601W_myh...	GRP2601	0.1.2.9	192.168.131.118	192.168.131.118	No Account	Default		[Icons]
C0:74:AD:22:4E:17	GRP2601_jlyu_test	GRP2601	0.2.0.55	192.168.126.157	192.168.126.157	No Account	Default		[Icons]

VoIP Device List

2. Enter the virtual device interface, the user can control the virtual buttons on the device and the LCD screen, as the screenshot shows below:

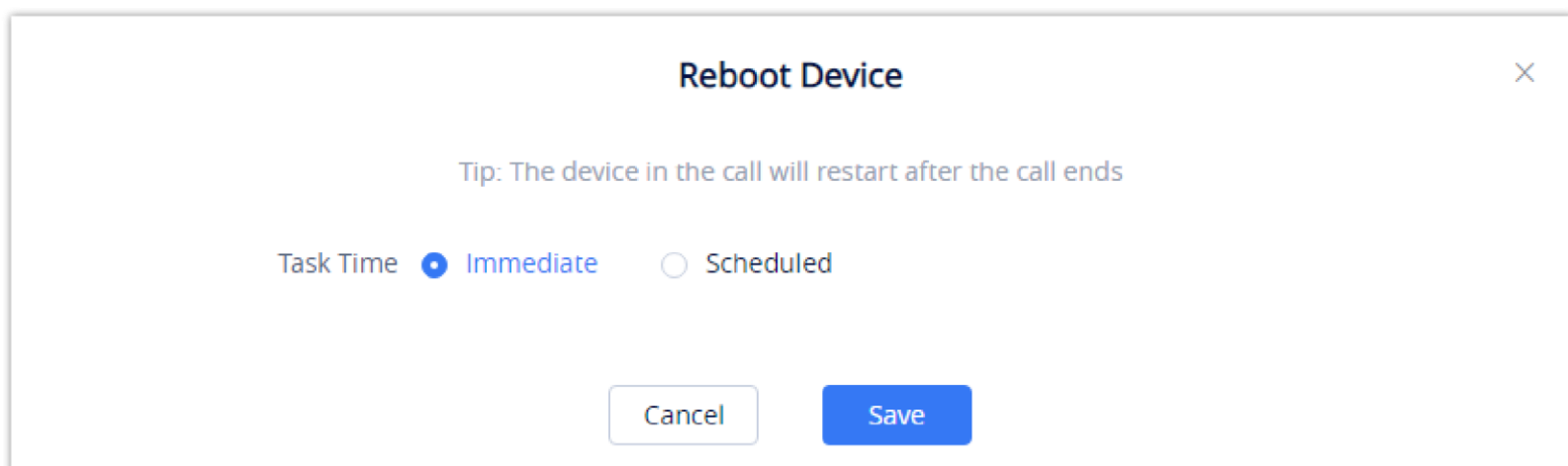


Virtual Device Interface

Reboot VoIP Device

Users could reboot one device or a batch of devices on the GDMS platform.

1. Select the desired devices and click on **More** → **Reboot Device**.



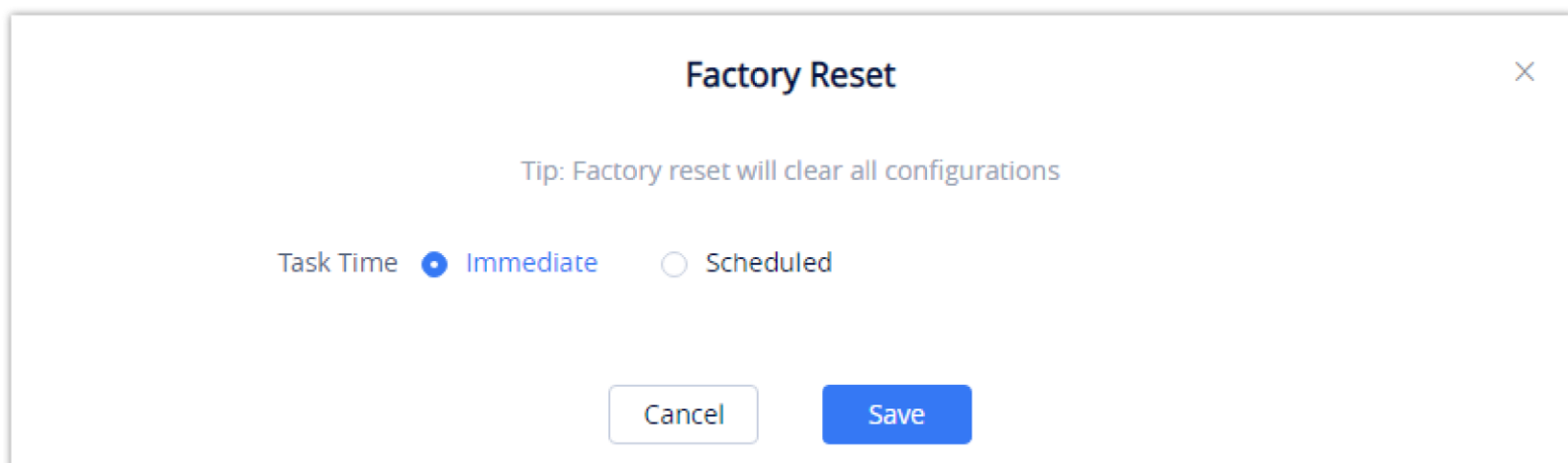
Reboot Device

2. **Task Time:** Select when to start the device reboot. Users can choose to reboot immediately or schedule the reboot for a specific time.
3. Click on the **Save** button to create the task. Users can check the status of the reboot by navigating to the **Task Management** page.

Factory Reset

Users could factory reset one device or a batch of devices on the GDMS platform.

1. Select the desired devices and click on **More** → **Factory Reset**.



Factory Reset

2. **Task Time:** Select when to factory reset the device. Users can choose to factory reset the device immediately or to schedule the factory reset for a specific time.

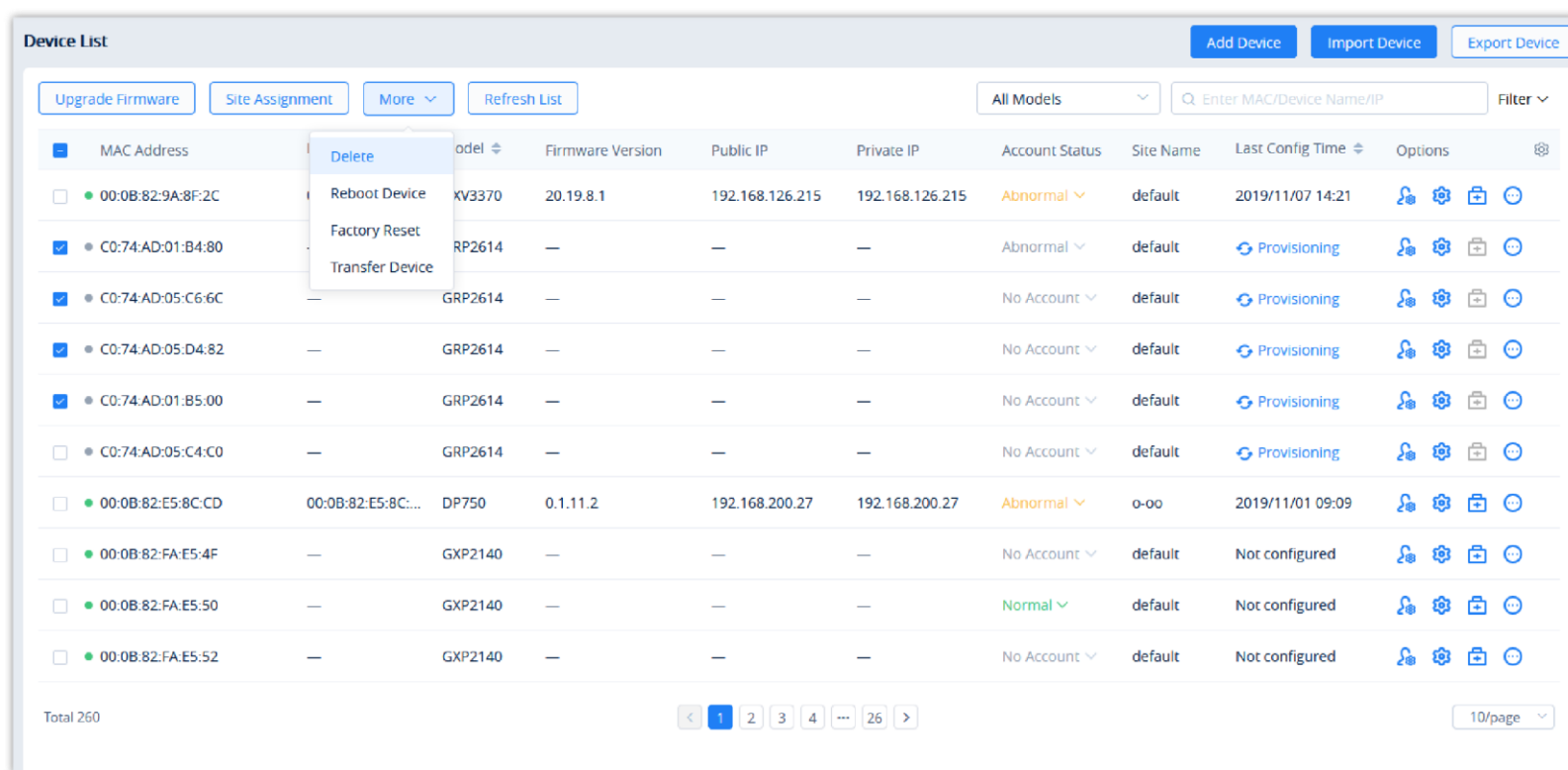
3. Click on the **Save** button to create the task. Users can check the status of the reboot by navigating to the **Task Management** page.

! Factory resetting a device will erase all existing settings on it such as accounts, call history, contacts, etc. The device will synchronize with GDMS the next time it goes online after the factory reset.

Delete VoIP Device

Users could delete one device or a batch of devices on the GDMS platform.

1. Select the desired devices and click on **More → Delete**.

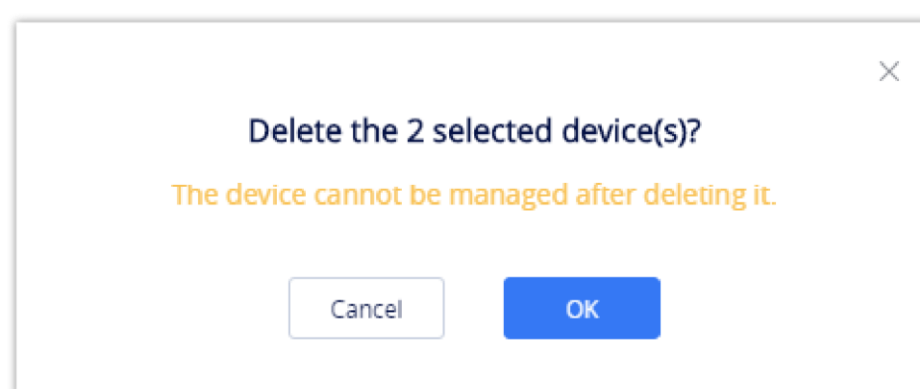


The screenshot shows the 'Device List' interface. At the top, there are buttons for 'Add Device', 'Import Device', and 'Export Device'. Below these are 'Upgrade Firmware', 'Site Assignment', 'More', and 'Refresh List' buttons. A search bar contains 'Enter MAC/Device Name/IP' and a 'Filter' dropdown. The table below has columns: MAC Address, Model, Firmware Version, Public IP, Private IP, Account Status, Site Name, Last Config Time, and Options. A 'More' dropdown menu is open over the first few rows, with 'Delete' selected. The table contains 10 rows of device information.

MAC Address	Model	Firmware Version	Public IP	Private IP	Account Status	Site Name	Last Config Time	Options
<input type="checkbox"/> 00:0B:82:9A:8F:2C	XV3370	20.19.8.1	192.168.126.215	192.168.126.215	Abnormal	default	2019/11/07 14:21	[Icons]
<input checked="" type="checkbox"/> 00:74:AD:01:B4:80	RP2614	—	—	—	Abnormal	default	Provisioning	[Icons]
<input checked="" type="checkbox"/> 00:74:AD:05:C6:6C	GRP2614	—	—	—	No Account	default	Provisioning	[Icons]
<input checked="" type="checkbox"/> 00:74:AD:05:D4:82	GRP2614	—	—	—	No Account	default	Provisioning	[Icons]
<input checked="" type="checkbox"/> 00:74:AD:01:B5:00	GRP2614	—	—	—	No Account	default	Provisioning	[Icons]
<input type="checkbox"/> 00:74:AD:05:C4:C0	GRP2614	—	—	—	No Account	default	Provisioning	[Icons]
<input type="checkbox"/> 00:0B:82:E5:8C:CD	DP750	0.1.11.2	192.168.200.27	192.168.200.27	Abnormal	o-oo	2019/11/01 09:09	[Icons]
<input type="checkbox"/> 00:0B:82:FA:E5:4F	GXP2140	—	—	—	No Account	default	Not configured	[Icons]
<input type="checkbox"/> 00:0B:82:FA:E5:50	GXP2140	—	—	—	Normal	default	Not configured	[Icons]
<input type="checkbox"/> 00:0B:82:FA:E5:52	GXP2140	—	—	—	No Account	default	Not configured	[Icons]

Delete Device

2. Click on the **OK** button on the pop-up window to confirm deleting the devices, and the selected devices will be deleted immediately from the GDMS platform. The scheduled tasks involving the deleted devices will be canceled too.



Delete Device Prompt

Export VoIP Device

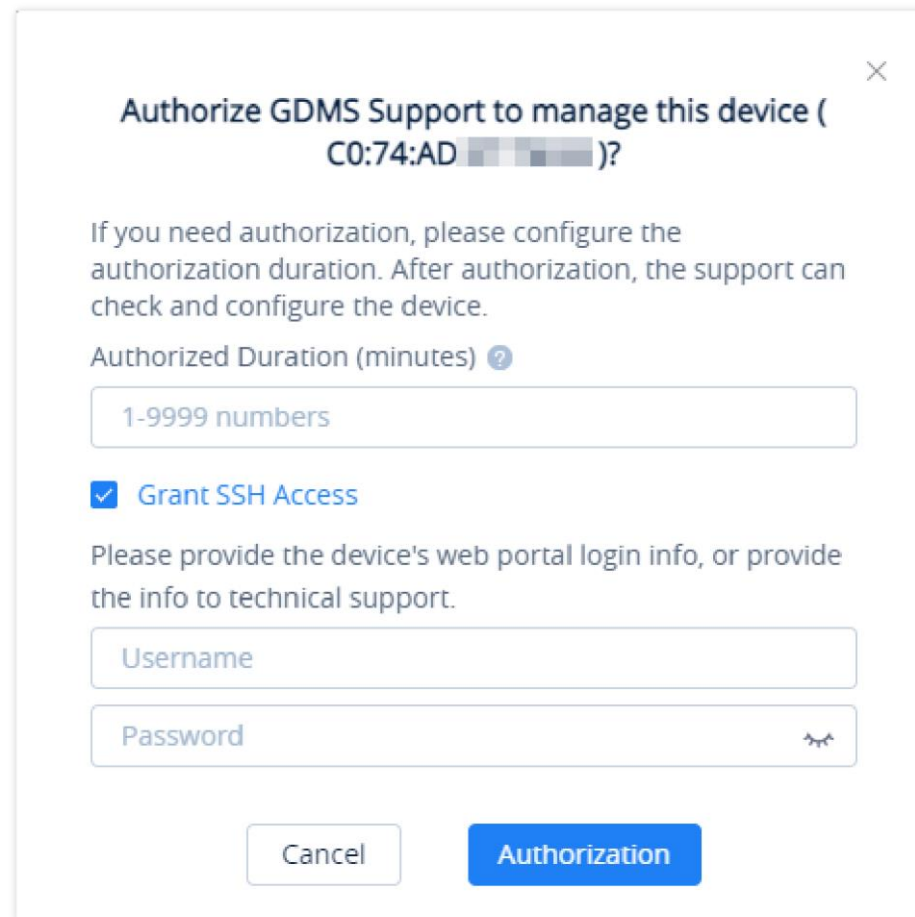
To export the entire device list, click on the **Export Device** button in the top-right corner of the device list page. The exported list includes all device and account information.

Manage Device via GDMS Support

If the user's device is abnormal and wants Grandstream Support to troubleshoot the problem, the user can enable to manage the device through GDMS Support.

After the authorization is assigned, Grandstream Support can diagnose the device and assign parameters to the device.


1. On the VoIP Device list, click the “More” button  following the device and select to access the “Authorization Management” interface, as the screenshot shows below:

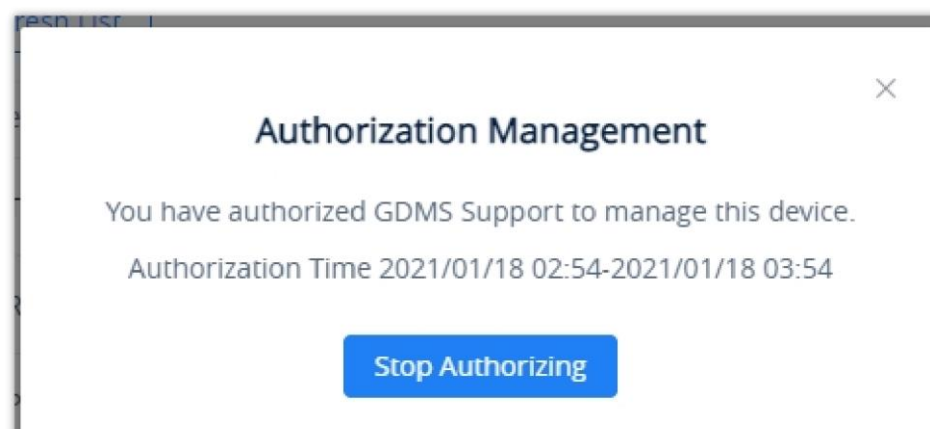


Authorization Management

2. Enter the authorization duration, which can be set between 1 to 9999 minutes, according to the time required for problem troubleshooting.
3. Tick “Grant SSH Access” box to grant access using SSH, then enter the username and password of the VoIP endpoint device SSH information.
4. Once the user clicks the “Authorization” button, Grandstream Support can only manage the device within the authorization period. Once the authorization period ends, Grandstream Support cannot manage the device.

Stop Authorizing Manually

1. When the problem is confirmed, the user can end authorization manually. The user can click the “More” button  following the device, and select to access the “Authorization Management” interface, as the screenshot shows below:



Stop Authorizing Manually

2. The user can click the “Stop Authorizing” button to stop managing the device immediately, and then Grandstream Support cannot manage the device.

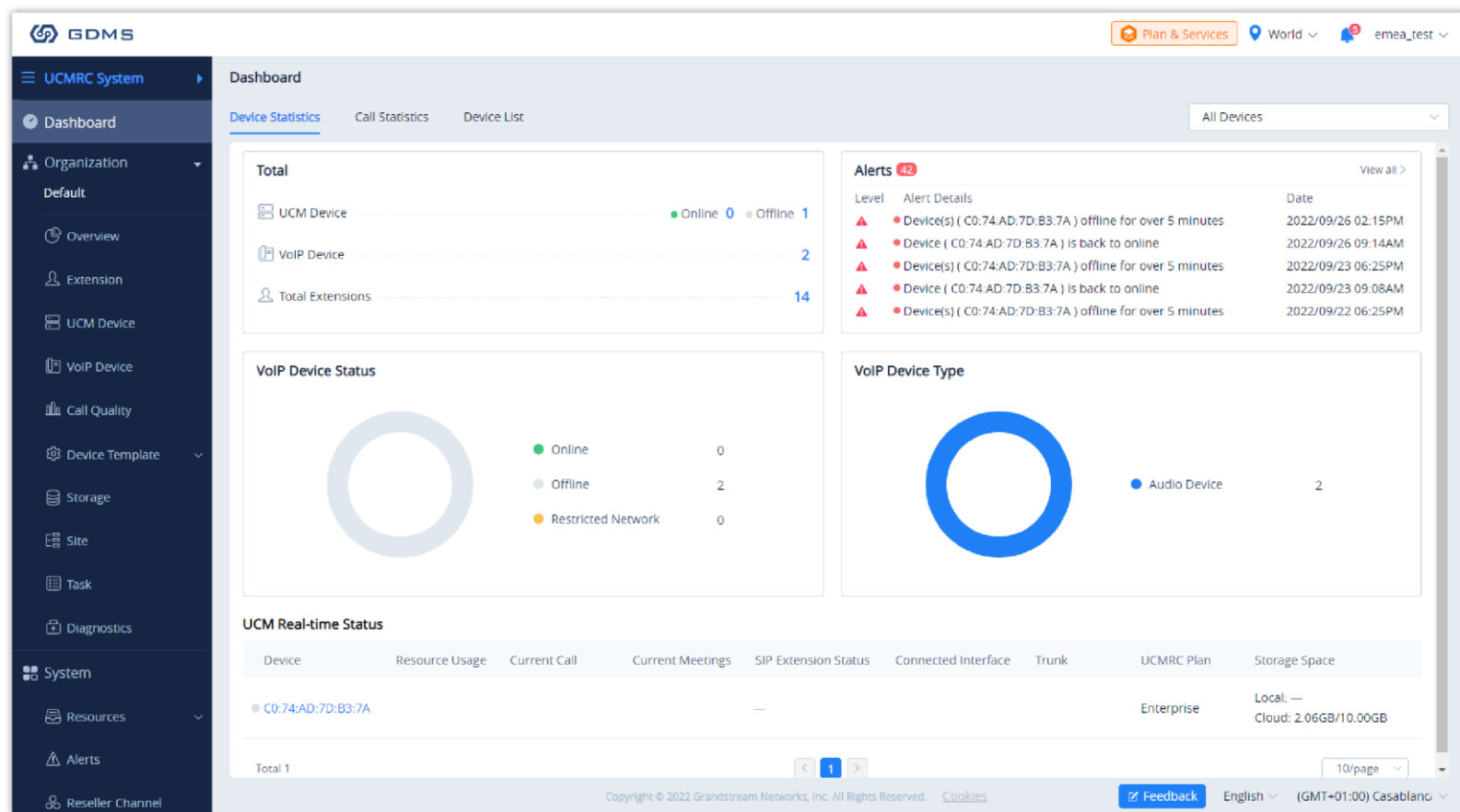
UCMRC SYSTEM

Dashboard

Device Statistics

The Device Statistics page provides an overview of the following information:

- Total Devices
- Alert Management
- VoIP Device Status
- VoIP Device Type
- UCM Real-time Status



UCMRC Dashboard

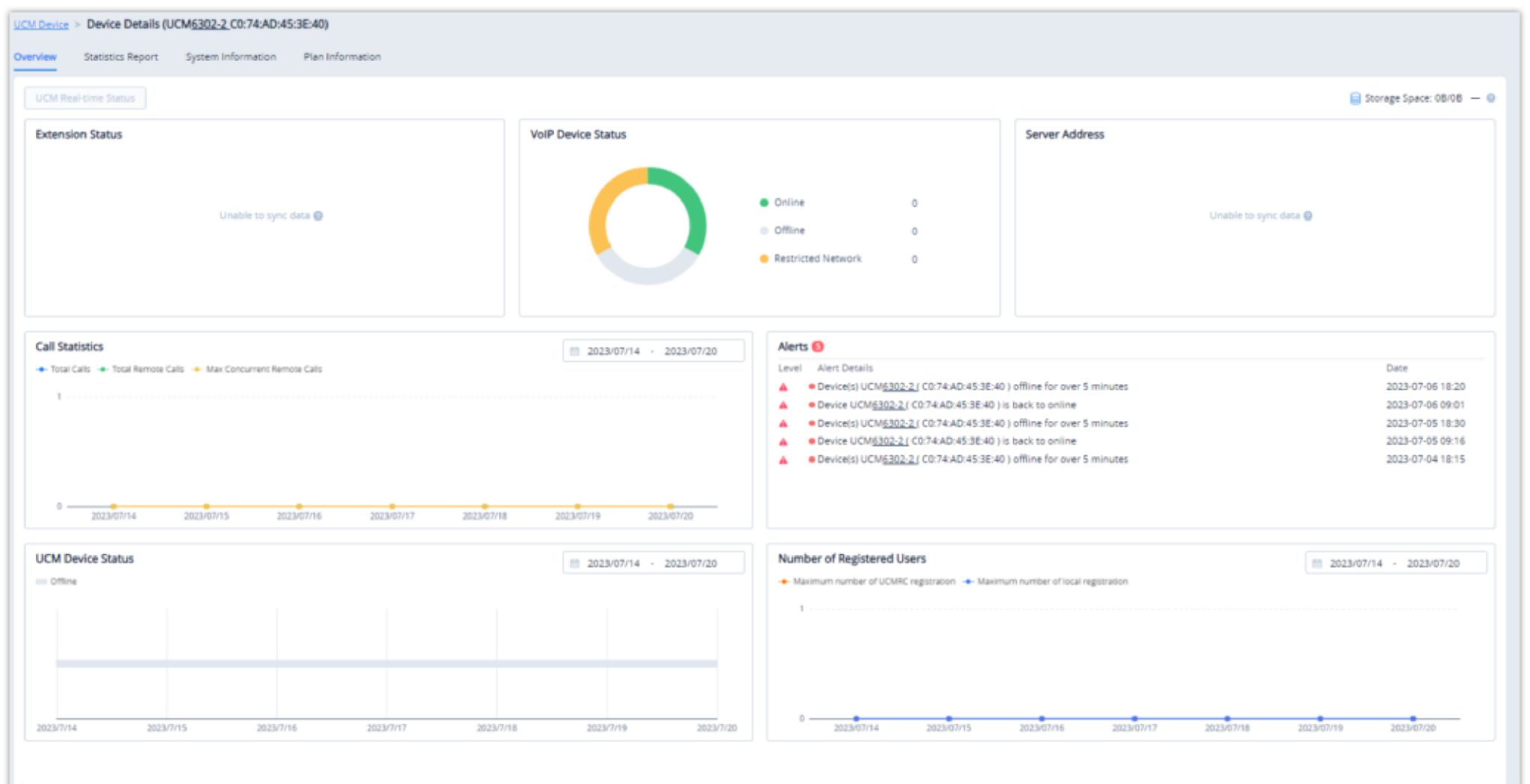
Module	Description
Total	<ul style="list-style-type: none"> ◦ UCM Device: Display the number of all UCM devices in the enterprise. ◦ VOIP Device: Display the number of VoIP devices that use the UCM extensions in the enterprise. ◦ Total Extensions: Display the number of extensions reported by all UCM devices in the enterprise.
Alert	Display the latest 5 high and medium-level alert messages of the UCM devices in the GDMS platform.
VoIP Device Status	<p>Display the number of devices that are currently online, offline, and network restricted:</p> <ul style="list-style-type: none"> ◦ Online: The network connection between the device and the GDMS platform is normal. ◦ Offline: The device is disconnected from the GDMS platform. ◦ Network Restricted: The network connection between the device and the GDMS platform is abnormal.
VoIP Device Type	<p>Display the number of devices in each category: audio and video.</p> <ul style="list-style-type: none"> ◦ Audio devices: GRP series, DP series, GXP series, and WP series ◦ Video devices: GXV series

Module	Description
UCM Real-time Status	<p>Display the real-time status of all UCM devices in the current GDMS platform:</p> <ul style="list-style-type: none"> ◦ Device: Display the MAC address of the device. ◦ Resource Usage: Display the usage of CPU and memory. ◦ Current Calls: Display the number of current calls and the remote calls. ◦ Current Meetings: Display the number of ongoing meetings. ◦ SIP Extension Status: Display the number of the extensions which have been registered and unregistered. ◦ Connected Interface: Display the names of the connected interfaces. ◦ Trunk: Display the number of total trunks, the number of trunks in idle/busy/abnormal state, and the number of trunks that are unmonitored. ◦ UCMRC Plan: Display the status of the UCMRC plans which are valid, almost expired, and expired. ◦ Storage Space: Display the storage space details of UCM local and cloud space usage. <p>Note:</p> <p>Only UCM devices firmware version 1.0.11.X or higher version support displaying the real-time status.</p>

UCMRC Dashboard Labels

UCM Device Statistics

When clicking one of the UCM devices added to the GDMS platform, the user will see an overview of the following information, **Extension Status**, **VoIP Device Status**, **Sever Address**, **Call Statistics**, **Alerts**, **UCM Device Status**, and **Number of Registered Users**.

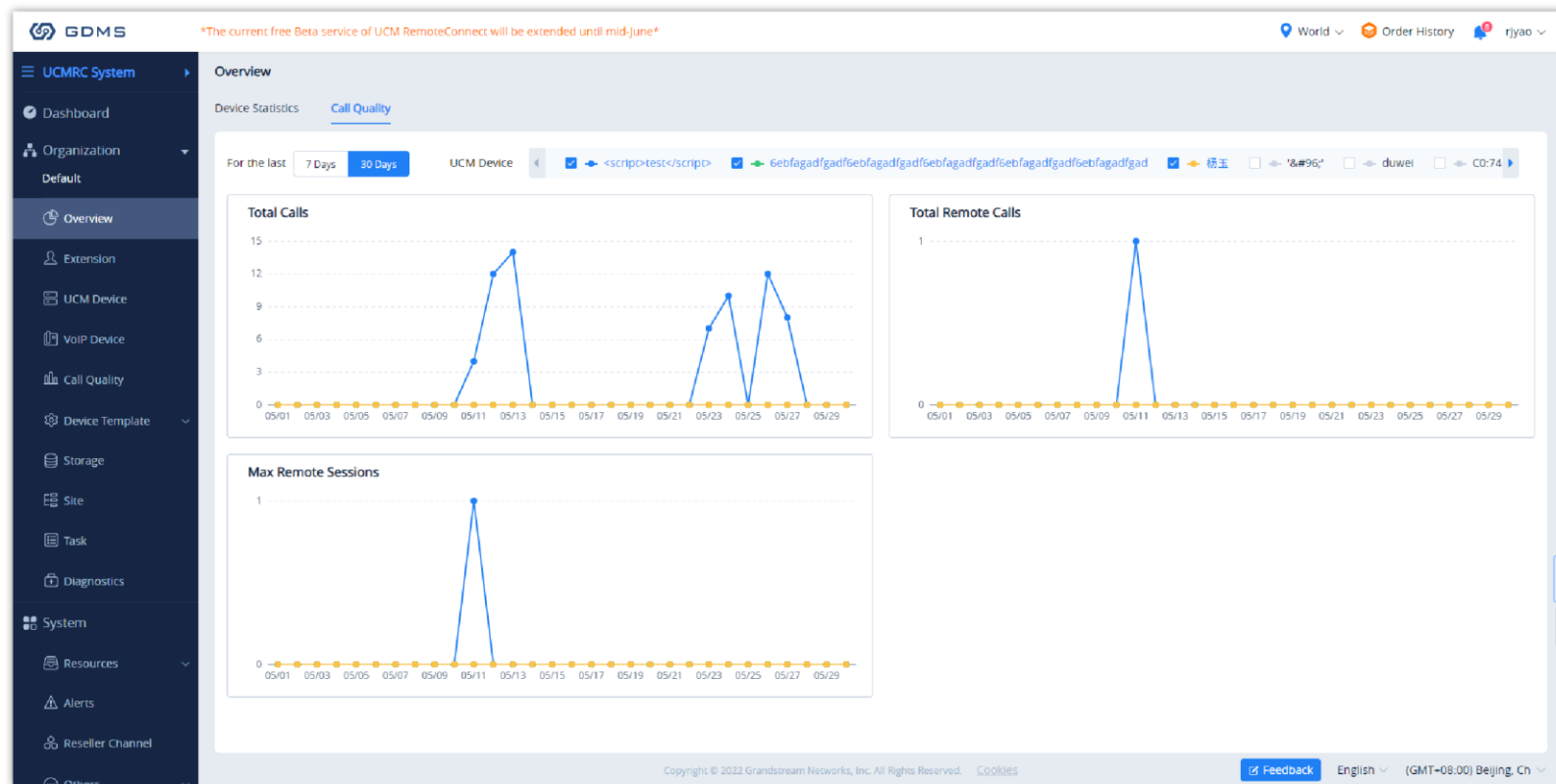


Call Statistics

The Call Statistics module displays all UCM devices' call statistics information in the current system.

The user can select up to 3 UCM devices at one time to view the call statistics information in the latest 7/30 days.

The call statistics information contents include the number of total calls, the number of total remote calls, and the number of maximum concurrent remote calls.



Call Statistics

Device List

The Device List module displays all devices listed in the UCMRC system of the current enterprise account, including the VoIP devices and PBX devices.

Users can search devices by the MAC addresses of the devices.

The screenshot shows the 'Device List' section of the GDMS dashboard. It displays a table with the following columns: MAC Address, Device Name, Device Model, Firmware Version, and Organization. The table contains 10 rows of device data. A search bar at the top right allows filtering by MAC/Device Name. The bottom of the table shows 'Total 1443' devices and a pagination control for 10/page.

MAC Address	Device Name	Device Model	Firmware Version	Organization
C0:74:AD:22:4D:32	C0:74:AD:22:4D:32	GRP2601	1.0.3.13	ylluo Organization
22:22:22:EA:11:23	—	UCM6301	—	Default Organization
12:12:12:12:12:12	ucm	UCM6202	—	Default Organization
C0:74:AD:41:63:69	C0:74:AD:41:63:69	GXW4248	—	Default Organization
C0:74:AD:11:50:00	C0:74:AD:11:50:00	UCM6308	—	Default Organization
C0:74:AD:48:8F:75	12:33:33:33:33:33	GRP2604	—	Default Organization
C0:74:AD:11:83:42	—	UCM6304	—	Default Organization
C0:74:AD:23:A7:8F	C074AD23A78F	GXW4200	3.5.4	ylluo Organization
00:0B:82:F6:65:90	yxuu的设11号	GXY3380	—	Default Organization
C0:74:AD:23:94:96	C0:74:AD:23:94:96	UCM6302	—	绩绩名称相同

Device List

Overview

The Overview module displays the overview information of each organization, including the Device Statistics and Call Statistics.

Device Statistics

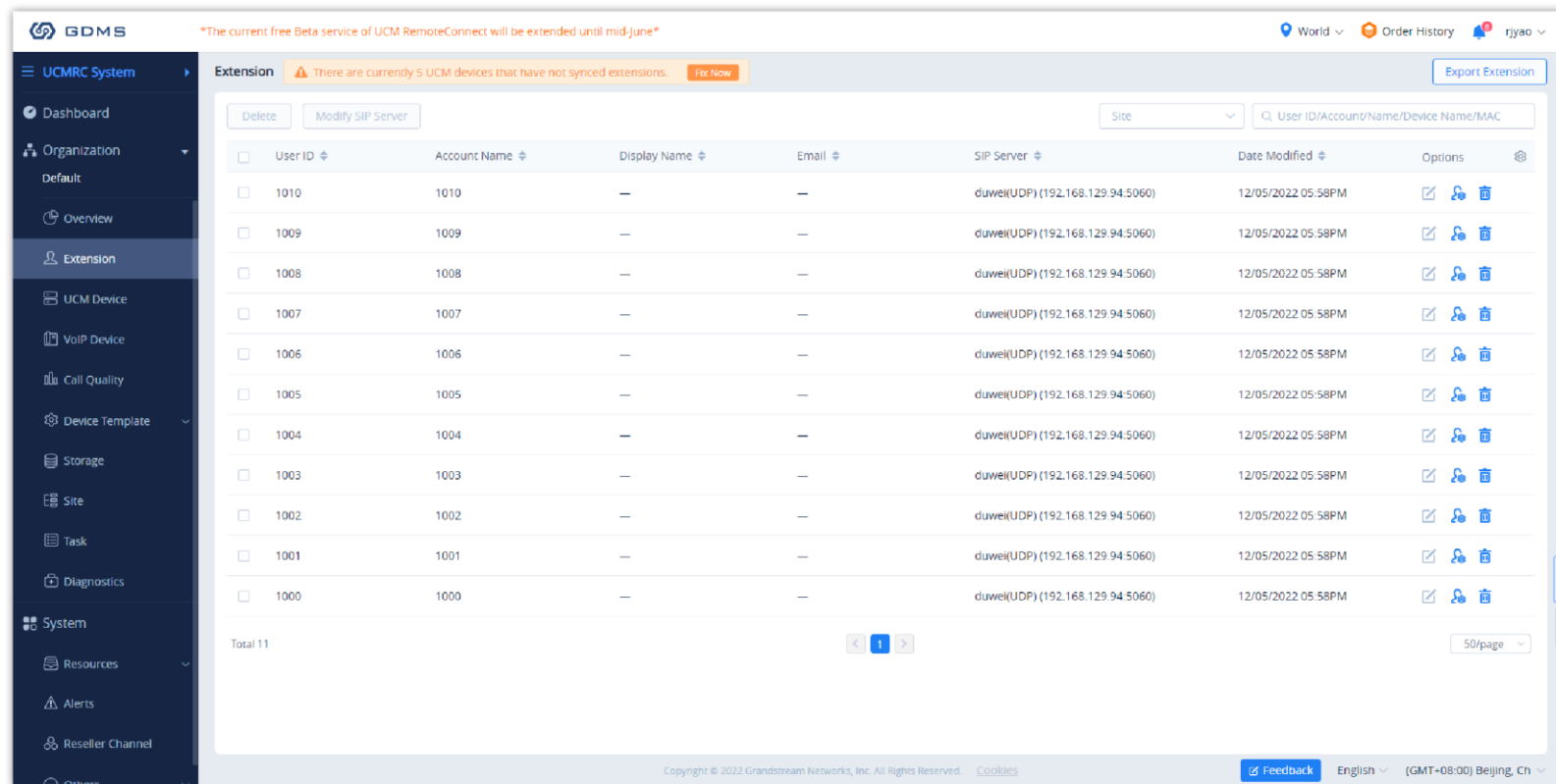
This module displays the same information in the **UCMRC system** → **Dashboard** → **Device Statistics**.

Call Statistics

This module displays the same information in the **UCMRC system → Dashboard → Call Statistics**.

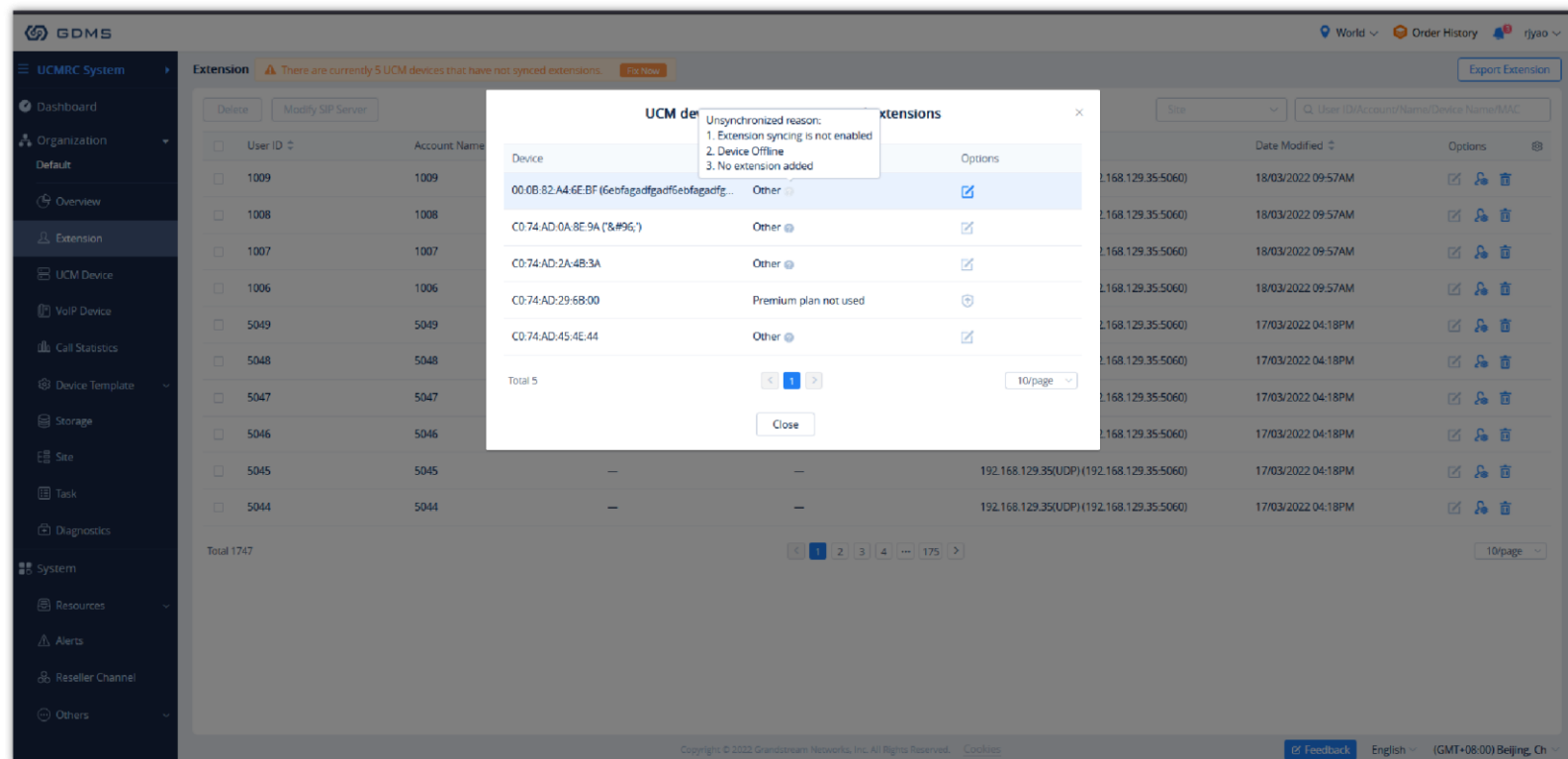
Extension

The module displays the extension information of all UCM devices in the selected organization.



Extension Management Interface

If the extensions in the UCM device have not been synchronized to the GDMS platform yet, the user can click to view the UCM devices which have not synchronized the extensions and the corresponding reasons on the GDMS platform. Please see the screenshot below:



UCM Devices That Have Not Synced Extensions

i Note

- If the user has not purchased a UCMRC plan with the corresponding feature, the user cannot synchronize the extensions in the UCM device to the GDMS platform account.
- If the user has purchased a UCMRC plan which contains the extension synchronization feature, the user needs to access the UCM device management platform to enable the “SIP Extension Synchronization” feature.

Edit Extension in UCM Web UI

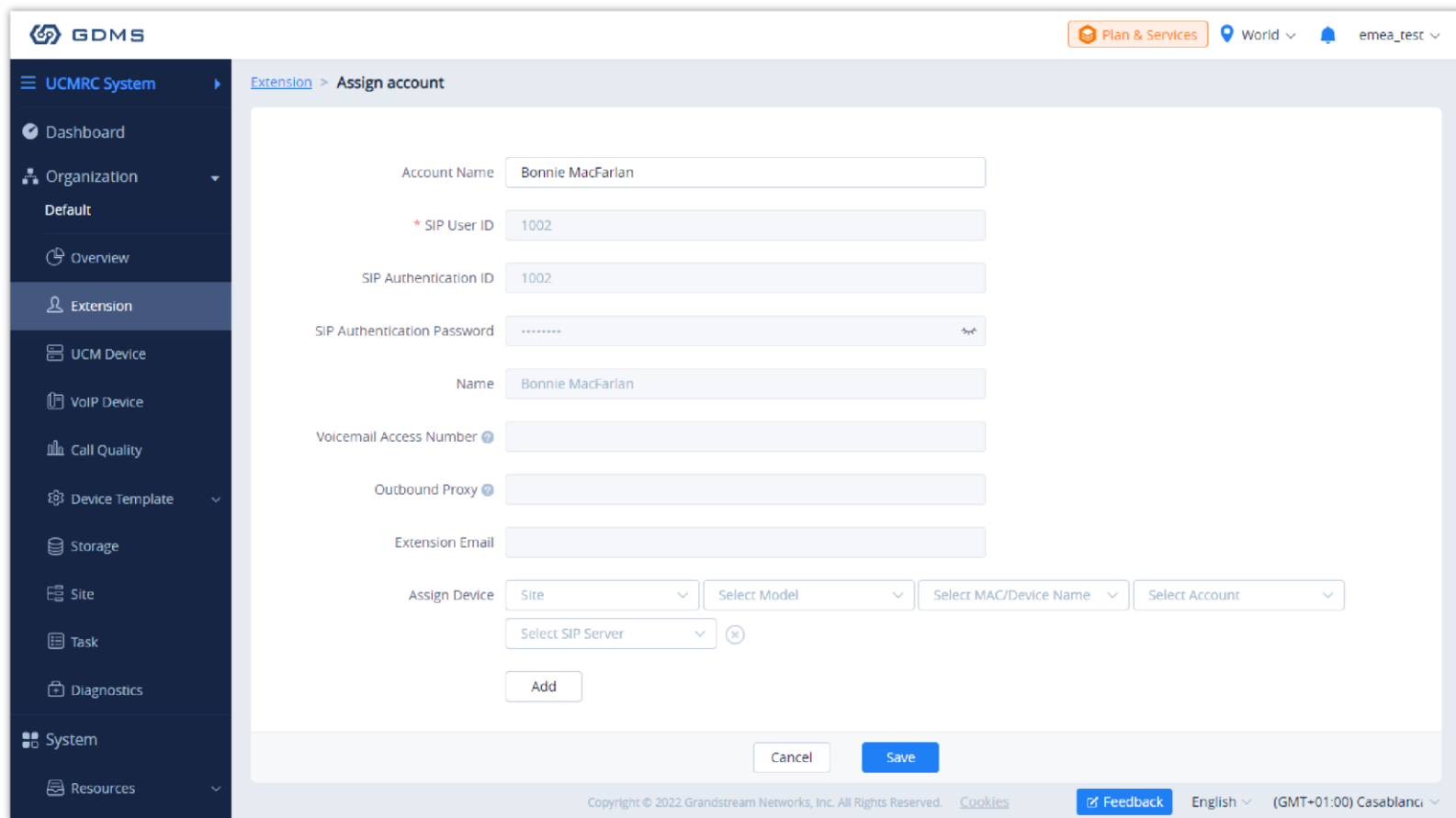
The user can click  button to access the UCM device Web UI to edit the extensions. As the screenshot shows below:

Edit Extension in UCM Web UI

! If the UCM device is currently offline, the user cannot access to the UCM device Web UI.

Assign Account

The user can click  button to assign accounts to the VoIP devices in the current system.


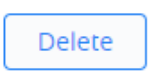


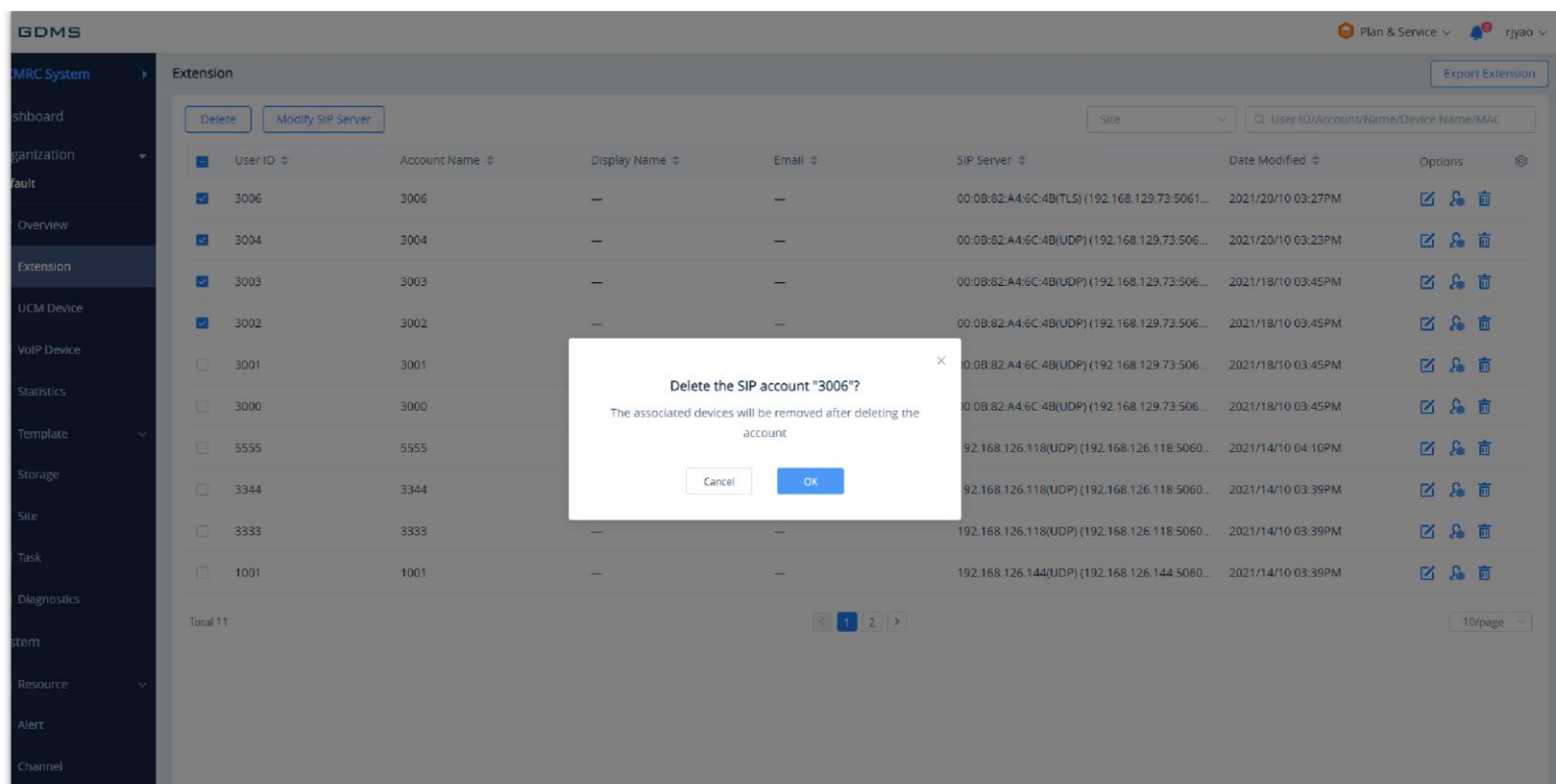
Assign Account

- !
 - Users cannot edit SIP User ID, Authentication ID, Authentication Password, Display Name, Voicemail Access Number, and Email options.
 - The SIP servers are synchronized from the UCM devices and the remote service addresses of the UCM devices. The SIP Server field cannot be edited.
 - The devices that can be assigned are the same as the devices in the VoIP system.

Delete Account

Users can delete one or multiple extensions in this module.

1. Select an extension to delete, click  button or  button to delete the extension. The user can select to delete one extension or select multiple extensions to batch delete the extensions.
2. Click on the “OK” button, the deleted extensions will be disassociated from the corresponding UCM devices.

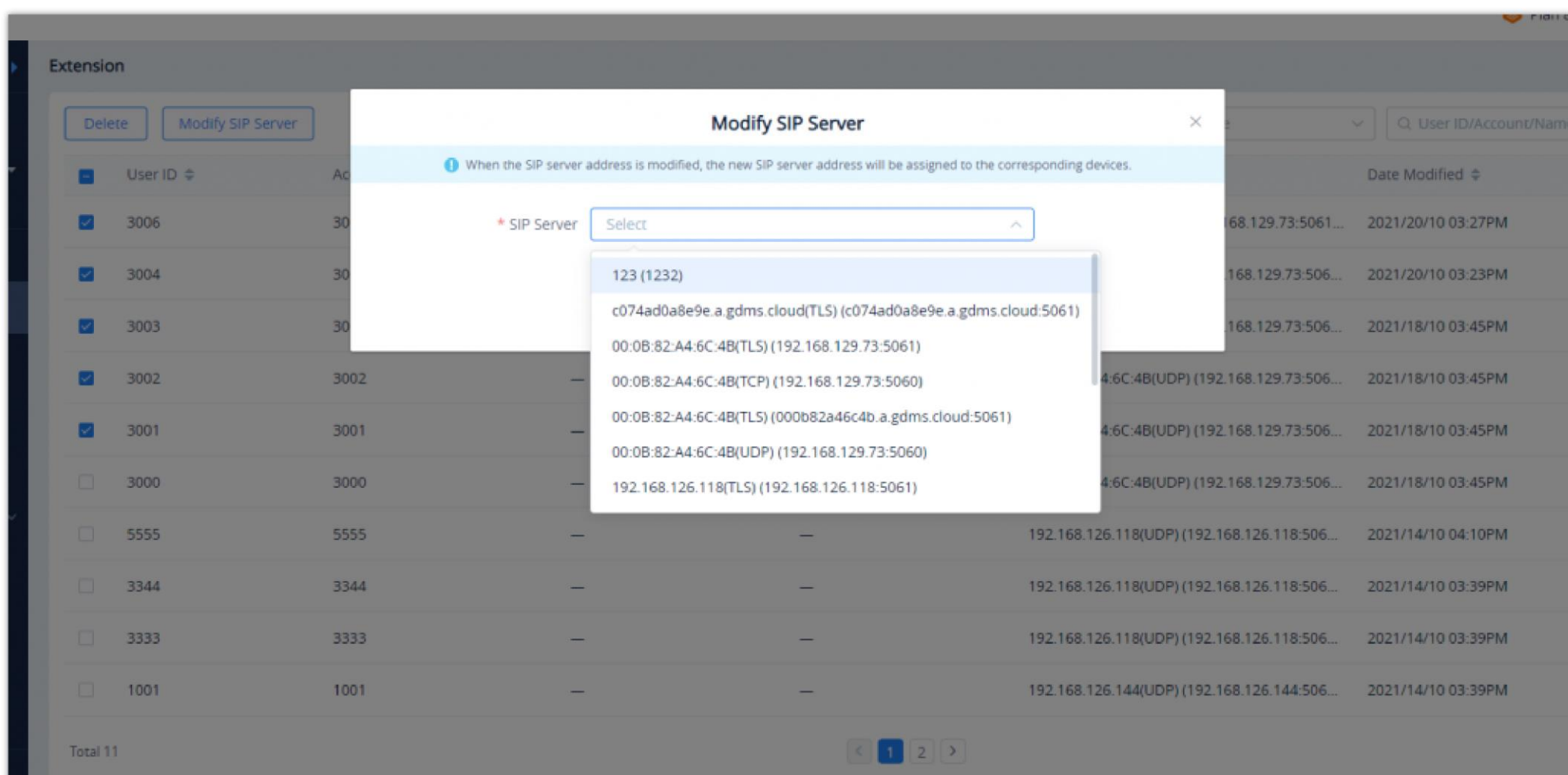


Delete Account

Modify SIP Server

Users can modify the SIP server of one or multiple extensions in this module.

1. Select the extension that the user wants to modify the SIP server.
2. Click on [Modify SIP Server](#) button and select the new preferred SIP server.
3. Click on the “OK” button to apply the changes. Once the SIP server is modified, the new SIP server settings will be assigned to the associated device.



Modify SIP Server

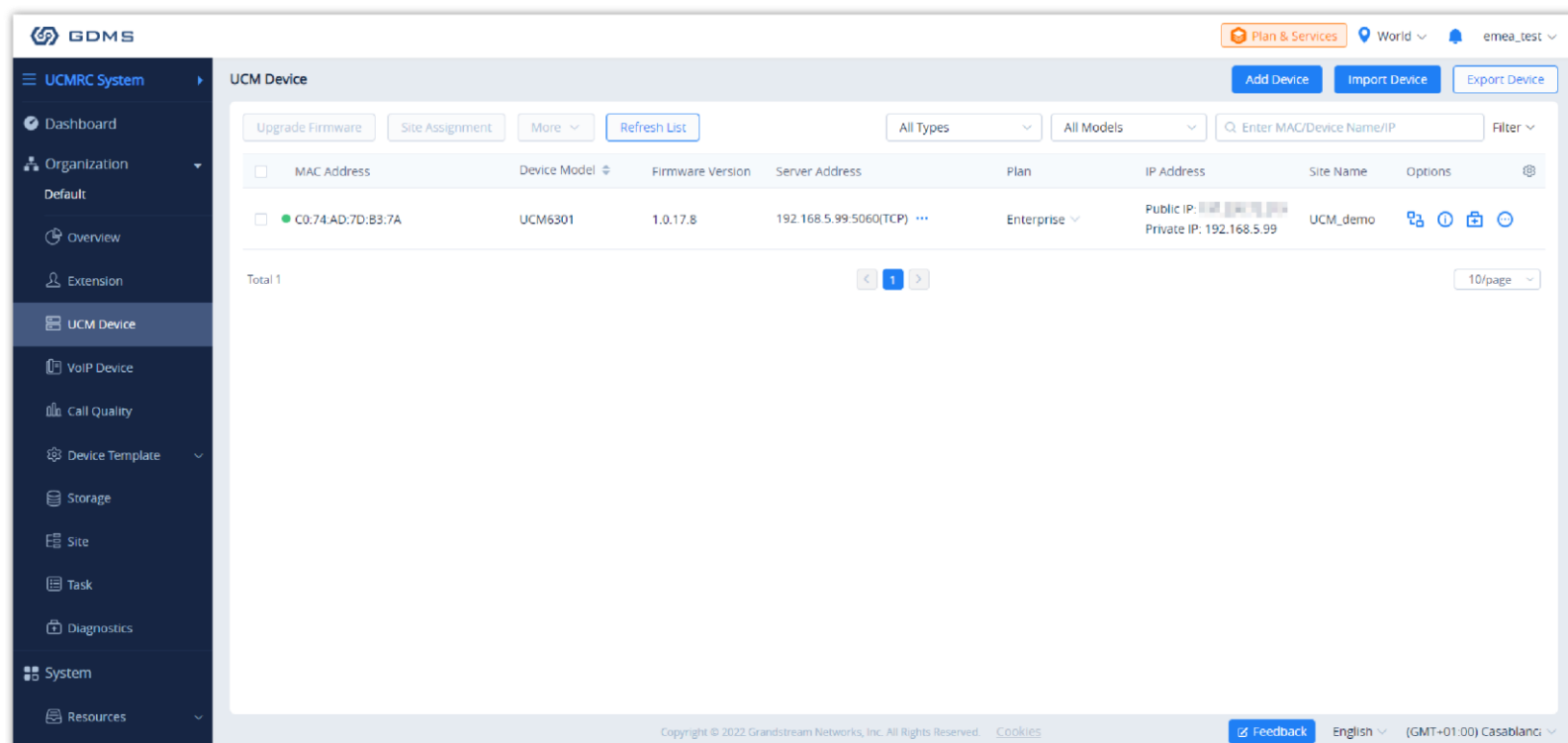
Export Extension

Users can click the “**Export Extension**” button on the right upper corner of the Extension module to export the extensions in the current enterprise in the GDMS platform.

i Users cannot add extensions in this module, and all extensions are synchronized from UCM devices.

UCM Device Management

The UCM Device menu shows all associated UCM devices. Users can view the firmware version numbers, IP addresses, plans, and other information of the UCM devices. It also allows users to access the device, upgrade firmware, reboot the devices remotely, etc.



UCM Device Management Interface

Status	Description
Status indicator	<ul style="list-style-type: none"> The device is offline. The device is online. The device network penetration (NAT) is abnormal, the GDMS server cannot connect to the device, but the device can periodically execute
Firmware version too low	<p>⚠ This icon indicates device firmware version too low and the device cannot be used normally with GDMS.</p>
Plan expiring	<p>Expire Soon This indicator means the plan is expiring soon or already expired.</p>

Table 17: UCM Device Management



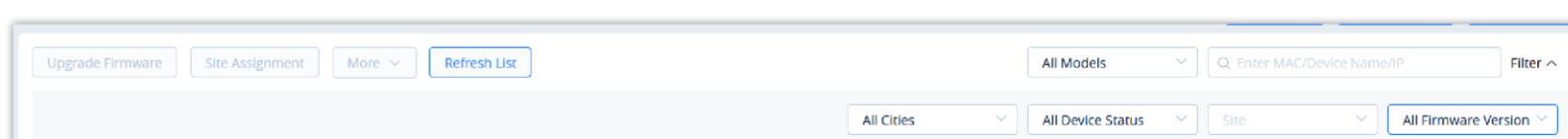
Operation	Description
Sorting	Click on the sorting buttons  to sort the list by various columns in ascending/descending order.
Custom Display Option	Click on the  button on the top right corner of the list to select the columns to show and/or hide.
Search	In addition to being able to search for devices with the search bar near the top-right corner of the page, users can further refine search results by clicking on the Filter button by specifying device status, site, city, and firmware version.

Table 18: Operation Instructions



Search Devices

Add UCM Device

To add a new UCM device to the GDMS platform, users can click on the **Add Device** button. Please see the screenshot below:

The screenshot shows a modal dialog titled "Add Device (To Default Organization)". It contains the following fields and options:

- Device Name:** A text input field with the placeholder "Enter Device Name (up to 64 characters)".
- * MAC Address:** Six individual input boxes separated by colons, representing the MAC address format.
- * Initial Password:** A text input field.
- * Site:** A text input field with the placeholder "Enter new site name". Below it is a link "Select from existing sites".
- Enable Cloud Storage for UCM:** A checkbox that is checked, with a help icon.
- Buttons:** "Cancel" and "Save" buttons at the bottom.

Add UCM Device

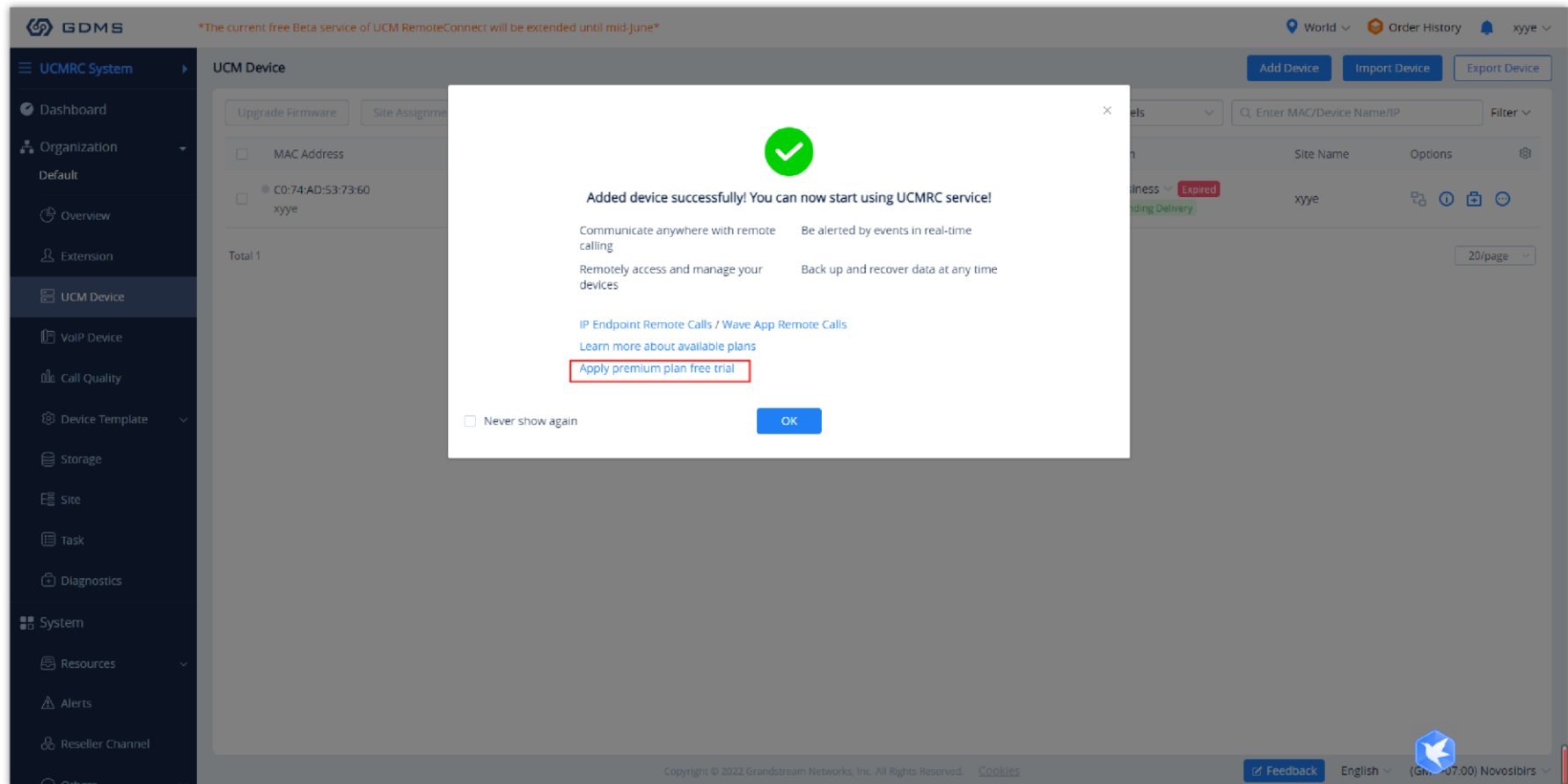
Device Name	(Optional) This option is used to set the name of the device so that the users could identify this device. The maximum number of the input characters is up to 64.
MAC Address	(Required) This option is used to enter the MAC address of the device. (Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package. Or the address can be viewed on the UCM Web GUI → System Status → System Information → Network interface (LAN MAC address).
Initial Password	(Required) This option is used to enter the Initial Password of the device. The original password can be viewed on the UCM's case or LCD.
Select Site	(Required) This option is used to set which site this device belongs to. The newly created site name is the same as the name of the UCM device, as the first level site. The user can also select another site.
Enable Cloud Storage for UCM	After enabling the option, the recording files and chats will be stored to the GDMS if the UCM device has the paid UCMRC plan.

Table 19: Add UCM Device



- Currently, users can only add UCM63xx and OEM devices to the GDMS platform.
- When the device is added to the GDMS platform successfully, the SIP accounts in UCM63xx will be synchronized to the GDMS platform by default. If the user wants to turn off the synchronization function, please refer to the UCM63xx RemoteConnect Guide for details.
- Users could click on the "Save" button to save the configuration.
- Each device can only be associated with only one GDMS account.
- Users can use the search bar on the Device page to find added devices via device name, MAC address, and sites.

After clicking the “Save” button, the device will be added to the GDMS platform successfully, and the user can apply for a UCMRC advanced plan free trial for this device



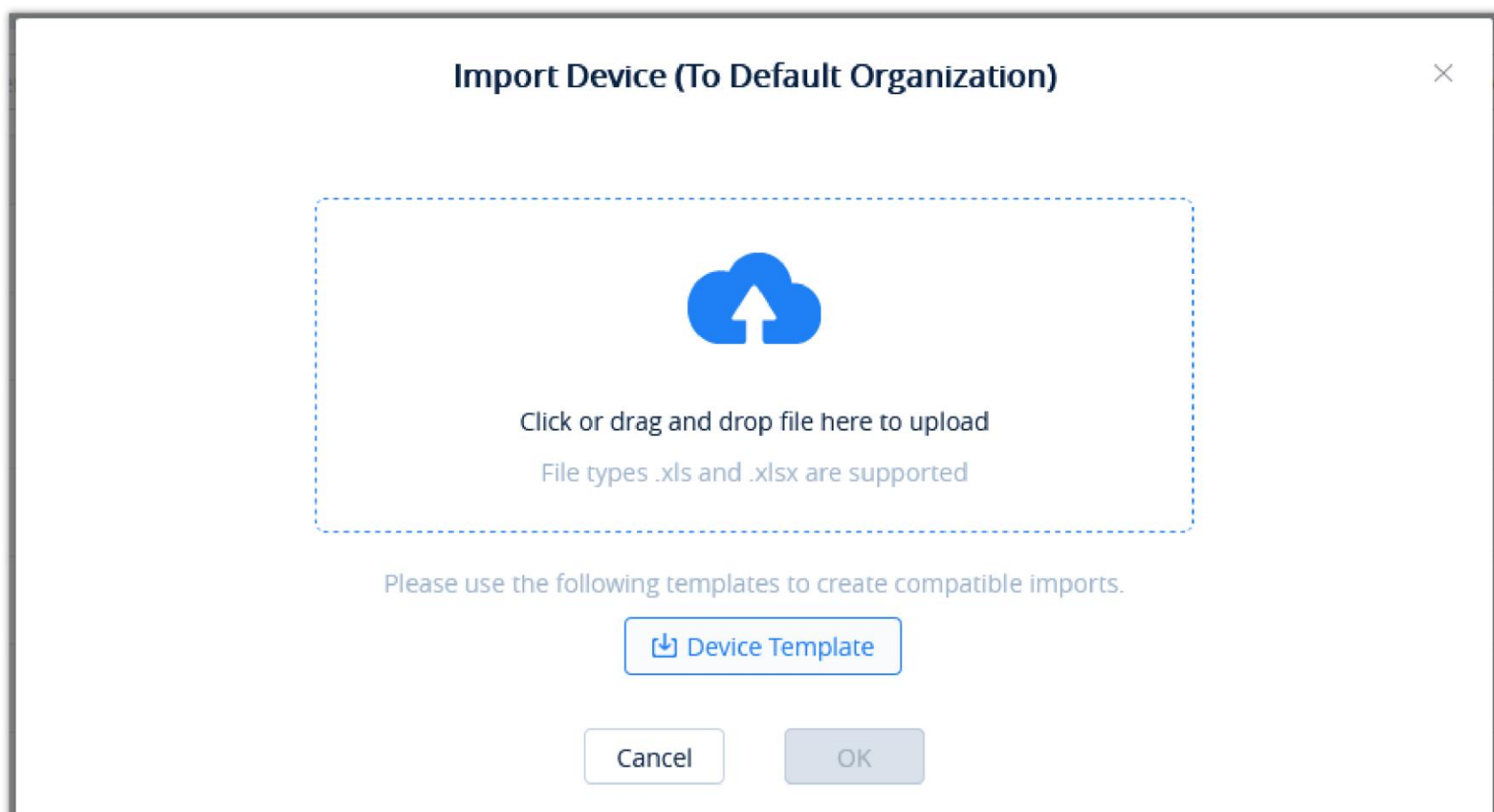
Added Device Successfully

i Notes

- Each UCM device only can apply for a UCMRC advanced plan free trial once for 3 months. If the user purchased a UCMRC plan before or applied for a UCMRC plan free trial before, the user cannot apply for another free trial anymore.
- If the user has not applied for a UCMRC plan free trial before, the user can apply for it on the “UCM Devices” list.

Batch Import UCM Devices

Users can import multiple devices by uploading a file. Click on the **Import Devices** button on the **Device** page to get started. The following window will appear:



Import UCM Device

- Click on the **Device Template** button to download the template. Users must follow the instructions to enter the required information.

- o The template will have the following fields:

MAC Address	Users need to fill in the MAC address of the device in this field (Required). For instance, 000B82E21234, and it supports to fill “:” and “-” characters in this field.
Original Password	Users need to fill in the original password of the device in this field (Required). The original password can be viewed on the UCM’s case or LCD.
Device Name	This option is used to set the name of the device so that the users could identify this device (Optional). The maximum number of the input characters is up to 64.
Site Name	Enter the site to assign this device to (Required). If the site is under more than one level, all site levels must be included in the site name (e.g. first_level/second_level/.../new_site). If the site level does not exist, it will be automatically created. The maximum character limit is 64.

