Grandstream Networks, Inc.

Grandstream Device Management System (GDMS)

User Guide

COPYRIGHT

©2021 Grandstream Networks, Inc. https://www.grandstream.com
All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this guide is available for download here:

https://www.grandstream.com/support

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe, and other countries.

Table of Content

DOCUMENT PURPOSE **21**

CHANGELOG **22**

Version 1.0.6.10 22

Version 1.0.5.5 22

Version 1.0.4.9 22

Version 1.0.3.4 22

Version 1.0.2.8 23

Version 1.0.1.16 23

Version 1.0.1.3 24

Version 1.0.0.65 24

Version 1.0.0.42 25

WELCOME **26**

PRODUCT OVERVIEW **27**

Feature Highlights 27

GDMS Technical Specifications 28

GETTING STARTED **30**

GDMS Overview 30

Main Functions Overview *30*

Prerequisites *31*

GDMS Account Registration 31

Supported Devices and Requirements 33

Connect with GDMS 33

OVERVIEW **34**

Device Statistics 34

Device Distribution 36
Device List 37
VOIP DEVICE MANAGEMENT 38
Add Device 40
Batch Import Devices 41
Configure SIP Account (Non-DP Devices) 43
Configure SIP Account/Line (DP Devices) 44
Device Parameters Configuration 46
Configure Resource Files 48
Synchronize Device Local Configuration 49
Disable Push Configuration 49
View Device Details 49
Edit Device 51
View Device Operation Logs 52
View Device Task History 52
Firmware Upgrade 53
Site Assignment 54
Move Device 54
Reboot Device 55
Factory Reset 56
Delete Device 56
Export Device 57
Manage Device via GDMS Support 58
Stop Authorizing Manually 58
ACCOUNT MANAGEMENT 60
Overview 60
Add SIP Server 61

Add SIP Account 64
Batch Import SIP Account 67
Allocate Device 70
Edit Account 70
Batch Modify SIP Server of SIP Accounts 71
Delete Account 72
Export Account 73
Edit SIP Server 73
Delete SIP Server 73
UCM REMOTE CONNECT - UCM DEVICE 75
Add Device 76
Batch Import Devices 77
View Device Details 79
View Device Plan 80
Remote Access to UCM Web UI 81
UCM Device Diagnosis 83
View Statistics 83
Daily Report 83
View Statistics Report (Last 30 days) 85
Set Daily Report Receiving Mailbox 87
View Operation Logs 88
Custom Remote Access Domain Name 89
Synchronize UCM Device Alert to GDMS 91
Reboot Device 91
Upgrade Firmware 92
Edit Device 93
Batch Modify Sites 94
Delete Device 95

Export Device 96

UCM REMOTE CONNECT – CONFIGURE PARAMETER FOR DEVICE 97

UCM REMOTE CONNECT - UCM BACKUP 99

View Backup File 99

Upload Backup File 100

Download Backup File 101

Restore UCM Backup File Remotely 101

Delete Backup File 102

UCM REMOTE CONNECT - CALL QUALITY 103

Statistics Overview 103

Call Quality Record 104

Enable/Disable Call Quality Reporting 105

DEVICE CONFIGURATION 107

By Model 107

Automatic Configuration Push 107

Manual Configuration Push 107

Add Template 108

Set Parameters 110

Configure Resource Files 112

Push Update 113

Edit Template 114

Download Configuration Template 114

Delete Template 114

By Group 115

Add Group 115

Set Parameters 117

Configure Resource Files *119*
Push Update *119*
Edit Group *120*
Download Configuration File *121*
Delete Group *121*
By CFG 121
Upload CFG File *121*
Push Update *123*
Download Configuration File *123*
Delete CFG File *123*
SITE MANAGEMENT 124
Add Site 124
Batch Import Sites 125
Edit Site 127
Delete Site 128
View Devices 128
Transfer Site 129
TASK MANAGEMENT 130
Add Task 130
View Task Status 133
Start Scheduled Tasks 135
Cancel Pending Tasks 135
End Task 135
Search Task 135
Delete Task 136
DEVICE DIAGNOSTICS 137
Start Diagnostics 137

View Device Details *138*
Ping/Traceroute *139*
Syslog *140*
Capture Trace *140*
Network Diagnostics *141*
System Status *142*
End Diagnostics *143*
Diagnostics Records 143
ALERT MANAGEMENT 145
Alert Notification Settings 145
Message Notification Settings *145*
Email Notification Settings *147*
SMS Notification Settings *150*
View Alert Notification 152
RESOURCE MANAGEMENT 154
Firmware Management 154
Custom Firmware *154*
Official Firmware *155*
Firmware Update Notification Settings *156*
Push to Upgrade Firmware *157*
Edit Firmware *158*
Download Firmware *159*
Delete Firmware *159*
Other Resources Management 159
Upload Resource *159*
View Resource List *161*
Copy File URL *161*

Download Resource *161*
Modify Resource *162*
Delete Resource *162*
View Storage Space 162
CHANNEL MANAGEMENT 164
Superior Channel Binding Address 164
Add Sub-channel *165*
Edit Subordinate Channel Customer *166*
Delete Subordinate Channel Customer *166*
Track Device 167
View Device *167*
Device Assignment Notification *168*
Device Assignment *168*
Configure Device *171*
USER MANAGEMENT 172
Add Role 172
Edit Role 173
Delete Role 173
Add Sub-user 173
Edit User 174
Delete User 174
Personal Information 175
Sign Out 176
Delete GDMS Account 176
ORGANIZATION MANAGEMENT 177
Switch Organization 177
Add Organization 178

Edit Organization 179
Delete Organization 180
SYSTEM LOG 181
VALUE-ADDED SERVICES 182
UCM Remote Connect Plan 182
Cloud Storage Space Plan 182
UCM CloudIM Plan 183
Trial Plan 183
View UCM CloudIM Plan Service ID and Key 186
Manage Bound UCM Device 187
Edit Enterprise Name 188
Purchase Service 189
Purchase UCM Remote Connect Plan（Pending） 189
Purchase UCM Cloud Storage Add-on Plan（Pending） 192
Purchase User Cloud Storage Plan 193
View My Plans 193
View Plan Details 195
Download Invoice 195
Assign Plan to UCM 196
Renew Plan 197
Upgrade Plan 199
Plan Expiration Notice 199
MULTI-FACTOR AUTHENTICATION 201
MFA Device Standards 202
Download Virtual MFA Application 202
Enable MFA Device 202
Enable Virtual MFA Device 203

Enable Physical MFA Device *205*

Remove MFA Device 207

Lost MFA Device/Invalid MFA Device 207

API DEVELOPER 208

ABOUT GDMS 210

EXPERIENCING GDMS.CLOUD SYSTEM 211

Table of Tables

Table 1: GDMS Technical Specifications 28

Table 2: Register GDMS Account 32

Table 3: Supported Devices 33

Table 4: Overview Labels 35

Table 5: VoIP Device Management 38

Table 6: Operation Instructions 39

Table 7: Add VoIP Device 40

Table 8: Import VoIP Device Template 42

Table 9: Configure SIP Account for DP Devices 44

Table 10: Account Status Description 60

Table 11: Operation Description 61

Table 12: Add SIP Server 61

Table 13: Add SIP Account 64

Table 14: Assign Device 66

Table 15: Import Account Template Options 68

Table 16:UCM Device Management 75

Table 17: Operation Instructions 76

Table 18: Add UCM Device 77

Table 19: Import UCM Device Template 78

Table 20: UCM Statistics Report 84

Table 21: Set Daily Report Receiving Mailbox 88

Table 22: Statistics Overview 103

Table 23: Add Template 109

Table 24: Add Group 116

Table 25: Add Site 125
Table 26: Site Template Options 127
Table 27: Add Task 130
Table 28: Task Status Description 133
Table 29: Task Status Detailed Description 134
Table 30: Ping/Traceroute Options 139
Table 31: Message Notification Settings 146
Table 32: Email Notification Settings 148
Table 33: Notification Settings 152
Table 34: Custom Firmware 154
Table 35: Custom Firmware 160
Table 36: Track Device 167
Table 37: Assign to Subordinate Channel 170
Table 38: Add Role 172
Table 39: Add Sub-user 173
Table 40: Personal Information 175
Table 41: Add Organization 179
Table 42: Purchase Plan 189
Table 43: MFA Device Standards 202
Table 44: Suitable Applications 202

Table of Figures

Figure 1: Welcome to GDMS 31

Figure 2: Register GDMS Account 32

Figure 3: Overview 34

Figure 4: Model Statistics 36

Figure 5: Device Distribution 36

Figure 6: Device List 37

Figure 7: VoIP Device Management 38

Figure 8: Search Devices 40

Figure 9: Add VoIP Device 40

Figure 10: Import VOIP Device 41

Figure 11: Import VoIP Device Template 42

Figure 12: Configure SIP Account 43

Figure 13: Configure SIP Account for DP Devices 44

Figure 14: Line Configuration 45

Figure 15: Device Parameter Configuration 46

Figure 16: Ringtone Configuration 47

Figure 17: Edit Configuration File 47

Figure 18: Resource Configuration 48

Figure 19: View VoIP Device Details 50

Figure 20: VoIP Device Details 50

Figure 21: Edit VoIP Device Option 51

Figure 22: Edit VoIP Device 51

Figure 23: View VoIP Device Operation Logs 52

Figure 24: View VoIP Device Task History 53

Figure 25: Upgrade Firmware 53
Figure 26: Site Assignment 54
Figure 27: Move Device 55
Figure 28: Reboot Device 55
Figure 29: Factory Reset 56
Figure 30: Delete Device 57
Figure 31: Delete Device Prompt 57
Figure 32: Authorization Management 58
Figure 33: Stop Authorizing Manually 59
Figure 34: Account Management 60
Figure 35: Add SIP Server 61
Figure 36: Finish Adding SIP Server to GDMS 64
Figure 37: Add SIP Account 64
Figure 38: Assign Device 66
Figure 39: Import SIP Account 67
Figure 40: Import Account Template – General Device Template 67
Figure 41: Import Account Template – DP Device Template 68
Figure 42: Import Account Template - HT Device Template 68
Figure 43: Example I 69
Figure 44: Example II 69
Figure 45: Example III 70
Figure 46: Example IV 70
Figure 47: Example V 70
Figure 48: Example VI 70
Figure 49: Example VII 70
Figure 50: Edit Account 71

Figure 51: Modify SIP Server 72
Figure 52: Delete Account 73
Figure 53: Delete SIP Server 74
Figure 54: Search Devices 76
Figure 55: Add UCM Device 76
Figure 56: Import UCM Device 78
Figure 57: View UCM Device Details 79
Figure 58: UCM Device Details 80
Figure 59: View UCM Device Plan 80
Figure 60: UCM List 81
Figure 61: UCM Login Interface 82
Figure 62: UCM Home Page 82
Figure 63: UCM Device Diagnosis 83
Figure 64: UCM Statistics Report 84
Figure 65: View UCM Device Statistics Report 86
Figure 66: View Connected Devices Type/Amount 86
Figure 67: View Call Type Statistics 86
Figure 68: View Call Statistics Chart 87
Figure 69: Set Daily Report Receiving Mailbox 87
Figure 70: View UCM Device Operation Logs 89
Figure 71: Device Edit Menu 89
Figure 72: Custom UCM Remote Access Domain Name 90
Figure 73: Enter Private Domain Name and Certificate 90
Figure 74: Reboot UCM on GDMS 91
Figure 75: UCM Devices Listed in GDMS 92
Figure 76: Upgrade Firmware Configuration on GDMS 92

Figure 77: Edit UCM Device Option 93
Figure 78: Edit Device 94
Figure 79: Site Assignment 95
Figure 80: Delete Device Prompt 96
Figure 81: Edit Account 97
Figure 82: Modify SIP Server Address 98
Figure 83: View Backup File 99
Figure 84: Upload File 100
Figure 85: Restore Backup File Remotely 101
Figure 86: View Results 102
Figure 87: Statistics Overview 103
Figure 88: Call Quality Record 104
Figure 89: Filter by Date 104
Figure 90: Call Quality Record Report 105
Figure 91: Enable/Disable Call Quality Reporting 106
Figure 92: Manual Configuration Push 107
Figure 93: Example – GXV3370 108
Figure 94: Add Template 109
Figure 95: Set Parameters 110
Figure 96: Ringtone Configuration 111
Figure 97: Resource Configuration 112
Figure 98: Push Configuration File 113
Figure 99: Schedule Config Update 113
Figure 100: Edit Model Template 114
Figure 101: Download Configuration Template 114
Figure 102: Delete Template 115

Figure 103: By Group 115
Figure 104: Add Group 116
Figure 105: Finish Adding Group 117
Figure 106: Ringtone Configuration 118
Figure 107: Resource Configuration 119
Figure 108: Push Update 120
Figure 109: Edit Group 120
Figure 110: Download Configuration File 121
Figure 111: By CFG 121
Figure 112: Upload CFG File 122
Figure 113: Finalize Import 122
Figure 114: Push Update 123
Figure 115: Site Management 124
Figure 116: Add Site 125
Figure 117: Import Site 126
Figure 118: Site Template 126
Figure 119: Edit Site 128
Figure 120: View Devices 128
Figure 121: Transfer Site 129
Figure 122: Add Task 130
Figure 123: Task Management List 132
Figure 124: View Task Status 133
Figure 125: Task Status 134
Figure 126: Search Task 136
Figure 127: Device Diagnostics 137
Figure 128: View Diagnostics Details 138

Figure 129: View Device Details 139
Figure 130: Ping/Traceroute 139
Figure 131: Syslog 140
Figure 132: Capture Trace 141
Figure 133: Network Diagnostics 142
Figure 134: System Status 143
Figure 135: Diagnostics Records 144
Figure 136: Message Notification Settings 145
Figure 137: Unread Message Icon 147
Figure 138: Email Notification Settings 148
Figure 139: Email Alert Notification 149
Figure 140: SMS Notification Settings 151
Figure 141: View Alert Notification 153
Figure 142: Custom Firmware 154
Figure 143: Finish Uploading Custom Firmware 155
Figure 144: Official Firmware 156
Figure 145: Firmware Update Notification Settings 157
Figure 146: Push to Upgrade Firmware 158
Figure 147: Custom Firmware 160
Figure 148: Other Resources 161
Figure 149: View Storage Space 163
Figure 150: View My Binding Channel Address 164
Figure 151: Superior Channel Binding Address 165
Figure 152: Link Address 165
Figure 153: Add Remarks 166
Figure 154: Disassociate Sub-channel 167

Figure 155: Track Device 167
Figure 156: Assign Single Device to Subordinate Channel 169
Figure 157: Device Operation Options 169
Figure 158: Assign Multiple Devices to Subordinate Channel 170
Figure 159: Copy and Paste Multiple MAC Addresses 170
Figure 160: Import to Manage Device 171
Figure 161: Add Role 172
Figure 162: Add Sub-user 173
Figure 163: Edit Sub-user 174
Figure 164: Edit Unverified Sub-user 174
Figure 165: Personal Information 175
Figure 166: Sign Out 176
Figure 167: Multiple Organizations and Administrators 177
Figure 168: Switch Organization 178
Figure 169: Add Organization 178
Figure 170: Edit Organization 180
Figure 171: System Log 181
Figure 172: Services List Interface 184
Figure 173: Apply Plans 184
Figure 174: Finish Applying UCM CloudIM Plan 185
Figure 175: Bind UCM Device 185
Figure 176: Bind UCM Device on Web UI 186
Figure 177: View Service ID and Key 186
Figure 178: Find UCM CloudIM Plan 187
Figure 179: View Bound UCM Devices 187
Figure 180: Find UCM CloudIM Plan 188

Figure 181: Edit Enterprise 188
Figure 182: Services Interface 189
Figure 183: Assign Plan 191
Figure 184: View Purchased Plan 191
Figure 185: UCM Cloud Storage Add-on Plan 192
Figure 186: View Purchased UCM Cloud Storage Add-on Plan 192
Figure 187: User Cloud Storage Plan 193
Figure 188: View My Plans 194
Figure 189: UCM Cloud Storage Add-on Plan Expiration 194
Figure 190: View Plan Details 195
Figure 191: Download Invoice 195
Figure 192: Assign Plan Options 196
Figure 193: Assign Plan to UCM 197
Figure 194: Renew Plan 198
Figure 195: Plan Expiration Notice 200
Figure 196: Access Personal Information Page 203
Figure 197: Scan QR Code 204
Figure 198: Input MFA Secret Code 205
Figure 199: Hardware MFA Device Authentication 206
Figure 200: Physical MFA Device 206
Figure 201: API Developer 208
Figure 202: Apply for API Developer 208
Figure 203: About GDMS 210

DOCUMENT PURPOSE

This document introduces the GDMS platform and how to use it to manage various Grandstream products. Currently, GDMS supports GXV33xx series, WP820, WP810, GRP series, GXP21xx series, HT8xx series, DP7xx series and GVC3210.

To learn more information about GDMS platform, please visit link www.grandstream.com to get more information.

The following topics will be covered in this guide:

- Product Overview
- Getting Started
- Device Management
- Account Management
- UCM Remote Connect
- Device Configuration
- Site Management
- Task Management
- Device Diagnostics
- Alert Management
- Channel Management
- User Management
- Organization Management
- Value-Added Services
- Multi-Factor Authentication
- API Developer
- About GDMS

CHANGELOG

Version 1.0.6.10

- Added UCM CloudIM Plan. [UCM CloudIM Plan]
- Added support to modify the UCM region. [Edit Device]

Version 1.0.5.5

- Added to support to synchronize UCM devices alert notifications to the GDMS platform. [Synchronize UCM Device Alert to GDMS]
- Added to support to restore UCM backup file remotely through the GDMS platform. [Restore UCM Backup File Remotely]
- Added to support to diagnose UCM devices through GDMS platform. [UCM Device Diagnosis]
- Added to authorize to 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 UCM Remote Connect service plan will report the call quality and statistical report. [UCM REMOTE CONNECT - CALL QUALITY]
- Added support to upload UCM device backup file to GDMS platform. [UCM REMOTE CONNECT - UCM BACKUP]
- Added SMS Notification function in the GDMS platform. [SMS Notification Settings]
- Added to allow users to add UCM devices to the GDMS platform with original password. [Add Device]
- 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. [Set Daily Report Receiving Mailbox]

Version 1.0.3.4

- Added to support network diagnosis and system diagnosis functions in 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. [Concurrent Upgrade]

Version 1.0.2.8

- Supported to add UCM63xx to 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 REMOTE CONNECT - UCM DEVICE
- Added Value-added services module in GDMS platform. Supported to purchase/renew/upgrade UCM Remote Connect Plan and UCM/User Cloud Storage Space Plan and view the order history. [VALUE-ADDED SERVICES]
- 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 configured mailbox. [View Storage Space]
- Supported to notify users when the plans will expire soon or has already expired. The alert notification can be sent to the user through configured mailbox. [View My Plans]
- Supported to create 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 GDMS platform. [Synchronize Device Local Configuration]
- Added “Disable Push Configuration” function. Users can disable pushing the configuration to the device through 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 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] [DEVICE CONFIGURATION]
- Added the function to support to copy configuration. [Device Parameters Configuration]

Version 1.0.0.65

- New independent region: EU region (for GDRP rules) [Region]
- Support GRP26XX, DP7XX, GXP21XX, GXV3380/3370/3350, HT80X, HT81X, GVC3210, GRP2616. [Supported Device Models]
- Add Sub-level organization feature.
- User's dashboard support statistic by sites. [Device Statistics]
- User's dashboard adds devices distribution Map. [Device Statistics]
- Add operation log for difference users and record the operation logs for each device. [SYSTEM LOG]
- Support repeating tasks. [Repeating]
- 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. [Clone Organization]
- Supported to transfer the devices to other organizations. [Move Device]
- Supported to divide group template to 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 Distribution Map. [Search]
- API Interfaces. [API DEVELOPER]

Version 1.0.0.42

- This is the initial version.

WELCOME

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 synchronize SIP accounts to 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 the 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

Table 1: GDMS Technical Specifications

Functions	• 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	• HTTPS protocol and two-way certificate verification to ensure data security between devices and GDMS. • 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	• 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	• 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 • GXW series (pending)

GETTING STARTED

GDMS Overview

Main Functions Overview

Import Devices and Management

Users need to import the devices into the GDMS platform first in order 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 through 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 to push 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 to upgrade a batch of devices' firmware by device model, site, firmware version range and other conditions. It also supports to upgrade 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 task 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 the administrators to diagnose faults of some devices in order to locate and resolve problems quickly.

Prerequisites

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

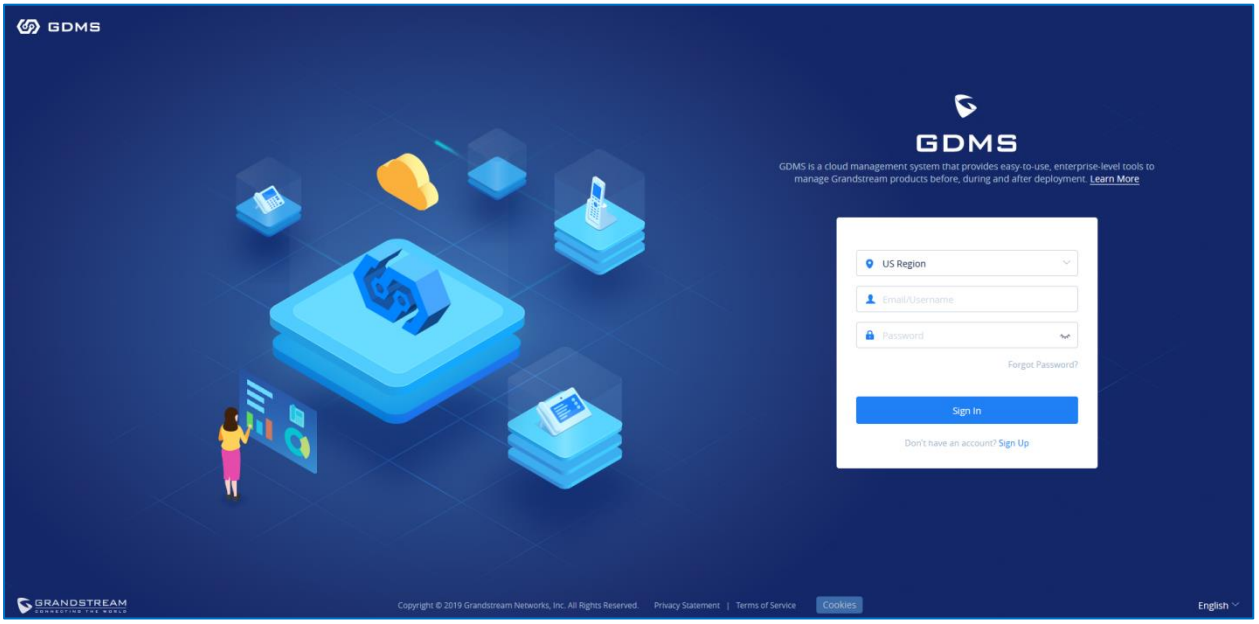


Figure 1: Welcome to GDMS

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

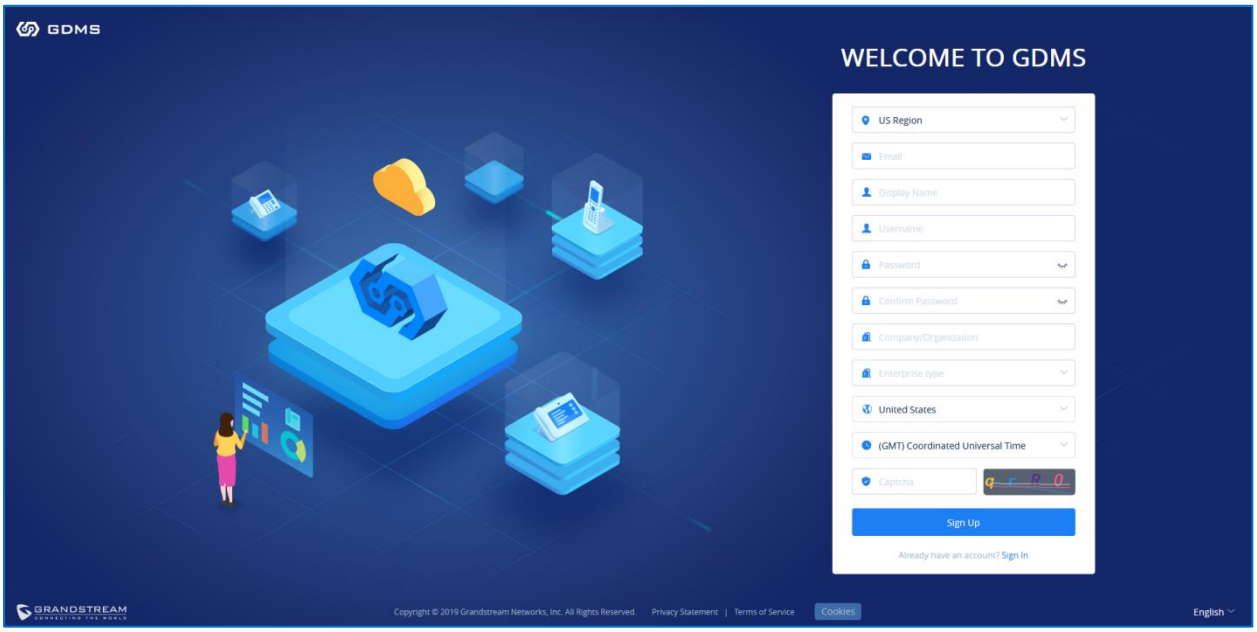


Figure 2: Register GDMS Account

Table 2: Register GDMS Account

Region	This option shows the user will be connected to which server. The data of the different servers are completely independent. The default setting is “United States”.
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.

3. 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.

Table 3: Supported Devices

Supported Device Models	
Audio Device	GXP21XX
	DP7XX
	GRP26XX
	WP810
	WP820
Video Device	GXV3370, GXV3380, GXV3350
Conference Device	GVC3210
ATA Device	HT80X, HT81X
IP-PBX	UCM63XX

Connect with GDMS

The devices must be upgraded to the 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.

OVERVIEW

Device Statistics

The Dashboard page provides an overview of the following information:

- Total accounts
- Total devices
- Total sites
- Accounts status
- Devices status
- Device Distribution
- Sites statistics
- Model statistics

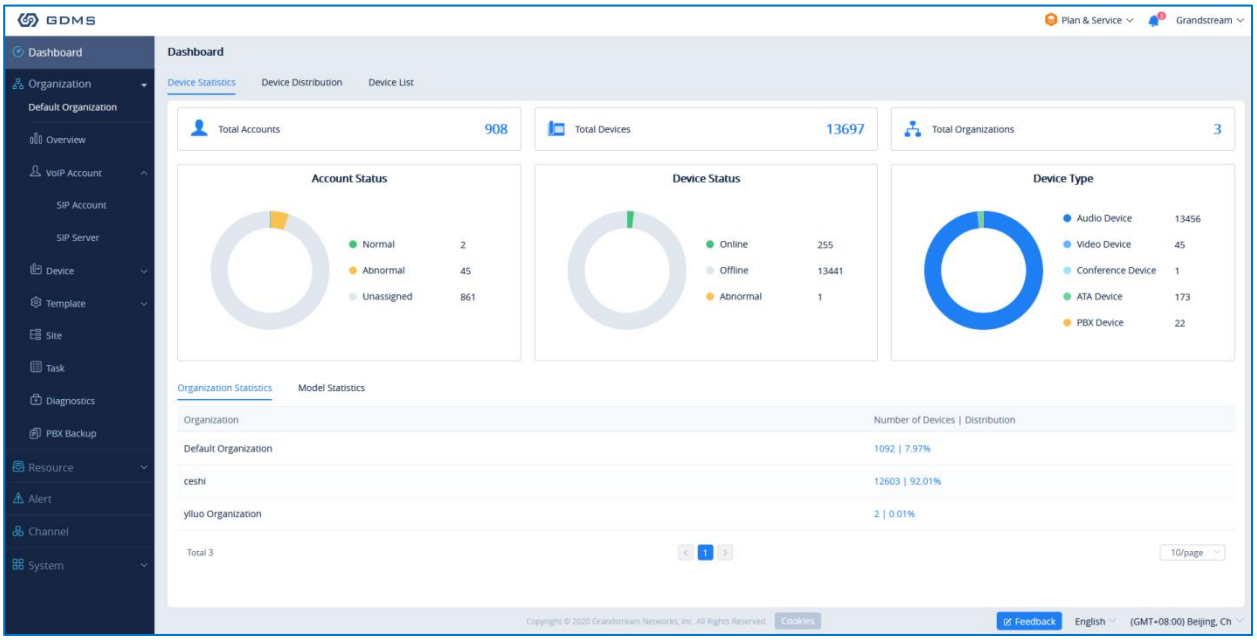


Figure 3: Overview

Table 4: Overview Labels

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	Displays the total number of accounts currently registered, unregistered, and unallocated. • **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	Displays the total number of devices currently online and offline. • **Online:** Device and GDMS platform network connection is normal. • **Offline:** Device and GDMS platform lose network connection.
Device Distribution	Displays the total number of devices in each category: audio, video, and conferencing. • **Audio devices:** GRP series, DP series, GXP series, and WP series • **Video devices:** GXV series • **Conference devices:** GVC series • **ATA devices:** HT series • **PBX devices:** UCM series
Sites 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.

Figure 4: Model Statistics

Device Distribution

This menu will show the distribution map of the devices which have been associated by 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 amount of the devices in that area.
- If certain city has the devices, it will be marked with green dot , and users could leave the cursor on the city to check the amount of the devices in that city. The user can click on the dot to see the devices list in this city.

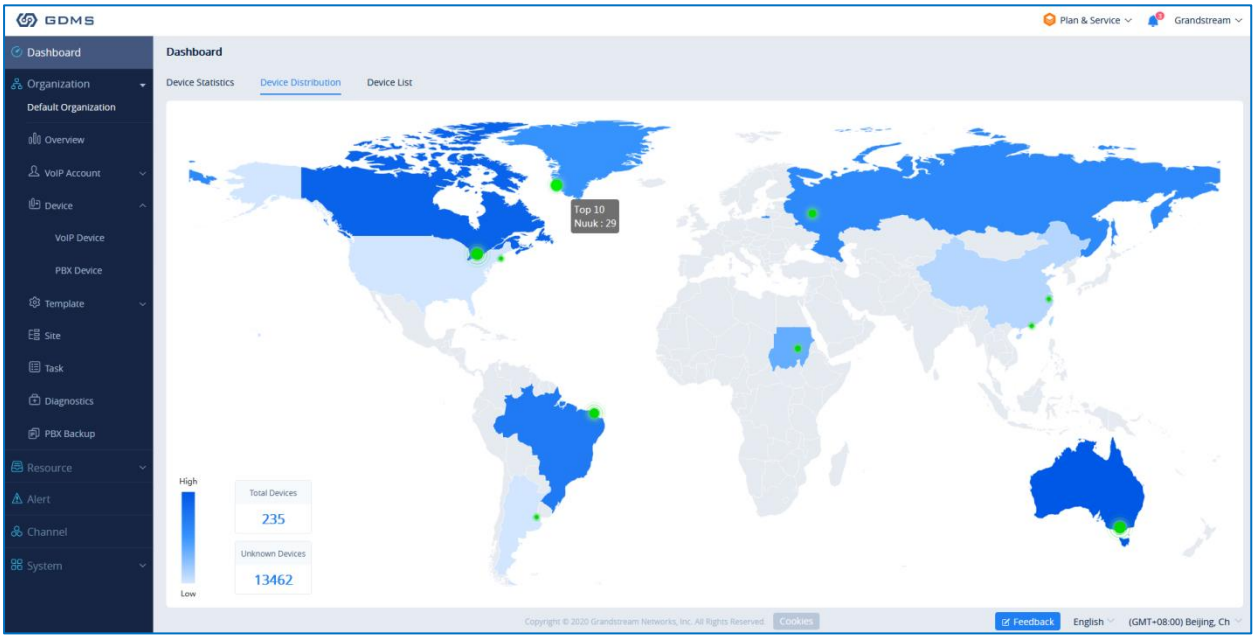


Figure 5: Device Distribution

Device List

This interface displays a list of all devices under the current enterprise account, including VOIP devices and PBX devices, and users can find devices by MAC addresses.

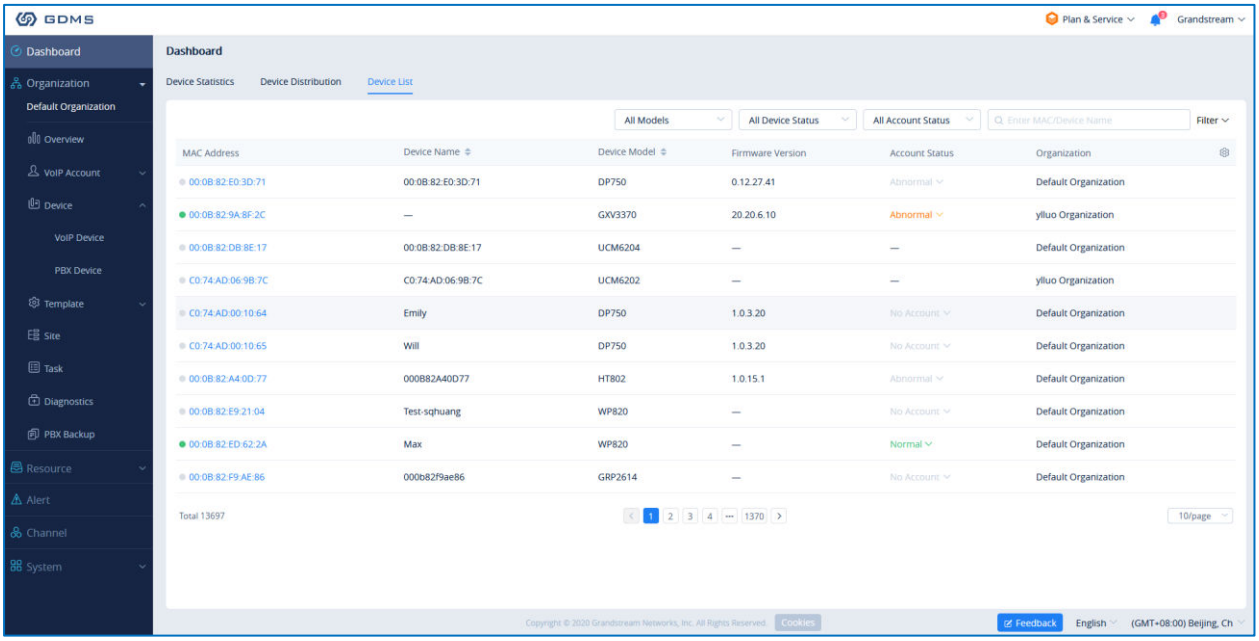


Figure 6: Device List

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 devices details, device diagnostics, and other operations.

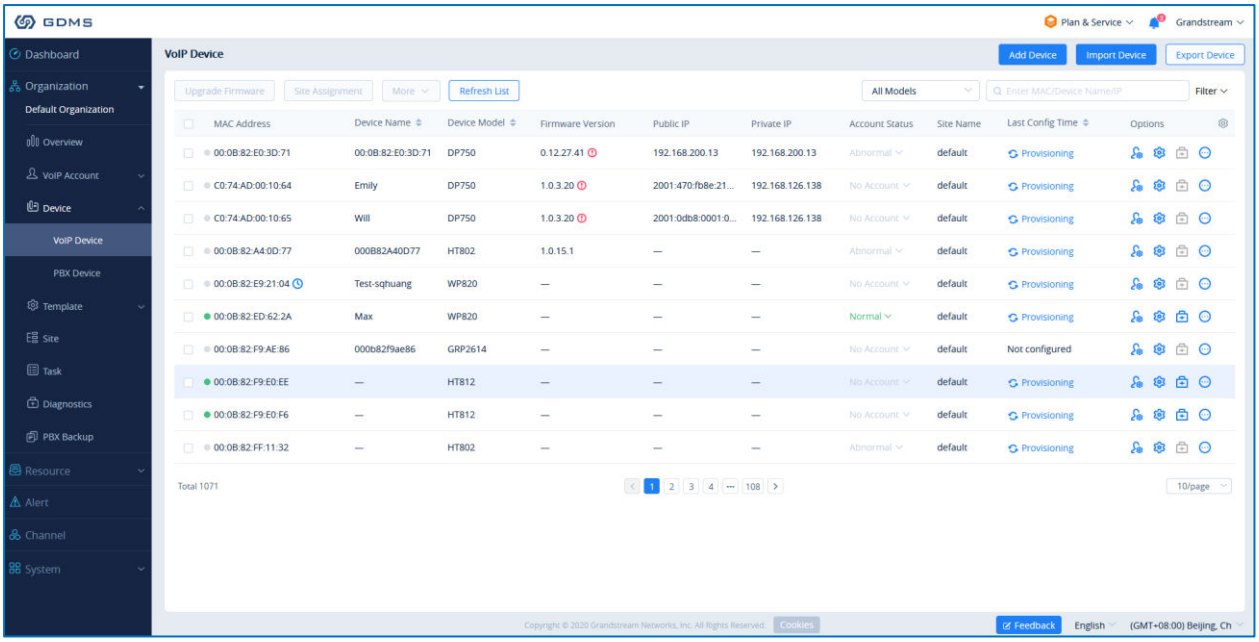


Figure 7: VoIP Device Management

Table 5: VoIP Device Management

Status	Descriptions
Status Indicator	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.
Account Status	Normal: The allocated accounts from GDMS platform to the devices are registered successfully, and all accounts can be used normally.

	Abnormal: Some of the device's allocated accounts are unregistered. This may be due to the following reasons: • The account is not activated. • The account registration credentials are incorrect. • The account was modified on the device. No Account: GDMS platform does not allocate any account to the device.
Last Config Time	**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. **Date/Time**: The date and time of the last successful provisioning.
Call Status	**Idle:** The SIP account is in idle state. **Busy:** The SIP account is in a call.
HS Status	The SIP account is configured on the handset. The SIP account is not configured on the handset.

Table 6: Operation Instructions

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.

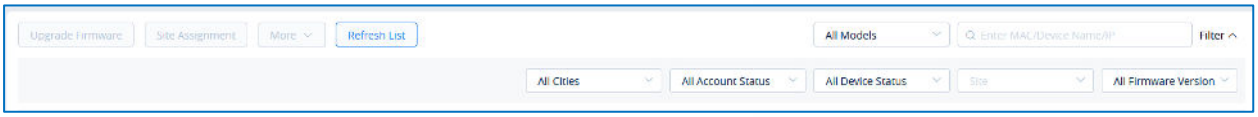


Figure 8: Search Devices

Add Device

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

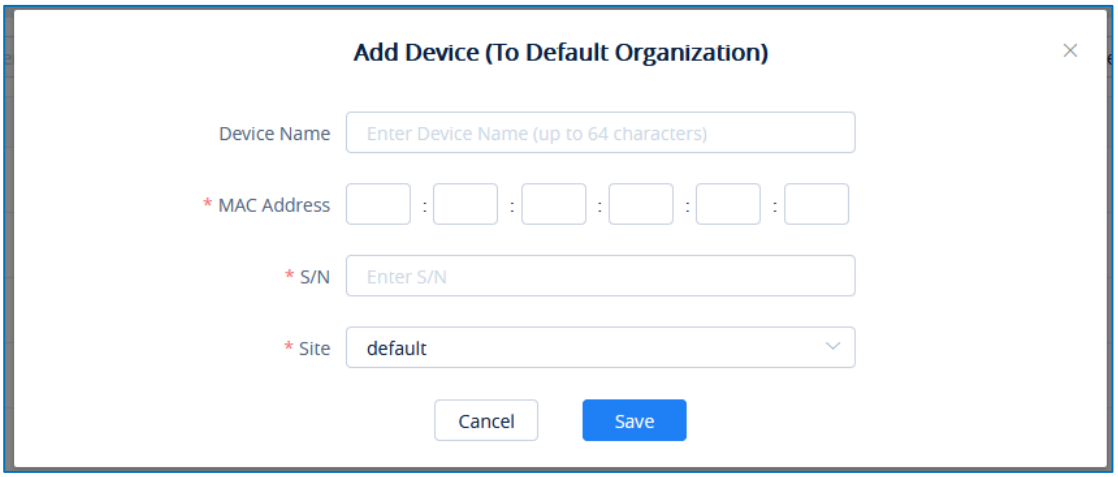


Figure 9: Add VoIP Device

Table 7: 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.

Notes:

- Users could click on “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 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:

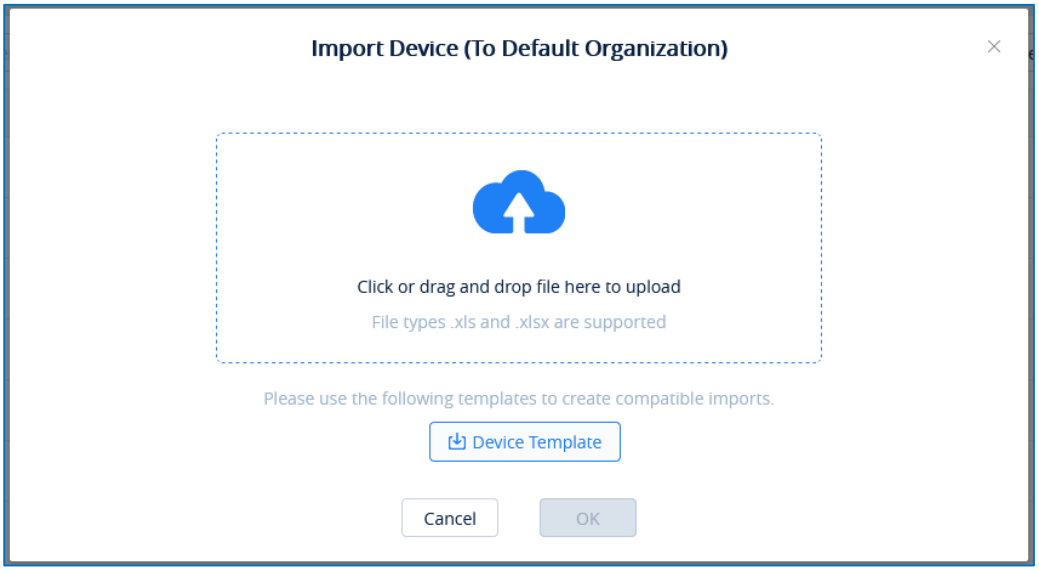


Figure 10: Import VOIP Device

1. Click on the

button to download the template. Users must follow the instructions to enter the required information.

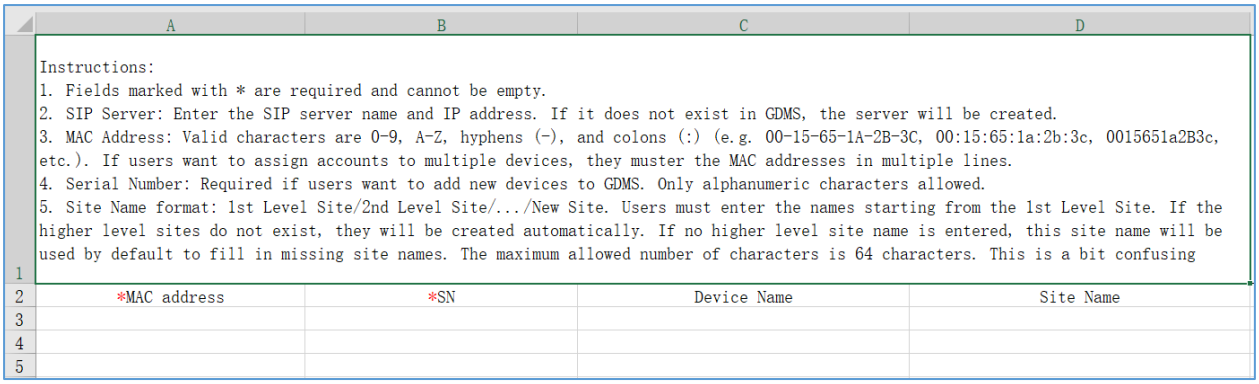


Figure 11: Import VoIP Device Template

2. The template will have the following fields:

Table 8: Import VoIP Device Template

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.

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.

Notes:

- 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:

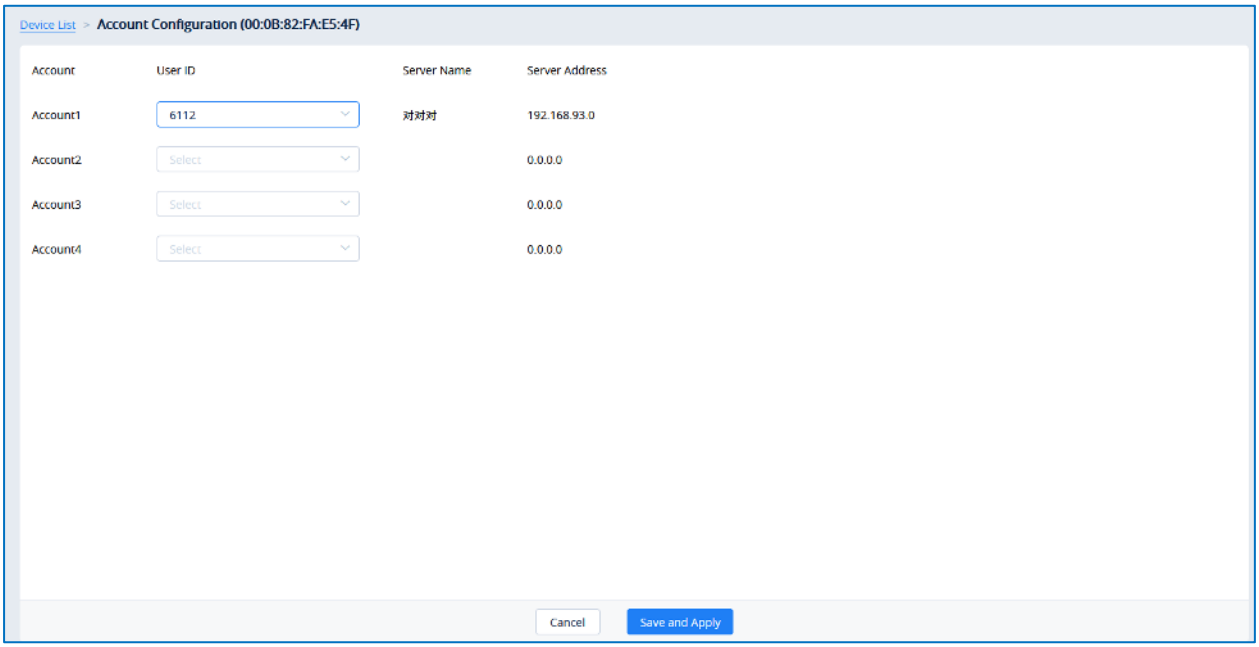


Figure 12: Configure SIP Account

3. On this **Account Configuration** page, users can select the SIP accounts created in the **SIP Account** page to assign to the device.

4. Users could also select to replace the existing SIP account for 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.

Notes:

- 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:

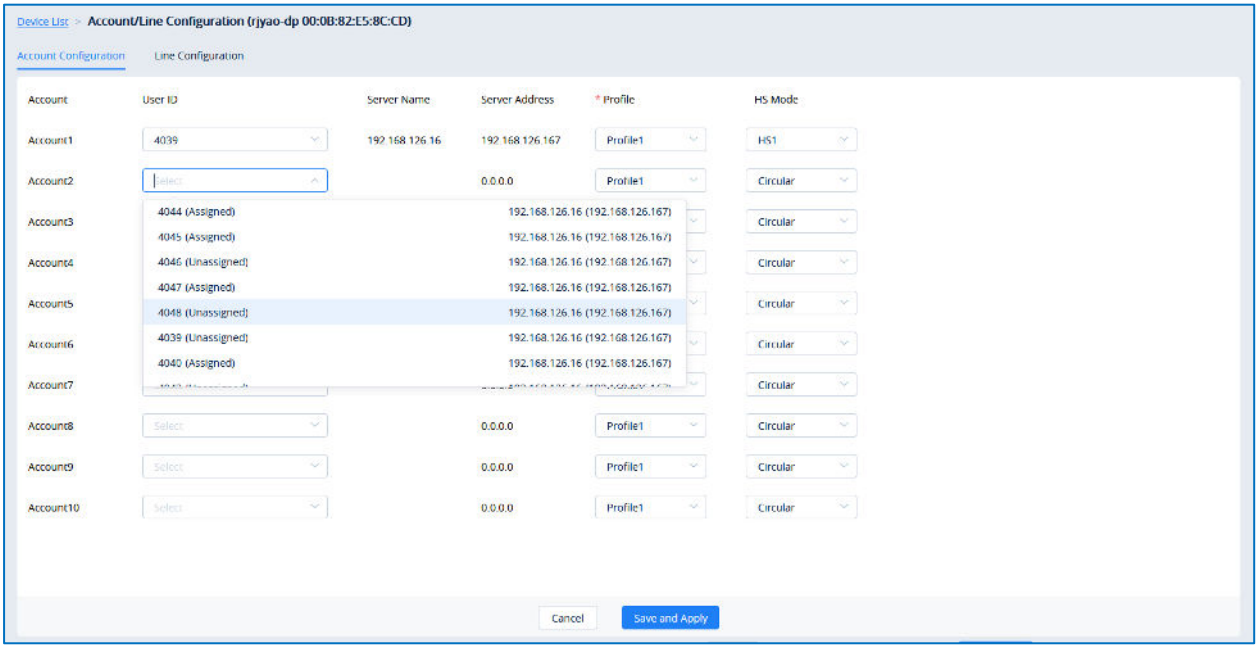


Figure 13: Configure SIP Account for DP Devices

Table 9: 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.

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

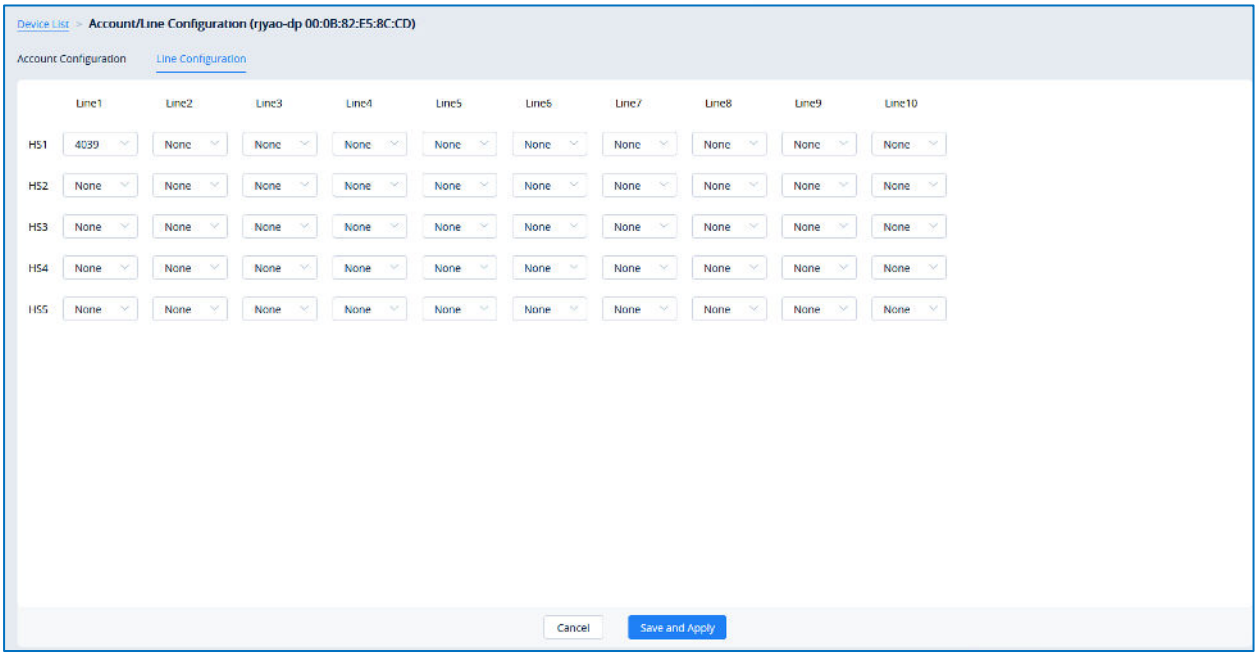


Figure 14: Line Configuration

Note:

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.

Notes:

- 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:

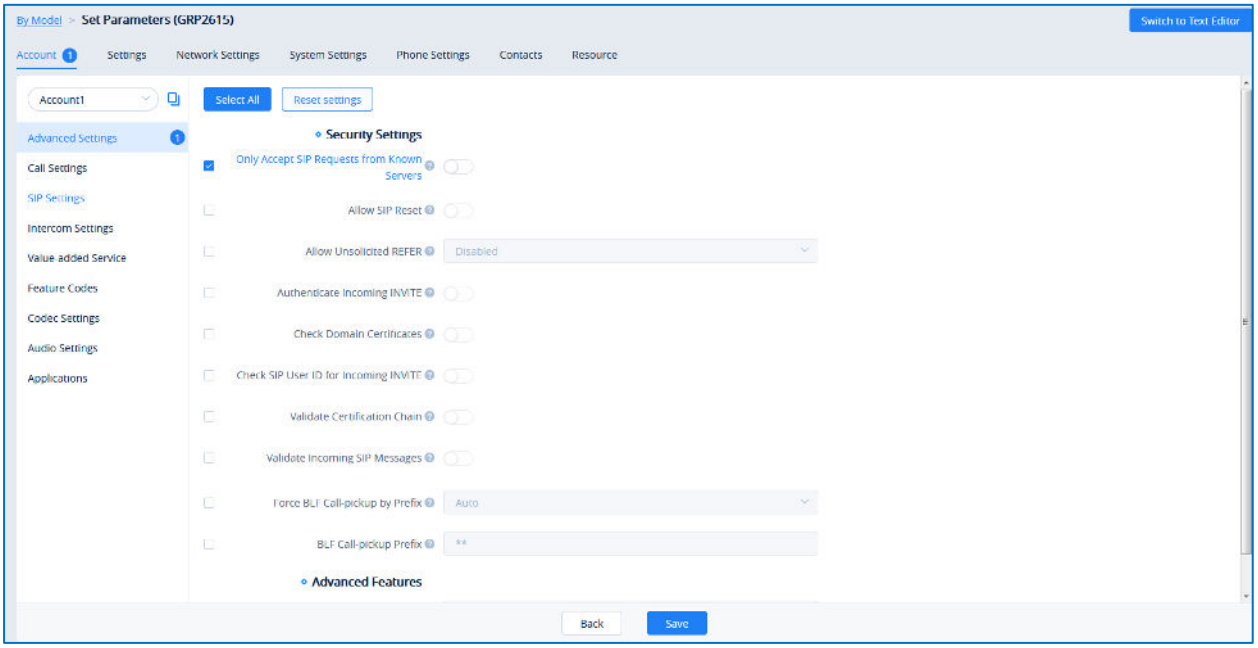


Figure 15: Device Parameter Configuration

a) Clicking on the **Select All** button will select every option on the current page. Clicking on it again will deselect all the options.

b) Clicking on the **Reset Settings** button will restore all settings on the current page to default values.

c) Clicking on the button following the account, users can copy and paste the current account configuration to other accounts.

d) When users try to configure 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.

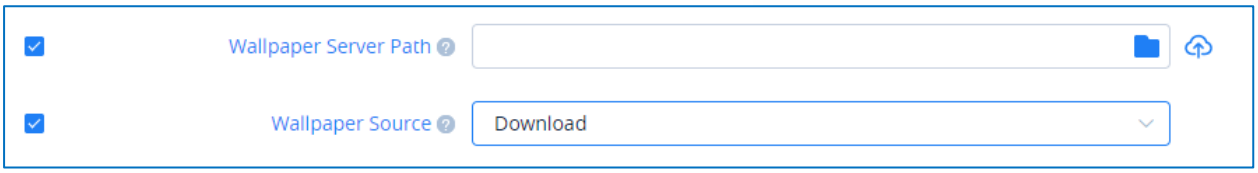


Figure 16: Ringtone Configuration

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).

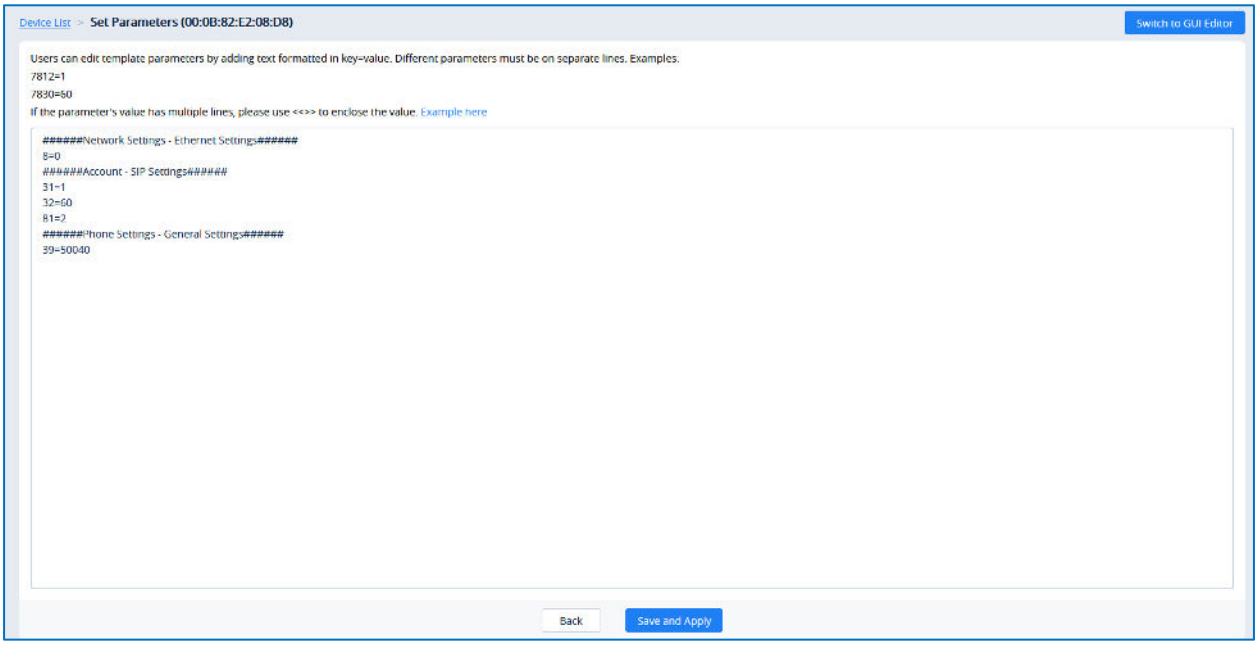


Figure 17: Edit Configuration File

a. The format requirement is key=value. Key can be either a P-value or an alias.

b. 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.

Notes:

- 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.

Configure Resource Files

Users can configure custom ringtone and language 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:

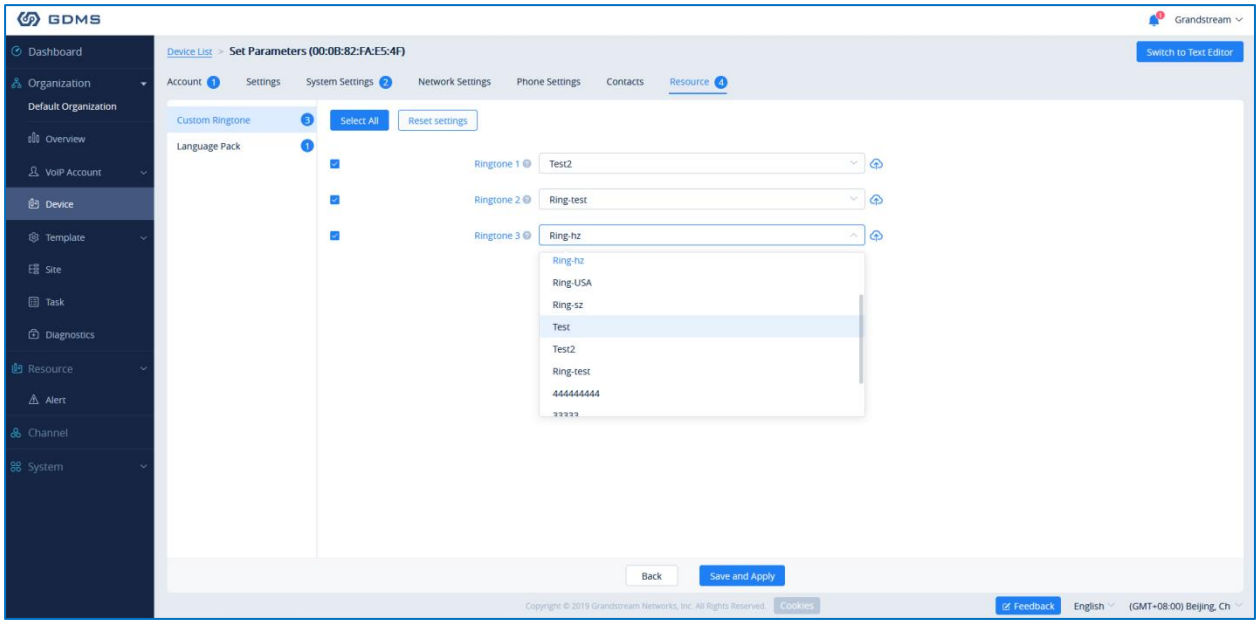


Figure 18: Resource Configuration

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 “Save and Apply” button, the device will download the selected resources from the firmware path.