Table 20: Import UCM Device Template

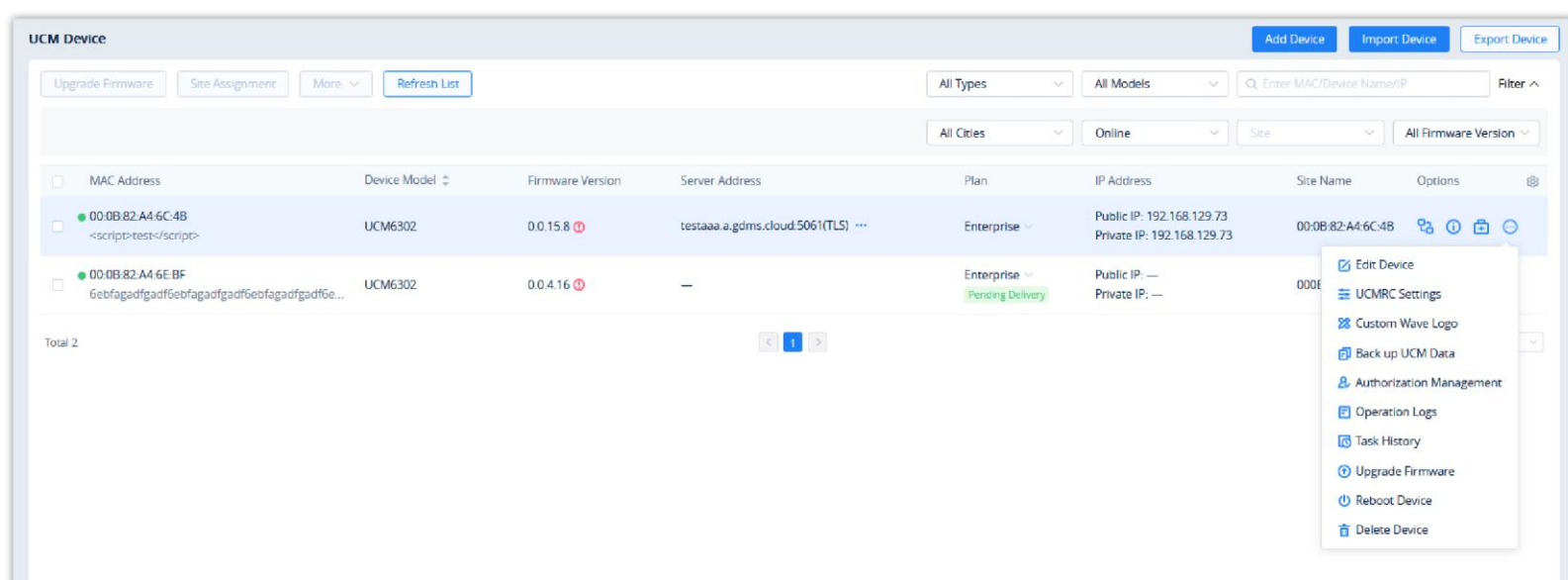
- o Users can drag the file to the pop-up window, or they can click the upload button to select a file from their PC to import.
- o Once the file is imported into GDMS, the result window will appear. If any data failed to import successfully, users can export the problematic data, re-edit, and attempt to import them into GDMS again.



- o Currently, users can only add UCM63xx devices to the GDMS platform.
- o When the device is added to the GDMS platform successfully, the SIP accounts in UCM63xx will be synchronized to the GDMS platform by default.
- o If the user wants to turn off the synchronization function, please refer to the UCM63xx RemoteConnect Guide for details.
- o If an existing device on GDMS is imported, the device’s existing information will be replaced with the newly imported information.
- o If a device’s MAC address and serial number are invalid, the import will fail.

View UCM Device Details

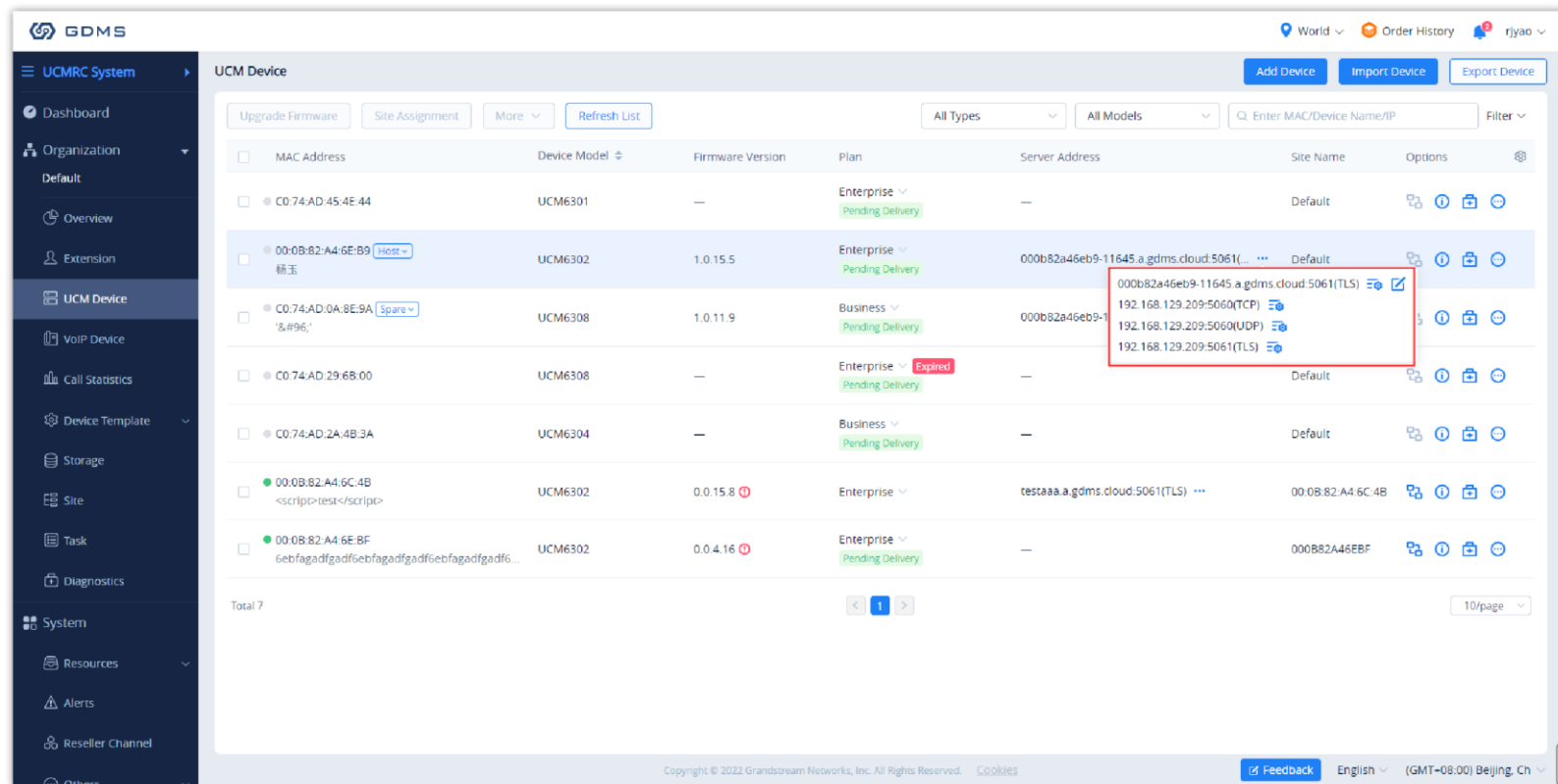
Click on the button to view a specific device’s system information.



View UCM Device Details

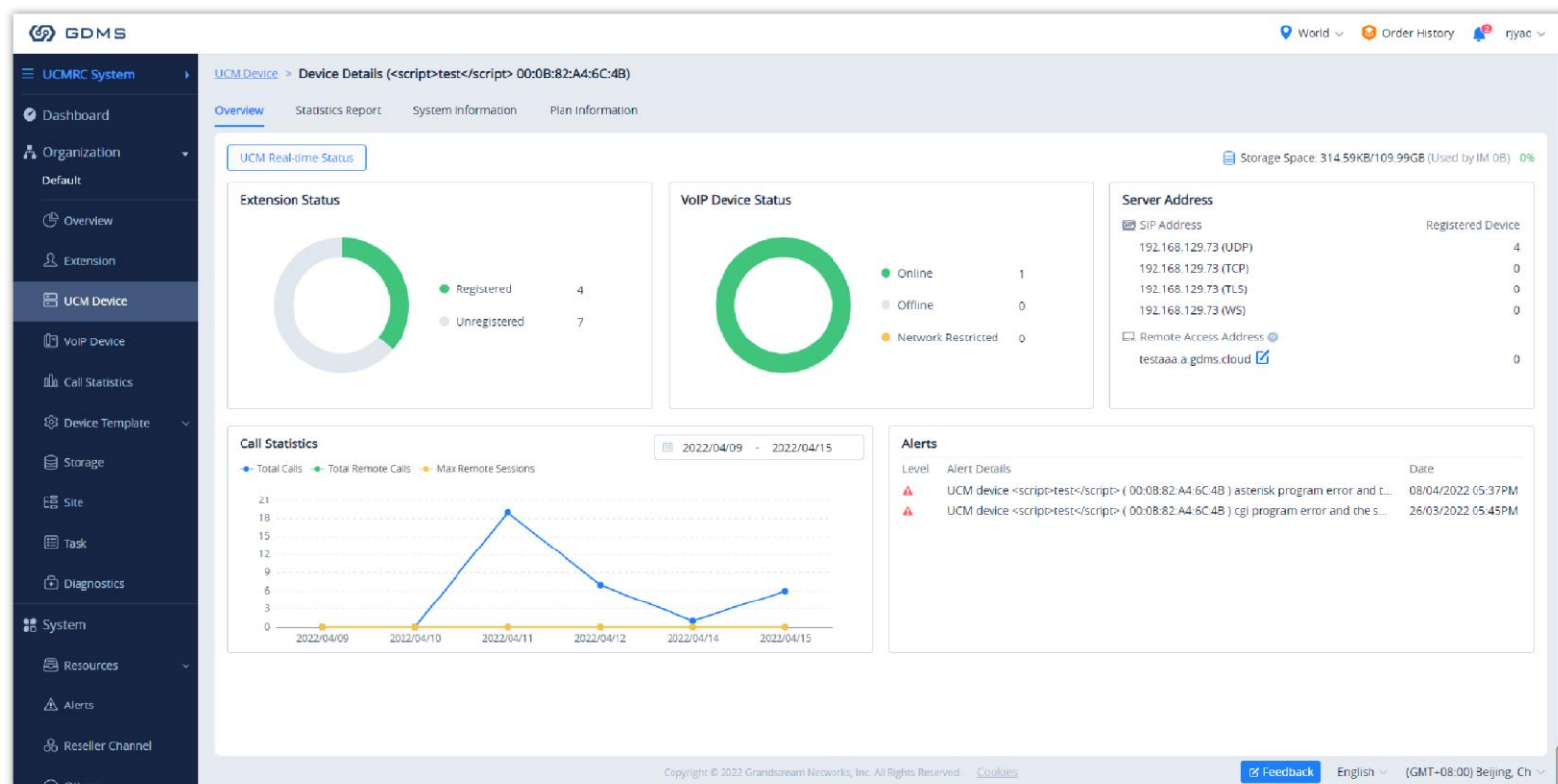
In the UCMRC system, the user can quickly view all SIP server addresses in the Device List. For a certain SIP server address, the user can quickly view the advanced settings of the SIP server, including all advanced settings of the SIP server in the VoIP system.

The device details include System information, Network information, etc.



UCM Device Details

The device details include System information, Network information, etc.

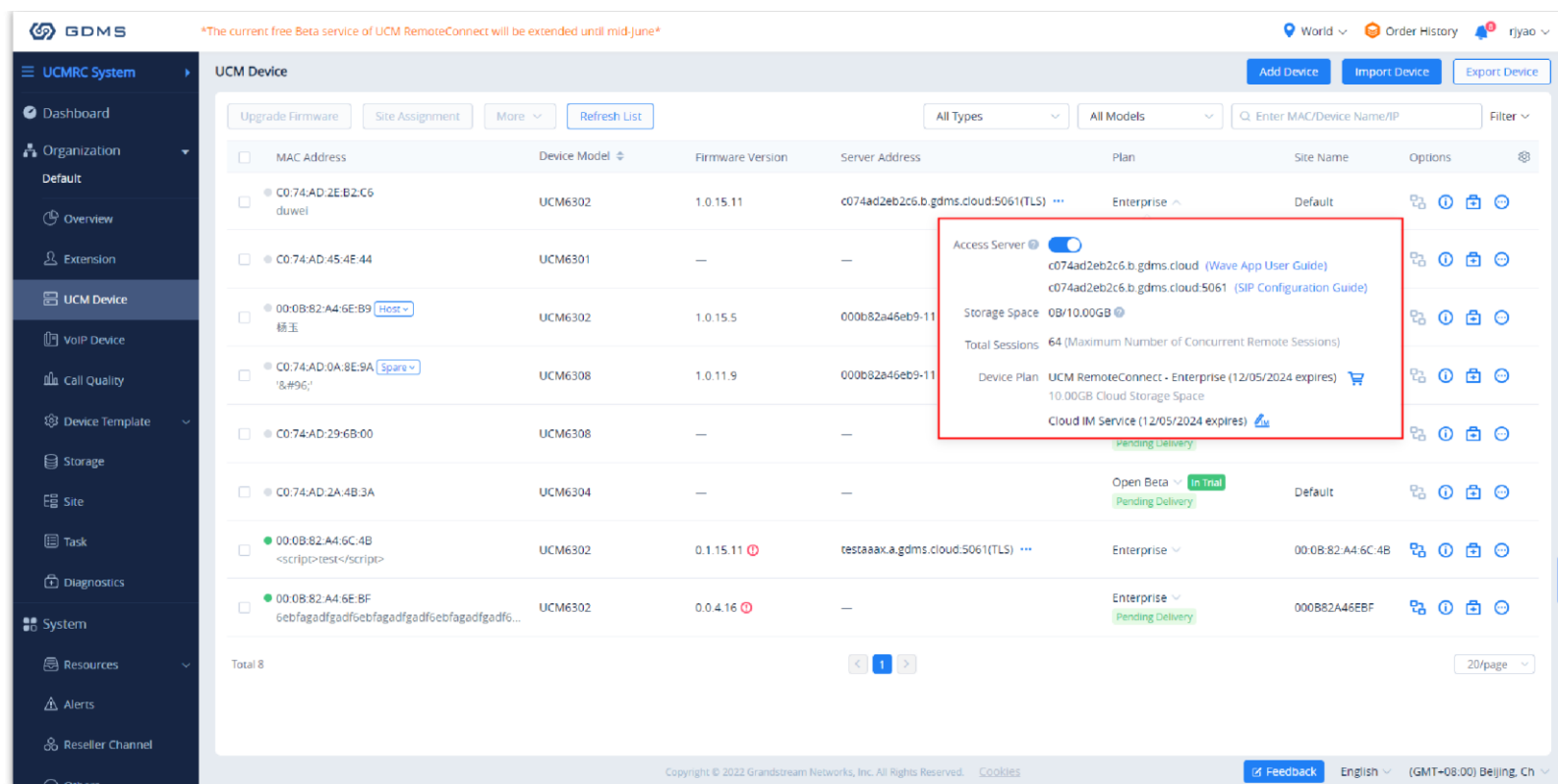


UCM Device Details


i The information on this page is obtained from the device in real-time. If the device is offline, the details page will be inaccessible.

View Device Plan

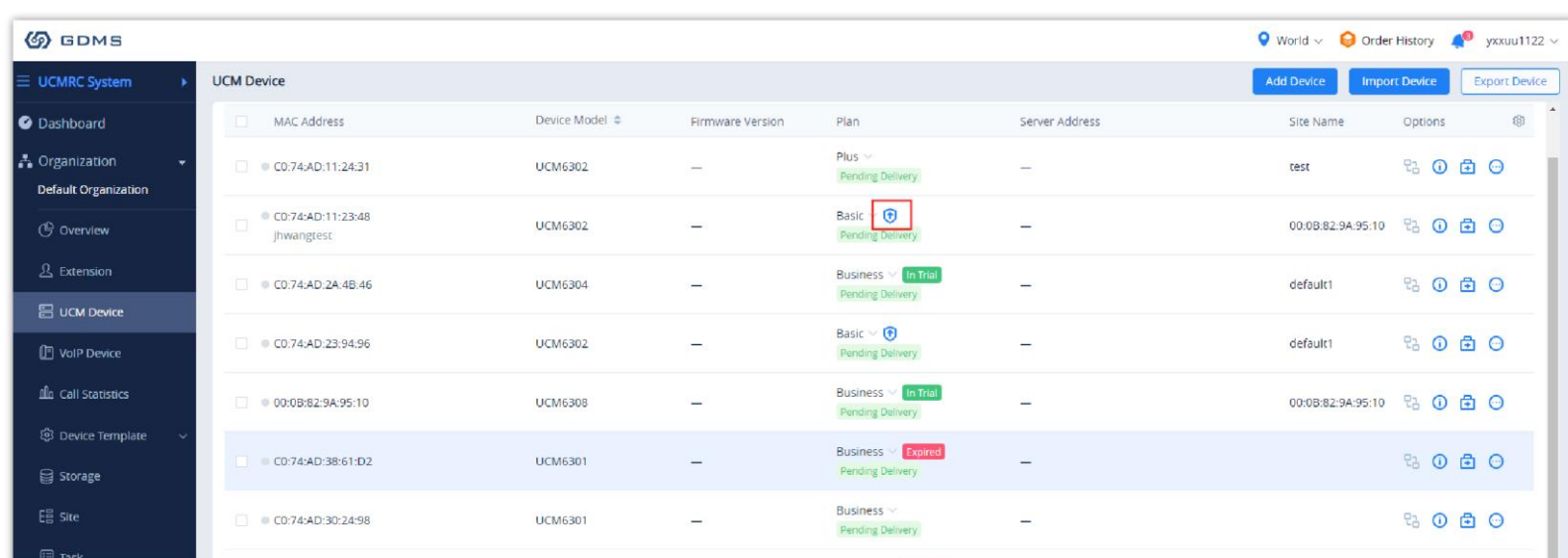
Select the plan for a specific UCM device to view the plan of the device, expiration date, currently used cloud storage space, and total cloud storage space.



View UCM Device Plan

<p>Access Server</p>	<p>This is used to configure Wave phones so that Wave users can connect to the UCM server and make calls at any time, anywhere on any network.</p> <p>If the user wants to configure the remote service address on the terminals for remote calls, the user can enable the button</p>  <p>and obtain the remote service address.</p>
<p>Storage Space</p>	<p>Refer to the current storage space used by the UCM device, and the total storage space of the UCM device. If there is not enough space, the backup files cannot be stored.</p> <p>The used storage space contains:</p> <ul style="list-style-type: none"> – 1 Used storage space by cloud storage (excluding the space allocated to the Cloud IM service) – The maximum storage space allocated to the Cloud IM service
<p>Device Plan</p>	<p>Refer to the current plan and add-on plan of the device. If the plan has expired, the user can only use the Basic plan as the current plan.</p>

After adding the device to the GDMS platform, the user can apply for a UCMRC advanced plan free trial for 3 months by clicking the button .



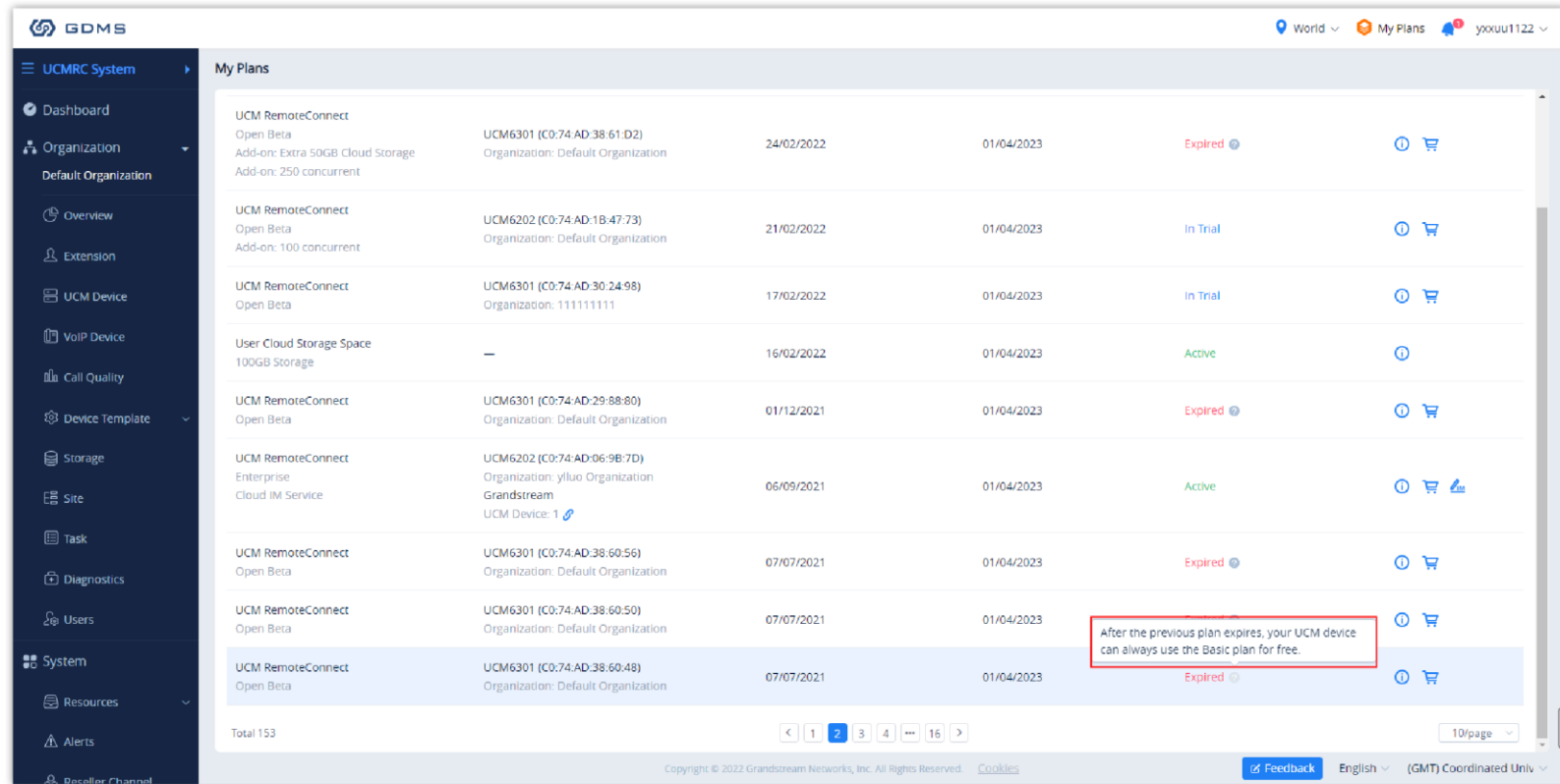
Apply for Free Trial

1. After the paid plan expires, it will be downgraded to the “Basic” plan and the UCM630x device will permanently stay on the Basic plan until the user decides to upgrade it.

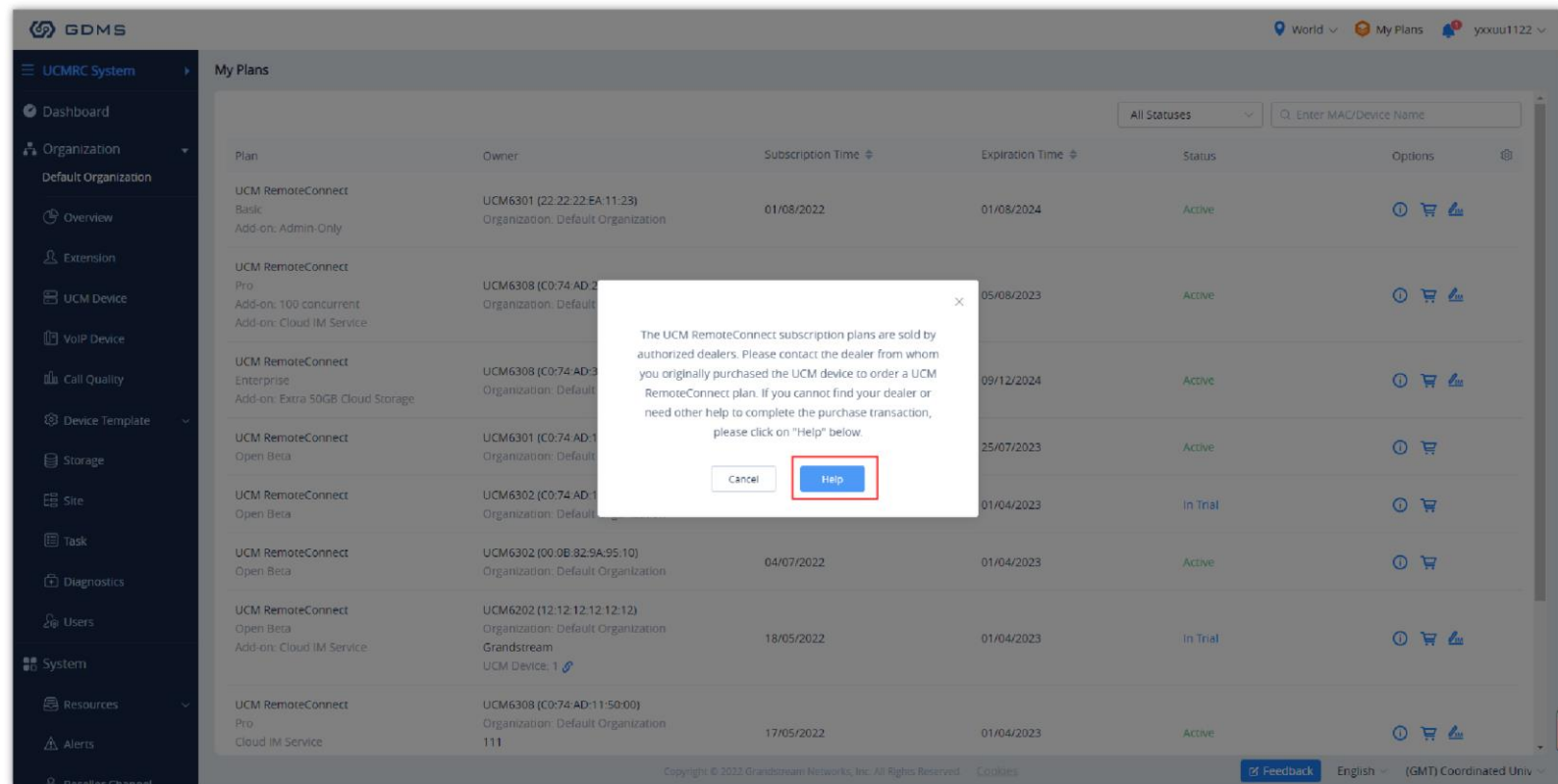
On the UCM Device -> Plan -> Expand the drop-down menu, users can view the information of “Device Original Plan” displayed on the interface. Please see the screenshot below:

2. After the paid plan expires, the user can go to the “My Plans” menu and move the cursor to the corresponding tip, the user will see the notification “After the previous plan expires, your UCM device can always use the Basic plan for free.”

We also updated the option “Order History” on the right upper corner to “My Plans”.



3. If the user cannot contact the dealer in the process of purchasing the plan, the user can click the “Help” button and fill in the relevant information. Then, we will send an email to the authorized distributor and the authorized distributor will contact the user as soon as possible.



4. Then, a form will appear for the user to fill in the necessary information.

Please fill in the UCM RemoteConnect plan you prefer to purchase and the contact information.

* Device MAC Address

* UCM RemoteConnect Plan [View plans](#)

* Company Name

* Your Name

* Phone Number

* Email Address

* Job Title

* Describe the problem

Submit



- When the plan has expired, the user can only use the Basic plan as the current plan, some functions will be unavailable.
- When the plan has expired, the files exceeding the storage space will be deleted after 7 days. Please download the backup file in advance or renew the plan.
- When the plan has expired, the UCM custom address will be deleted after 7 days.
- If the user has purchased a UCMRC plan before or applied for a free trial before, the user cannot apply for another UCMRC plan free trial anymore. The duration of the free trial is 3 months. When the free trial expires and the user has never purchased any plan for the UCM device, the plan of the UCM device will be downgraded to the Basic plan.

Remote Access to UCM Web UI

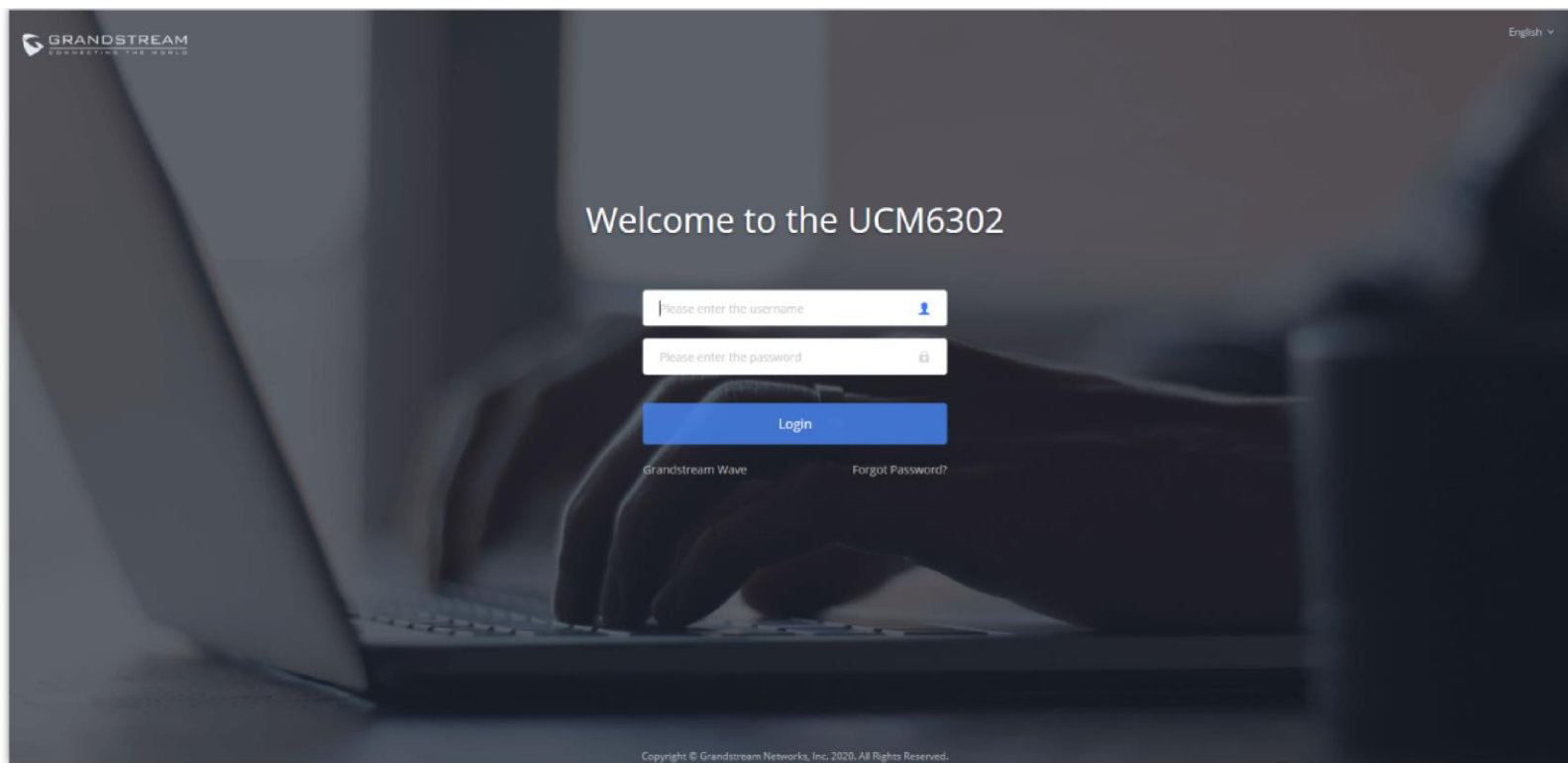
On the GDMS platform interface, even though the UCM is under the internal network, the user can remotely access the UCM Web UI through the external network for viewing data and configuration.

Prerequisite: UCM device firmware version must be later than 1.0.15.1.

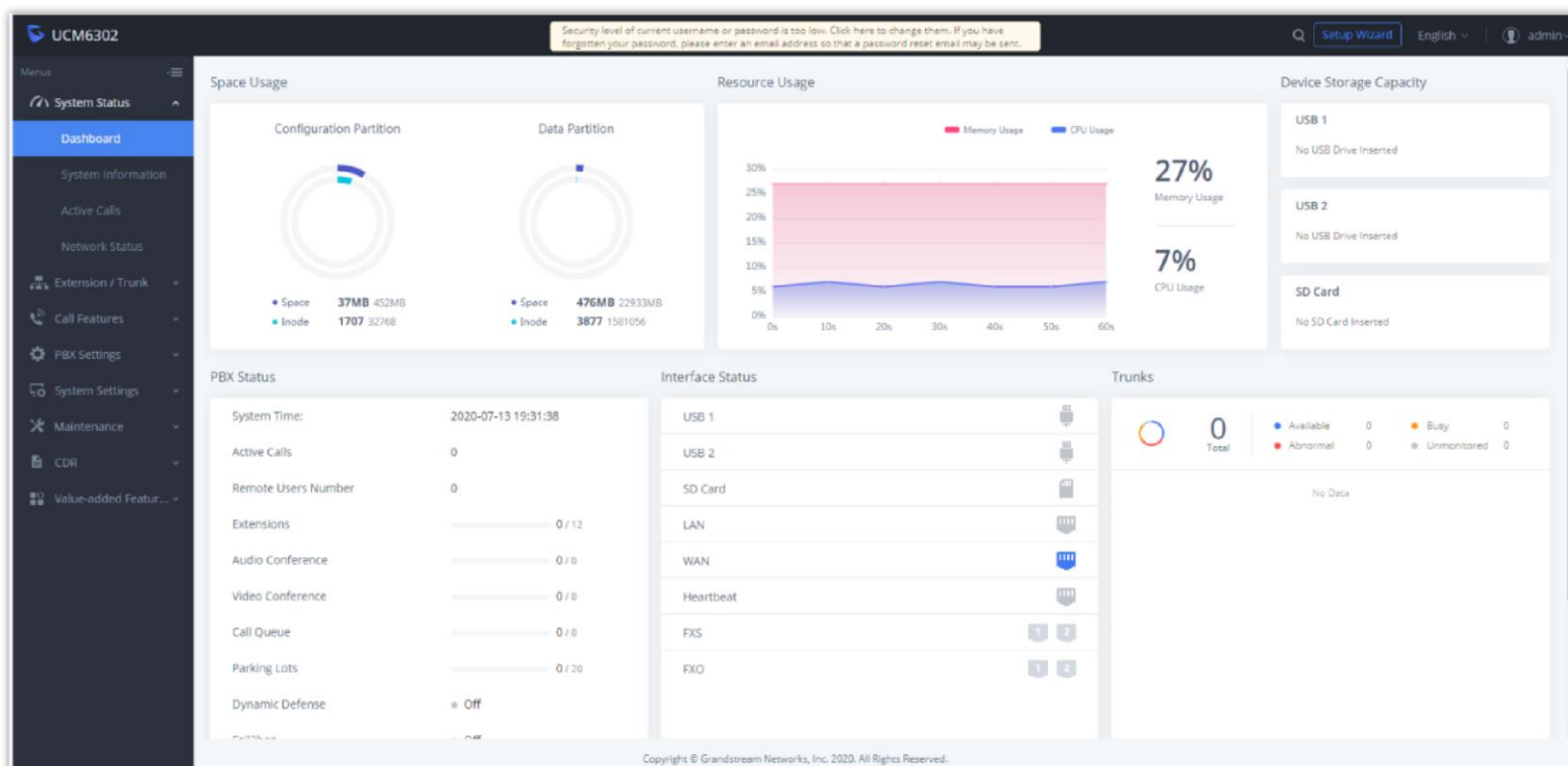
1. Go to **Device Management** → **UCM Device** interface, click on the button  of the specific UCM device, as the screenshot shows below:

UCM
List

2. Go to the UCM Web UI, and log in to the UCM device through the username and password, as the screenshot shows below:



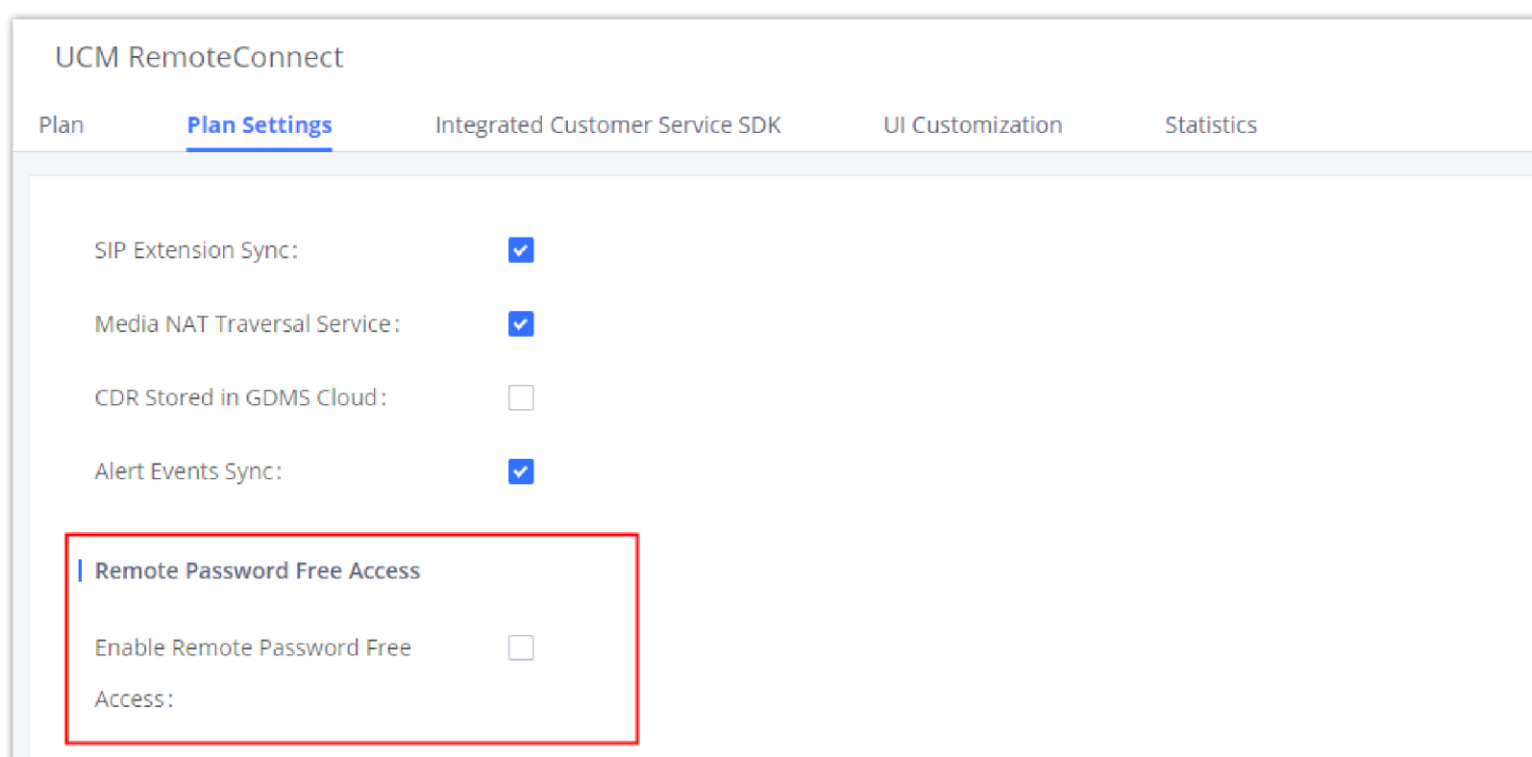
3. After logging in, the user can operate this UCM remotely by accessing the UCM device under the local network, as the screenshot shows below:




UCM Home Page

Notes:

- Users do not need to configure the external network for UCM devices and access the UCM devices with encryption through the GDMS platform. However, the network environment of the UCM devices is allowed access through external networks.
- Users can assign permission that remote access to UCM Web UI without entering a password. Once the permission is assigned, the user can remotely access the UCM Web UI through the GDMS platform without entering the UCM password.



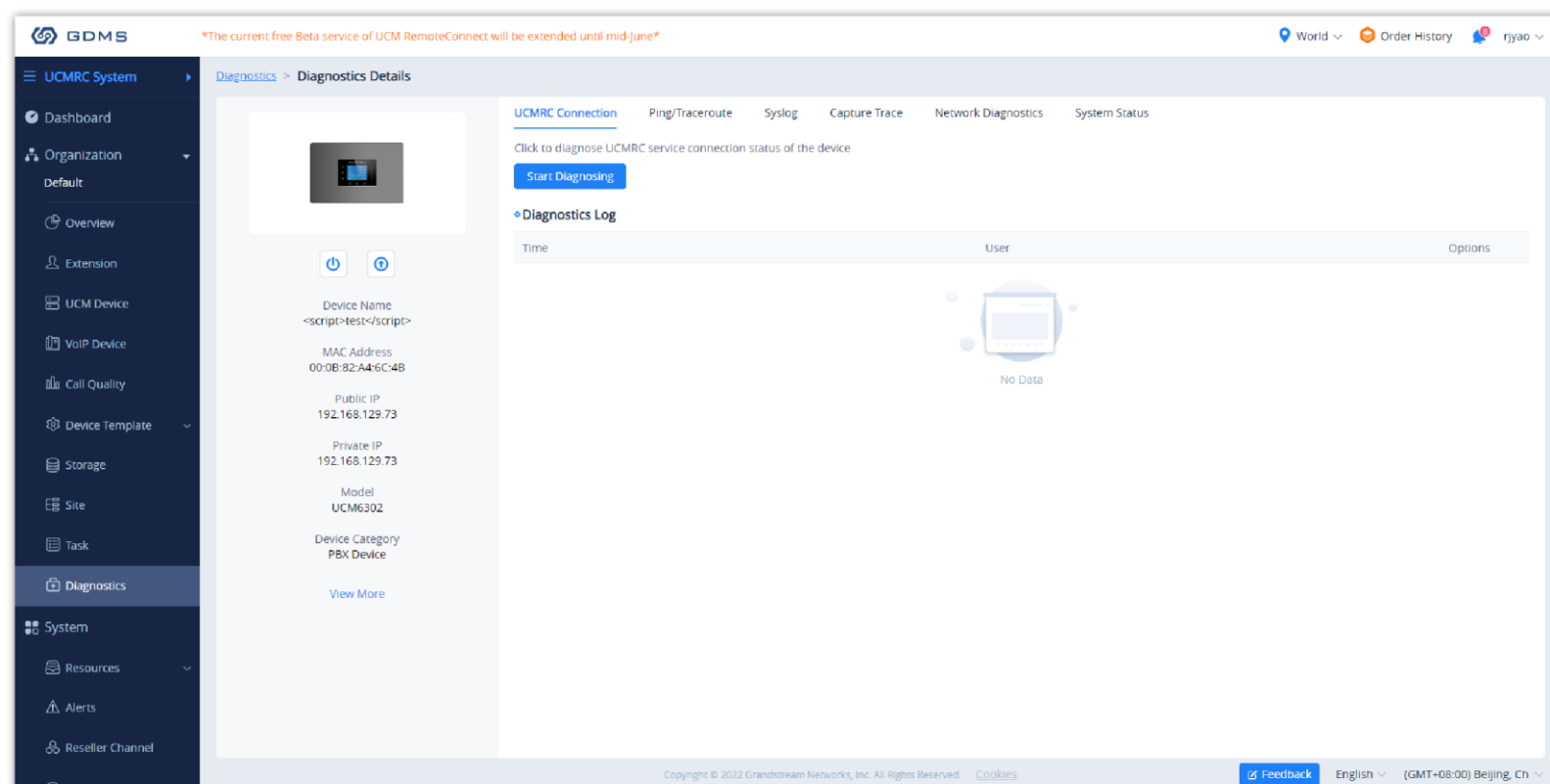
UCM Device Diagnosis

On the UCM Device list, users can click the Diagnosis button  following the UCM device to diagnose the UCM device, including UCMRC Connection, Ping/Traceroute, Syslog, Capture Trace, Network Diagnostics, and System Status.



UCM Device Diagnosis

If the UCM device which is using the UCMRC services has any problems, the user can diagnose the UCM device and troubleshoot the problems remotely. The user can try to fix the problems based on the suggestions and click on the “**Feedback**” button to send the logs and descriptions to our technical support.



Diagnostic Details

View Statistics

Daily Report

Prerequisite: The UCM plan contains permission for this function.

The UCM device collects the data report of the day and sends it to the GDMS user or the configured email box.

Please refer to the screenshot below for the daily report email:

UCM Statistics Report
2022/05/29

UCM Device MAC	00:0B:82:A4:6C:4B	
Device Time Zone	Etc/GMT-8	
Software Version	0.1.15.11	
Run Time	12days 14:6:27	
Device Storage	718.04MB/23.11GB	
Cloud Storage	0B/59.99GB	
Total Calls	0	
Remote Total	0	
Max Concurrent	0	
Number of Calls by Type	Audio Call	0
	Access Control Call	0
	Multimedia Meetings	0
	Surveillance Camera Call	0
	Video Call	0
Max Allowed UCMRC Registrations	—	
Max Allowed Local Registrations	GXP2160	1
	GXP2200	1
	GXV3240	1
	Wave Web	1

UCM Statistics Report

Statistics Time	The time of sending the data is displayed according to the local time zone of the UCM device.
Device	The MAC address of the UCM device is counted.
Time Zone	The local time zone of the UCM device.
Firmware Version	The current firmware version number.
Running Time	The running time displays the deadline for reporting the data.
Storage Space	By the reporting data time, it displays the usage of the local storage space of the device. If the usage reaches 80%, the indicator will be marked in red.
Cloud Storage Space	By the reporting data time, it displays the cloud storage space usage of the device. If the usage reaches 80%, the indicator will be marked in red.


Total Calls	The total number of calls on the reported day.
Total Remote Calls	The total number of calls made by the remote users on the reported day.
Max Remote Sessions	The maximum number of concurrent remote calls on the reported day.
Call Type Statistics	The distribution of all call types on the reported day.
Max Allowed UCMRC Registrations	The maximum number of remote registered extensions on the reported day.
Max Local UCMRC Registrations	The maximum number of local registered extensions on the reported day.
Max Time Per Remote Call/Meeting	The maximum call duration of the single remote call on the reported day. If the maximum call duration of the single remote call reaches 90% of the plan limitation, the value will be marked in red.
Aggregate Time for Remote Calls/Meetings	The total remote call duration on the reported day. If the total remote call duration reaches 90% of the plan limitation, the value will be marked in red.

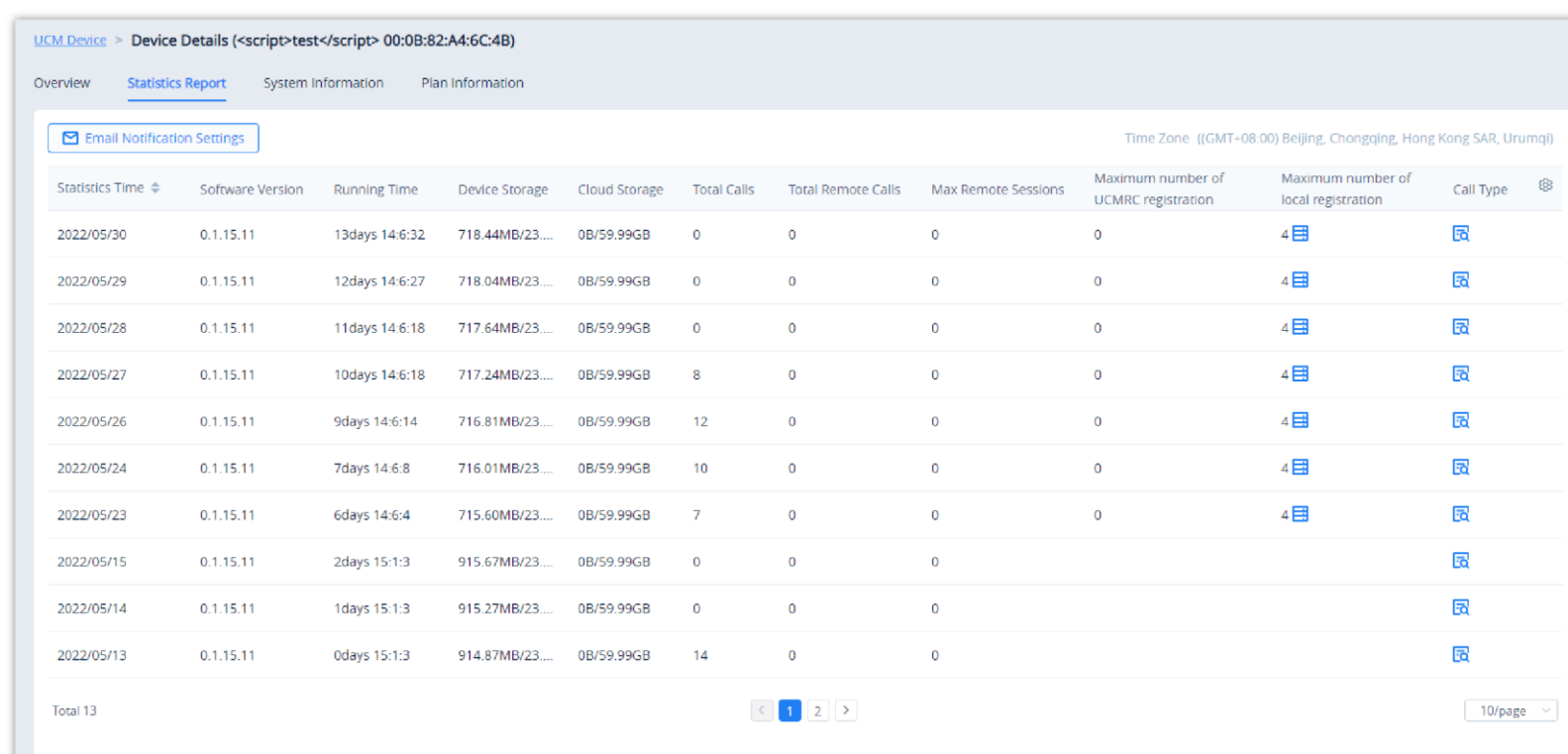


- Some data are only available for data statistics in the premium plan.
- The daily report sending time is according to the 0 a.m. of the UCM local time zone.

View Statistics Report (Last 30 days)


Prerequisite: The UCM plan contains permission for this function.

1. Go to the **Device Management** → **UCM Device** interface, click on the button  of the specific UCM device, and select the “**Statistics Report**” menu.
2. Users can only view the statistics report for the last 30 days. The reports will be sorted by the local time zone of the UCM devices, as the screenshot shows below:




Statistics Time	Software Version	Running Time	Device Storage	Cloud Storage	Total Calls	Total Remote Calls	Max Remote Sessions	Maximum number of UCMRC registration	Maximum number of local registration	Call Type
2022/05/30	0.1.15.11	13days 14:6:32	718.44MB/23....	0B/59.99GB	0	0	0	0	4	☒
2022/05/29	0.1.15.11	12days 14:6:27	718.04MB/23....	0B/59.99GB	0	0	0	0	4	☒
2022/05/28	0.1.15.11	11days 14:6:18	717.64MB/23....	0B/59.99GB	0	0	0	0	4	☒
2022/05/27	0.1.15.11	10days 14:6:18	717.24MB/23....	0B/59.99GB	8	0	0	0	4	☒
2022/05/26	0.1.15.11	9days 14:6:14	716.81MB/23....	0B/59.99GB	12	0	0	0	4	☒
2022/05/24	0.1.15.11	7days 14:6:8	716.01MB/23....	0B/59.99GB	10	0	0	0	4	☒
2022/05/23	0.1.15.11	6days 14:6:4	715.60MB/23....	0B/59.99GB	7	0	0	0	4	☒
2022/05/15	0.1.15.11	2days 15:1:3	915.67MB/23....	0B/59.99GB	0	0	0			☒
2022/05/14	0.1.15.11	1days 15:1:3	915.27MB/23....	0B/59.99GB	0	0	0			☒
2022/05/13	0.1.15.11	0days 15:1:3	914.87MB/23....	0B/59.99GB	14	0	0			☒

View UCM Device Statistics Report

3. Click on the button  to view the type and amount of the connected device on the current day to the UCM device:

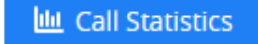
Number and device of bound extension account	
1.GXV3240	1
2.GXV3370	1
3.Wave/webrtc_chrome	1
4.Wave/webrtc_firefox	1

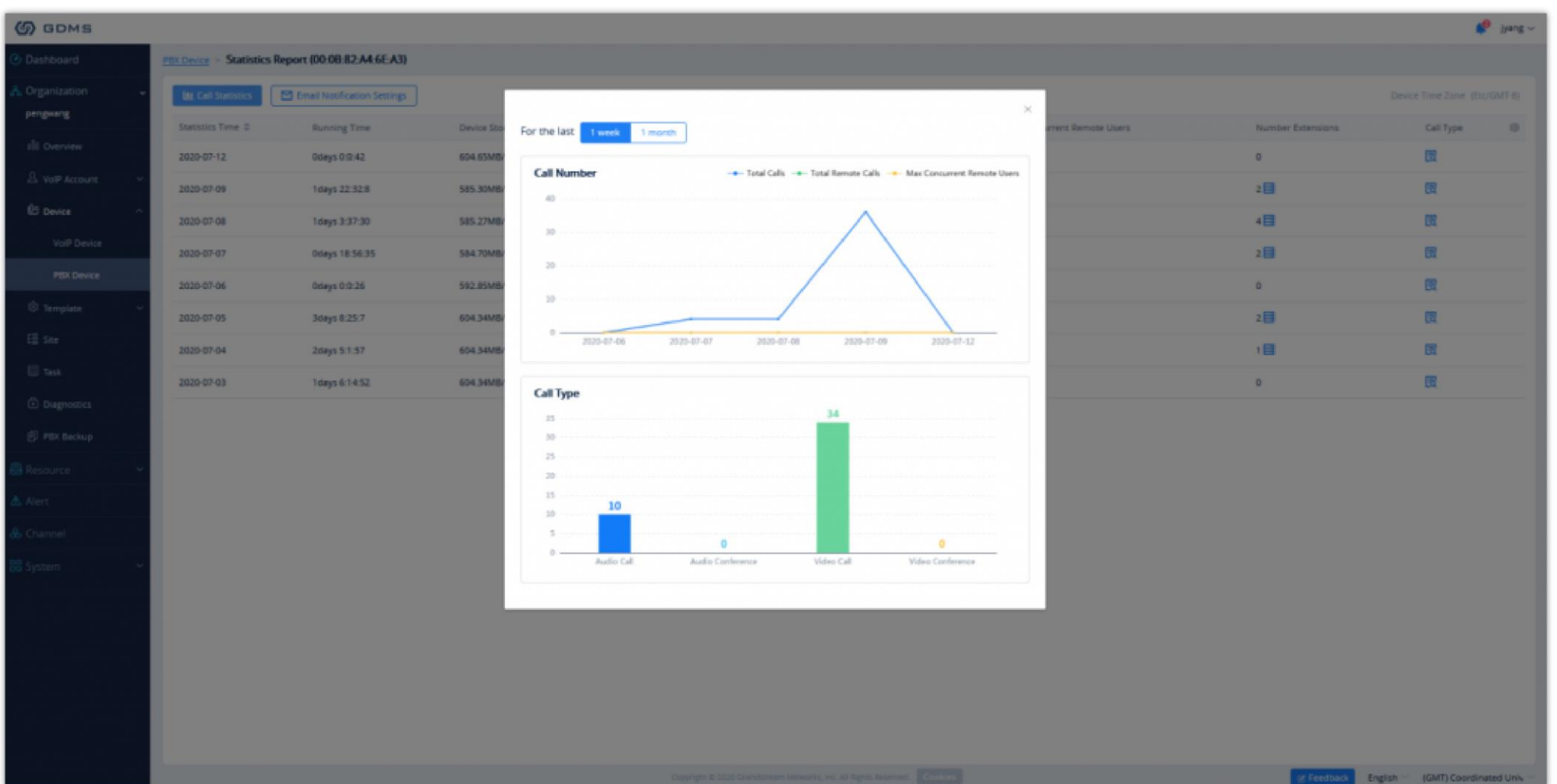
View Connected Devices Type/Amount

4. Click on button  to view the call type statistics of the current day:

Number of calls by type	
1.Audio Call	10
2.Audio Conference	0
3.Video Call	26
4.Video Conference	0

View Call Type Statistics

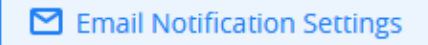
5. Click on button  to view chart statistics of the number/type of calls in the last 7 days or last 30 days, as the screenshot shows below:



View Call Statistics Chart

Set Daily Report Receiving Mailbox

Prerequisite: The UCM plan contains permission for this function.

GDMS platform will send a daily report email of the UCM device every day. Click on the button  on the UCM Device → **Statistics Report** interface to configure the email-receiving mailbox, as the screenshot shows below:

Email Notification Settings ✕

Daily Email Notification

Time Zone

* Send Time

Repeating Daily

Every

Per month

Per month

* Receiving Email Address

[+ Add Email Address](#)

Set Daily Report Receiving Mailbox

Daily Email Notification	This is used to configure whether the user wants to send the daily report to the mailbox every day. If not, no mail notification will be sent, and users can view the statistics report on the GDMS platform.
Time Zone	This is used to set the time zone of the daily report.
Send Time	This is used to set the sending time of the daily report.
Repeating	This is used to set the repeating sending time of the statistical report. Once this configuration is set, the statistical report will be sent to the configured email box periodically.
Receiving Email Address	Supports entering any email address. Users can click “ Add Email Address ” to add multiple email addresses to receive the daily report.

Table 22: Set Daily Report Receiving Mailbox

View Operation Logs

Prerequisite: The UCM plan contains permission for this function.

Users can view all operation logs on the GDMS platform for the UCM devices.

1. On the UCM Device List, select the menu button following the specific device, and click on the “**Operation Log**” button.
2. Operation logs include Remote accessing UCM Web UI logs, restarting logs, and firmware upgrading logs.

Users could only view the device operation logs for the last 30 days.

PBX Device > Operation Logs (00:0B:82:DB:8E:17 00:0B:82:DB:8E:17)

All Levels All Operations Q Enter Username Filter

Username	Log Contents	Level	Operating Time
Grandstream	Cancel/Stop "Reboot Device" Immediate task: 11	Medium	2020/07/13 11:37
Grandstream	Add "Reboot Device" Immediate task: 11	High	2020/07/13 11:36
Grandstream	log.pbx_device_add	Medium	2020/07/10 19:50

Total 3 10/page


View UCM Device Operation Logs

Custom Remote Access Domain Name

Remote Access Domain Name is used to configure the Wave application so that Wave application can connect to the UCM server and make calls at any time, anywhere under any network environment.

Prerequisite: The UCM plan contains permission for this function.

You can also customize your domain to access Wave Web RTC page/ UCM portal.

1. Go to **Device Management** → UCM Device interface, click the Edit Device option for the specific UCM device, and access to the “**Device Edit**” menu.
2. If the user wants to configure this address on the soft terminals for remote calls, the user can click the button  and customize the remote domain address. Please see the screenshot below:

Edit Device

MAC Address 00:0B:82:A4:6C:4B

Device Name

* Site

Remarks

Access Server

Zone

Default Server Address 000b82a46c4b.a.gdms.cloud

[Switch to Custom Domain](#)

* Custom Server Address .a.gdms.cloud

Device Edit Menu

3. Click on the “**Personal URL**” field, and enter the preferred URL, such as {yourdomain}.zoneb.gdms.cloud

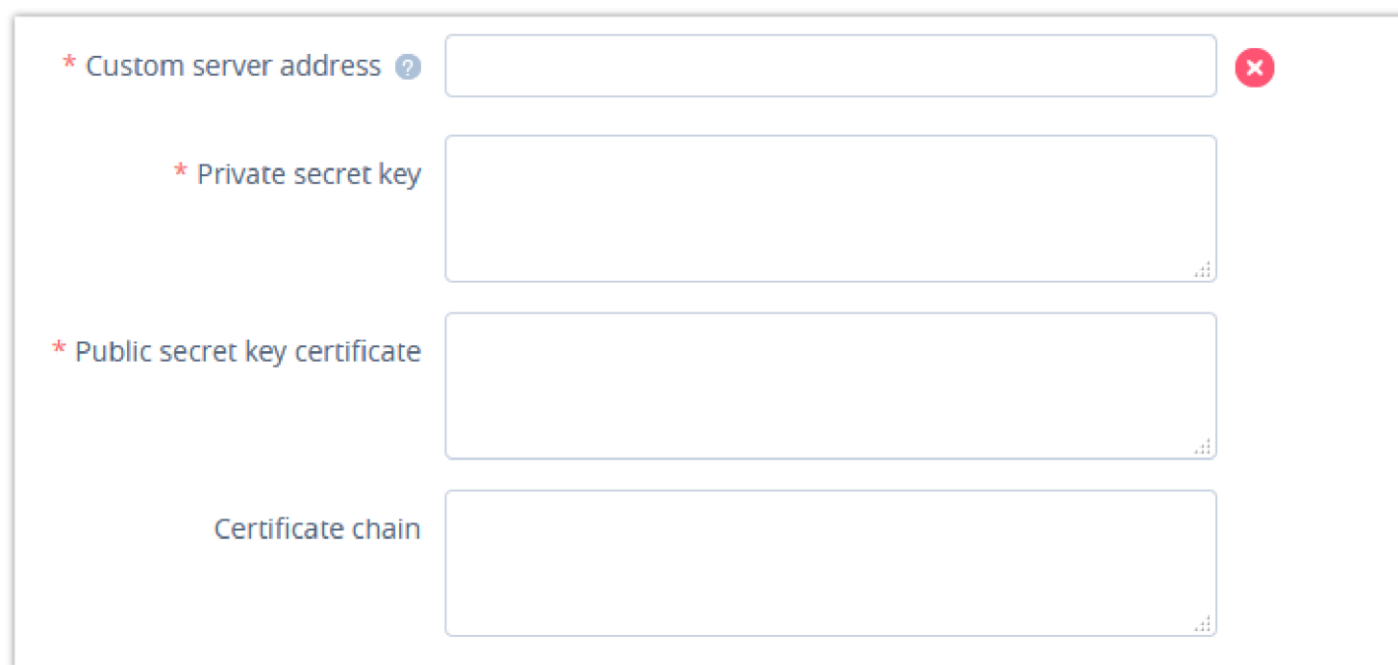
* Custom server address .zoneb.gdms.cloud

Custom UCM Remote Access Domain Name

4. If the plan has a custom domain name function, the user can click on the “**Custom Domain**” option and enter the server address with the private domain name, and the user also needs to enter the custom certificate of the domain name.

Note

The custom address needs to be resolved to the existing default server address (e.g. xxxxxxxx.zonea.gdms.cloud), otherwise the custom address cannot be recognized, and Wave users cannot connect to the UCM device through the custom address.



The screenshot shows a configuration form with four input fields. The first field is labeled '* Custom server address' and has a red 'x' button to its right. The second field is labeled '* Private secret key'. The third field is labeled '* Public secret key certificate'. The fourth field is labeled 'Certificate chain'. All fields are empty and have a small grid icon in the bottom right corner.

Enter Private Domain Name and Certificate

5. If the user needs to modify the information, the user can click on the button  to add a new custom server address.

6. Click on the “Save” button to apply the settings. Then, both the default server address and the new custom server address can be used.

Note If the user modifies the custom server address, the phones or Wave applications that use the previous custom server address need to be re-configured with the new custom server address. Otherwise, the service cannot be used normally.

Synchronize UCM Device Alert to GDMS

Only the advanced UCM Remote Control plans support synchronizing UCM device alerts to the GDMS platform. For UCM Remote Control plans details, please refer to our official website.

1. Users need to enable UCM alert notifications on the management platform of the UCM device. For details, please refer to the UCM User Guide on the UCM product page.
2. The alerts generated in the UCM device will be synchronized to the GDMS platform.
3. Users can view all UCM alert notifications in the GDMS platform, and set the alert notification methods: Email Notification, Message Notification, or SMS Notification.

Reboot Device

Users can reboot UCM devices from GDMS instantly or set up a schedule to reboot the UCM devices.

1. Select a UCM device from the **GDMS → Device → UCM Device** page, and click on “**Reboot Device**”. Or select multiple UCM devices by clicking **More → Reboot Device**.
2. The users can select to reboot the device immediately or set up a schedule to reboot the device. For a scheduled reboot, please select the start and end times of the task. Reboot will be performed during this period.

Upgrade Firmware ✕

* Firmware Version

Task Time Immediate Scheduled

* Task Name

* Run Time

Upgrade Firmware Configuration on GDMS

3. Save the configuration. Then the users can view the task status under the GDMS **Task** page.

i If the task is failed, the GDMS platform will send the system notification to the user.

Edit Device

Users could edit the UCM Device name and which site the device belongs to.

1. In the device list, click on the button to **Edit Device** to access the device editing page.

MAC Address	Device Model	Firmware Version	Plan	Server Address	Site Name	Options
<input type="checkbox"/> C0:74:AD:45:4E:44	UCM6301	—	Enterprise Pending Delivery	—	Default	
<input type="checkbox"/> 00:0B:82:A4:6E:B9 杨玉	UCM6302	1.0.15.5	Enterprise Pending Delivery	000b82a46eb9-11645.a.gdms.cloud.5061(L...	Def	
<input type="checkbox"/> C0:74:AD:0A:8E:9A '`'	UCM6308	1.0.11.9	Business Pending Delivery	000b82a46eb9-11645.a.gdms.cloud.5061(L...	CO:	
<input type="checkbox"/> C0:74:AD:29:6B:00	UCM6308	—	Enterprise Expired Pending Delivery	—	Def	
<input type="checkbox"/> C0:74:AD:2A:4B:3A	UCM6304	—	Business Pending Delivery	—	Def	
<input type="checkbox"/> 00:0B:82:A4:6C:4B <script>test</script>	UCM6302	0.0.15.8	Enterprise	testaaa.a.gdms.cloud.5061(TLS) ...	000	
<input type="checkbox"/> 00:0B:82:A4:6E:BF 6ebfagadfgadl6ebfagadfgadl6ebfagadfgadl6...	UCM6302	0.0.4.16	Enterprise Pending Delivery	—	000B82A46EBF	

Edit UCM Device Option

2. Users will see the device editing page as the figure shows below:

Edit Device

MAC Address 00:0B:82:A4:6C:4B

Device Name <script>test</script>

* Site 00:0B:82:A4:6C:4B

Remarks

Access Server

Zone Los Angeles

Default Server Address 000b82a46c4b.a.gdms.cloud

[Switch to Custom Domain](#)

* Custom Server Address testaaa.a.gdms.cloud

Cancel Save

Edit Device

3. Users can modify the GDMS server region by clicking on the drop-down menu of the “**Zone**” option. When the device is online for the first time, the GDMS platform system will set the region based on the nearest region to the device automatically.
4. If the plan has the custom server address function, the user can click “**Personal URL**”; If the plan has permission to custom private domain name function, the user can click on the “**Custom Domain**” option to configure it.
5. Click on the “**Save**” button to apply the changes on the GDMS platform.

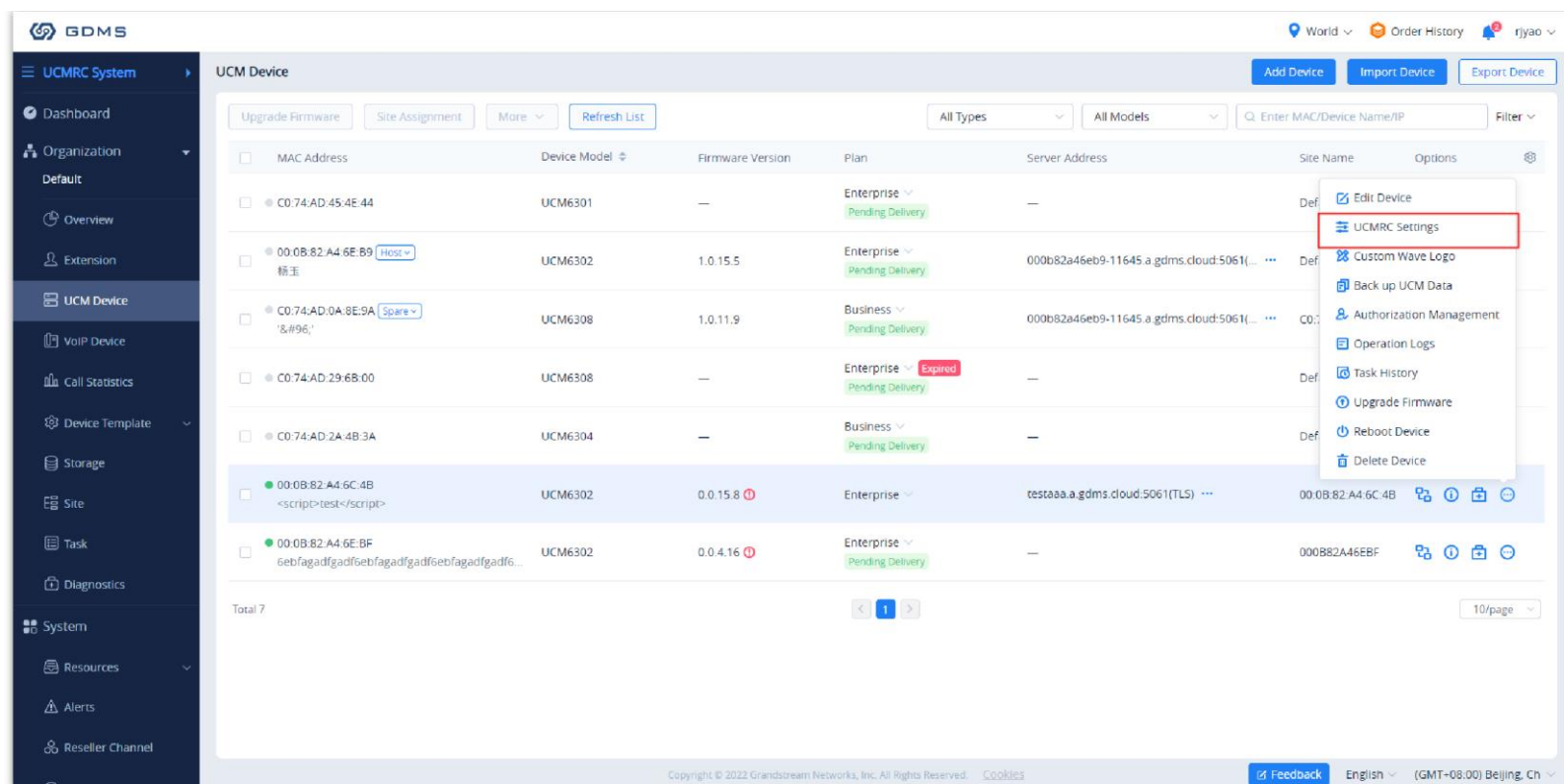
! After modifying the GDMS server region, the GDMS platform system will generate a new Access Server address, and the Wave users and the phones which are not connected to the GDMS platform need to be configured with the new Access Server address manually. If the user is using the Custom Domain, the user does not need to update the address.

UCMRC Settings

Prerequisite: The user has the corresponding UCMRC plan including this function.

The user can remotely access the PBX device to set the plan of the UCMRC service.