Note:

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 local configuration to the GDMS server.

1. Select a specific device, click icon and select 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 configuration and parameters of the current device to the GDMS server.

Notes:

1. If the device's parameter configuration conflicts with the server's configuration, the device's local configuration prevails.
2. If the account on the device does not exist on the GDMS server, the SIP account and server are automatically created in GDMS server.

Disable Push Configuration

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

1. Select a specific device, click icon and select option "**Disable Push Configuration**".

2. Click "**OK**" to confirm the operation, the account configuration or parameters will not be pushed to the device through 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.

Notes:

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 Device Details

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

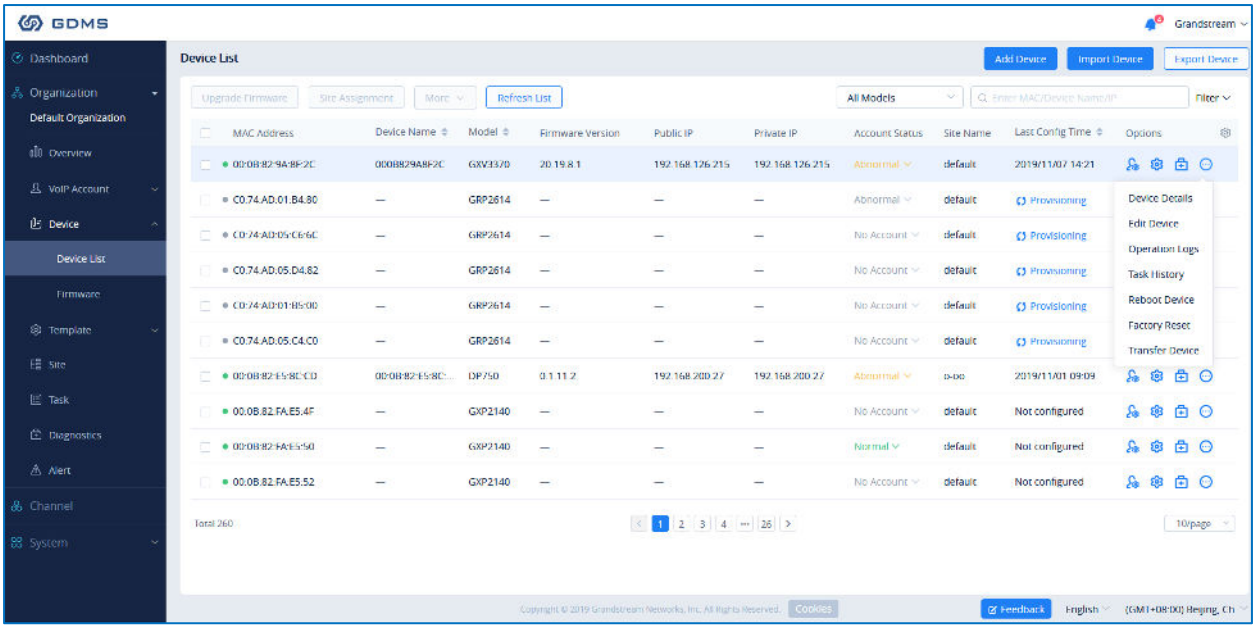


Figure 19: View VoIP Device Details

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

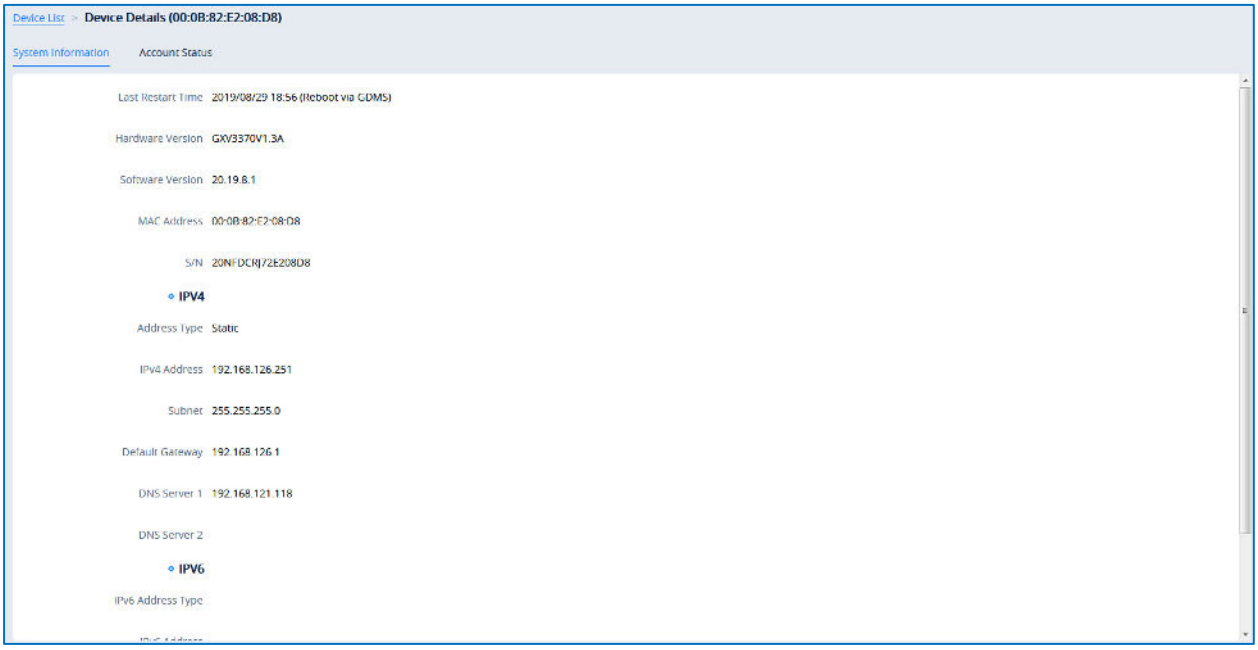


Figure 20: VoIP Device Details

Note:

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

Edit 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 to the device editing page.

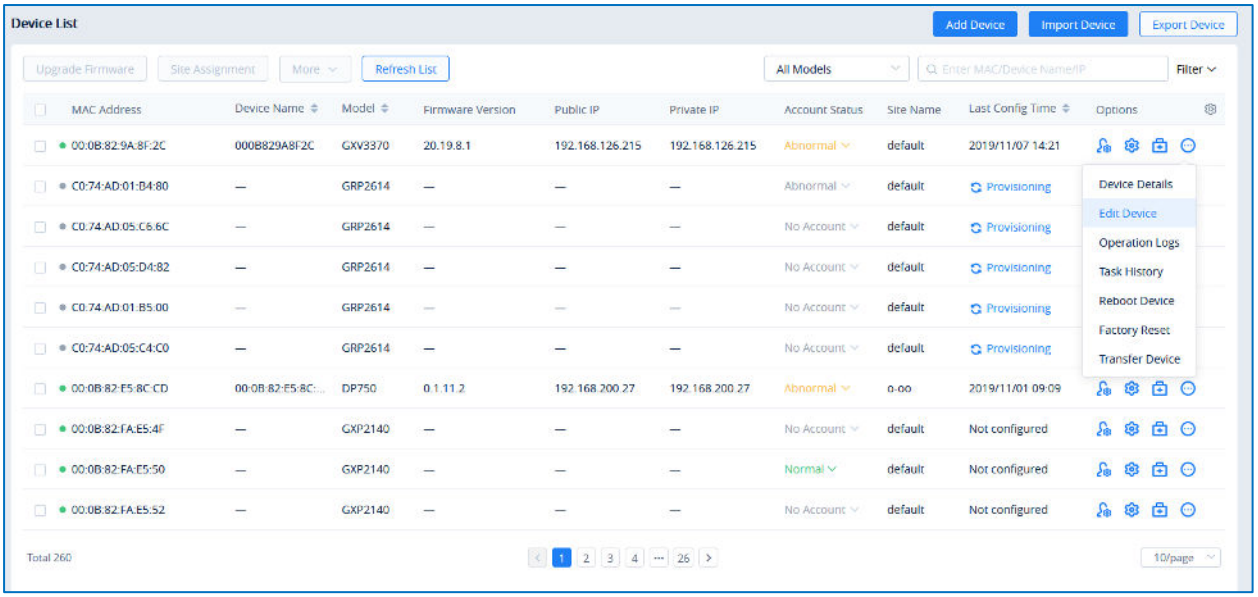


Figure 21: Edit VoIP Device Option

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

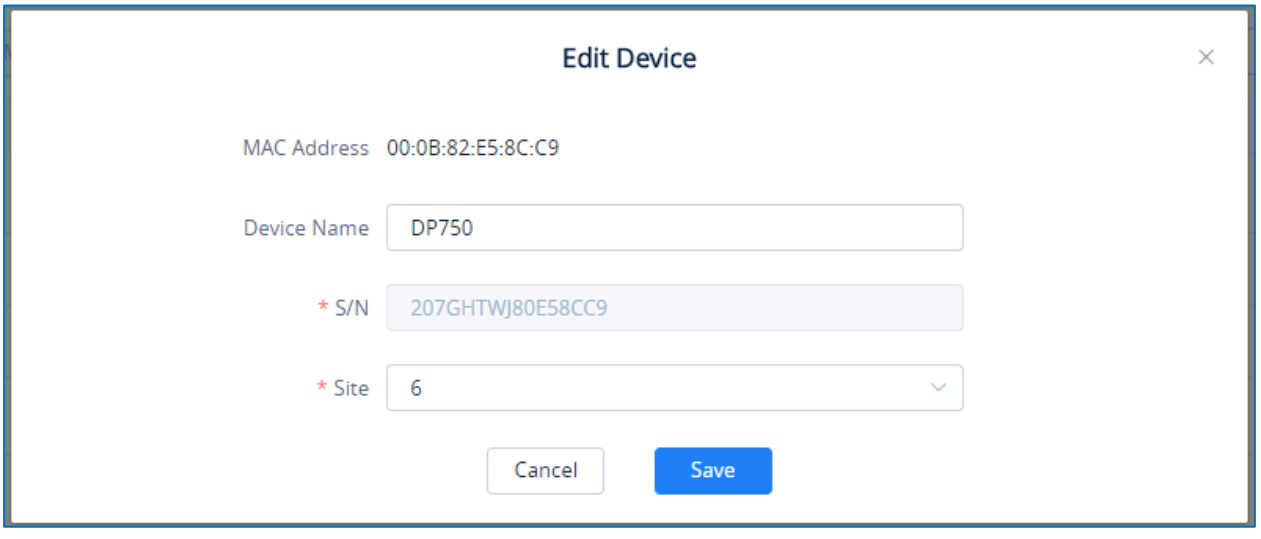


Figure 22: Edit VoIP Device

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

View 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 “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, and etc.

Note:

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

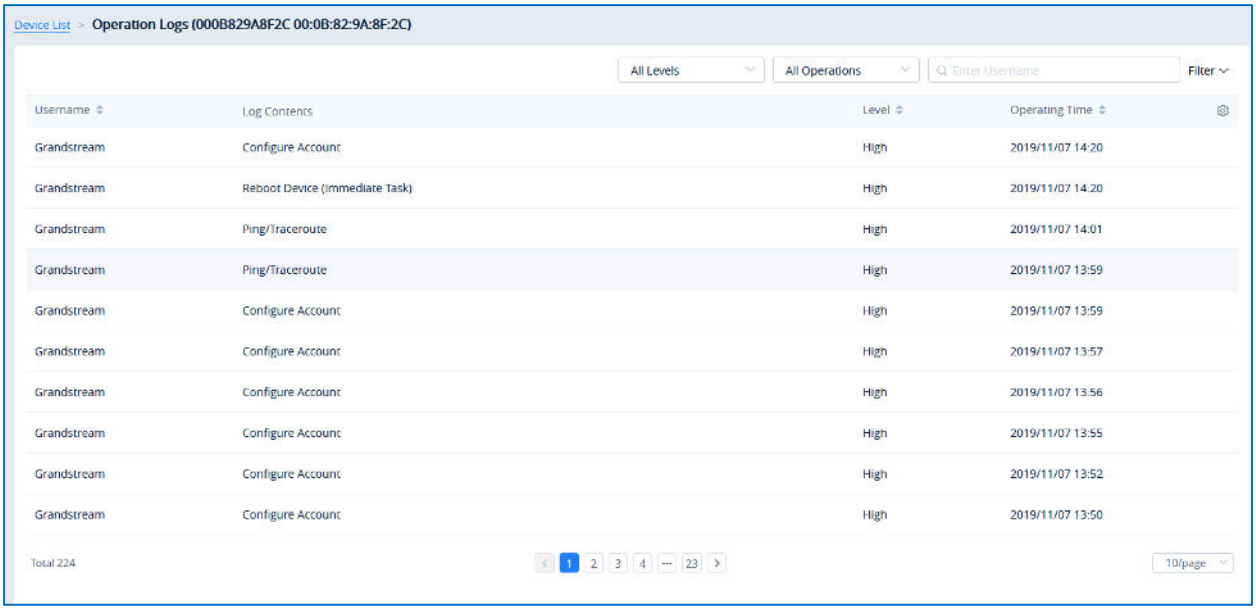


Figure 23: View VoIP Device Operation Logs

View Device Task History

Users could view all task histories 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 “Task History” button.

2. Access to the Task management page, and search for all tasks of the specific device.

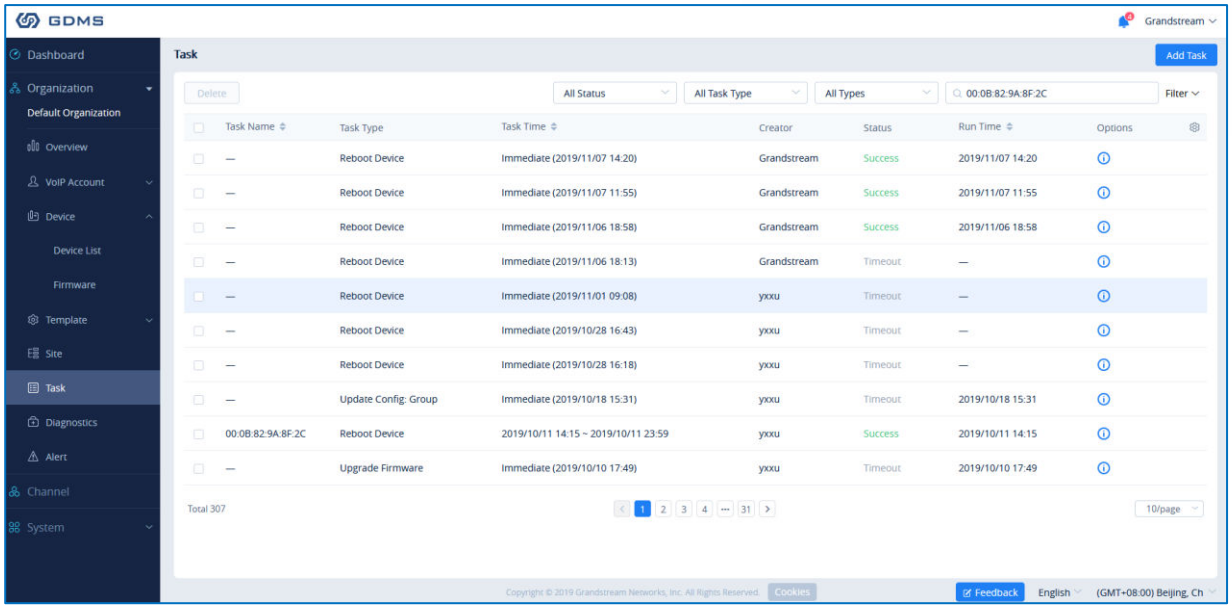


Figure 24: View VoIP Device Task History

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 button **Upgrade Firmware** on the top of the Device page.

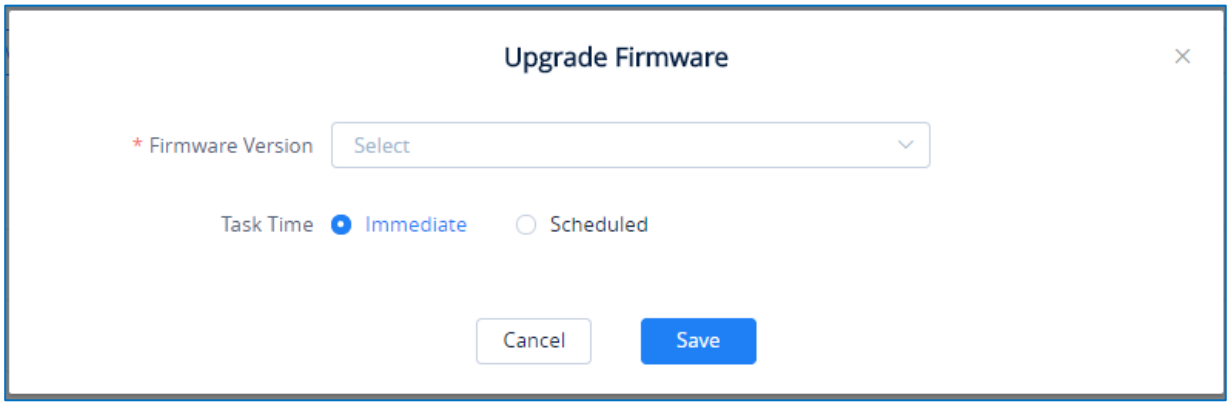


Figure 25: Upgrade Firmware

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.

Notes:

- 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.

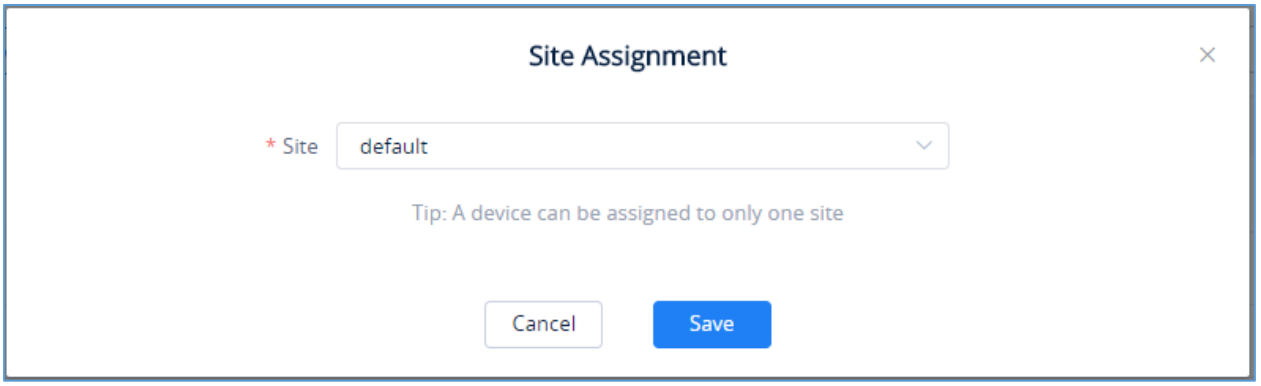


Figure 26: Site Assignment

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

Note:

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**.

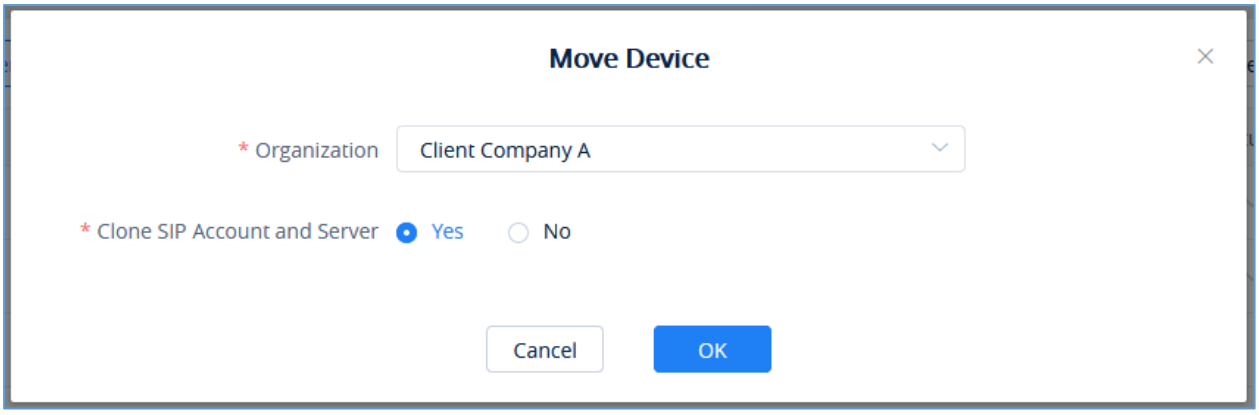


Figure 27: Move Device

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

Reboot 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**.

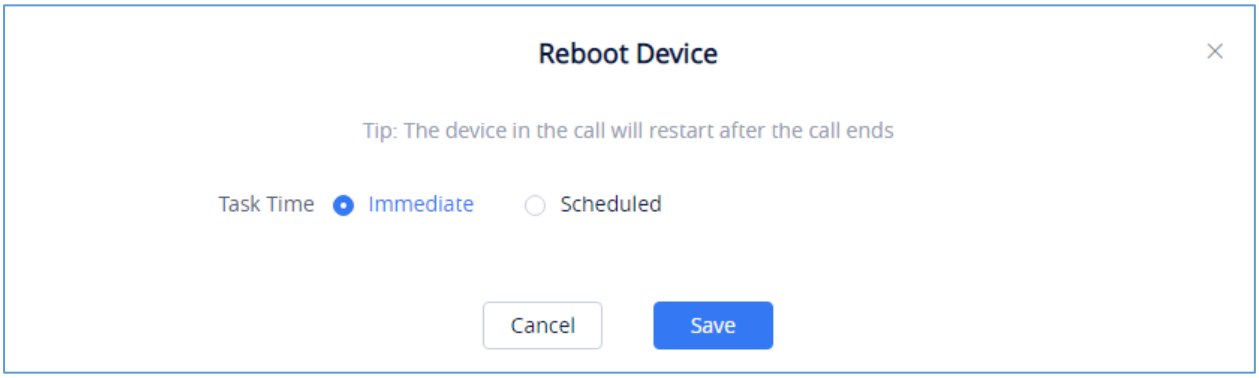


Figure 28: Reboot Device

2. **Task Time**: Select when to start the device reboot. Users can choose to reboot immediately or to 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**.

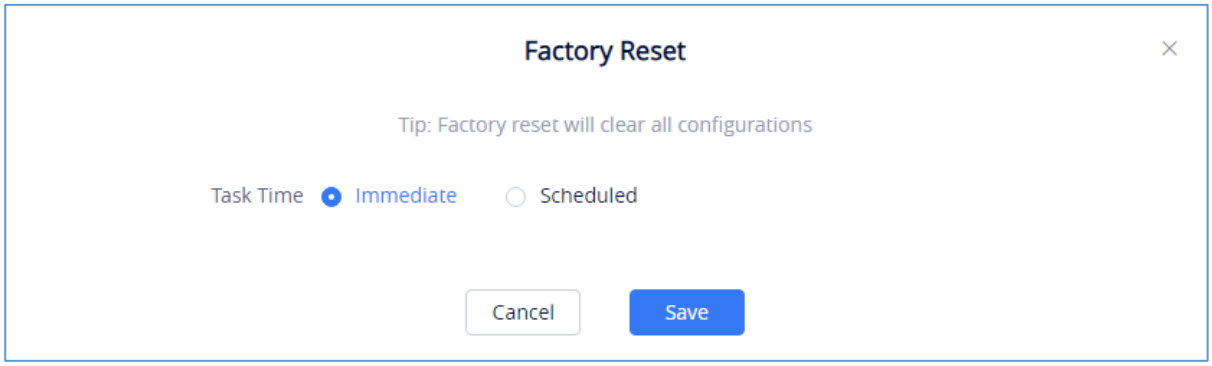


Figure 29: Factory Reset

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.

Notes:

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 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**.

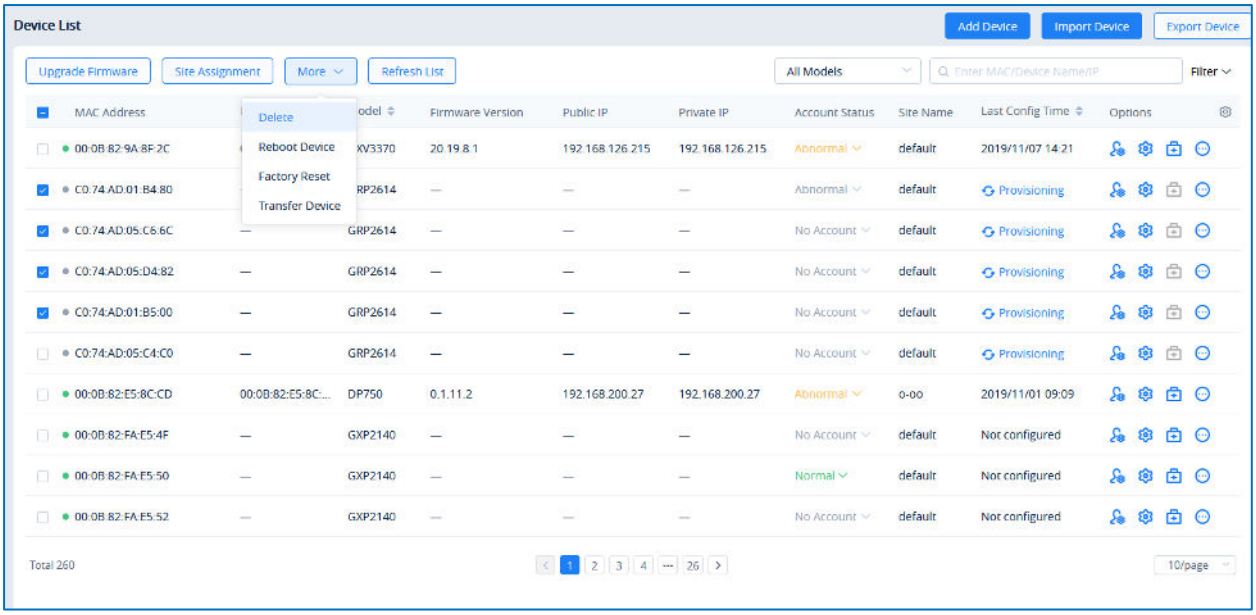


Figure 30: Delete Device

2. Click on **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 involve the deleted devices will be canceled either.

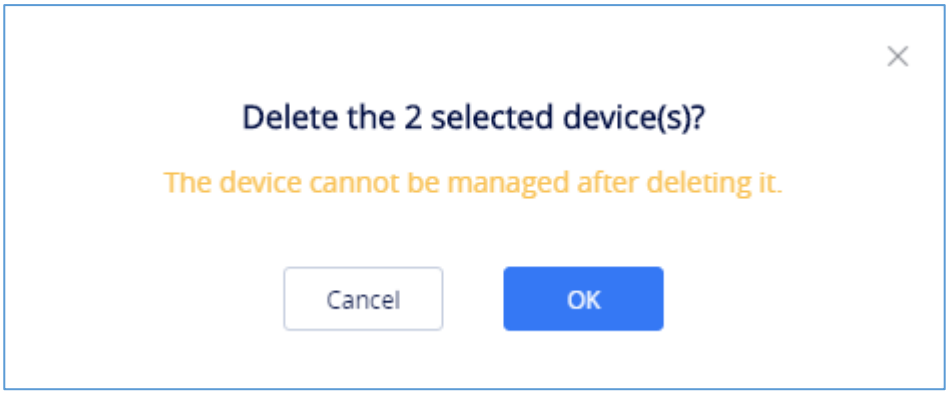
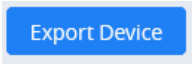


Figure 31: Delete Device Prompt

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 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 “More” button following the device and select to access “Authorization Management” interface, as the screenshot shows below:

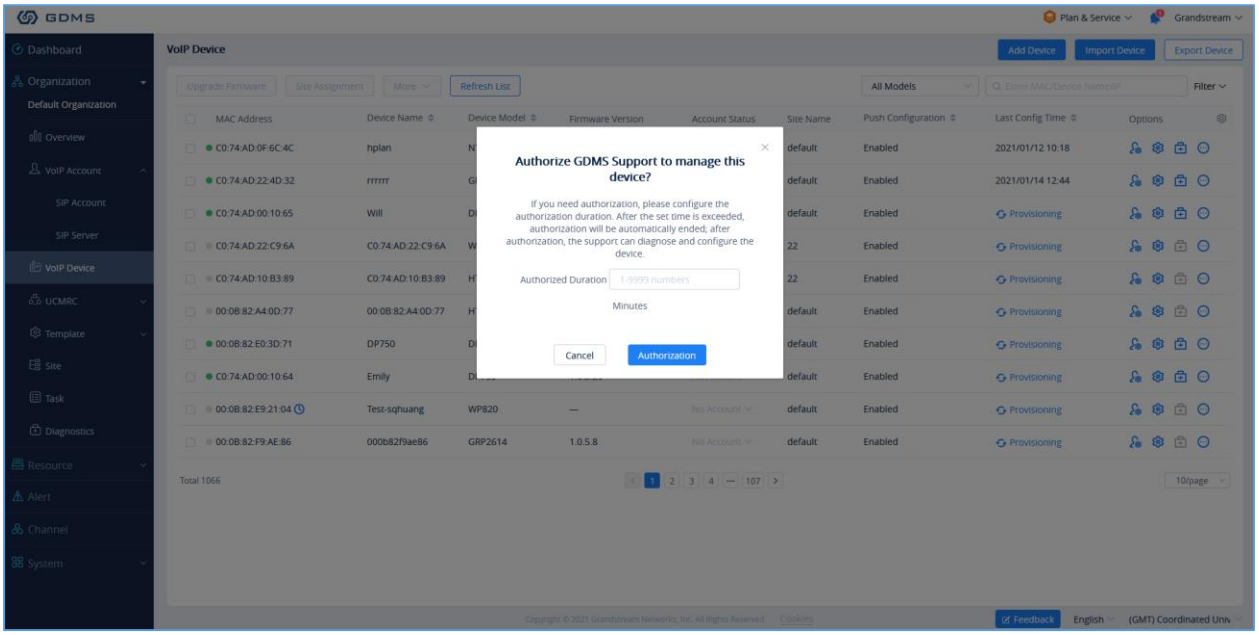


Figure 32: Authorization Management

1. Enter the authorization duration, which can be set between 1 to 9999 minutes, according to the time required for problem troubleshooting.

2. Once the user clicks “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 “More” button following the device, and select to access “Authorization Management” interface, as the

screenshot shows below:

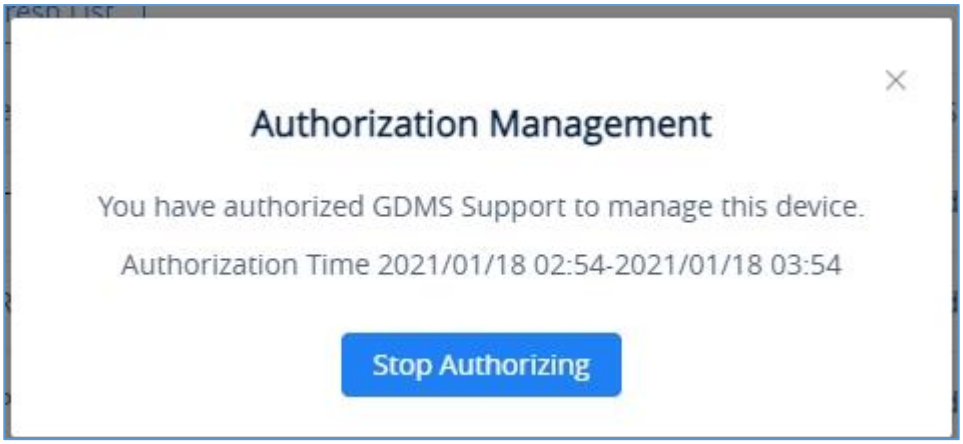


Figure 33: Stop Authorizing Manually

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

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.

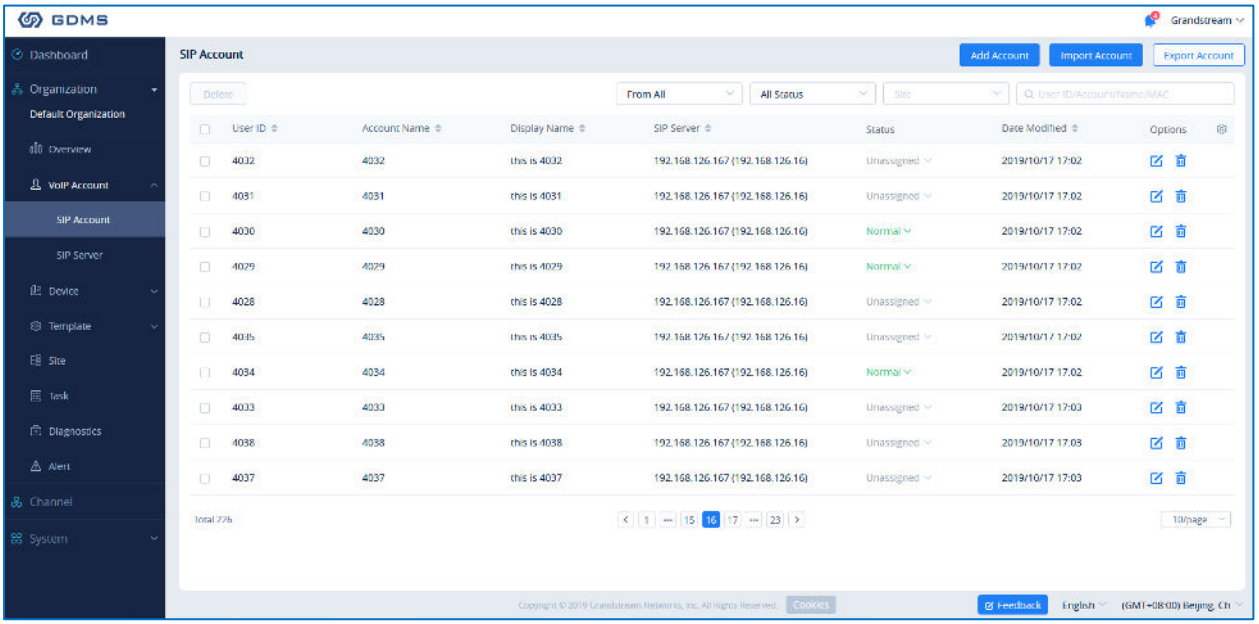


Figure 34: Account Management

Table 10: Account Status Description

Status	Description
Status	Normal: All devices using the account are registered, and the account is working normally. Abnormal: At least one device using this account is not registered. Possible reasons include: • The device is unable to register successfully. • The account was modified through other means such as through the endpoint device web portal or provisioning. Unassigned: No devices are using this account.
From UCM	UCM: 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. The user can only edit SIP server, assign device, and cannot edit other information.

Table 11: Operation Description

Operation	Descriptions
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/hided options.
Filter and Search	Filter accounts by status, site, and search for specific accounts by entering in their user IDs, account names, or display names.

Add SIP Server

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

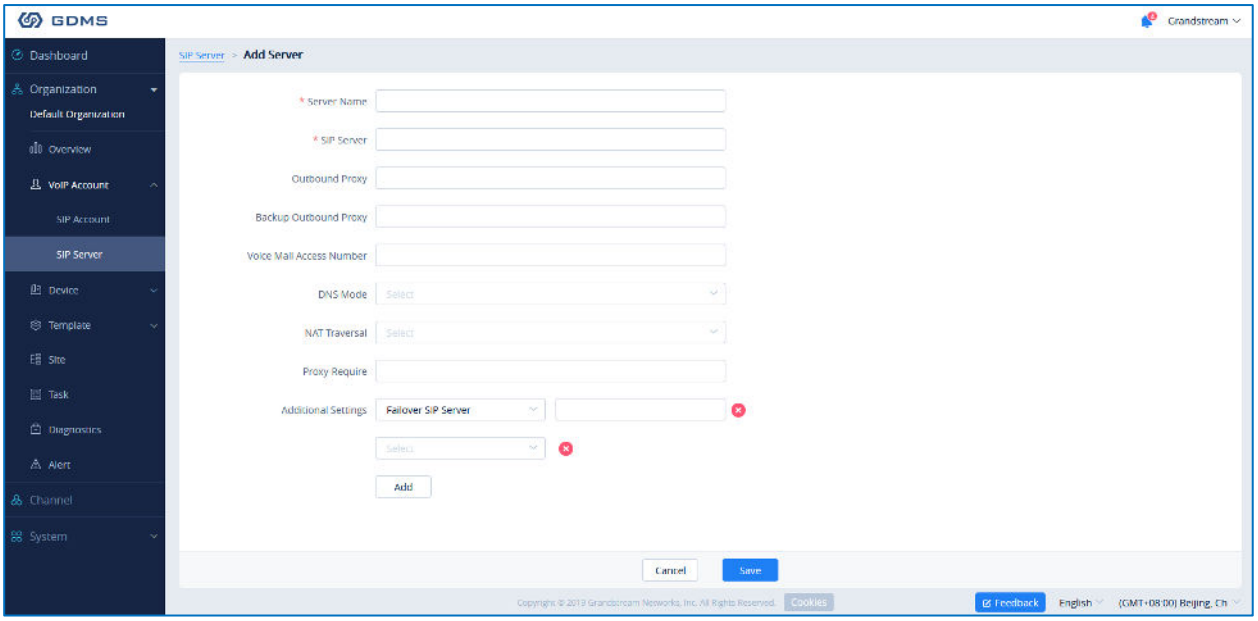


Figure 35: Add SIP Server

Table 12: 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 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 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	Defines which DNS service will be used to lookup IP address for SIP server's hostname. There are three modes: • **A Record** • **SRV** • **NATPTR/SRV** To locate the server by DNS SRV set this option to "SRV" or "NATPTR/SRV".
NAT Traversal	Specifies which NAT traversal mechanism will be enabled on the phone system. It can be selected from the dropdown list: • **NAT NO** • **STUN** • **Keep-alive** • **UPnP** • **Auto** • **VPN** If the outbound proxy is configured and used, it can be set to "NAT NO". If set to "STUN" and STUN server is configured, the phone system will periodically send 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. If set to “Keep-alive”, the phone system will send the STUN packets to maintain the connection that is first established during 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. If it needs to use OpenVPN to connect host server, it needs to set it to “VPN”. 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 which port to allow SIP through.
Proxy-Require	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.
Custom Field	Users could add the custom fields below. Some custom fields are only available for some certain device models: (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 For detailed filling rules, please refer to the User Guide of the devices.

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

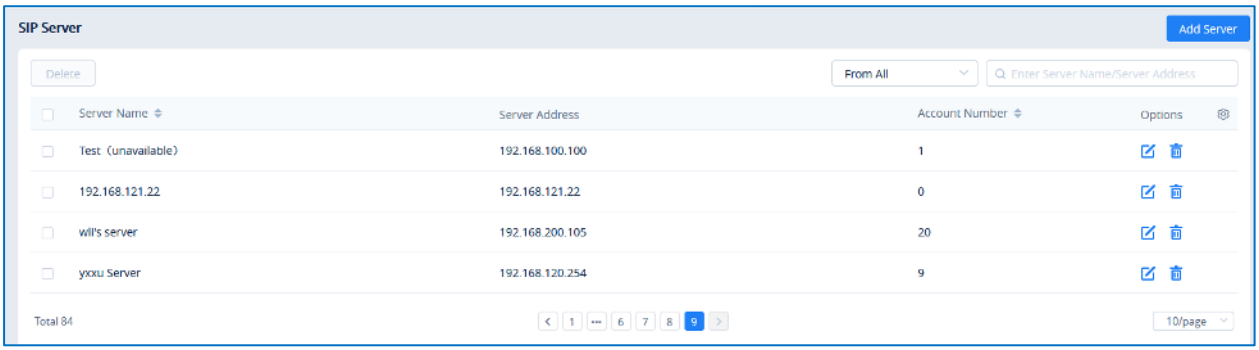


Figure 36: Finish Adding SIP Server to GDMS

Add SIP Account

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

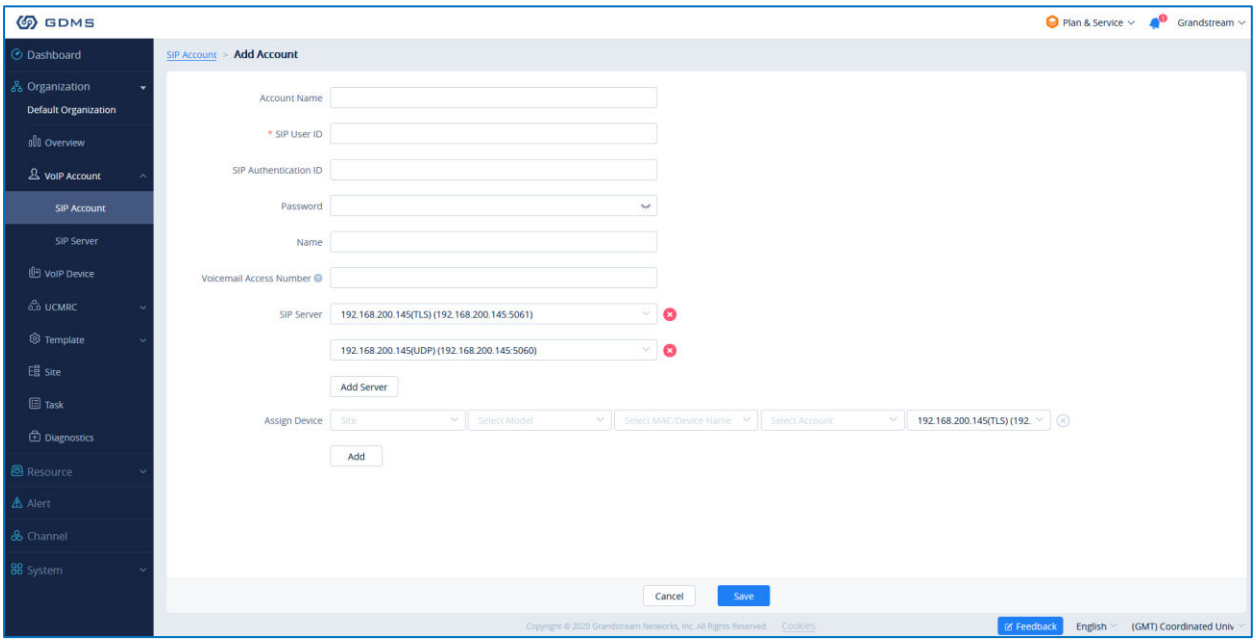


Figure 37: Add SIP Account

Table 13: Add 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 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 purpose.
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 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 “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 Remote Connect plan can synchronize multiple protocol server addresses to GDMS platform), the user can configure it and assign to devices separately.
Assign device	This option will allow to assign 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:

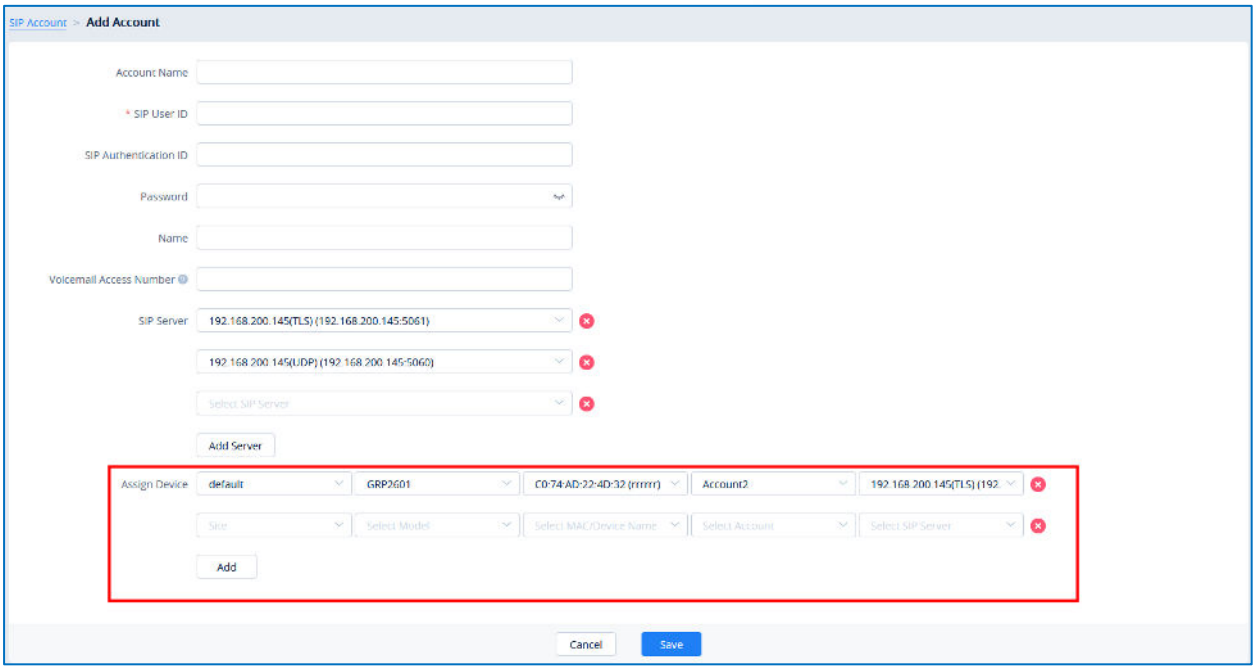


Figure 38: Assign Device

Table 14: 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 which the account will be allocated to.
Select Device MAC Address	This is a necessary option. Users need to select the device MAC address which the account will be allocated to.
Select Account Index	This is a necessary option. Users need to select the account index 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 UDP server address or UCM Remote Connect server address.

Notes:

- Assigning accounts to DP devices and HT devices from this page are 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 SIP accounts to it.

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 to the devices via Excel files.

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

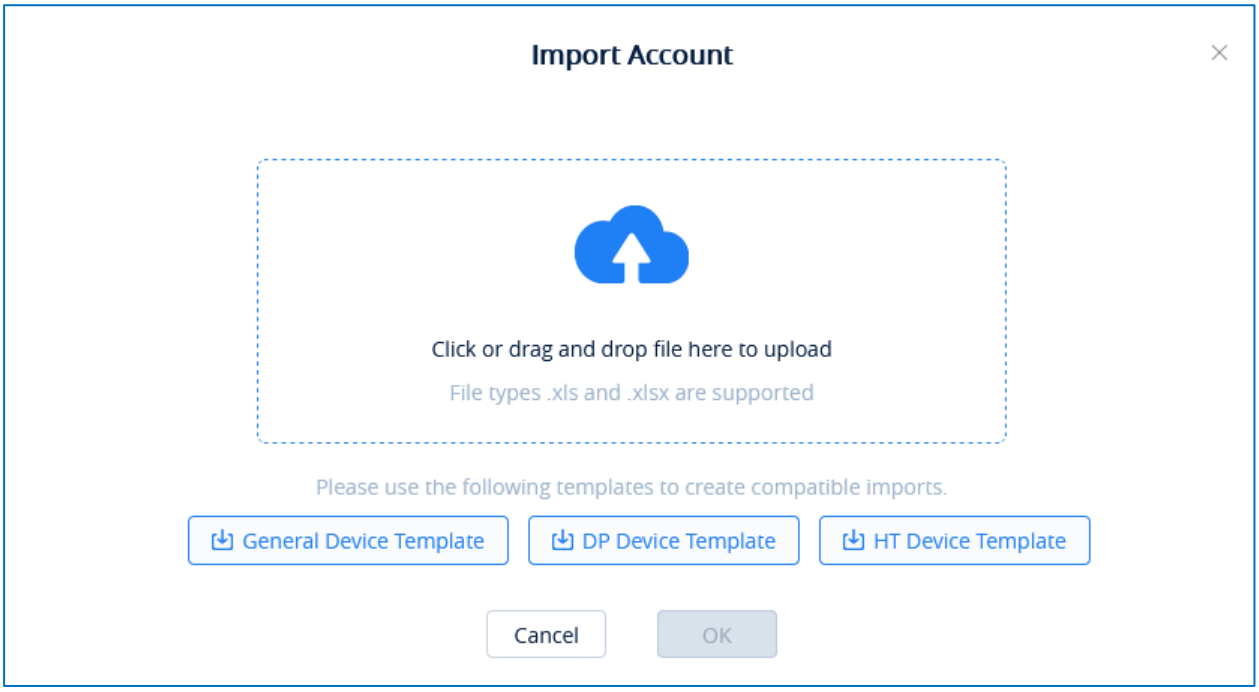


Figure 39: Import SIP Account

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

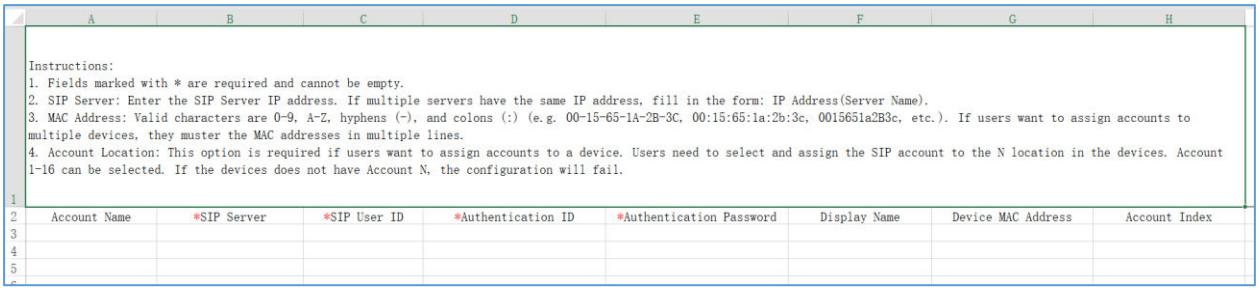


Figure 40: Import Account Template – General Device Template

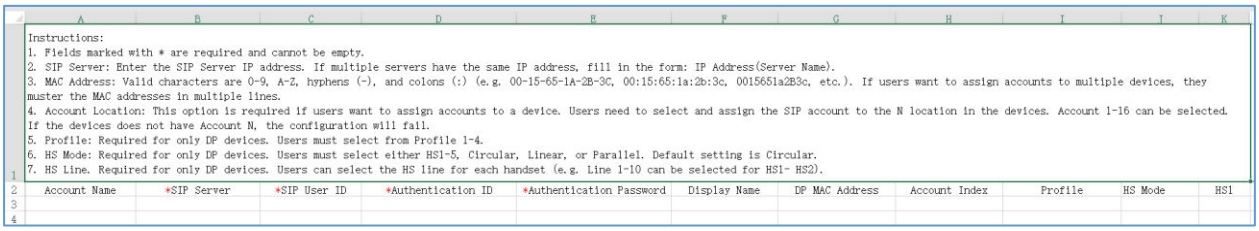


Figure 41: Import Account Template – DP Device Template

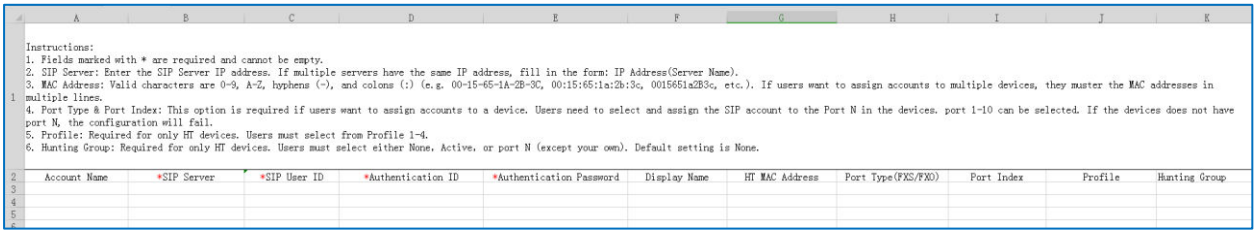


Figure 42: Import Account Template - HT Device Template

Table 15: Import Account Template Options

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 purpose.
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 which the account will be allocated to (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 besides your own.

3. 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.

4. 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 correct information to allocate to the devices. Please see the example below, the SIP account display name “Sqhuang” will be allocated to 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	Sqhuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	100	100	123456	Sqhuang123	00:0B:82:D2:11:22	Account1

Figure 43: 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:aa:bb: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	Sqhuang	00:aa:bb:cc:ee:dd	Account1

Figure 44: Example II

3. If the user wants to allocate multiple SIP accounts to a single device, here is the 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	Sqhuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	200	200	123456	Sqhuang	00:0B:82:E2:08:D8	Account2
Work Account	192.168.200.100	300	300	123456	Emily	00:0B:82:E2:08:D8	Account3

Figure 45: Example III

4. If the user wants to allocate multiple SIP accounts to a single DP device, here is the 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	Sqhuang	00:0B:82:E2:08:D8	Account1	Profile1	HS1	Line 1				
Work Account	192.168.120.100	200	200	123456	Sqhuang	00:0B:82:E2:08:D8	Account2	Profile1	Circular	Line 2	Line 1			
Work Account	192.168.200.100	300	300	123456	Sqhuang	00:0B:82:E2:08:D8	Account3	Profile2	Circular	Line 3	Line 2			

Figure 46: 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	Sqhuang	00:0B:82:E2:08:D8	Account1
Work Account	192.168.120.100	200	200	123456	Sqhuang	00:0B:82:E2:08:D8	Account1

Figure 47: 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	Sqhuang	00:0B:82:E2:08:D8	Account2	Profile1
Work Account	192.168.200.200	300	300	123456	Sqhuang	00:0B:82:E2:08:D8	Account3	Profile1

Figure 48: 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	Sqhuang	00:0B:82:E2:08:D8	Account2	Profile1	Circular	Line 1	Line 1			
Work Account	192.168.200.200	300	300	123456	Sqhuang	00:0B:82:E2:08:D8	Account3	Profile2	Circular	Line 1	Line 2			

Figure 49: 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 **Edit Account** configuration page.

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

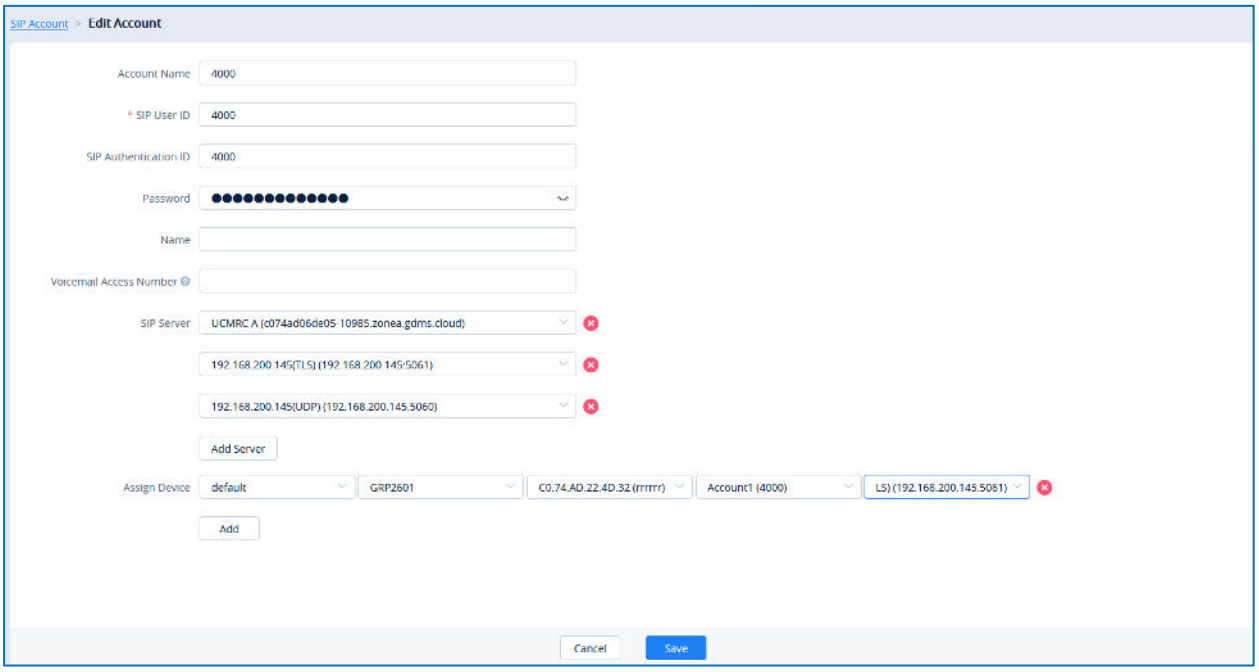


Figure 50: Edit Account

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.

Note:

1. If the device is offline at the time, its SIP account information will be updated when it is online again.

2. If the SIP server is synchronized from 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.

Note:

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 Sever**" button on the top of the interface.

3. Select the target SIP server, which can be searched by the server name.

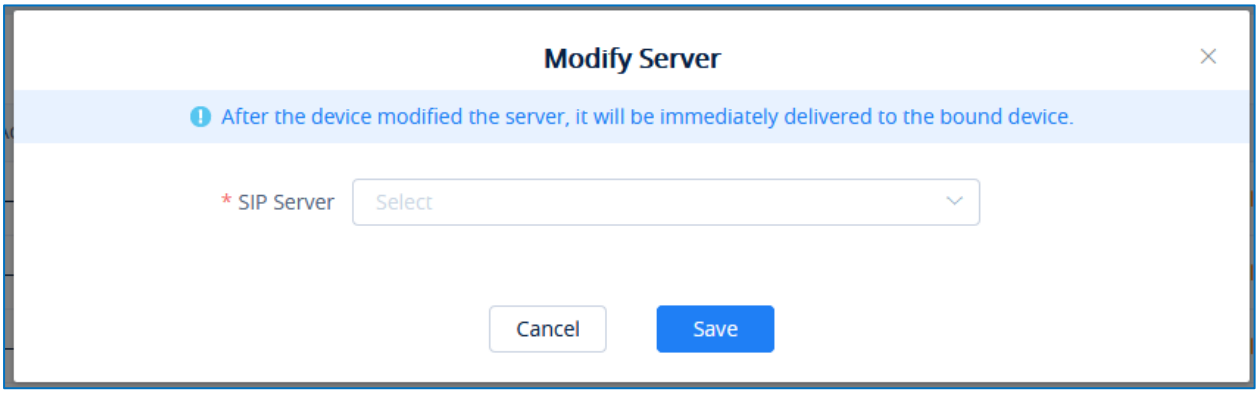


Figure 51: Modify SIP Server

4. After clicking "**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.

Note:

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:

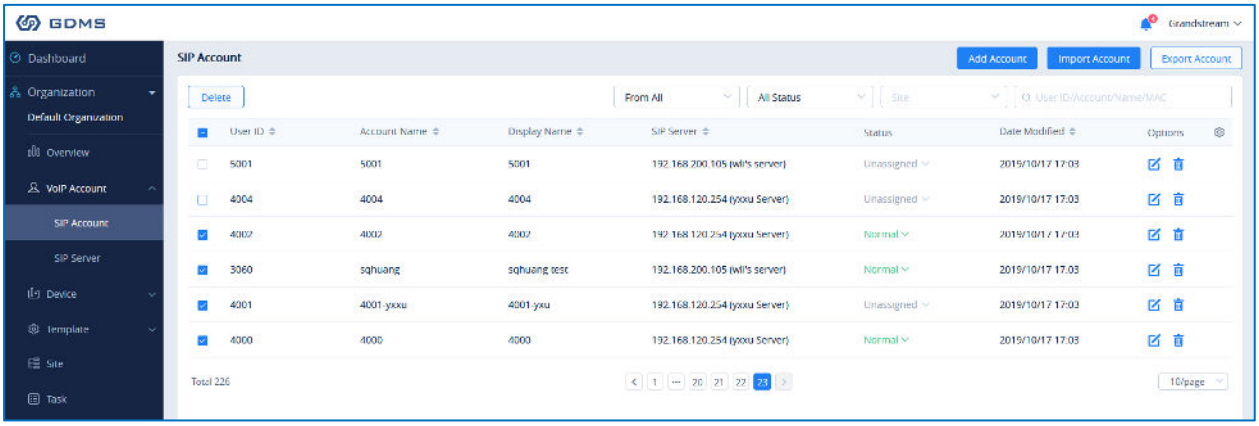


Figure 52: Delete Account

Note：

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.

Note： 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.

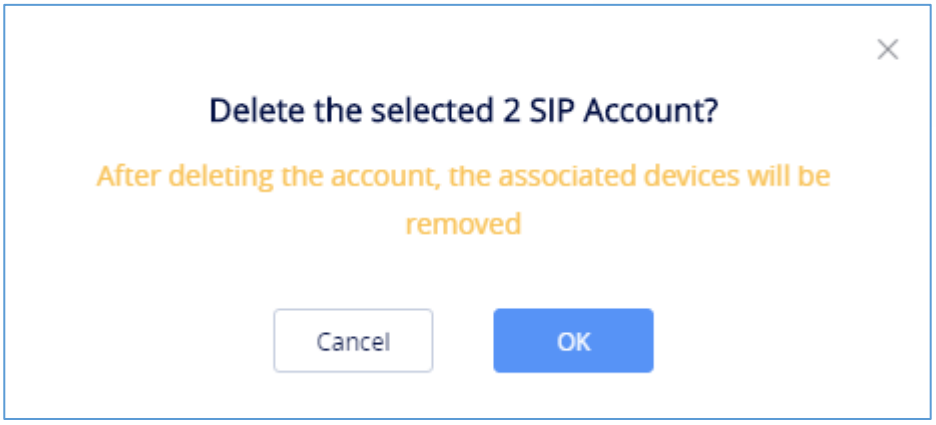


Figure 53: Delete SIP Server

Note：

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.