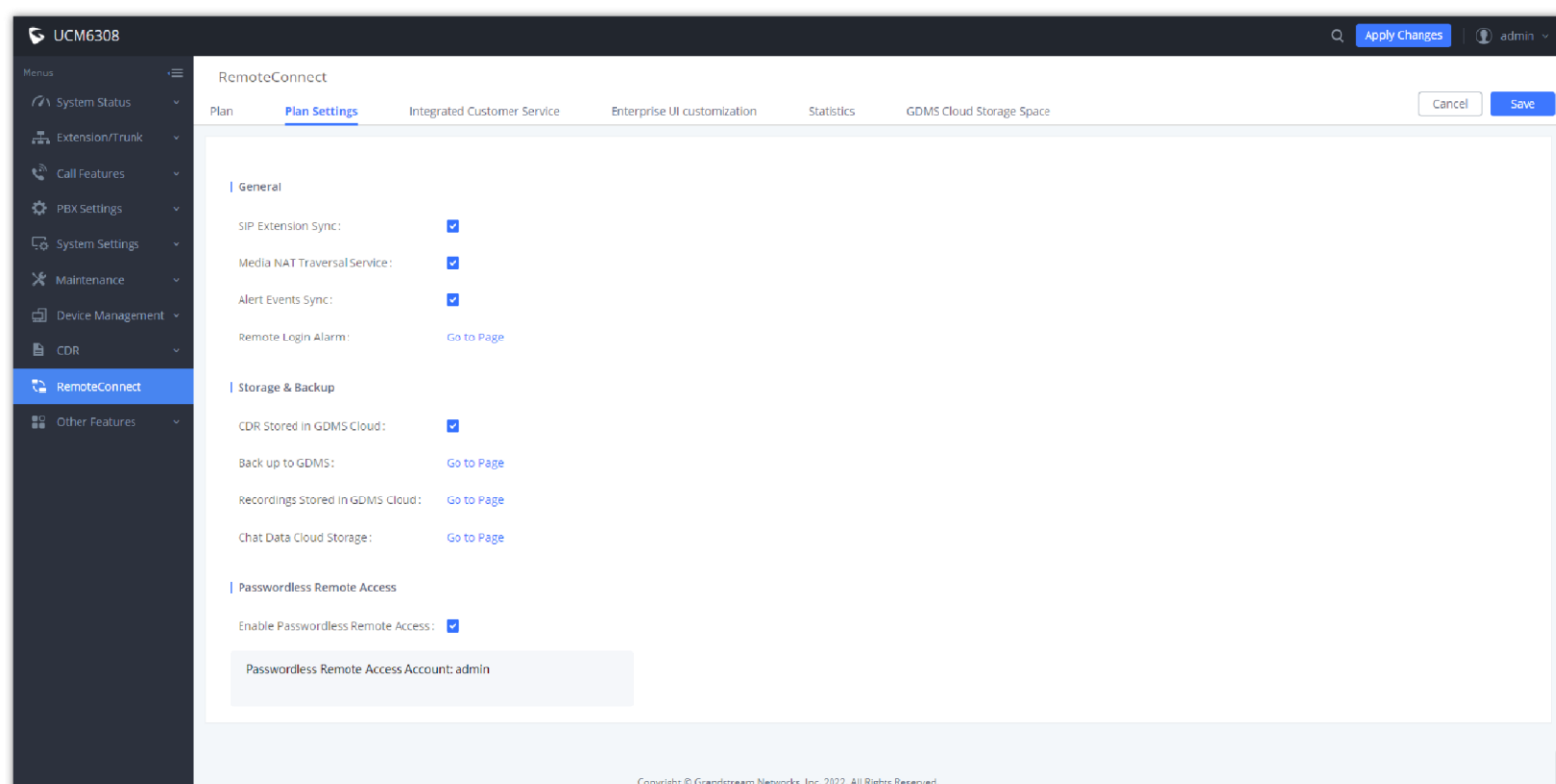
1. In the UCM Device list, the user can select the UCM device which the user prefers to access and click button to set the UCM device.



UCMRC Settings Interface

2. After clicking the UCMRC Settings button, the user will be directed to the UCM Web UI remotely.

3. The user will be directed to the UCM Web UI → UCM RemoteConnect → Plan Settings interface. As the screenshot shows below:



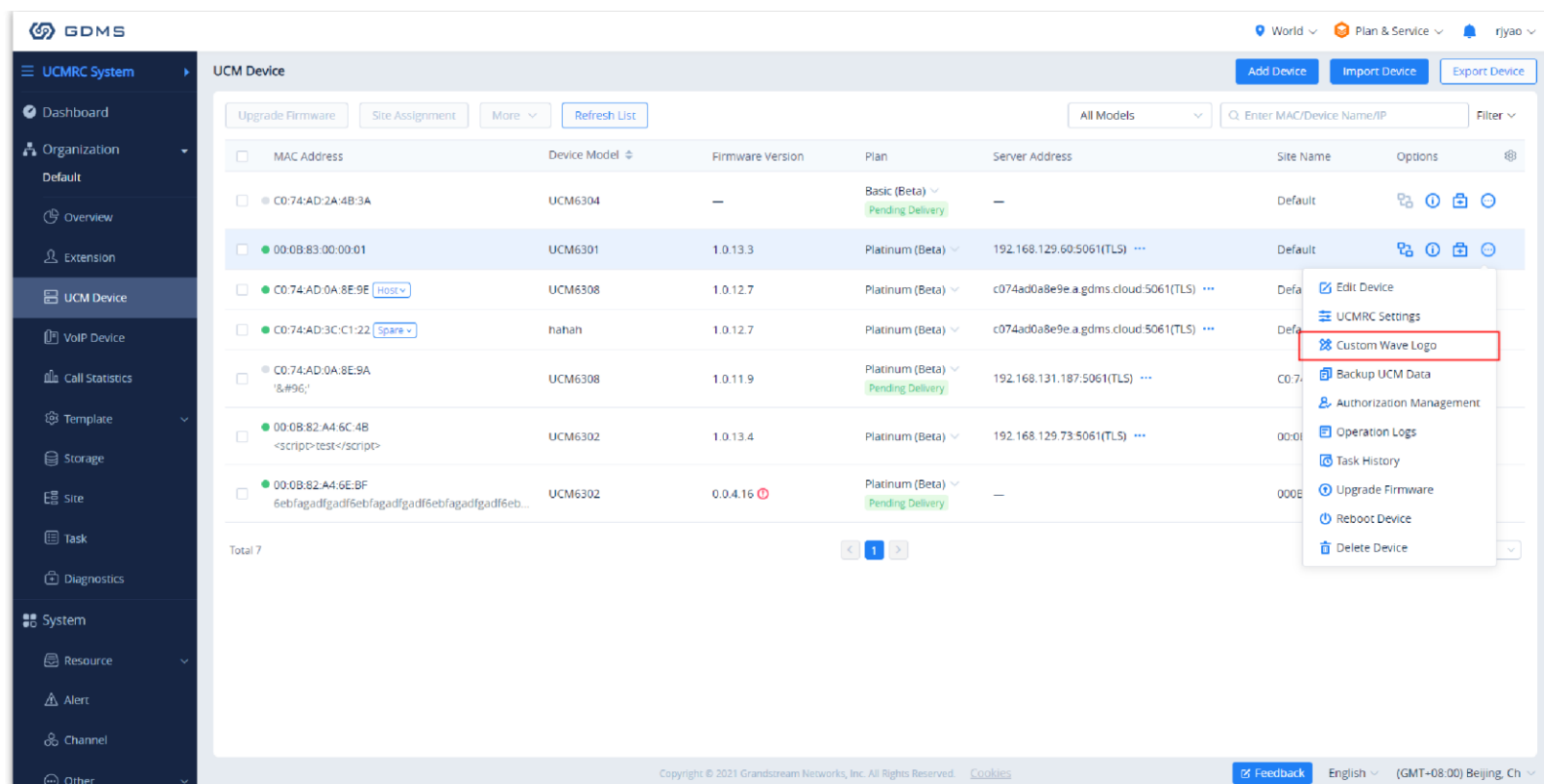
Plan Settings for UCMRC

Custom Enterprise Logo

Prerequisite: The user has the corresponding UCMRC plan including this function.

The user can remotely access the UCM device Web UI to customize the enterprise logo.

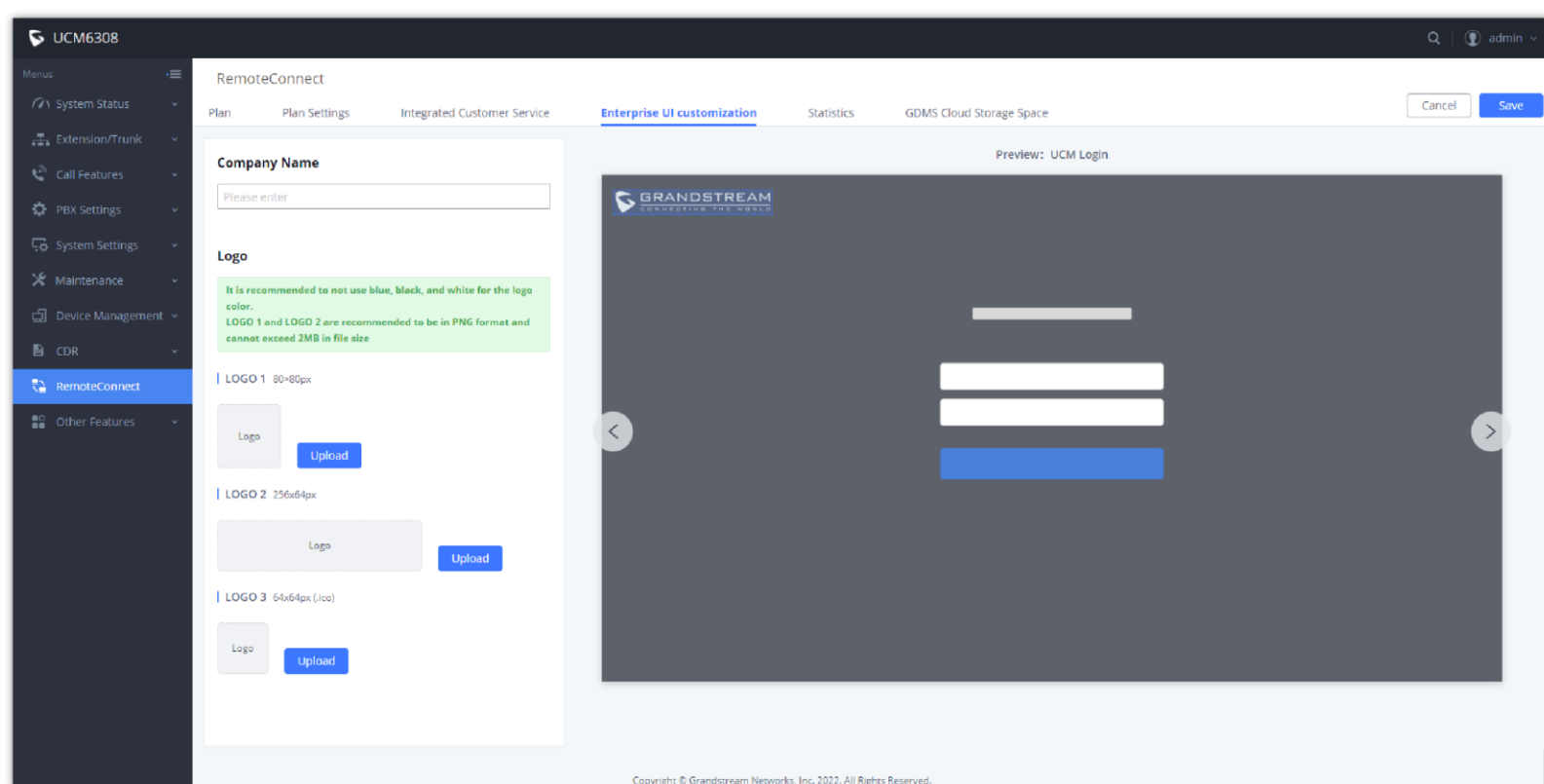
1. In the UCM Device list, the user can select the UCM device which the user prefers to customize the logo and click  button to access the UCM Web UI.



Custom Enterprise Logo Interface

2. After clicking the custom logo button, the user will be directed to the UCM device Web UI.

3. The user will be directed to the UCM Web UI → UCM RemoteConnect → Custom Logo to customize the enterprise logo. As the screenshot shows below:



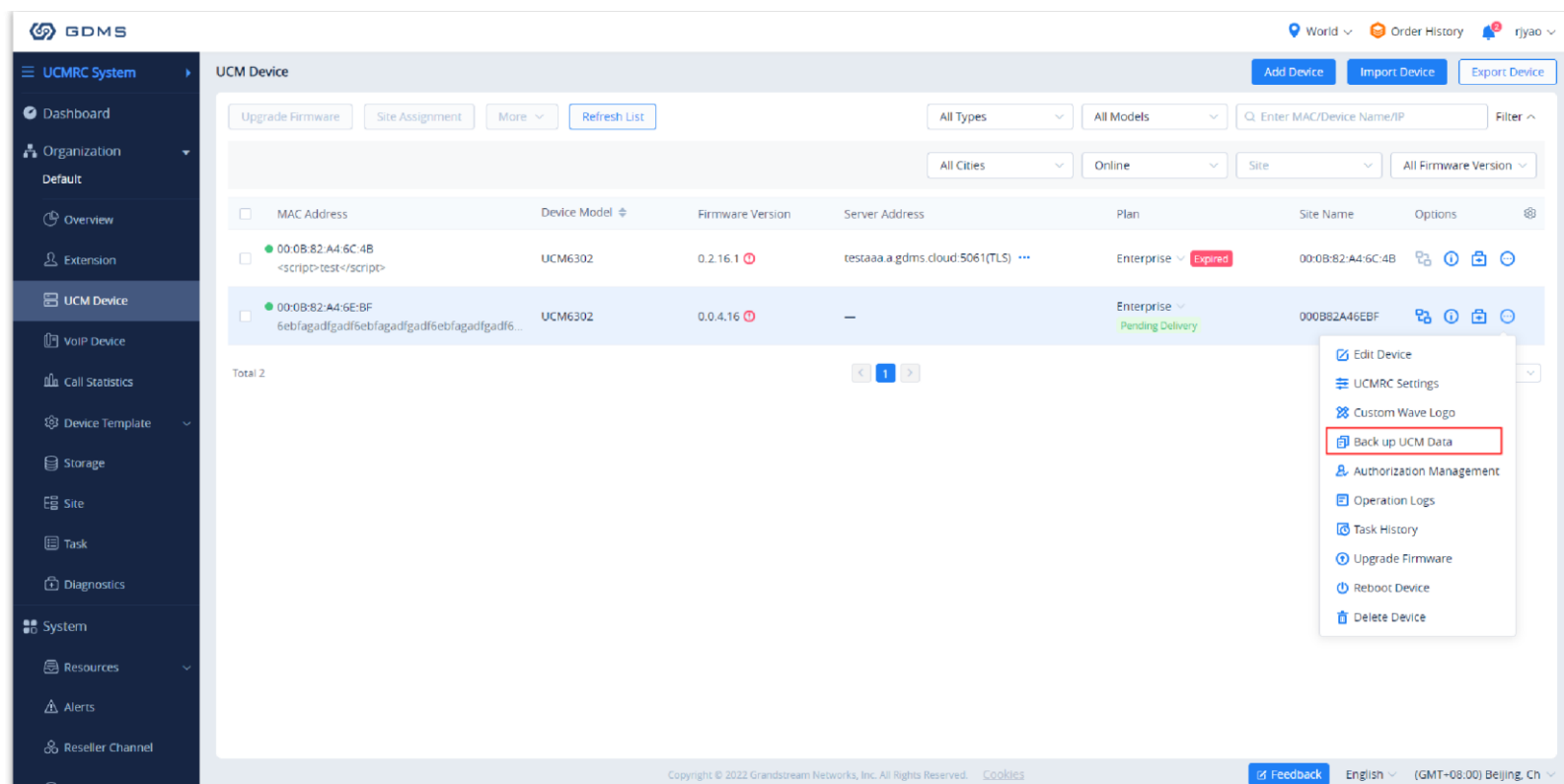
Custom Logo

Back up UCM Data

Prerequisite: The user has the corresponding UCMRC plan including this function.

The user can remotely access the UCM device to enable the UCM data backup function.

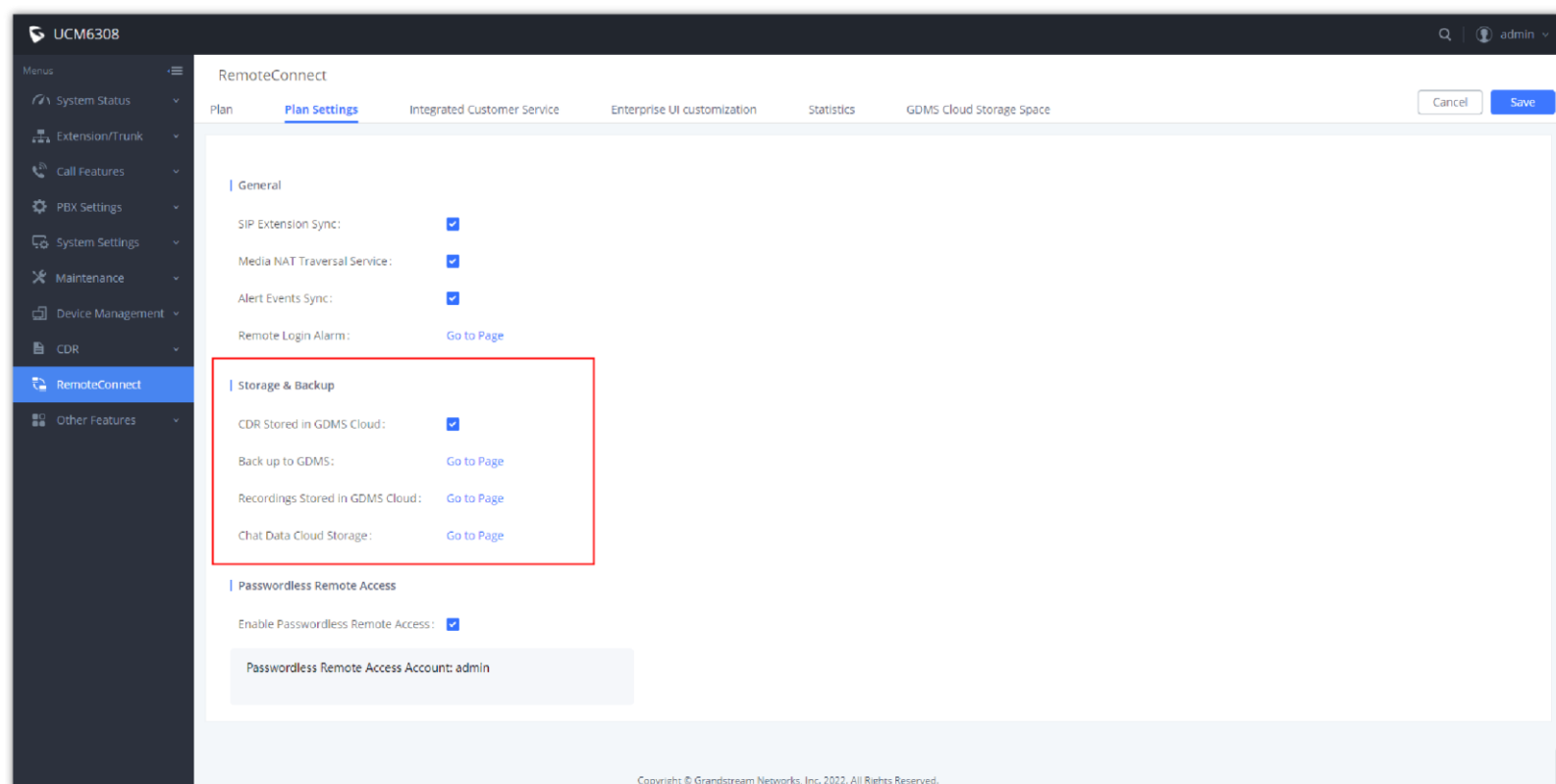
1. On the UCM Devices list, the user can select the UCM device, click the button  to access the UCM Web UI, and set the UCM data backup function for the GDMS platform account.



Back up UCM Data

2. After clicking the UCM data backup button, the user will be directed to the UCM device Web UI.

3. The user will be directed to the UCM Web UI UCM RemoteConnect à Plan SettingsàStorage & Backup interface and set to back up the UCM data to the GDMS platform account. Please see the screenshot below:

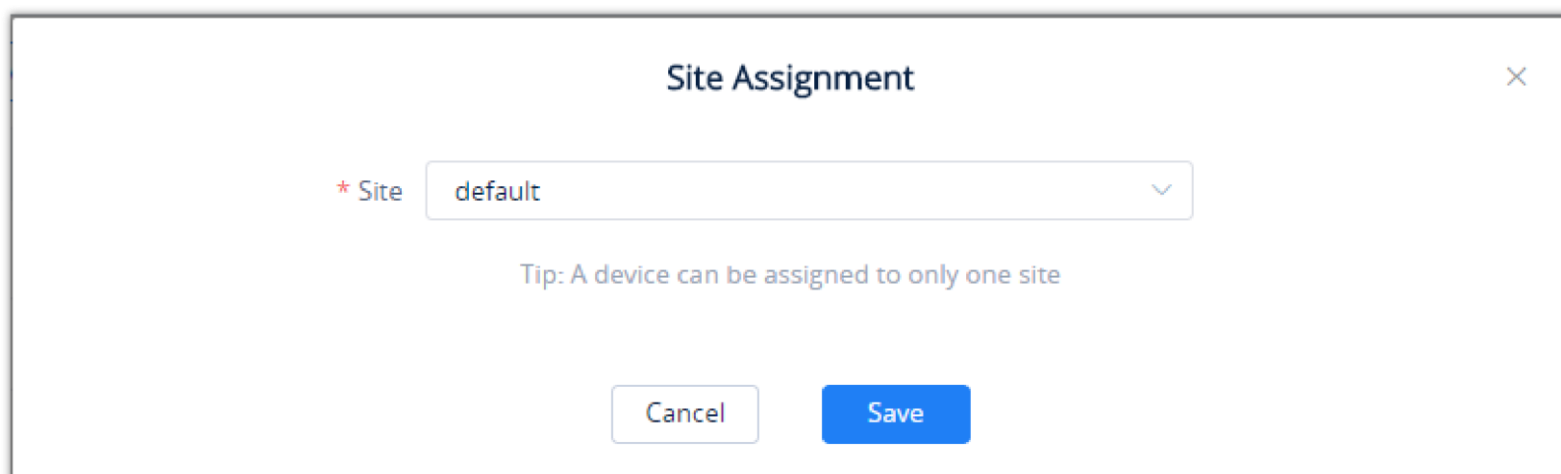


Storage & Backup

Batch Modify Sites

Users could edit the site of a batch of UCM devices on the GDMS platform. The default site is “**default**”.

1. Select the desired devices and click on the “**Site Assignment**” button.



Site Assignment

2. Select the site to assign the selected devices.

3. Click on the” **Save**“ button, and all selected devices will be transferred to the selected site.

i Each device can only be allocated to one single site.

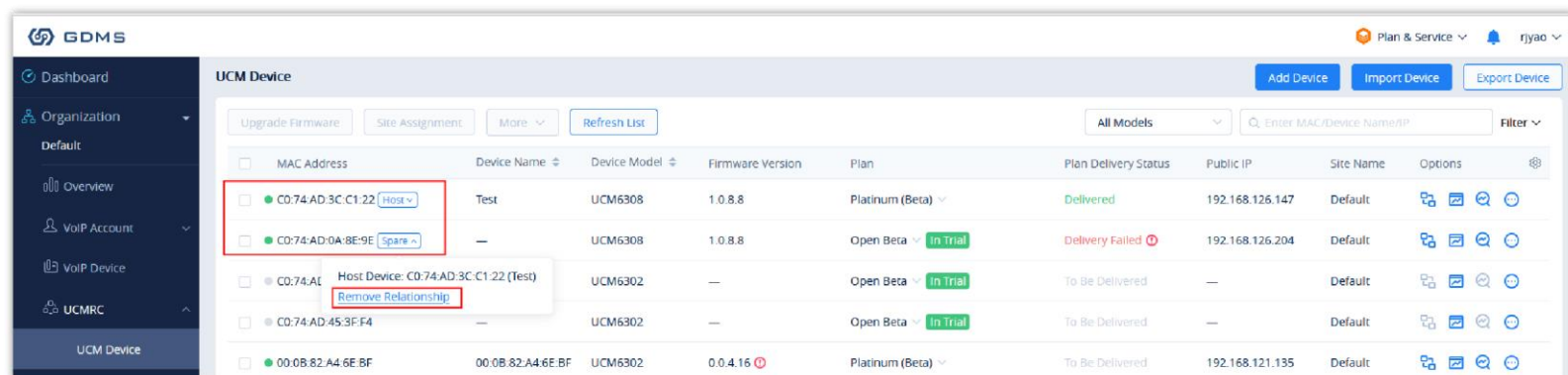
View/Disassociate Host/Spare UCM Device

Prerequisite: The user has the corresponding UCMRC plan including this function.

Users can view Host/Spare UCM devices in the UCM devices list, the Host/Spare icon will be marked following the MAC address, and users can view the corresponding MAC address of the Host/Spare devices.

When the Host/Spare association is established, and once the Host UCM server is down, the Spare UCM device can still get connected through the Host UCM device’s UCMRC domain name.

The user can click “Remove Relationship” to remove the UCMRC Host/Spare relationship. However, the local Host/Spare relationship configuration in the UCM devices is still retained. If the user also wants to remove this relationship, the user needs to go to the UCM management platform to disassociate the relationship.



The screenshot shows the GDMS UCM Device management interface. A table lists several UCM devices with columns for MAC Address, Device Name, Device Model, Firmware Version, Plan, Plan Delivery Status, Public IP, and Site Name. Two devices are highlighted with a red box: one with MAC address C0:74:AD:3C:C1:22 (Host) and another with MAC address C0:74:AD:0A:8E:9E (Spare). A tooltip for the Host device shows a 'Remove Relationship' button.

MAC Address	Device Name	Device Model	Firmware Version	Plan	Plan Delivery Status	Public IP	Site Name	Options
C0:74:AD:3C:C1:22 (Host)	Test	UCM6308	1.0.8.8	Platinum (Beta)	Delivered	192.168.126.147	Default	[Icons]
C0:74:AD:0A:8E:9E (Spare)	—	UCM6308	1.0.8.8	Open Beta - In Trial	Delivery Failed	192.168.126.204	Default	[Icons]
C0:74:AD:45:3F:F4	—	UCM6302	—	Open Beta - In Trial	To Be Delivered	—	Default	[Icons]
00:08:82:A4:6E:BF	00:08:82:A4:6E:BF	UCM6302	0.0.4.16	Platinum (Beta)	To Be Delivered	192.168.121.135	Default	[Icons]

View Host/Spare UCM Device

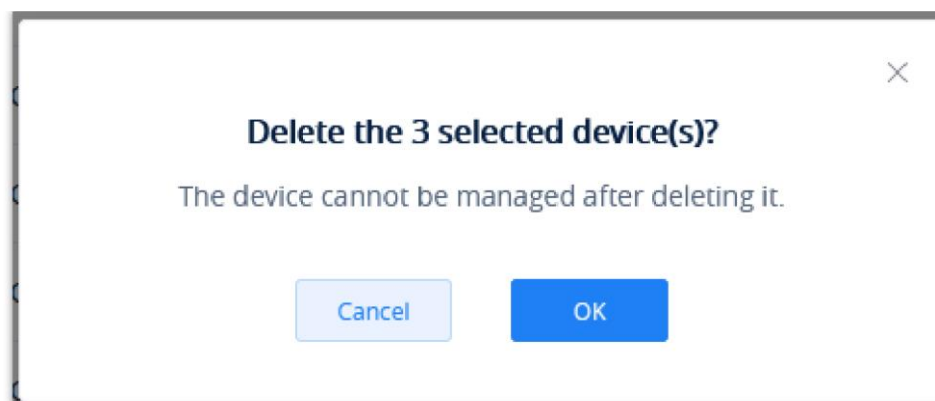
i Note

- If the user only purchases one UCMRC plan which contains the HA service for one of the UCM devices, the HA features for the UCM devices cannot be used normally.
- To ensure that the UCM devices can be used normally under the HA mode, the user needs to purchase two UCMRC plans with the same specifications and both plans contain the HA service.

Delete Device

Users could delete one UCM device or a batch of UCM devices on the GDMS platform.

1. Select the desired devices and click on **More → Delete**.
2. Select a UCM device from **GDMS → Device → UCM Device** and click on “**Delete Device**”. Users can also select multiple UCM devices and then click on **More → Delete** to perform a batch delete for all selected UCMs.
3. Click on the” **OK**“ button on the pop-up window to confirm deleting the devices, and the selected devices will be deleted immediately from the GDMS platform. The timing tasks involving the deleted devices will be canceled either.



Delete Device Prompt

Export Device

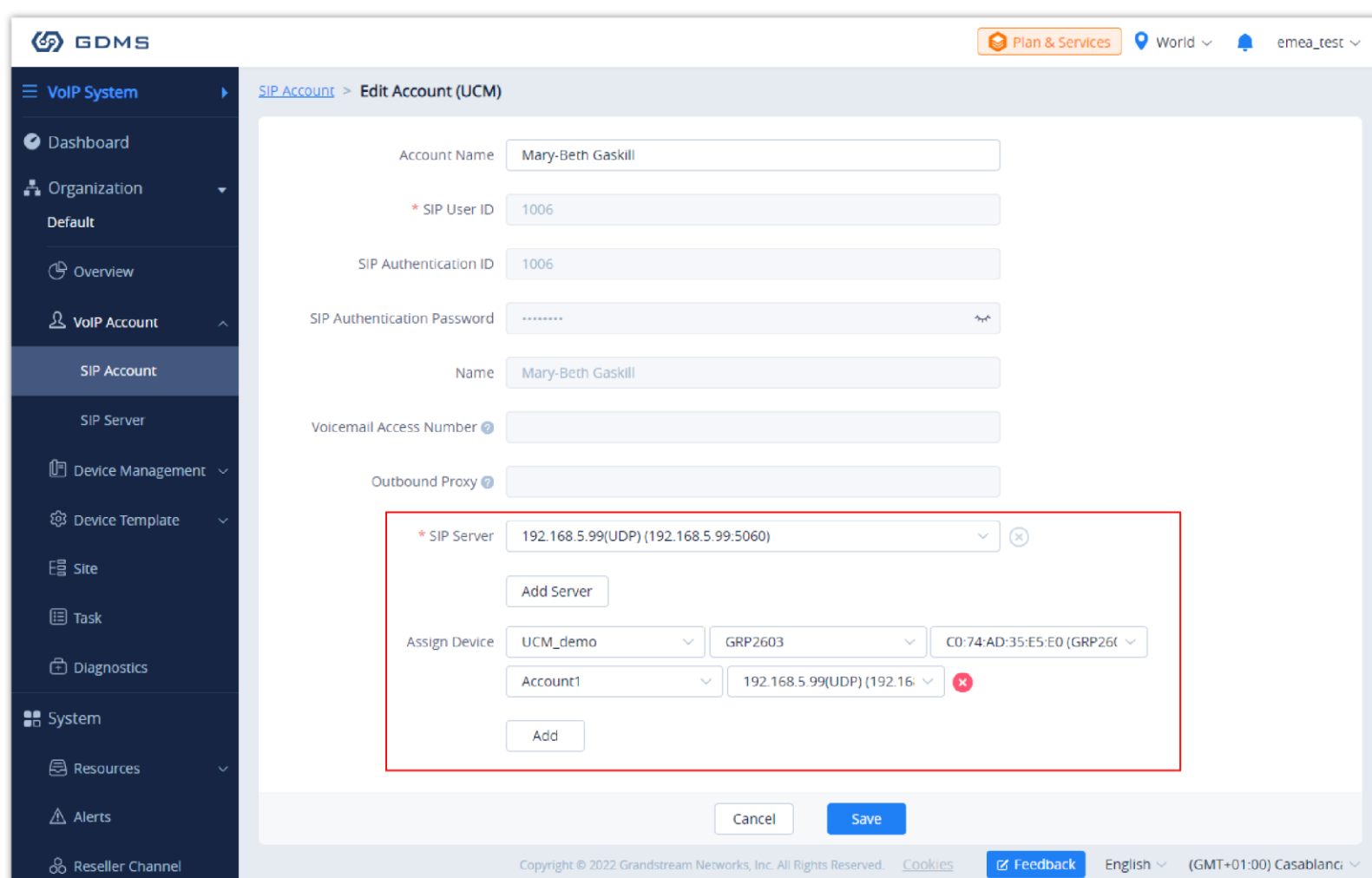
To export the entire device list, click on the  button in the top-right corner of the device list page. The exported list includes all device information.

Configure Parameter For Device

GDMS platform administrator can configure the parameters of UCM RemoteConnect for the device remotely. Once the device has been configured following the methods below, the device can use the UCM RemoteConnect functions.

Method 1:

1. GDMS platform administrator can go to **VoIP Account** → **SIP Account** interface, select the SIP accounts which will be assigned to the device, and click on the edit button  to access the account editing interface:

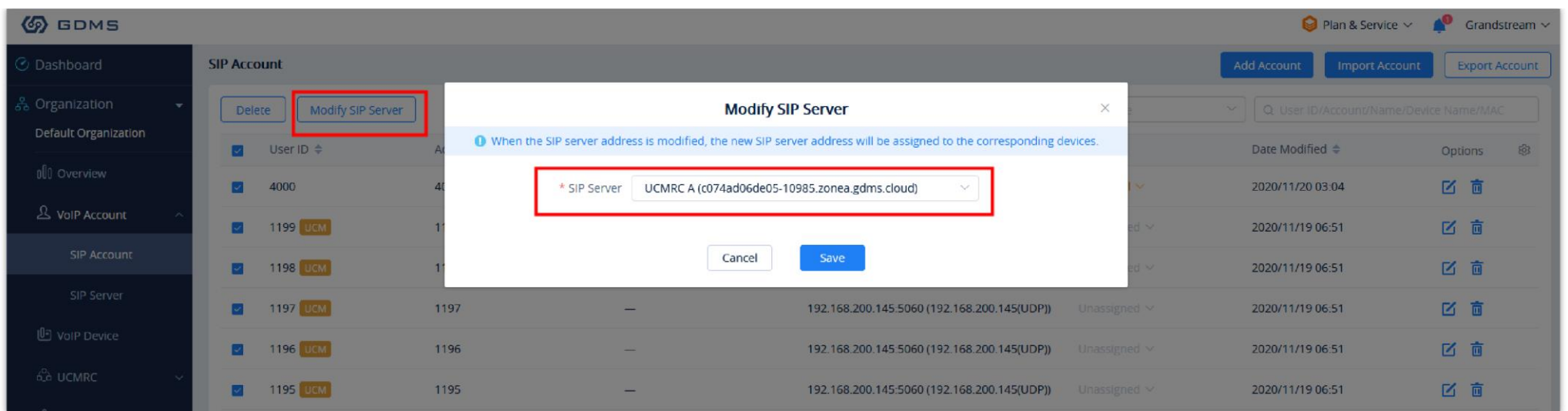


Edit Account

2. Click **Add Server** option and select the external network server address reported by the UCM RemoteConnect.
3. Assign the SIP server to the device and enter the device MAC address and Account index, then select the SIP server of the UCM RemoteConnect.
4. Click to save and apply the changes for UCM RemoteConnect for the device.

Method 2:

Users can select multiple SIP accounts, click the “Modify SIP Server” option on the top of the interface, and then select the server address of UCM RemoteConnect to modify the SIP server address (internal network) to the server address of UCM RemoteConnect for a batch of devices.



Modify SIP Server Address



When the user configures the server address of UCM RemoteConnect for the device, the following settings will be assigned to the device automatically to ensure the UCM RemoteConnect service can be used successfully:

- SIP Protocol – TLS
- STUN server setting will be changed to the TURN server address of UCM RemoteConnect.

When the UCM RemoteConnect account is deleted from the device, the STUN server setting will be removed automatically from the device.

Storage

View Backup File

For backup files generated from UCM manually or automatically, they can be stored in GDMS cloud storage. On the GDMS platform, users can view all backup files.

1. Go to the UCM Backup page, all backup files available for connected UCM devices will be displayed. The file type includes CDR files, config files, etc.



It only displays all the backup files of the UCM devices under the current organization. Users can switch the organization to view the backup files of the UCM devices under other organizations.

2. Click the searching box at the top of the interface to search the backup files by device MAC address, backup file type, and device model.

Storage (Used space 72.88MB | IM has used 12.59MB) Refresh List Convert Config File Upload File

Delete Download All Models All File Types

<input checked="" type="checkbox"/>	MAC Address	Device Name	File Type	File Name	File Size	File URL Address	Storage Time	Options
<input checked="" type="checkbox"/>	[REDACTED]	—	Conference Audio Rec...	meeting-6300-16698...	477.58KB	[REDACTED]	2022/11/30 10:23AM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	Conference Audio Rec...	meeting-6300-16697...	69.14KB	[REDACTED]	2022/11/29 03:28PM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	Conference Audio Rec...	meeting-6300-16697...	89.45KB	[REDACTED]	2022/11/29 12:30PM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	Conference Audio Rec...	meeting-6300-16697...	180.86KB	[REDACTED]	2022/11/29 12:07PM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	Conference Audio Rec...	meeting-6300-16697...	631.02KB	[REDACTED]	2022/11/29 11:22AM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	IM	GRP2634_frontv2_we...	69.79KB	[REDACTED]	2022/11/14 10:04AM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	IM	GRP2634_frontv2_we...	168.63KB	[REDACTED]	2022/11/14 10:04AM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	IM	20211113_210009_p...	89.74KB	[REDACTED]	2022/11/08 12:03PM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	IM	20211113_210009.jpg	1.19MB	[REDACTED]	2022/11/08 12:02PM	<a>Copy <a>Download <a>Share <a>Delete
<input type="checkbox"/>	[REDACTED]	—	IM	GCE-UC-Presentation...	7.62MB	[REDACTED]	2022/10/26 03:27PM	<a>Copy <a>Download <a>Share <a>Delete

Total 25 < 1 2 3 > 10/page

© 2023 Grandstream Networks, Inc. Cookies Feedback English (GMT) Casablanca, Mon

[View Backup File](#)




- If the storage space of the UCM device is insufficient, the backup file cannot be stored. Please clear the storage space or renew the plan to get more storage space.
- Users can subscribe to the email notifications so that the alert message will be sent to the configured email box by default when the device storage space is insufficient.

Upload Backup File

Users can upload the backup file and recover the backup file on UCM.

1. Go to the UCM Backup page, and click on the “Upload File” button in the right upper corner to access the interface:

Upload File ✕



Click or drag and drop file here to upload

Supported file type: tar, cenc, venc

* MAC Address

* File Name

File Type

Upload File

File	Click to select the backup file from the local PC or drag the backup file to this field to upload the backup file. The backup file can be the configuration file of the device.
MAC Address	Enter the MAC address of the UCM device for uploading this backup file. Note: The UCM device must be in the current organization, otherwise, the backup file cannot be uploaded.
File Name	Enter the name of the backup file.
File Type	Enter the file type of the backup file so that the UCM device can obtain the backup file accordingly by the file type.

2. Click the **OK** button to upload the backup file.

i If the UCM device does not have enough storage space, the backup file cannot be uploaded. The user can clean up the cloud storage space file for this UCM or purchase an additional plan.

Download Backup File

1. On the **”UCM Backup“** page, click the button  following the backup file to download the file.

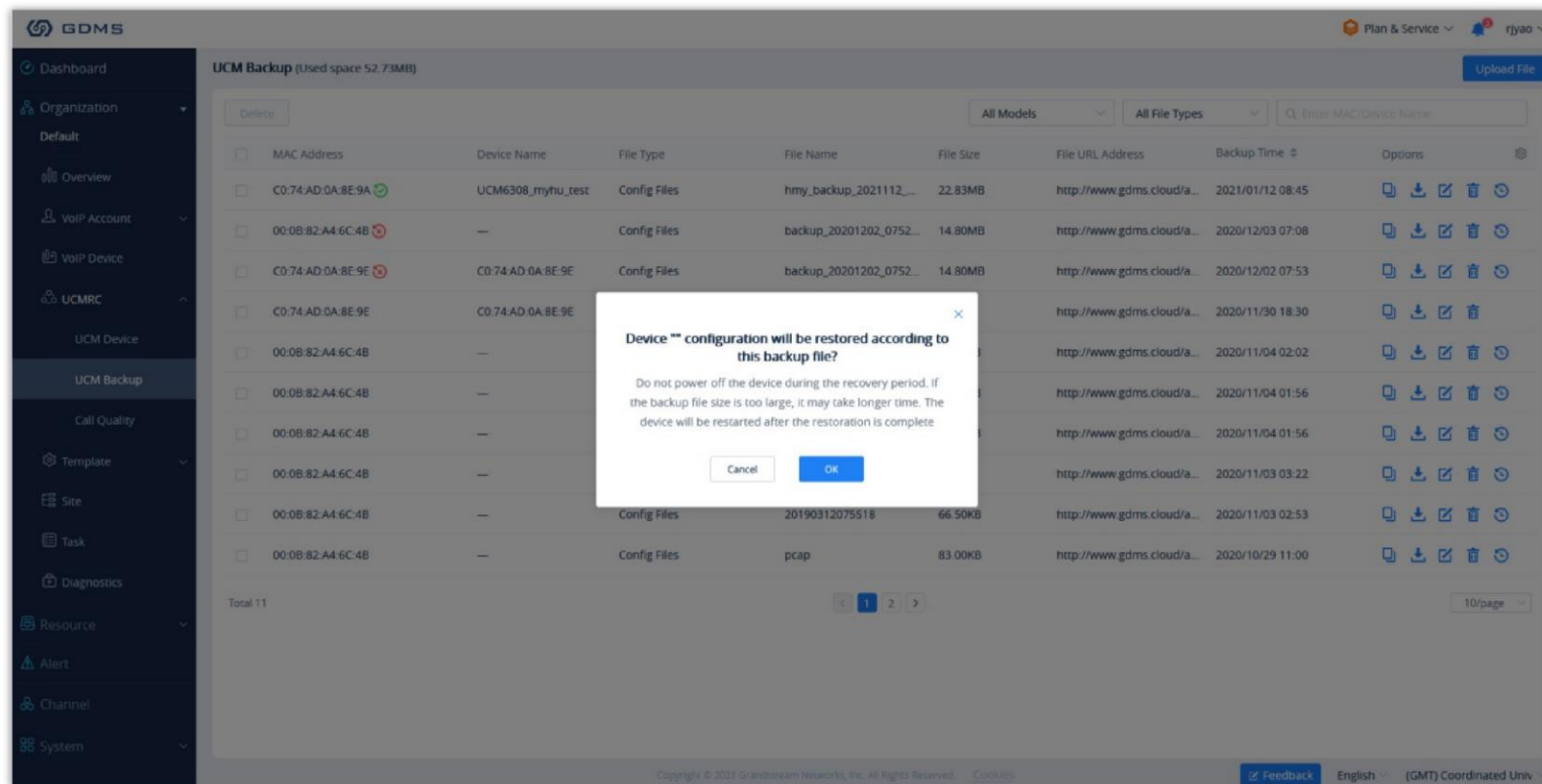
2. Download the files locally.

- i**
- Users can view the backup files and restore the UCM device quickly without downloading.
 - Users can download the backup file manually and restore the UCM device.
 - Users can download the files in batches by selecting them on the UI and then click “Download”

Restore UCM Backup File Remotely

Users can restore backup files for UCM devices remotely through the GDMS platform.

1. On the “UCM Backup” interface, select a UCM backup file and click the “Restore” button  to restore the UCM device.

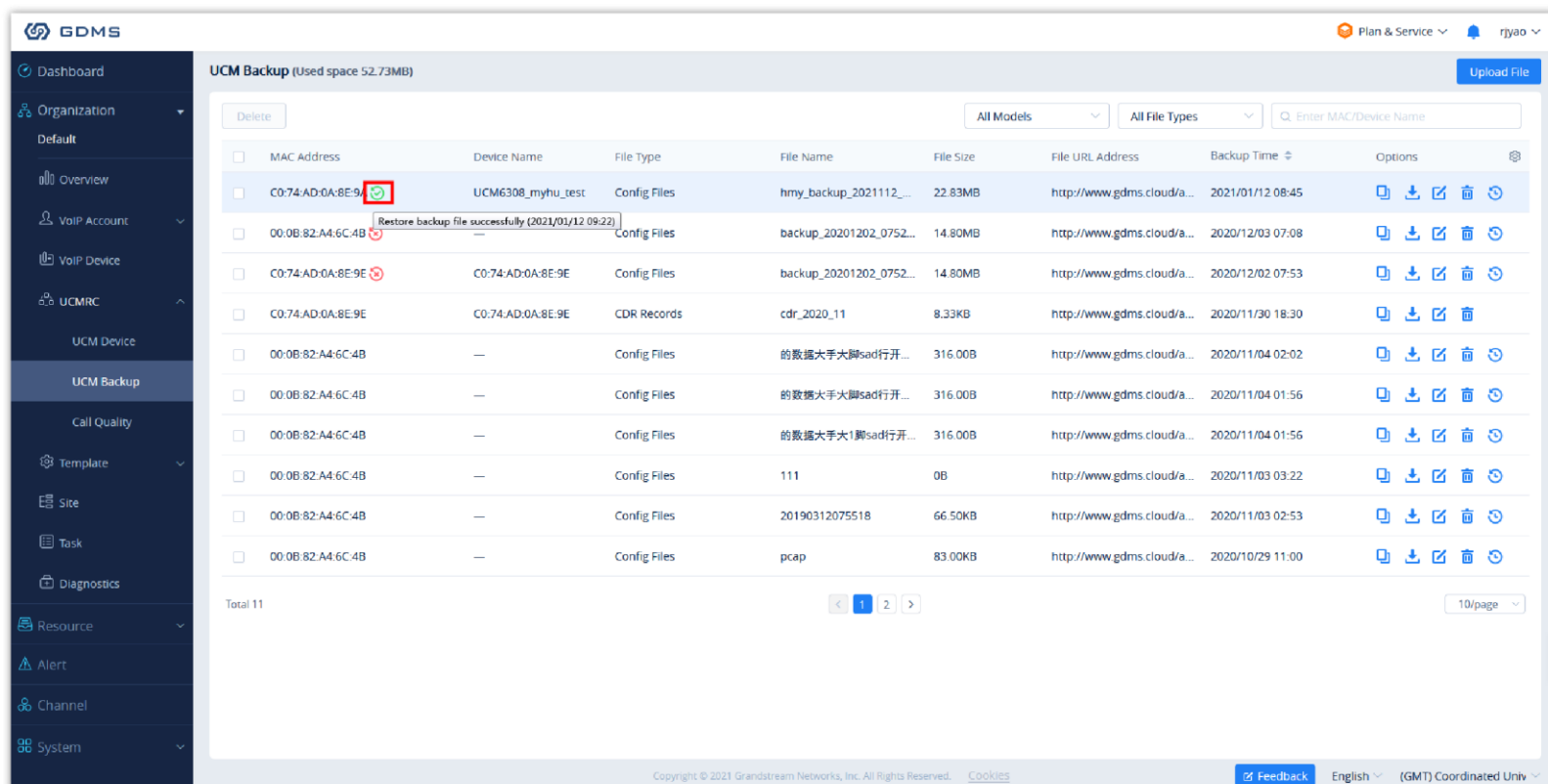


Restore Backup File Remotely

2. Once the user clicks the “OK” button, the UCM backup file will be assigned to the UCM device to restore the UCM device.
3. It may take several minutes to restore the backup file for the UCM device. The user can refresh the interface to view the results next to the MAC address of the UCM device on the interface. As the screenshot shows below:

 : Restored successfully. The user can leave the cursor on the icon to view the last restoring time.


 : Restored failed. The user can leave the cursor on the icon to view the last restoring operation time.



View Results

Delete Backup File

If the user wants to clean up the storage space of the UCM device, the user can delete the backup files in the UCM device.

1. On the “UCM Backup” page, click the button  following the resource file to delete the backup file. Users can also select multiple backup files and click the Delete button on the top of the page to batch delete the backup files.

2. When the user confirms to delete, the selected files will be deleted from the GDMS platform.

Note

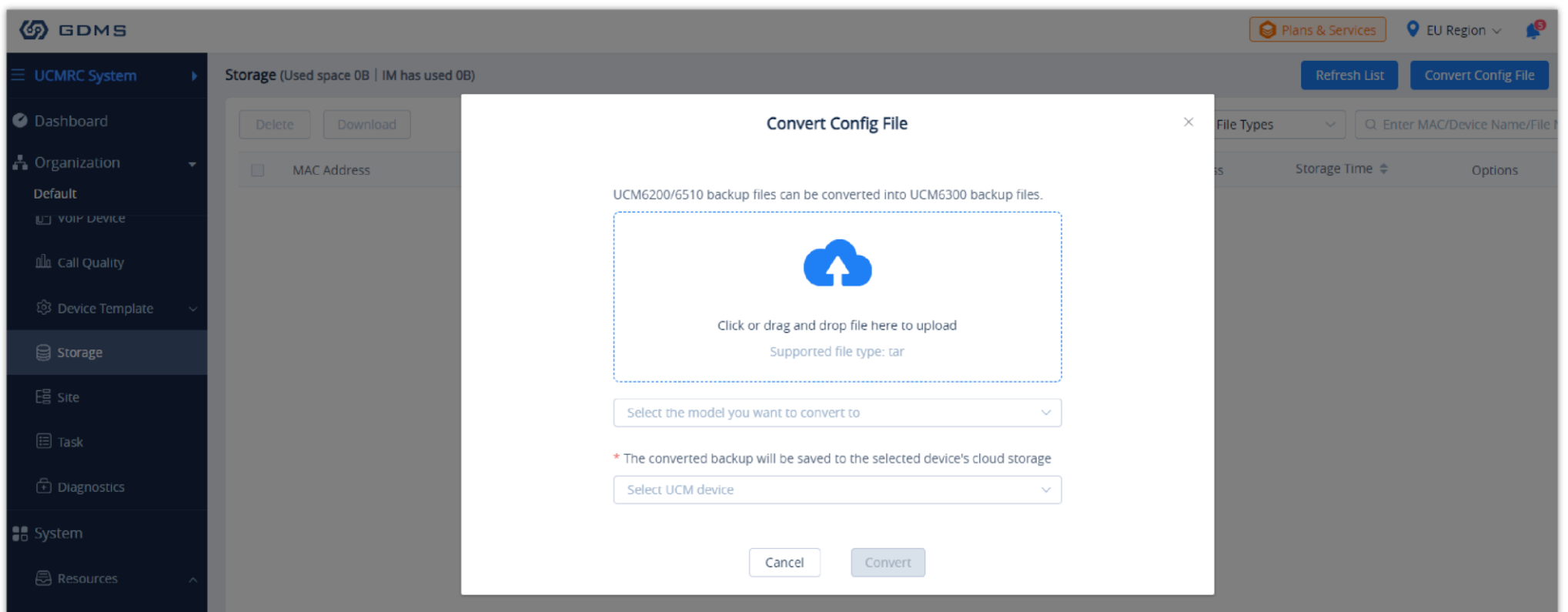
To delete multiple files at once, please select them by then click on “Delete”.

 Please note that when the backup file is deleted, it cannot be restored.

Convert Configuration File

If the user has upgraded the UCM device model, the user can use this function to convert the configuration file of UCM62xx/UCM65xx to the configuration file of UCM63xx.

1. Go to the **UCMRC System** → **Storage** interface, the user can click the “**Convert Config File**” button to access the conversion interface, as the screenshot shows below:



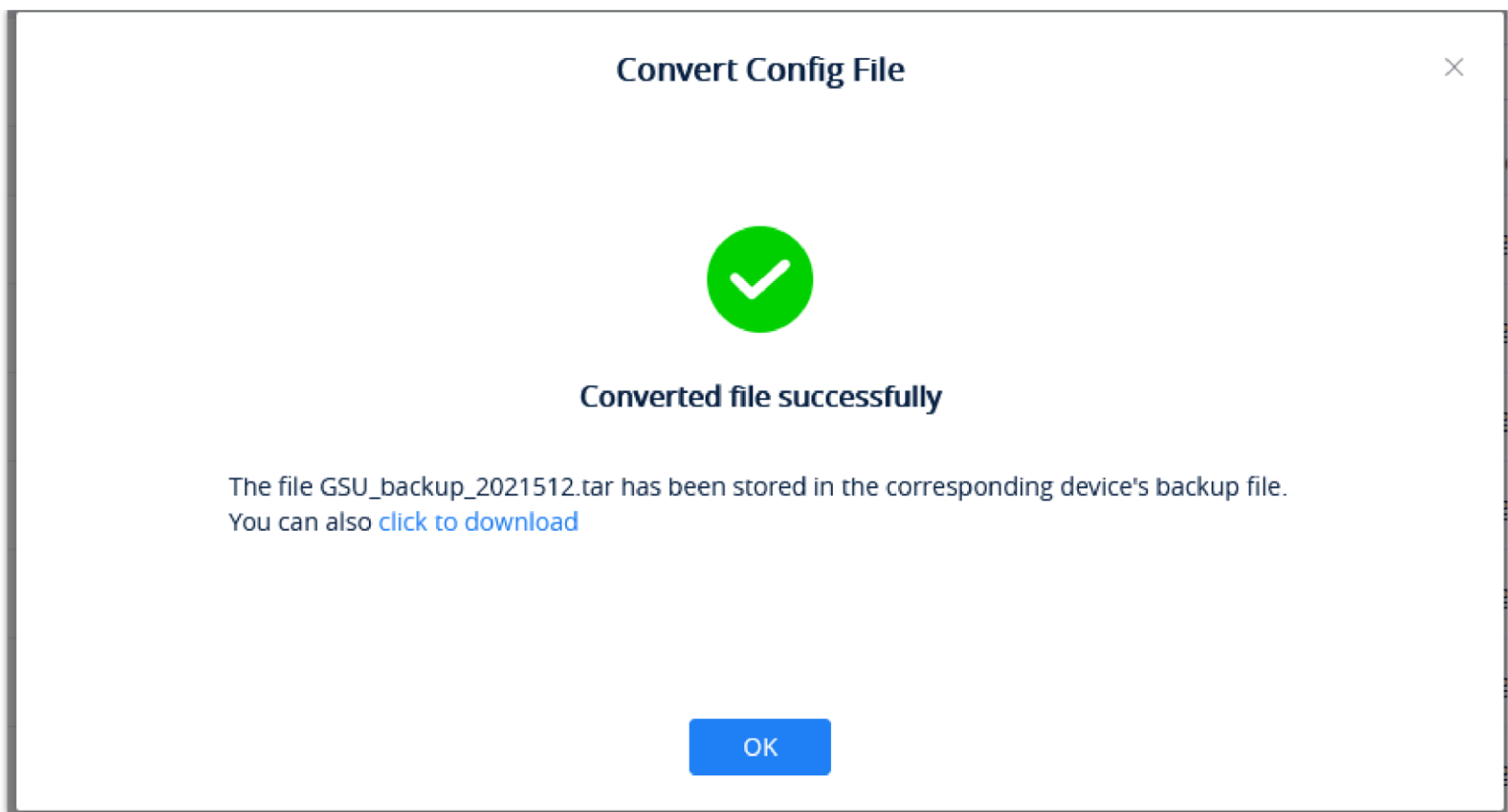
Convert Config File

2. The user can click to upload or drag the configuration file of UCM62xx/UCM65xx to the uploading area.

3. Select the target model to be converted, which means the model of your new UCM device.

4. Select the converted configuration file and save it to the cloud storage space of the new UCM device.

5. The converting duration will last for several minutes. When the conversion is done, the user can download the converted configuration file on the UCM Backup interface. Or the user can click to download the converted configuration file directly to the local PC. The user can also restore the configuration file in the new UCM device directly.



Converted File Successfully

i The original configuration file format needs to be a .tar file, and the file size limit is 10GB.

VoIP Device

This module displays all VoIP devices in the current organization.

For more details, please refer to the VoIP System -> VoIP Device module.

Call Statistics

Statistics Overview

The interface below displays the call quality reported by the device on the GDMS platform.

Prerequisites: The device must use the SIP account in the UCM server which has the UCM RemoteConnect service so that the device can report the call quality to the GDMS platform. This function is only supported for certain UCM RemoteConnect plans. To check which plans support this feature please refer to the RemoteConnect website: <https://ucmrc.gdms.cloud/home>

Module	Description
Total VoIP Devices	Display the number of VoIP devices reported by the current organization (only display the statistics report for the current filter time)
Total Calls	Display the number of calls reported by the current organization (only display the statistics report for the current filter time)
Call Quality	Display the call quality ratio and average values for the reported call history by the current organization (only display the statistics report for the current filter time)
Call Type	Display the call types for the reported call history by the current organization (only display the statistics report for the current filter time)

Table 23: Statistics Overview

Note

- The user needs to purchase the advanced UCMRC plan which contains this service before using the features. If the phone which has been associated with the GDMS platform has registered the extension which was synchronized from the UCM device to the GDMS platform (assigned through the GDMS platform), the phone will report the call quality to the GDMS platform (the audio will not be collected).
- Supported models: HT8XX, GXV33XX, and GRP260X series.

Call Quality Record

GDMS platform displays all reported call quality records on the **Call Quality** interface.

Please see the screenshot below:

MAC Address	Device Name	Call Quality	SIP Account	Average Jitter	Packet Loss Rate	MOS-LQ	MOS-CQ	Round Trip Delay
C0:74:AD:22:4D:32	rrrrrr	Bad	4002	27.00ms	0.00%	4.4	4.4	100.00ms

Call Quality Record

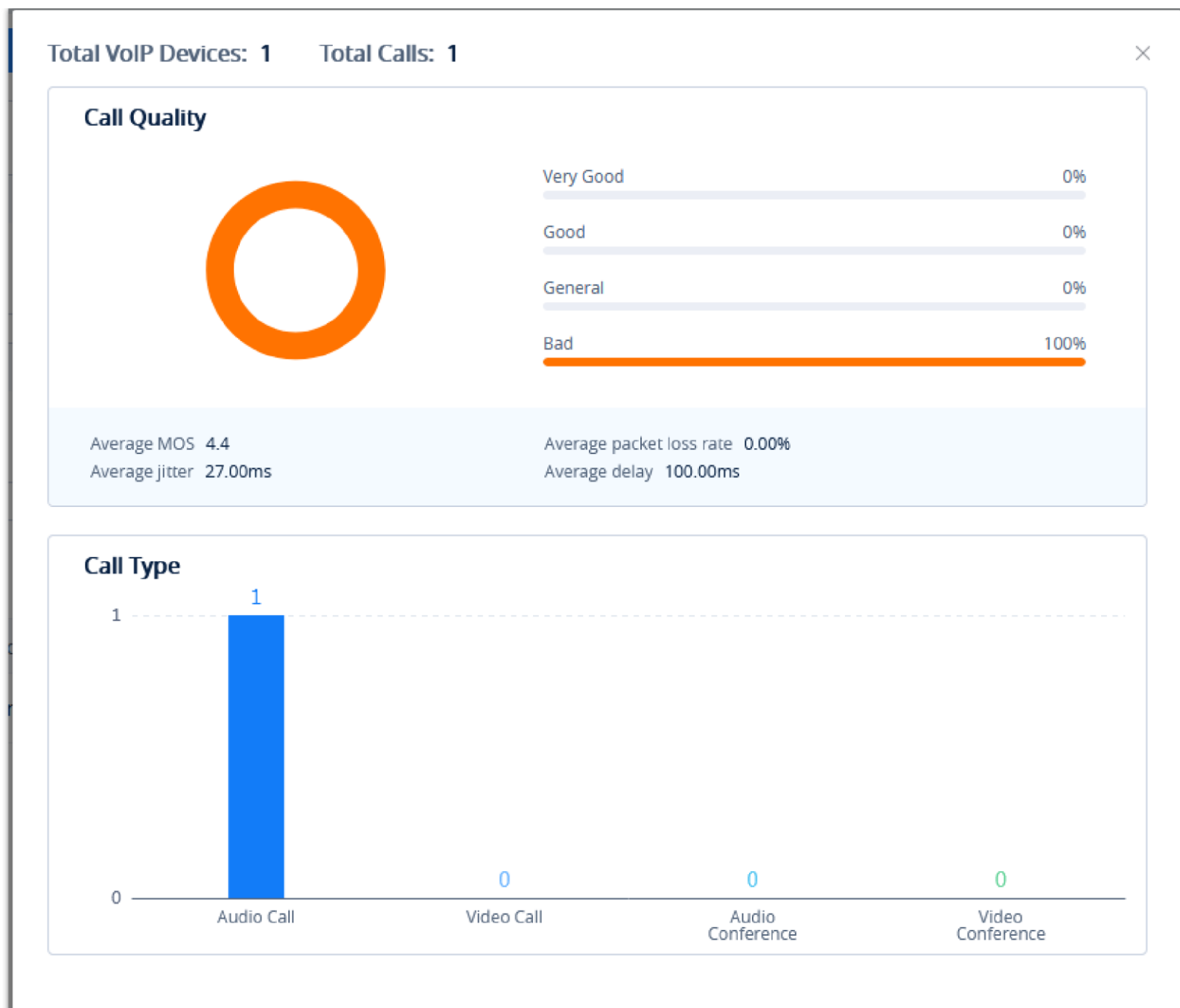
1. GDMS platform supports filtering call quality records by date.

Filter by Date

2. GDMS platform supports search call quality records by site, device model, call quality, and call type.

3. GDMS platform supports to search of call quality records by device MAC address, device name, and SIP Account.

4. Click the **Call Statistics** button  to view the statistical report of the filtered call quality records.

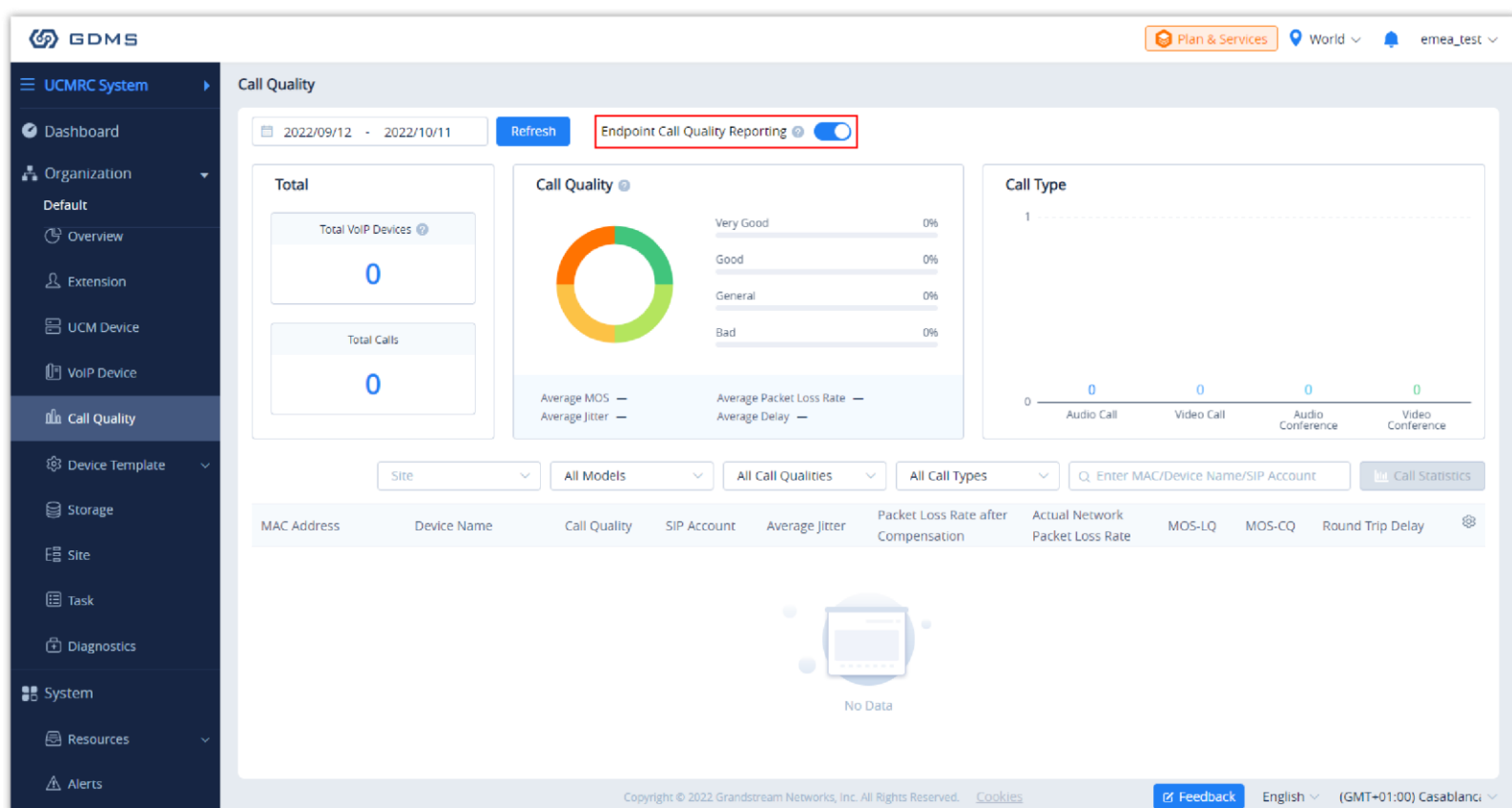


Call Quality Record Report

Enable/Disable Call Quality Reporting

Users can enable/disable reporting call quality on the GDMS platform. If the user does not want to view the call quality report, the user can disable this function on the GDMS platform.

On the **Call Quality** interface, the user can click **Phone reports the call quality** button **Phone reports the call quality** to disable reporting call quality. When this function is disabled, the devices under the current organization will no longer report the call quality to the GDMS platform.



Enable/Disable Call Quality Reporting

DEVICE CONFIGURATION

The **Device Configuration** page allows users to create templates that can be used to provision devices of the same model or in the same group. Additionally, users can upload configuration files for individual devices and manage them individually.

! Users can only manage the devices in the current organization of the current system.

By Model

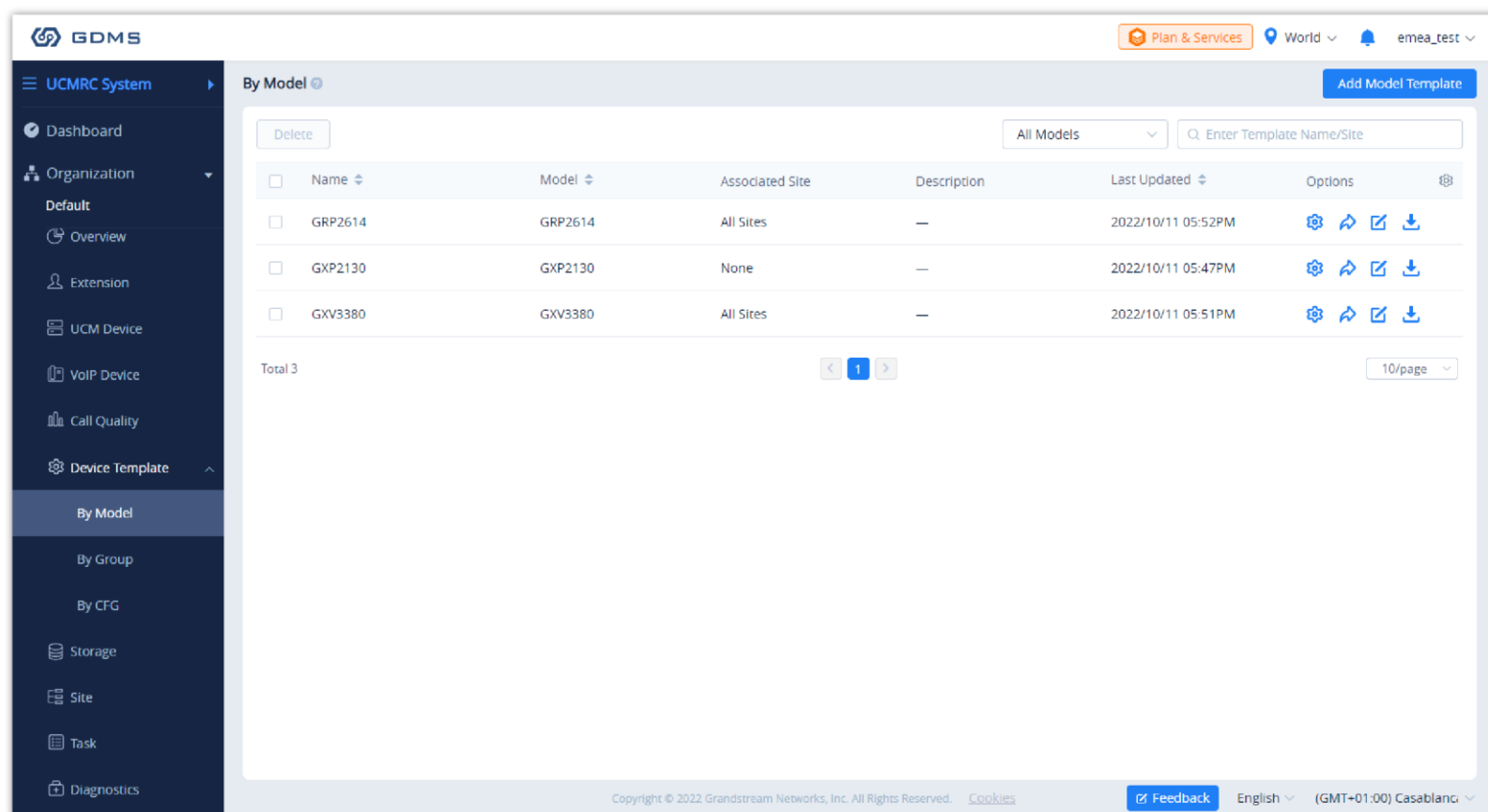
Users could customize the configuration template and classify the templates by device model and site. Users could also configure a batch of devices on the GDMS platform, which means users could create a configuration template for all same models of devices or create multiple templates for different sites.

Automatic Configuration Push

When a device is added to GDMS for the first time, it will automatically obtain and use the configuration template for its model.

Manual Configuration Push

To manually push the configuration to specific device models, click on the  button of the desired models.