UCM REMOTE CONNECT - UCM DEVICE

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.

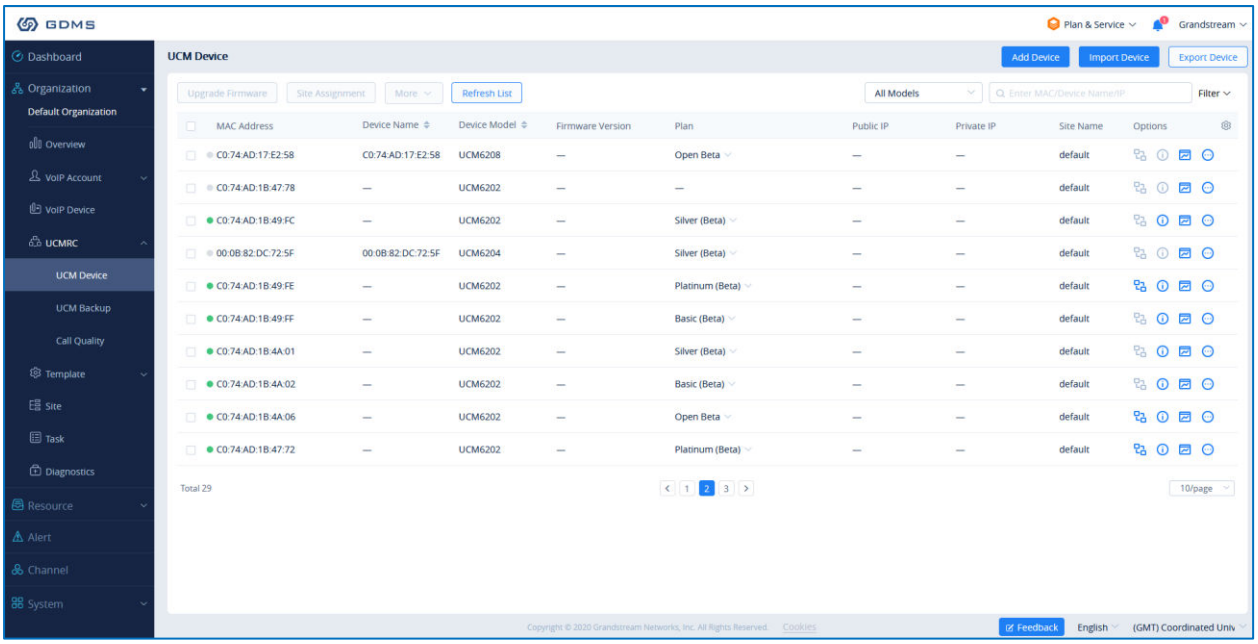


Table 16:UCM Device Management

Status	Descriptions
Status indicator	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	This icon indicates device firmware version too low and the device cannot be used normally with GDMS.
Plan expiring	Expire Soon This indicator means the plan is expiring soon or already expired.

Table 17: Operation Instructions

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.

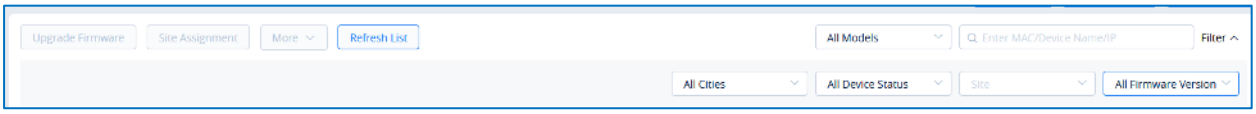


Figure 54: Search Devices

Add Device

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

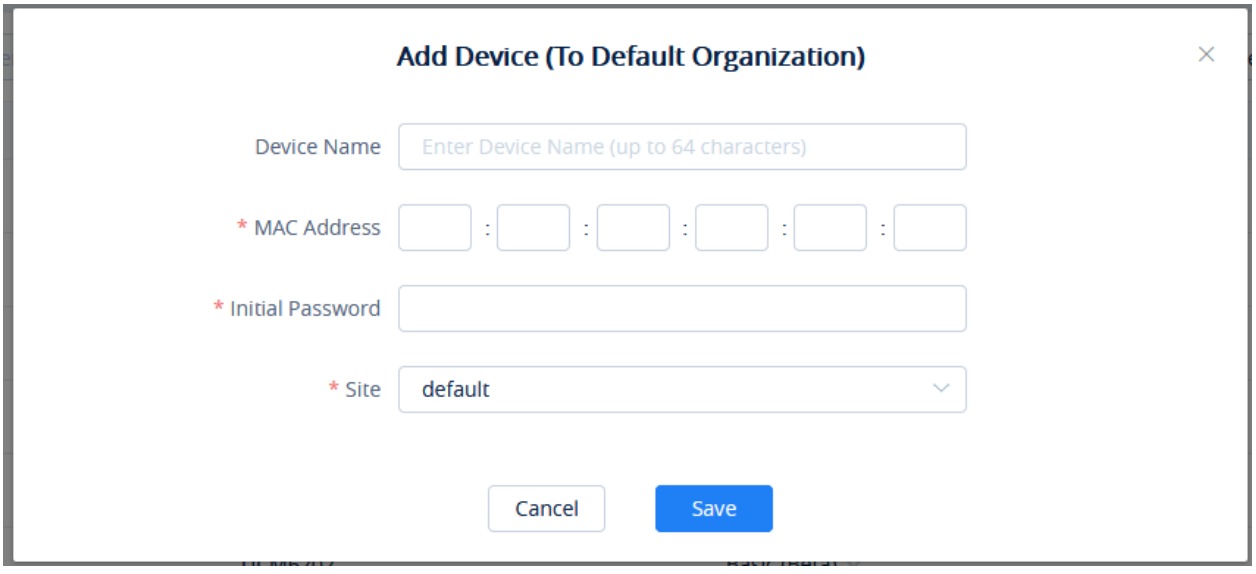


Figure 55: Add UCM Device

Table 18: 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 default setting is "Default" site.

Notes:

- Currently, users can only add UCM63xx devices to GDMS platform.
- When the device is added to GDMS platform successfully, the SIP accounts in UCM63xx will be synchronized to 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 "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 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:

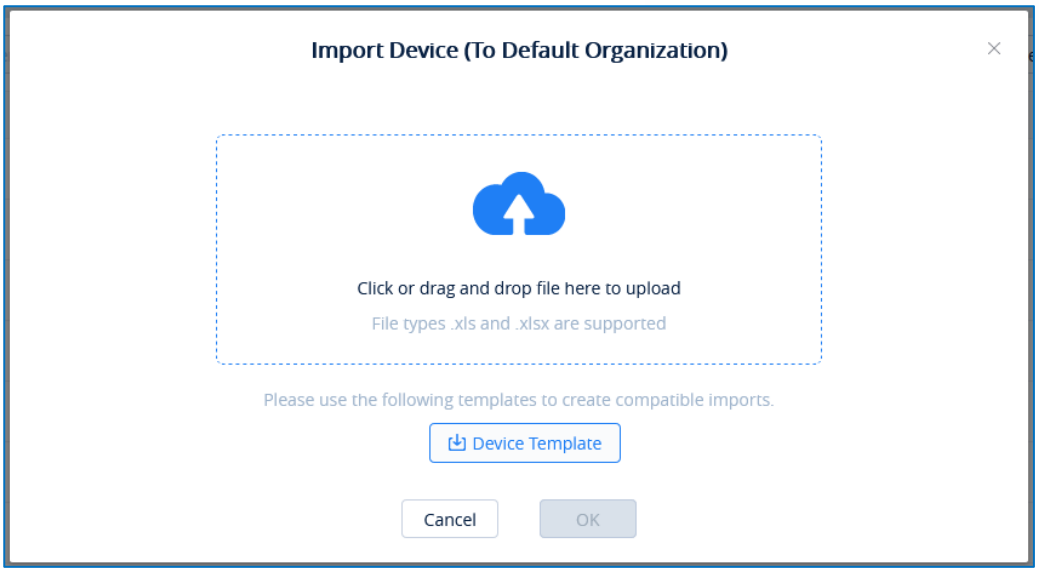


Figure 56: Import UCM Device

1. Click on the Device Template button to download the template. Users must follow the instructions to enter the required information.
2. The template will have the following fields:

Table 19: Import UCM Device Template

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. Maximum character limit is 64.

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.

Notes:

- Currently, users can only add UCM63xx devices to GDMS platform.
- When the device is added to GDMS platform successfully, the SIP accounts in UCM63xx will be synchronized to GDMS platform by default. If the user wants to turn off the synchronization function, please refer to the UCM63xx Remote Connect Guide for details.
- 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.

View Device Details

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

Figure 57: View UCM Device Details

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

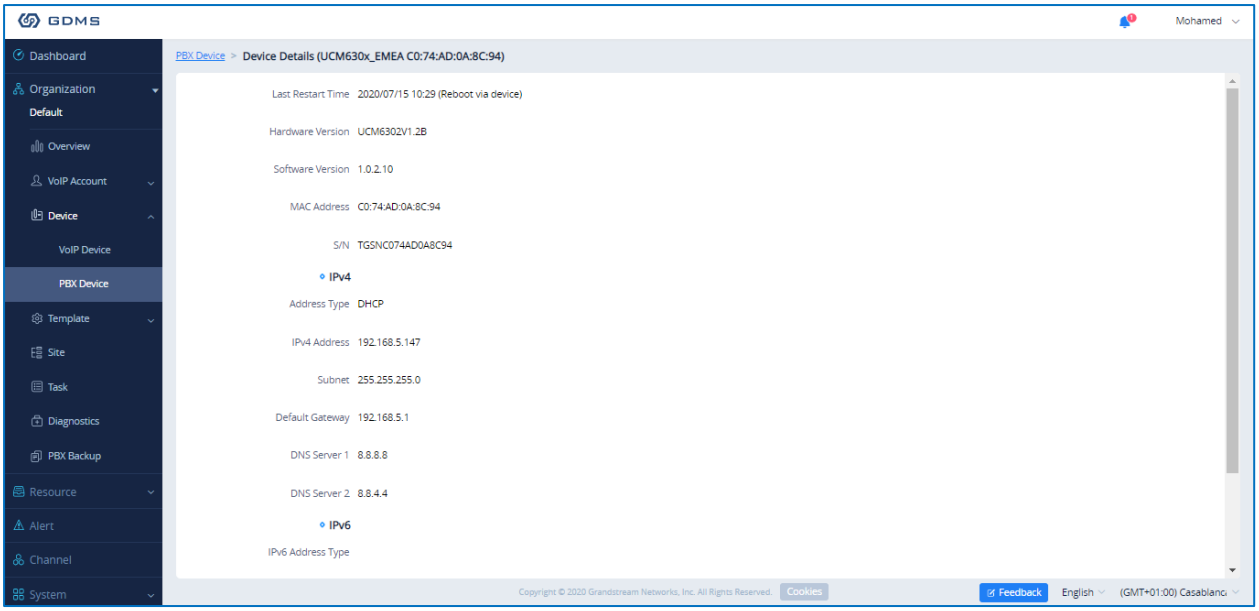


Figure 58: UCM Device Details

Note:

The information in 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, current used cloud storage space and total cloud storage space.

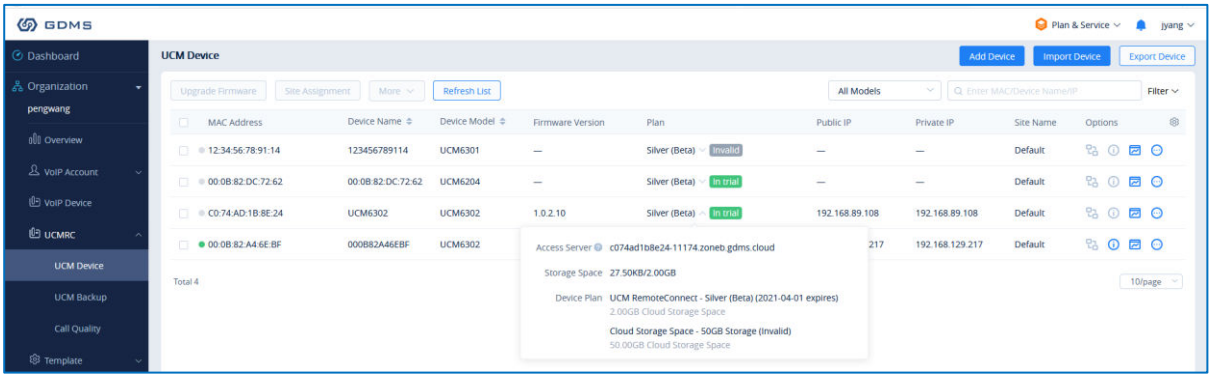


Figure 59: View UCM Device Plan

Access Server	This is used to configure on GS Wave phones so that GS Wave users can connect to the UCM server and make calls at anytime, anywhere on any network.

	If your current plan has the permission to customize the server address, you can click on the button on the right side of the device to access the Device Edit interface to implement this operation.
Storage Space	Refer to the current storage space used by UCM device, and the total storage space of the UCM device. If there is not enough space, the backup files cannot be stored.
Device Plan	Refer to the current plan and add-on plan of the device. If the plan has expired, the user can only use Basic plan as the current plan.

Notes:

- When the plan has expired, the user can only use 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.

Remote Access to UCM Web UI

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

Prerequisite: The UCM plan contains the permission of this function.

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

Figure 60: UCM List

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

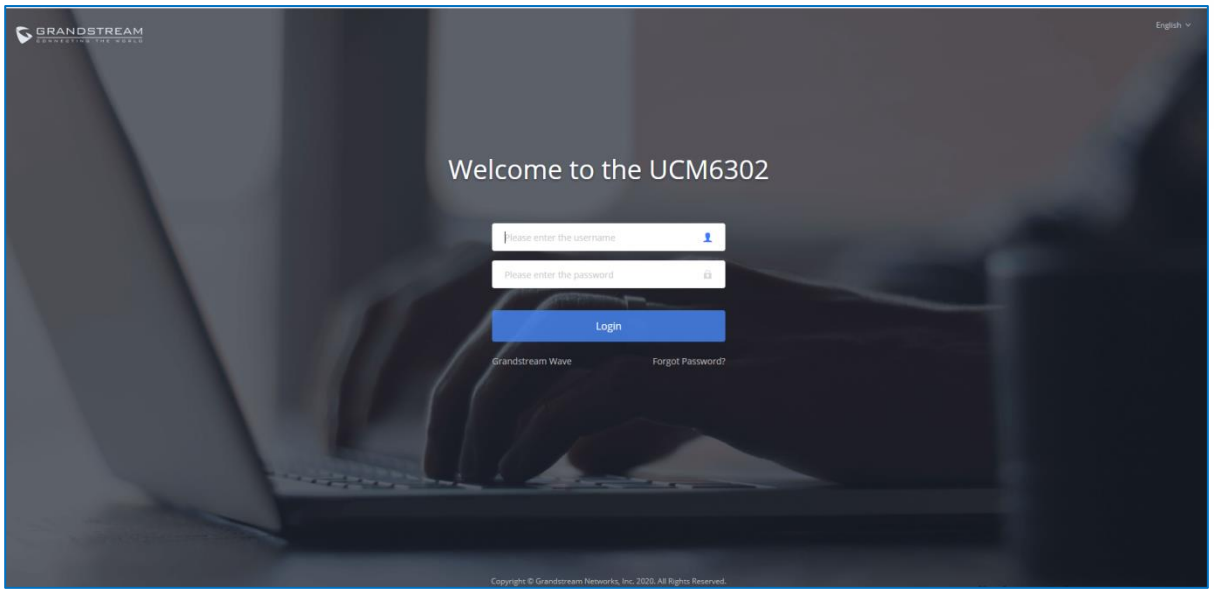


Figure 61: UCM Login Interface

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

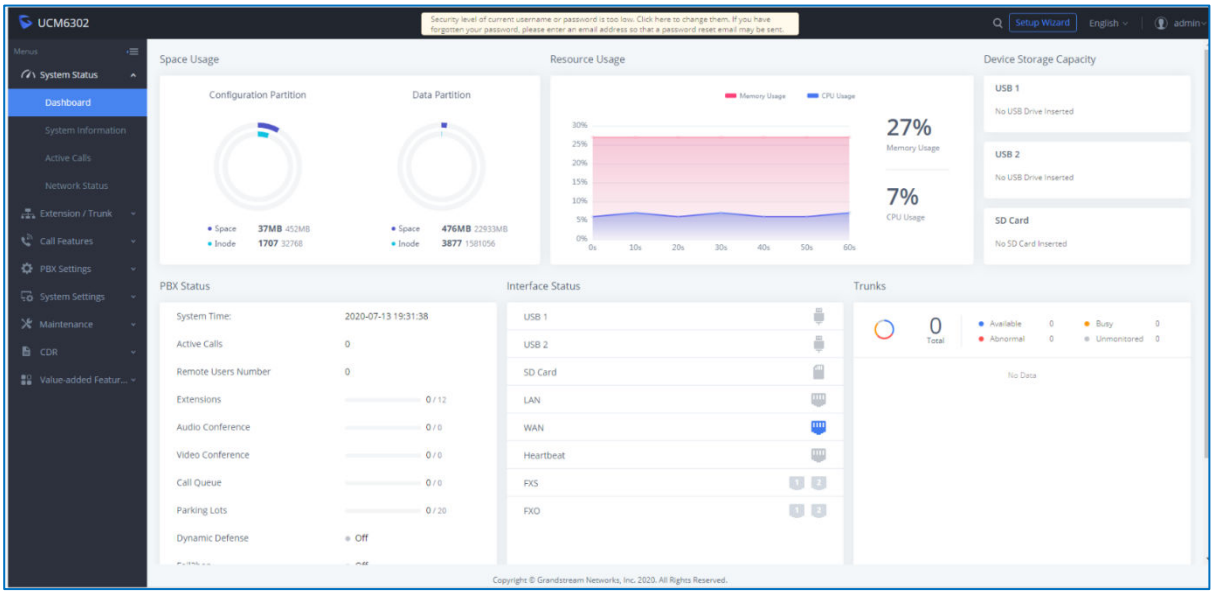


Figure 62: UCM Home Page

Note:

Users do not need to configure external network for UCM devices, and access to the UCM devices with encryption through GDMS platform. However, the network environment of the UCM devices is allowed accessing through external network.

UCM Device Diagnosis

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

Figure 63: UCM Device Diagnosis

View Statistics

Daily Report

Prerequisite: The UCM plan contains the permission of 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:

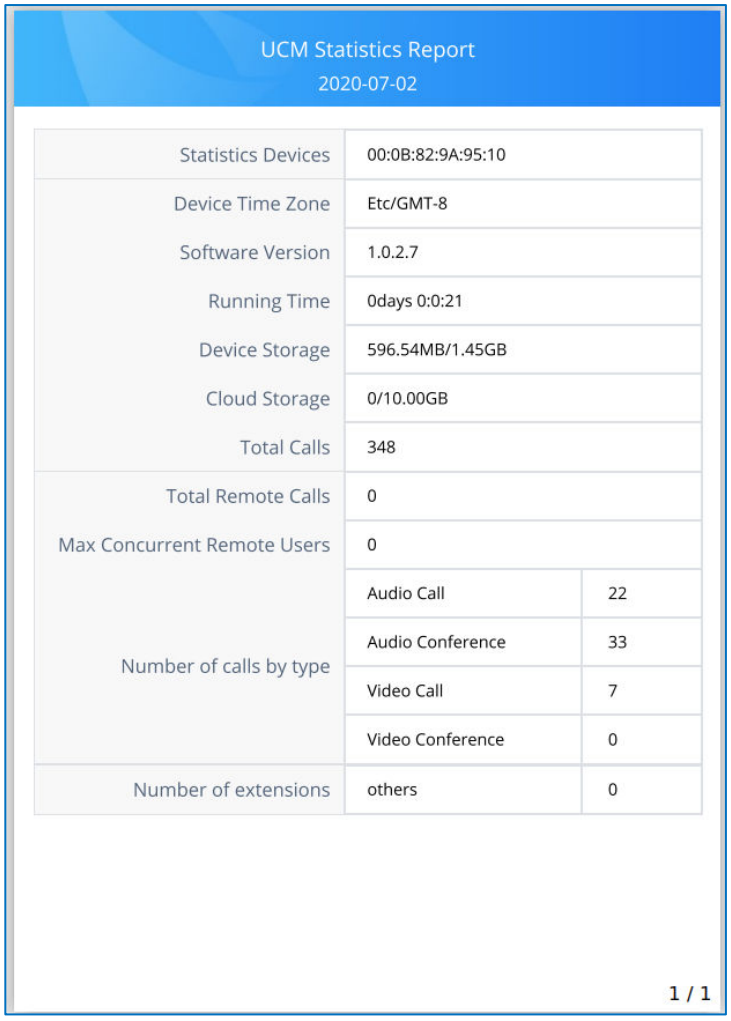


Figure 64: UCM Statistics Report

Table 20: UCM Statistics Report

Statistics Time	The time of sending the data, this is displaying according to the local time zone of the UCM device.
Device	The MAC address of the UCM device which 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 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.
Concurrent Remote Users (Max.)	The maximum number of concurrent remote users on the reported day. If the number exceeds the maximum number of concurrent remote users of the current plan, the indicator will be marked in red.
Extension Model	The model type and the number of devices connected to the UCM on the reported day.
Call Type Statistics	The distribution of all call types on the reported day.

Note:

1. Some data are only available for data statistics in premium plan.
2. 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 the permission of this function.

1. Go to **Device Management** → UCM **Device** interface, click on the button of the specific UCM device, and select "**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:

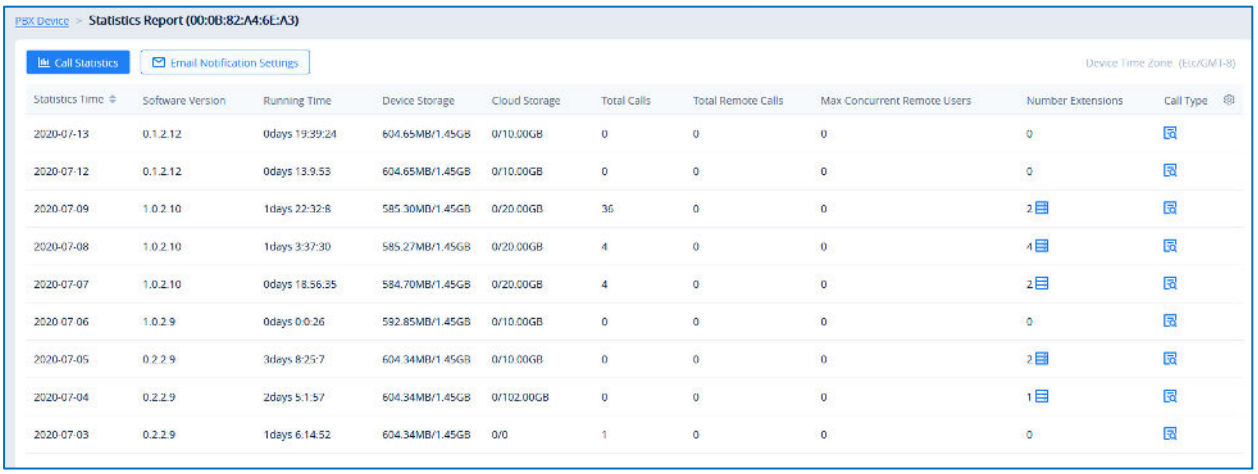


Figure 65: View UCM Device Statistics Report

3. Click on button 4 to view the connected devices type and amount on the current day to the UCM device:

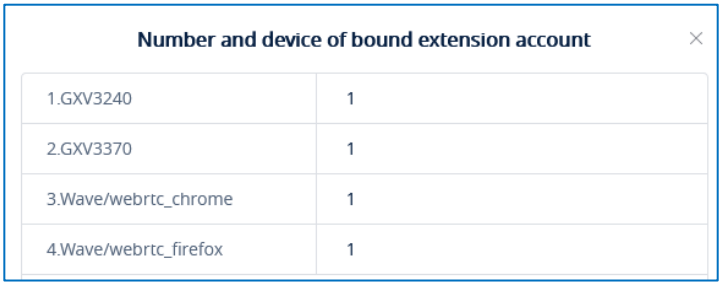


Figure 66: View Connected Devices Type/Amount

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

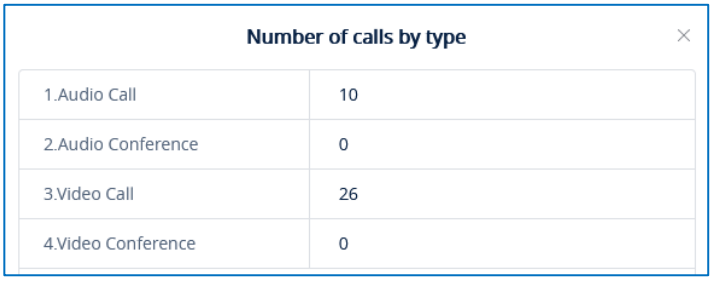


Figure 67: View Call Type Statistics

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

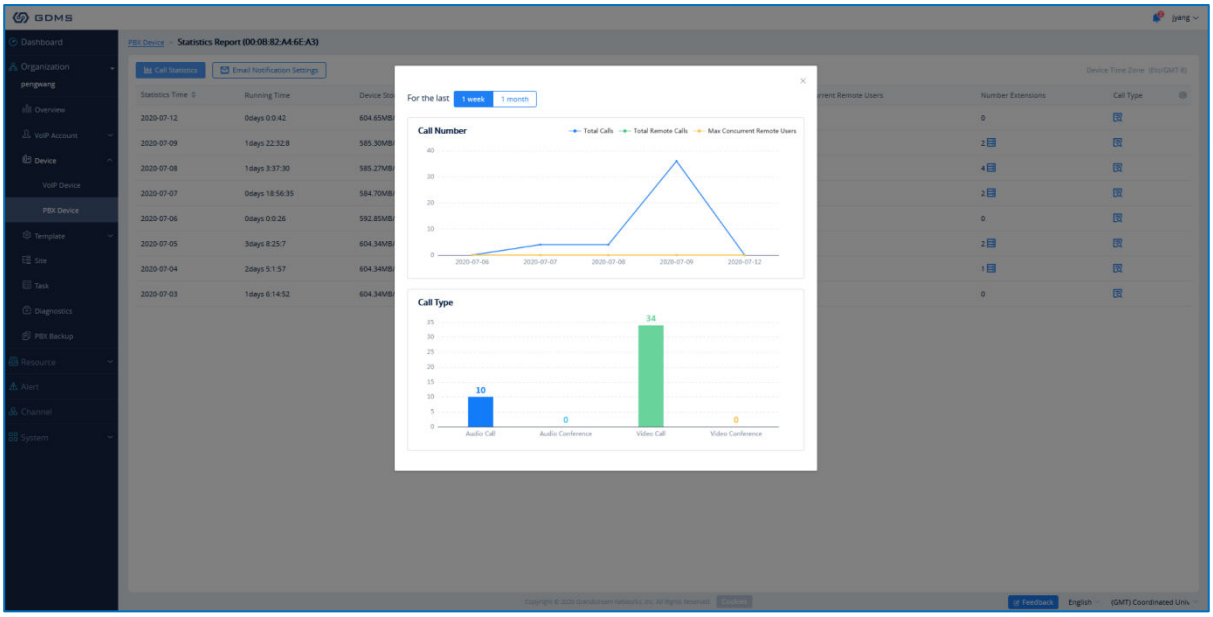


Figure 68: View Call Statistics Chart

Set Daily Report Receiving Mailbox

Prerequisite: The UCM plan contains the permission of this function.

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

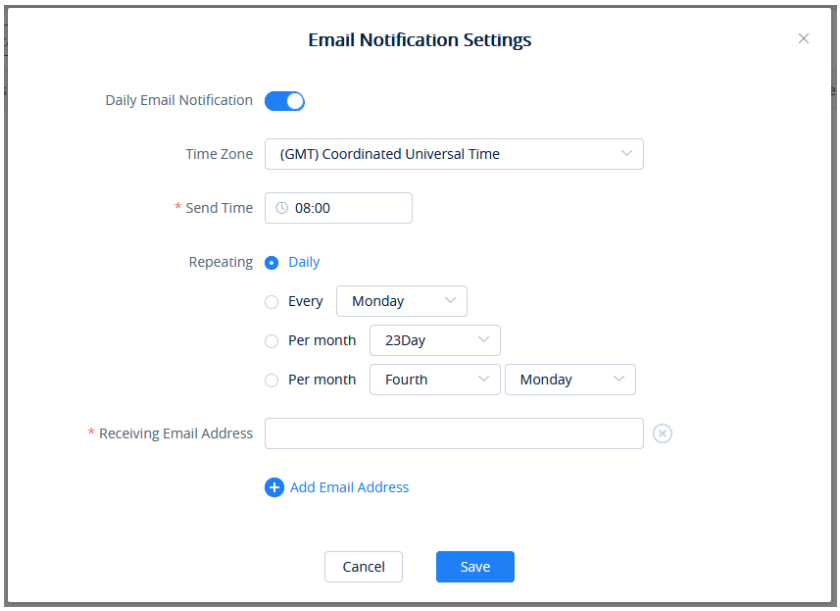


Figure 69: Set Daily Report Receiving Mailbox

Table 21: Set Daily Report Receiving Mailbox

Daily Email Notification	This is used to configure whether if 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 to enter any email address. Users can click "**Add Email Address**" to add multiple email addresses to receive the daily report.

View Operation Logs

Prerequisite: The UCM plan contains the permission of 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 "**Operation Log**" button.

2. Operation logs include: Remote accessing UCM Web UI logs, restarting logs, and firmware upgrading logs.

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

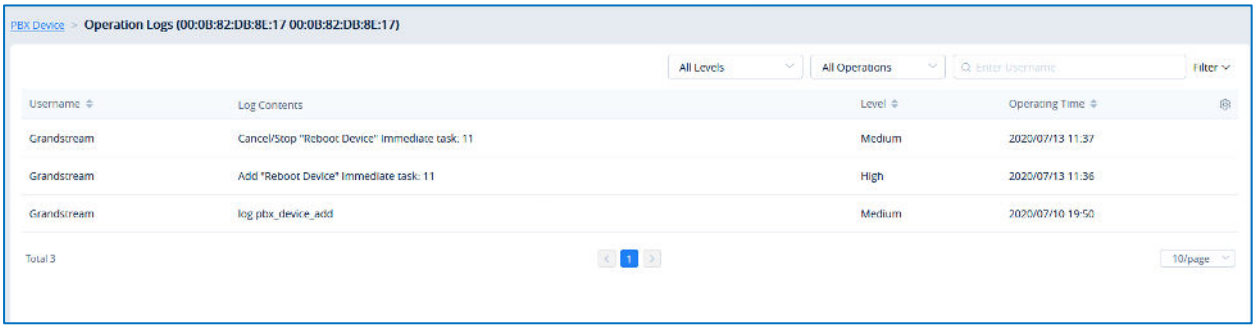


Figure 70: View UCM Device Operation Logs

Custom Remote Access Domain Name

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

Prerequisite: The UCM plan contains the permission of this function.