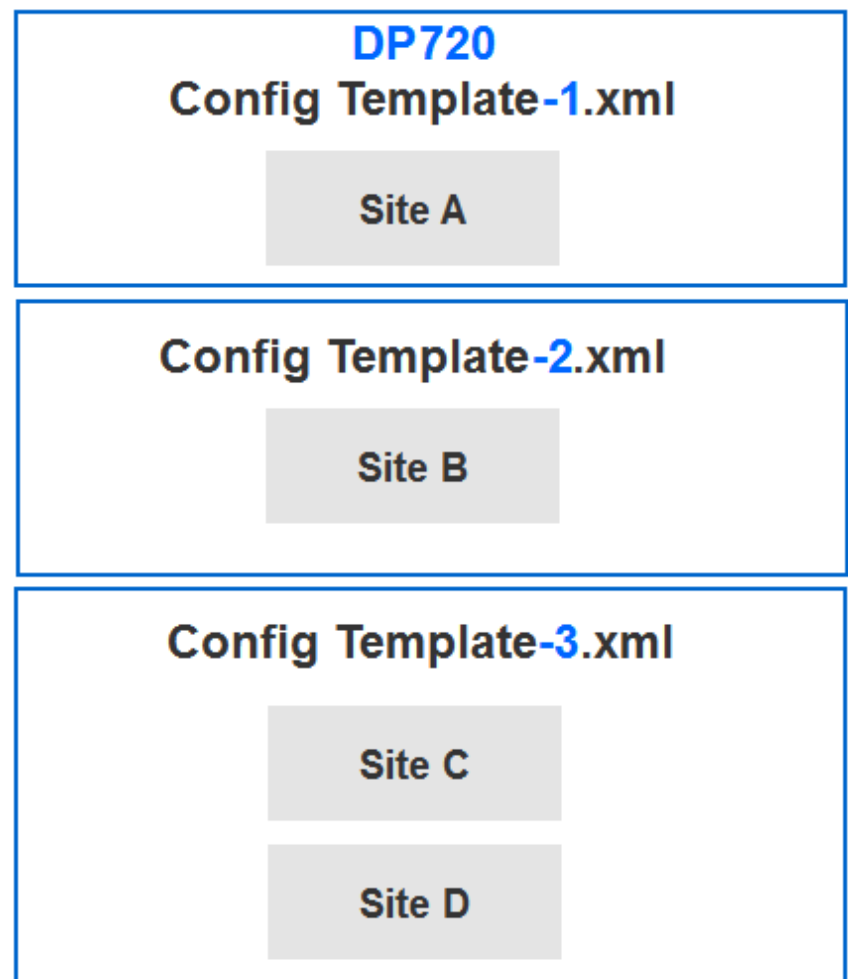
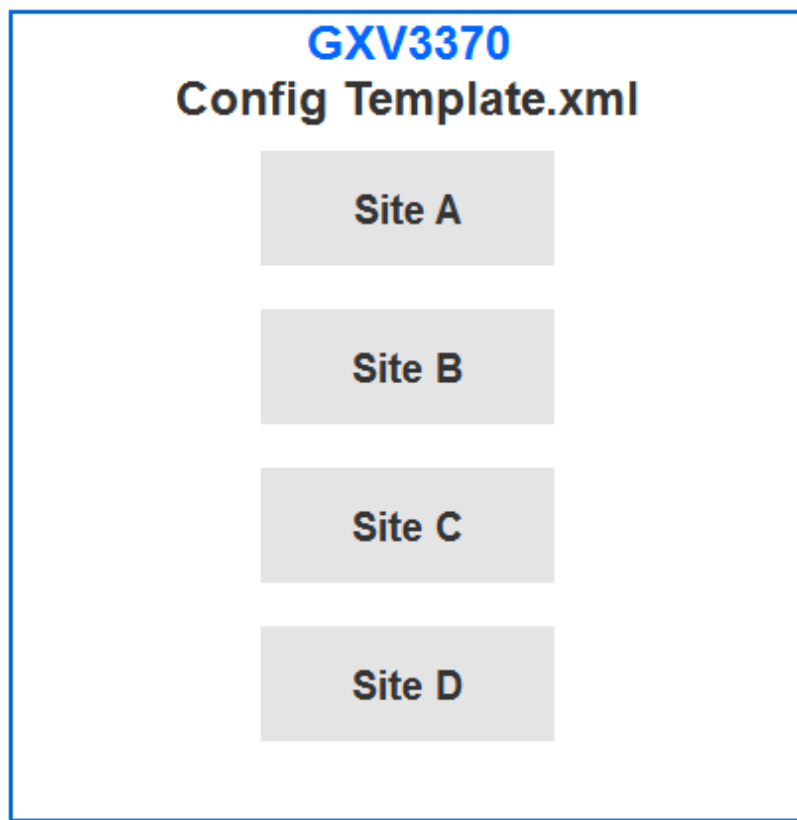
Manual Configuration Push

✓ If a device's setting has not been modified in the Device Management → Device → Set Parameters page, GDMS will automatically update the device with the template settings created in the Device Configuration page.

Example:

For GXV3370 devices, all sites are using the same configuration template, and all the devices under site A – D will acquire the same configuration template – GXV3370 Config Template.xml.

For DP720 devices, different sites have different configuration templates. The DP720 in site A will acquire the DP720 configuration file – Config Template -1.xml; the DP720 in site B will acquire the DP720 configuration file – Config Template -2.xml.



Example – GXV3370

Add Template

To add a configuration template for a specific device model, click on the **Add Template** button in the **By Model** page and enter the following information:

Add Model Template ×

* Name

* Model

* Auto Provision to Devices in All Sites Select Site None

i This template is automatically pushed only when the device under the site is connecting to GDMS for the first time.

Remember current selection

CFG File

Description

Add Template

Name	Enter the name of the template. This name must be unique and has a maximum character limit of 64.
Model	Select the device model of the template.
Select Site	Select the site for which the template will be used. <ul style="list-style-type: none"> • All Sites: All devices in all sites will use this template.

	<ul style="list-style-type: none"> • Select Site: All devices in the selected sites will use this template. Multiple sites can be selected. • None: GDMS platform will not allocate the template to any device. The user could allocate the template to the device manually.
Description	Users could input the descriptions of the template and the purpose.

Add Template

Once complete, users will be redirected to the **Set Parameters** page to modify the device settings of the template.



- For the new associated device, when the device first time connects to the GDMS platform, it will acquire the configuration template according to the device model and site automatically. Users do not need to push the configuration template manually.
- Devices already on GDMS will not automatically obtain the settings from newly added configuration templates. Users will need to update these devices manually.



If the GDMS platform has the model configuration template for the current device, and the user does not modify the configuration parameters from the Device Management → Device → Set Parameters menu, the GDMS platform will push the default model configuration template to the device when the device is online. Otherwise, if the user updates the device configuration on the “Set Parameters” menu on the GDMS platform and pushes it to the device, the device will use this configuration as the default configuration.


Set Parameters

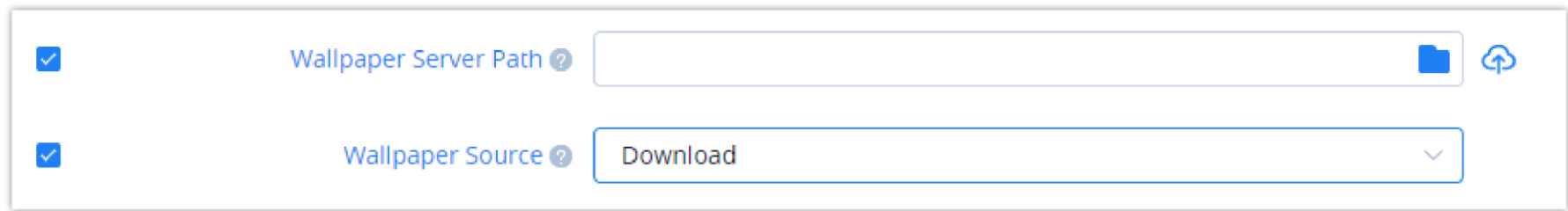
Users can configure model-specific settings when editing model templates.

1. To configure these model-specific settings, click on the  of the desired template.

Set Parameters

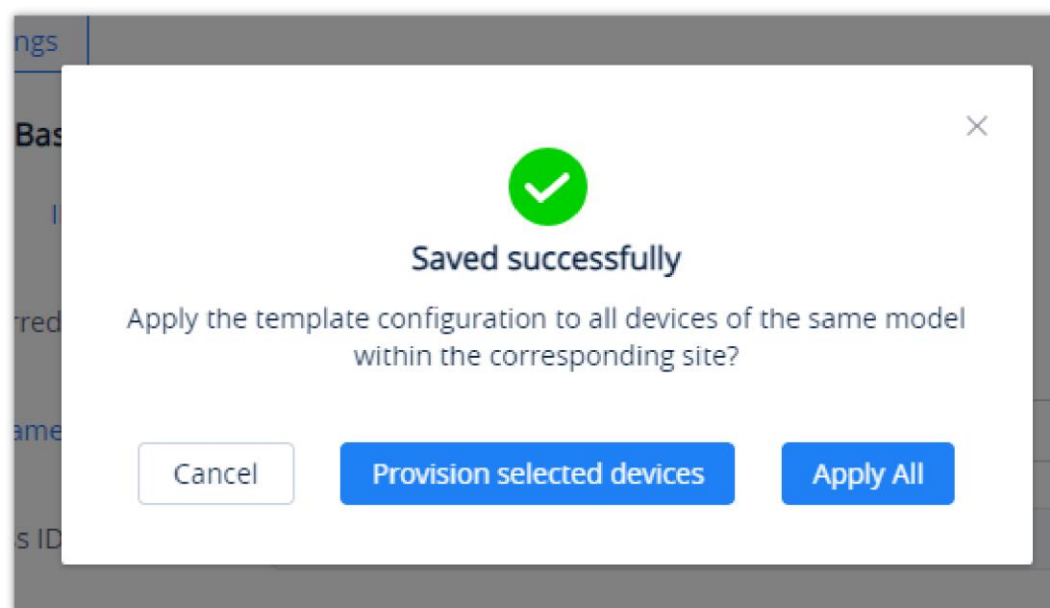
2. Clicking on the **Select All** button will select every option on the current page. Clicking on it again will deselect all the options.
3. Clicking on the **Reset Settings** button will restore all settings on the current page to default values.

- Clicking on the button  following the account, users can copy and paste the current account configuration to other accounts.
- When users try to configure the device wallpaper or screensaver image, users can select a picture from the resources list, or upload the local picture to GDMS and configure it to the device.



Ringtone Configuration

- Modify the desired settings on the page or click on the **Switch to Text Editor** to configure device settings via text editing (e.g. p-values). The key can be either a P-value or an alias.
- After setting the parameters, the user can click the “Save” button to save the changes. The user can select to apply the template configuration to all same model devices on the corresponding site. The user can click the option “Provision to Selected Devices” to select the devices to which the user wants to push the parameters to. The user can also click the button “Apply All” to push the parameters to all devices.




Saved Parameters Successfully

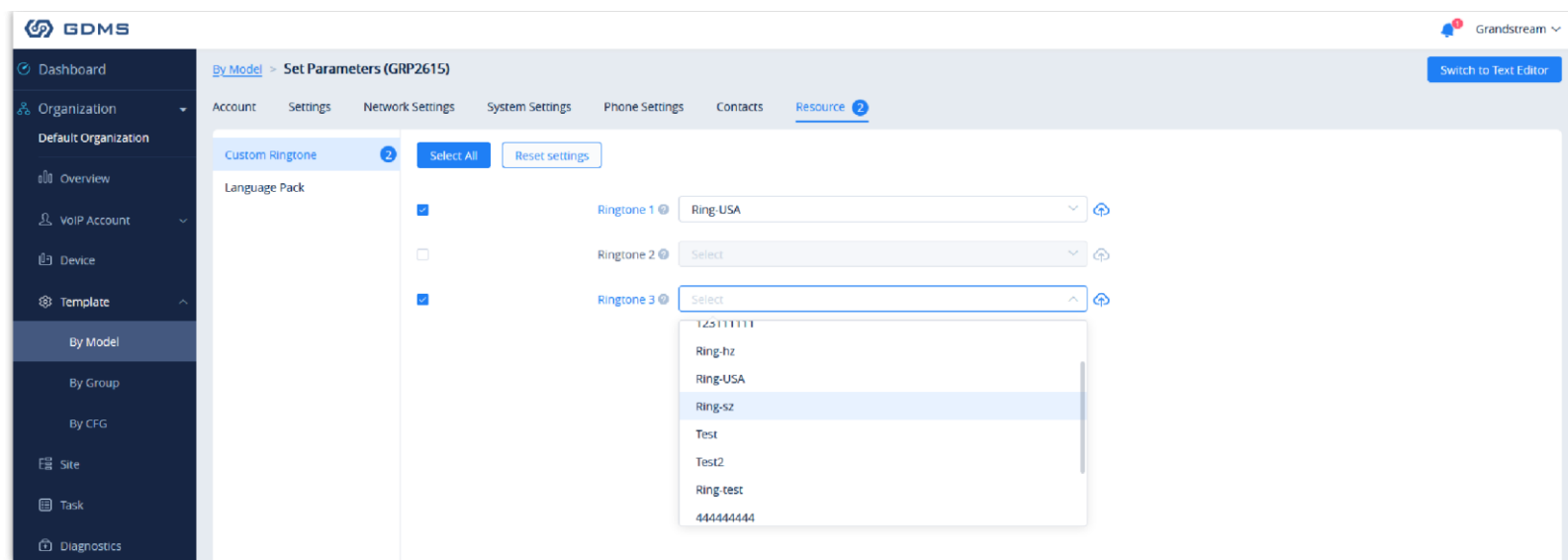


- The available settings for each model template are different. For more details on acceptable configuration values, please refer to the user guide for each device model.
- When the user adds a new model configuration template in the GDMS platform, the GDMS platform will not push the template to the existing devices in the GDMS platform, and the GDMS platform will only push the newly added template automatically to the new associated devices in the system.
- When the settings of a template are modified, the changes will not be automatically applied to related devices. Users will need to manually push the configuration to devices.
- For the newly added devices, the devices will acquire the updated configuration template automatically.
- If a scheduled task involves a modified template, the task will use the template settings at the time of scheduling, not the newly modified settings.
- Users can use the Search function to find the needed parameter.

Configure Resource Files

Users can configure custom ringtones and language for devices (Supported models: GXP/DP series).

- To configure these model-specific settings, click on the button  of the desired template to go to the **Parameters Configuration → Resource Configuration** page, as shown in the figure below:



Resource Configuration

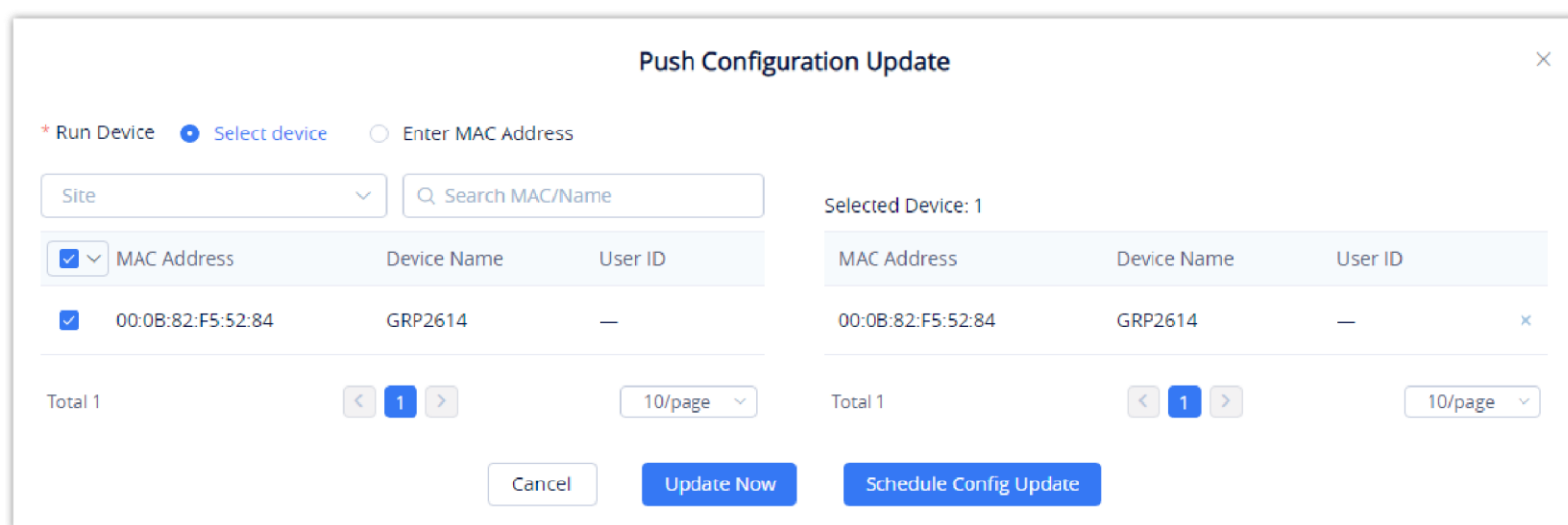
2. On the “Custom Ringtone” page, for Ringtone 1 to Ringtone N, select a ringtone file from the resources for each ringtone index.
3. On the “Language Configuration” page, select a language pack from the resources for the device.
4. After clicking the “Save” button, the device of this model will download the resource file from the firmware path once the device is connected to the GDMS platform for the first time.
5. Or, users can click the “Push” button to push the template of the model to the device. Then, the device will download the resource file from the firmware path.

i For each device model, the size and duration of each ringtone are different. If the duration and size exceed the limit, the system will intercept the resource file to the maximum limit automatically.

Push Update

Users could push the configuration template to the device manually.

1. Select a specific configuration template, and click on the button  following the template.



Push Configuration File

2. Users could select any device in this device model to push the configuration template, the device will be updated with the configuration template.
3. Users can either push the configuration template immediately or schedule the configuration push for a specified time. If the latter is selected, users will need to enter a name and time for the scheduled push.

Schedule Config Update

* Task Name

* Run Time

🕒 2019-04-04 14:55 - End Time

Schedule Config Update

4. Click on the **Save** button to finalize the task. Users can check the task status on the **Task Management** page.

Edit Template

To edit the configuration template's name, site, and description, click on the button for the desired template.

Edit Model Template

🔔 This template is automatically pushed only when the device under the site is connected to GDMS for the first time.

* Name

* Model

GRP2614
▼

* Auto Provision to Devices in

All Sites
 Select Site
 None

Description

Edit Model Template

Download Model Template Configuration

To download the configuration template of a device model, click on the button for the desired template.

<input type="checkbox"/>	DP All	DP750	All Sites	test	2019/01/09 07:47	
--------------------------	--------	-------	-----------	------	------------------	--

Download Configuration Template

Copy Model Template

On the main page of the Model Template, the user can copy one or multiple templates and apply them to a different organization, this allows the user to copy the configuration easily across many organizations.

To copy a template, please tick the box on the left side of the template name, then select .

Copy Template

- **Target Organization:** Select the organization to which you want to copy the template to.
- **Auto Provision to Devices in:** You can select “All Sites”, “Select Sites”, or “None”. The rules are the same as those for creating model template.

After the templates have been copied successfully, the templates will be added to the “By Model” page of the selected organization, and the templates name will be “Original Template Name_Copy”.

Delete Model Template

To delete configuration templates from GDMS, select the desired templates and click on the **Delete** button in the top left corner of the **By Model** page.

i template saved at the time of scheduling. A scheduled task will not fail due to deleted templates.

Delete Template

By Site

Users can customize device templates based on sites. The users will be able to configure devices based on the sites to which they have been assigned to.

The screenshot shows the 'By Site' view of the Device Template management interface. The left sidebar contains navigation options: UCMRC System, Dashboard, Organization, Default, Overview, Extension, UCM Device, VoIP Device, Call Quality, Device Template (expanded), By Model, By Site (selected), By Group, By CFG, Storage, Site, Task, and Diagnostics. The main content area displays a table with the following data:

<input type="checkbox"/>	Name ↕	Associated Site	Description	Last Updated ↕	Options
<input type="checkbox"/>	Home Template	home	—	2022/12/30 09:21	

Below the table, it shows 'Total 1' and a pagination control with '1' selected. A search bar at the top right contains the text 'Enter Template Name/Site'. The footer includes copyright information for Grandstream Networks, Inc. and a 'Feedback' button.

Device Template: By Site

Add Site Template

To add a template, please click [Add Site Template](#)

The 'Add Site Template' dialog box contains the following fields:

- Name:** A text input field containing 'Main Office'.
- Auto Provision to Devices in:** A dropdown menu with 'Default' selected.
- Description:** A text area containing 'Template for the IP phones located in the main office.'

At the bottom of the dialog, there are 'Cancel' and 'Save' buttons.

Add Site Template

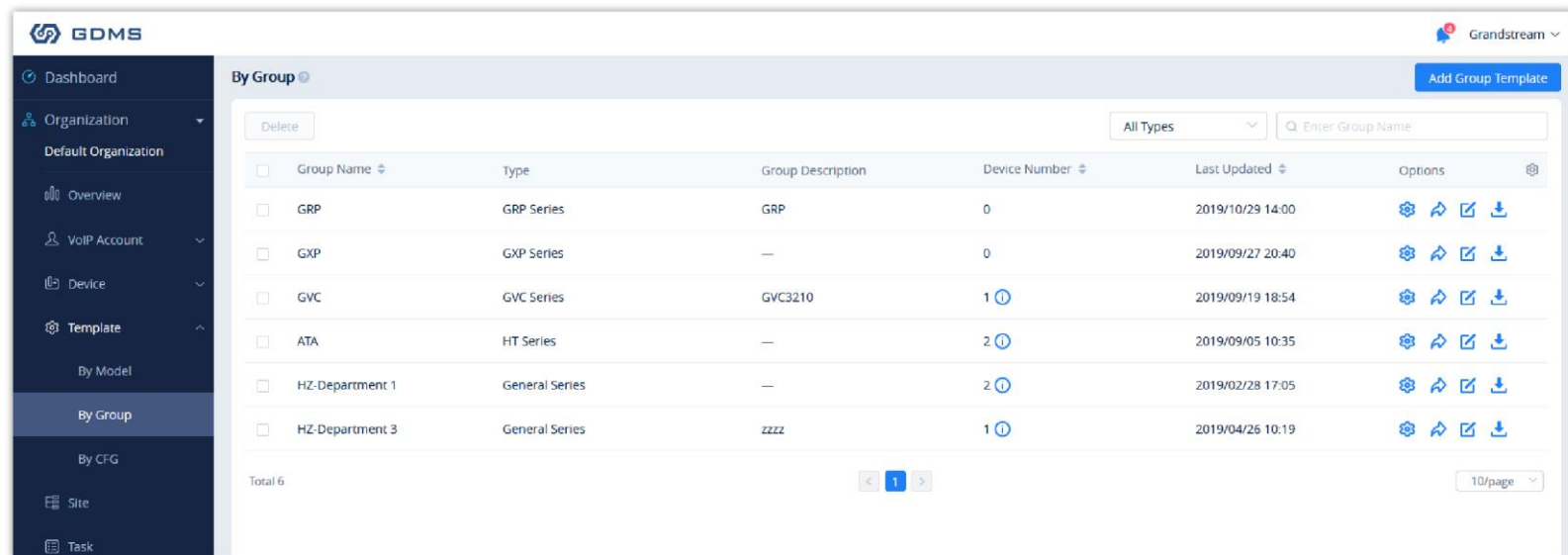
- **Name:** Enter the name of the template.
 - **Auto Provision to Devices in:** Choose the site on which the template will be applied to.
 - **Description:** Enter a description for the template.
- : Use this button to edit the information related to the template.
- : Use this button to change the configuration of the template.

By Group

Users could customize the configuration template by group. Users could configure a group and update the configuration template by group. For example, users could classify a batch of devices into a group and configure/manage the devices in the group. Users could push the configuration template to the group members on the GDMS platform.

Users could view the group configuration template, and the devices list in each group.

Users could modify the configuration parameters, push the configuration to the devices, edit the group and members, and download the configuration template by group.



The screenshot shows the 'By Group' page in the GDMS interface. It features a sidebar with navigation options like 'Dashboard', 'Organization', 'Overview', 'VoIP Account', 'Device', 'Template', 'By Model', 'By Group', 'By CFG', 'Site', and 'Task'. The main content area displays a table of groups with columns for Group Name, Type, Group Description, Device Number, Last Updated, and Options. A 'Delete' button and a search bar are at the top. A 'Total 6' indicator and pagination controls are at the bottom.

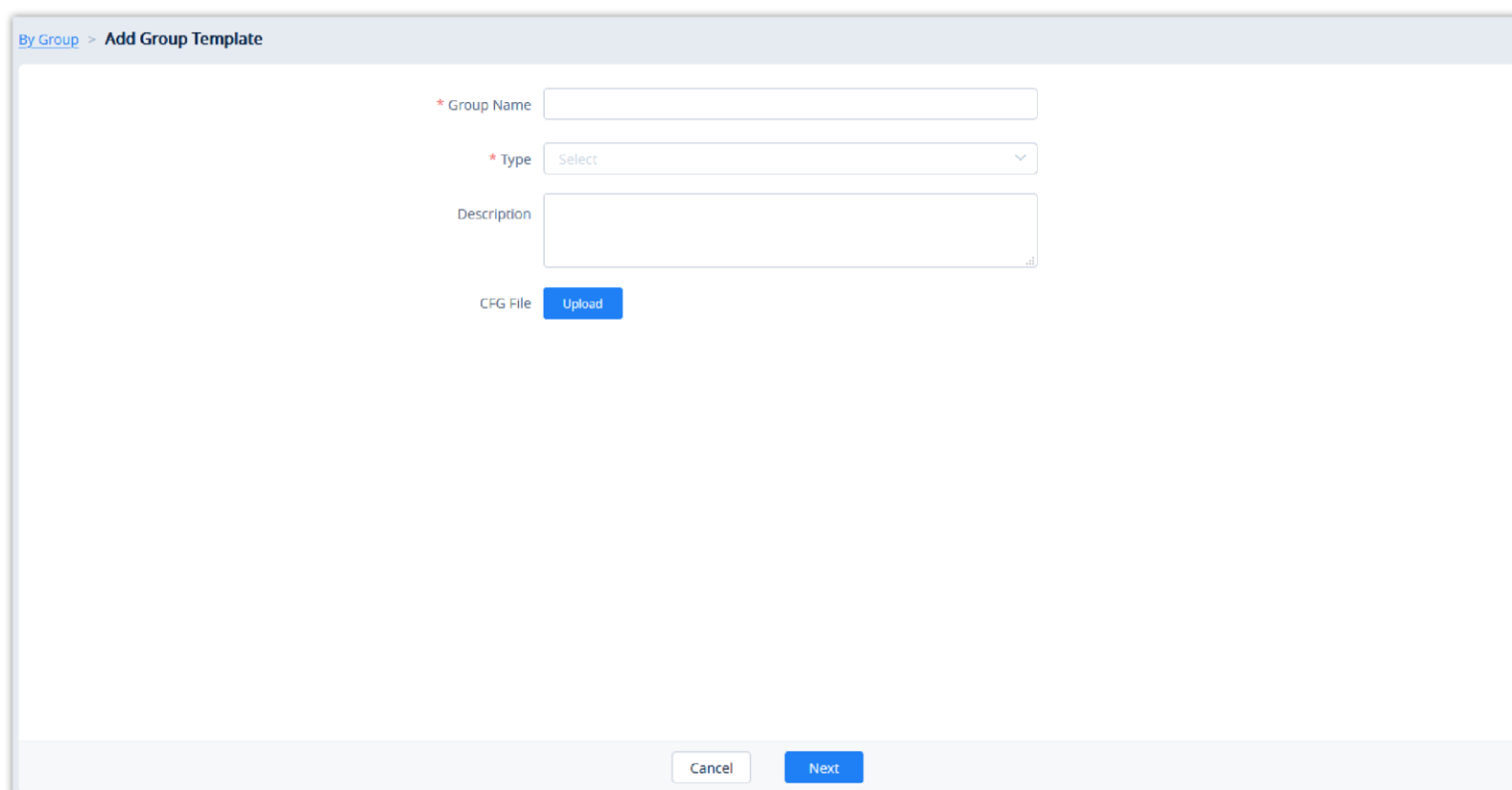
Group Name	Type	Group Description	Device Number	Last Updated	Options
GRP	GRP Series	GRP	0	2019/10/29 14:00	[Settings] [Share] [Edit] [Download]
GXP	GXP Series	—	0	2019/09/27 20:40	[Settings] [Share] [Edit] [Download]
GVC	GVC Series	GVC3210	1	2019/09/19 18:54	[Settings] [Share] [Edit] [Download]
ATA	HT Series	—	2	2019/09/05 10:35	[Settings] [Share] [Edit] [Download]
HZ-Department 1	General Series	—	2	2019/02/28 17:05	[Settings] [Share] [Edit] [Download]
HZ-Department 3	General Series	zzzz	1	2019/04/26 10:19	[Settings] [Share] [Edit] [Download]

By Group

Add Group

Users could add a group at any time on the GDMS platform.

1. Click on the **Add Group** button at the top right of the **By Group** page.



The screenshot shows the 'Add Group Template' form. It includes fields for 'Group Name' (required), 'Type' (required dropdown), 'Description', and 'CFG File' with an 'Upload' button. 'Cancel' and 'Next' buttons are at the bottom.

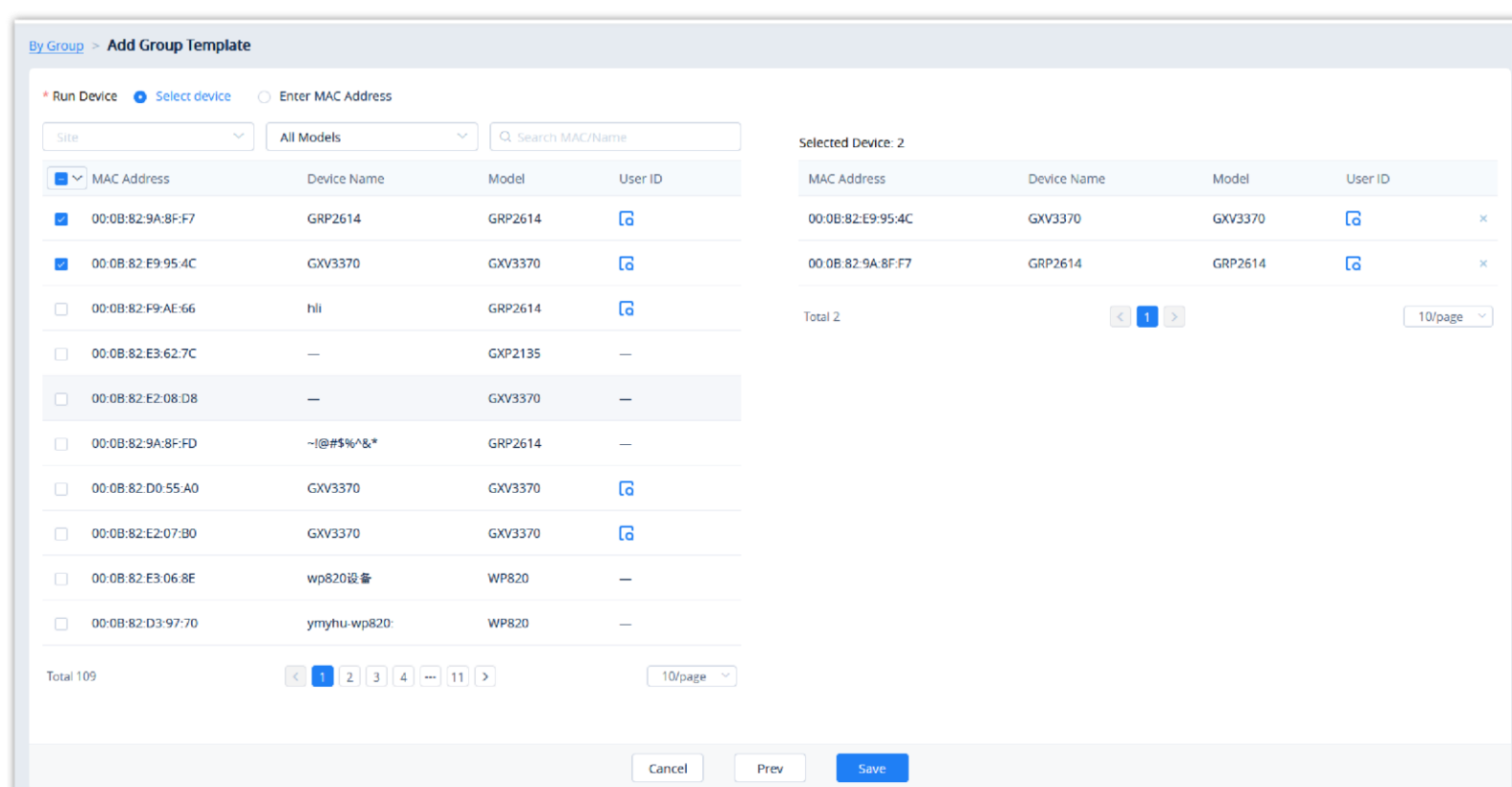
Add Group

Group Name	Enter the name of the group to easily identify it. Names must be unique and have a maximum character limit of 64.
-------------------	---

Type	<p>Users need to select the type:</p> <ul style="list-style-type: none"> ◦ Audio phone series: This is used to configure the common configuration parameters of the GXP and GRP series. ◦ DP series: Use the configuration template for the DP7xx series. ◦ HT series: Use the configuration template for the HT8xx series. ◦ GRP series: Use the configuration template for the GRP series. ◦ GXP series: Use the configuration template for the GXP21xx series. ◦ GXV series: Use the configuration template for the GXV33xx series. ◦ GVC series: Use the configuration template for GVC3210.
Description	Enter the detailed description and purpose of the configuration template.

Add Group

2. Once complete, users will be redirected to the device selection page to add devices to the group. Users can either select devices from the list or manually enter the MAC addresses of the devices. Selected devices will be moved to the **Selected Device** list on the right of the page.



Finish Adding Group

3. Users could click on the “Prev” button to go back to the group configuration page to re-edit the group information.

4. Click on the **Save** button to complete the group member selection. Users will then be redirected to the **Set Parameters** page.

i Users need to set the parameters of the configuration template for the newly added group.

Set Parameters

Users could set the unique parameters of the devices in the group in the configuration template to push the unique parameters to the devices in the group.

Select a specific group, and click on the button to access the group member parameters configuration page.

- Clicking on the **Select All** button will select every option on the current page. Clicking on it again will deselect all the options.
- Clicking on the **Reset Settings** button will restore all settings on the current page to default values.
- Clicking on the button following the account, users can copy and paste the current account configuration to other accounts.

- When users try to configure the device wallpaper or screensaver image, users can select a picture from the resources list, or upload the local picture to GDMS and configure it to the device.

The screenshot shows a configuration panel with two rows. The first row is labeled 'Wallpaper Server Path' and has a checked checkbox on the left, a text input field, a folder icon, and an upload icon. The second row is labeled 'Wallpaper Source' and has a checked checkbox on the left, a dropdown menu currently showing 'Download', and a downward arrow icon.

Ringtone Configuration

- Modify the desired settings on the page or click on the Edit Configuration File to configure device settings via text editing (i.e. p-values). The key can be either a P-value or an alias.



- The available settings for each model template are different. For more details on acceptable configuration values, please refer to the user guide for each device model.
- When the user adds a new model configuration template in the GDMS platform, the GDMS platform will not push the template to the existing devices in the GDMS platform, and the GDMS platform will only push the newly added template automatically to the new associated devices in the system.
- When the settings of a template are modified, the changes will not be automatically applied to related devices. Users will need to manually push the configuration to devices.
- For the newly added devices, the devices will acquire the updated configuration template automatically.
- If a scheduled task involves a modified template, the task will use the template settings at the time of scheduling, not the newly modified settings.

Configure Resource Files

Users can configure custom ringtones and language for devices (Supported models: GXP/DP series).

1. Select a specific group, and click on the button to access the group member parameters configuration page.

The screenshot shows the 'Set Parameters (GXP)' page in the GDMS interface. The 'Resource' tab is active. Under 'Custom Ringtone', there are three rows for Ringtone 1, 2, and 3. Ringtone 1 is set to 'Ring-sz', Ringtone 2 is set to 'Select', and Ringtone 3 is set to 'Ring-USA'. A dropdown menu is open for Ringtone 3, showing a list of resources including 'testtesttest', '123411', '123111111', 'Ring-hz', 'Ring-USA' (highlighted), 'Ring-sz', and 'Test'. There are 'Select All' and 'Reset settings' buttons. The 'Language Pack' section is also visible on the left.

Resource Configuration

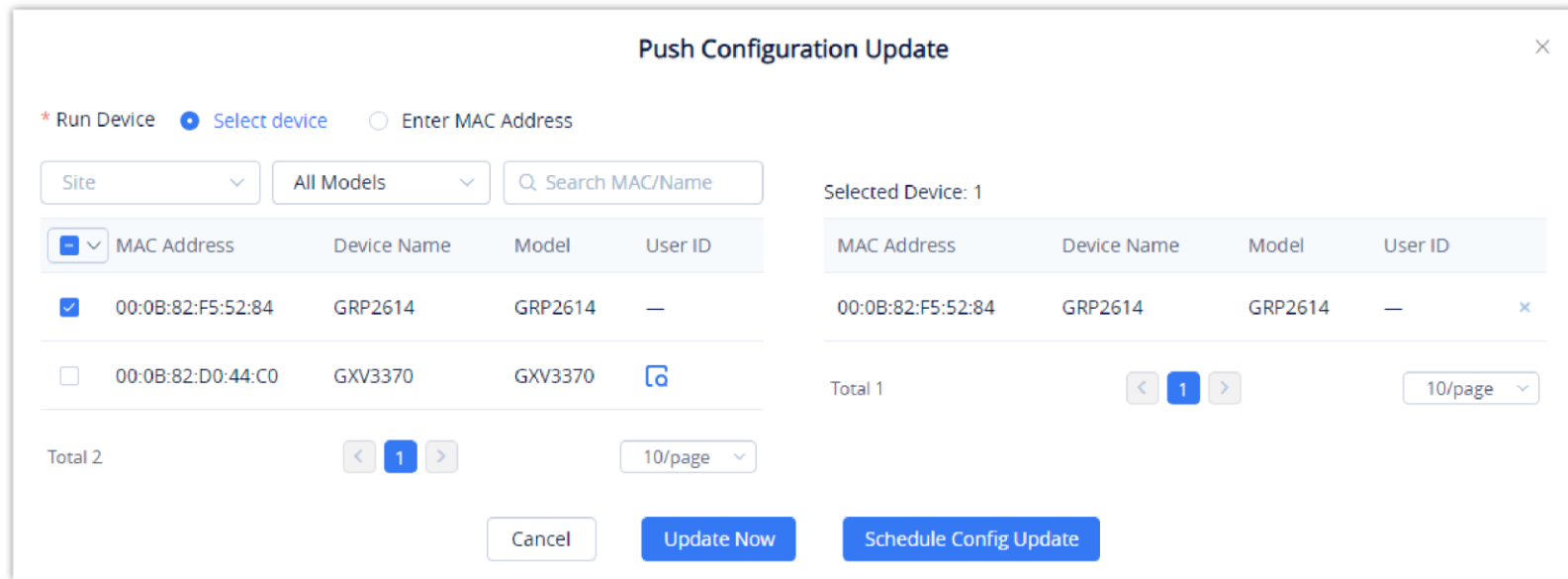
2. On the “Custom Ringtone” page, for Ringtone 1 to Ringtone N, select a ringtone file from the resources for each ringtone index.
3. On the “Language Configuration” page, select a language pack from the resources for the device.
4. After clicking the “Save” button, the configured parameters and resources will be saved in the system. When the user clicks the “Push” button to push the template to the device, the device will download the resource file from the firmware path.

❗ For each device model, the size and duration of each ringtone are different. If the duration and size exceed the limit, the system will intercept the resource file to the maximum limit automatically.

Push Update

Users could push the group configuration template to the device manually.

1. Click on the  button for the desired group.



MAC Address	Device Name	Model	User ID	
<input checked="" type="checkbox"/>	00:0B:82:F5:52:84	GRP2614	GRP2614	—
<input type="checkbox"/>	00:0B:82:D0:44:C0	GXV3370	GXV3370	

Total 2

MAC Address	Device Name	Model	User ID	
<input checked="" type="checkbox"/>	00:0B:82:F5:52:84	GRP2614	GRP2614	—

Selected Device: 1

Total 1

Push Update

2. In addition to being able to push the configuration template to all or select members of the group, users can also push it to non-members.
3. Users can either push the configuration template immediately or schedule the configuration push for a specified time. If the latter is selected, users will need to enter a name and time for the scheduled push.
4. Click on the **Save** button to finalize the task. Users can check the task status on the Task Management page.

Edit Group Template

Users could edit the group name, descriptions, and group members.

1. Click on the  button for the desired group.

<input type="checkbox"/>	HZ-Department 1	Non-DP Series	—	2	2019/01/17 03:29	
--------------------------	-----------------	---------------	---	---	------------------	--

Figure 138: Edit Group

2. Modify the desired settings and click on the **Save** button to finalize changes.

❗ New members of an existing group will not automatically obtain the group configuration template. The template must be manually pushed to the new member devices.

Download Group Template Configuration

Users can download the group configuration template by clicking on the  button for the desired group.

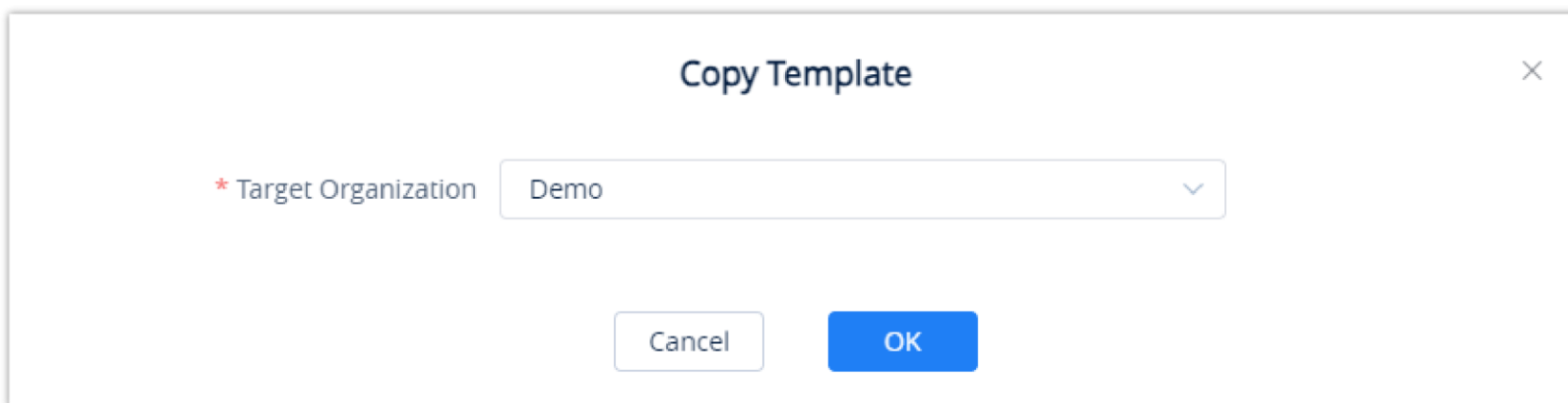
<input type="checkbox"/>	HZ-Department 1	Non-DP Series	—	2	2019/01/17 03:29	
--------------------------	-----------------	---------------	---	---	------------------	--

Download Configuration File

Copy Group Template

On the main page of the Group Template, the user can copy one or multiple templates and apply them to a different organization, this allows the user to copy the configuration easily across many organizations.

To copy a template, please tick the box on the left side of the template name, then select [Copy Template](#).



The image shows a modal dialog box titled "Copy Template" with a close button (X) in the top right corner. Inside the dialog, there is a label "* Target Organization" followed by a dropdown menu currently showing "Demo". At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

Copy Group Template

Select the organization to which you want to copy the template to by selecting the organization name from the "Target Organization" list.

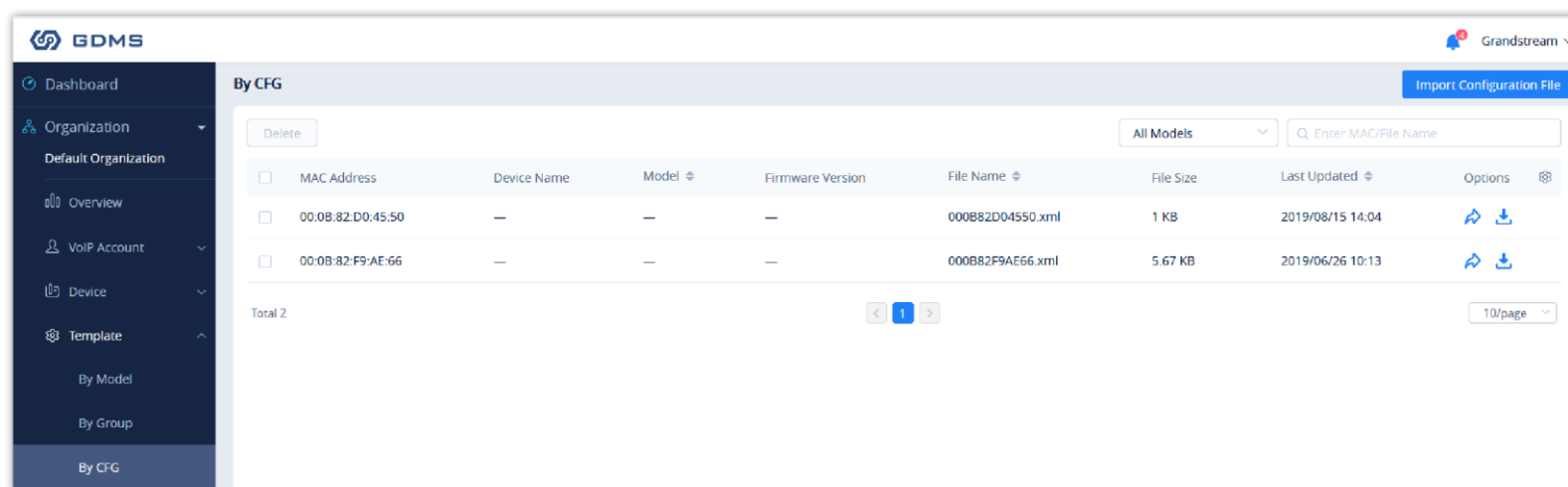
Delete Group Template

Users can delete groups by selecting the desired groups and clicking on the **Delete** button in the top-left corner of the **By Group** page.

i The existing timing tasks involving the group configuration template will be reserved, and the timing task will be executed with the original group configuration template.

By CFG

Users can import configuration files for specific devices. Settings in these uploaded files will be used for their specified device.



The screenshot shows the "By CFG" page in the GDMS interface. The page has a sidebar on the left with navigation options: Dashboard, Organization, Default Organization, Overview, VoIP Account, Device, Template, By Model, By Group, and By CFG (selected). The main content area is titled "By CFG" and includes a "Delete" button, a search bar for "Enter MAC/File Name", and a table of configuration files. The table has columns for MAC Address, Device Name, Model, Firmware Version, File Name, File Size, Last Updated, and Options. There are two rows of data, and a "Total 2" summary at the bottom. A "10/page" dropdown is also visible.

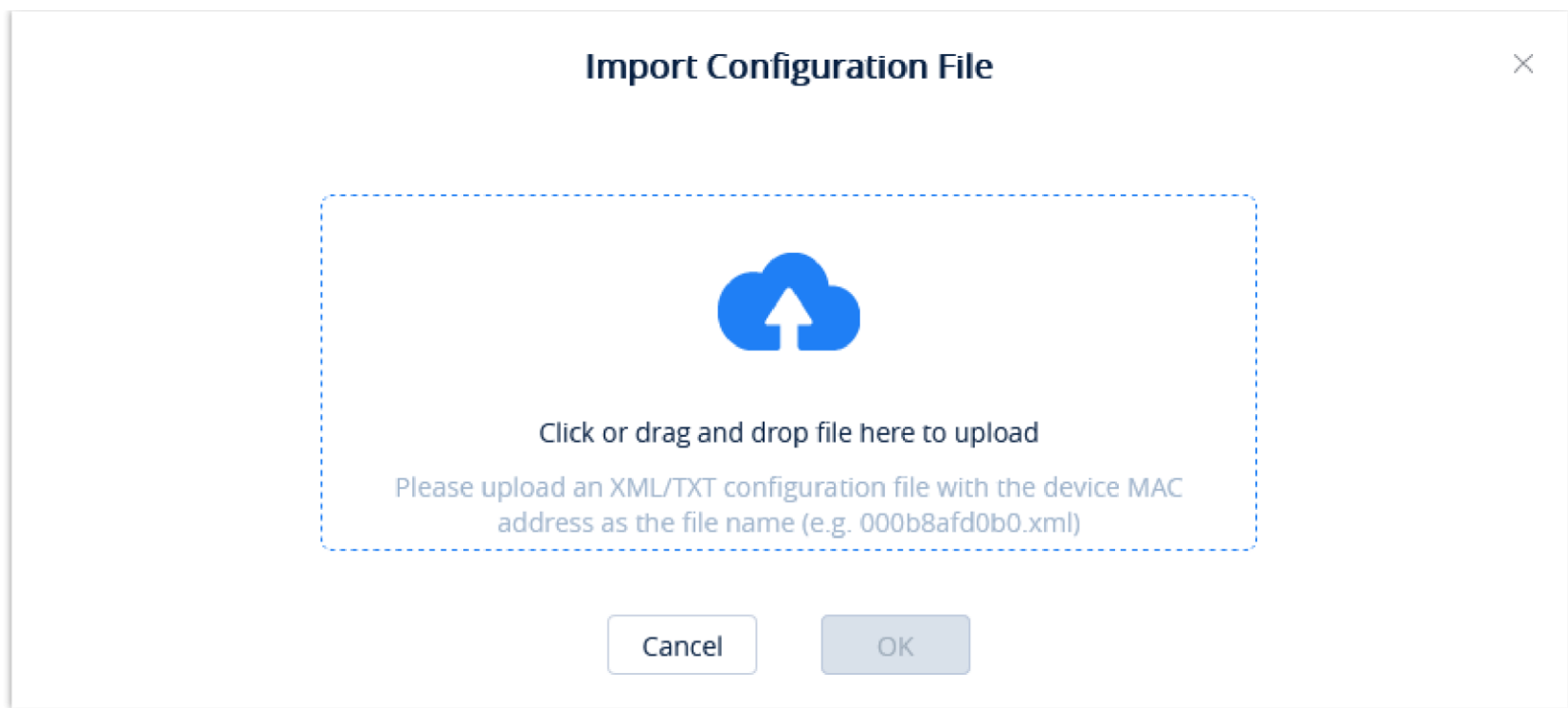
MAC Address	Device Name	Model	Firmware Version	File Name	File Size	Last Updated	Options
<input type="checkbox"/>	00:0B:82:D0:45:50	—	—	000B82D04550.xml	1 KB	2019/08/15 14:04	↶ ↷
<input type="checkbox"/>	00:0B:82:F9:AE:66	—	—	000B82F9AE66.xml	5.67 KB	2019/06/26 10:13	↶ ↷

By CFG

Upload CFG File

Users could upload the custom configuration file to the GDMS platform and push the custom configuration file to the device.

1. Click on the **Import Configuration File** button at the top-right corner of the **By CFG** page. The following window will appear:



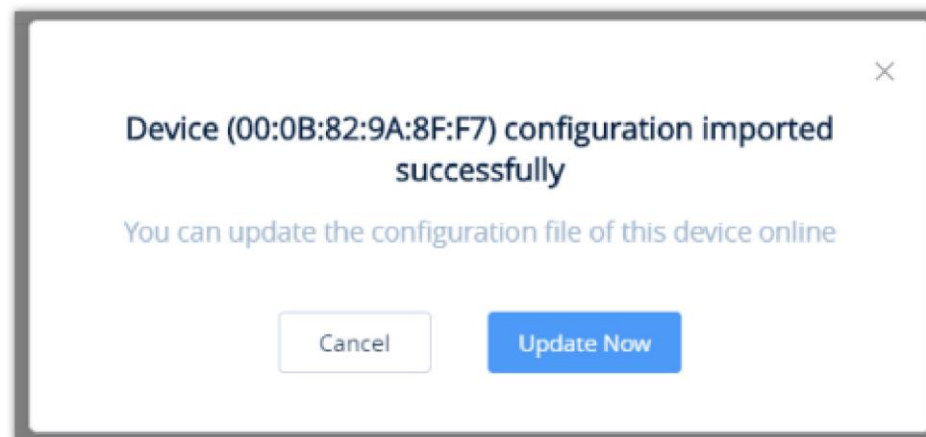
Upload CFG File

2. Drag and drop the file to the window or click on the upload icon to select a file from your PC.

i The uploaded file must be named as the device's MAC address (e.g. 000b82afd0b0.xml).

3. Click on the **OK** button to finalize the import.

4. The following window will appear asking the user to either push the configuration to the specified device immediately or to cancel the configuration push.





Finalize Import

- i**
- Only XML file format is supported for the uploaded custom configuration file.
 - If the file name does not meet MAC address format requirements, the import will fail. When uploading another configuration file for an existing device, the previous configuration file will be overwritten

Push Update

Click on the  button for the desired device to manually push the configuration to it.

<input type="checkbox"/>	00:0B:82:E5:8C:C9	DP750	1.0.6.3	000B82E58CC9.xml	41.79 KB	2019/01/24 11:41	 
--------------------------	-------------------	-------	---------	------------------	----------	------------------	---

Push Update

Download Configuration File

Click on the  button for the desired device to get its configuration file.

Delete CFG File

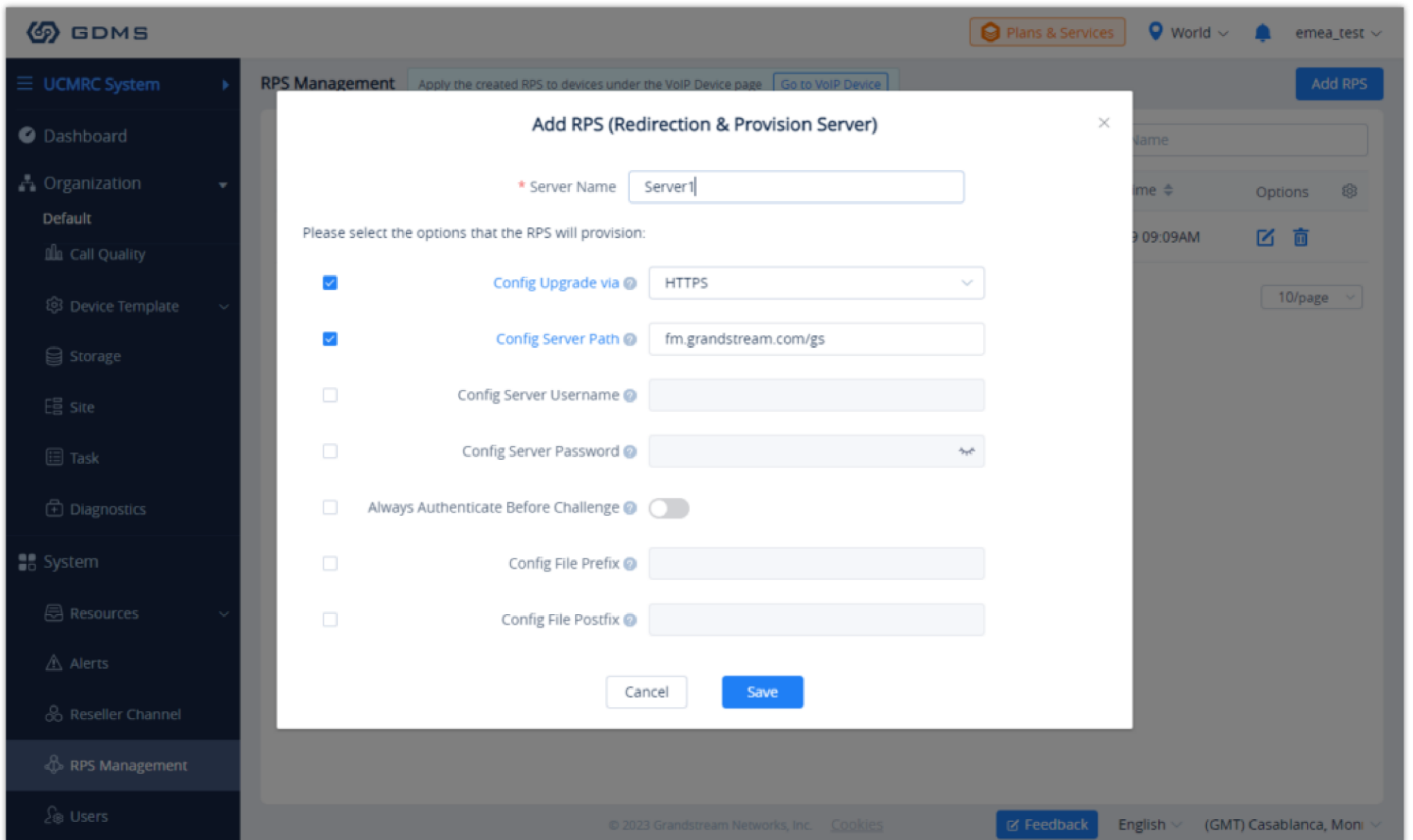
To delete uploaded configuration files from GDMS, select the desired devices in the list and click on the **Delete** button at the top left of the **By CFG** page.

RPS MANAGEMENT

RPS (Redirection & Provision Server) allows creating and pushing configuration to many Grandstream devices, this reduces the time and effort spent on configuring the devices manually, which improves the deployment process greatly and lessens the frequency of mistakes that occur when configuring the device manually.

The user can create instances of RPS (Redirection and Provisioning Server).

To configure this option, the user needs to create an RPS server by providing the IP address or FQDN domain of the server, then select the protocol used for upgrading.



The screenshot shows the GDMS interface with a modal dialog titled "Add RPS (Redirection & Provision Server)". The dialog contains the following fields and options:

- Server Name:** A text input field containing "Server1".
- Config Upgrade via:** A dropdown menu with "HTTPS" selected.
- Config Server Path:** A text input field containing "fm.grandstream.com/gs".
- Config Server Username:** An empty text input field.
- Config Server Password:** An empty password input field with a visibility toggle.
- Always Authenticate Before Challenge:** A toggle switch that is currently turned off.
- Config File Prefix:** An empty text input field.
- Config File Postfix:** An empty text input field.



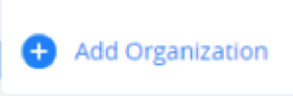
At the bottom of the dialog are "Cancel" and "Save" buttons. The background shows the RPS Management page with a table of existing RPS instances.

Add Redirection & Provision Server

Server Name	Enter the server name.
Config Upgrade Via	Select the protocol used for configuration upgrade. <ul style="list-style-type: none">• TFTP• HTTP• HTTPS• FTP• FTPS
Config Sever Path	Enter configuration server path.

Config Server Username	Enter the username to authenticate into the server.
Config Server Password	Enter the password to authenticate into the server.
Always Authenticate Before Challenge	Only applies to HTTP/HTTPS. If enabled, the phone will send credentials before being challenged by the server.
Config File Prefix	If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
Config File Postfix	If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.

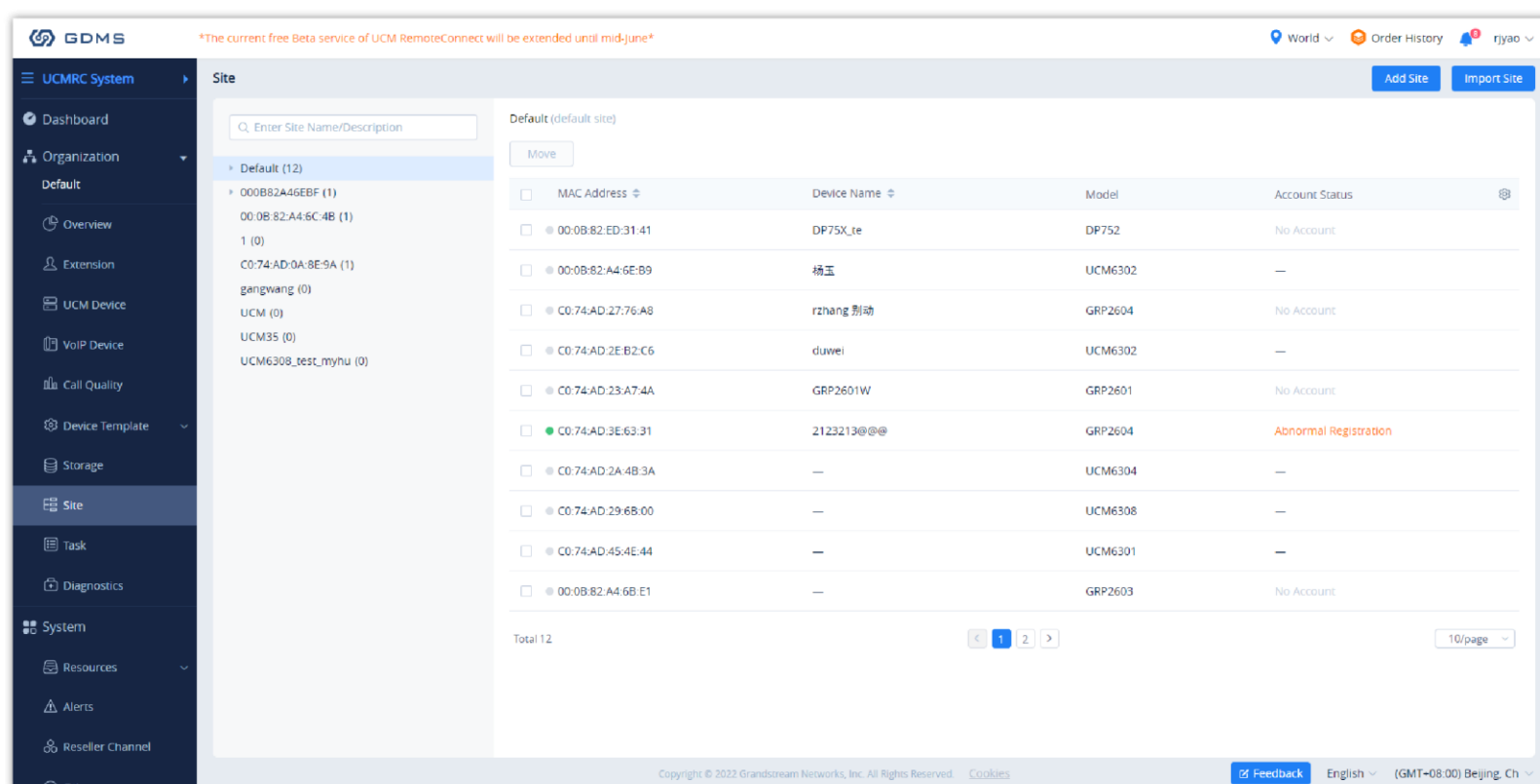
To assign a specific RPS to an organization, click on the three dots and add an organization as indicated in the figure below.

Server Name	Upgrade Via	Config Server Path	Number of Organizations	Updated Time	Options
Server1	HTTPS	fm.grandstream.com/gs	0	2023/03/29 09:09AM	 
Total 1					10/page

When an RPS is edited, the new RPS will be automatically delivered to the associated devices. If an RPS has been deleted, it only deletes the association between the RPS and the device. The RPS configuration will not be deleted from the device.

SITE MANAGEMENT


Site Management allows users to organize their devices by sites and categories.



Site Management

Add Site

Users could add a site at any time on the GDMS platform.

1. Click on the **Add Site** button at the top right of the **Site Management** page. To quickly add a sub-site under a specific site, click on the  button next to the desired site. Users can create a total of 7 different levels of sites.

Add Site ×

* Name

Parent Site

Description

Cancel
Save

Add Site

Site Name	Enter a name for the site to easily identify it. Sites on the same level cannot have the same name.
Superior Site	The parent level of the site. This field can be left blank if the created site is a top-level site.
Site Description	Enter the descriptions of the site.

Table 26: Add Site

2. Once the site is created, users can then assign devices to it.

Batch Import Sites

Users could import a batch of sites into the GDMS platform.

1. Click on the **Import Site** button at the top right corner of the **Site Management** page. The following window will appear:

Import Site ×

Click or drag and drop file here to upload

File types .xls and .xlsx are supported

Please use the following template to create compatible imports.

↓ Site Template

Cancel
OK

Import Site

2. Click on the **Download** button to get a template that will be used to import site information.

	A	B
1	Instructions: 1. Fields marked with * are required and cannot be empty. 2. Site Name format: 1st Level Site/2nd Level Site/.../New Site. Users must enter the names starting from the 1st Level Site. If the higher level sites do not exist, they will be created automatically. If no higher level site name is entered, this site name will be used by default to fill in missing site names. 3. Site Name maximum character limit is 64 characters. 4. Site Description maximum character limit is 256 characters.	
2	*Site Name	Description
3		
4		
5		
6		
7		

Site Template

Site Name	Enter the name of the site. If the site is the child of another site, users must enter the entire path (e.g. top-level site/second level site/third level site/...new site name).
Description	Enter the descriptions of the site.

Table 27: Site Template Options

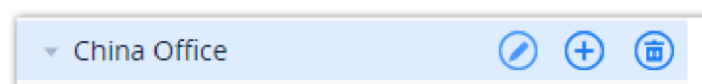
- Once the template is filled out, drag, and drop the file to the upload window or select the file from your PC. Click on the Import button to confirm the import.
- When the Excel file is imported into the GDMS platform successfully, the GDMS platform will prompt the execution result. If there is data that failed to be imported, the user could export the failed data and re-edit the Excel file.

! If an imported site has the same name as another site on the specified level, the import will fail.

Edit Site

Users could edit the information of the site on the GDMS platform.

- Click on the  button next to the desired site.



- Edit the desired fields and click on the **Save** button to finalize changes.

Edit Site ✕

* Name

Parent Site

Description

Edit Site

Delete Site

To remove a site from GDMS, click on the button next to the desired site.

If the selected site has devices assigned to it, the site cannot be deleted unless the devices are assigned to another site beforehand.

View Devices

To view all the devices under a specific site, click on the desired site in the **Site Management** list.

<input type="checkbox"/>	MAC Address	Device Name	Model	Account Status	
<input type="checkbox"/>	00:0B:82:E9:95:4C	GXV3370	GXV3370	Abnormal	
<input type="checkbox"/>	00:0B:82:D0:55:A0	GXV3370	GXV3370	Normal	
<input type="checkbox"/>	00:0B:82:E2:07:80	GXV3370	GXV3370	Abnormal	

View Devices

Transfer Site

Users can select devices on a site and move them to another site by clicking on the **Move** button.

Move ✕

* Site

Transfer Site

Clicking on the **Save** button will finalize the move to the specified site.

TASK MANAGEMENT

The **Task Management** page displays all queued and completed tasks in GDMS such as configuration pushes, firmware upgrades, reboots, and factory resets. Users can add, edit, and delete tasks from this page.

i Users can only manage the devices in the current organization of the current system. If the user does not have the permissions on the device, the user cannot manage tasks on the device.

Add Task

To add a task to GDMS, click on the **Add Task** button.

The screenshot shows the 'Add Task' form with the following fields and options:

- Task Name:** Enter Task Name (up to 64 characters)
- Task Time:** Immediate, Scheduled, Interval
- Task Type:** Upgrade Firmware
- Device Model:** Select Device Model
- Firmware Version:** Select Firmware Version
- Upgrade Method:** Concurrent Upgrade (10 device(s)), Sequential Upgrade
- Current Firmware Range:** All Versions
- Target Device(s):** All devices of this model, Select Device, Enter MAC Address

Add Task

Task Name	Enter the name of the task.
Task Time	<ul style="list-style-type: none"> ● Immediate: The task will be run immediately. If the task is not run after 5 minutes, GDMS will automatically close it. ● Scheduled: Schedule the task to run at a specified time. The task will end at the specified end time, even if there are still devices queued up to run the task. ● Interval: Users could configure the recurring tasks such as daily, weekly, monthly, Nth week of each month, and perform a certain task. Specify the start date and time when the task will start, then specify the Duration of the task. If a device goes online during the duration of the task, the scheduled task will be performed as soon as the device goes online. If the device goes online after the task's duration, the task will not be performed on that specific device. ● Permanent: This option applies only when the task type is Firmware Upgrade. Every time a corresponding device is added, the device will be upgraded. This is a reoccurrent task.
Task Type	<ul style="list-style-type: none"> ● Reboot Device: VOIP device and UCM device. ● Factory Reset: VOIP device only. ● Upgrade Firmware: Users will need to select the device model and firmware version to upgrade to. VoIP device and UCM device. ● Update Config: Model: Select the model template that will be used for the configuration update push. VOIP device only. ● Update Config: Group: Select the group template that will be used for the configuration update push. VOIP device only.


Upgrade Method	<p>This option is available only when Upgrade Firmware is selected as the Task Type.</p> <ul style="list-style-type: none"> • Sequential Upgrade: Devices are upgraded one by one in a sequence. Recommended to minimize network traffic. • Concurrent Upgrade: All devices are upgraded simultaneously. This option may cause heavy network traffic. To ensure network quality, the user can also limit the maximum number of concurrent devices, such as upgrading 10 devices at the same time. 
Current Firmware Range	<p>This option is available only when Firmware Upgrade is selected as the Task Type. Devices will be upgraded only if they meet certain requirements:</p> <ul style="list-style-type: none"> • All: Upgrade all devices regardless of their current firmware version. • Specific Firmware Version: Upgrade devices on the specified firmware version. • Firmware Version Range: For the selected devices, only the devices in a specified firmware version range (Lowest firmware version \leq x \leq Highest firmware version) will be upgraded.
Target Device(s)	<ul style="list-style-type: none"> • All devices of this model. • Select Device. • Enter MAC Address.

Table 28: Add Task

Click on the **Save** button to finalize the task creation. Users can view this task in the **Task Management** list.

Task Name	Task Type	Task Time	Creator	Status	Run Time	Operation
Immediate Task	Upgrade Firmware	Immediate	yxxu123	Success	2019/03/25 07:06	i
1111	Reboot Device	2019/03/20 12:00 - 2019/03/21 12:00	yxxu123	Cancelled	—	i
Immediate Task	Update Config: Model	Immediate	yxxu123	Timeout	—	i
Immediate Task	Update Config: CFG	Immediate	yxxu123	Failed	—	i
Immediate Task	Update Config: CFG	Immediate	yxxu123	Failed	—	i
Immediate Task	Upgrade Firmware	Immediate	yxxu123	Success	2019/02/21 03:14	i
222	Reboot Device	Immediate	yxxu123	Success	2019/02/19 02:51	i
222	Upgrade Firmware	2019/02/19 17:00 - 2019/02/20 17:00	yxxu	Success	2019/02/19 17:00	i

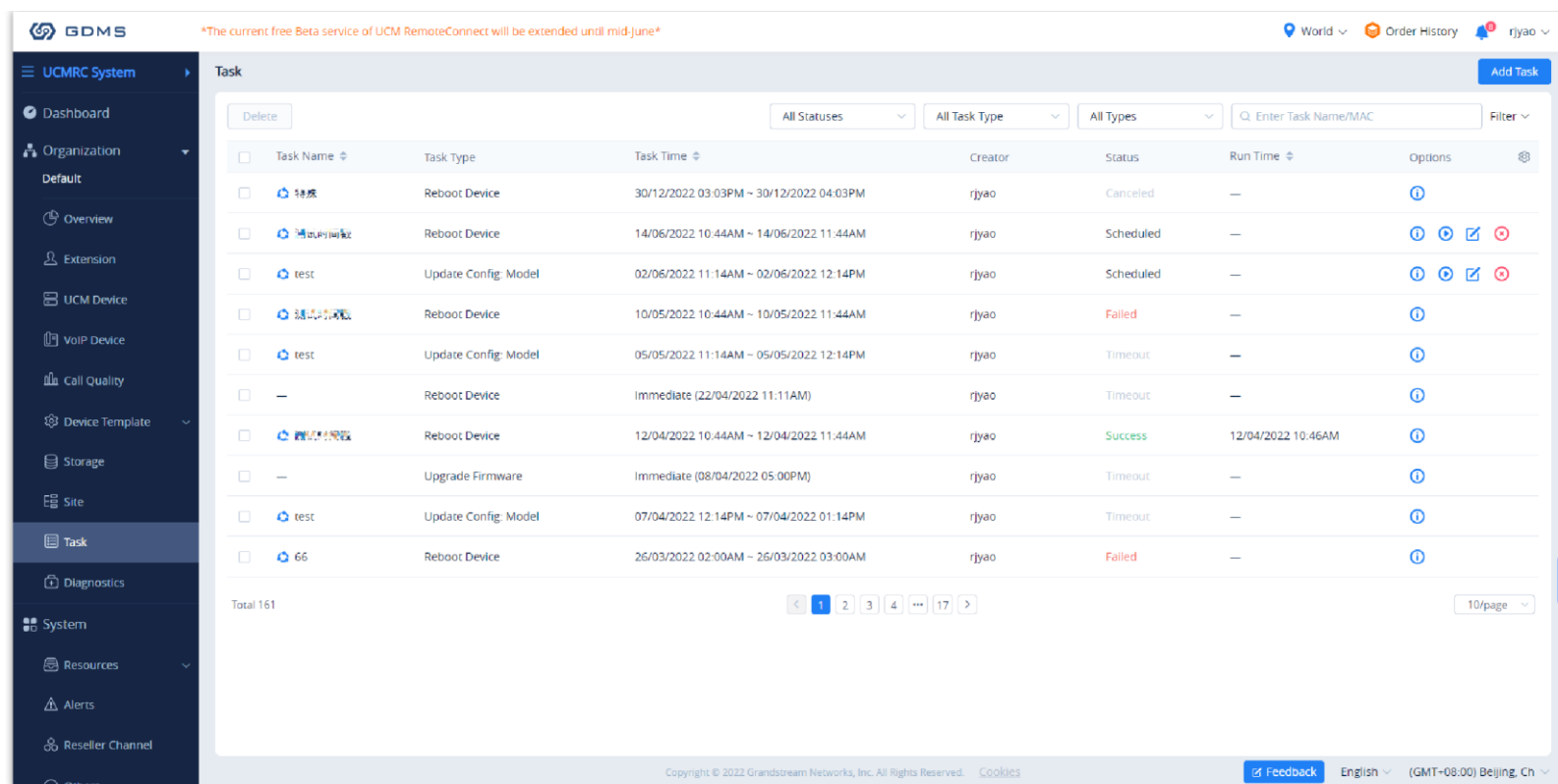
Task Management List



- If there are multiple tasks for 1 device, they will be queued up to run in order of their configured start time.
- If a device is offline, pending tasks associated with the device will be run the next time the device is offline.
- Certain tasks and device setting changes can cause a device to reboot.
- Firmware upgrade tasks may require more time to run due to the size of some firmware files.
- The latest configuration files or firmware will be generated for each cycle of the recurring tasks, and the system will collect all devices of this specific model, then execute the corresponding task.
- If the task is created in a specific sub-system, the user can view the task only in the corresponding sub-system, and other sub-system users cannot view it.