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

1. Go to **Device Management** → UCM **Device** interface, click **Edit Device** option for the specific UCM device, and access to "**Device Edit**" menu.

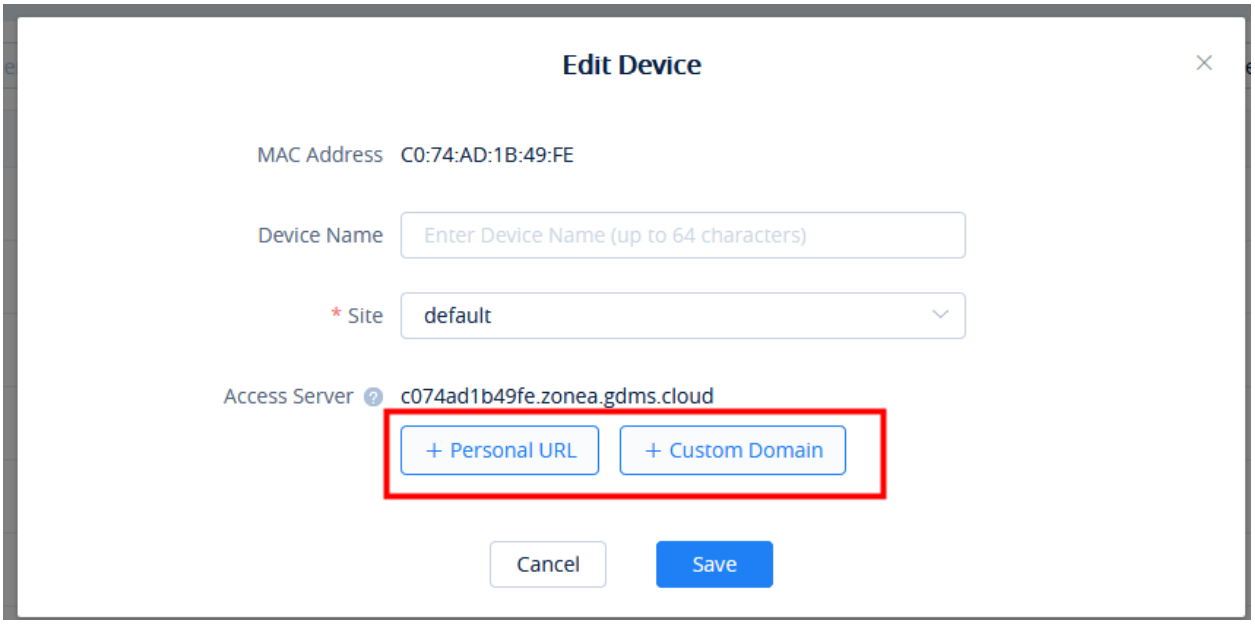


Figure 71: Device Edit Menu

2. Click on "**Personal URL**" field, and enter the preferred URL, such as: {yourdomain}.zoneb.gdms.cloud

Figure 72: Custom UCM Remote Access Domain Name

3. If the plan has custom domain name function, the user can click on "**Custom Domain**" option and enter the server address with 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 GS Wave users cannot connect to UCM device through the custom address.

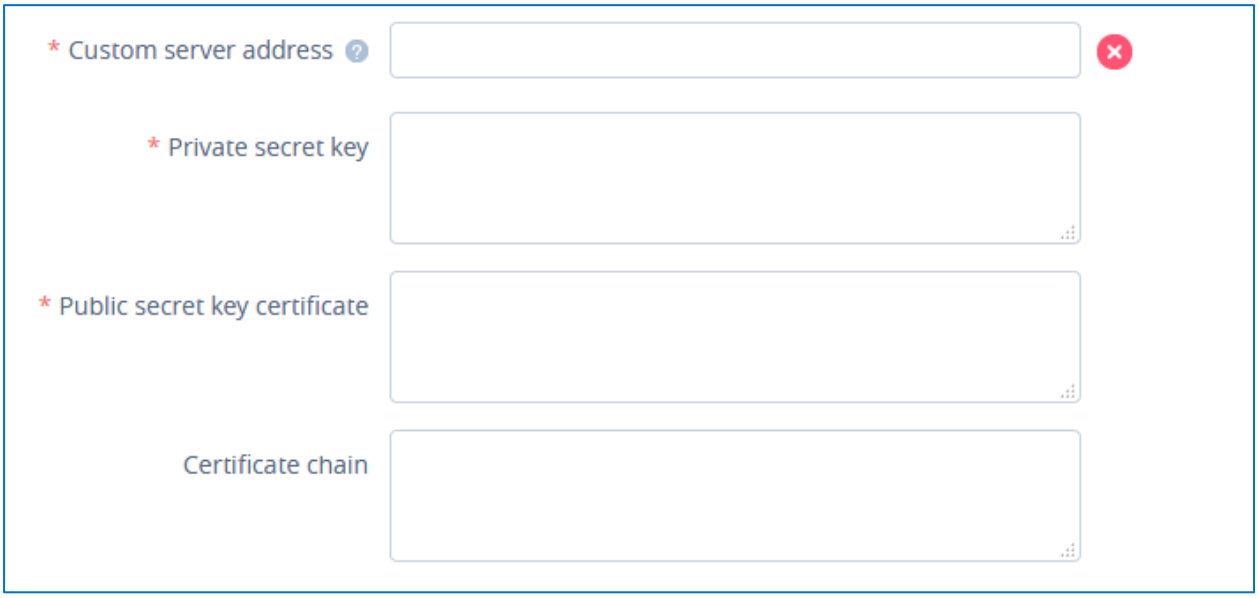


Figure 73: Enter Private Domain Name and Certificate

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

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

Note:

If the user modifies the custom server address, the phones or GS Wave applications which use previous custom server address need to re-configure 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 to synchronize UCM device alert to the GDMS platform. For UCM Remote Control plans details, please refer to our official website.

1. Users need to enable UCM alert notification on the management platform of UCM device. For details, please refer to the UCM User Guide in 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 schedule to reboot the UCM devices.

1. Select a UCM device from **GDMS → Device → UCM Device** page, 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 scheduled reboot, please select the start and end time of the task. Reboot will be performed during this period.

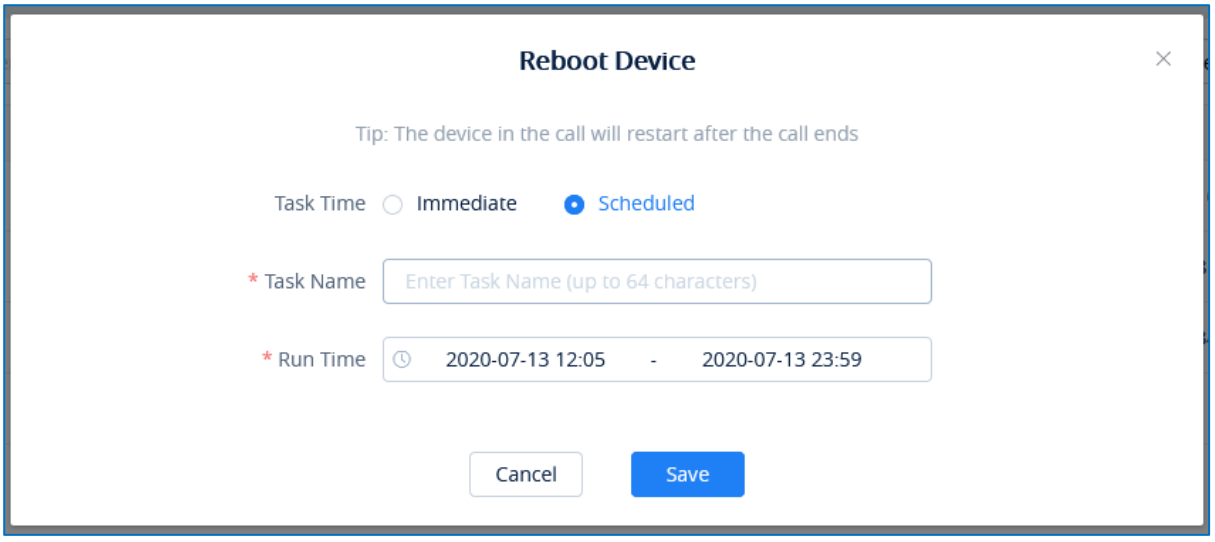


Figure 74: Reboot UCM on GDMS

3. After saving the reboot configuration, users can view the status of this task from **GDMS → Task** page.

Note:

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

Upgrade Firmware

Prerequisite: The UCM plan contains the permission of this function.

Upgrading UCM firmware via GDMS is supported. Please note there must have UCM official firmware or customized firmware available on GDMS platform first.

1. Select a UCM device from **GDMS** → **Device** → UCM **Device** and click on "**Upgrade Firmware**" as shown in below picture. Users can also select multiple UCM devices and then click on "**Upgrade Firmware**" to perform batch upgrade for all selected UCMs.

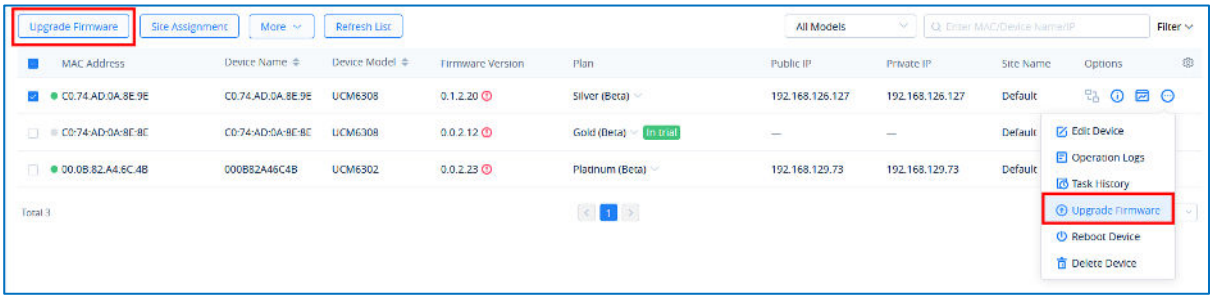


Figure 75: UCM Devices Listed in GDMS

2. Select upgrade immediately or set up schedule to perform the upgrade. For scheduled upgrade, please select the start and end time of the task. Upgrade will be performed during this period.

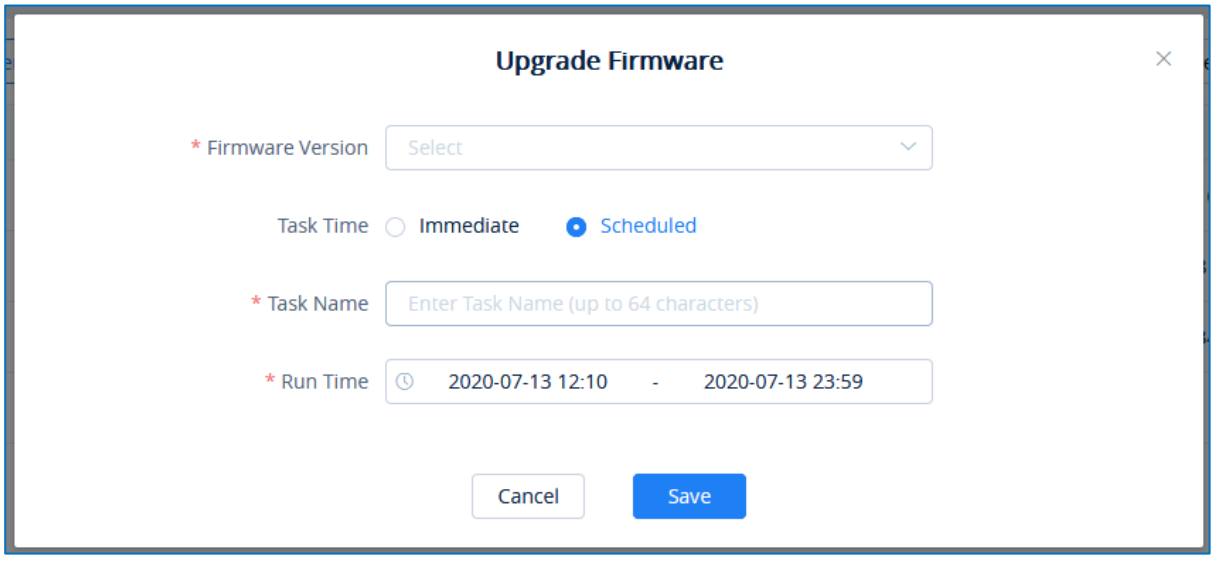


Figure 76: Upgrade Firmware Configuration on GDMS

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

Note:

If the task is failed, 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 to the device editing page.

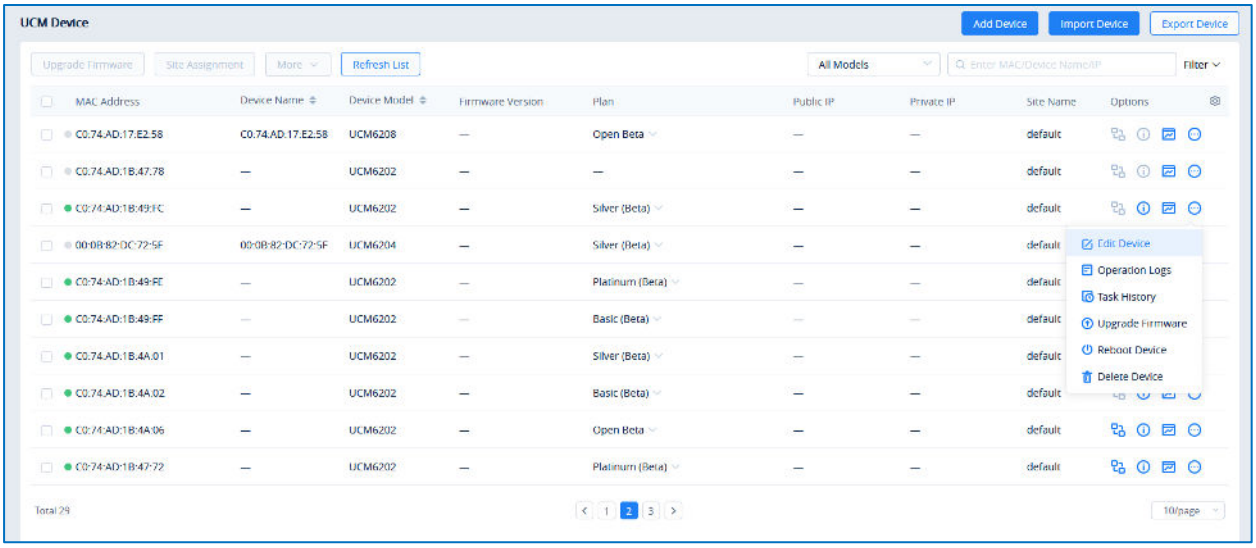


Figure 77: Edit UCM Device Option

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

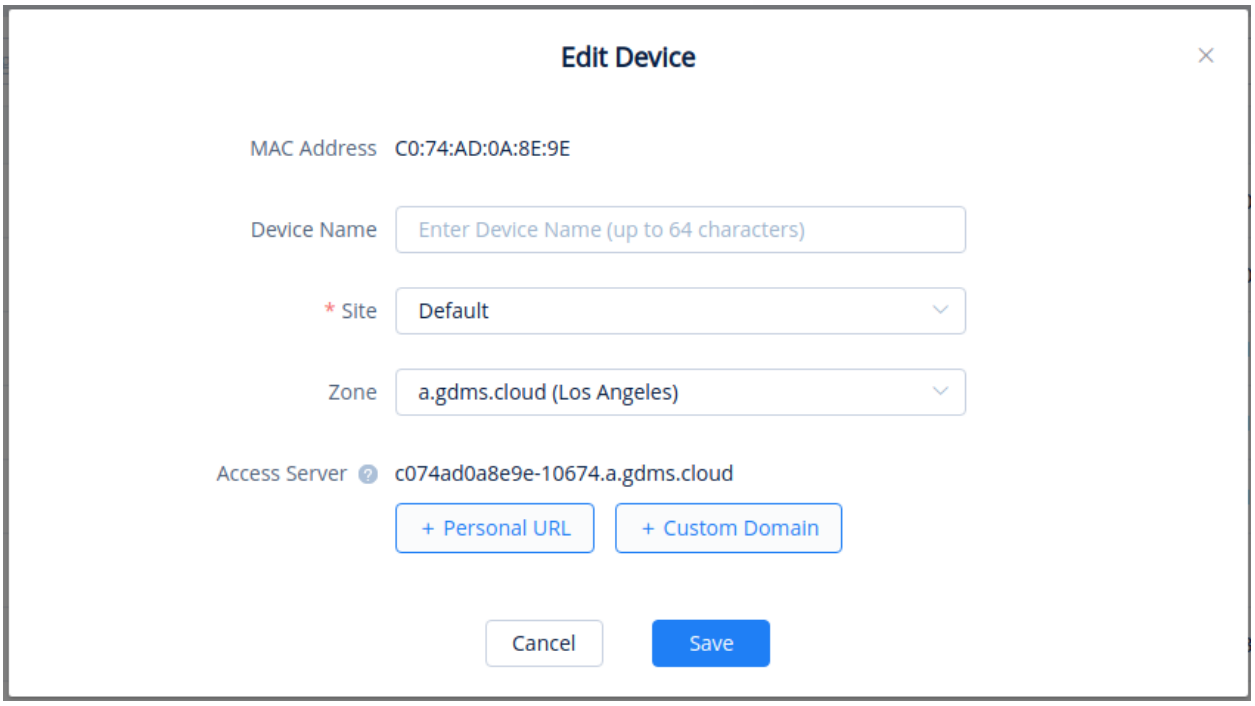


Figure 78: Edit Device

3. Users can modify the GDMS server region by clicking on the drop-down menu of "**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 the permission to custom private domain name function, the user can click on "**Custom Domain**" option to configure it.

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

Note:

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.

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.

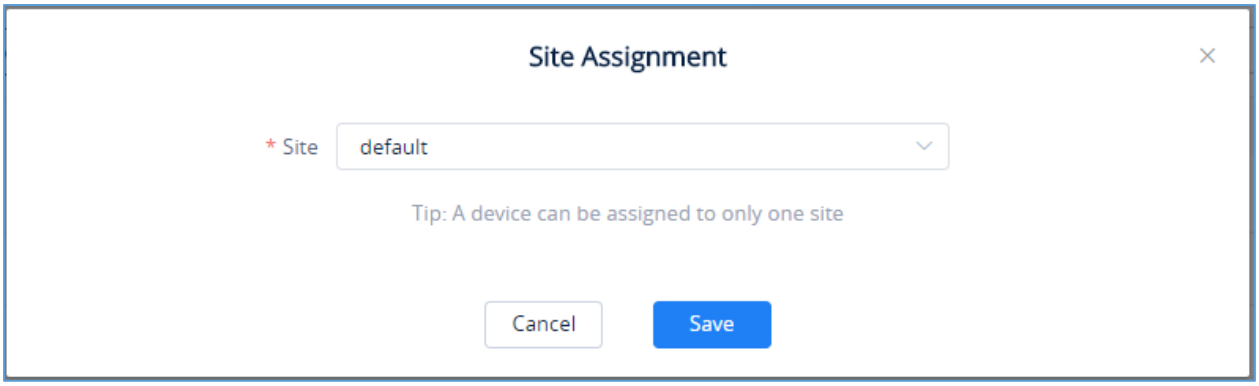


Figure 79: Site Assignment

2. Select the site to assign the selected devices to.

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

Note:

Each device can only be allocated to one single site.

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 batch upgrade for all selected UCMs.

3. Click on "**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 involve the deleted devices will be canceled either.

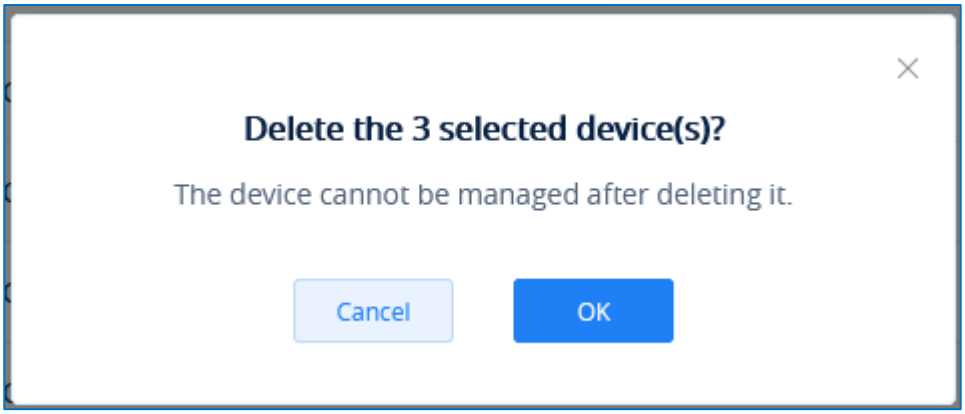
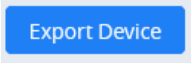


Figure 80: Delete Device Prompt

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.

UCM REMOTE CONNECT – CONFIGURE PARAMETER FOR DEVICE

GDMS platform administrator can configure the parameters of UCM Remote Connect for the device remotely. Once the device has been configured following the methods below, the device can use the UCM Remote Connect 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, click on edit button to access to the account editing interface:

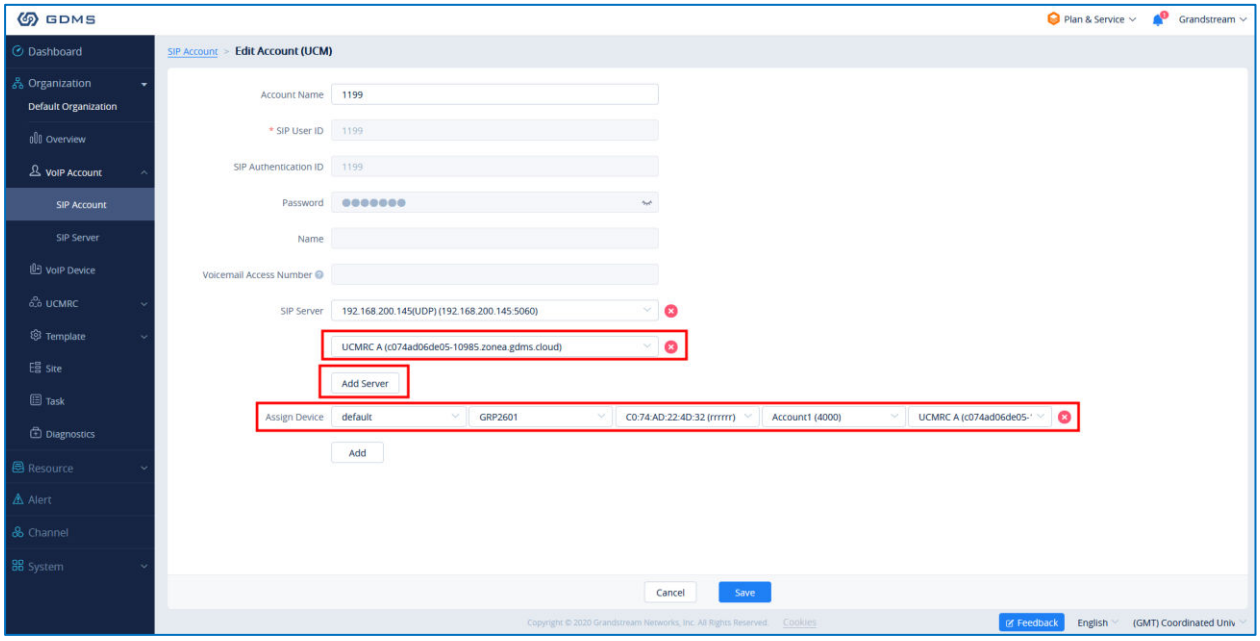


Figure 81: Edit Account

2. Click **Add Server** option and select the external network server address reported by the UCM Remote Connect.

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 Remote Connect.

4. Click to save and apply the changes for UCM Remote Connect for the device.

Method 2:

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

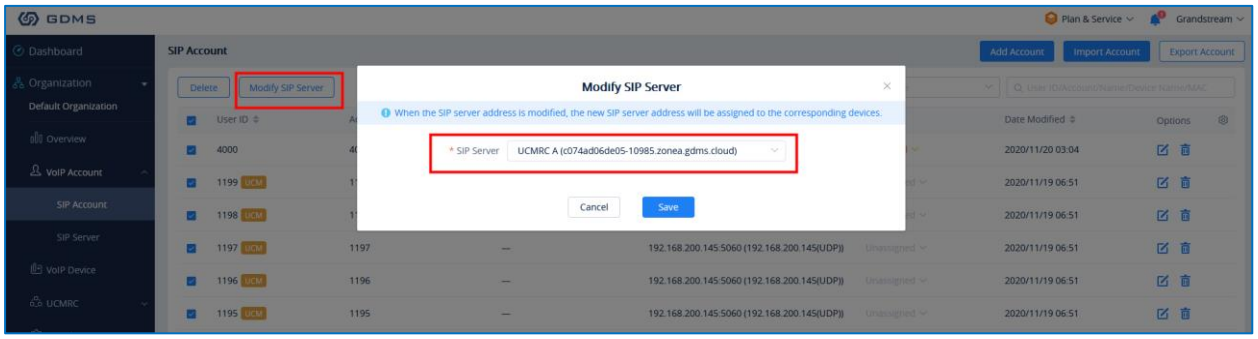


Figure 82: Modify SIP Server Address

Note:

1. When the user configures the server address of UCM Remote Connect for the device, the following settings will be assigned to the device automatically to ensure the UCM Remote Connect service can be used successfully:
   - SIP Protocol - TLS
   - STUN server setting will be changed to the TURN server address of UCM Remote Connect.
2. When the UCM Remote Connect account is deleted from the device, the STUN server setting will be removed automatically from the device.

UCM REMOTE CONNECT - UCM BACKUP

View Backup File

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

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

Note:

It only displays all the backup files of the UCM devices under 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.

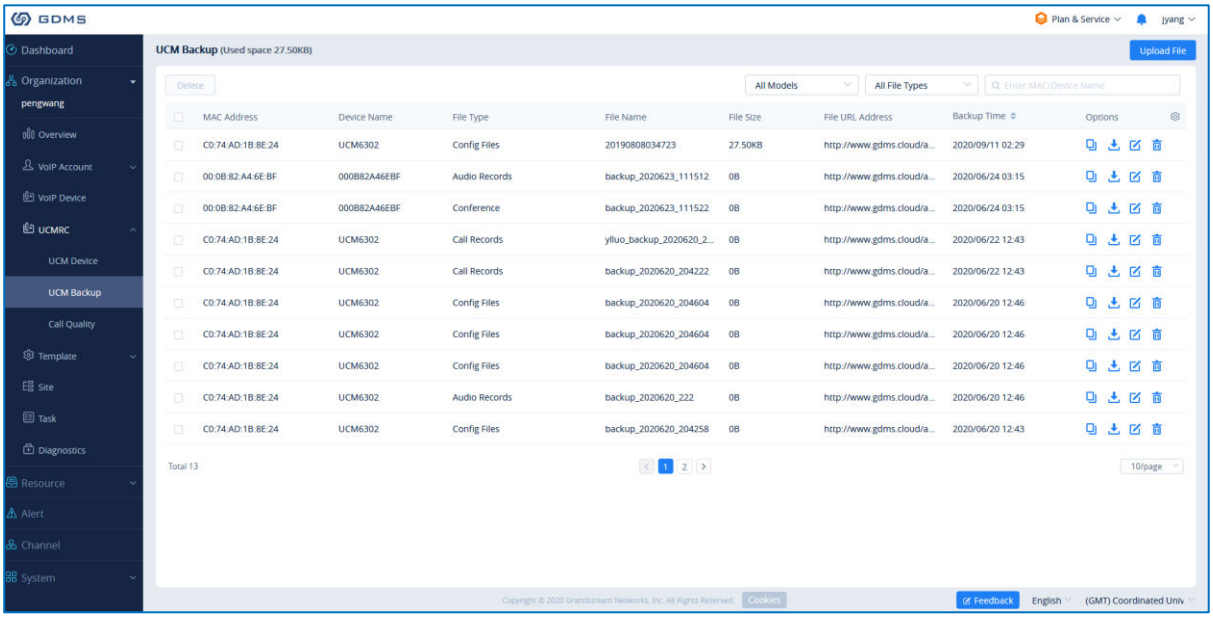


Figure 83: View Backup File

Note:

- 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 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 UCM Backup page, click on the "**Upload File**" button on the right upper corner to access to the interface:

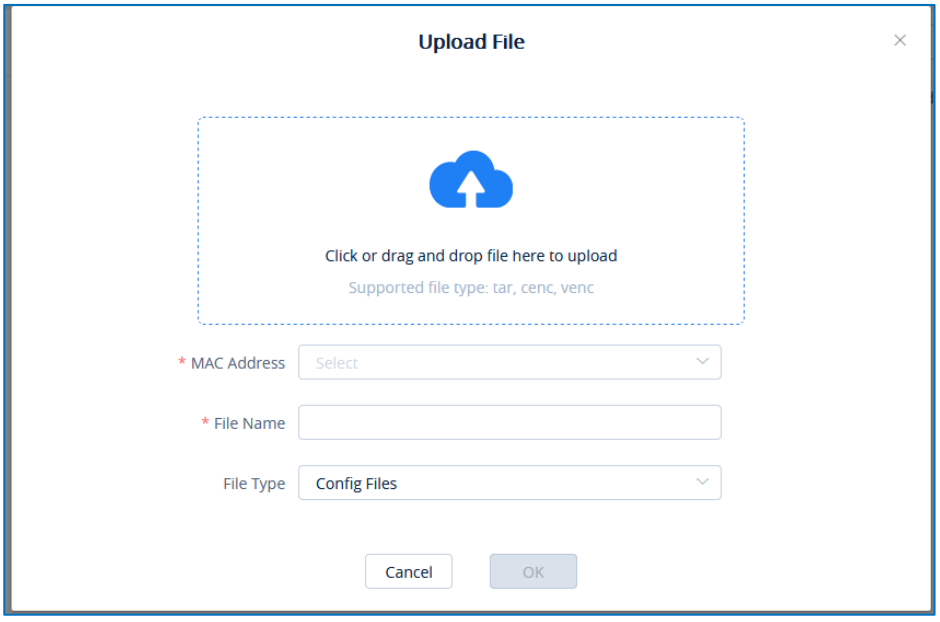


Figure 84: Upload File

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

Note:

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.