View Task Status

Users can see the status of all completed and pending tasks by looking at the **Status** column.

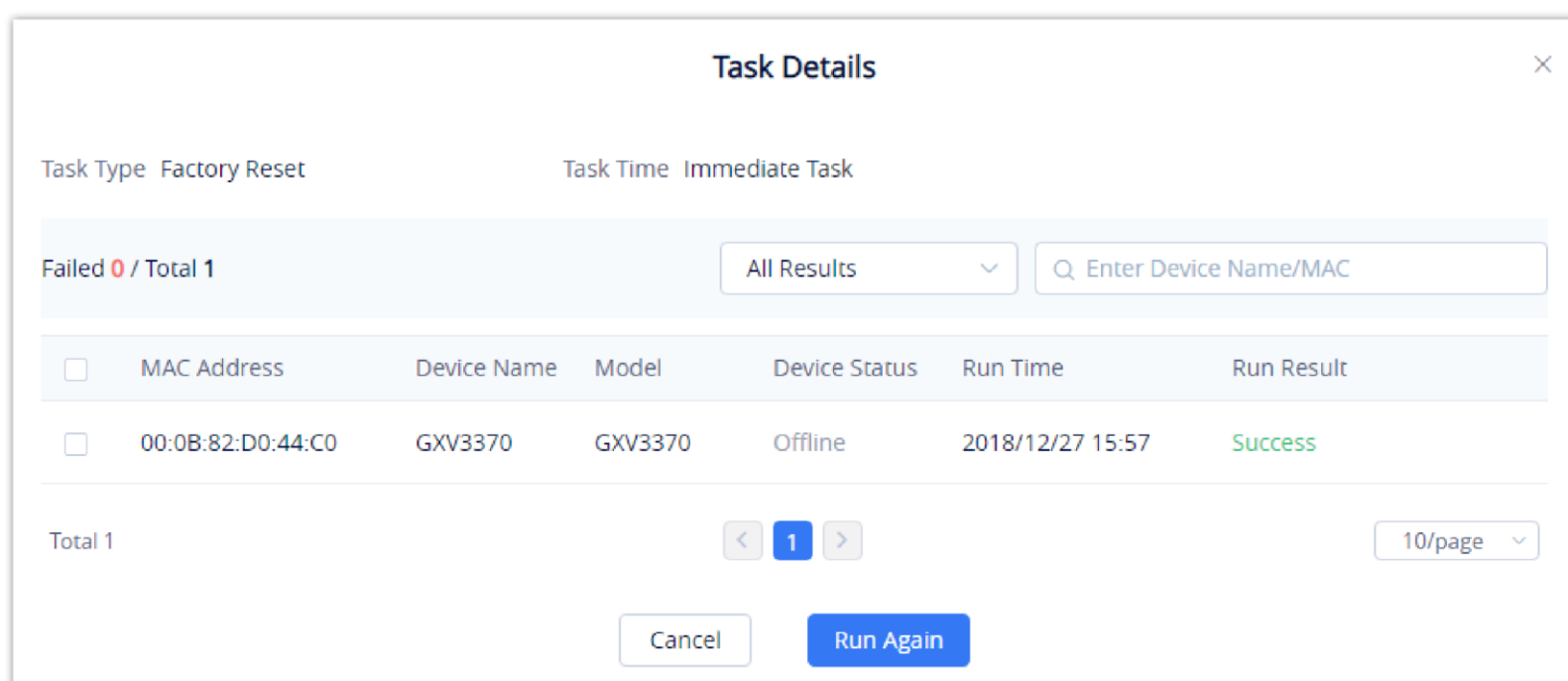


View Task Status

Pending	The task has not been executed yet.
Executing	The task is currently in progress.
Success	The task has been completed successfully.
Failed	The task has failed.
Canceled	The task was canceled.
Timeout	The task was not executed when it arrives at the ending time.
Ended	The task was ended before it could be completed. Some of the involved devices may not have run the task before it ended.

Task Status Description

To view more details about a task, click on the  button for the desired task. Users can view the task status of each device involved.



Task Status


Pending Executed	The task has not been run yet.
-------------------------	--------------------------------

Executing	The task is currently ongoing.
Success	The task has been completed successfully.
Failed	The task has failed. A failure reason will be shown.
Timeout	The task has been sent to the device, but the device has not responded yet.
Success (Timeout)	The task has been completed successfully for this device, but it was completed later than the specified time.
Canceled	The task has been canceled before the starting time.
Ended	The task was ended before it could be completed. Some of the involved devices may not have run the task before it ended.

Table 30: Task Status Detailed Description

Users could re-create tasks for the executed failed devices or all devices. If the user re-creates tasks for certain devices, all attributes of the task and all executed devices information will be logged on the “Re-create Task” page.

Start Scheduled Tasks

Users can start pending scheduled tasks immediately by clicking on the  button.

Cancel Pending Tasks

To cancel a pending task, click on the  button for the desired task. The task status will be changed to Cancelled. To run the task again after it is completed, click on **Task Details** → **Run Again** for the desired task.

If the task is recurring, users could select whether to cancel the entire recurring task or just cancel the single task.

End Task

To stop a running task, click on the  button to immediately end it.

If the device has already executed the task (e.g. Reboot Device), the device will finish the task; if the device does not start to execute the task, the device will not execute the task anymore.

Search Task

Users can search for specific tasks by using the search bar and filters at the top-right of the top right corner of the **Task Management** page.

Task								Add Task
Delete								<input type="text" value="All Status"/> <input type="text" value="All Task Type"/> <input type="text" value="All Types"/> <input type="text" value="Enter Task Name/MAC"/> <input type="button" value="Filter"/>
								<input type="text" value="Start Time"/> - <input type="text" value="End Time"/>
<input type="checkbox"/>	Task Name	Task Type	Task Time	Creator	Status	Run Time	Options	
<input type="checkbox"/>	yxxu	Reboot Device	2019/11/30 20:11 ~ 2019/11/30 22:11	yxxu123	Scheduled	—		
<input type="checkbox"/>	---factory reset---	Factory Reset	2019/10/01 12:19 ~ 2019/10/01 13:19	yxxu123	Scheduled	—		
<input type="checkbox"/>	upgrade cycle1111...	Upgrade Firmware	2019/09/11 13:50 ~ 2019/09/11 14:50	sqhuang	Scheduled	—		
<input type="checkbox"/>	cycle26	Reboot Device	2019/08/29 18:33 ~ 2019/08/29 20:33	yxxu123	Timeout	—		
<input type="checkbox"/>	cycle	Reboot Device	2019/08/29 18:23 ~ 2019/08/29 19:23	yxxu	Success	2019/08/29 18:54		
<input type="checkbox"/>	censi01	Upgrade Firmware	2019/08/29 08:00 ~ 2019/08/31 07:59	yxxu1	Ongoing	2019/08/29 08:00		
<input type="checkbox"/>	TASK	Reboot Device	2019/08/28 19:13 ~ 2019/08/28 21:13	yxxu123	Cancelled	—		
<input type="checkbox"/>	cycle	Reboot Device	2019/08/28 18:23 ~ 2019/08/28 19:23	yxxu	Failed	—		
<input type="checkbox"/>	cycle26	Reboot Device	2019/08/28 14:17 ~ 2019/08/28 16:17	yxxu123	Timeout	—		
<input type="checkbox"/>	2222	Upgrade Firmware	2019/08/28 08:00 ~ 2019/08/31 07:59	yxxu1	Ongoing	—		

Total 1140

1 2 3 4 ... 114

10/page

Search Task

Delete Task

Users can delete tasks at any time. Select one or more tasks and click on the **Delete** button at the top of the page to delete them.

i When deleting ongoing tasks, GDMS will automatically suspend and delete them. Any changes made before the task was suspended cannot be undone.

DEVICE DIAGNOSTICS

Device Diagnostics allows users to check devices on GDMS for issues, view device information, obtain network captures and Syslog, and conduct traceroutes.

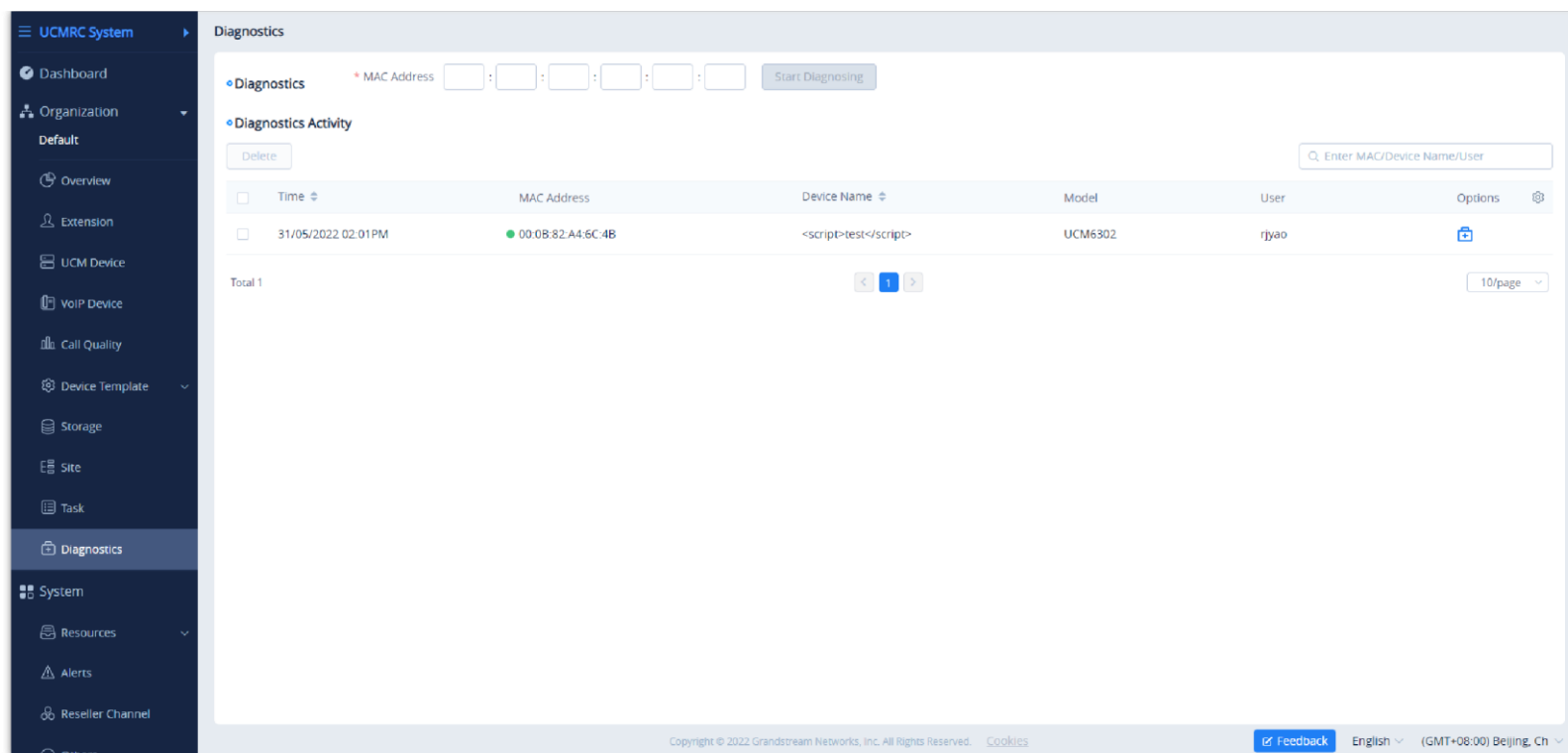
i Support to diagnose VoIP devices and UCM devices.

The user can view the diagnosis status of the device in the current organization of the current system. If the user does not have the relevant permissions, the user cannot diagnose the corresponding device.

Start Diagnostics

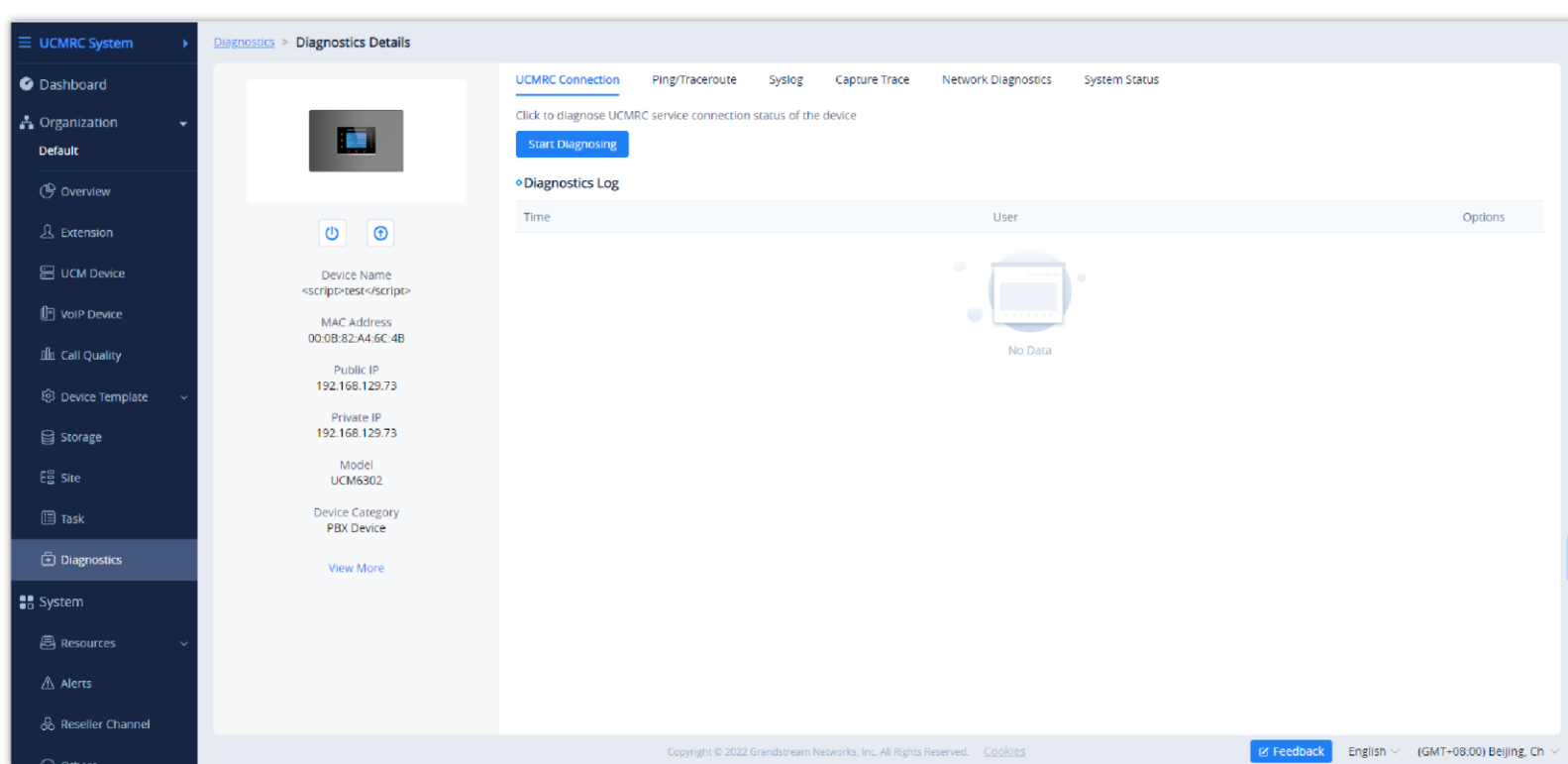
To start diagnosing a device, users can do one of the following:

1. Enter the device's MAC address and click on the **Start Diagnostics** button.
2. Click on the button for the desired device in the list to diagnose the device.



Device Diagnostics

To view the diagnostic details of a device, click on the  button for the desired device.



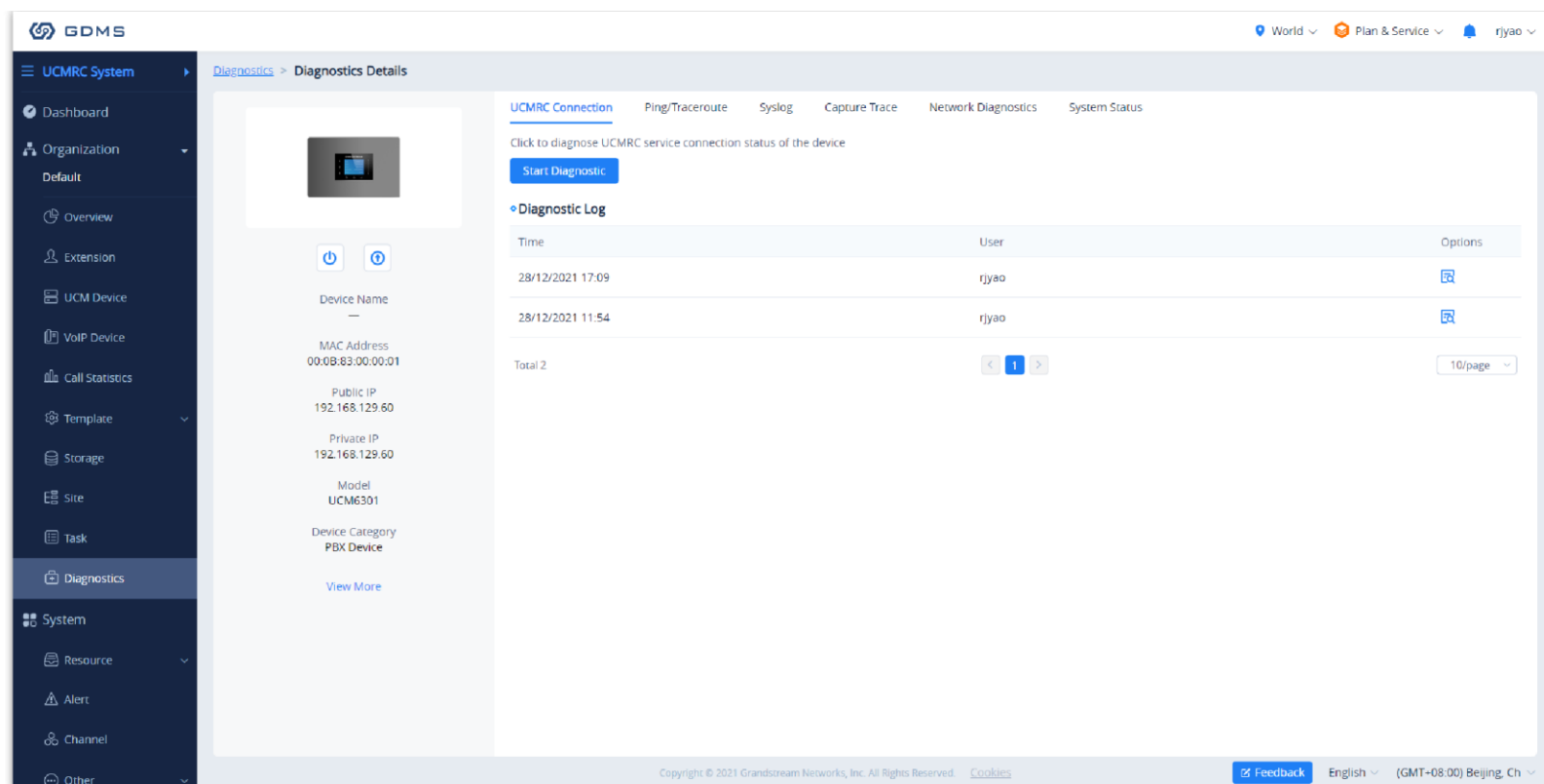
View Diagnostics Details



- If the device is offline, users cannot diagnose this device on the GDMS platform.
- Devices that are currently being diagnosed by a user cannot be diagnosed by other users.

View Device Details

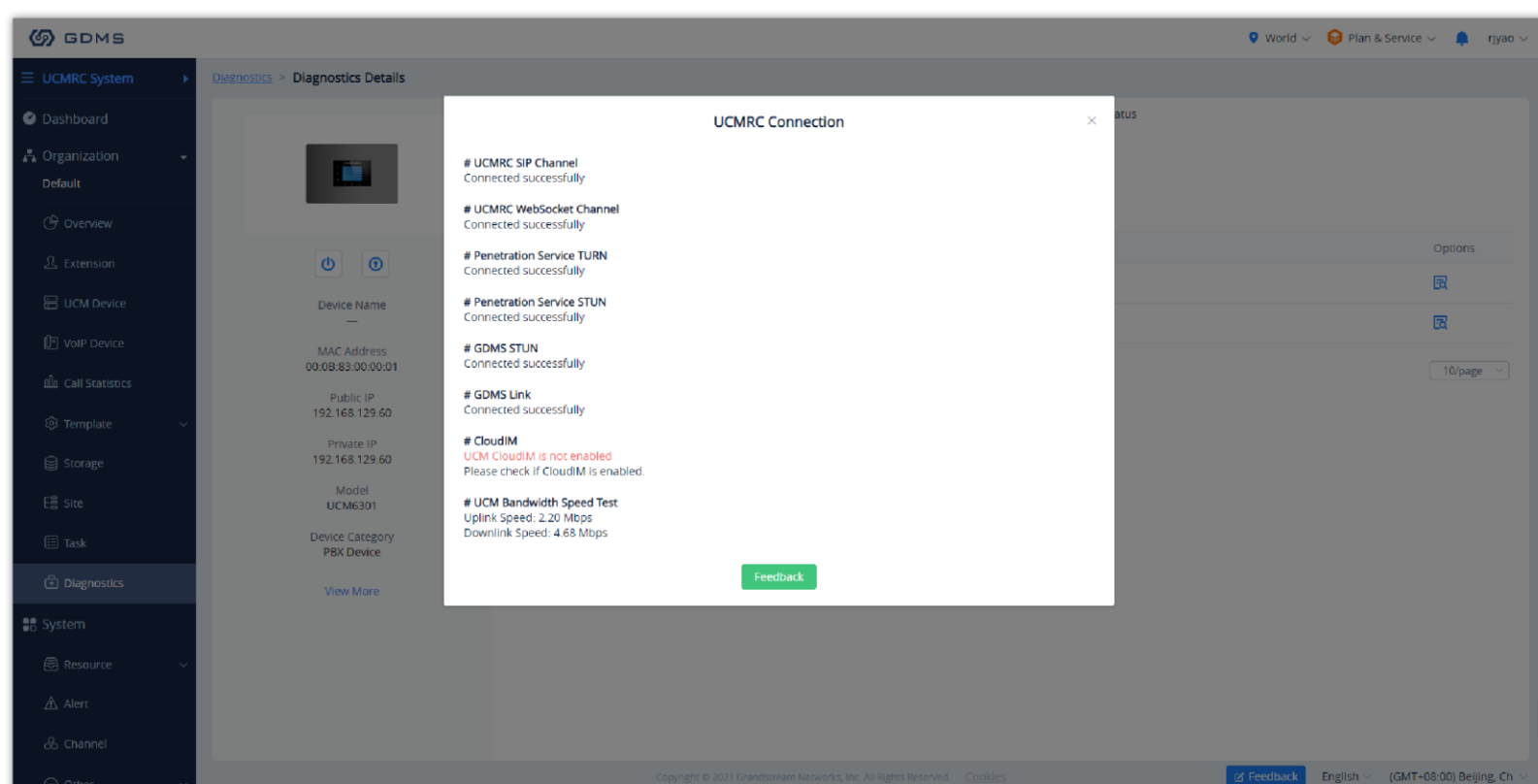
Click on the  button on the right of the **Device Diagnostics** page to view information about the device.



View Device Details

On the Diagnostics Details page, users can quickly perform operations on the devices, including restarting the devices, factory reset the devices, updating the configuration, and upgrading the devices. Users can also view the detailed information of the device, including device name, MAC address, public/private IP address, device model, and device type on this page.

Click on the button  next to the diagnosis record to view the specific diagnosis result of the device.



View Diagnosis Result

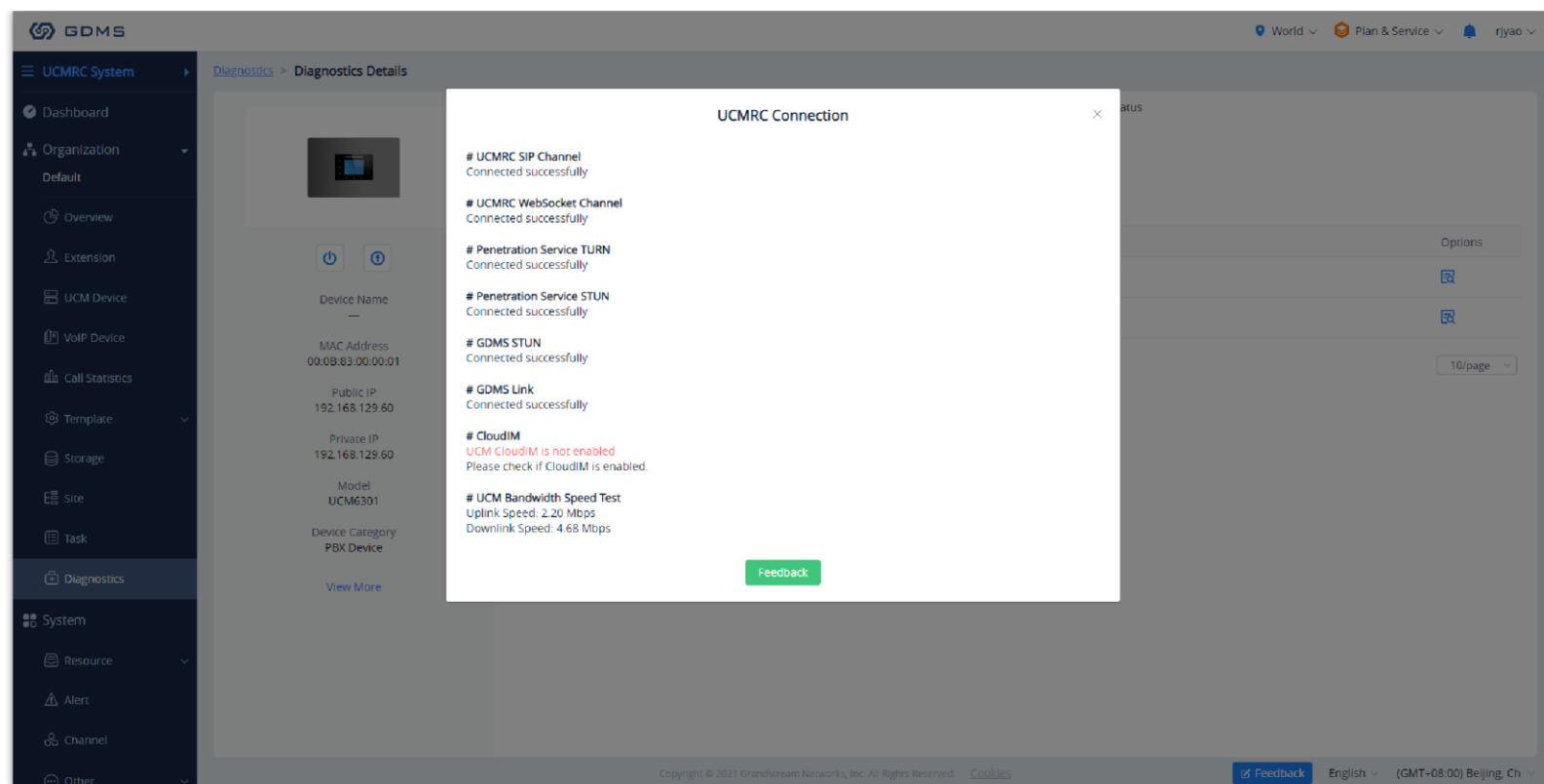
Notes

- The UCM series and GXW45XX devices do not support to reset to factory and updating configuration file through the GDMS platform.
- In the diagnosis record, it only displays the diagnosis data of the device in the last 30 days.
- If the device is offline, the user still can view the diagnosis record of the device.

UCMRC Connection

Users can diagnose the current UCMRC connection status in the GDMS platform.

Click on the button “Start Diagnosis” and wait for the GDMS platform to diagnose the device. The GDMS platform will display the diagnosis result of the UCMRC connection.



UCMRC Connection Diagnosis

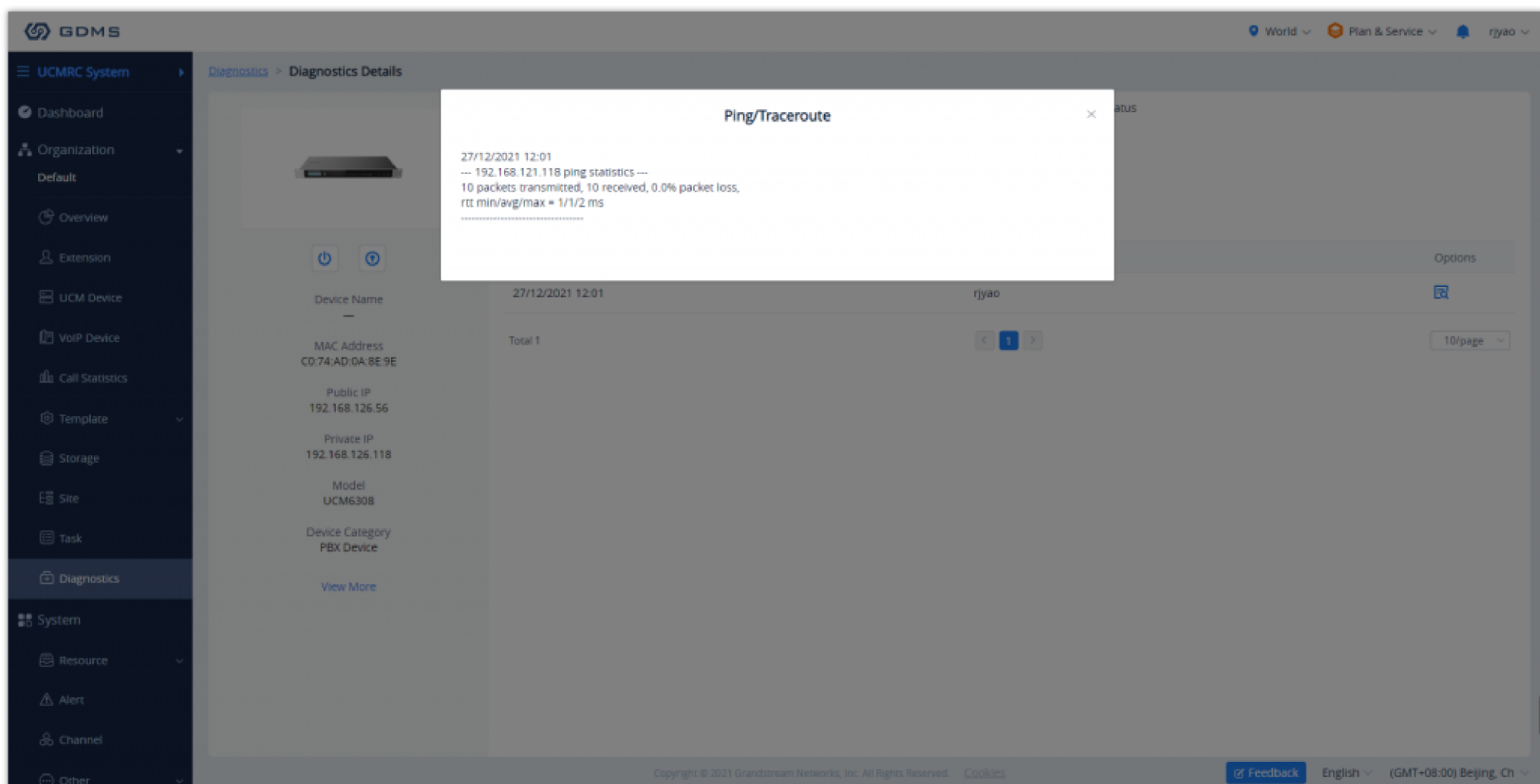
If the UCM device which is using the UCMRC services has any problems, the user can diagnose the UCM device and troubleshoot the problems remotely. The user can try to fix the problems based on the suggestions and click on the “**Feedback**” button to send the logs and descriptions to our technical support.

Note

It only displays the UCMRC connection diagnosis records of the device in the last 30 days.

Ping/Traceroute

Clicking on the **Ping/Traceroute** tab in the Device Diagnostics page will show the following:



Ping/Traceroute

<p>Operation Method</p>	<ul style="list-style-type: none"> ○ Ping: Checks the connection status and speed between the device and the target host. Results include packet loss information, maximum/minimum data packets size, and the round-trip time of the packets. ○ Traceroute: Displays the route and transit delays of packets from the device to the target host. Up to 30 hops can be monitored.
--------------------------------	--

Target Host	Enter the IP address or hostname of the target host.
--------------------	--

Table 31: Ping/Traceroute Options


Users could click on the “Start” button, wait for the GDMS system to diagnose the device, and the GDMS platform will print out the results of the diagnostics.

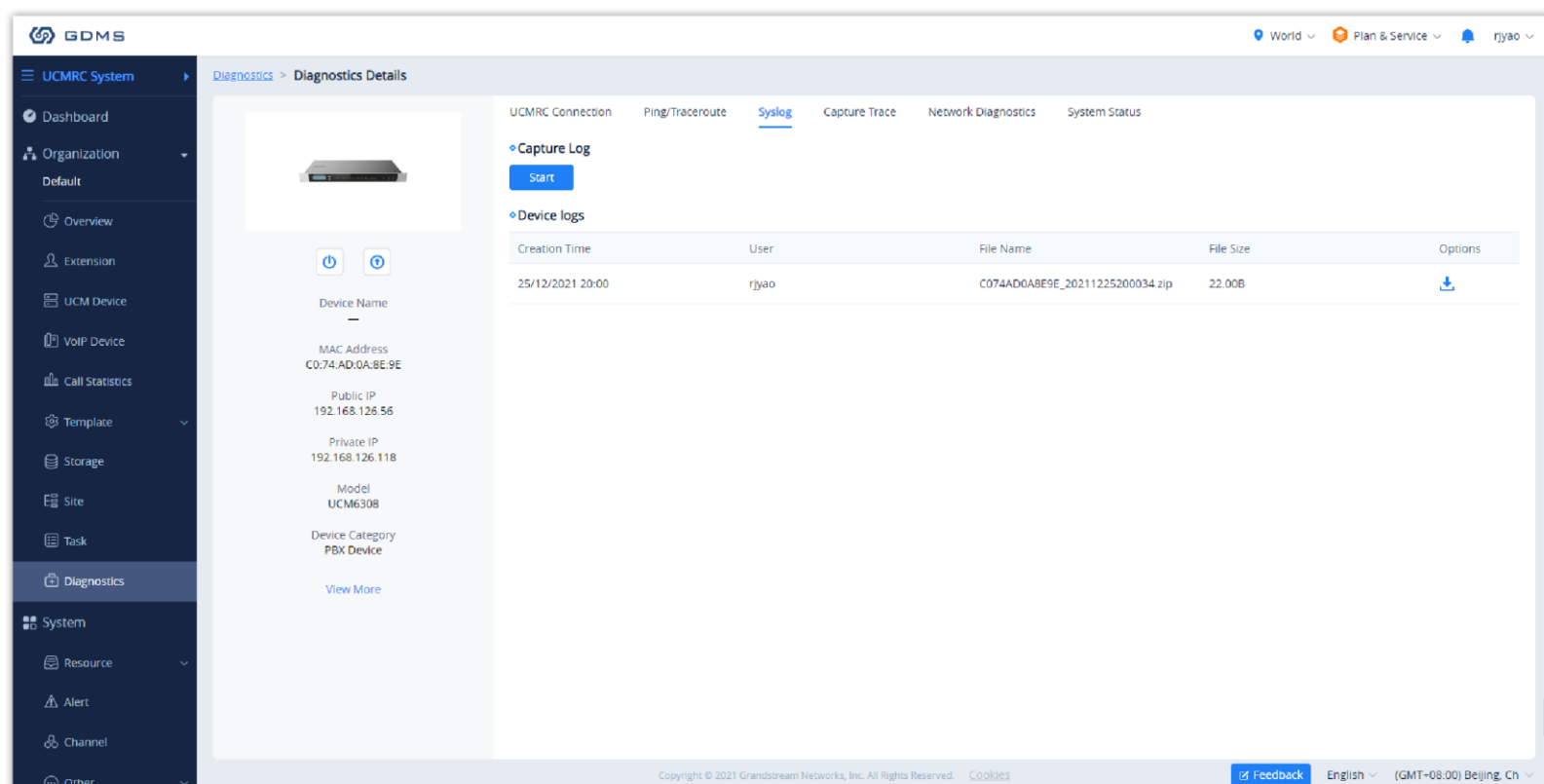
Each operation prints the diagnostics result once, and users could operate the diagnostics multiple times.

i To avoid canceling the ping/traceroute, do not leave the Ping/Traceroute page.

Syslog

The Syslog tool allows users to capture logs from a device.

1. To start a capture, click on the **Start** button on the **Syslog** page. At any time during the capture, users can click on the  button to download the Syslog.
2. Clicking on the **End** button will stop the capture, and the Syslog will be saved to GDMS.
3. Users can access these saved logs at any time.




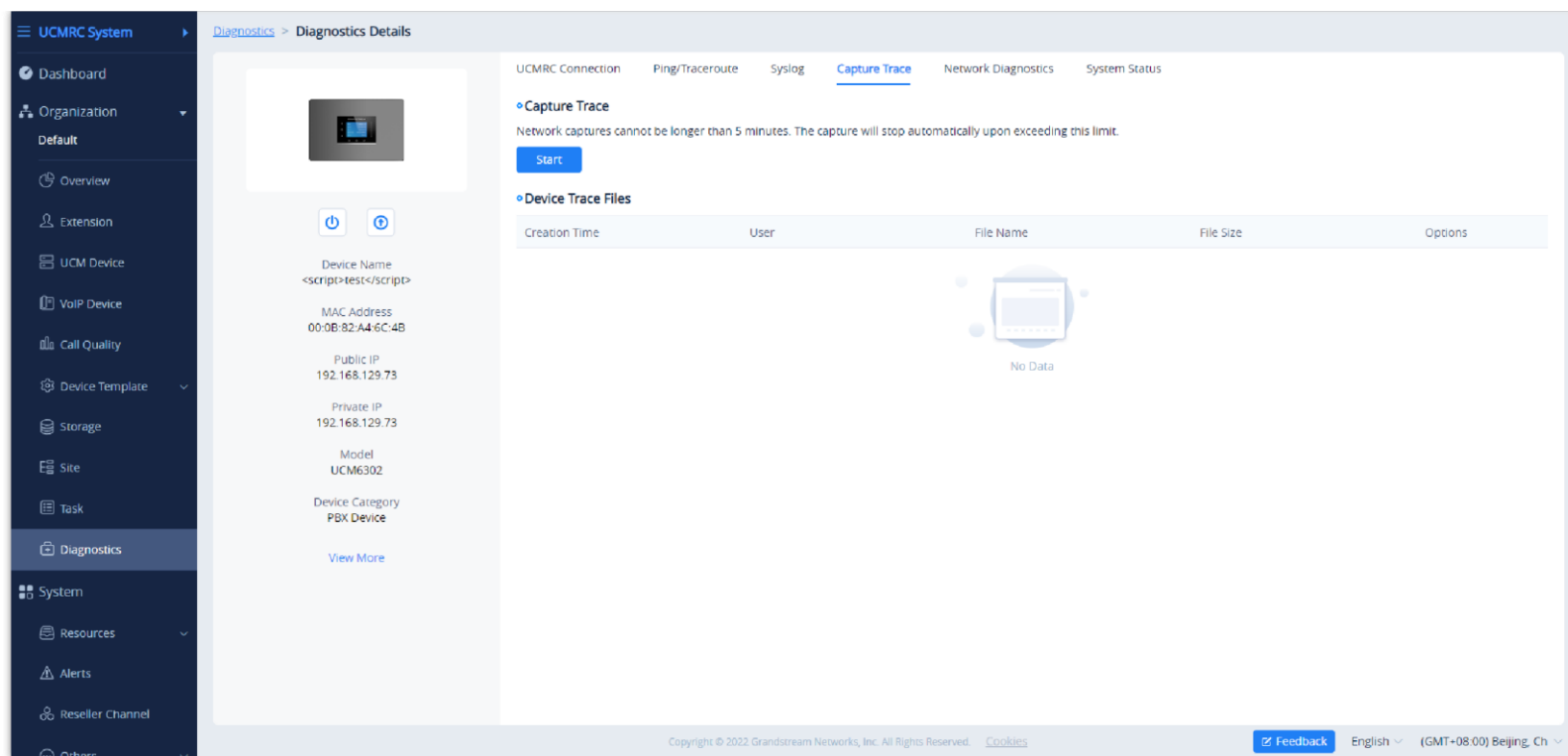
Syslog

- i**
- An ongoing Syslog capture will end automatically after 7 days.
 - For UCM devices, the Syslog download function is temporarily not available.

Capture Trace

The Capture Trace tool allows users to get a network packet capture of a device.

1. Click on the **Start** button to start the packet capture.
2. Click on the **Stop** button to end the packet capture.
3. Click on the  button to download the capture file.



Capture Trace

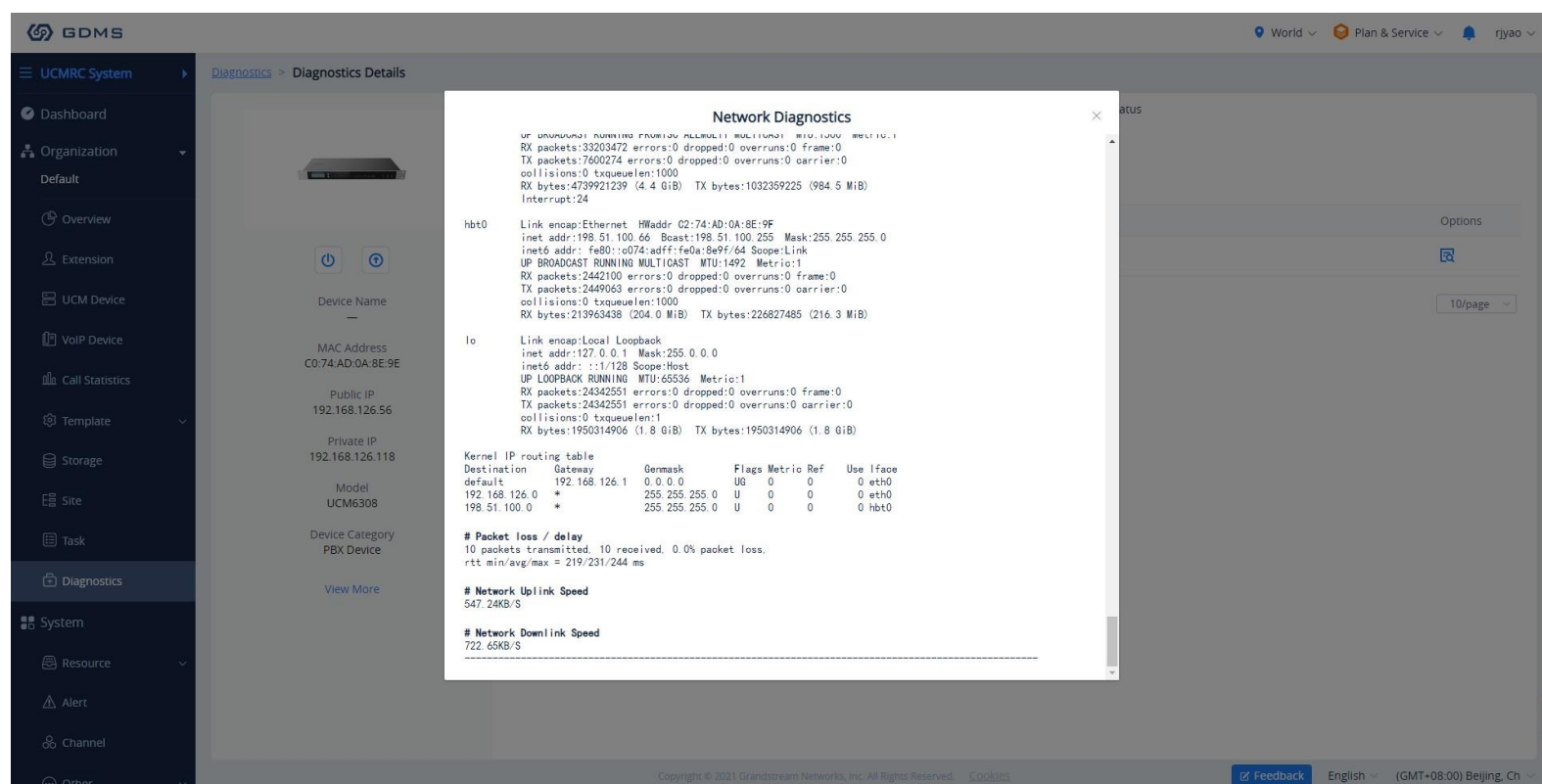


- GDMS can only capture up to 5 minutes. An ongoing capture will end automatically after 5 minutes.
- Some models do not support capturing the trace file remotely.

Network Diagnostics

Users can perform network diagnostics on a specific device, including local network status, network packets loss rate and latency, uplink/downlink network rates, etc.

1. Click the “**Start Diagnostic**” button to start network diagnosis.




Network Diagnostics

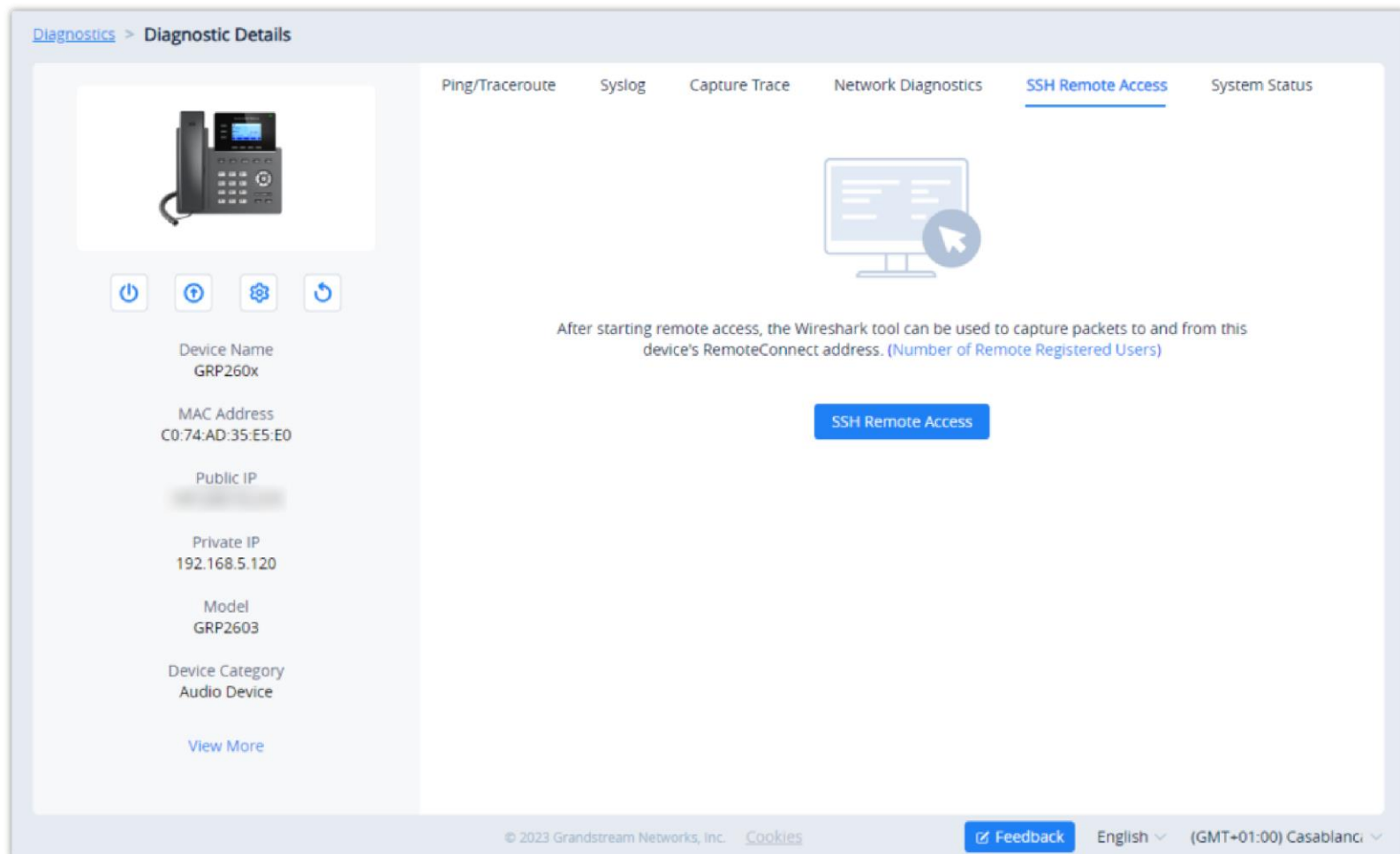
SSH Remote Capture

One of the diagnostic tools that the GDMS provides is the ability to perform a capture trace through SSH remotely.

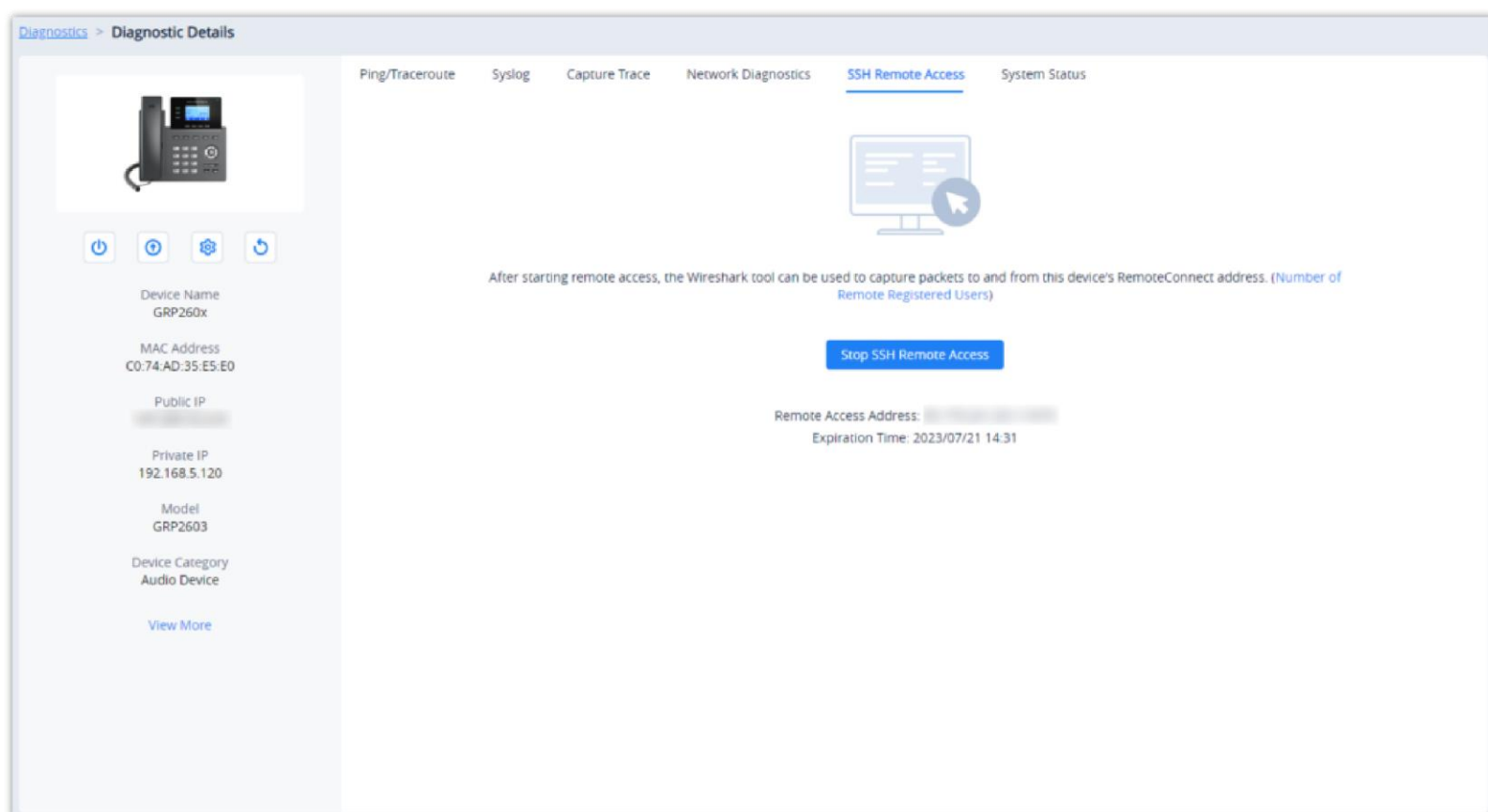
Important Note

Please note that SSH Remote Capture is supported currently on the GRP260X IP phones only.

To access the SSH Remote Capture feature please navigate to **Diagnostics** tab, then click  on the corresponding device on which you would like to enable SSH Remote Capture. Then select “SSH Remote Access” tab.



Enable SSH Remote Capture



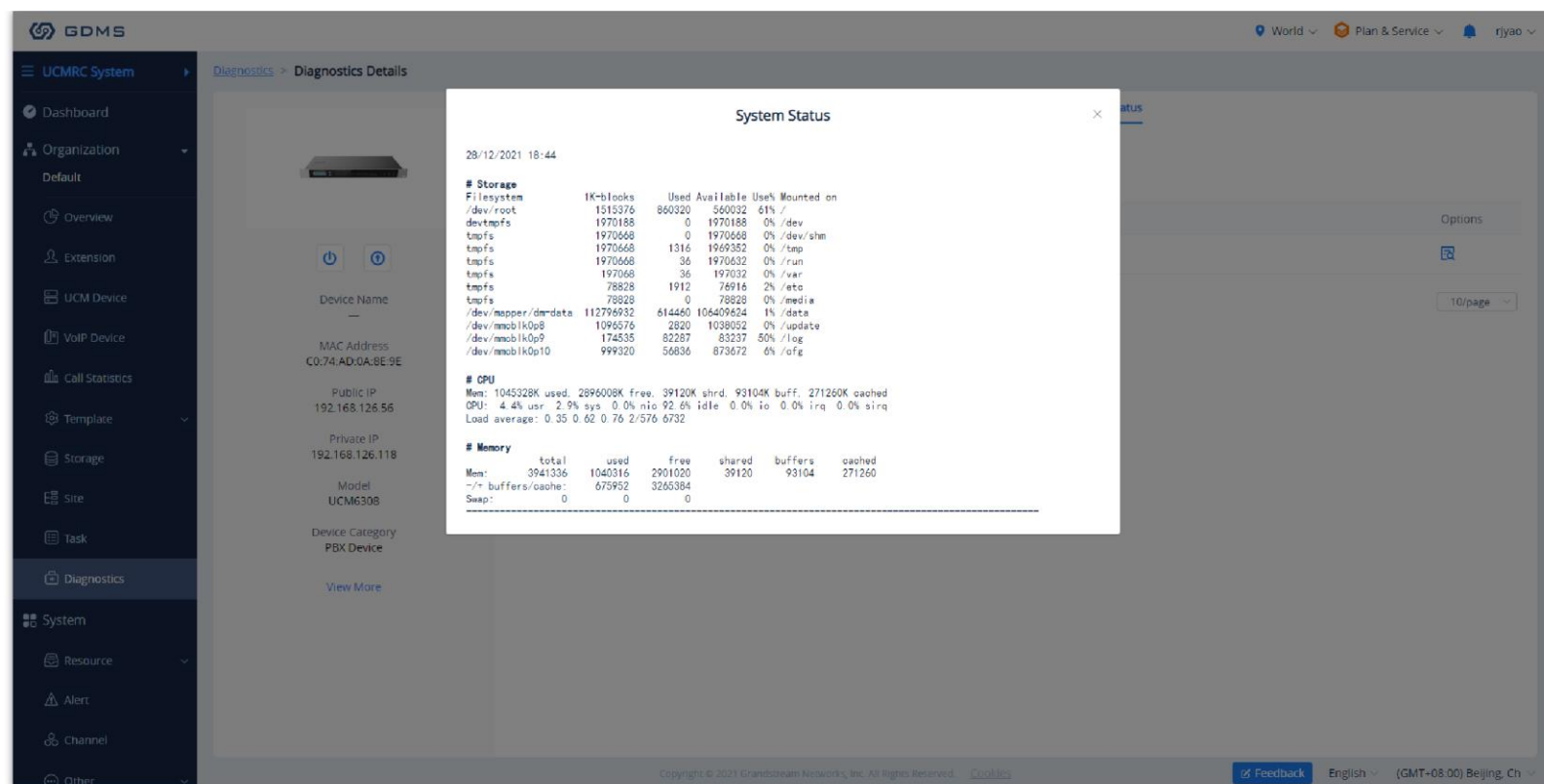
SSH Remote Capture Enabled

After enabling Remote SSH Capture, a Remote Access Address will be displayed, the user can use the Remote Access Address to capture the ethernet packets using a packet analyzer like Wireshark. For more information, refer to the following chapter: <https://documentation.grandstream.com/knowledge-base/grp260x-series-administration-guide/#remote-ssh-capture>

System Status

Users can view the system status of a specific device through the GDMS platform to diagnose the device problems, including storage space, CPU, memory information, etc.

1. Click the “**Start to Get**” button to get the system status from the device in real-time.



System Status

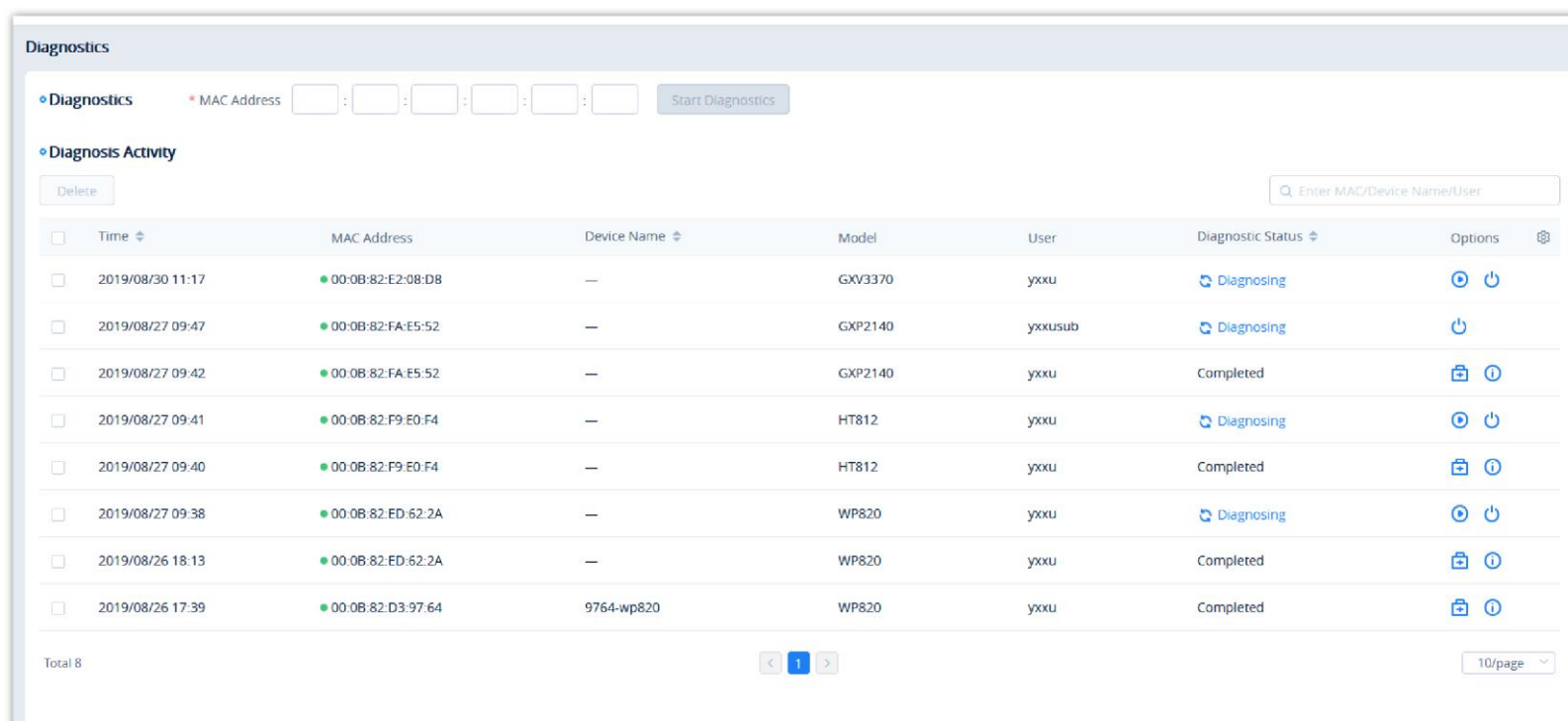
End Diagnostics

Click on the **End Capture** button on the **Device Diagnostics** page to end diagnostics for the device. All diagnostic processes will stop.

- Since GDMS does not allow multiple users to diagnose the same device simultaneously, please make sure that a diagnosis is properly ended by clicking on the End Diagnostics button.

Diagnostics Records

Users can view the entire diagnostic history of all devices associated with the current account.



Diagnostics Records

- If a device is currently being diagnosed, click on the [Refresh] button to continue diagnosing or the [End] button to end it.
- If a device has been diagnosed already, click on the [Refresh] button to start another round of diagnosis or the [View] button to view the results.
- View the diagnostic history of a specific device by using the search bar on the top right of the **Diagnostic Records** page.
- Users can delete records by selecting one or more items and clicking on the **Delete** button.

ALERT MANAGEMENT

GDMS has an alert system that will trigger when certain conditions are fulfilled. There are 3 alert levels: High, Medium, and Low.

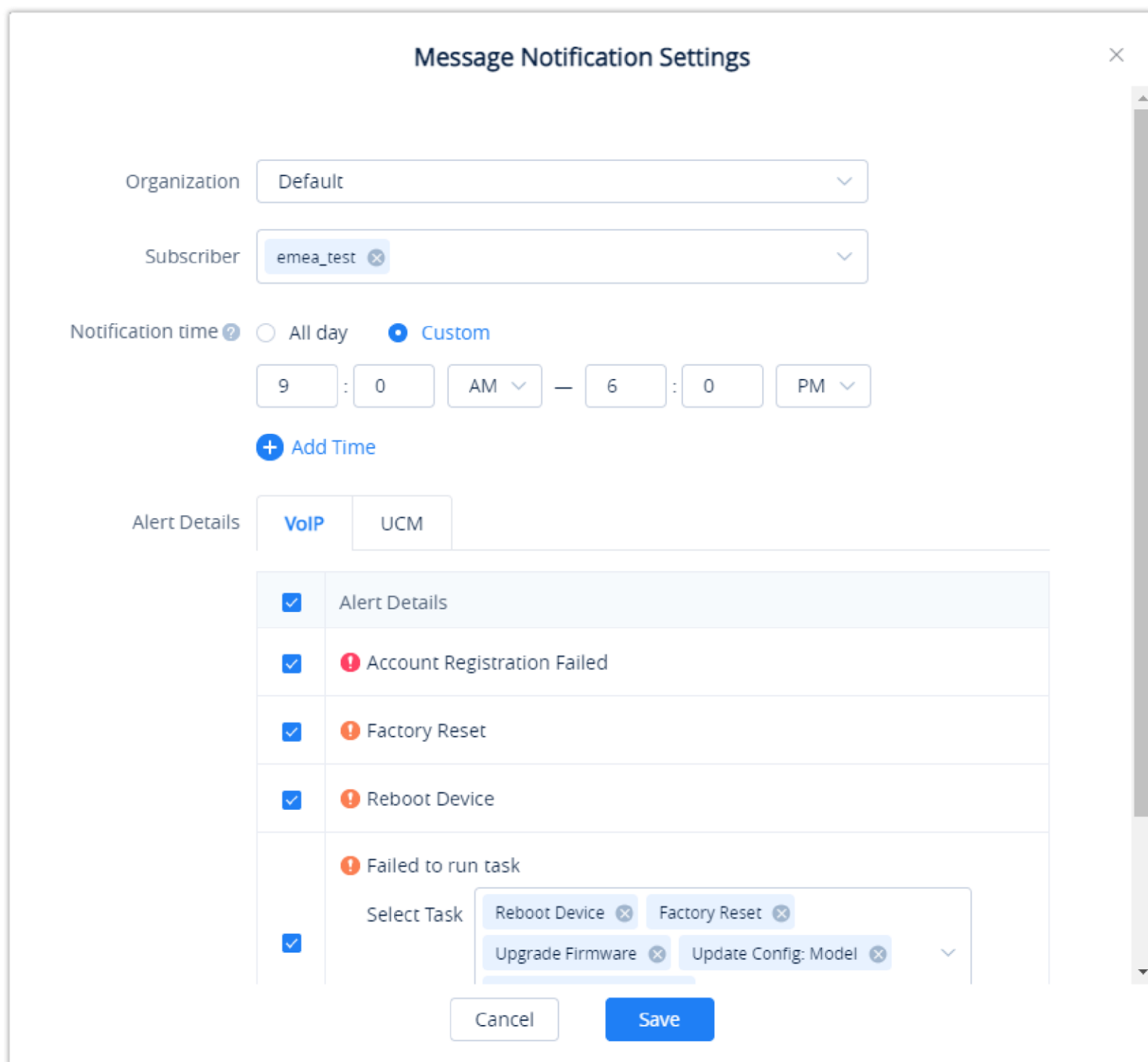
Alert Notification Settings

Users can view and receive alert notifications in two ways: **Message Notification** and **Email Notification**.

Message Notification Settings

This displays the alert as a notification under the  icon in the top right corner of the GDMS page.

1. To manage message alert notifications, click on the **Message Notification Settings** button  on the top-right corner of the **Alert Management** page.




Message Notification Settings

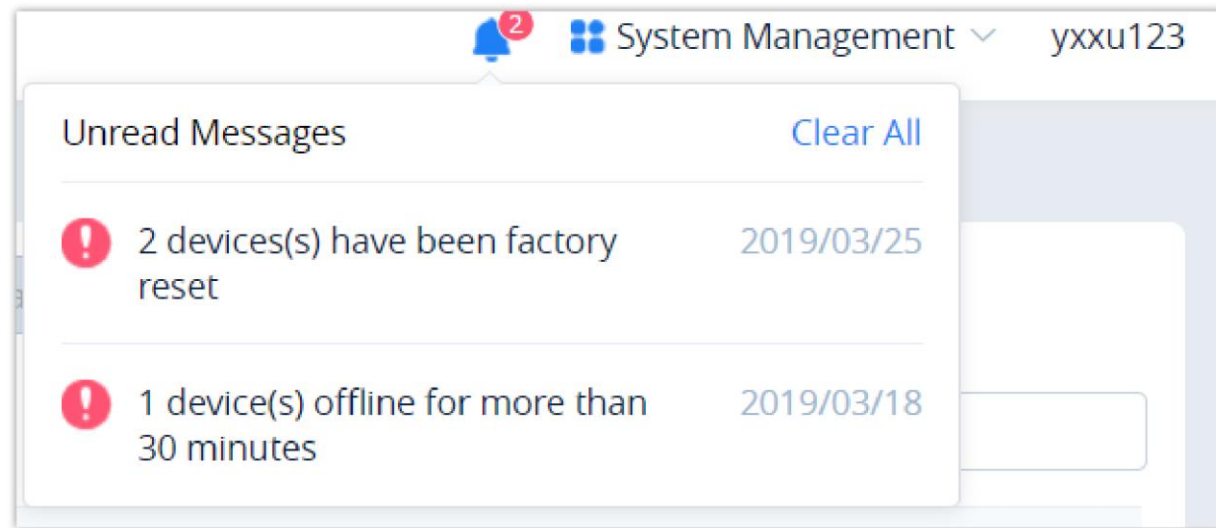
Organization	Select the organization in question.
Alert Details (VoIP UCM)	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.

VoIP	
Alert Details	<p>High Level:</p> <ul style="list-style-type: none"> • Account Registration Failed <p>Medium Level:</p> <ul style="list-style-type: none"> • Factory Reset • Reboot Device • Failed to Run Task • Device Offline
UCM	
Alert Details	<p>Users can specify what alerts to receive. The following alert priority levels are available:</p> <p>High Level:</p> <ul style="list-style-type: none"> • Device is back online • Device Offline • UCM cloud storage space is insufficient or full • CPU Traffic Control • Local Disk Usage • Memory Usage • Abnormal System Reboot • System Crash • Fail2ban Blocking • SIP Peer Trunk Status • Network Disk Status • Remote Concurrent Calls Amount Exceeds Upper Limit • External Disk Usage • TLS Certificate Expired • Remote Login • Network Port Traffic Alert • High-frequency Outbound Call • Flood Attack • Outbound Trunk Call Duration Usage • Outgoing Call Duration Limit Has been Reached <p>Medium Level:</p> <ul style="list-style-type: none"> • Failed to Run Task • Modify Super Admin Password • System Upgrade • User Login Banned <p>Note: Only the UCM devices that have UCM RemoteConnect advanced plans can report the alert contents and send the alert notifications.</p>
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected.

Table 32: Message Notification Settings

i If a scheduled task fails to run, the alert notification will be sent only to the task creator.

2. When there are unread alerts, and a user subscribed to alerts logs in, the  icon will shake. Hovering over the icon will show the unread messages. Clicking on these messages will show more details about the alerts.

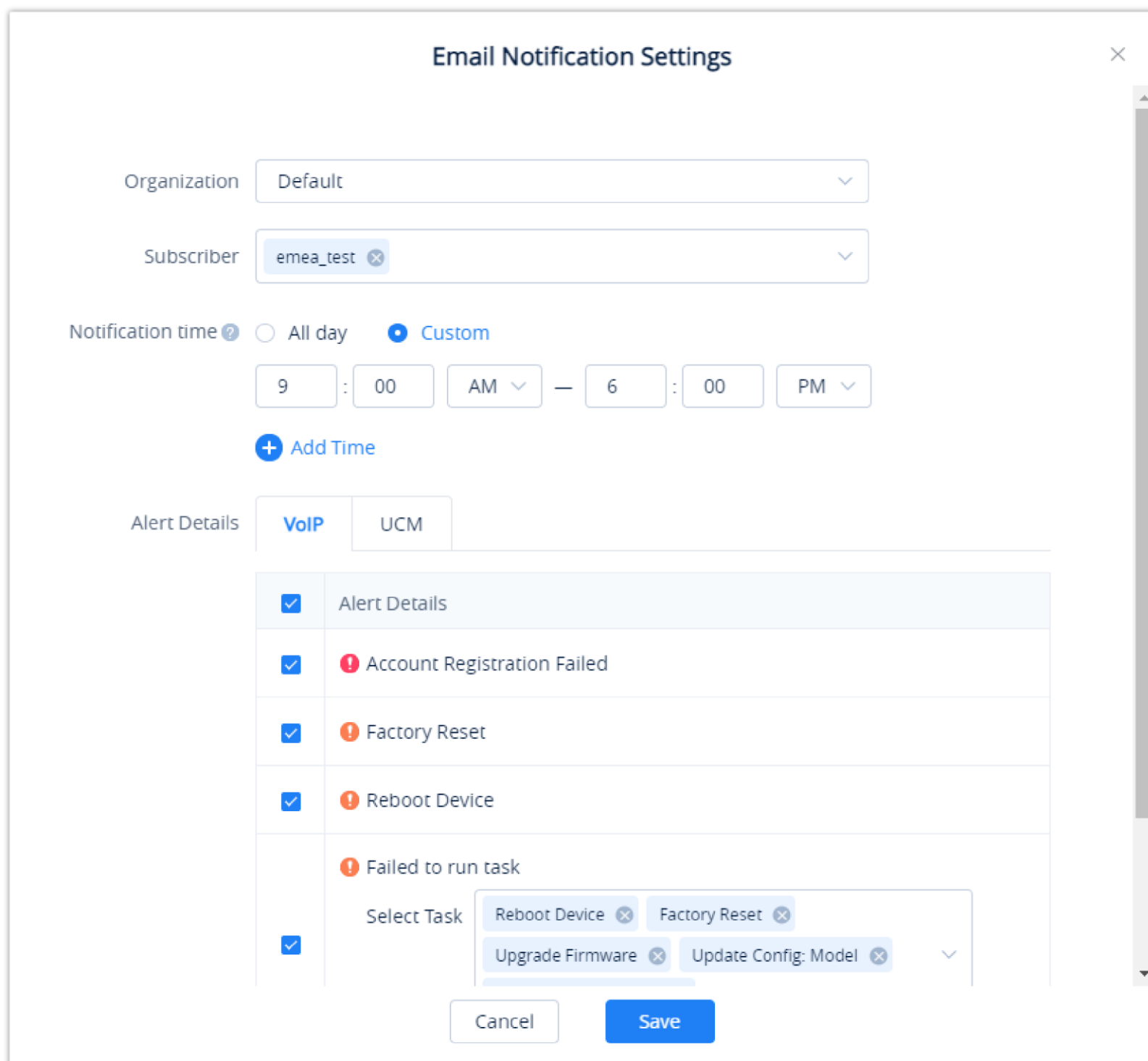


Unread Message Icon

Email Notification Settings

Alerts will be sent as emails to subscribers.

1. To manage email alert notifications, click on the  button on the top-right corner of the **Alert Management** page.



Email Notification Settings

Organization

Select the organization in question.

Alert Details (VoIP UCM)	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
VoIP	
Alert Details	<p>High Level:</p> <ul style="list-style-type: none"> ● Account Registration Failed <p>Medium Level:</p> <ul style="list-style-type: none"> ● Factory Reset ● Reboot Device ● Failed to Run Task ● Device Offline
UCM	
Alert Details	<p>Users can specify what alerts to receive. The following alert priority levels are available:</p> <p>High Level:</p> <ul style="list-style-type: none"> ● Device is back online ● Device Offline ● UCM cloud storage space is insufficient or full ● CPU Traffic Control ● Local Disk Usage ● Memory Usage ● Abnormal System Reboot ● System Crash ● Fail2ban Blocking ● SIP Peer Trunk Status ● Network Disk Status ● Remote Concurrent Calls Amount Exceeds Upper Limit ● External Disk Usage ● TLS Certificate Expired ● Remote Login ● Network Port Traffic Alert ● High-frequency Outbound Call ● Flood Attack ● Outbound Trunk Call Duration Usage ● Outgoing Call Duration Limit Has been Reached <p>Medium Level:</p> <ul style="list-style-type: none"> ● Failed to Run Task ● Modify Super Admin Password ● System Upgrade

	<ul style="list-style-type: none"> • User Login Banned <p>Note: Only the UCM devices that have UCM RemoteConnect advanced plans can report the alert contents and send the alert notifications.</p>
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected.

Table 33: Email Notification Settings

i If a scheduled task fails to run, the alert notification will be sent only to the task creator.

2. When the subscriber receives the alarm notification, the GDMS platform will send an email to inform the subscriber. To avoid the alarm notification emails disturbing the subscriber, the GDMS platform only can send one alarm notification email to the subscriber's email box per hour.

GDMS

Hi, Williamxu

GDMS currently has **2** unread alert(s). Please check your notifications. [Click here for details:](#)

Alert Details	Alert Type	Level	Date
Device GXV3370_Test (00:0B:82:E9:A1:08) registration failed	Device Registration Failed	High	2019/03/25 00:29
Device GXV3370_Test (00:0B:82:E9:A1:08) Factory Reset	Factory Reset	Medium	2019/03/25 00:28

This is an automatically generated email. Please do not reply.

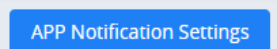
[About Us](#) | [Contact Us](#)

Copyright © 2019 Grandstream Networks, Inc. All rights reserved.

Email Alert Notification

App Notification Settings

The alerts can be pushed to the subscribers through the App notifications.

1. The user can click the button  to access the App notification settings interface.

×

App Notification Settings

Organization Default

Subscriber emea_test

Notification time ? All day Custom

9 : 00 AM — 6 : 00 PM

+ Add Time

Alert Details VoIP UCM

<input checked="" type="checkbox"/>	Alert Details
<input checked="" type="checkbox"/>	! Account Registration Failed
<input checked="" type="checkbox"/>	! Factory Reset
<input checked="" type="checkbox"/>	! Reboot Device
<input checked="" type="checkbox"/>	! Failed to run task Select Task Reboot Device Factory Reset Upgrade Firmware Update Config: Model

Cancel
Save

App Notification Settings

Organization	Select the organization in question.
Alert Details (VoIP UCM)	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
VoIP	
Alert Details	<p>High Level:</p> <ul style="list-style-type: none"> ● Account Registration Failed <p>Medium Level:</p> <ul style="list-style-type: none"> ● Factory Reset ● Reboot Device ● Failed to Run Task ● Device Offline
UCM	
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available:

High Level:

- Device is back online
- Device Offline
- UCM cloud storage space is insufficient or full
- CPU Traffic Control
- Local Disk Usage
- Memory Usage
- Abnormal System Reboot
- System Crash
- Fail2ban Blocking
- SIP Peer Trunk Status
- Network Disk Status
- Remote Concurrent Calls Amount Exceeds Upper Limit
- External Disk Usage
- TLS Certificate Expired
- Remote Login
- Network Port Traffic Alert
- High-frequency Outbound Call
- Flood Attack
- Outbound Trunk Call Duration Usage
- Outgoing Call Duration Limit Has been Reached

Medium Level:

- Failed to Run Task
- Modify Super Admin Password
- System Upgrade
- User Login Banned

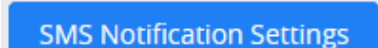
Note: Only the UCM devices that have UCM RemoteConnect advanced plans can report the alert contents and send the alert notifications.

Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected.
-------------------	--

App Notification Settings

SMS Notification Settings

UCM devices that have UCM RemoteConnect service plan can use the SMS Notification function. This function is only supported by some of the UCM RemoteConnect plans.

1. To manage email alert notifications, click on the  button on the top-right corner of the **Alert Management** page.

SMS Notification Settings ✕

📌 UCM devices with advanced plan support SMS notification function, only available in Mexico, USA, Canada.

Organization

Notification time ? All day Custom

: — :

+ Add Time

Alert Details	
<input type="checkbox"/>	Alert Details
<input type="checkbox"/>	🚨 Device is back to online
<input type="checkbox"/>	🚨 Device Offline
<input type="checkbox"/>	🚨 Local Disk Usage ?
<input type="checkbox"/>	🚨 Abnormal System Reboot
<input type="checkbox"/>	🚨 Network Disk Status ?
<input type="checkbox"/>	🚨 Remote concurrent calls amount exceeds upper limit
<input type="checkbox"/>	🚨 External Disk Status ?
<input type="checkbox"/>	🚨 ...

SMS Notification Settings

Organization	Select the organization in question.
Alert Details (VoIP UCM)	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
VoIP	
Alert Details	<p>High Level:</p> <ul style="list-style-type: none"> • Account Registration Failed <p>Medium Level:</p> <ul style="list-style-type: none"> • Factory Reset • Reboot Device • Failed to Run Task • Device Offline
UCM	
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available:

	<p>High Level:</p> <ul style="list-style-type: none"> ● Device is back online ● Device Offline ● UCM cloud storage space is insufficient or full ● CPU Traffic Control ● Local Disk Usage ● Memory Usage ● Abnormal System Reboot ● System Crash ● Fail2ban Blocking ● SIP Peer Trunk Status ● Network Disk Status ● Remote Concurrent Calls Amount Exceeds Upper Limit ● External Disk Usage ● TLS Certificate Expired ● Remote Login ● Network Port Traffic Alert ● High-frequency Outbound Call ● Flood Attack ● Outbound Trunk Call Duration Usage ● Outgoing Call Duration Limit Has been Reached <p>Medium Level:</p> <ul style="list-style-type: none"> ● Failed to Run Task ● Modify Super Admin Password ● System Upgrade ● User Login Banned <p>Note: Only the UCM devices that have UCM RemoteConnect advanced plans can report the alert contents and send the alert notifications.</p>
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected.

Notification Settings

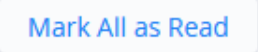

2. Click the **Save** button to apply the changes.

View Alert Notification

The **Alert Management** page shows all alerts that have been generated by GDMS.


 Users can be limited by their privileges on the alerts they can view on the Alert Management page. Please refer to the User Management section for more details.

View Alert Notification

- **Search:** Users can find specific alerts by using the filter and search features in the top right corner of the **Alert Management** page.
- **Latest alarm notification:** If the alarm notification includes a red dot at the beginning of the item, it means the alarm notification is an unread notification. Users could click on the button  to mark all unread notifications as “Read.”
- **View Details:** Users could click on the button  following the alert notification to view the alert notification details, and the red dot will disappear if the user has viewed the alert notification details.

Note: When you click on , the following information will appear.

Device Alert Details

- **Device Diagnostics:** For the device which has a fault, the user could click on the option  to access the **Device Diagnostics** page to diagnose the device.
- **Delete Alerts:** Users can delete notifications by selecting one or more items and clicking on the **Delete** button.
- To display the device that has generated the event, the user can click on the hyperlinked MAC address to view more information about the device.

RESOURCE MANAGEMENT

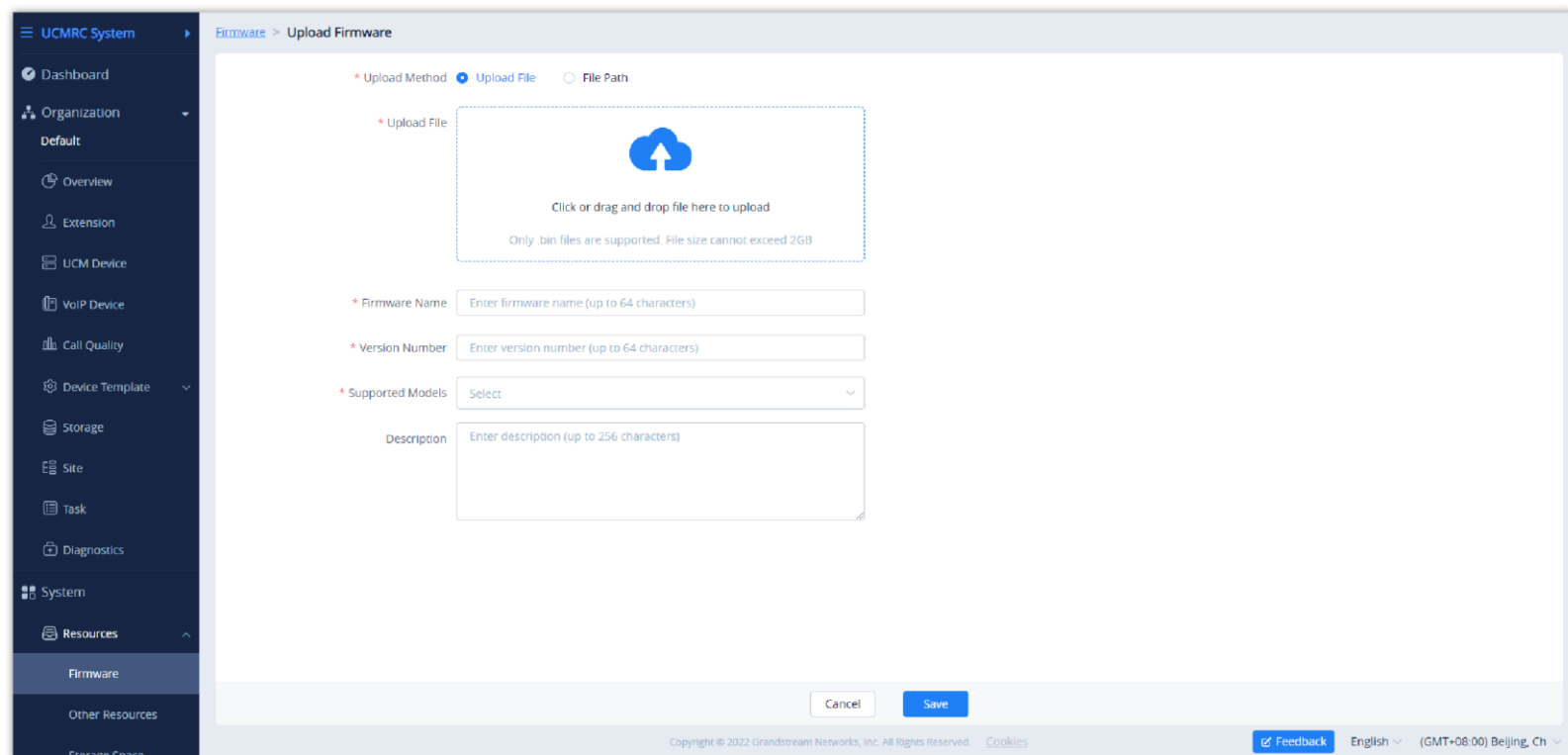
Firmware Management

Custom Firmware

Users could upload the firmware of the devices to upgrade the associated devices on the GDMS platform.

✔ It is recommended to download the device's firmware from Grandstream Official website to avoid devices failure.

1. On the Custom Firmware page, click on the Upload Firmware button.
2. Either drag and drop the firmware file to the upload area or enter the firmware file path.

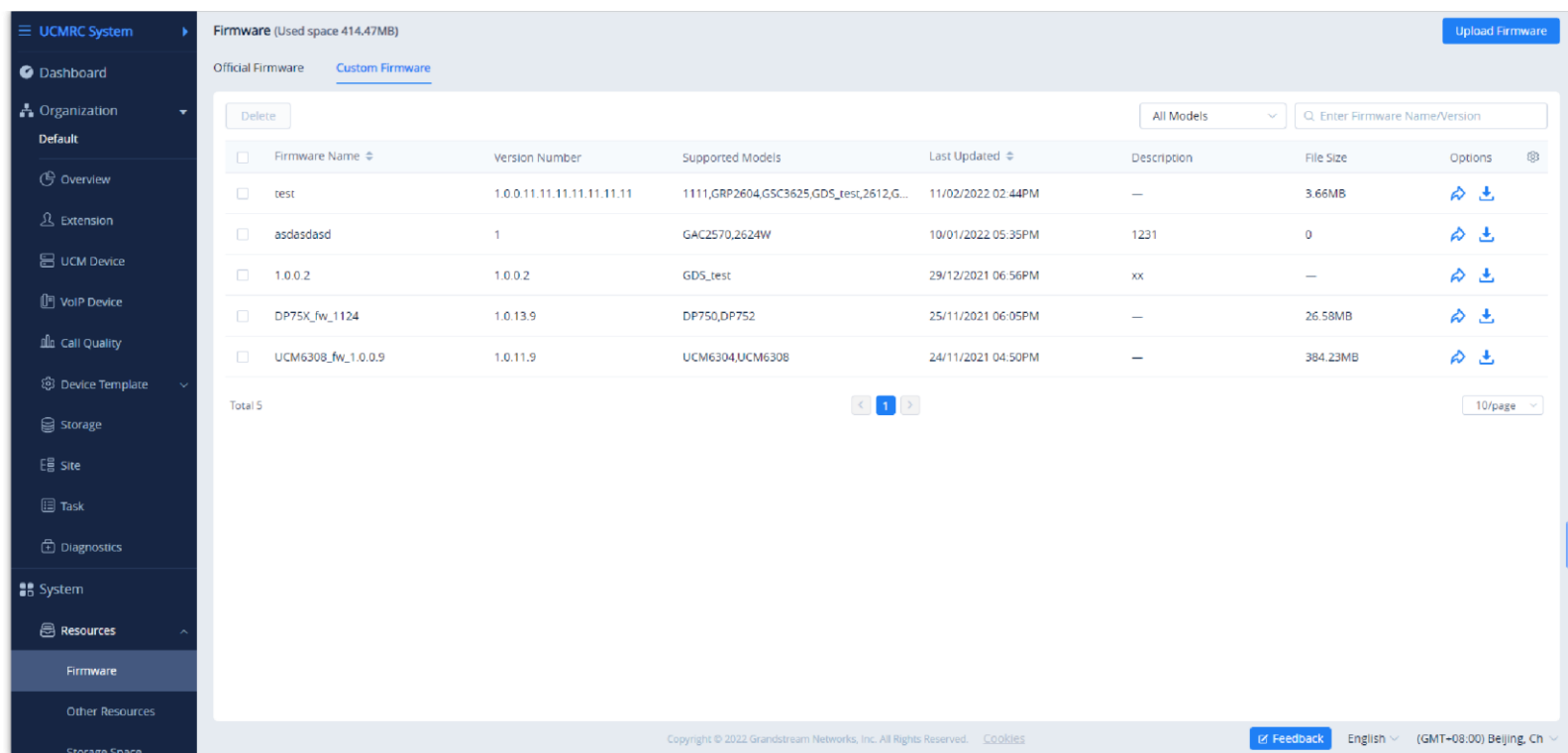


Custom Firmware

Upgrade Path	<ul style="list-style-type: none">◦ Upload File: Upload the firmware file directly. Users could drag the firmware file to the uploading area or click on the uploading area to select the uploading firmware.◦ Enter File Path: File path of the firmware. Please make sure that this file path can be accessed by your devices.
Firmware Name	This is used to identify the firmware file name. The limit is 1 – 64 characters.
Version Number	Fill in the actual version number of the uploaded firmware.
Supported Model	Select the supported device models of the firmware.
Description	Description of the firmware. The maximum character limit is 256.

Custom Firmware

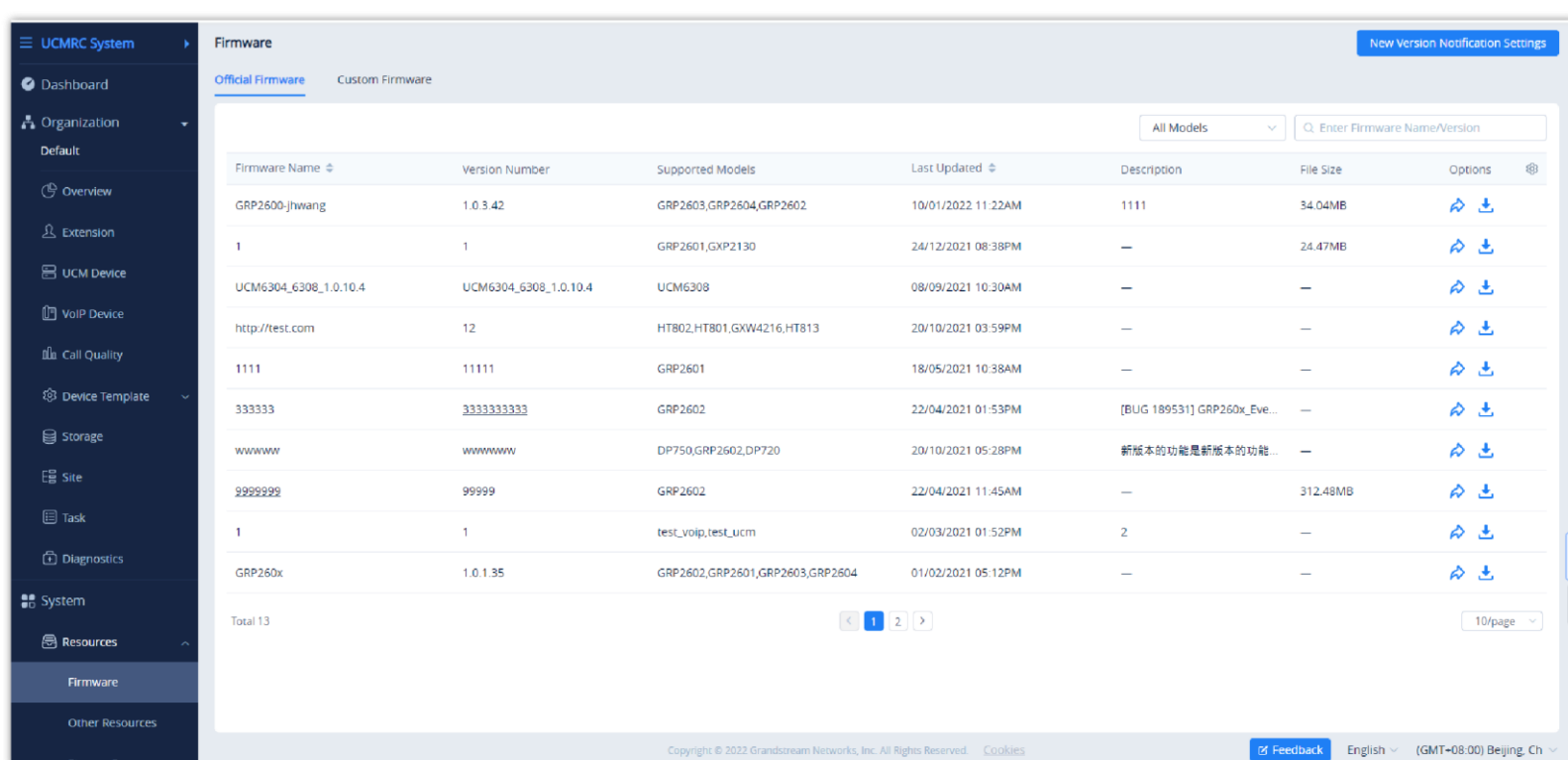
3. Once the firmware is uploaded successfully, it will appear in the custom firmware list. Devices will be able to select the firmware when upgrading via GDMS.



Finish Uploading Custom Firmware

Official Firmware

The official firmware page lists the latest official firmware for every supported device. This list is maintained and updated by Grandstream.



Official Firmware

i Official firmware cannot be edited or deleted, and users can only download or push the firmware to upgrade the devices.

Firmware Update Notification Settings

Users can subscribe to firmware update email notifications to keep up to date with the latest firmware releases.

1. Click on the **New Version Notification Settings** button at the top of the **Firmware** page. The following window will appear:

New Version Notification Settings ×

If a new firmware version is available on GDMS, please send an email to the following address:

<input type="checkbox"/>	Model
<input checked="" type="checkbox"/>	DP720
<input checked="" type="checkbox"/>	DP750
<input checked="" type="checkbox"/>	GRP2612
<input checked="" type="checkbox"/>	GRP2614
<input checked="" type="checkbox"/>	GXP1780
<input type="checkbox"/>	GXP2135
<input checked="" type="checkbox"/>	GXP2170
<input checked="" type="checkbox"/>	GXV3370
<input checked="" type="checkbox"/>	GXV3380
<input checked="" type="checkbox"/>	HT801
<input checked="" type="checkbox"/>	WP820

Firmware Update Notification Settings

2. Users can select the device models they want firmware update notifications for.
3. Click on the **Save** button to finalize changes.

Push Firmware Update

Using this feature, the user can push firmware updates to the devices directly; this can be performed for devices with various firmware version number, or the if the user wants to upgrade devices which have a specific firmware version number, the user will be able to specify that version number or specify a range of firmware versions to be upgraded.

1. Click on the button for the desired firmware. The following window will appear:

Push Firmware Update ×

* Task Time Immediate Scheduled Permanent

* Current Firmware Range

* Target Device(s) All devices of this model Select Devices Enter MAC Address

Includes devices added in the future

Select Corresponding Organizations

Select Device Model


Push Firmware Upgrade


2. Select the devices to push the firmware to. Users can search for specific devices by entering in a MAC address or name or filter devices by specific sites.

3. Click on **Update Now** to immediately push the firmware upgrade to devices or **Schedule Config Update**.

4. Click on the **Save** button to create the task. Users can check the status of the firmware upgrade on the **Task Management** page.


Edit Custom Firmware File Info

Users could edit the custom firmware file name, firmware version, and other information on the GDMS platform. Click on the button  to access the firmware editing page.

 If the firmware file is changed, existing scheduled tasks involving that firmware will still use the original file, not the newly uploaded file.


Download Firmware

Users can download firmware on GDMS by clicking on the  button.

 If a firmware on GDMS is using a configured file path, that path will be used when downloading it.

Delete Custom Firmware

Users can delete custom firmware by selecting them in the firmware list and clicking on the **Delete** button in the top-left corner of the list.

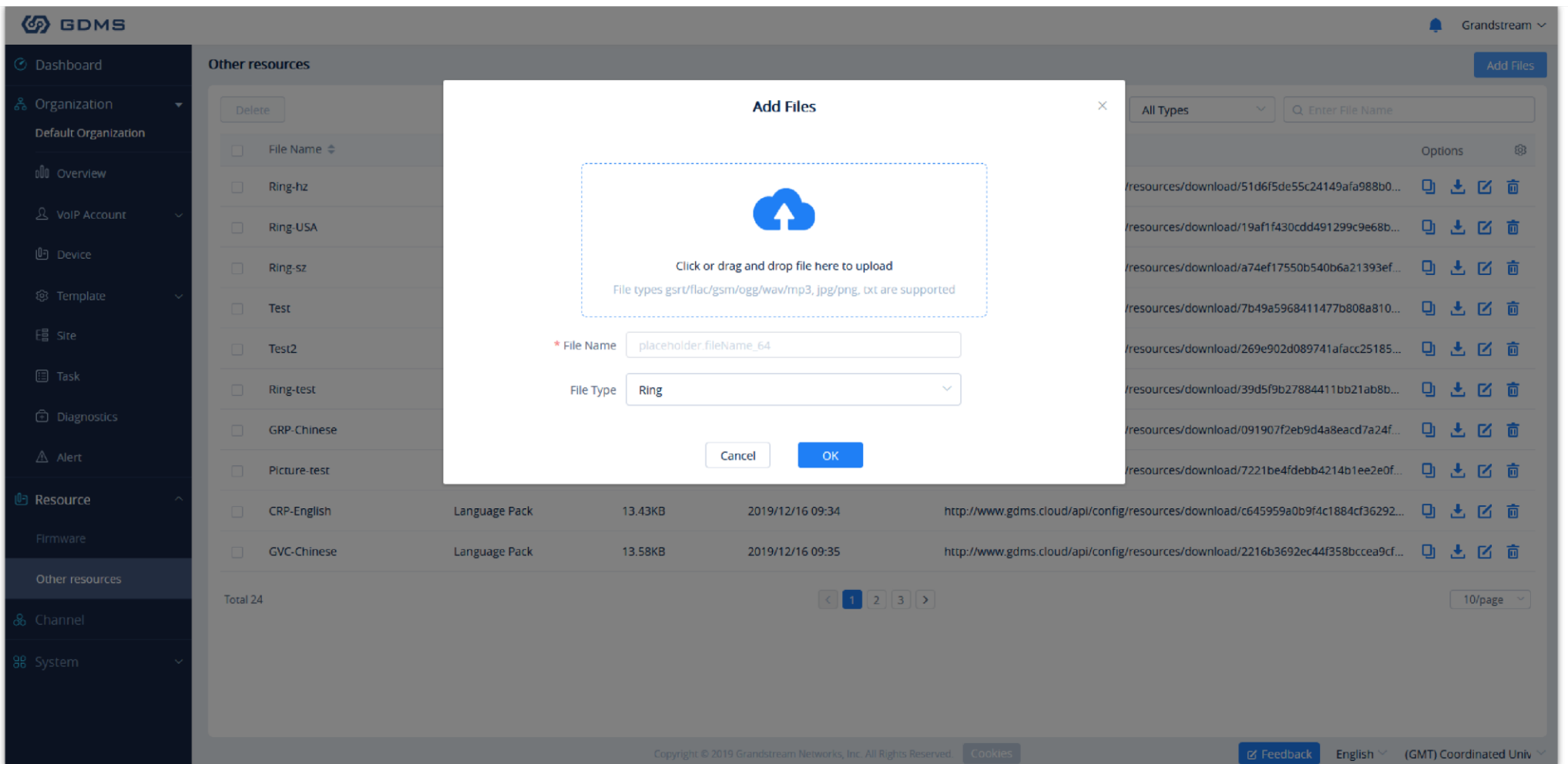
 If a firmware is deleted, scheduled tasks associated with it will continue as normal anyway. Once all associated scheduled tasks are completed, the firmware file will automatically be removed from GDMS

Other Resources Management

Users can upload the resource files (such as ringtone files, wallpapers, language packs, etc.) to the GDMS platform so that users can configure or assign the resource files to devices at any time.

Upload Resource

1. On **Resource Management** → **Other Resources** page, click on the resource files uploading button.
2. Users can drag or click to upload ringtone files, pictures, language packs, and other files, as the figure shows below:



Custom Firmware

File	<p>Users could drag the file to the uploading area or click on the uploading area to select the file.</p> <p>Supported file format: gsrt/flac/gsm/ogg/wav/mp3/jpg/png/txt. If the user selects the file type as “Other,” the GDMS platform will not restrict the file format.</p> <p>File size limit: Bin file/Ringtone – 128KB; Picture/Language pack – 500KB; Other – 5MB.</p>
File Name	<p>This is used to identify the file name. The limit is 1 – 64 characters.</p>
File Type	<p>This is used to identify the file type, such as ringtone, picture, language pack, and Others.</p>

Table 37: Custom Firmware

3. Click the “OK” button to save the file to the GDMS server.

The user can also choose to edit a file, this basically allows the user to upload a file and overwriting the existing one.

- When the resource file is uploaded to the GDMS server, users can configure the resource file for the device on the “Set Parameters” page.
- Only some specific models support configuring custom ringtones and language packs, and the supported file sizes are different.
- The new resource files will be loaded after the device is restarted.

View Resource List

Users can view all resources on **Resource List** under the enterprise, including the uploaded resources.

1. Users can go to **Resources** → **Other Resources** to view the resources list.
2. Users can also search the resources by resource type or file name on the resources list.

Other Resources (Used space 319.45KB) Create GUI Config File Upload File


All Types ▼

<input type="checkbox"/>	File Name ↕	File Type	File Size	Updated Time ↕	File URL Address	Options ⚙
<input type="checkbox"/>	ca-bundle	Other	228.96KB	2022-09-19 12:23	https://eu.gdms.cloud/api/config/resources/do...	<input type="button" value="Copy"/> <input type="button" value="Download"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	ring2	Ringtone	26.94KB	2021-04-08 15:19	https://eu.gdms.cloud/api/config/resources/do...	<input type="button" value="Copy"/> <input type="button" value="Download"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	ring1	Ringtone	63.55KB	2021-04-08 15:18	https://eu.gdms.cloud/api/config/resources/do...	<input type="button" value="Copy"/> <input type="button" value="Download"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>


Total 3 < 1 > 10/page ▼

Other Resources


Copy File URL


1. On **Resource Management** → **Other Resources** page, click the button  following the resource file to copy the resource URL.
2. Copy the file URL and paste it to another file download path.

Download Resource


1. On **Resource Management** → **Other Resources** page, click the button  following the resource file to download the resource.
2. Download the resource file locally.

Modify Resource

1. On **Resource Management** → **Other Resources** page, click the button  following the resource file to modify the resource.
2. Users can modify the file and file name.

 If the user wants to re-upload the resource file, the device using this file URL may download and use the new resource file.

Delete Resource

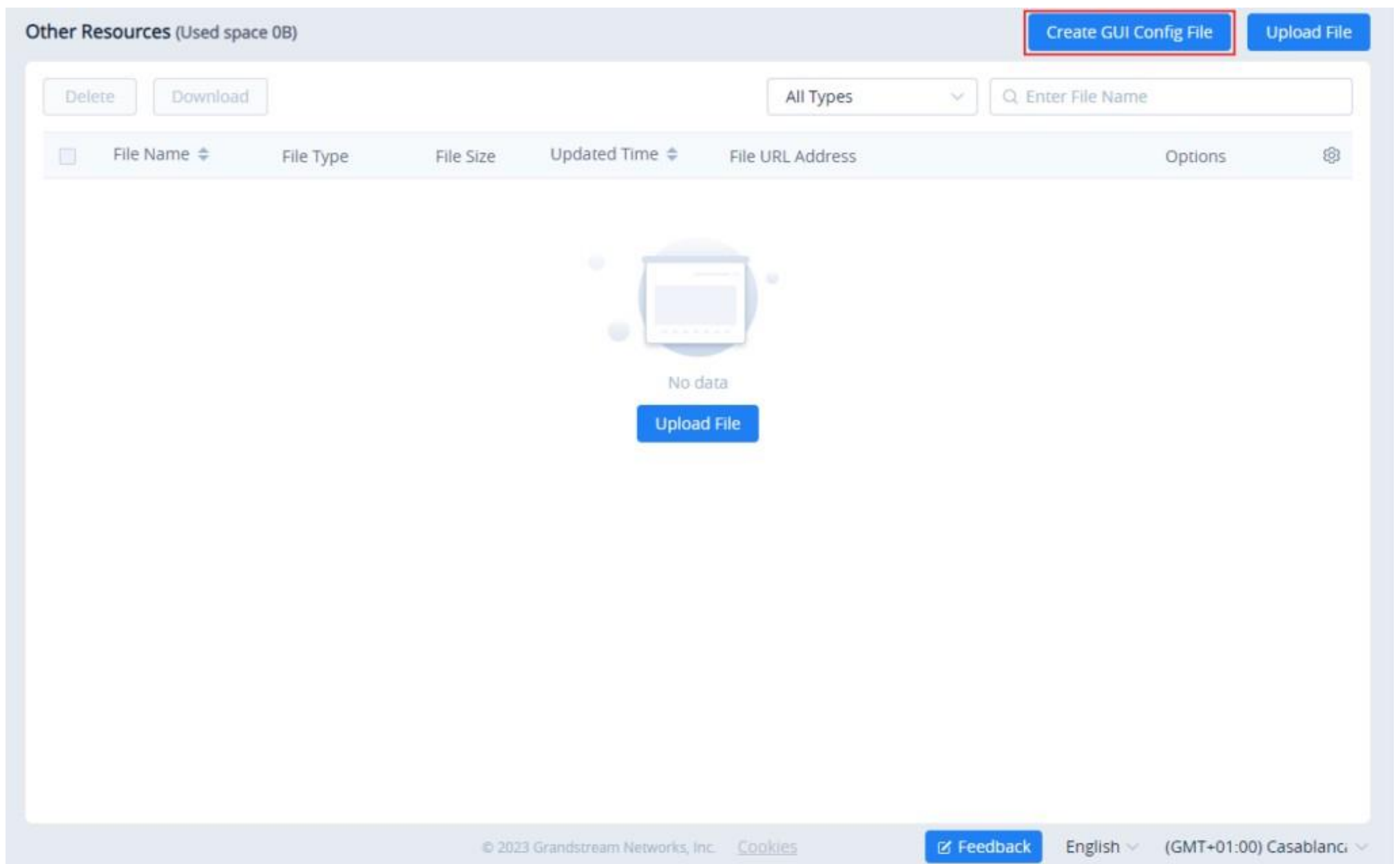
1. On **Resource Management** → **Other Resources** page, click the button  following the resource file to delete the resource. Users can also select multiple resource files and click the Delete button on the top of the page to batch delete the resource files.
2. When the user confirms to delete the resource file, the selected file will be deleted from the GDMS platform.

i When the file is deleted from the GDMS platform, the device using this file URL still can use the downloaded resource file in the device locally.

GUI Config File

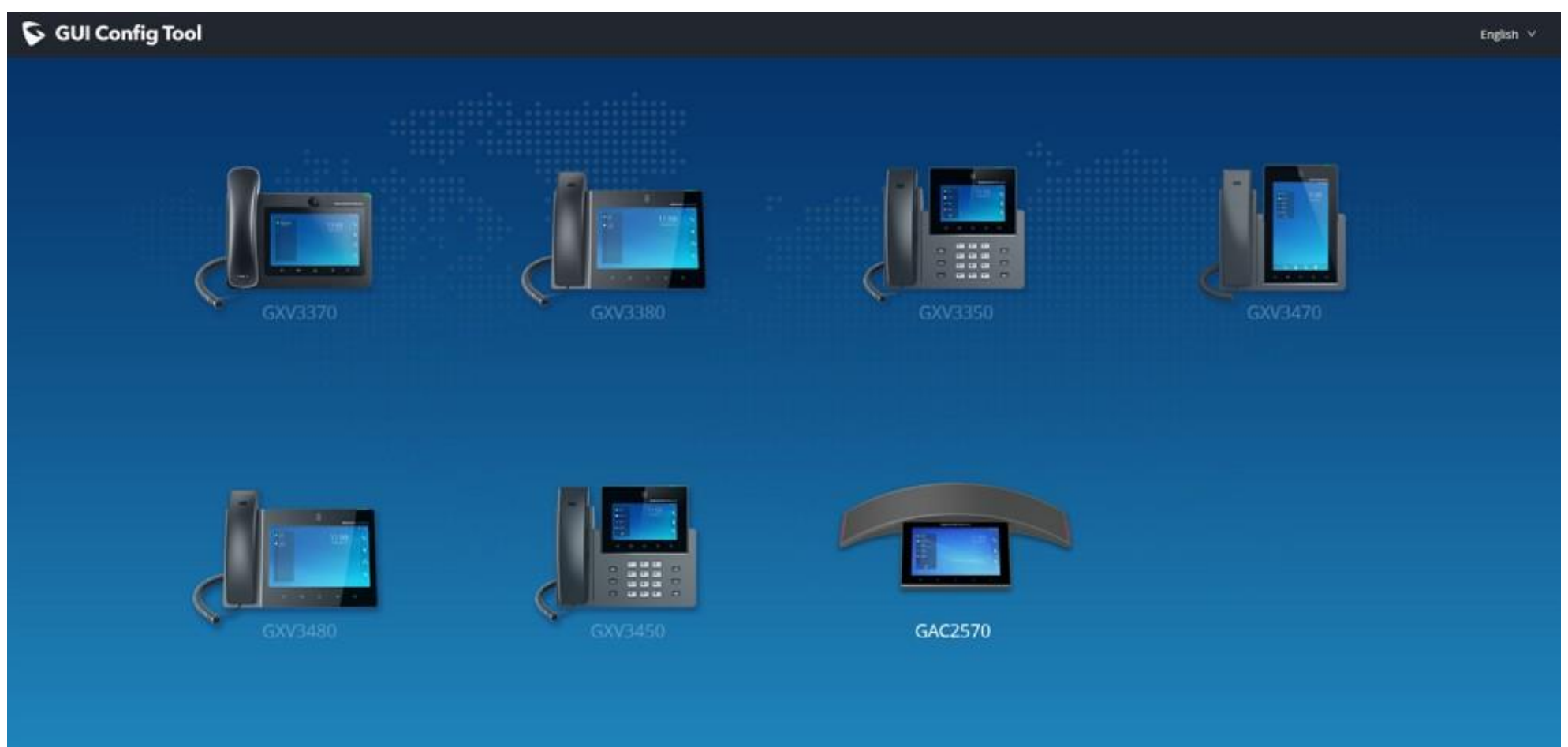
The user can use the GUI Config tool to create a configuration file for a specific model device and store the configuration file on the GDMS storage space.

- On **Other Resources**, please click “Create GUI Config File”



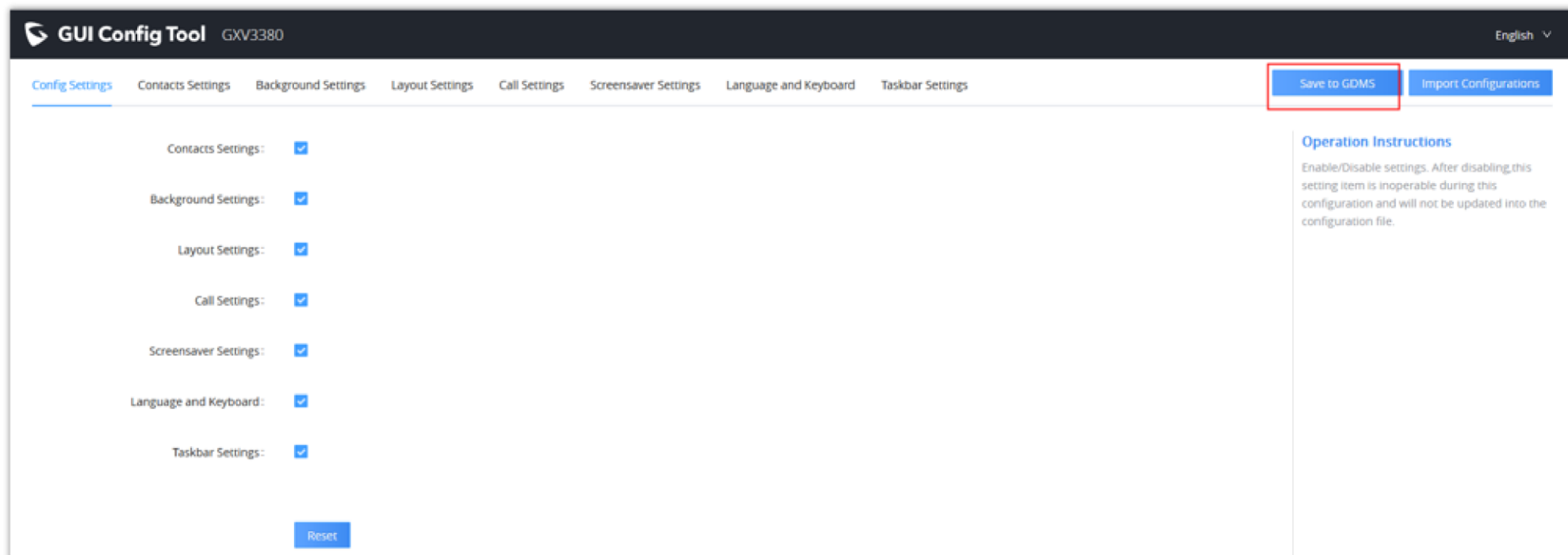
Create GUI Config File

- Choose the model of which you want to create the configuration file.



Choose a model

- Once the configuration has been customized, click on “Save to GDMS”.

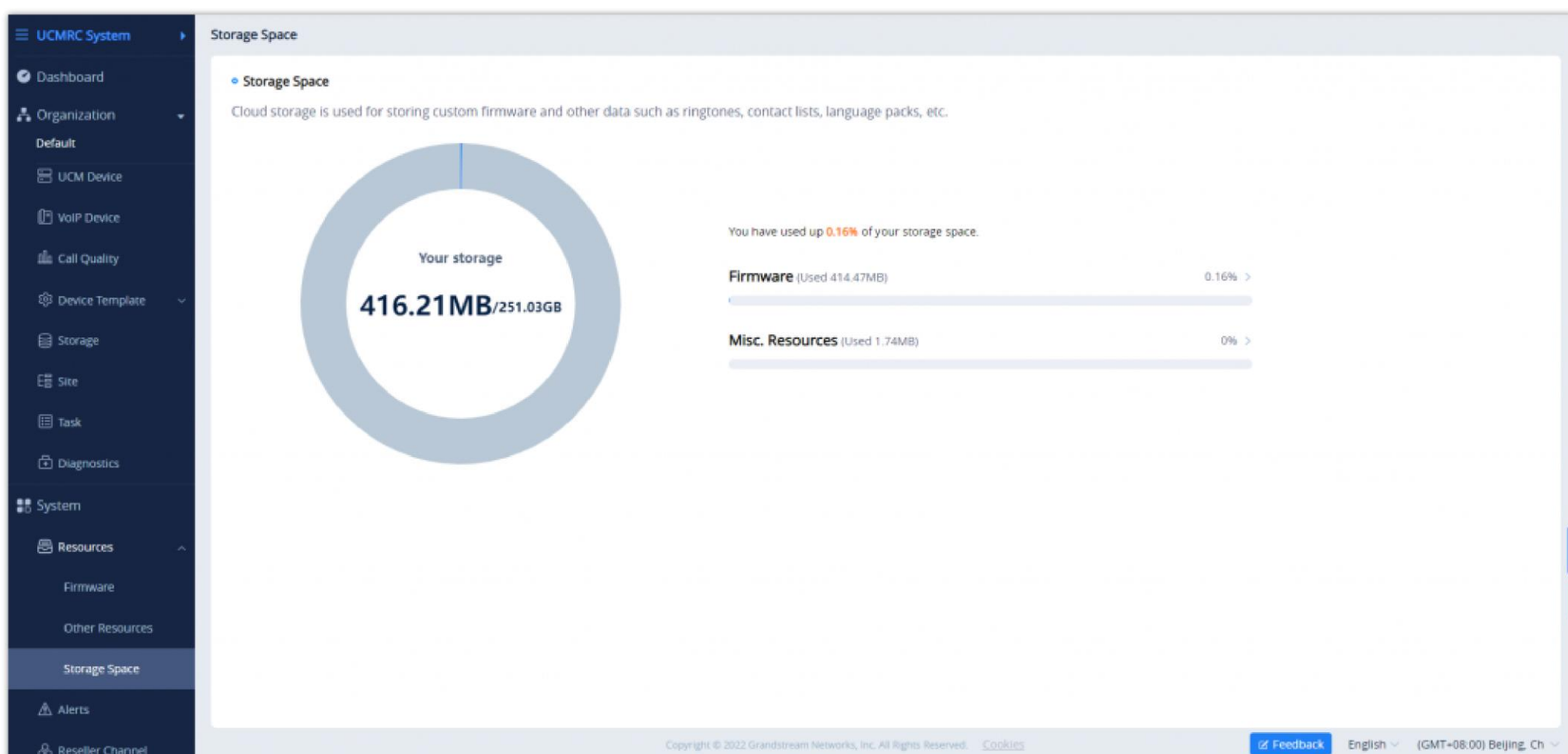


Save to GDMS

View Storage Space

All resource files are stored in the enterprise’s storage space. This interface shows the storage space occupied and the total storage space:

- On the” **Resource Management**“ → ”**Storage Space**“ interface, go to the **Storage Space** statistics page. This interface shows the storage space taken up by the custom firmware and the other resource files.



View Storage Space

Note

If the current storage space is less than 10% or full, the user can upgrade the plan or clean up the storage space to get more available storage space.

CHANNEL MANAGEMENT

Channel customers and service providers can obtain a list of purchased devices from Grandstream ERP. This list will allow the channel customer or service provider to:

- Quickly assign devices to sub-channel customers. These customers will then be able to log into GDMS to manage the devices.

2. Manage devices directly for customers.

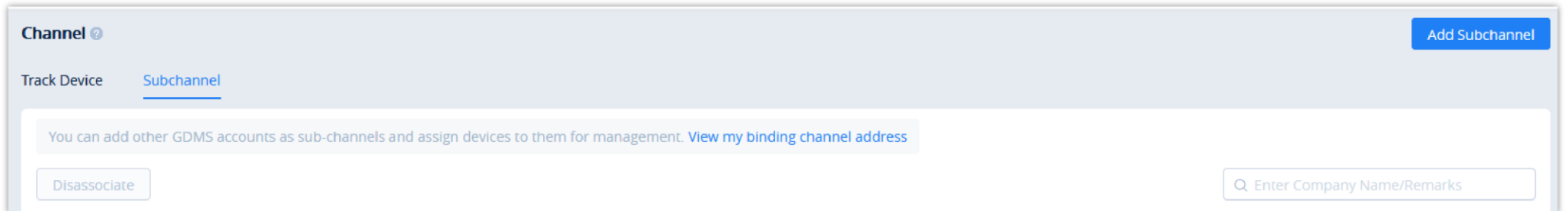
- ✔ Channel customers and service providers will need to contact Grandstream support to associate their GDMS account with an ERP account.

Superior Channel Binding Address

If a superior channel wants to assign devices to the user, the superior channel needs to add the user's GDMS account as a subordinate channel.

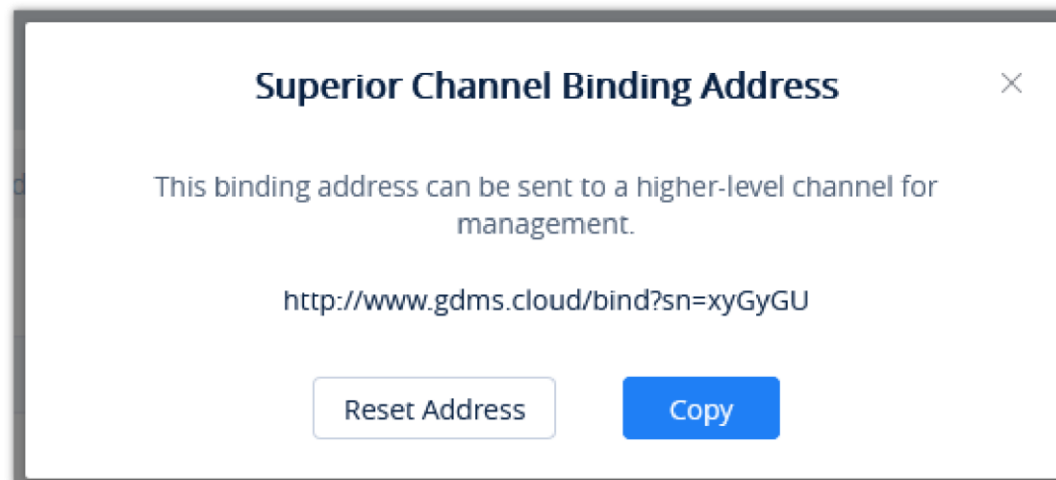
The user needs to copy and send the binding address to the superior channel.

1. Click on the link at the top of the Channel page "View my binding channel address," as the figure shows below:



View My Binding Channel Address

2. View my superior channel binding address, users could reset/copy the binding address.



Superior Channel Binding Address

- **Copy:** Click to copy the link address to the clipboard.
- **Reset Address:** Generate another address. The previous link will be invalid.

Add Sub-channel

Users can add sub-channels to GDMS accounts at any time. Once added, the user can assign devices to the sub-channels. To properly add a sub-channel:

Obtain the bind-address from sub-channels to add their GDMS accounts.

1. On the **Channel Management** page, click on the **Add Sub-channel** button. The following window will appear:

Add Subchannel ×

* Link Address

Please contact the subchannel to acquire a "Channel Binding URL".

Remarks

Link Address

2. Enter the provided bind address from the sub-channel into the **Link Address** field.
3. Add a description or comment for this sub-channel.
4. Click on the Save button to finalize changes.
5. Once the sub-channel is added, users can now assign devices to it via the Trace Devices tab.



- Each user could be the subordinate channel customer for multiple GDMS users.
- Each user could be the superior channel distributor for multiple GDMS users.
- Users could only add subordinate channel customers which are in the same region (If the user is in the region of the United State, the user could only add the enterprises in the United State region as the subordinate channel customers).

Edit Subordinate Channel Customer

After adding a sub-channel, users can only edit the **Remarks** field for it. To edit it, click on the button for the desired sub-channel.

Edit Channel ×

Company Name

Remarks

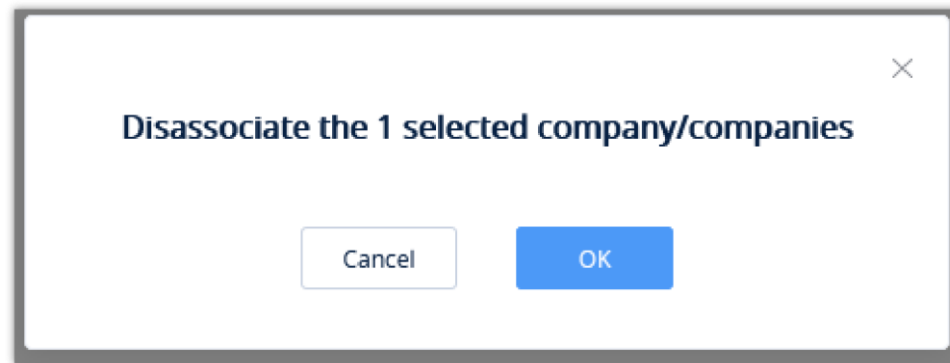
Assigned Device Number

Add Time

Add Remarks

Delete Subordinate Channel Customer

To remove sub-channels from GDMS, select the desired sub-channels and click on the **Disassociate** button. Devices can no longer be assigned to this sub-channel.

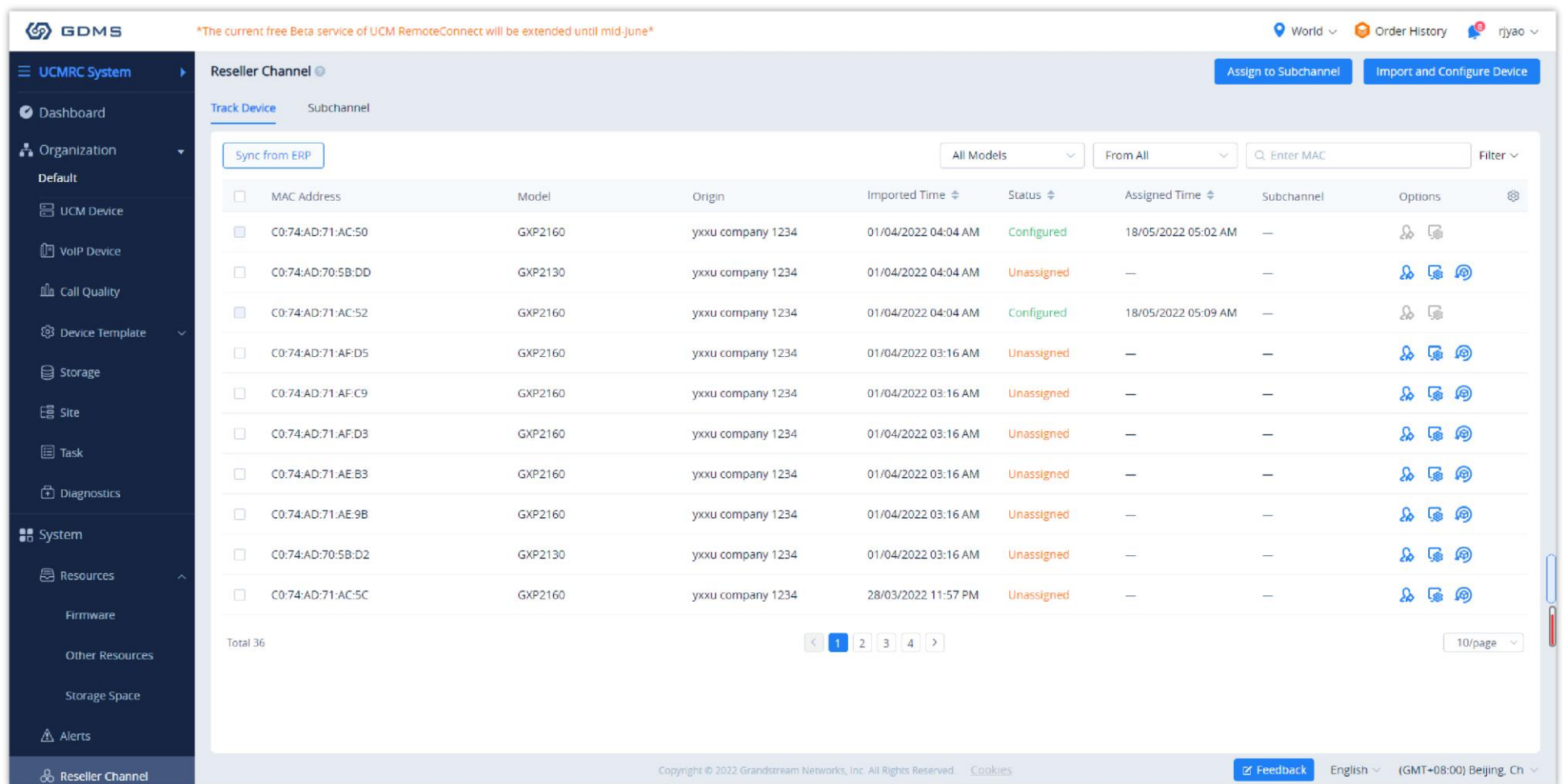


Disassociate Sub-channel

Track Device

View Device

To view all devices assigned to the account, click on the **Track Device** tab.



Track Device

MAC Address	The MAC address of the device.
Device Model	The model of the device.
Resource	Where the device originated from. Currently, there are two values: <ul style="list-style-type: none"> ◦ ERP Order – The device’s data was synchronized from Grandstream ERP. ◦ Main Channel – The device was added by the main channel.
Warehousing Time	The date/time the device was assigned to the account.
Status	<p>Allocated: The device has been assigned to a sub-channel and cannot be assigned to other sub-channels.</p> <p>Unallocated: The device is not allocated to any sub-channel yet.</p>

Outgoing Time	The date/time the device was assigned to a sub-channel. The company name of the sub-channel will also be displayed.
----------------------	---

Table 38: Track Device

Users can search for specific devices by using the filter and search options in the top-right of the **Channel Management** page.

! Users cannot directly upgrade the firmware or update the configuration file of the devices from this list. Please refer to Configure Device section.

Device Assignment Notification

When devices are assigned to an account, the  icon will show a notification. Clicking on the notification will show the list of assigned devices.

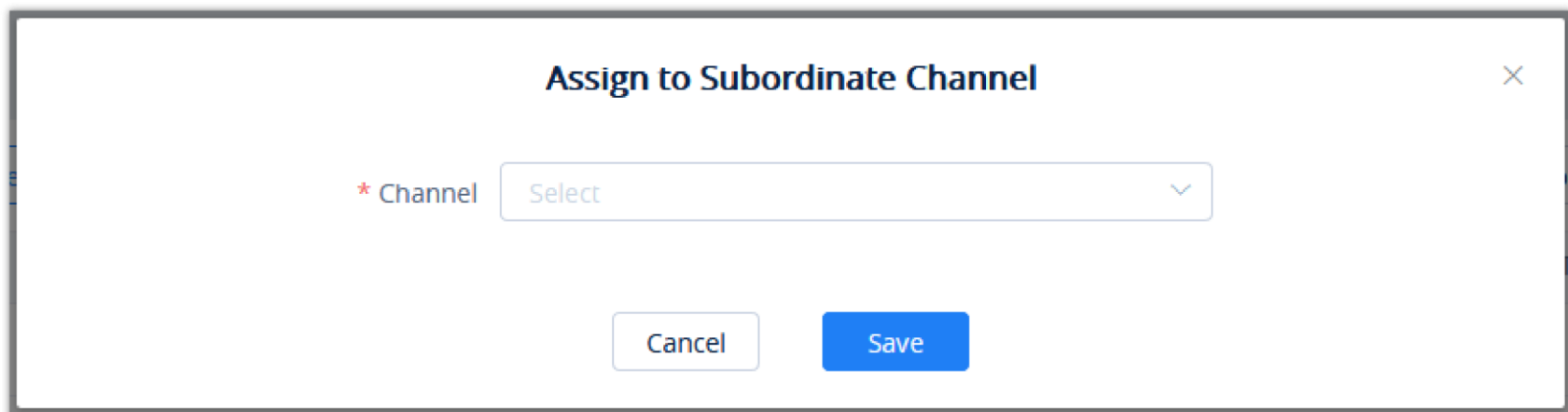
Device Assignment

For the devices which have been sold to the subordinate channel customer, the user could allocate the devices to them. The subordinate channel customer could log in to the GDMS platform to view and manage the devices.

The user could allocate a single device or allocate a batch of devices:

Assign a Single Device:

1. Click on the  button for the desired device. The following window will appear:

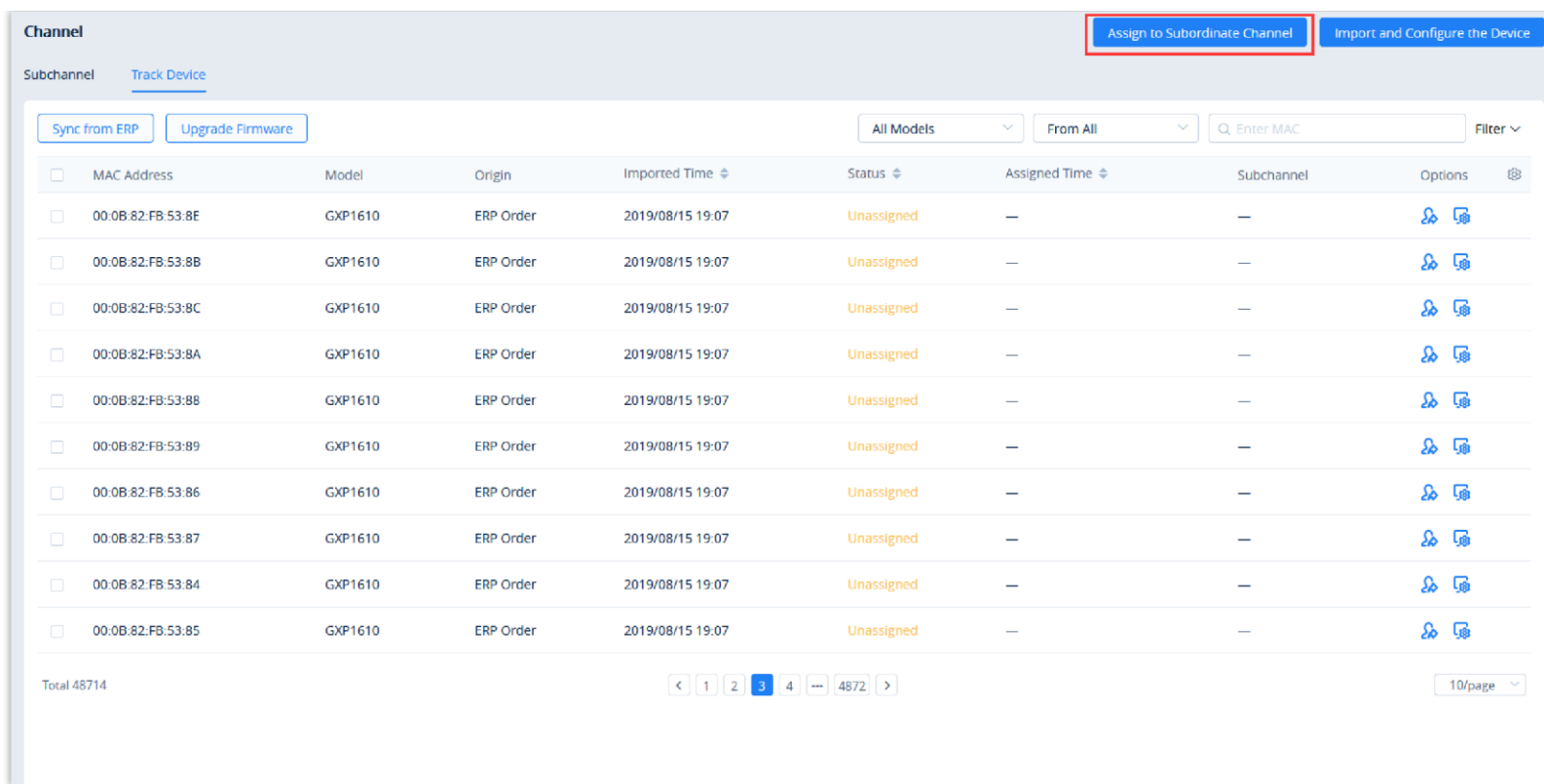


Assign Single Device to Subordinate Channel

2. Select the sub-channel to assign the device to.

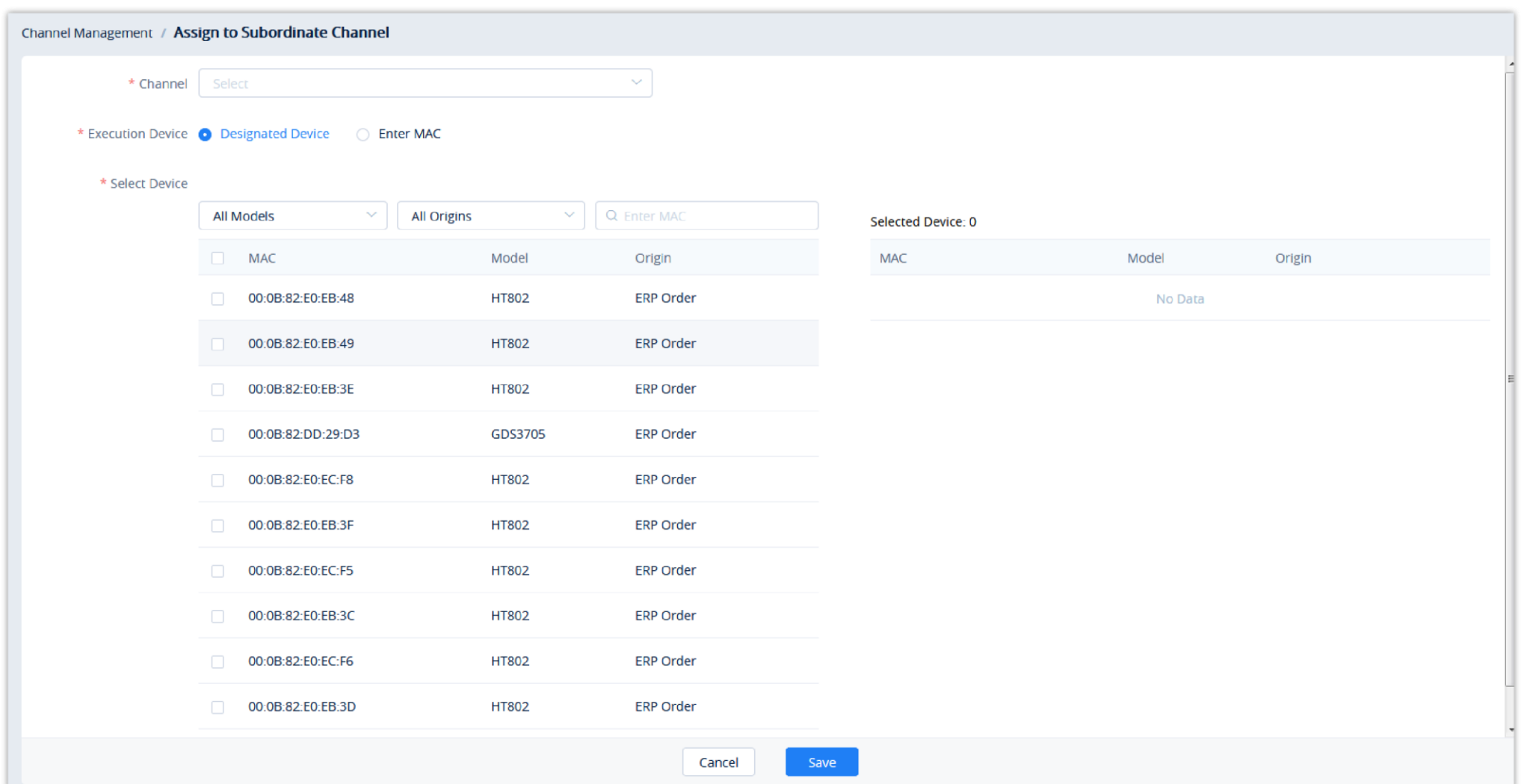
Assign Multiple Devices:

1. Click on the Device Operation button at the top-right of the **Channel Management** page.
2. Click on **Assign to Subordinate Channel** on the **Track Device** page. The user will be redirected to the batch device assignment page.



Device Operation Options

3. The user will be directed to the batch devices allocating page:



Assign Multiple Devices to Subordinate Channel

Select Subordinate Channel Customer	Select the sub-channel to assign the devices to
Device	Select the devices to assign to the sub-channel from the list or enter the MAC addresses of the devices.

Table 39: Assign to Subordinate Channel



Copy and Paste Multiple MAC Addresses

4. Click the **Save** button to finalize changes and the assignment. The sub-channel will then be notified of the device assignment.

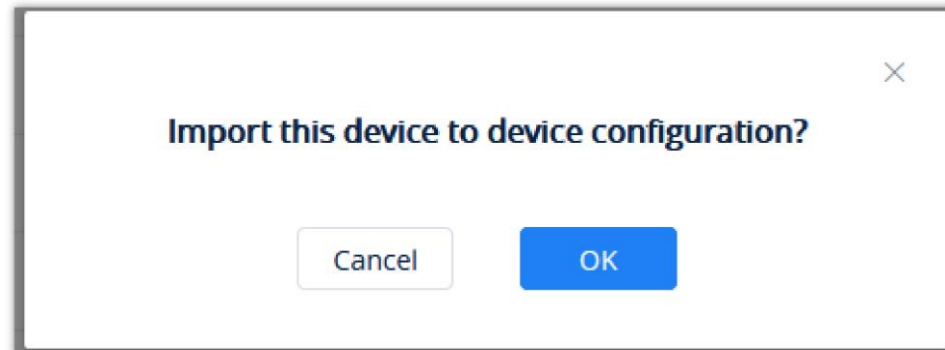
- The device which has been allocated to a customer cannot be allocated to any customer else.
- When the device is allocated, the user cannot acquire back the device. If the device is allocated to a customer incorrectly, the user could contact the subordinate channel customer to allocate the device back to the user.

Configure Device

To manage devices from the **Channel Management** device list, users must first import the devices to **GDMS Device Management**.

Import Single Device

1. Click on the  button for the desired device. The following window will appear:



Import to Manage Device

2. Click on the “OK” button to finalize the import.

Upgrade Task

Users can perform an upgrade task to devices which belong to a specific channel. The upgrading can be triggered to many devices at once or it can be performed subsequently.

[Reseller Channel](#) > **Add Upgrade Task**

* Task Name

Firmware Version

* Upgrade Method Concurrent Upgrade device(s) Sequential Upgrade

* Current Firmware Range

* Target Device(s) All devices of this model Select Devices Enter MAC Address

© 2023 Grandstream Networks, Inc. [Cookies](#) English

Add Upgrade Task

Task Name	Enter the task name.
------------------	----------------------

Firmware Version	Select the device model and firmware version number
Upgrade Method	Select the upgrade method <ul style="list-style-type: none"> • Concurrent Upgrade: Enter the maximum number of devices which will be upgraded simultaneously. The valid range is 1-9999. • Sequential Upgrade: The devices will be upgrade one at a time.
Current Firmware Range	<ul style="list-style-type: none"> • All Versions: All version are taken into consideration. • Specified Firmware Version: Enter a specific firmware version. • Firmware Version Range: Enter a range of version number.
Target Device(s)	<ul style="list-style-type: none"> • All Devices of This Model: All the devices of the selected model will be upgraded. • Select Devices: Select the devices to upgrade. • Enter MAC Address:

USER MANAGEMENT

The **User Management** page allows users to view, add, and edit users and manage role privileges. By default, GDMS has one administrator, which has all available privileges. Roles are sets of privileges that admins can assign sub-users.