Note:

- 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.

Restore UCM Backup File Remotely

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

1. On "UCM Backup" interface, select an UCM backup file and click "Restore" button to restore the UCM device.

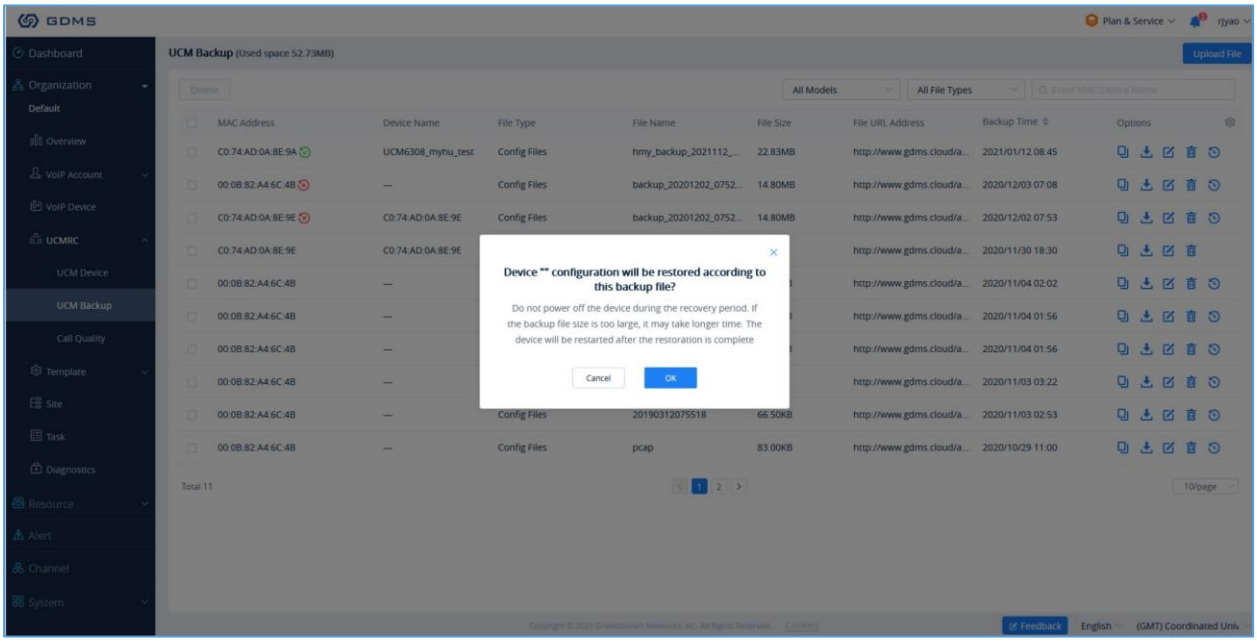


Figure 85: Restore Backup File Remotely

2. Once the user clicks "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.

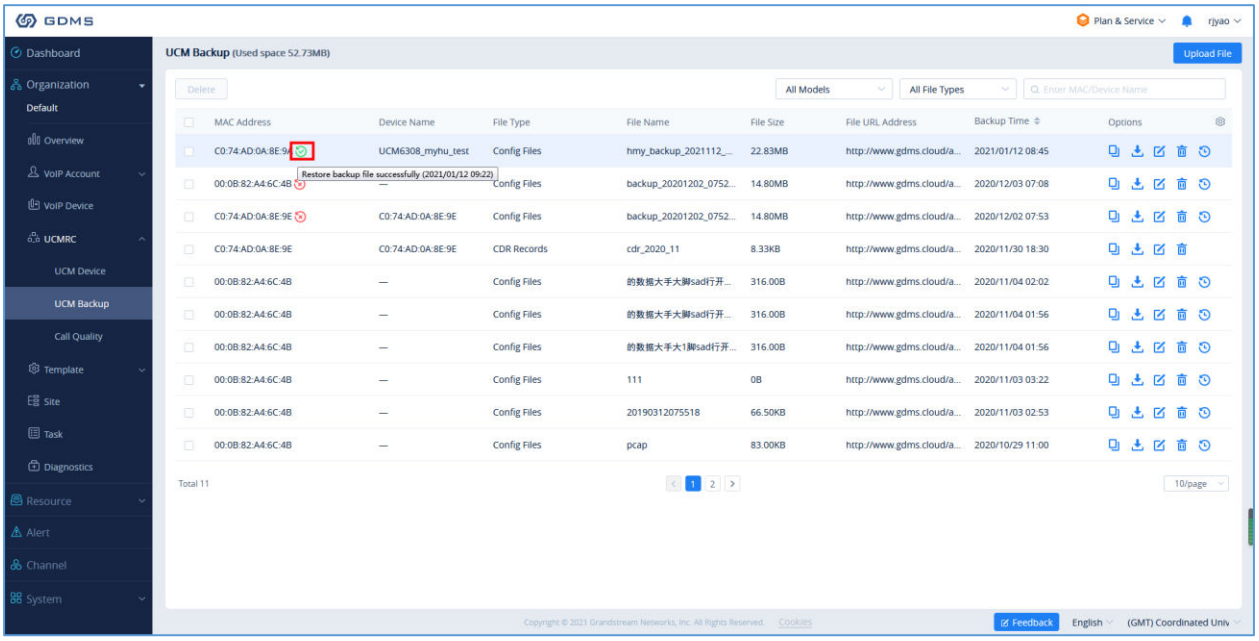


Figure 86: View Results

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 "**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 GDMS platform.

Note:

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

UCM REMOTE CONNECT - CALL QUALITY

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 Remote Connect service so that the device can report the call quality to the GDMS platform. This function is supported in some of the UCM Remote Connect plans, not all plans. Please refer to the official website for plans descriptions.

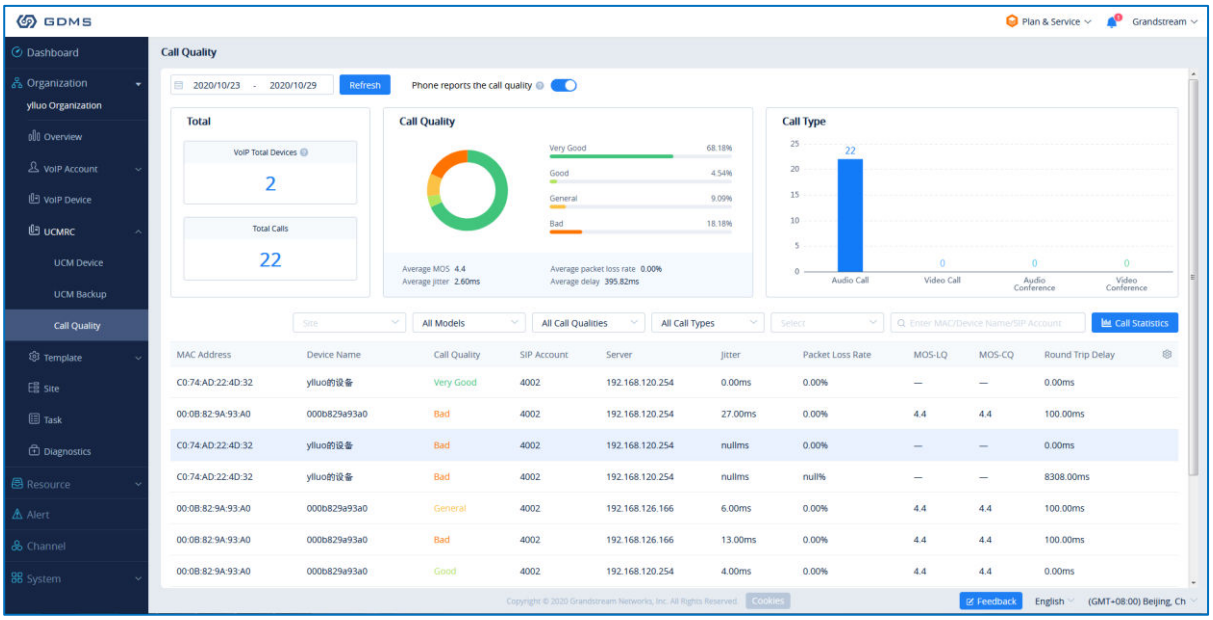


Figure 87: Statistics Overview

Table 22: Statistics Overview

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

Call Quality Record

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

Please see the screenshot below:

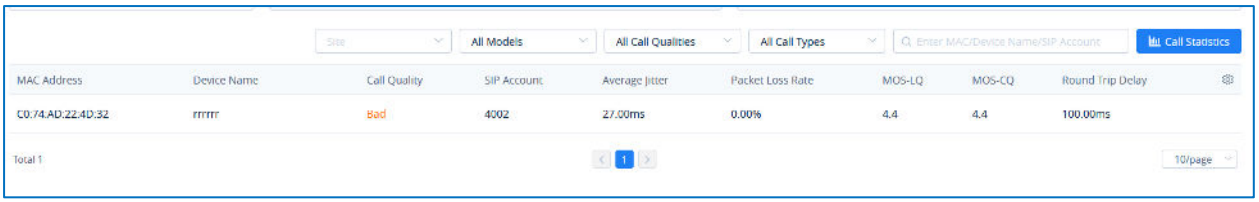


Figure 88: Call Quality Record

1. GDMS platform supports to filter call quality records by date.

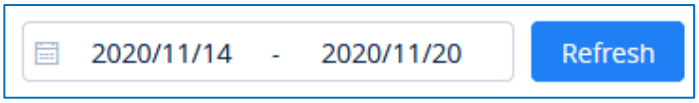
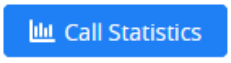


Figure 89: Filter by Date

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

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

4. Click **Call Statistics** button 

to view the statistical report of the filtered call quality records.

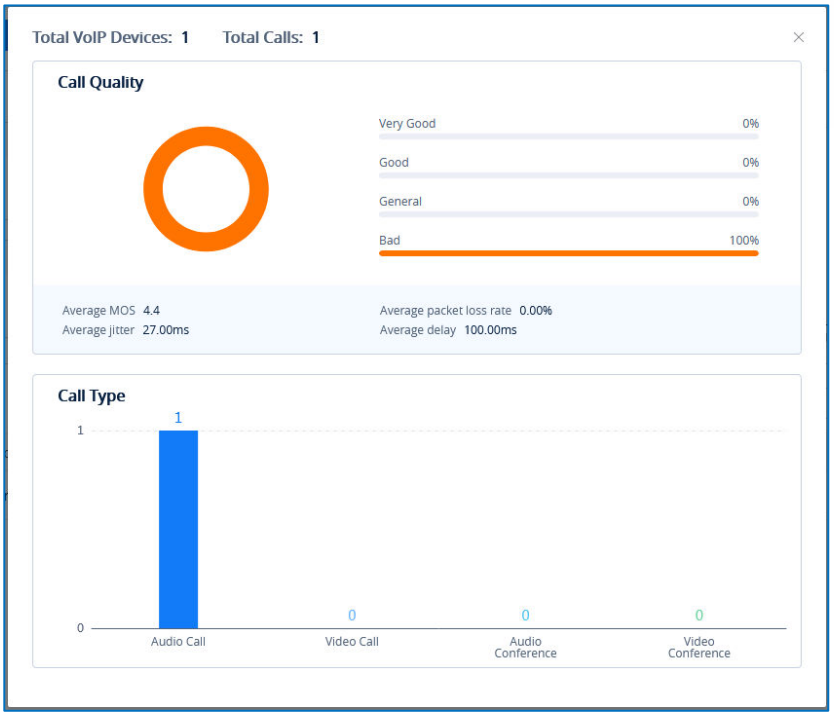
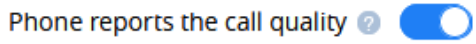


Figure 90: Call Quality Record Report

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 

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.

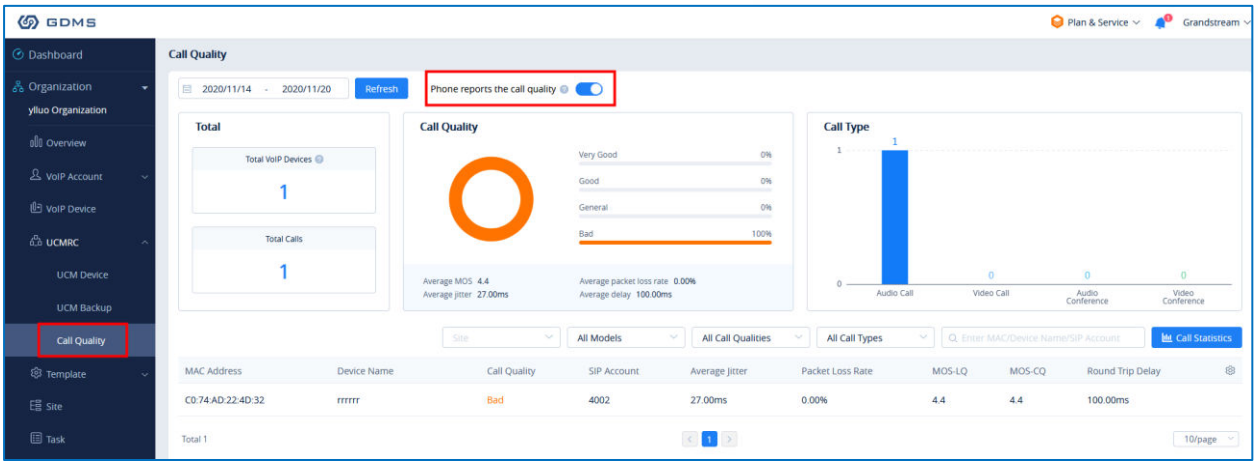


Figure 91: Enable/Disable Call Quality Reporting

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.

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 model 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.

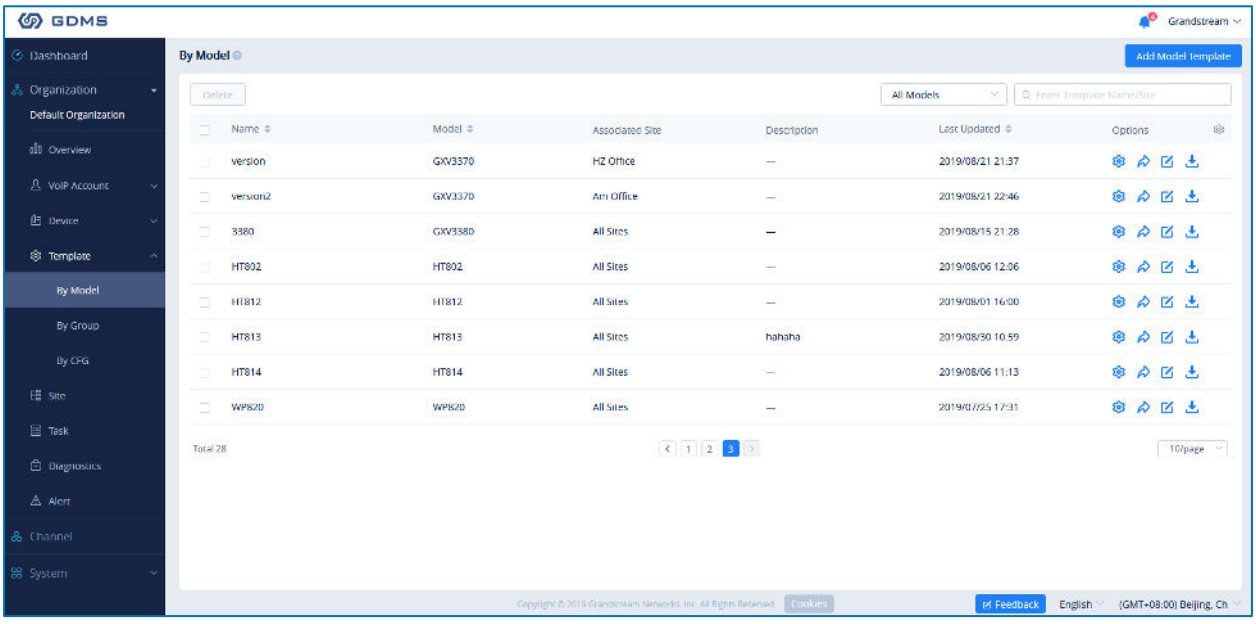


Figure 92: Manual Configuration Push

Note:

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 the site A – D will acquire the same configuration template – GXV3370 Config Template.xml.

For DP720 devices, different sites have different configuration template. 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.

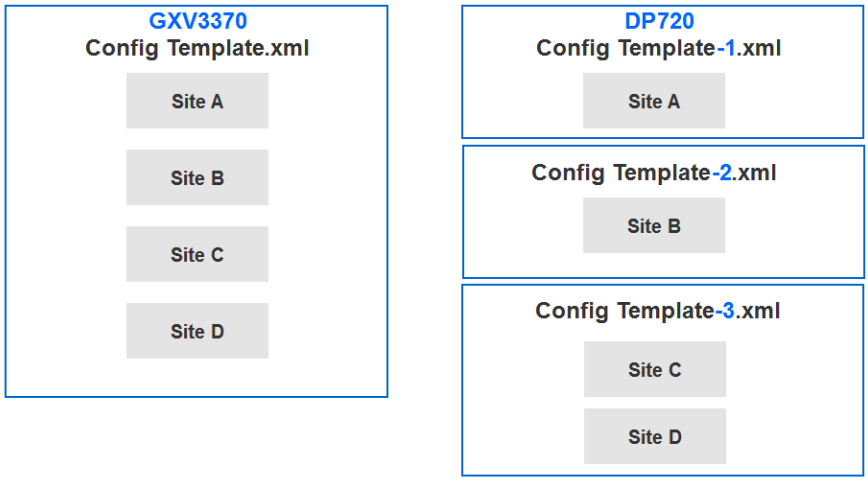


Figure 93: Example – GXV3370

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:

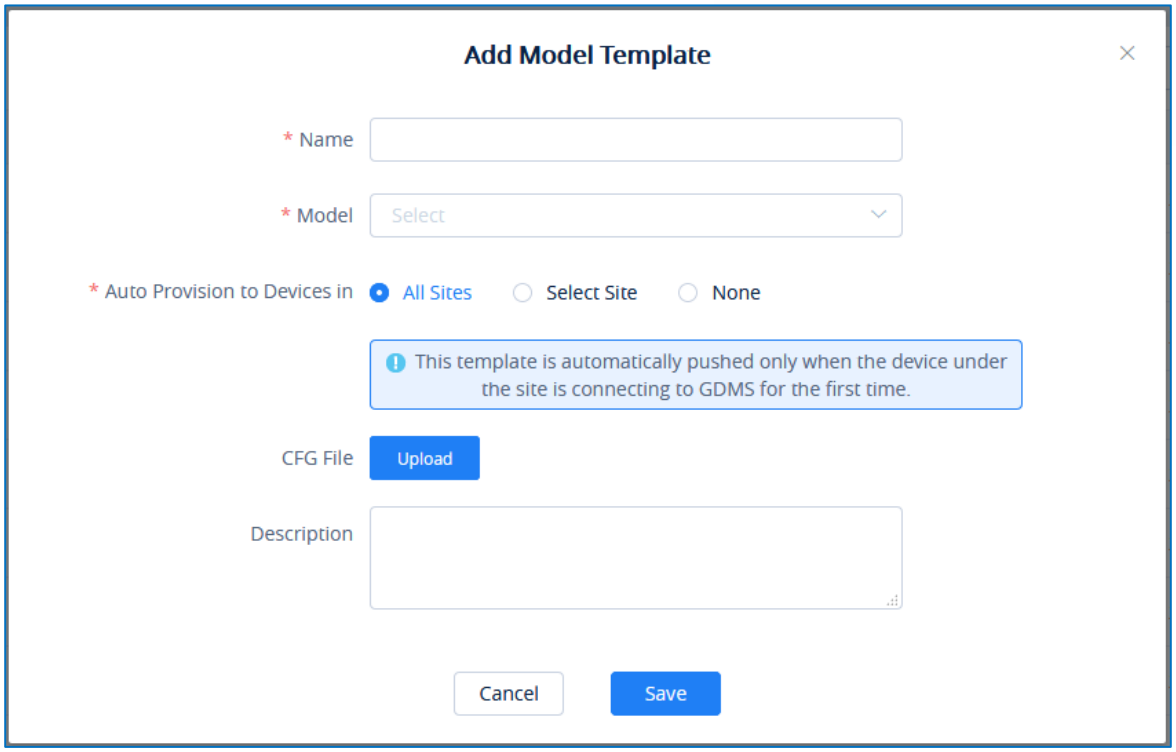


Figure 94: Add Template

Table 23: 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 which the template will be used for. **All Sites:** All devices in all sites will use this template. **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.

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

Notes:

- 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.

Important Note:

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 "Set Parameters" menu on the GDMS platform and push 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.

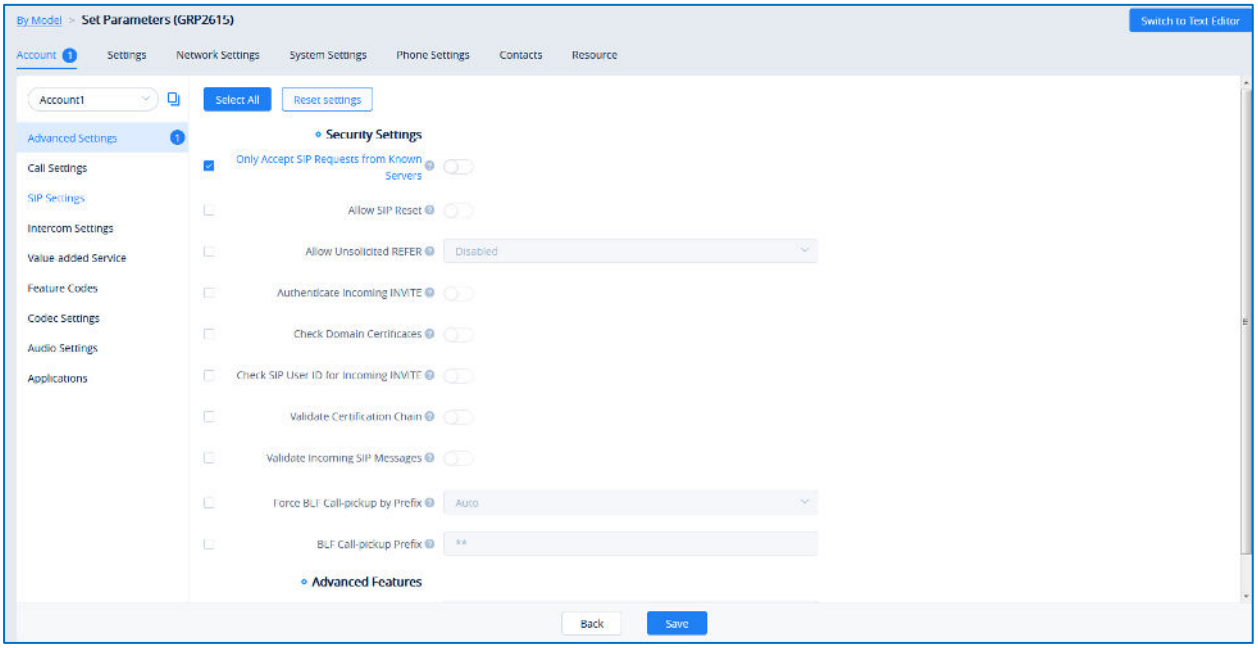


Figure 95: Set Parameters

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.

4. Clicking on the button following the account, users can copy and paste the current account configuration to other accounts.

5. When users try to configure 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.

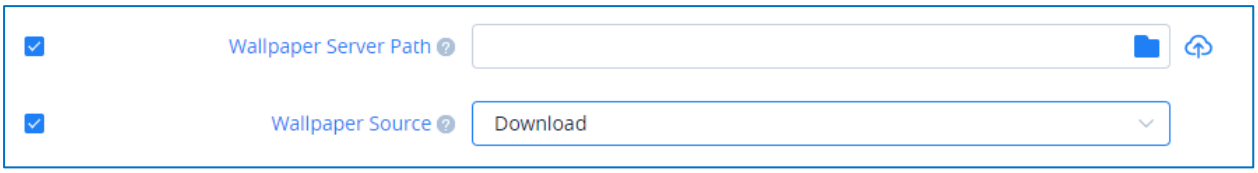


Figure 96: Ringtone Configuration

6. 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). Key can be either a P-value or an alias.

Notes:

- 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 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 new 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 new 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 ringtone and language for devices (Supported models: GXP/DP series).

1. 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:

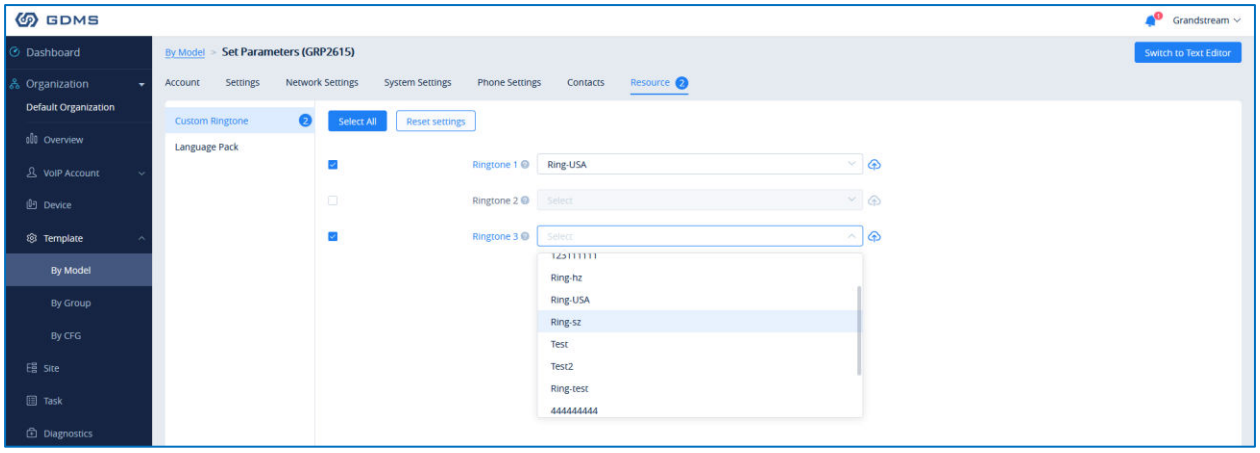


Figure 97: Resource Configuration

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 “Save” button, the device of this model will download the resource file from the firmware path once the device is connected to GDMS platform for the first time.

5. Or, users can click “Push” button to push the template of the model to the device. Then, the device will download the resource file from the firmware path.

Note:

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, click on the button following the template.

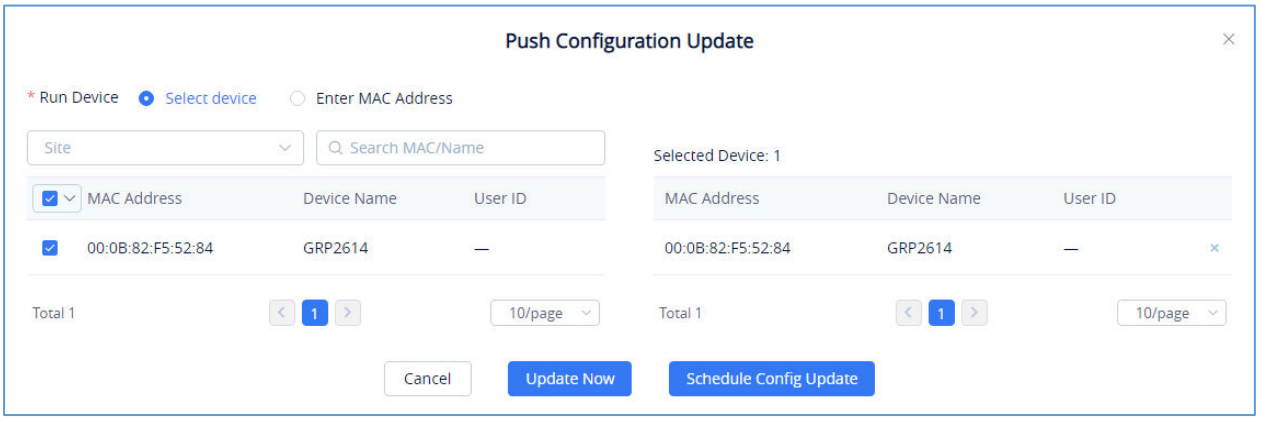


Figure 98: Push Configuration File

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.

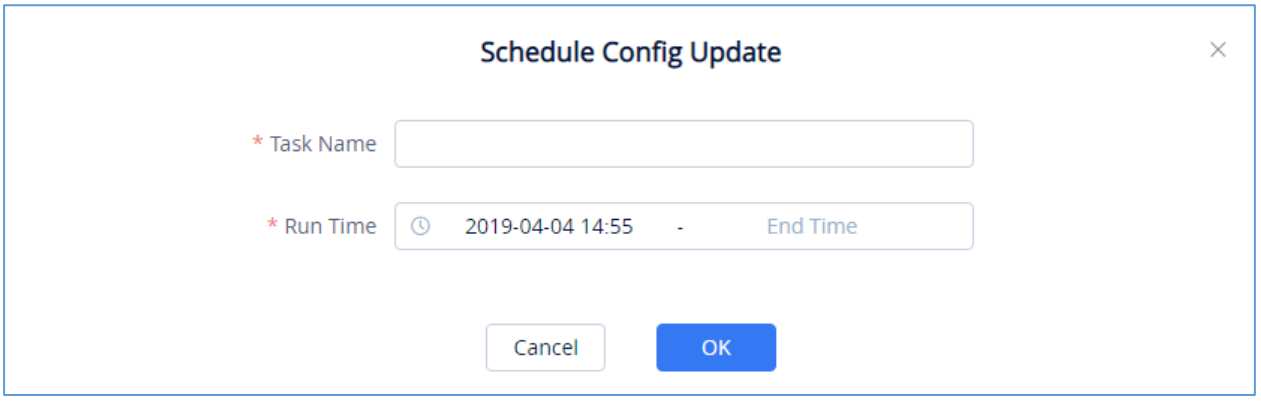


Figure 99: Schedule Config Update

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

Edit Template

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

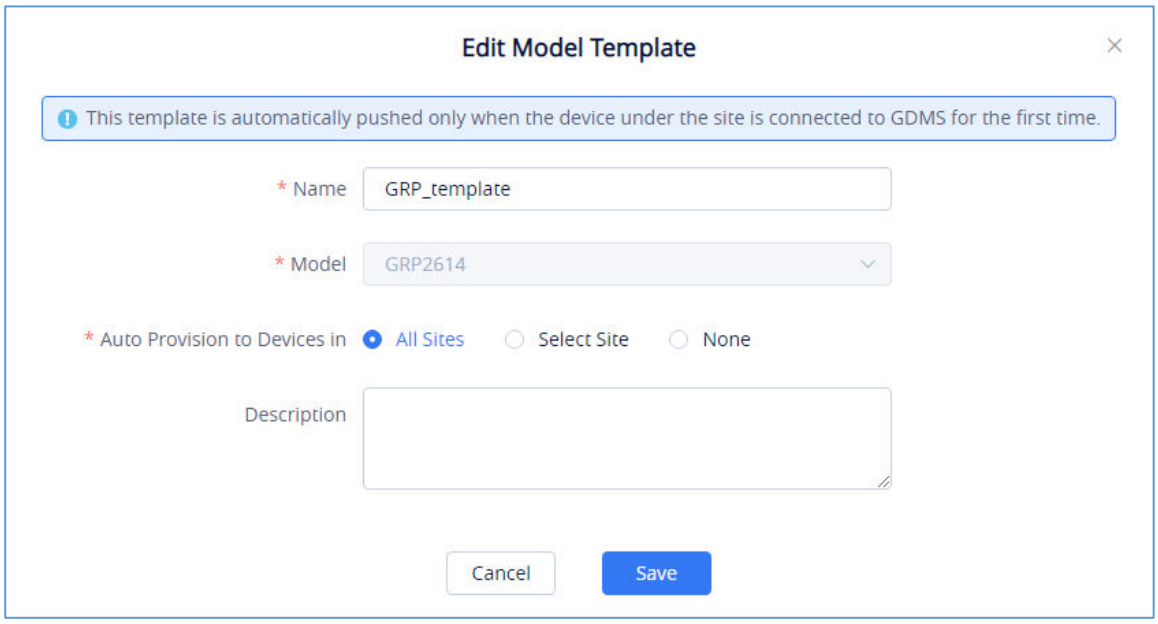


Figure 100: Edit Model Template

Download Configuration Template

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

Figure 101: Download Configuration Template

Delete 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.