Add Role

To add a role with specific privileges, click on the **Add Role** button at the top right of the **User Management** → **Role** page and enter the following information:

The screenshot shows the 'Add Role' form in the UCMRC System. The form has a sidebar on the left with navigation options like Dashboard, Organization, UCM Device, VoIP Device, Call Quality, Device Template, Storage, Site, Task, Diagnostics, System, Resources, Alerts, Reseller Channel, Others, and Users. The main form area is titled 'Role > Add Role' and contains the following fields and sections:

- Role Name:** A text input field.
- Description:** A text input field.
- Select Permissions:** A section with tabs for VOIP, UCMRC, Resources, Alerts, Reseller Channel, Others, and Order History. Under the VOIP tab, there are several groups of checkboxes:
 - All:**
 - Dashboard:**
 - Overview:**
 - Device Management - VoIP Device:**
 - Device List, Import Device, Upgrade Firmware, Site Assignment, Task History, Sync Device Local Configuration
 - Transfer Device, Export Device, Reboot Device, Set Parameters, Reconfigure, Remote Access to Web UI
 - Add Device, Edit Device, Factory Reset, Account Configuration, Device Details, Remote Access to Device Interface
 - Authorization Management, Delete Device, Device Diagnostics, Operation Logs, Enable/Disable Push Notifications
 - Device Management - GKW4500 Series:**
 - Device List, Export Device, Reboot Device, Device Details
 - Remote Access to Device Web UI, Assign Site, Device Diagnostics
 - Add Device, Delete Device, Operation Logs
 - Import Device, Upgrade Firmware, Task History
 - VoIP Account - SIP Account:**

At the bottom of the form, there are 'Cancel' and 'Save' buttons. The footer of the page includes copyright information for Grandstream Networks, Inc. and a language selector set to English.

Add Role

Role Name	Users need to input the name of the role in this field.
Description	Users need to input the description of the role in this field.
Select Permissions	Users need to select the privileges of the role.

Add Role

❗ If a role does not have the privilege of a feature, the GDMS portal will not show it.

Edit Role

To edit a role's name, description, and privileges, click on the  button for the desired role.

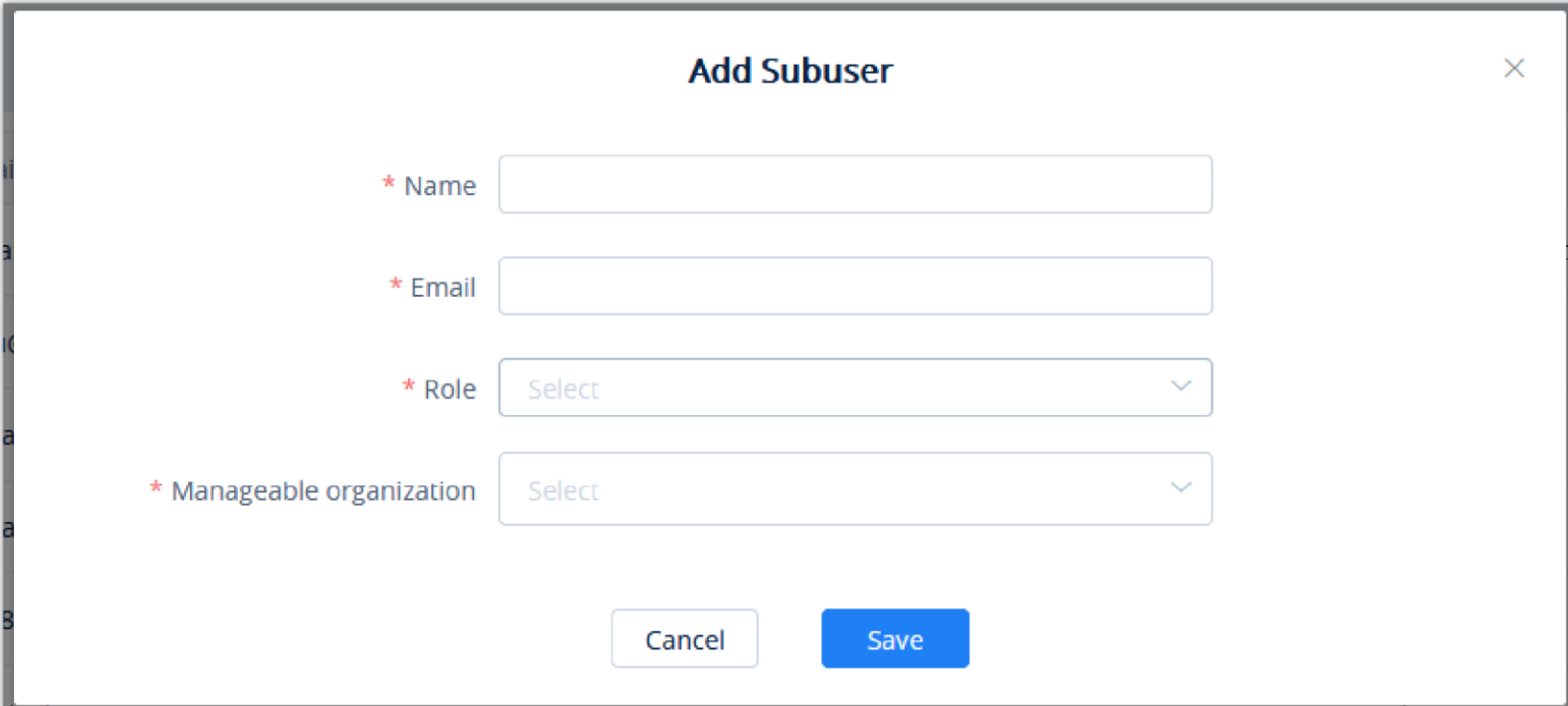
❗ Users cannot edit the roles of the default admin account.

Delete Role

To delete a role, click on the  button for the desired role. If the role includes some sub-users accounts, the role cannot be deleted.

Add Sub-user

To add a sub-user to the GDMS account, click on the **Add Sub-user** button and enter the following information:



The image shows a modal window titled "Add Subuser" with a close button (X) in the top right corner. It contains four required fields, each marked with a red asterisk: "Name" (text input), "Email" (text input), "Role" (dropdown menu with "Select" and a downward arrow), and "Manageable organization" (dropdown menu with "Select" and a downward arrow). At the bottom of the form are two buttons: "Cancel" (white with grey border) and "Save" (blue).


Add Sub-user

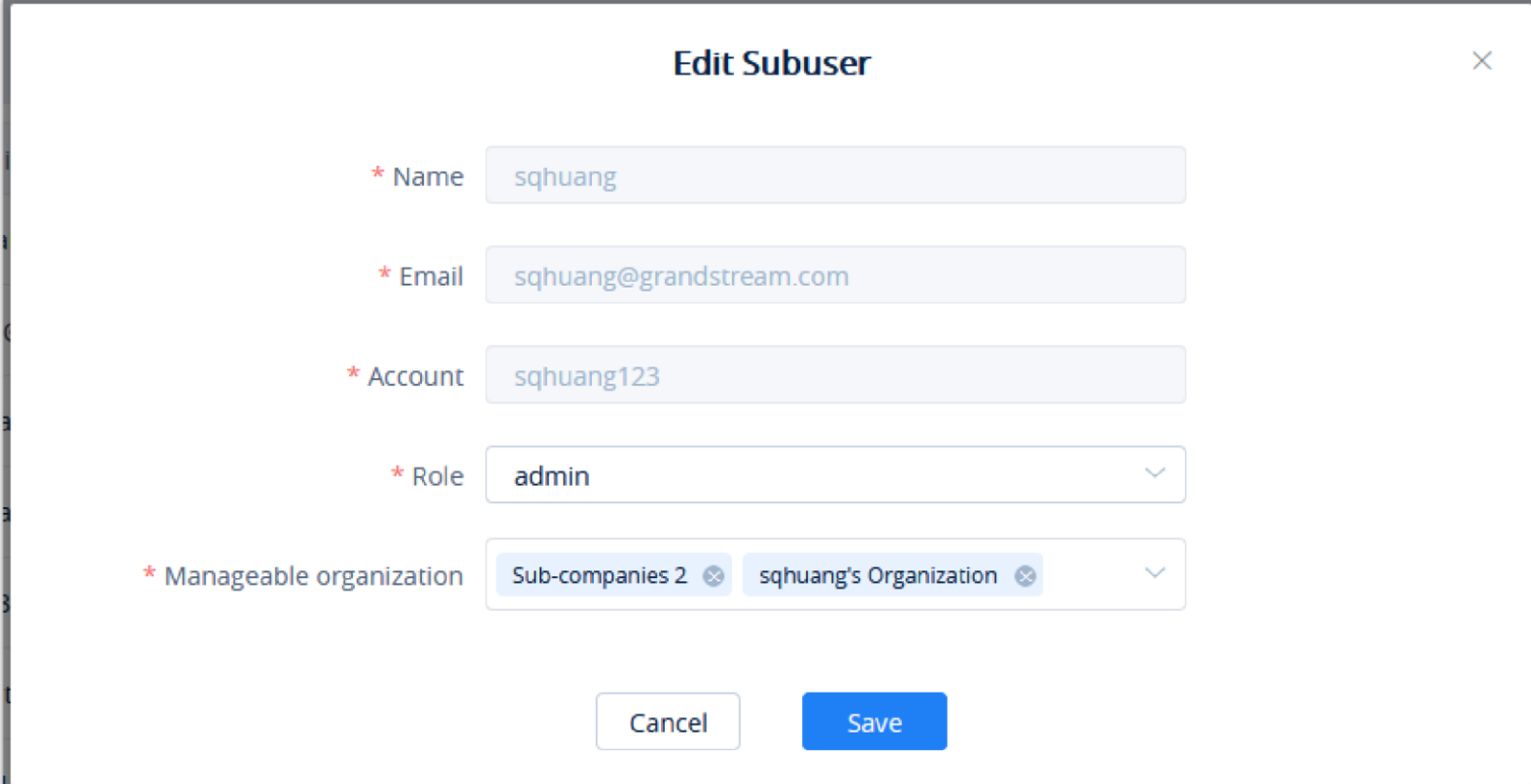
Name	Users need to input the name of the sub-user in this field.
Email Address	Users need to input the email address of the sub-user. The sub-user will use this to verify and activate this account, log into GDMS, and receive email notifications.
Role	Users need to select the role of the sub-user.
Manageable Organization	Assign the manageable organization to the user, and the administrator could select the manageable organizations from the existing organizations.

Add Sub-user

Upon creating the sub-user, an activation email will be sent to the configured email address. The sub-user must click on the provided link to activate the account.

Edit User

To edit a verified sub-user's role, click on the  button for the desired sub-user and select the new role. The sub-user's other information cannot be modified even by an administrator.



The image shows a modal dialog box titled "Edit Subuser" with a close button (X) in the top right corner. It contains five form fields, each with a red asterisk indicating it is required:

- Name:** Text input field containing "sqhuang".
- Email:** Text input field containing "sqhuang@grandstream.com".
- Account:** Text input field containing "sqhuang123".
- Role:** Dropdown menu with "admin" selected.
- Manageable organization:** Multi-select dropdown menu with "Sub-companies 2" and "sqhuang's Organization" selected.

At the bottom of the dialog are two buttons: "Cancel" (white with grey border) and "Save" (blue).

Edit Sub-user

For unverified sub-users, administrators can modify the name, email address, and role. Additionally, they can send an account activation email to the configured email address.




The image shows a single row from a table representing an unverified sub-user. The row contains the following information from left to right:

- Profile icon and name:  jhwang-test
- Email address: 123@test.com
- Role: admin_backstage
- Other identifier: yxxu
- Status: Inactivated (text is orange)
- Actions: Three icons for email, edit, and delete.

Edit Unverified Sub-user

Delete User

To delete user accounts, click on the  button for the desired user. Deleted users cannot log into GDMS.

User Settings

The user can customize his/her settings when logged into the account. To access the settings of the account, the user must click on the name of the account on the top right corner, then select **User Settings**.

User Settings
Delete business account

Basic Info

Main Region Europe (Users/Devices data in the EU server) Delete

* Display Name Modify

Email Modify

Username Modify

Password ***** Modify

* Company Grandstream Networks, Inc. Modify

Company Type Company User

Country/Region Morocco(المغرب) Modify

Timezone (GMT+01:00) Casablanca, Monrovia Modify

Time 24-hour clock Modify

Date YYYY/MM/DD Modify

Security

Multi-Factor Authentication Disabled Enable

Allow Multiple Device Logins Enabled Close

Role Info

Role admin

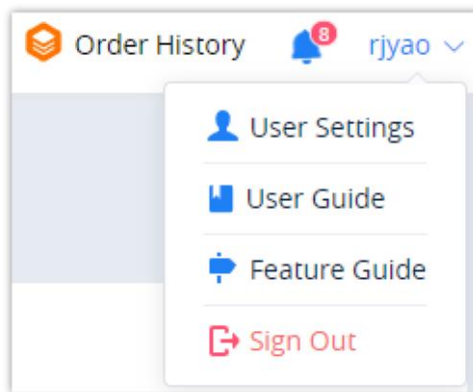
© 2023 Grandstream Networks, Inc. [Cookies](#) [Feedback](#) English (GMT+01:00) Casablanca

User Settings

Main Region	This option displays the primary region of the current GDMS account. This can be deleted. After deleting the main region, the data in the current regional server cannot be restored.
Name	This option shows the display name for the account.
Email Address	This option shows the email address associated with the account. To modify this email address, the user will need to enter the current login password.
Login Name	This option shows the username for the account. This is used for logging into GDMS, and it can be modified. The user needs to enter the password and new login name for authentication. The new login name must be unique.
Password	The login password is editable. The user needs to input the original login password to modify the current login password.
Company	This option shows the name of the user's company.
Country	This option shows the country of the user.
Time Zone	This option shows the time zone of the user.
Time Format	Users can modify the time format to 12 hours or 24 hours on the interface.
Date Format	Users can modify the date format to MM/DD/YYYY, DD/MM/YYYY, or YYYY/DD/MM on the interface.
Role Info	This option shows the current role of the user.

Sign Out

Log out of the account by clicking on the username on the top-right corner of the GDMS portal and clicking **Sign Out**.



Sign Out

Delete GDMS Account

If the user does not want to use the GDMS platform to manage devices anymore, the user can delete the GDMS account and all sub-accounts of the enterprise.

⚠ After deleting the GDMS account, all data of the GDMS account will be deleted.

1. Click the “**Personal Information**” option on the name menu at the upper right corner of the main page to enter the personal information configuration page.
2. Click the “**Delete business account**” button at the top of the page to delete the current GDMS account. If the enterprise GDMS administration account is deleted, all sub-accounts under the main GDMS account will also be deleted.

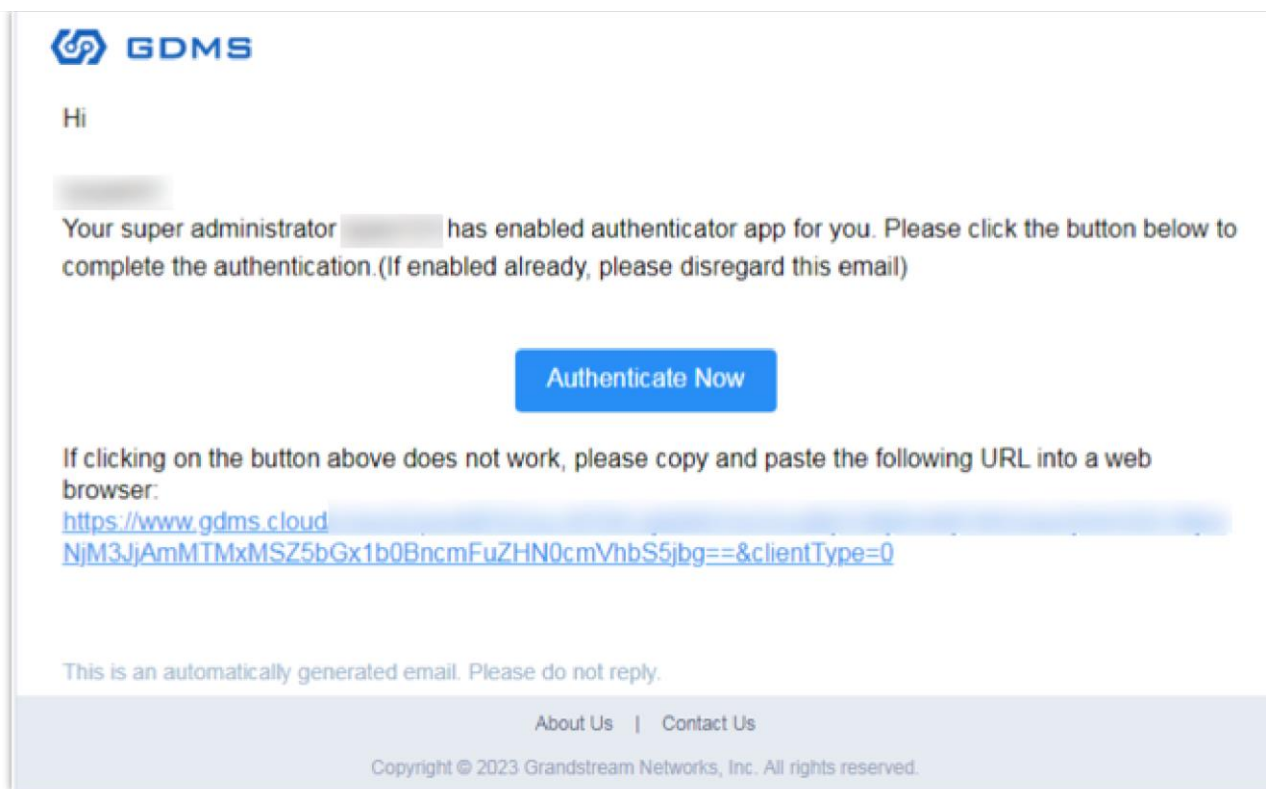
Enable Multifactor Authentication For a User

The administrator can enable the multi-factor authentication for the associated user. To do that please navigate to **Users** section under **System**, then check the box next to the user for which you want to enable multi-factor authentication then click on “Enable Multi-Factor Authentication”.

<input checked="" type="checkbox"/>	Name	Email	Account	Role	Organization	Multi-factor Authentication	Creator	Status	Options
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]	admin	World: Default, My Orga...	Disabled	—	Active	
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]	admin	World: Default, My Orga...	Disabled	emea_test	Active	[edit] [delete]
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]	admin	World: Default, My Orga...	Disabled	emea_test	Active	[edit] [delete]

Enable Multi-Factor Authentication For Users

After the multi-factor authentication has been enabled, the users will receive an email to activate multi-factor authentication.



MFA Enabled Email

The user can click on “Authenticate Now” button to access the multi-factor authentication page. The sub-user can only log into his/her account after setting multi-factor authentication. Otherwise, the user will not be able to log in.

Allow Multiple Device Logins

When this option is disabled, GDMS users will be restricted to open one session from one device using a web browser and one session from the GDMS mobile application. By default, multiple device logins is enabled. To change this specific settings please click on your account name then select **User Settings**, then change the setting on the “Security” category. When the user clicks “Close” this will disconnect the sessions opened and only this specific session will remain open, in addition to the latest session opened on the GDMS mobile application. Logging in from another device will close the formerly opened session.



User Settings

ASSOCIATED COMPANY MANAGEMENT

Users can add associated companies for management in the GDMS platform. After establishing the association relationship, users can select the associated companies and share the organizations with the associated companies for management.

Add Associated Company

After adding the associated enterprise, the user can select the associated enterprise and share the organization with the enterprise, so that the user and the associated enterprise can manage the organization together or assign management permission to the associated enterprise for management.

The user can obtain the binding address from the enterprise with which the user wants to establish the association relationship.

1. The user can access User Management -> Associate Company page, and click the “Add Associated Company” button to add the associated company.

Please see the screenshot below:

Add Associated Company [X]

* Associated Company Binding Address

Contact the company administrator to obtain the "Associated Company Binding Address"

Remarks

Add Associated Company

2. Enter the binding address of the associated company in the field “My Company Associating Address”.

3. Fill in the remarks of the associated company.

4. The user can click the “Save” button to add the associated company. Once done, the user can view the associated company name, remarks, and association time on the “Associated Companies” list. Please see the screenshot below:

Users Add Associated Company

Users Role Organization Associated Company

Other GDMS accounts (e.g., customers) can be added as associated companies and managed by your organization. View my associated company binding address

<input type="checkbox"/>	Company Name	Remarks	Add Time	Options
<input type="checkbox"/>	yxxu company 1234	yxxu公司	25/02/2022 09:54 AM	<input type="button" value="Edit"/>
<input type="checkbox"/>	jhwang's company	jhwang的企业	16/02/2022 09:36 AM	<input type="button" value="Edit"/>

Total 2 10/page

Associated Companies List

Edit Associated Company

On the “Associated Company” list, the user can click the button to access the “Edit Associated Company” interface to modify the remarks of the associated company.

Edit Associated Company [X]


Company Name

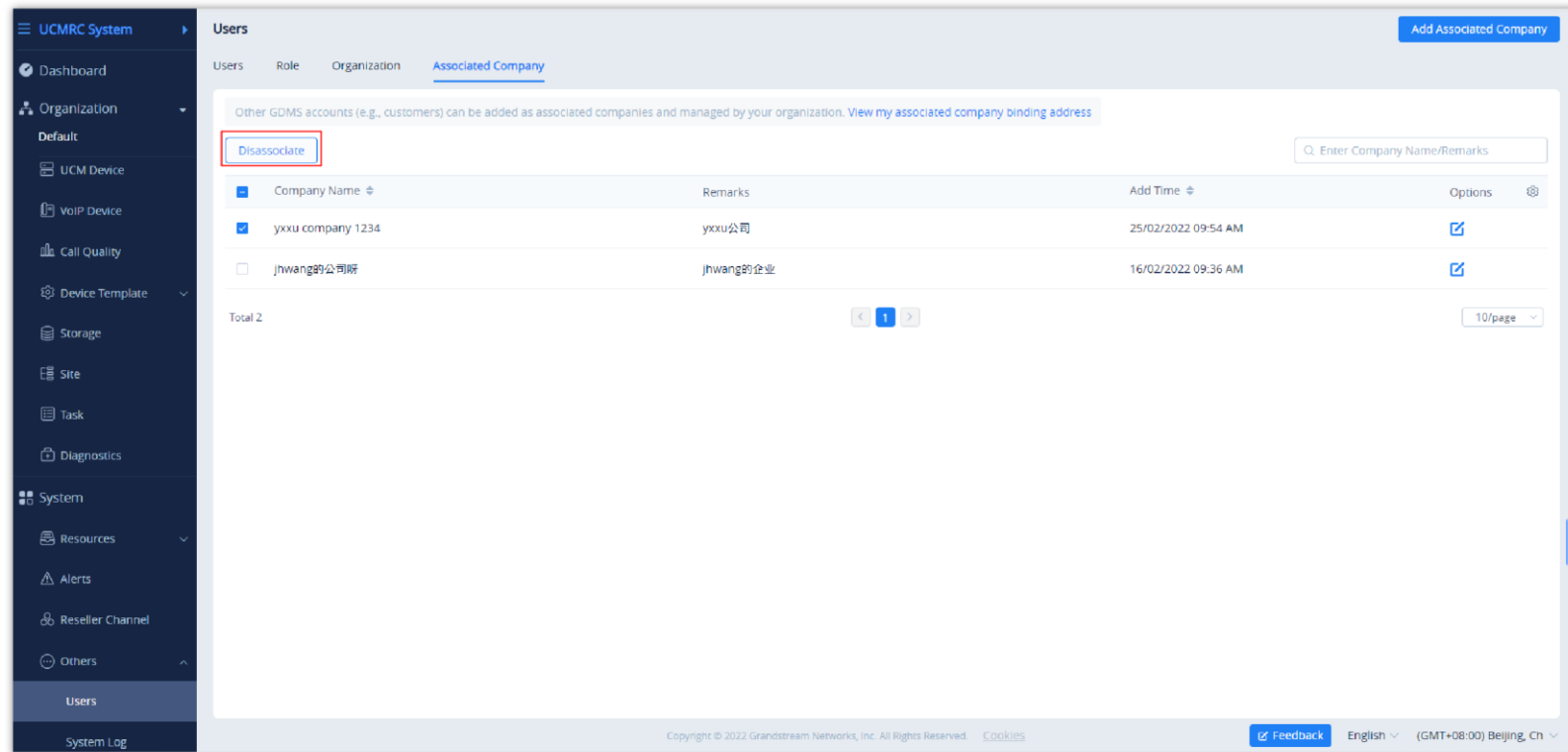
Remarks

Add Time

Edit Associated Company

Disassociate Company

If the user wants to disassociate the relationship with the associated company, the user can select the enterprise and click the button  to disassociate the association relationship.



Disassociate Company

Note

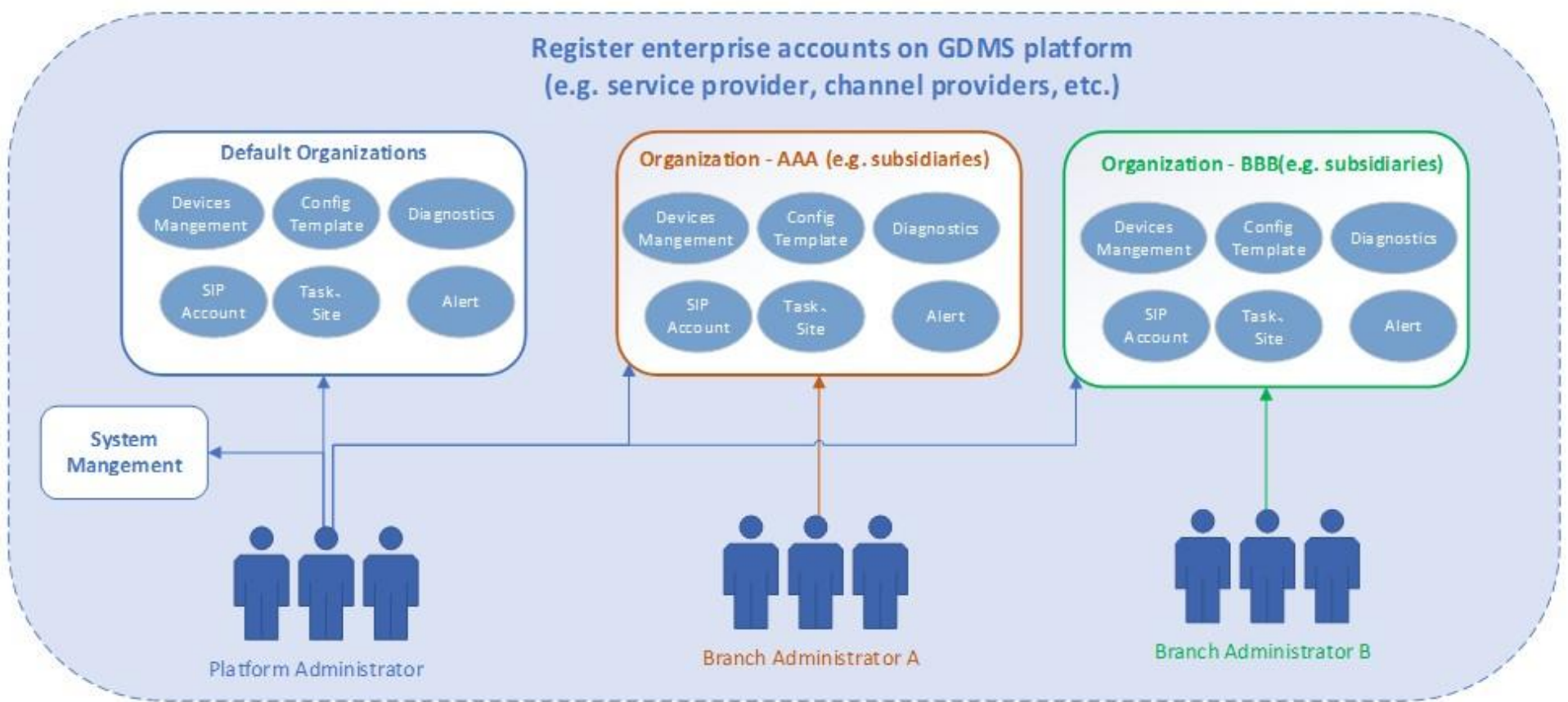
After disassociating the association relationship, the shared organizations will not be affected, the organization can also be managed by the previously associated enterprise.

ORGANIZATION MANAGEMENT

If users want to manage devices in multiple subordinate organizations, users could create multiple organizations (such as customer enterprises, sub-companies), and assign the devices to multiple users to manage separately. The devices, SIP accounts, and other parameters are separated between different organizations. The data in a specific organization can only be viewed and managed by the administrator who has permission.

All devices and data are in the “**Default**” organization by default.

Multiple organizations and administrators:

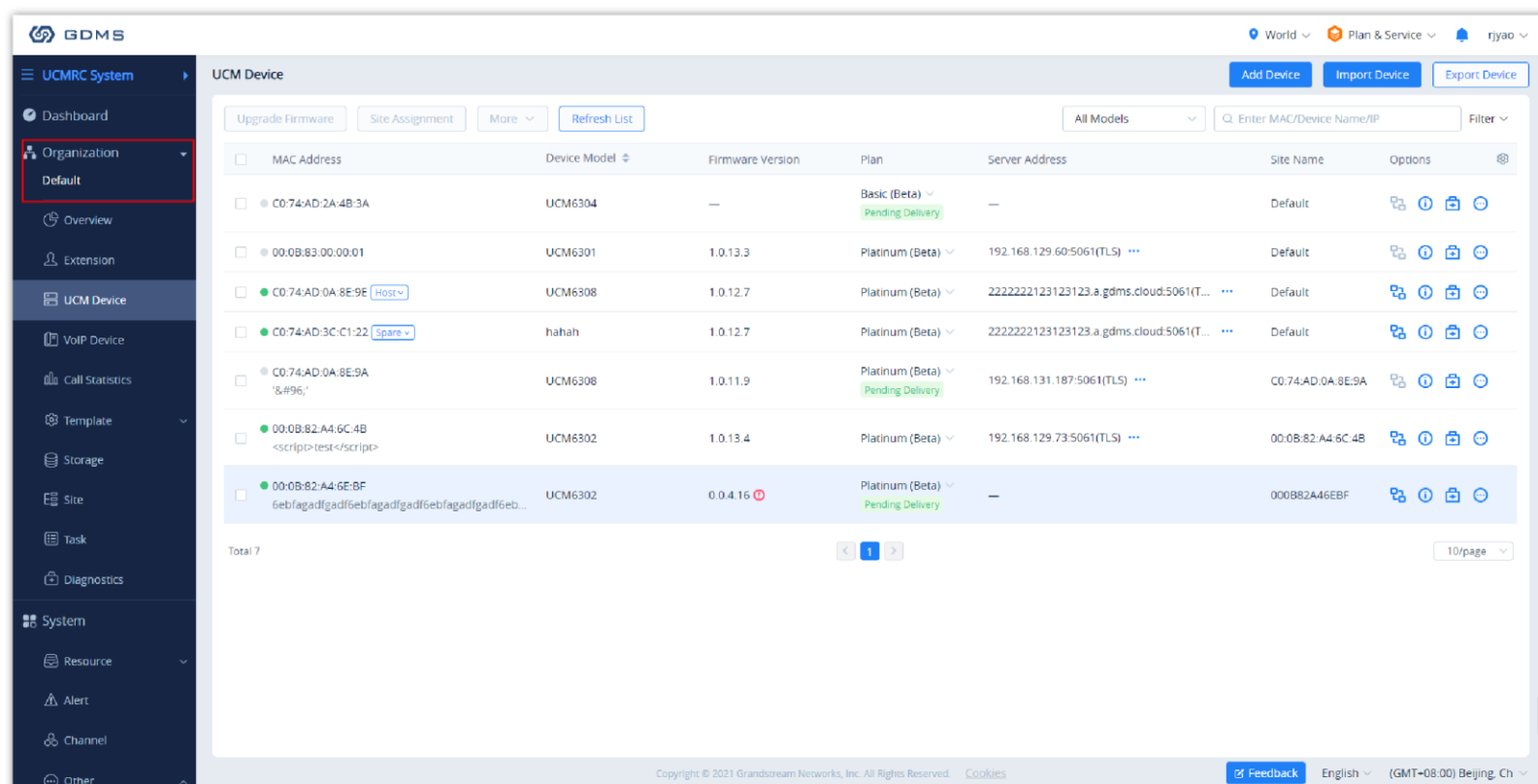


Multiple Organizations and Administrators

Switch Organization

If the user has permissions for multiple organizations, the user could switch to manage different organizations.

1. Click the drop-down box of the Organizations menu at the upper left corner of the page to select the organization the user wants to manage.
2. After switching the organization, the user only could view/edit the Device, SIP Account, Template, and other data under the organization.



Switch Organization

Add Organization

The user could create an organization if the user has permission.

1. On the menu at the right side of the page, select System Management → User Management, and select the “Organization” tab, click the “Add Organization” button at the upper right corner.
2. Fill in the information of the organization as shown in the following figure:

Add Organization ✕

! Create subordinate organization (e.g. customer's company). Devices and SIP accounts for each organization will be managed separately. [View detail](#)

* Organization Name

Assign User

Clone Organization

* Owned Subsystem VoIP System UCMRC System

Description

Add Organization

Organization Name	Input the name of the organization.
Assign User	Select the users who will have permission to manage the organization.
Clone Organization	This is used to select to copy data from other organizations, the data include SIP accounts, model templates, group templates, sites, etc. When the organization is created successfully, the data under the specific organization will be copied to the current organization.
Owned Subsystem	Select the subsystems that the current organization belongs to, including the VoIP system and UCMRC system. If it belongs to multiple systems, the relevant data such as site data, VoIP device, and SIP account information can be shared across systems in the organization.
Description	Input detailed descriptions of the organization.

Table 43: Add Organization

3. Click the Save button to save the organization in the GDMS platform.
4. The system will switch to the newly created organization by default, and the user could add devices to the newly created organization for management.

Edit Organization

Users could edit the organization's information at any time.

1. On the menu at the right side of the page, select System management → User Management, and select the "Organization" tab to view all organizations under the account.
2. Click on the button following the organization name to access the editing page. The user could edit the organization name, the administrator of the organization, and descriptions, as the figure shows below:

Edit Organization

Delete Organization

1. On the menu at the right side of the page, select System management → User Management, and select the “Organization” tab to view all organizations under the account.
2. Click on the Delete button following the organization name, the organization will be deleted completely after confirmation, including the SIP accounts, templates, tasks, diagnostics histories, and other data under the organization.

⚠ If there are devices in the organization, the organization cannot be deleted. Please transfer the devices to other organizations before deleting the organization.

Share Organization

The user can select to share the organizations with the associated enterprises. There are 2 methods of sharing permissions: Co-management and Authorized Management.

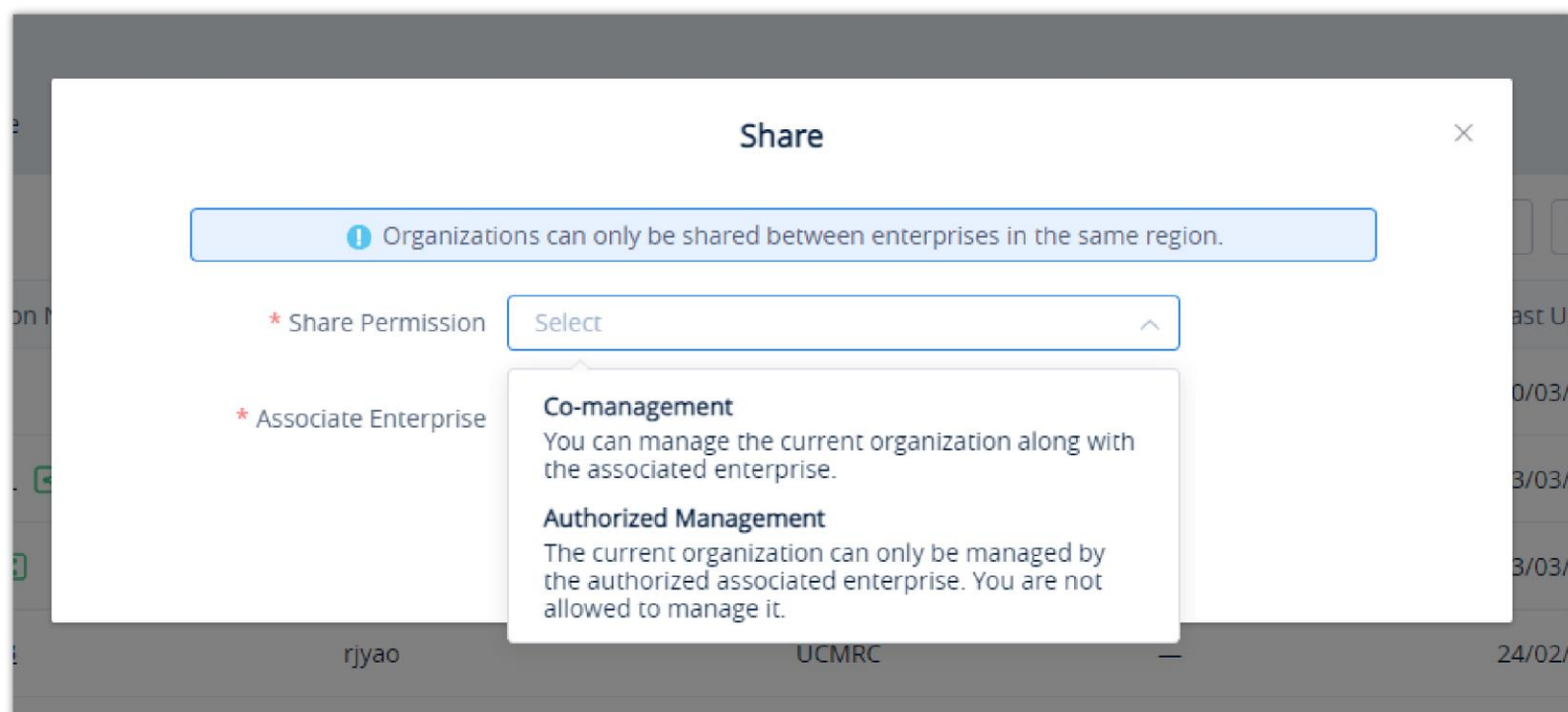
1. On the “Organization” management interface, the user can select the organization that the user wants to share with another enterprise for management and click the button to access the “Share” organization interface. Please see the screenshot below:

Share Organization

<p>Share Permission</p>	<p>There are 2 methods of sharing permissions to another enterprise: Co-management and Authorized Management.</p> <p>Co-management: After sharing the organization, the user can manage the organization with the associated enterprise together. The associated enterprise can manage all devices in the shared organization and view the related data.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the user sets to “Co-management”, the associated enterprise can manage the organization, but the associated enterprise cannot delete the shared organization. • If the user has shared the organization with one associated enterprise for management, the user cannot share the organization again with any other enterprise. <p>Authorized Management: After sharing the organization to the associated enterprise, the user can fully authorize the management permissions to the associated enterprise for management, and the user does not have permission to manage this organization anymore.</p> <p>Note:</p> <ul style="list-style-type: none"> • If the user sets to “Authorized Management”, the user cannot make any operation to this organization, and the organization information will be removed from the user’s “Organization” list. The data in the organization will be transferred to the associated enterprise for management. • After sharing the organization through the “Authorized Management” method, the associated enterprise can manage/edit/delete the organization. • After sharing the organization through the “Authorized Management” method, the associated enterprise can share the organization again with another associated enterprise.
<p>Associate Enterprise</p>	<p>The user needs to select the associated enterprise with which the user wants to share the organization.</p>

Share Organization

2. The user can select the “Share Permission”: “Co-management” or “Authorized Management”.



Share Permission

3. Select the associated enterprise to which the user wants to share the organization.

4. After clicking the “Save” button, the selected organization will be shared with the selected associated enterprise.

5. After the operation steps above, the user can view the organizations which were shared with other associated enterprises and shared with other associated enterprises on the “Organization” list. Please see the screenshot below:

Organization Name	User	Owned Subsystem	Description	Last Updated	Options
Default Organization	yxxu, yxxusub, 333, 444, yxxuchild, zhdeng-re...	VoIP, UCMRC	—	2021/09/28 05:43AM	[Edit]
1111111111	yxxu, jhwangsub	VoIP, UCMRC	www	2022/03/03 08:20AM	[Edit] [Share]
1111111111 共享-共同管理111111_20220224200...	yxxu	VoIP, UCMRC	—	2022/03/16 10:52PM	[Edit] [Share] [Delete]
12123	yxxu, jhwangsub, rjyao@grandstream.cn	VoIP, UCMRC	—	2022/01/07 05:40AM	[Edit] [Share] [Delete]
123123	yxxu	VoIP	—	2022/03/03 08:20AM	[Edit] [Share]
123321-共同管理	yxxu, 111111111@test.com, 222222222@tes...	VoIP, UCMRC	来自yxxu企业的	2022/03/01 12:48AM	[Edit] [Share] [Delete]
aaaaaaaaaaaa	yxxu	VoIP, UCMRC	—	2022/03/03 09:09AM	[Edit] [Share] [Delete]
ceshi	yxxu, 10@test.com, 222222222@tes.com, 1...	VoIP	—	2020/07/30 12:06AM	[Edit] [Share] [Delete]
gateway	yxxu, 333, 383961310@qq.com	VoIP	—	2021/09/01 12:19AM	[Edit] [Share] [Delete]
grp260x	yxxu, 10@test.com, 11@test.com	VoIP	—	2022/02/25 05:33AM	[Edit] [Share] [Delete]

Organization List – Shared Organization

: The label indicates the organization has been shared with another associated enterprise for management together.

: The label indicates the organization is shared with another associated enterprise for management together.

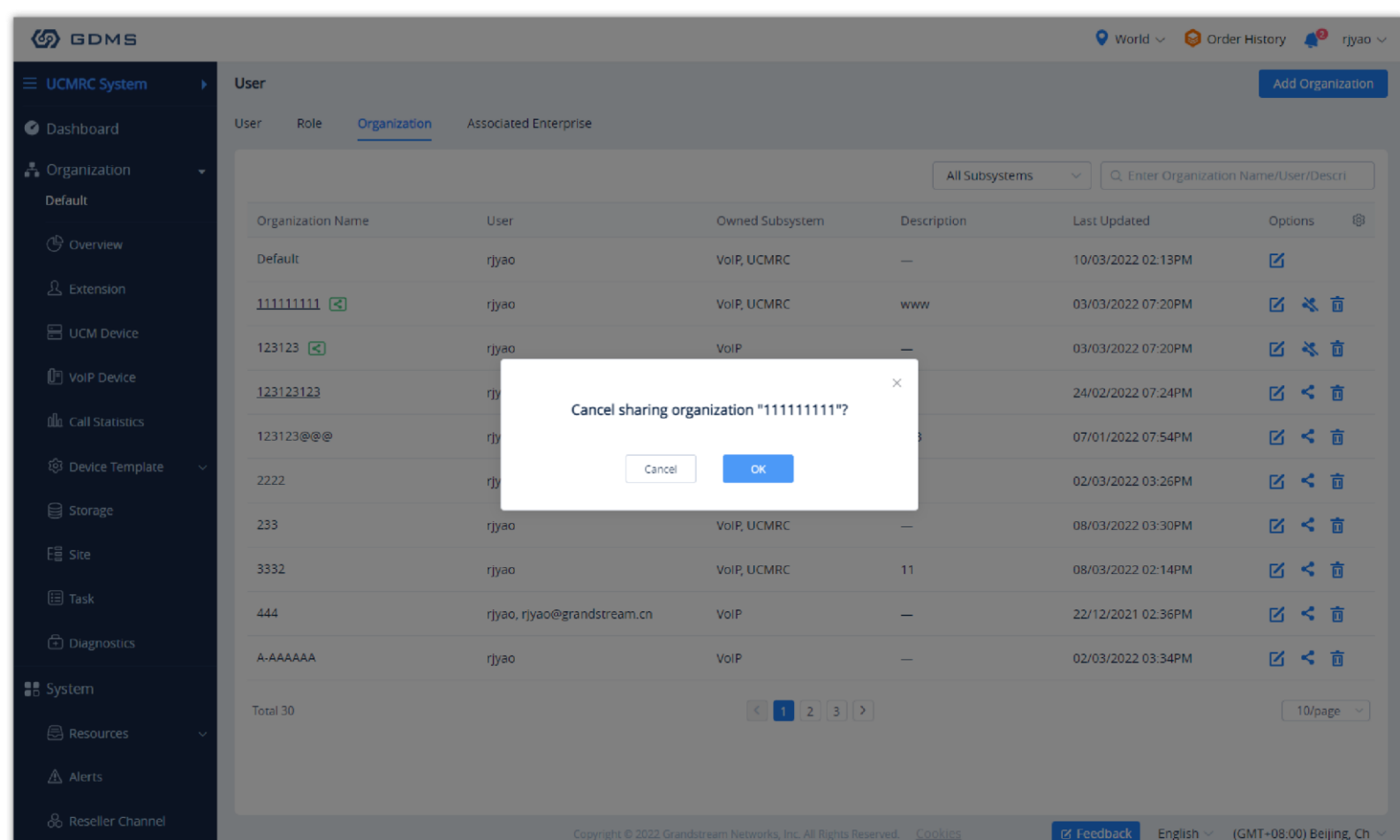
Notes

- The organization can only be shared between the enterprises in the same region. If the selected associated enterprise does not enable the service in the current region, the user needs to inform the associated enterprise to enable the service in the current region so that the organization can be shared with the associated enterprise.
- The user can access the User Management -> Associated Enterprises interface to add the associated enterprises.

Cancel Sharing Organization

The user can cancel sharing the organization with the associated enterprise.

1. On the “Organization” list, the user can select the organization with which the user wants to cancel sharing with the associated enterprise and click the button to cancel sharing with the organization. Please see the screenshot below:



Cancel Sharing Organization


2. After canceling sharing the organization, the user will get the organization management permission back, and the associated enterprise cannot manage this organization anymore.

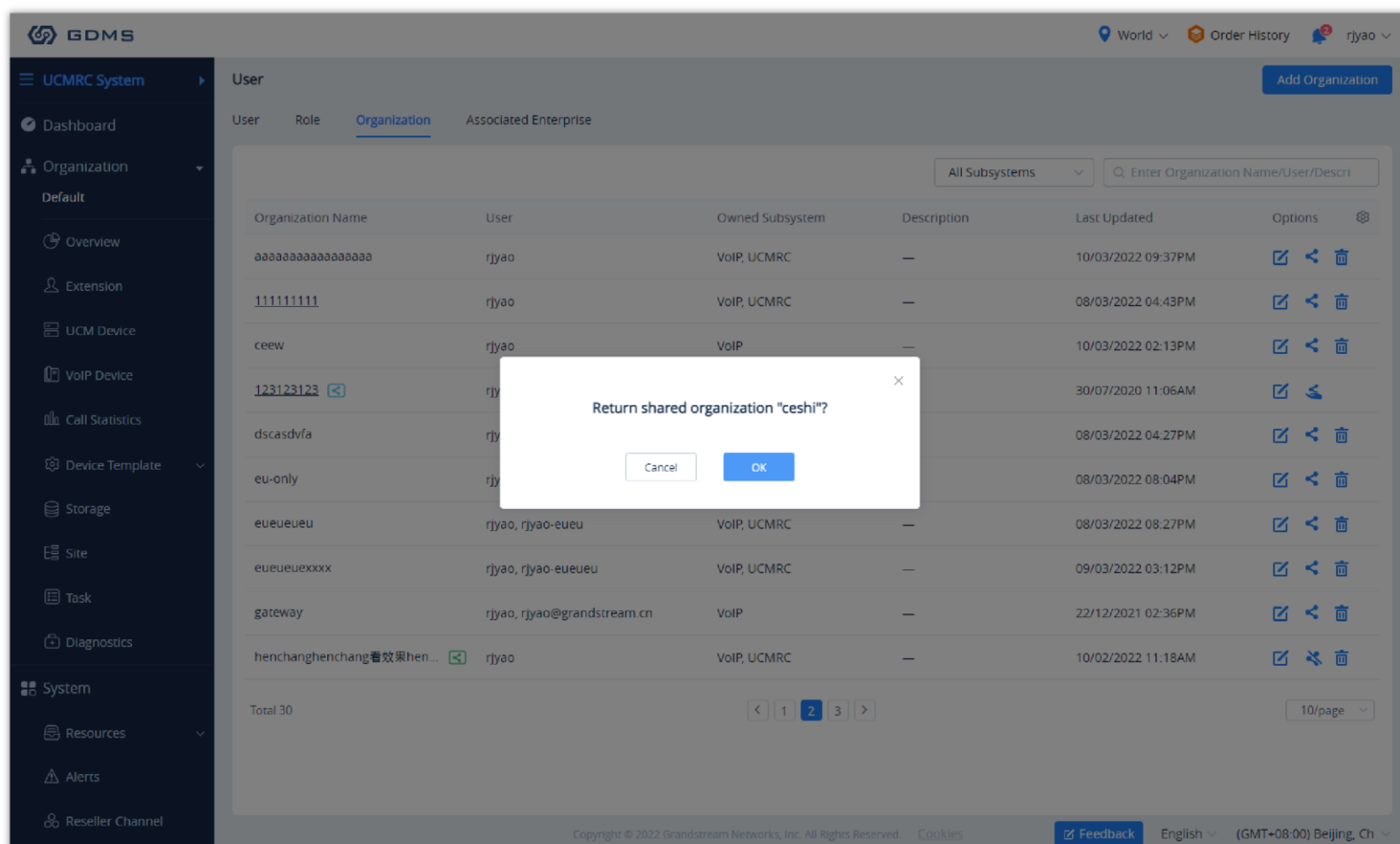
i Notes

- After canceling sharing an organization, the user can share the organization again with another associated enterprise.
- The user can cancel sharing the organization only if the user sets the “Co-management” method when sharing the organization. If the user sets the method to “Authorized Management”, the user does not have any management permission after sharing the organization with the associated enterprise.

Return Organization

After receiving the shared organization, the associated enterprise can return the management permission to the user.

On the “Organization” list, the user can view the received shared organizations and select the organization to which the user wants to return it by clicking the button  as the screenshot shows below:



Return Organization

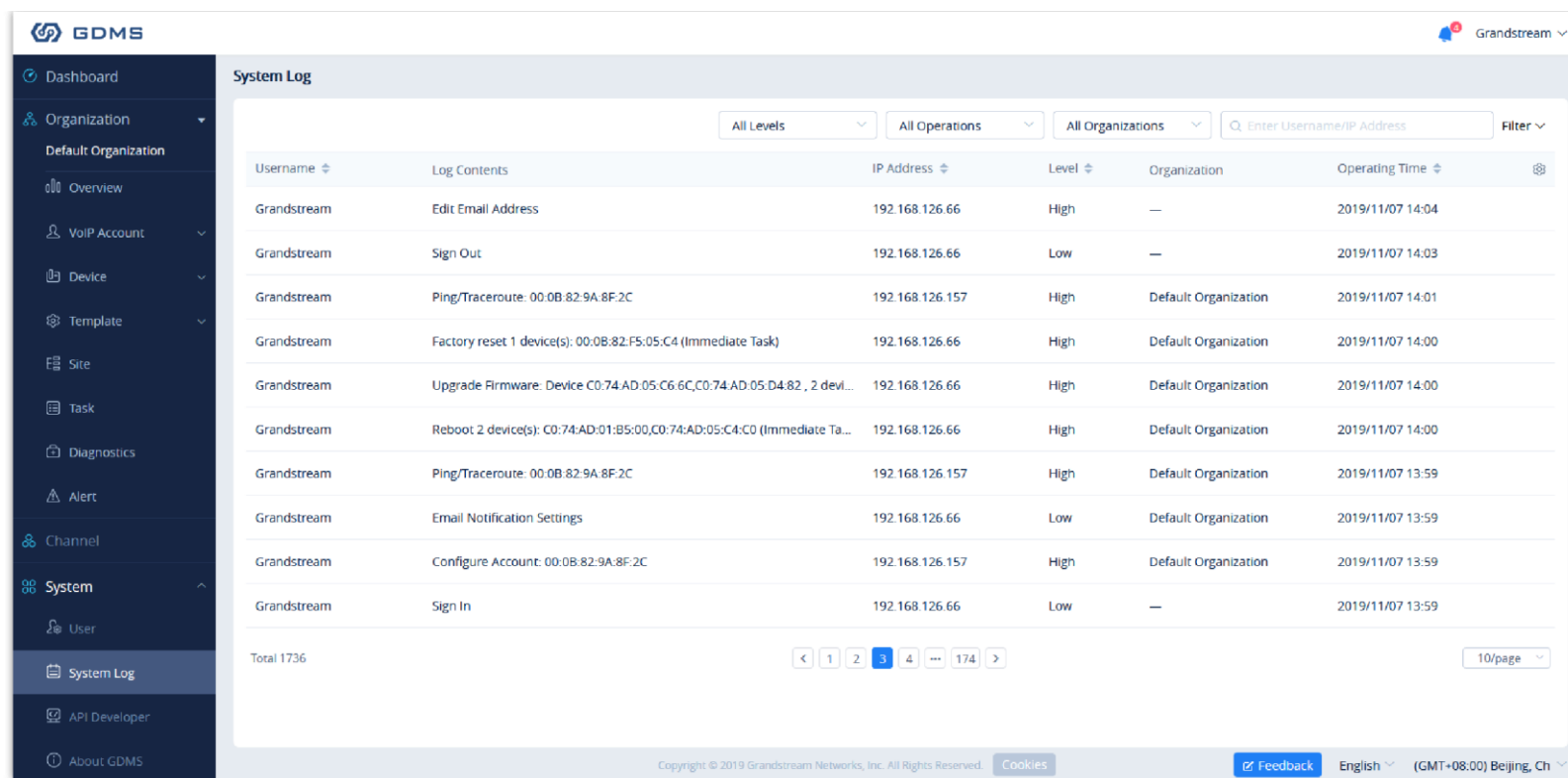
2. After returning the organization, the organization will be removed from the “Organization” list of the associated enterprise, and the associated enterprise will lose the management permission the organization.

SYSTEM LOG

Users could view all operation logs of the system, including the login/logout logs of the user, adding new devices, deleting devices, adding SIP accounts, deleting SIP accounts, firmware upgrading/downgrading logs, updating configuration files for devices, devices factory reset logs, devices diagnostics logs, creating model template logs, etc.


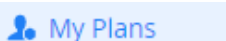
On the menu at the right side of the page, select System management → System Log, and users could view all operation logs of the system. Users could also search the operation logs by level, operation contents, operators, and time.

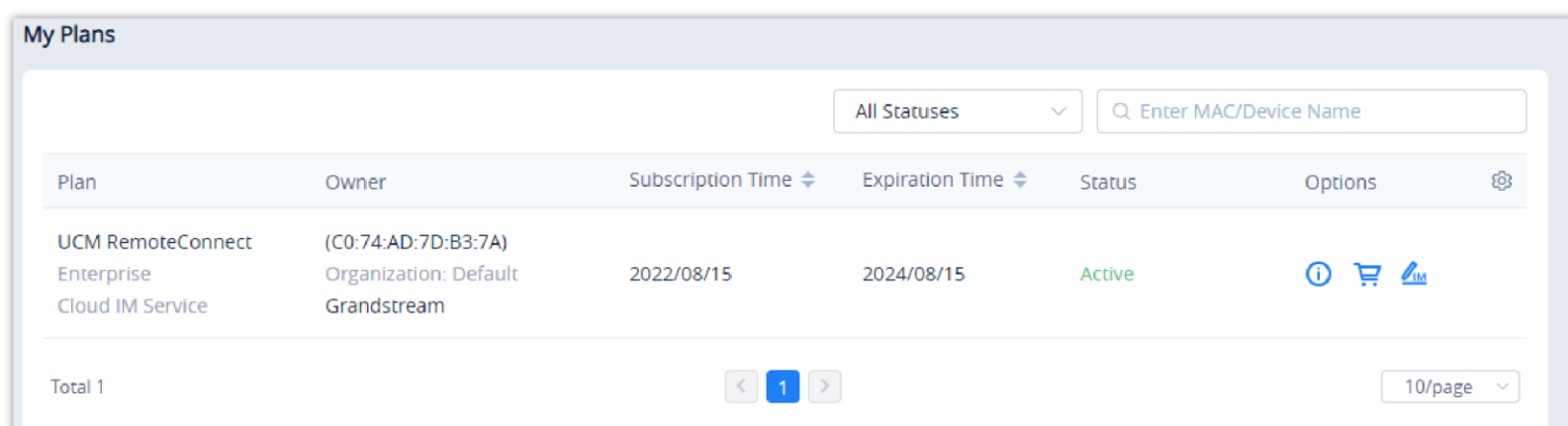
i Users could only view the system logs for the last 30 days.






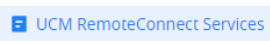
System Log

PLAN & SERVICES

Users can click on the button  in the top right corner to view UCM RemoteConnect plans and the services offered with each plan. When the user clicks on  he/she will be able to view general information about the types of purchased plans.



- To view the history of all purchases, the user should click on .
- To ask for help to purchase a RemoteConnect plan, the user should click on .
- To edit Cloud IM settings, the user should click on .

By hovering over with the mouse pointer and clicking on  you will access the UCM RemoteConnect website, on which the user can find all the details of the services provided by RemoteConnect.

Info

The user can access the UCM RemoteConnect by typing the address <https://ucmrc.gdms.cloud/home> in the address bar in the web navigator.

UCM RemoteConnect Plan

- Supports only for UCM63xx. When the user adds the UCM63xx device to the GDMS platform, the user can apply for a UCMRC advanced plan for a free trial.
- Complete NAT penetration mechanism. Users can use it directly without complicated configuration, so it can ensure the remote communication requirements through external networks (including Wave application in mobile phones/desktop clients for registration/communication through external networks).
- **UCM Remote Management:** There are 3 levels according to the plans, including View device information (e.g. Firmware version), SIP accounts synchronization, remote restarting UCM device, upgrading UCM, and remote access to the UCM Web UI.

- GDMS Cloud Storage service is provided with bonus cloud storage space. This is used for backup configuration files and user data for UCM.
- UCM data statistics report is provided and sent to the administrator through email.
- UCM Cloud IM Plan provides cloud IM communication services for UCM devices. After purchasing this plan, Wave users can use the cloud IM system, and the chat data will be stored in the cloud system.

Notes

- Users can view the details of different plans on the official website.
- Users can only apply for the free trial of the UCMRC advanced plan once for each UCM device that is associated with the GDMS platform. If the user purchases a UCMRC plan which is different from the free trial plan, the current free trial will expire and the purchased UCMRC plan will take effect immediately.
- Please refer to UCM63xx User Guide on the official website for details about Using the remote call function on UCM/Wave application, backup files to GDMS cloud storage space, restoring backup files, and viewing the details of remote call records.

UCM Cloud IM Service

UCM CloudIM Plan provides cloud IM communication services for UCM devices. After purchasing this plan, Wave users can use the cloud IM system, and the chat data will be stored in the cloud system. UCM Cloud IM service is an add-on service of the UCM RemoteConnect plan, and it provides cloud IM communication services for UCM devices. After purchasing a UCMRC plan that contains the Cloud IM service, the Wave user can use the cloud IM system, and the chat data will be stored in the cloud system. UCM CloudIM Plan provides cloud IM communication services for UCM devices. After purchasing this plan, Wave users can use the cloud IM system, and the chat data will be stored in the cloud system.

- Supports unified communication across multiple UCM devices in different regions.
- Provides cloud communication service with high performance, large storage, and multi-function.
- Starts to use UCM CloudIM service, which is not limited by the performance and storage space of UCM devices. Phone calls and messages are not affected by each other.

- The user needs to purchase the UCM RemoteConnect plan which contains the Cloud IM service. After purchasing the plan, the user needs to enable the service on the GDMS platform before using the service.
- After enabling the UCM CloudIM plan in the UCM device, all chat data will be stored in the cloud system. The local chat history will not be viewable.
- Each UCM CloudIM plan can be bound to the multiple UCM devices in a certain enterprise so that the users of the multiple UCM devices can send IM messages, create groups, send meeting notifications to each other, etc.
- When the UCM RemoteConnect plan which contains the Cloud IM service expires, the Wave user

Enable Service

Prerequisite: The UCM plan contains the permission for this function.

1. The user can click the button  to access the “My Plans” list, select a UCM RemoteConnect plan which contains the Cloud IM service, and enable the Cloud IM service on the GDMS platform.

Plan	Owner	Subscription Time	Expiration Time	Status	Options
UCM RemoteConnect Enterprise Cloud IM Service	(C0:74:AD:7D:B3:7A) Organization: Default Grandstream	2022/08/15	2024/08/15	Active	Info, Cart, Edit

My Plans

2. The user can click the button to access the “Edit Cloud IM” interface. Please see the screenshot below:

Edit Cloud IM

<p>Enable Cloud IM</p>	<p>After purchasing a UCMRC plan that contains the Cloud IM service, the user needs to enable the Cloud IM service on the GDMS platform.</p> <p>Note:</p> <p>If the user wants to disable the Cloud IM service which is currently in use and will no longer use it, the data in the Cloud IM server will be cleared after disabling it.</p>
<p>Region</p>	<p>US Region / EU Region</p> <p>Note:</p> <ul style="list-style-type: none"> • It is recommended to select the nearest region to the UCM device. • If the user switches to another region, the data in the Cloud IM server will be cleared.
<p>Enterprise Name</p>	<p>The user can customize the name of the enterprise which will use the Cloud IM service.</p>
<p>Cloud IM Maximum Storage Space</p>	<p>The user can edit the maximum available storage space for the Cloud IM service.</p> <p>Note:</p> <ul style="list-style-type: none"> • The user needs to allocate some space from the cloud storage space for Cloud IM service usage. • The configured storage space must be larger than the space currently used by the Cloud IM service and smaller than the available cloud storage space.

Edit Cloud IM

Note

On the UCM Devices list, the user can click to view the plan information of the selected device and enable the Cloud IM service for the specific device.

MAC Address	Device Model	Firmware Version	Server Address	Plan	Site Name	Options
C0:74:AD:2E:B2:C6 duwei	UCM6302	1.0.15.11	c074ad2eb2c6.b.gdms.cloud:5061(TLS)	Enterprise	Default	
C0:74:AD:45:4E:44	UCM6301	—	—			
00:0B:82:A4:6E:B9 杨玉	UCM6302	1.0.15.5	000b82a46eb9-11			
C0:74:AD:0A:8E:9A '`'	UCM6308	1.0.11.9	000b82a46eb9-11			
C0:74:AD:29:68:00	UCM6308	—	—			

Access Server

c074ad2eb2c6.b.gdms.cloud (Wave App User Guide)
c074ad2eb2c6.b.gdms.cloud:5061 (SIP Configuration Guide)

Storage Space 0B/10.00GB

Total Sessions 64 (Maximum Number of Concurrent Remote Sessions)

Device Plan UCM RemoteConnect - Enterprise (12/05/2024 expires)

10.00GB Cloud Storage Space

Cloud IM Service (12/05/2024 expires)

Pending Delivery

UCM Device -> Enable Cloud IM

3. Click the “Save” button to get the UCM Cloud IM Service, and the user can view the Cloud IM service domain name, service ID, and Key.

Apply successfully!

Service Domain	im.gdms.cloud
Service ID	100008
Service Key	07b2b2775154411232328c7852c
Expiration Time	2021/07/11

You can copy the above information to bind CloudIM plan in UCM device, or bind it in GDMS now.

[More](#)

Bind UCM Device

Not now

Cloud IM Credentials on Web Interface

4. The user can quickly bind the UCM device for the Cloud IM service so that the UCM device can start to apply the Cloud IM service quickly.

Bind UCM Device

A CloudIM account supports binding multiple cross-region UCM devices, and can also be bound on the UCM device management platform.

Enter the department, MAC address of the device and dial prefix ?

US-UCM	C0:74:6D:0A:8E:88 (sqhua)	99	
CN-UCM	C0:74:AD:06:9B:7D	88	

Add Device

Cancel **OK**

Bind UCM Device

Note


The user can also copy the service ID and service key and bind the UCM device to the UCM device management platform. The user can go to the **UCM Web UI à System Settings à Cloud IM** interface and enter the Cloud IM involved information in the blanks. The corresponding IM data are placed in the Cloud IM external server.

Bind UCM Device on Web UI


- The bound UCM device also needs the UCMRC plan which contains the Cloud IM service.
- For the Cloud IM service in the UCMRC plan free trial, when the free trial expires, the user cannot use the Cloud IM service on the GDMS platform, and if the user wants to use the UCM device data in the Cloud IM service in the UCMRC plan free trial, the user needs to transfer the data to the newly purchased Cloud IM service.

View UCM CloudIM Plan Service ID and Key

In “My Plan” interface, find the UCM CloudIM plan, click the icon  to view the service domain name, service ID, and Key of this plan.





Order ID	Plan	Type	Subscription Time	Expiration Time	Options
16311909435628432	Enterprise UCM RemoteConnect Additional 100 Concurrent Remote Sessions Concurrent Remote Sessions 100GB Storage Cloud Storage Space	Upgrade	09/09/2021	14/04/2025	

View Service ID and Key

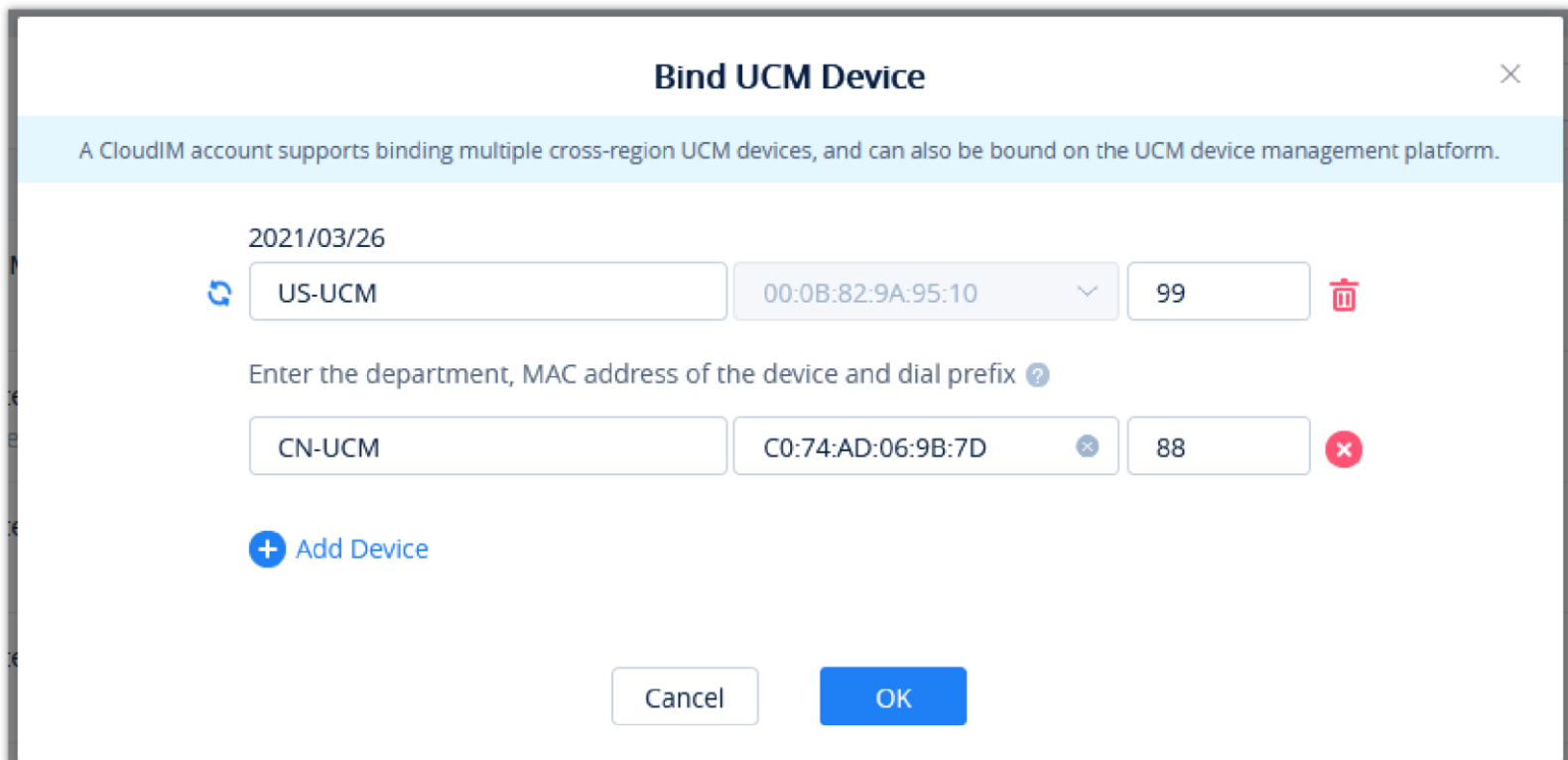
 If the storage space of this plan is full, the user cannot send files and pictures.

Manage Bound UCM Device

1. In My Plan interface, find the UCM CloudIM plan, click the icon .

UCM RemoteConnect Enterprise Cloud IM	UCM6302 (00:08:82:A4:6E:BF) Organization: Default yyy UCM Device: 1 	26/08/2021	26/08/2022	Active	  
---	--	------------	------------	--------	---


2. View the UCM devices which are bound to the UCM CloudIM plan. It allows users to add/delete devices. Please see the screenshot below:



View Bound UCM Devices

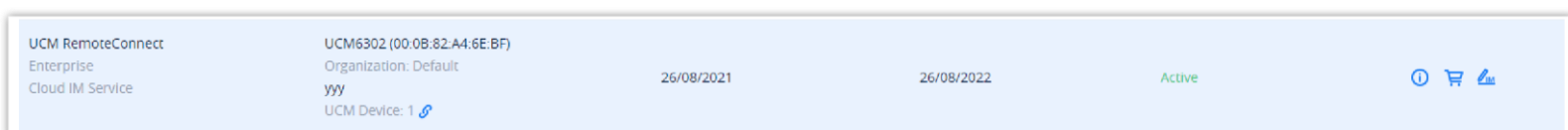
Department Name	Enter the name of the department using this UCM device so that the contact details in the Wave application can be viewed.
UCM MAC Address	<p>Enter the MAC address of the UCM that uses the UCM CloudIM plan. It only supports the UCM devices which have been associated with the GDMS platform.</p> <p>Note:</p> <ul style="list-style-type: none"> For the UCM devices which have not been associated with the GDMS platform, the user can only log in to the UCM management platform to configure the Cloud IM services. The bound UCM device also needs the UCMRC plan which contains the Cloud IM service.
Dial Prefix	<p>The dial prefix required to dial this UCM device must be the same as the trunk dial prefix configured in the UCM. Please refer to the UCM Administration Guide for more details.</p> <p>For example, there are UCM A, UCM B, and UCM C. If the configured prefix of UCM B and C to dial A is 99 (configured trunk), then when the user adds UCM A, the user needs to configure the dial prefix to 99.</p>

Note

If the user adds/deletes/edits department names, the status will show as the icon  until the UCM is online and synchronized, and then the updates will be applied.

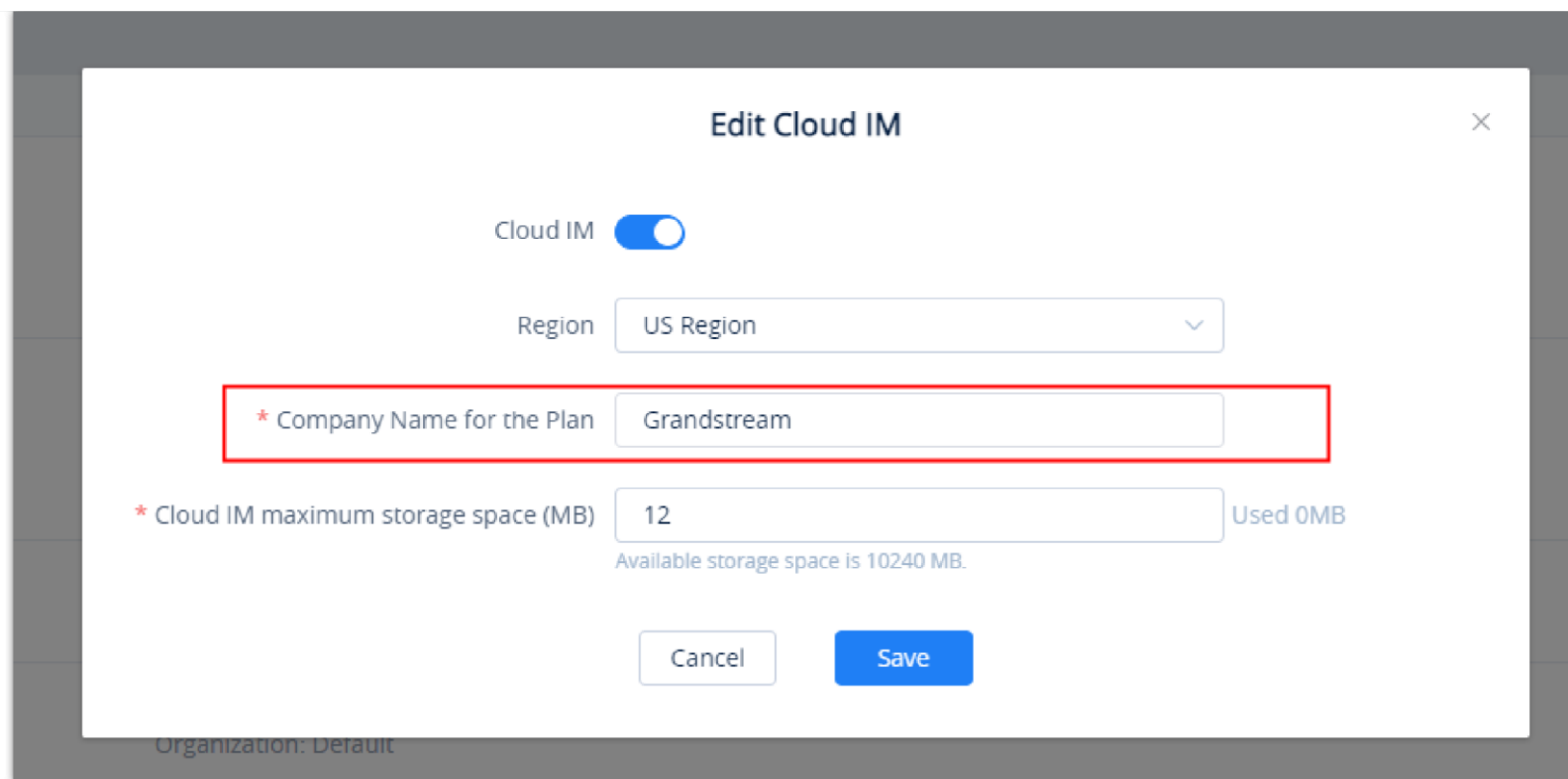
Edit Enterprise Name

1. In My Plan interface, find the UCM CloudIM plan, click the icon .



Find UCM Cloud IM Plan

2. The user can modify the name of the enterprise, and the new name will be applied immediately.

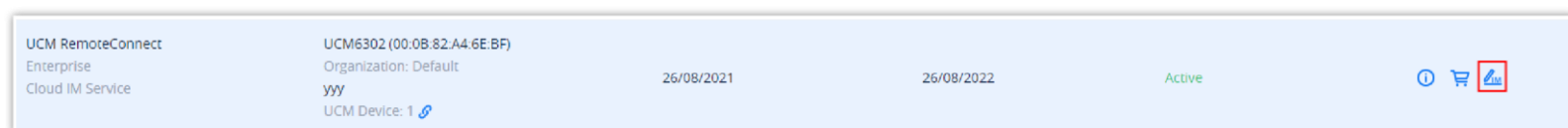


Edit Enterprise

i Currently, the enterprise name is only used to remark the UCM CloudIM plan, and it will not be displayed elsewhere.

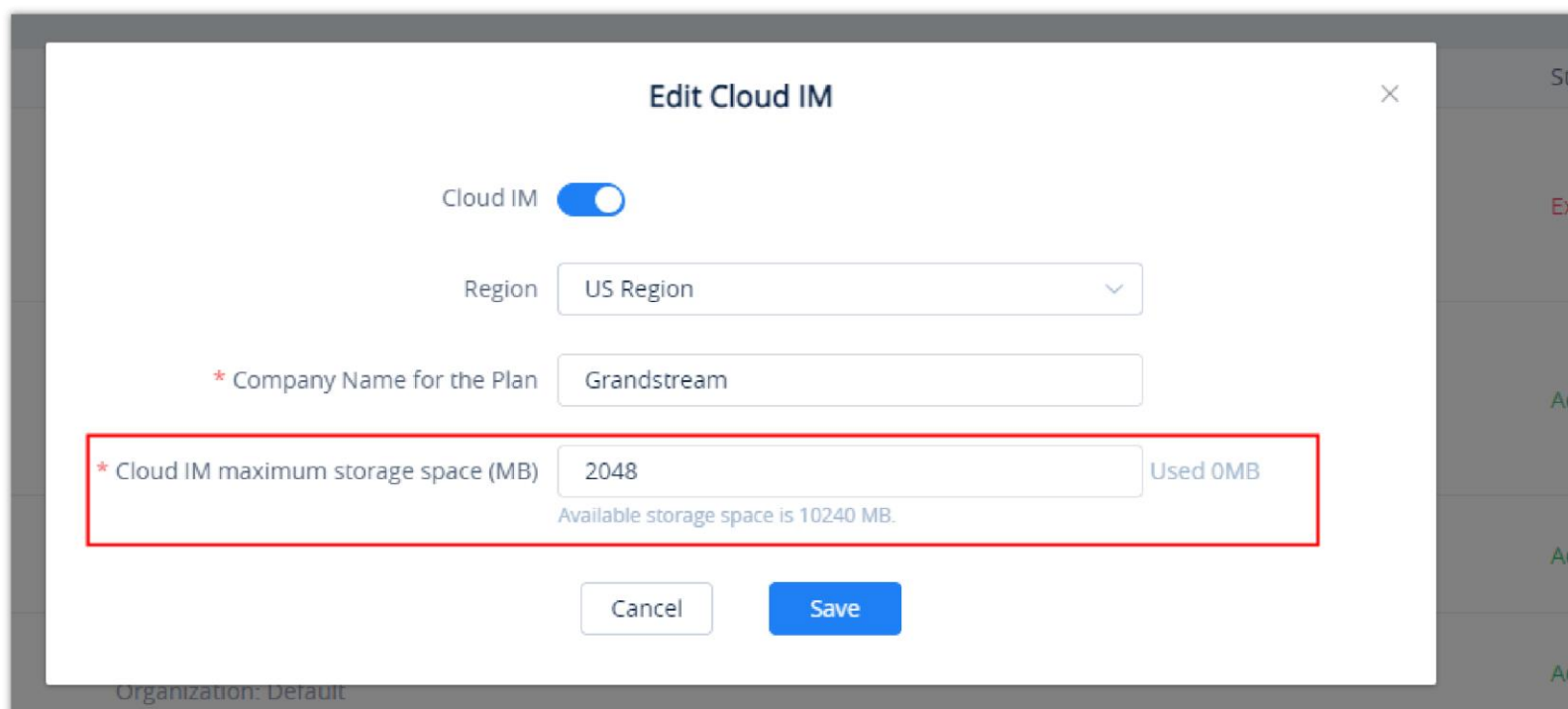
Cloud IM Maximum Storage Space

1. In the “My Plans” interface, find the UCM Cloud IM Service, and click the icon .



Find UCM Cloud IM Plan

2. The user can modify the maximum storage space of the Cloud IM service. The configured Cloud IM service usage storage space must be smaller than the currently available storage space and larger than the currently used storage space.



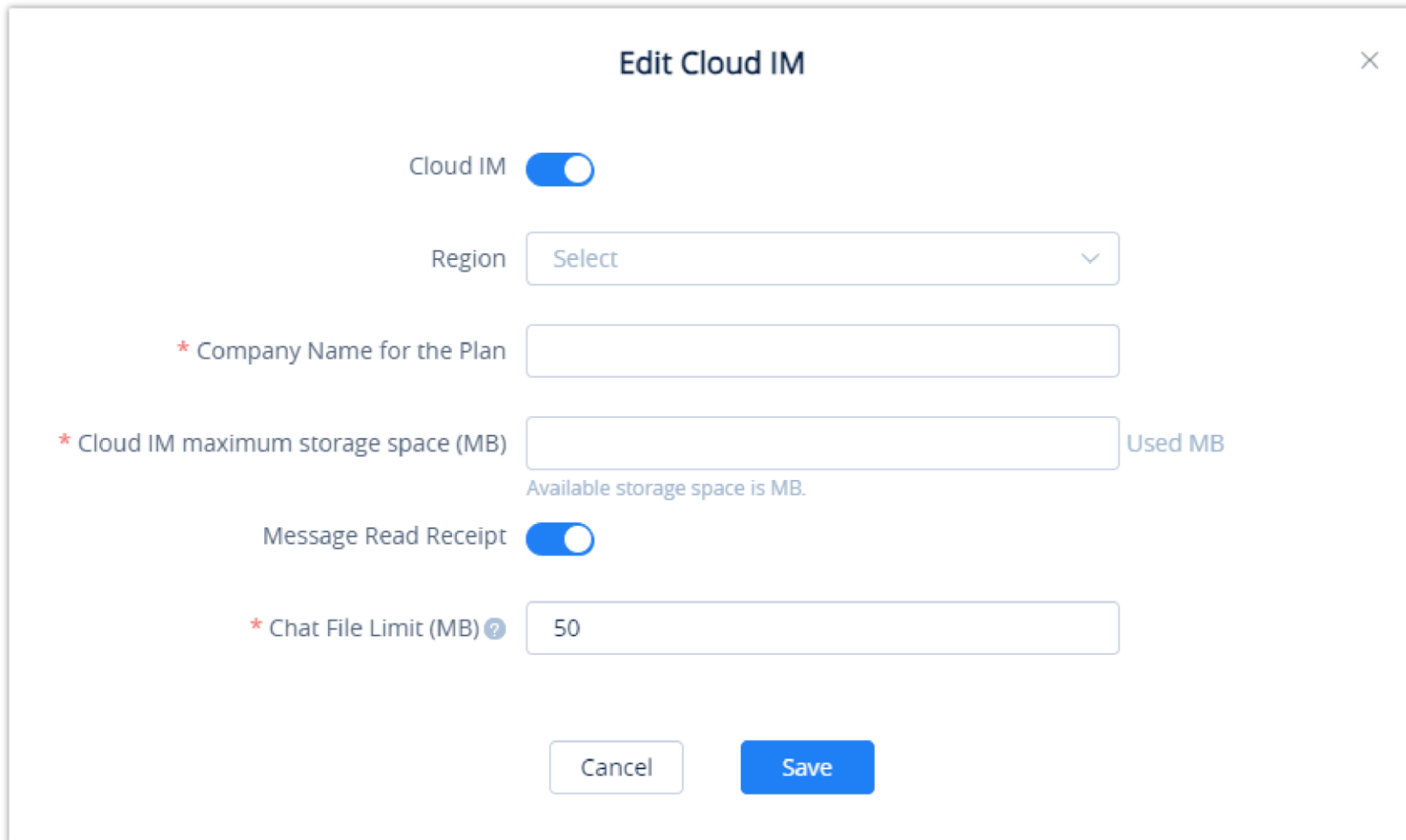
Cloud IM Maximum Storage Space

i Notes

- The user needs to allocate some space from the cloud storage space for the Cloud IM service usage.
- If there is no more available cloud storage space, the user can contact the device distributor to upgrade the UCM RemoteConnect plan to a higher-level plan or purchase an add-on storage space plan to obtain more cloud storage space.

IM File Limit

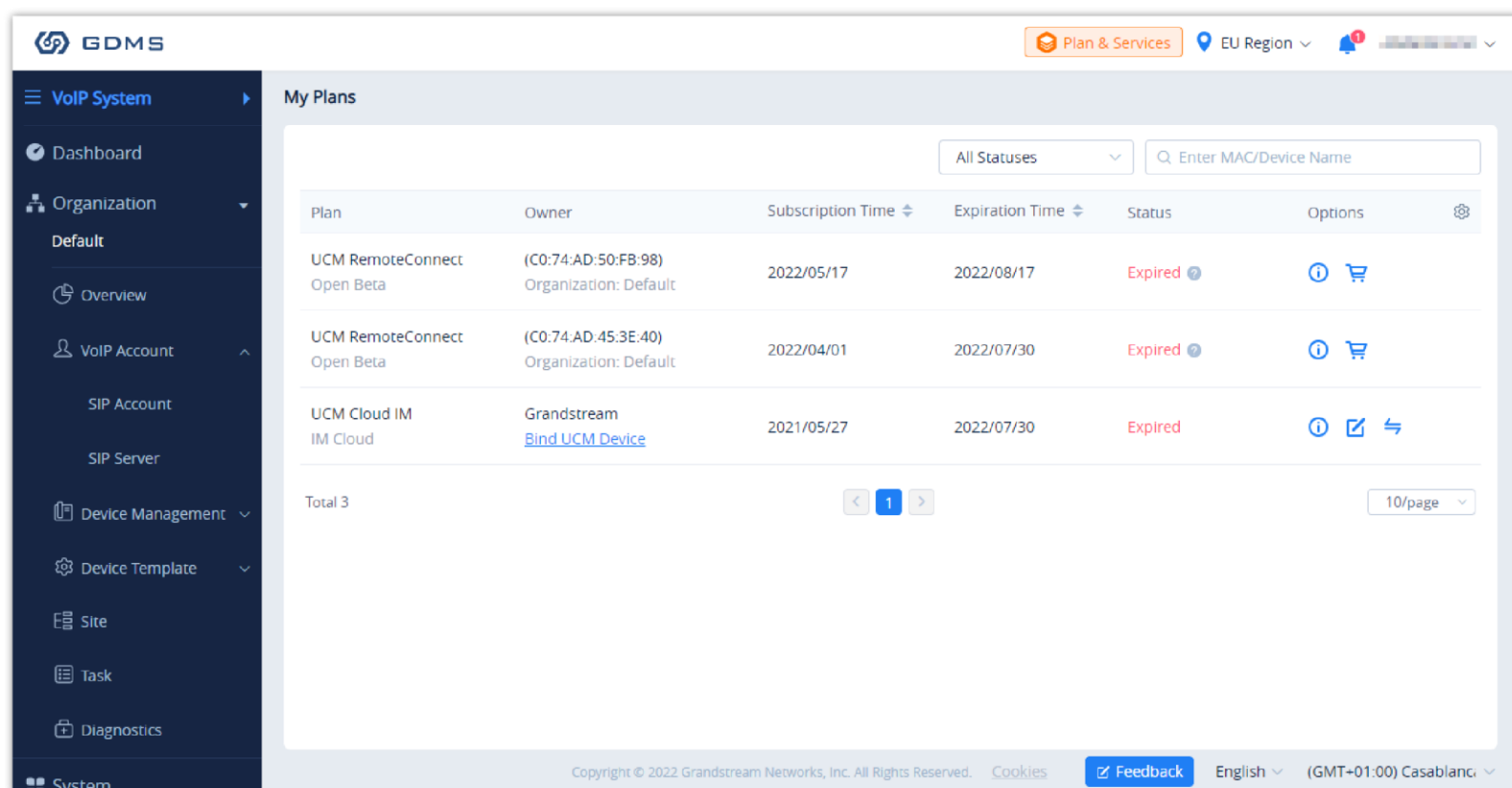
The user can set the maximum limit size of the file that the user can send at one time. To set the limit, please refer to the screenshot below.



- **Chat File Limit (MB):** The single file size limit in the Wave instant chat. The size limit is between 10MB and 100MB. It also cannot be greater than the total size of Cloud IM Maximum Storage Space.

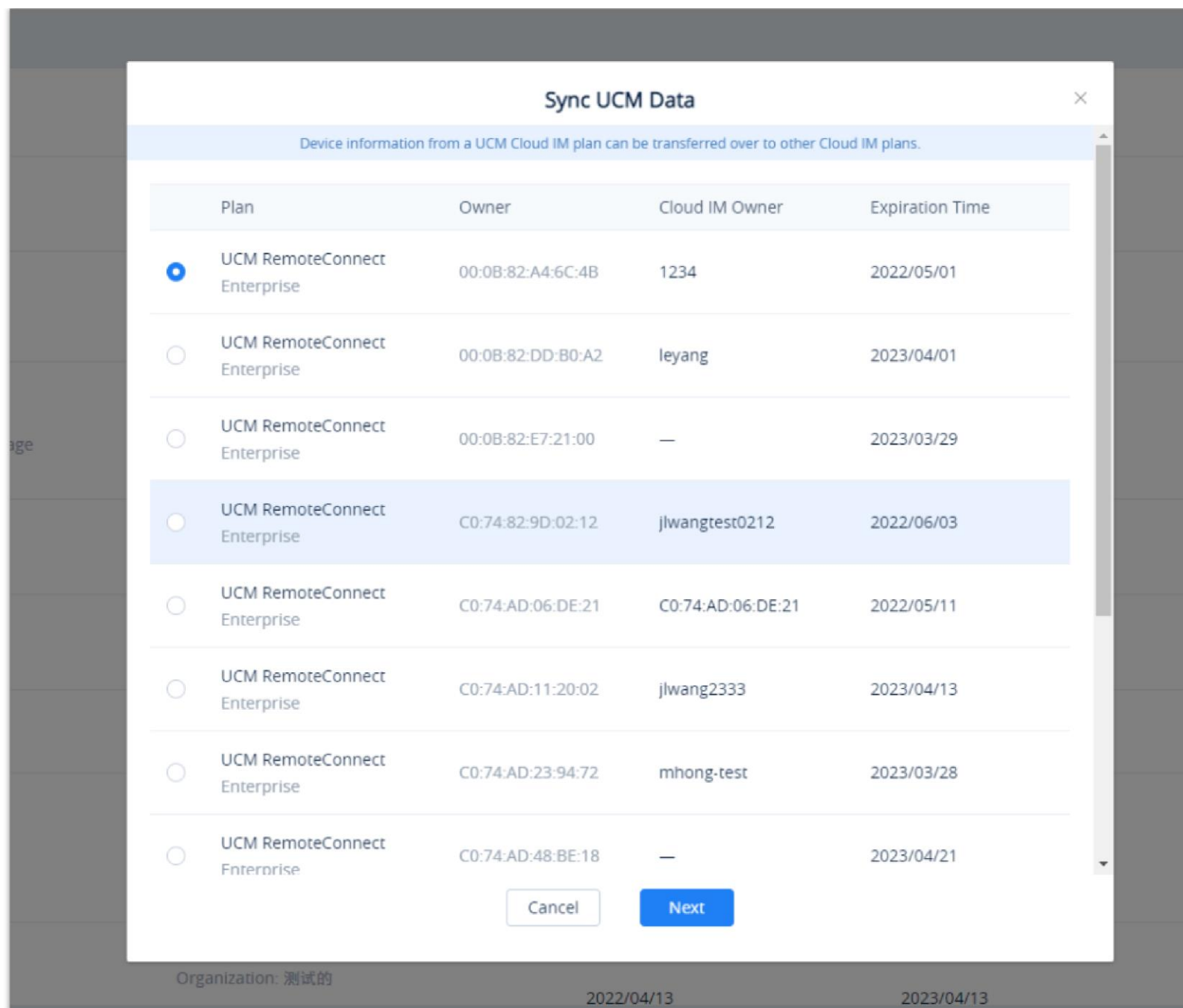
Synchronize UCM Data in Cloud IM Service Free Trial

For the Cloud IM service in the UCMRC plan free trial, when the free trial expires, the user cannot use the Cloud IM service on the GDMS platform, and if the user wants to use the UCM device data in the Cloud IM service in the UCMRC plan free trial, the user needs to transfer the data to the newly purchased Cloud IM service.



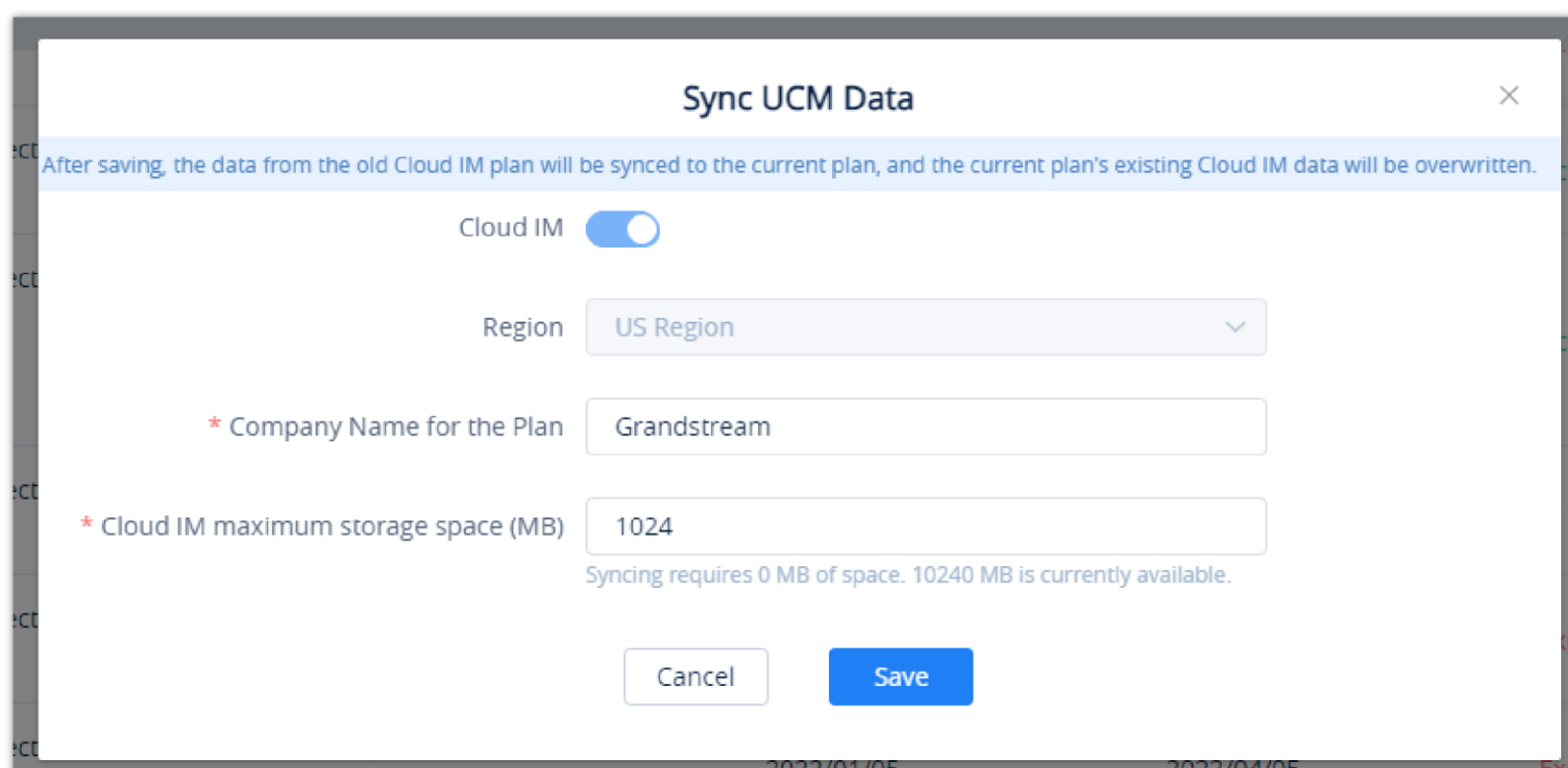
Cloud IM Service Free Trial

1. The user can hover the mouse pointer on [Plan & Services](#) click the button [My Plans](#) to access the “My Plans” interface, select the previous Cloud IM service on the list of the plans, click the button [↔](#) and select the newly purchased Cloud IM service so that the UCM device data in the previous Cloud IM service will be transferred to the newly purchased Cloud IM service.



Sync UCM Data

2. The user needs to select the main plan which contains the Cloud IM service, click the button **Next** to access the Cloud IM service editing interface, and the user can customize the enterprise name, and allocate the maximum storage space for the Cloud IM service.



Sync UCM Data – Edit Cloud IM

3. After clicking the “Save” button, the UCM device data in the previous Cloud IM service will be transferred to the newly purchased Cloud IM service of the UCMRC plan.

Note

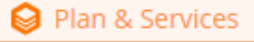
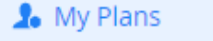

- If the newly purchased Cloud IM service has been enabled and there are some existing data in the service, after transferring the UCM data to the Cloud IM service, the data in the newly purchased Cloud IM service will be cleared.

- If the previous Cloud IM service has expired over 1 month, the synchronized UCM data will not contain the chat history and files, and it will only synchronize the UCM device information.

Purchase Service

Users can purchase one or more UCM RemoteConnect plans and assign them to the corresponding UCM63xx devices. If the user wants to purchase a UCM RemoteConnect plan, the user needs to contact the device distributor to learn more details about the plan and purchase the plan. The GDMS platform does not provide the purchasing service online. Users can purchase one or more UCM RemoteConnect plans and assign them to the corresponding UCM63xx devices.

Note:

If the user cannot contact the device distributor, the user can access the “UCM Devices” list -> Plans or by hovering on  the clicking on  to view the “My Plans” list and click the button  to access purchasing interface. Then, the user can click the “Help” button so that the GDMS platform will inform the device distributor to contact the user as soon as possible.

Purchase Plan


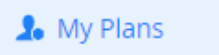
UCM RemoteConnect plans are sold by authorized dealers. [View All Plans](#)
Please contact the dealer from whom you originally purchased the UCM device from to order a UCM RemoteConnect plan.




Ask for Help:

- I want to purchase a UCM RemoteConnect plan, but I cannot contact the dealer.
- I have questions about the plan specifications.
- Other problems

Services Interface

View My Plans

Click on the **Plan and Services**  on the upper right corner, the click on . This page displays all purchased plans by the current enterprise.

Plan	Owner	Subscription Time	Expiration Time	Status	Options
UCM RemoteConnect Enterprise Cloud IM Service	(C0:74:AD:7D:B3:7A) Organization: Default Grandstream UCM Device: 1	2022/08/15	2024/08/15	Active	  

View UCM RemoteConnect Plans

View all plans on the Plans menu:

- Active
- Expired
- About to expire (Less than 15 days from expiration date)
- Invalid (The plan has been revoked or has not been approved)
- In trial (The plan is a free trial plan)

Notes:

1. If the user can see icon , it means the Add-on Plan will expire soon.

UCM Cloud Storage Add-on Plan Expiration

2. If the user can see the icon **Expire Soon**, it indicates that the plan will expire soon. Please renew or upgrade the plan as soon as possible.

View Plan Details



On **My Plans** interface, select a specific plan and click on the button  to view all order history of this device.

- Users could check the ID, Plan, Transaction, Type (upgrade/renew/purchase), Subscription Time, and Expiration Time.
- The user can view all the additional plans under the current plan, as well as the record of orders of the additional plans.
- The plan details contain the main plan and the add-on plan.

My Plans > Plan Details

Cloud IM

Service Domain: _____ Service ID: _____
 Plan Storage: nullB (0B Used —) Service Key: _____


Order ID	Plan	Type	Subscription Time	Expiration Time	Options
UCMRC-1874	Enterprise UCM RemoteConnect	Upgrade	2022/08/15	2024/08/15	
UCMRC-1020	Enterprise UCM RemoteConnect	Subscribe	2022/04/18	2022/07/18	

Total 2 10/page

View Plan Details

Export Receipt



The user can download the receipt for a specific plan renewal or upgrade from the plan details page.

1. View all plans for My Plans menu.
2. Select  of the plan of which you want to export the receipt

My Plans > Plan Details

Cloud IM


Service Domain: _____ Service ID: _____
 Plan Storage: nullB (0B Used —) Service Key: _____

Order ID	Plan	Type	Subscription Time	Expiration Time	Options
UCMRC-1874	Enterprise UCM RemoteConnect	Upgrade	2022/08/15	2024/08/15	
UCMRC-1020	Enterprise UCM RemoteConnect	Subscribe	2022/04/18	2022/07/18	

Total 2 10/page

Export Receipt

The receipt will be downloaded as a PDF file and below is an example of a receipt



UCM RemoteConnect Service Order Receipt

Service Name: UCM RemoteConnect Service
Order Date: Aug 15 2022
MAC Address: C0:74:AD:7D:B3:7A
Device Type: —

Transaction	Plan Name	Service Period
Upgrade	◆ Enterprise	Aug 15 2022 - Aug 15 2024

UCM RemoteConnect Order Receipt

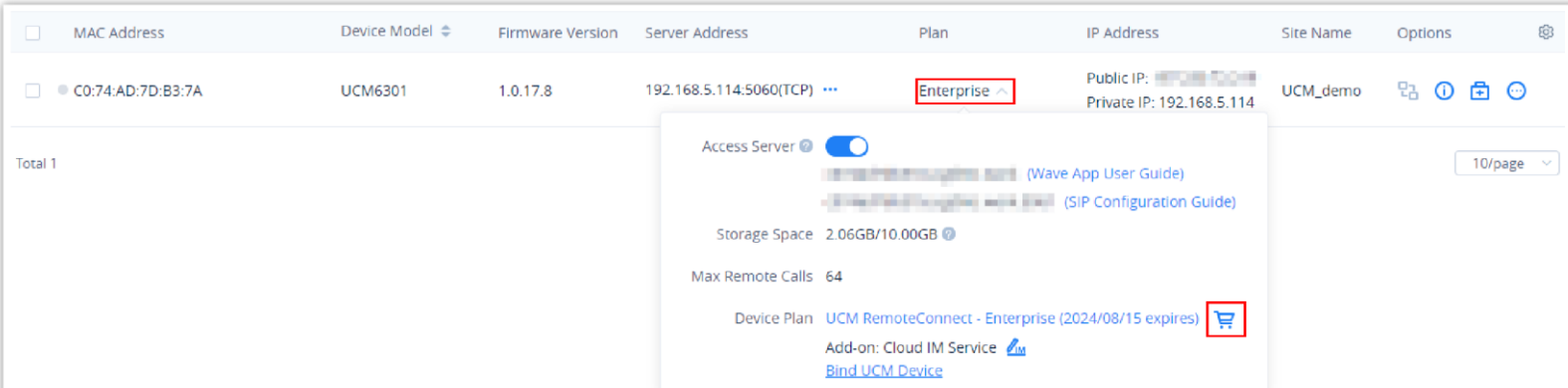
Renew/Upgrade Plan

If the user wants to renew the current UCM RemoteConnect plan or upgrade it, the user needs to contact the device distributor to learn more details about the plan and renew or upgrade the plan.

Note

If the user cannot contact the device distributor, the user can access the “My Plans” interface, select the UCM device which the user wants to renew the plan for, and click the button to access the purchasing page.

1. Please click on the name of your plan, then select 



Renew Plan

2. This window will appear, please select “I want to purchase a UCM RemoteConnect plan, but I cannot contact the dealer.”

Purchase Plan

UCM RemoteConnect plans are sold by authorized dealers. [View All Plans](#)

Please contact the dealer from whom you originally purchased the UCM device from to order a UCM RemoteConnect plan.

Ask for Help:

I want to purchase a UCM RemoteConnect plan, but I cannot contact the dealer.

I have questions about the plan specifications.

Other problems

Cancel
OK

Ask for Help

3. Fill in the form with the corresponding information:

Please fill in the UCM RemoteConnect plan you prefer to purchase and the contact information.

* Device MAC Address

* UCM RemoteConnect Plan [View plans](#)

* Company Name

* Your Name

* Phone Number

* Email Address

* Job Title

* Describe the problem

Submit

Contact Form

Device MAC Address	Enter the address MAC of the UCM device that you wish purchase/renew/upgrade the RemoteConnect plan for.
UCM RemoteConnect Plan	Choose the RemoteConnect plan that you want to purchase/renew/upgrade to. For more information about RemoteConnect plans, please visit: https://ucmrc.gdms.cloud/plans
Company Name	Enter the name of the company.
Your Name	Enter your full name.

Phone Number	Enter your phone number.
Email Address	Enter your email address.
Job Title	Enter your job title.
Describe the problem	Give details of the problem you have encountered.

Plan Expiration Notice

If the plan in the account will be expired after 15 days or already expired, the user will receive a notification through registered email.

An example of plan expired email notification:

The screenshot shows an email from GDMs. The header includes the GDMs logo and the name 'Hi, jyang123'. The main body of the email states: 'The following UCM RemoteConnect plan has expired. Corresponding services are no longer available.' Below this is a table with the following data:

Plan	Expiration Date	Owner	Directions
Extra 50GB Cloud Storage	2022/05/24	C0:74:AD:12:03:35 UCM6202 Organization: 3—ytesy	Exceeding storage space:0GB

Below the table, there is a tip in orange text: 'Tip: When the plan expires, the files that exceed the storage space will be deleted. Please backup in advance. If the UCM device is set with a custom access address, the address will be deleted. You can click [here](#) to see more details about the effect of plan expiration.' This is followed by a link: 'You can log in <https://www.gdms.cloud/plan/myPlan> to view the plan details and contact the device channel partner to renew the plan.' At the bottom, it says 'This is an automatically generated email. Please do not reply.' The footer contains 'About Us | Contact Us' and 'Copyright © 2022 Grandstream Networks, Inc. All rights reserved.'

Plan Expiration Notice



- Once the plan expires, the files that exceed the maximum storage space will be deleted after 7 days. Please download the files as soon as possible or renew them in advance.
- Once the plan expires, if the user configures a custom access server address for the UCM device, the custom access server address will be deleted after 7 days.
- If the previous Cloud IM service has expired over 1 month, the synchronized UCM data will not contain the chat history and files, and it will only synchronize the UCM device information. If the user renews the UCMRC plan which contains the Cloud IM service within 1 month, the chat history and files will be preserved.

MULTI-FACTOR AUTHENTICATION

GDMS Multi-Factor Authentication (MFA) is the simple and best security practice method that adds extra protection to account username and password. When MFA is enabled, the user will be required to enter the login username and password (the first security method) and an authentication code (the second security method) from the MFA device when they log on to the GDMS platform. These multiple methods will improve the security of the settings and resources of your GDMS account.

Users can purchase supported physical devices or virtual MFA devices to enable MFA for GDMS accounts.

- **Virtual MFA Device**

Virtual MFA Device is an application that runs and simulates physical devices on mobile phones or other devices. Virtual MFA device will generate a six-digit code based on a one-time time-synchronized cryptographic algorithm.

When logging into the GDMS platform, the user must type in a valid code from the specific device. Each virtual MFA device assigned to the user must be unique. The user cannot type in the code with another user's virtual MFA device code for authentication. Since the virtual MFA device may be executed on an unsafe mobile device, it may not provide the same level of security as a physical MFA device.

- **Physical MFA Device**

A physical MFA Device is a device that can generate a six-digit code based on a one-time time-synchronized cryptographic algorithm.

When logging into the GDMS platform, the user must type in a valid code from the specific device. Each physical MFA device assigned to the user must be unique. The user cannot type in the code with another user's physical MFA device code for authentication.

MFA Device Standards

	Virtual MFA Device	Physical MFA Device
MFA Device	Refer to table 2	Purchase physical MFA device
Cost	Free	Price by supplier
Physical Device Standard	Use your smartphone/tablet/PC which can execute applications that support open TOTP standards to install virtual MFA device	The physical device supports open TOTP standards. It is recommended to use the devices from Microcosm manufacturer .
Function	Support multiple tokens on a single device	The financial service institutions and IT enterprises use the same model of the device.

MFA Device Standards

Download Virtual MFA Application

Install virtual MFA application for your smartphone/tablet/PC from your device's app store. The following table lists some applications that are suitable for multiple kinds of smartphones.

Android	Google Authenticator ; Authy 2-Factor Authentication
----------------	--

iPhone	Google Authenticator; Authy
Windows Phone	Authenticator

Suitable Applications

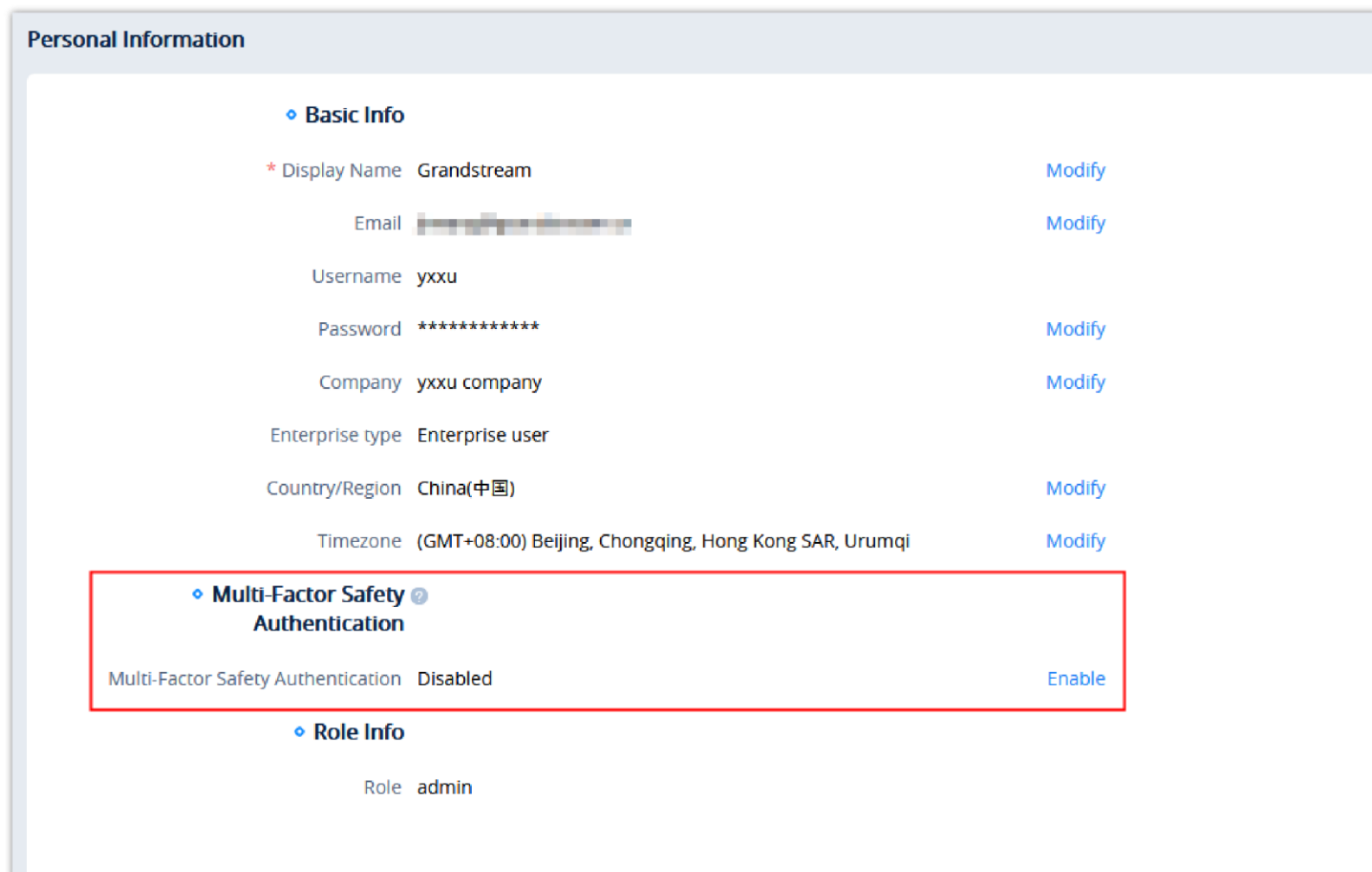
Enable MFA Device

To enhance security, it is recommended that users can configure Multi-Factor Authentication (MFA) to help protect GDMS resources. Users can enable MFA for GDMS accounts.

Authenticator App

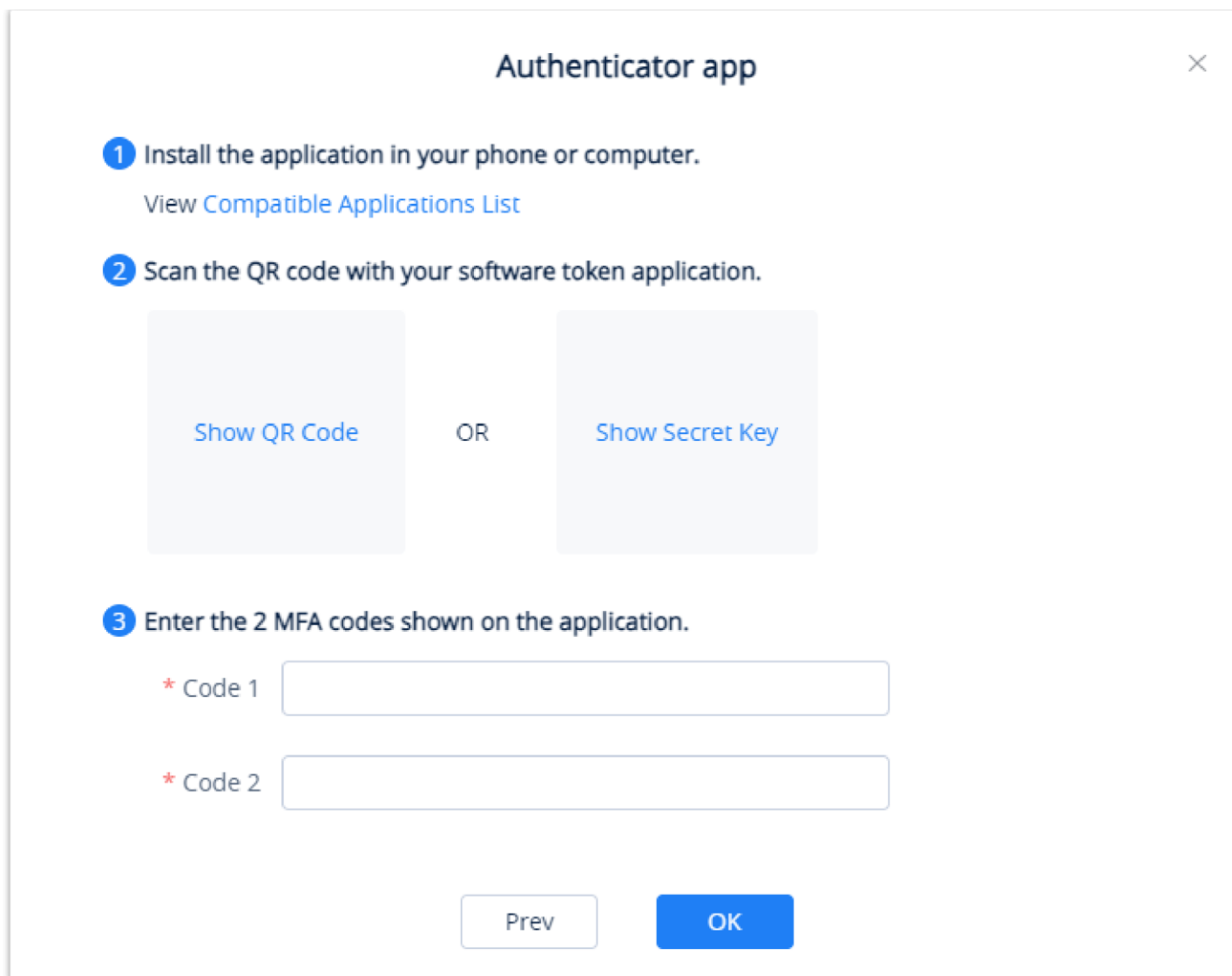
Prerequisite: Users need to install a virtual MFA application on the smartphone/tablet/PC before enabling a virtual MFA device.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page:



Access Personal Information Page

2. Click to enable the “**Multi-Factor Safety Authentication**” option and select to use “**Virtual MFA Device**” on the pop-up window, then click the “**Next**” option to continue.
3. Then, it will generate and display the configuration information of the virtual MFA device, including QR code graphics. This figure represents the configuration of the virtual MFA device as a secret key, users can scan the QR code to finish setting the virtual MFA device. Users can also input the secret key manually into the smartphone/tablet/PC to finish setting virtual MFA devices if your smartphone/tablet/PC does not support scanning QR codes.



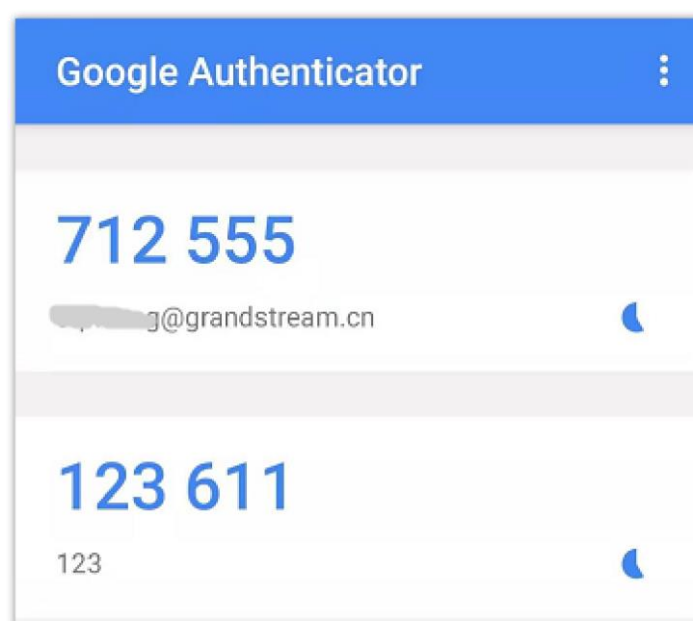
Scan QR Code

4. Open virtual MFA application in your smartphone/tablet/PC, ensure that the application in your smartphone/tablet/PC supports scanning QR code, and then perform one of the following actions below:
- If the MFA application in the smartphone/tablet/PC supports scanning QR code, the user can use the application to scan QR code to finish setting virtual MFA device. For example, the user can select the camera icon or scanning QR code option to use the device's camera to scan the QR code.
 - If the smartphone/tablet/PC does not support scanning QR codes, the user can click on the “**Show secret key**” option and input the private secret key manually in the MFA application.

i If a virtual MFA application supports multiple virtual MFA devices or accounts, the user can select the appropriate options to create new virtual MFA devices or accounts.

5. When the operations above are completed, users can use the virtual MFA device to generate one-time passwords.

In the MFA secret code box Code 1, the user enters the one-time password which is displayed in the virtual MFA device currently. Then, wait for 30 seconds so that the virtual MFA device will generate a new one-time password, the user enters the second one-time password in the MFA secret code box Code 2.



Input MFA Secret Code

6. Click on the “Start Verification” option to start to verify the password. When the verification is passed, the GDMS account and the virtual MFA device have been bound successfully. When the user tries to log in to the GDMS platform, the user must input the MFA device code.



- When the secret code is generated, the user needs to use the secret code to proceed verification process immediately. If the user does not submit the secret code and waits for a too long time, the one-time secret code (TOTP) may be expired. Then, the user may need to start the verification process again from the beginning.
- The user can only bind the virtual MFA device to a single account.

Hardware TOTP Token

Prerequisite: The user needs to purchase the physical MFA device before using this verification function.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page.
2. Click to enable the “**Multi-Factor Safety Authentication**” option and select to use “**Physical MFA Device**” on the pop-up window, then click the “**Next**” option to continue.
3. Enter the interface below to bind the physical MFA device with the GDMS account:

Hardware TOTP token

1 Enter the secret key received from the company. [How to obtain secret key?](#)

2 Press the button on the device and enter the 6-digit code.

3 Wait 30 seconds then press the button to enter the 6-digit code.

Prev OK

Hardware MFA Device Authentication

4. Input the secret key of the device. Please contact the manufacturer for the secret key.



The key format is required to be “**DEFAULT HEX SEEDS**” (seeds.txt), or “**BASED32 SEEDS**”.

Examples:

HEX SEED: B12345CCE6DA79B23456FE025E425D286A116826A63C84ACCFE21C8FE53FDB22

BASE32 SEED: WNKYUTRG3KE3FFTZ7UIO4QS5FBVBC2HJKY6IJLCP4QOH7ZJ12YUI====

5. In the MFA secret code box Code1, the user enters the six-digit one-time password which is displayed in the physical MFA device currently. The user needs to press the button on the front of the physical MFA device to display the secret code. Then, wait for 30 seconds and press the display button on the front of the physical MFA device again, so that the MFA device will generate the second six-digit one-time password. The user needs to enter the second one-time password in the MFA secret code box Code 2.



Physical MFA Device

6. Click on the “Start Verification” option to start to verify the password. When the verification is passed, the GDMS account and the physical MFA device have been bound successfully. When the user tries to log in to the GDMS platform, the user must input the MFA device code.

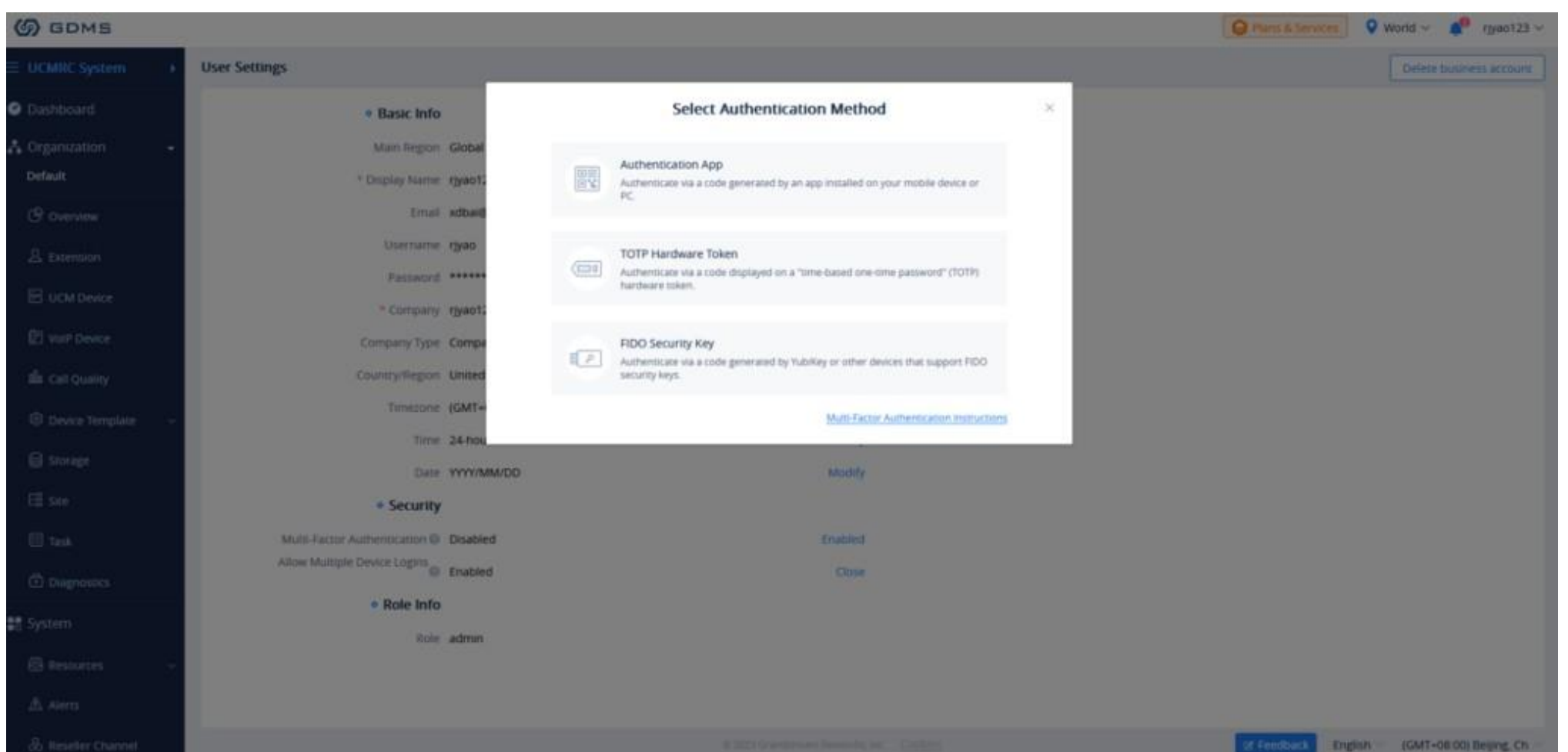


- When the secret code is generated, the user needs to use the secret code to proceed verification process immediately. If the user does not submit the secret code and waits for a too long time, the one-time secret code (TOTP) may be expired. Then, the user may need to start the verification process again from the beginning.
- The user can only bind the physical MFA device to a single account.

Enable FIDO Security Key

FIDO security keys are an authentication hardware which are provided by third-party companies, e.g., Yubico. These devices use complex encryption algorithms to ensure a safe authentication into your GDMS account.

The user can select “FIDO Security Key” as a method of multi-factor authentication. When this method is selected, the user needs to connect the FIDO hardware to the computer and configure the hardware as prompted for authentication.



Important Note

Please note that GDMS Mobile App does not support FIDO Security Key multi-factor authentication. If this method has been selected, then you will not be able to logging to GDMS platform through GDMS application.

Remove MFA Device

If the user does not need to proceed with MFA verification, the user can remove the MFA device and restore the normal login authentication method.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page.
2. Click the “**Remove**” button to remove the MFA Authentication function for the current GDMS account.

Lost MFA Device/Invalid MFA Device

If your MFA device is lost or does not work properly, you can remove the MFA device first and then re-enable the new MFA device.

Method 1: If your GDMS account is a sub-account, you can contact the main GDMS account to remove your multi-factor authentication from the **User** management page. After removal, you can log in to the GDMS platform with the password, and then re-enable the new MFA device.

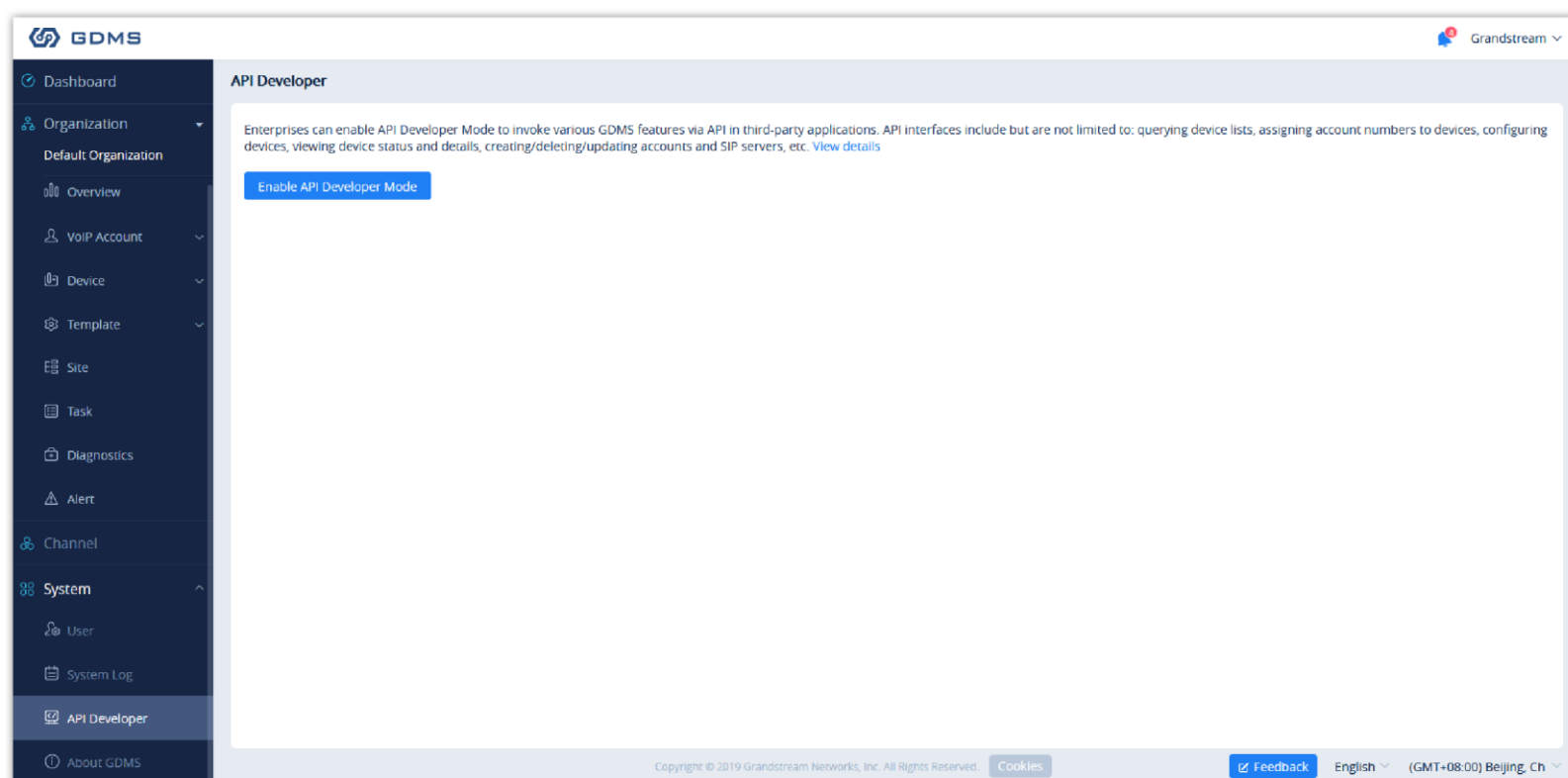
Method 2: If your GDMS account is the main GDMS account and you cannot log in to the GDMS platform, you can contact our Technical Support, provide your relevant information to our Technical Support, and they will help you remove the multi-factor authentication (Our Technical Support will send the removal email to the user and the user needs to input account password and check removal).

API DEVELOPER

GDMS platform opens API interfaces for public users. Users can apply for API Developer to use the services. Users can click to view the details about API interfaces.

API document access address: <https://doc.grandstream.dev/GDMS-API/>

1. Click on “**API Developer**” on the menu on the left side and click to apply for API Developer.



API Developer

2. Click on “**Apply for API Developer**”, the GDMS platform will assign the API Client ID and secret key to the GDMS account, and the GDMS account can use the API Client ID and secret key to invoke the API interfaces.



Apply for API Developer

3. If the user wants to disable the API Developer feature, the user can click on “**Disable API Developer**” to stop invoking the API interfaces.

Notes:

1. Call API Address:

The API Address is `https://{gdms_domain}/oapi/xxx`

- If your GDMS account is in the US region, the {gdms_domain} can be filled with `www.gdms.cloud`
- If your GDMS account is in the EU region, the {gdms_domain} can be filled with `eu.gdms.cloud`

2. When the API Developer is disabled, the previous API secret key will be invalid, the user cannot invoke the GDMS interfaces. If the user tries to re-apply for the API Developer feature, the system will assign another secret key to the GDMS account.

ABOUT GDMS

Users can view GDMS “System Version”, “Server information”, and “Supported Models and Firmware” by clicking on **System** → **About GDMS**.

- “System Version” includes:
 - GDMS Version: The current version of the GDMS platform and the “Release Notes” link.
 - App Version: iOS and Android application version and QR codes to scan to download the app.
- “Server Information” includes links to:
 - [GDMS & UCMRC Server Information](#)
 - [GDMS Security Whitepaper](#)
 - [Privacy Statement](#)
- “Supported Models and Firmware” includes the supported products and the minimum/recommended firmware version.

Model	Minimum Firmware Version	Recommended Firmware Version
DP750	1.0.9.9	1.0.19.5
DP752	1.0.9.9	1.0.19.5
GHP610 Beta	1.0.1.29	1.0.1.37
GHP611 Beta	1.0.1.29	1.0.1.37
GHP620 Beta	1.0.1.29	1.0.1.37
GHP621 Beta	1.0.1.29	1.0.1.37
GRP2601	1.0.1.3	1.0.3.98

About GDMS

The GDMS platform supports the following languages:

- English, Chinese, Spanish (Spain), Spanish (Latin America), French, Greek, and Arabic.

CHANGELOG

Version 1.0.13.19

- Added “Account Active” option on the “Add Account” page and “Edit Account” page under the “SIP Account” module. [[Add SIP Account](#)] [[Edit Account](#)]

Version 1.0.13.15

- Add FIDO U2F multi-factor authentication method. (GDMS platform mobile apps do not support this feature) [[Enable FIDO Security Key](#)]
- Added ability for the administrator to forcibly enable multi-factor authentication for sub-users, and remove multi-factor authentication for sub-users in batches. [[Enable Multifactor Authentication For a User](#)]
- Added a new setting “Allow Multiple Device Logins”. Users can enable or disable simultaneous login from multiple terminals. [[Allow Multiple Device Logins](#)]
- Integrated GUI Config Tools. Users can quickly create GUI Config files on the Resource Management page and parameters configuration page. [[GUI Config File](#)]
- Added new features for VoIP devices on the parameters configuration page: Print MPK Sticker, select firmware path or upload firmware from the firmware list, and move up and down the tables. [[Device Parameters Configuration](#)]
- Supported copying model templates and group templates to another organization. [[Copy Model Template](#)]
- Supported creating permanent firmware upgrade task and it can take effect on newly added devices [[Add Task](#)]
- Added ability to edit the custom firmware files. [[Edit Custom Firmware File Info](#)]
- Added the SSH remote diagnosis switch in Diagnostics module for devices (Currently only supported by GRP260x). [[SSH Remote Capture](#)]
- Added the following updates in the UCM device details statistics report: Device status statistics chart and remote user registration statistics chart. The alert list is also added to the PDF report file. [[UCM Device Statistics](#)]
- Added the device model info to the alert emails and alert details. [[View Alert Notification](#)]
- Added the alert for restoring the online status of the VoIP devices.
- Added ability to set chat file size limit after enabling Cloud IM service. [[IM File Limit](#)]
- Added the following APIs: View template list and push the configuration template with a specific ID to some devices. [[API Developer](#)]

Version 1.0.12.18

- Added “RPS Management” module. Users can manage multiple RPS (Redirection & Provision Server) in a unified manner and configure RPS for device organizations. [[RPS Management](#)]
- Added ability to quickly configure RPS for the current organization on the “VoIP Device” menu. [[Assign RPS](#)]
- Added SSH access authorization to the UCM device or VoIP device for remote support to troubleshoot problems. [[Manage Device via GDMS Support](#)]
- Added ability to select whether to enable/disable GDMS cloud storage space when adding UCM device or importing UCM device to the GDMS platform. This feature is only for the UCMRC paid plan users. [[UCM Device Management](#)]
- Added ability to batch download files on the UCM cloud storage space interface. [[Storage](#)]
- Added ability to select to upgrade firmware for “All devices in this model” when creating the upgrade tasks on the “Task” module. [[Add Task](#)]
- Added ability to edit the “Alert” settings for multiple organizations in batches. [[Alert Notification Settings](#)]

- Added ability to directly upgrade firmware for the devices in the “Reseller Channel” module. [[Upgrade Task](#)]
- Added “GDMS Security Whitepaper” document and “Privacy Statement” in the “About” module. [[About GDMS](#)]

Version 1.0.12.6

- Added “By Site” option under “Device Template” module. It allows users to configure the template for a specific site and provision the devices in that site. [[By Site](#)]
- Added the “Energy Saving Inform” tab under the VoIP Device Details module. Users can configure the energy saving settings through the device configuration template. [[View Device Details](#)]

Version 1.0.11.19

- Added an add-on plan for UCM RemoteConnect service: Extra 100 Concurrent Calls. If the user purchases this add-on plan, the corresponding UCM63xx device can add the capacity of 100 concurrent calls. [[Plan & Service](#)]
- Added an option to export order receipts. Users can export the order receipts after placing the orders. [[Export Receipt](#)]
- Added an option to ask the user whether to synchronize the local configurations of the device when adding/importing VoIP devices to the GDMS platform. [[Add VoIP Device](#)]
- Added an option to ask the user whether to import the local SIP account configuration of the device when synchronizing the VoIP device’s local configuration to the GDMS platform. [[Batch Import SIP Account](#)]
- Added a new alert type for the UCM63xx device “Outbound trunk call duration usage”, and combined “Network Disk Status” and “External Disk Status” alert types to “External Disk Usage”. [[Alert Notification Settings](#)]
- Added the time range settings for “Message notification settings”, “App notification settings”, and “Email notification settings”. If the user sets the time range for alerts, the user can only receive the alert notifications during that specific period. The user can select the whole day, or a specific time period, or multiple different time periods during a day. [[Alert Notification Settings](#)]
- Supported editing resource files. The user can upload the resource file again, and leave the URL unchanged. [[Other Resources Management](#)]
- Added an entrance to view UCM RemoteConnect plan specifications on the GDMS main page. [[Plan & Services](#)]
- Added “Outbound Proxy” field for SIP accounts importing the template. [[Batch Import SIP Accounts](#)]
- Supported adding OEM devices to the GDMS platform account for management. [[UCM Device Management](#)]
- Improved the user experience on the GDMS platform.

Version 1.0.10.41

- No major changes

Version 1.0.10.23

- Added to share organizations between enterprises. Organizations can be managed by the other associated enterprises. [[Share Organization](#)]
- Added UCM-related alert types and App notification setting module. [[Alert Notification Settings](#)]
- Added an option to apply the changes to all devices when editing the “By Model” template. Added an option to remember the current setting for option “Auto Provision to Devices in”, and the option will be set following the setting for the previous model template when the user creates a new one. [[Add Template](#)]
- Optimized the “UCM Devices” interface and added the feature to apply for the free trial plan. [[Add SIP Server](#)]
- Optimized the “My Plans” interface and added the feature to apply for the Cloud IM service. [[Enable Service](#)]
- Optimized interface according to the specifications of the UCM RemoteConnect plans.

Version 1.0.9.13

- Unified the account login center. Users do not need to select US regional server or EU server for login. [[GDMS Account Registration](#)]
- VoIP System is classified by supporting VoIP device and GXW45XX Device. [[Supported Device Model](#)]
- Added search function in Set Parameters module. [[Set Parameters](#)]
- Improved the function performances in Diagnostics module. [[Device Diagnostics](#)]

Version 1.0.8.16

- Assigned permissions to separate the different sub systems in the GDMS platform.
- Added UCMRC system module and the navigation structure has been updated. Added Dashboard module and Overview module and added displaying more UCM device status information. [[UCMRC SYSTEM](#)]
- Optimized the UCM device list. Added Overview module and Plan Details information module in Device Details module. [[Figure 72: UCM Device Details](#)]
- Added new default site when adding a new UCM device to the GDMS platform. [[Add SIP Server](#)]
- Added supporting remote access to the UCMRC, UCM permissions settings, and supporting accessing the UCM Web UI without entering a password through the GDMS platform. [[UCMRC SYSTEM](#)]
- Added managing SIP server address for UCM devices, and support configuring the advanced settings of SIP servers. [[Add SIP Server](#)]
- Added to support Spanish, Latin Spanish, French, Greek, and Arabic languages in the GDMS platform. [[About GDMS](#)]
- Added to support UCMRC and VoIP sub systems in GDMS mobile application.
- Added alert messages pushing function in GDMS mobile application.

Version 1.0.7.11

- Supported Host/Spare functionality for UCMRC services. Users can view the Host/Spare associations in the GDMS platform and disassociate the relationship. [[View/Disassociate Host/Spare UCM Device](#)]
- Supported to allow users to diagnose UCMRC services availability. [[UCM Device Diagnosis](#)]
- Supported access to the Web UI of the VoIP devices remotely. [[Remote Access to Device Web UI](#)]
- Added time and date format settings in Personal Settings. [[User Settings](#)]
- Added the ability to convert configuration files. Supported converting the configuration file of UCM62xx to the configuration file of UCM63xx. [[Convert Configuration File](#)]
- Added to display VPN IP address in VoIP Device Details interface. [[View Device Details](#)]

Version 1.0.6.10

- Added UCM CloudIM Service. [[UCM Cloud IM Service](#)]
- Added support to modify the UCM region. [[Add SIP Server](#)]

Version 1.0.5.5

- Added support to synchronize UCM devices' alert notifications to the GDMS platform. [[Synchronize UCM Device Alert to GDMS](#)]
- Added support to restore UCM backup files remotely through the GDMS platform. [[Restore UCM Backup File Remotely](#)]
- Added to support to diagnose UCM devices through the GDMS platform. [[UCM Device Diagnosis](#)]

- Added to authorize Grandstream Support to manage devices. [[Manage Device via GDMS Support](#)]

Version 1.0.4.9

- Added Call Statistics module for VoIP devices. The SIP accounts in the devices which are using the UCM RemoteConnect service plan will report the call quality and statistical report. [[Call Statistics](#)]
- Added support to upload UCM device backup file to GDMS platform. [[Upload Backup File](#)]
- Added SMS Notification function in the GDMS platform. [[SMS Notification Settings](#)]
- Added to allow users to add UCM devices to the GDMS platform with the original password. [[Add SIP Server](#)]
- Added to support to configure multiple SIP servers for a single SIP account. [[Add SIP Account](#)]
- Added to allow users to set sending time for UCM daily statistical report. [[View Statistics](#)]

Version 1.0.3.4

- Added to support network diagnosis and system diagnosis functions in the device diagnosis module. [[DEVICE DIAGNOSTICS](#)]
- Added to support to configure the concurrent upgrading devices amount for concurrent upgrade tasks. [[Supported Devices and Requirements](#)]
- Added WP810 to supported devices. [[Add Task](#)]

Version 1.0.2.8

- Supported adding UCM63xx to the GDMS platform. Added PBX Device module: Remote access to UCM63xx, restart UCM63xx, upgrade UCM63xx, view UCM63xx device details, data statistics report, synchronize SIP accounts in the UCM63xx to GDMS platform, etc. [[UCM Device Management](#)]
- Added Value-added services module in GDMS platform. Supported to purchase/renew/upgrade UCM RemoteConnect Plan and UCM/User Cloud Storage Space Plan and view the order history.
- Supported to view statistics report of UCM63xx device. The system can send the daily report to the configured mailbox. [[UCM Device Diagnosis](#)]
- Supported to view the enterprise/UCM cloud storage space usage. Users can receive alert messages through a configured mailbox. [[View Storage Space](#)]
- Supported to notify users when the plan will expire soon or has already expired. The alert notification can be sent to the user through a configured mailbox. [[View My Plans](#)]
- Supported creating tasks to reboot/upgrade PBX devices. [[TASK MANAGEMENT](#)]

Version 1.0.1.16

- Added device local configuration synchronization function. Users can synchronize the SIP accounts and parameters to the GDMS platform. [[Synchronize Device Local Configuration](#)]
- Added “Disable Push Configuration” function. Users can disable pushing the configuration to the device through the GDMS platform. [[Disable Push Configuration](#)]
- Added file type “Others” in Resources Management module. There is no file type limit if the user selects the file type as “Others”. [[Other Resources Management](#)]
- Added to allow users to manage devices with GDMS mobile application. Users can use the application to scan the bar code of the device to add the device to the GDMS platform, configure SIP accounts and view alert messages, etc.
- Added GDMS account deletion function. [[Delete GDMS Account](#)]

Version 1.0.1.3

- Added Resource Management module in GDMS platform. [[RESOURCE MANAGEMENT](#)]

- Added Custom Ringtone configuration and involved settings. [[VoIP Device Management](#)]
- Added the function to support copy configuration. [[Device Parameters Configuration](#)]

Version 1.0.0.65

- New independent region: EU region (for GDPR rules)
- Support GRP26XX, DP7XX, GXP21XX, GXV3380/3370/3350, HT80X, HT81X, GVC3210, GRP2616. [[Supported Devices and Requirements](#)]
- Add Sub-level organization feature.
- User's dashboard support statistic by sites. [[Device Statistics](#)]
- User's dashboard adds devices distribution Map. [[Device Statistics](#)]
- Added operation logs for different users and record the operation logs for each device. [[SYSTEM LOG](#)]
- Support repeating tasks. [[Add Task](#)]
- ACS server support load-balance.
- Supported Multi-Factor Authentication function in GDMS platform to provide higher security protection for GDMS account. [[MULTI-FACTOR AUTHENTICATION](#)]
- Supported to copy and paste the data from other organizations when users try to create a new organization. [[Add Organization](#)]
- Supported to transfer the devices to other organizations. [[Move Device](#)]
- Supported to divide group templates into multiple series templates, which is easier for users to configure devices in different groups. [[By Group](#)]
- Supported to delete organizations. [[Delete Organization](#)]
- Supported to filter the devices in the specific city on Device Geo Map. [[Device List](#)]
- API Interfaces. [[API DEVELOPER](#)]

Version 1.0.0.42

- This is the initial version.