Note:

If a scheduled task involves a deleted template, the task will still use a temporary copy of the template saved at the time of scheduling. A scheduled task will not fail due to deleted templates.

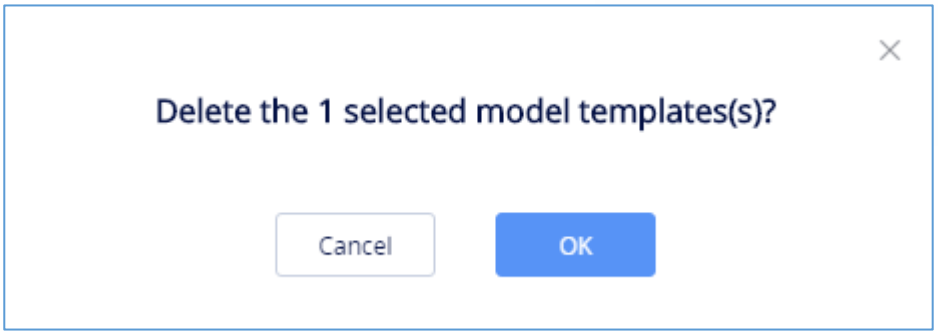


Figure 102: Delete Template

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 to 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.

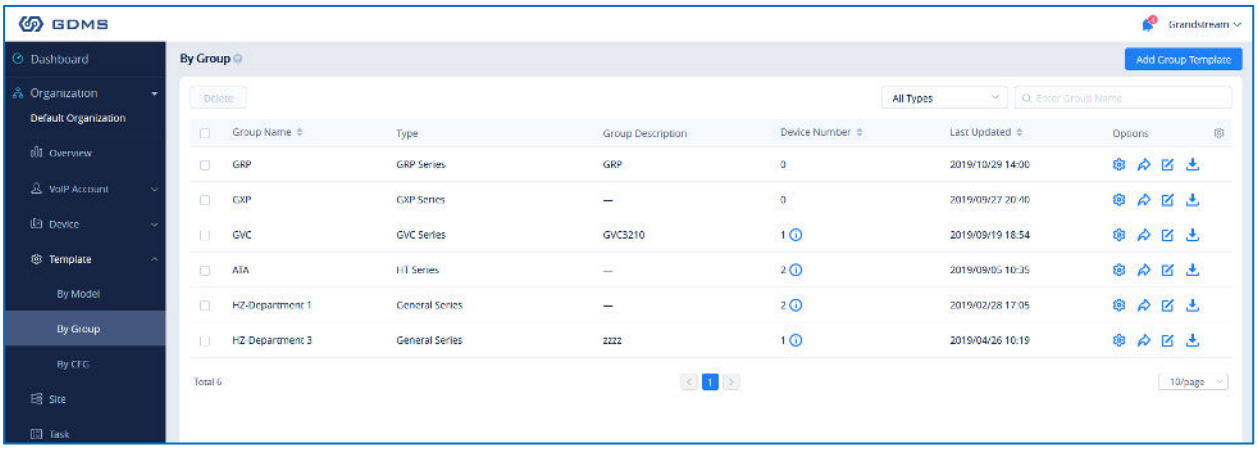


Figure 103: By Group

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.

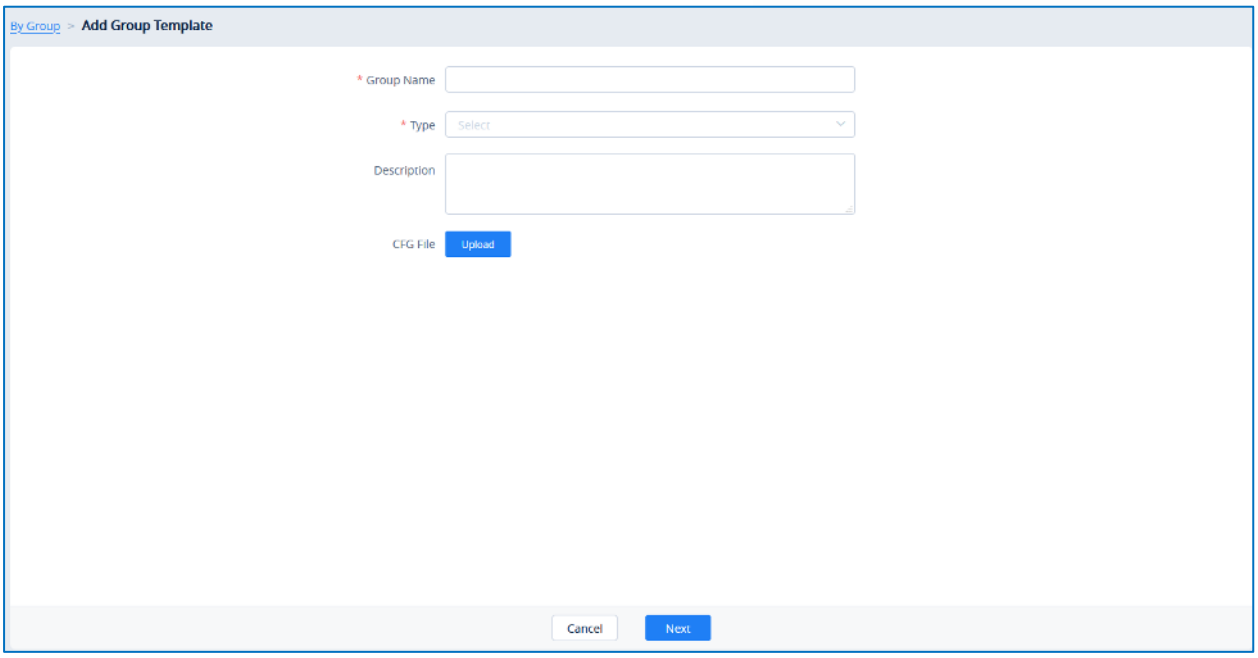


Figure 104: Add Group

Table 24: 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	Users need select the type: • Audio phone series: This is used to configure the common configuration parameters of GXP and GRP series. • DP series: Use the configuration template for DP7xx series. • HT series: Use the configuration template for HT8xx series. • GRP series: Use the configuration template for GRP series. • GXP series: Use the configuration template for GXP21xx series. • GXV series: Use the configuration template for GXV33xx series. • GVC series: Use the configuration template for GVC3210.
Description	Enter the detailed description and purpose of the configuration template.

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.

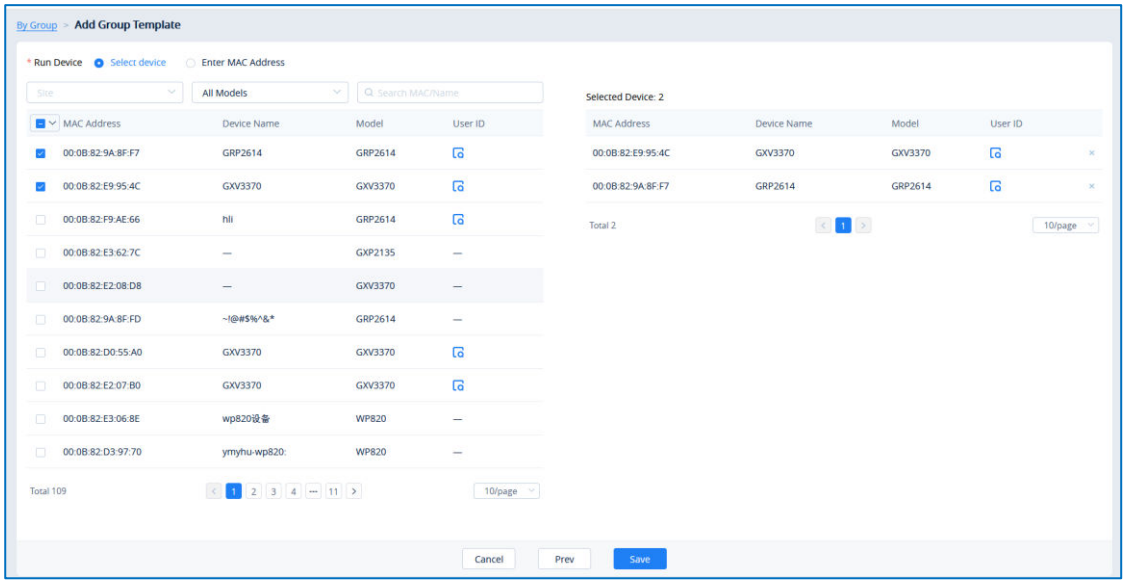


Figure 105: Finish Adding Group

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

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

Note:

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 in order to push the unique parameters to the devices in the group.

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

    a. Clicking on the **Select All** button will select every option on the current page. Clicking on it again will deselect all the options.

b. Clicking on the **Reset Settings** button will restore all settings on the current page to default values.

c. Clicking on the button following the account, users can copy and paste the current account configuration to other accounts.

d. When users try to configure 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.

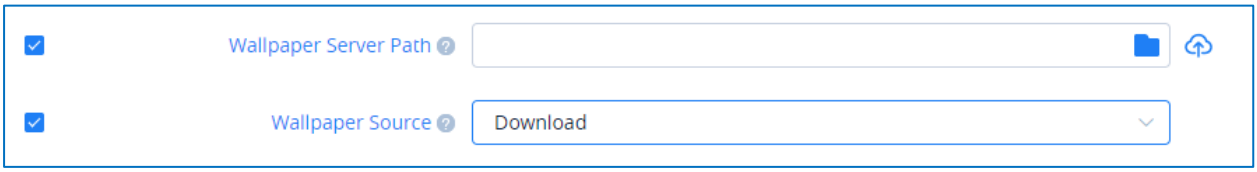


Figure 106: Ringtone Configuration

2. 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). Key can be either a P-value or an alias.

Notes:

- 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 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 new 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 new 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 ringtone and language for devices (Supported models: GXP/DP series).

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

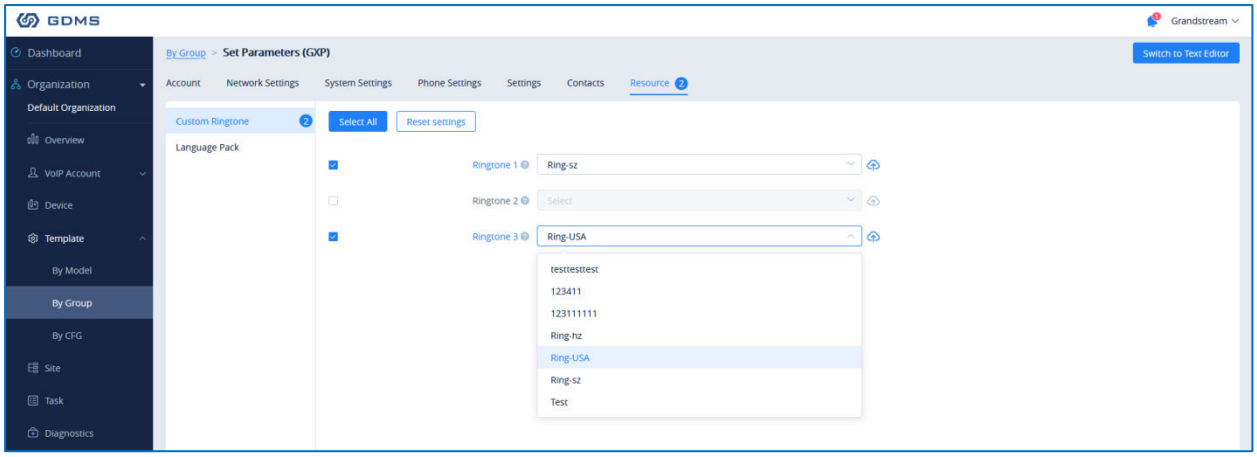


Figure 107: Resource Configuration

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 “Save” button, the configured parameters and resources will be saved in the system. When the user clicks “Push” button to push the template to the device, the device will download the resource file from the firmware path.

Note:

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.

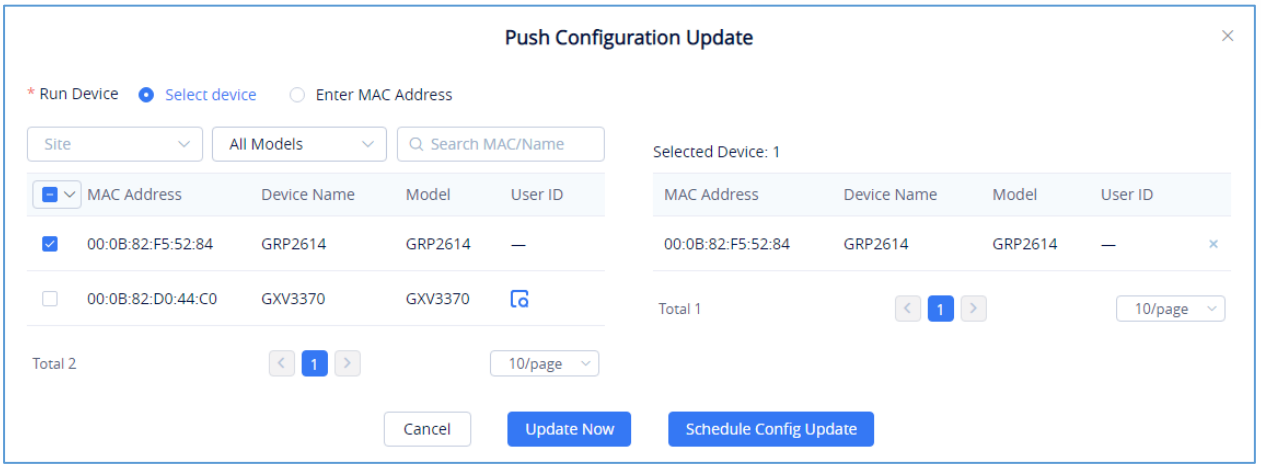


Figure 108: Push Update

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 in the Task Management page.

Edit Group

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

1. Click on the button for the desired group.

Figure 109: Edit Group

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

Note:

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 Configuration File

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

Figure 110: Download Configuration File

Delete Group

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.

Note:

The existing timing tasks involved 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.

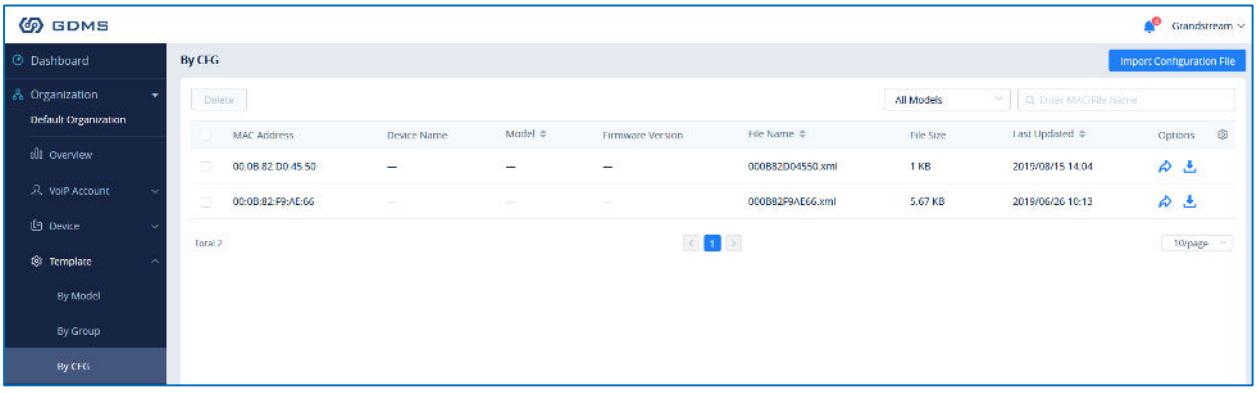


Figure 111: By CFG

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:

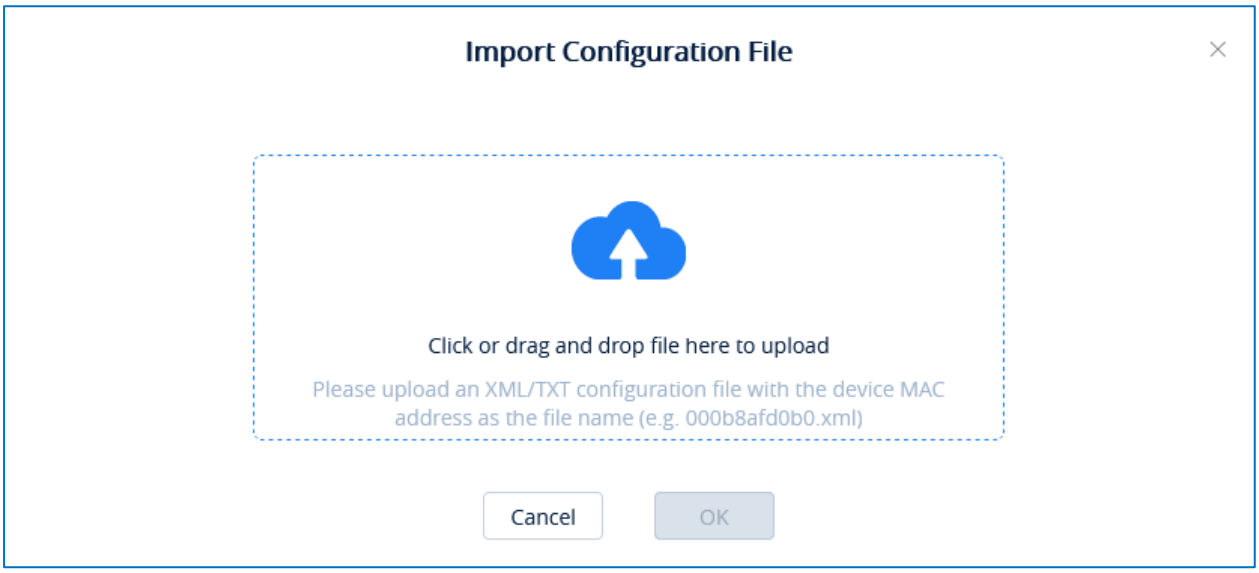


Figure 112: Upload CFG File

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

Note:

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.

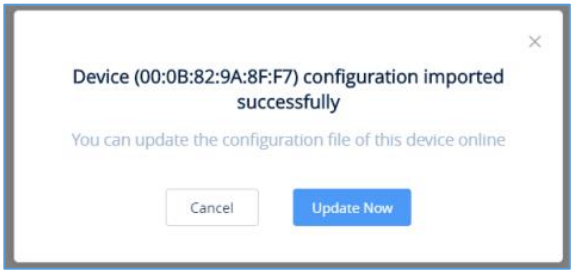


Figure 113: Finalize Import

Notes:

- 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.

Figure 114: 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.

SITE MANAGEMENT

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

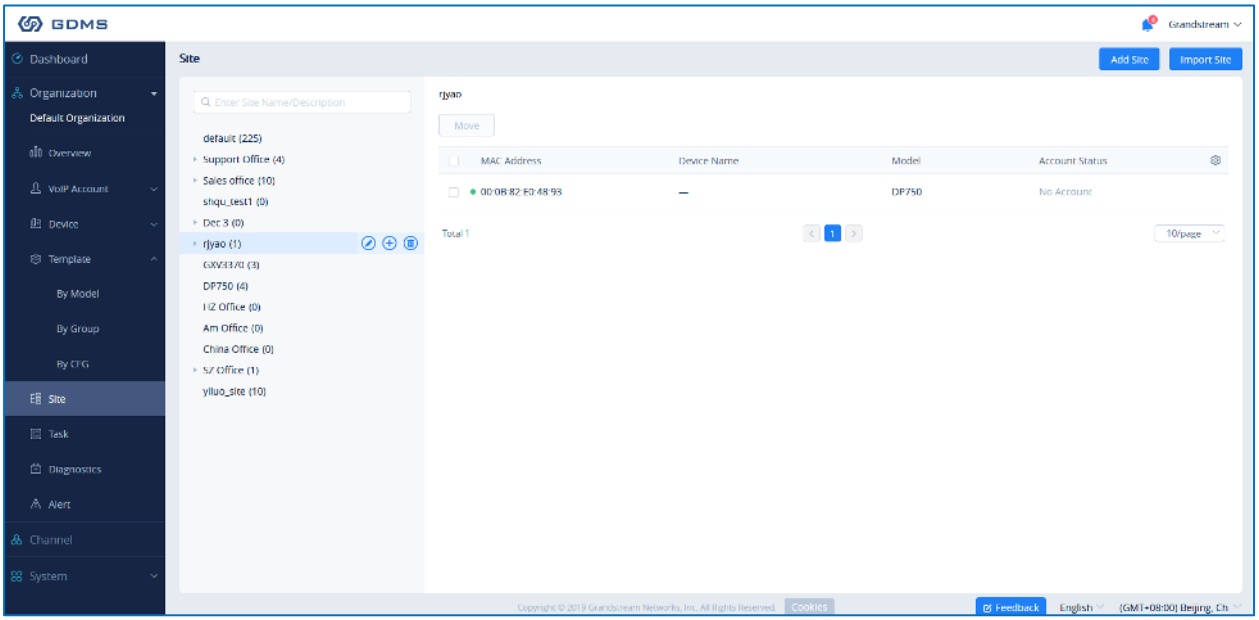


Figure 115: Site Management

Add Site

Users could add a site at any time on 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.

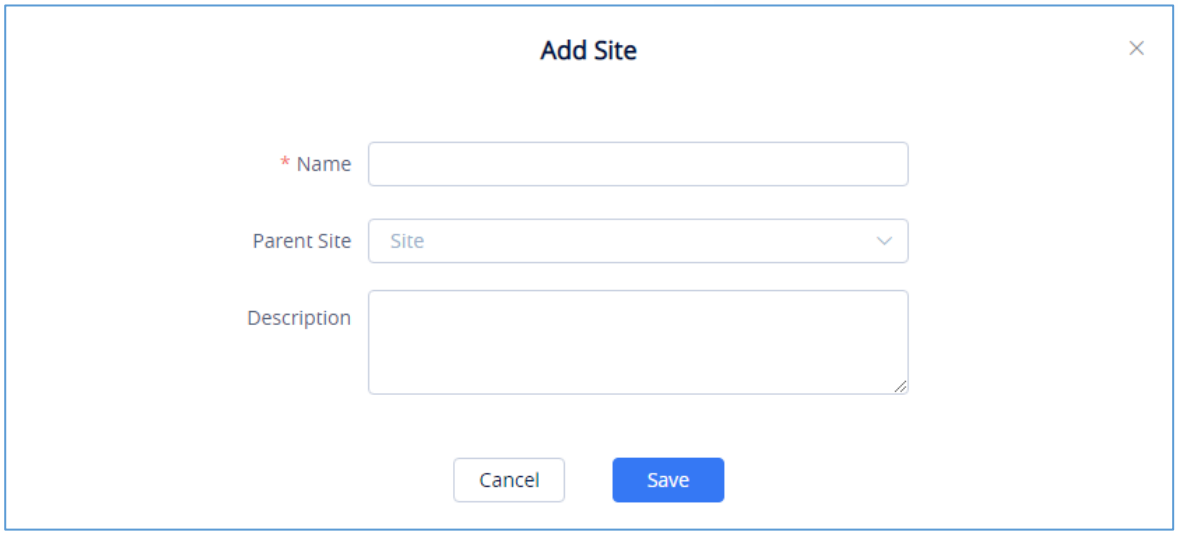


Figure 116: Add Site

Table 25: 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.

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

Batch Import Sites

Users could import a batch of sites into GDMS platform.

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

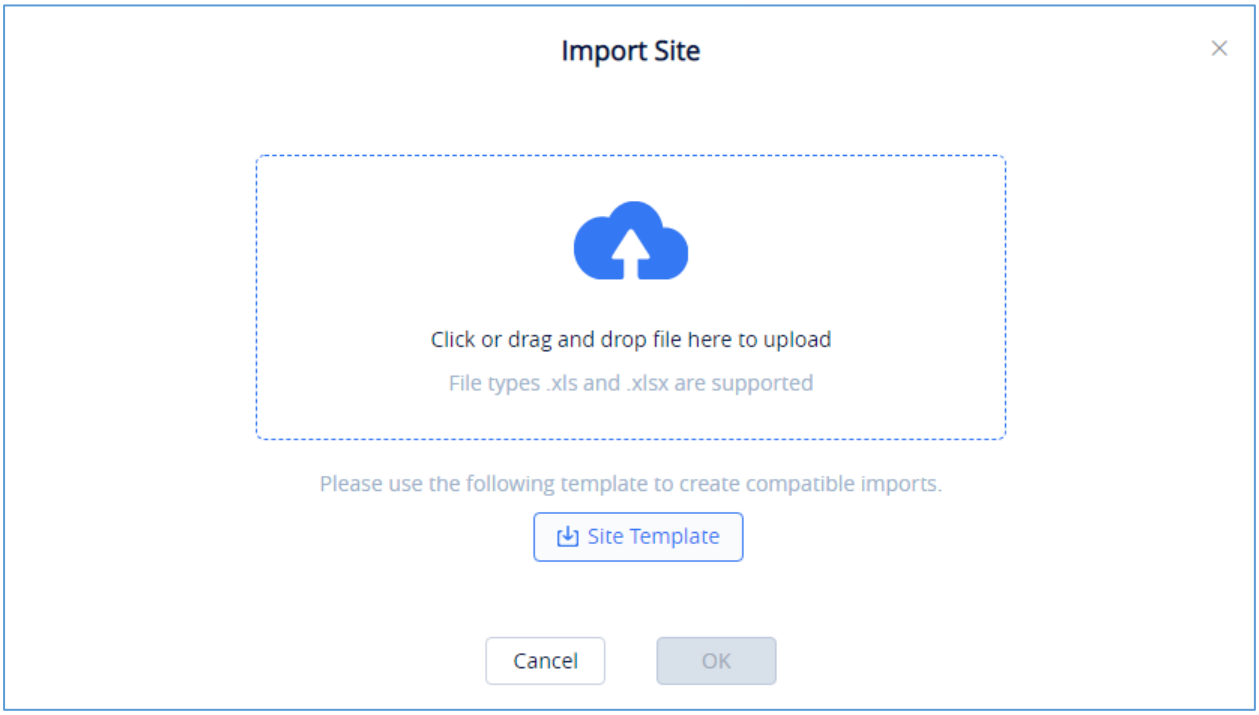


Figure 117: Import Site

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

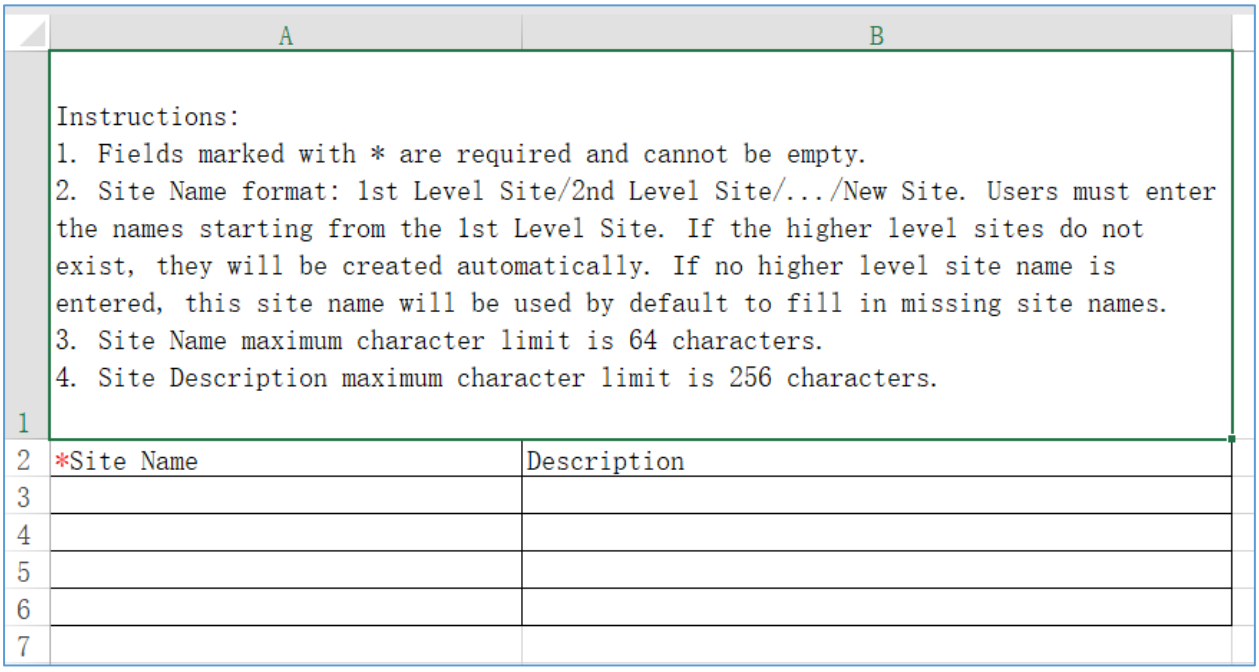


Figure 118: Site Template

Table 26: Site Template Options

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.

3. 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.

4. 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.

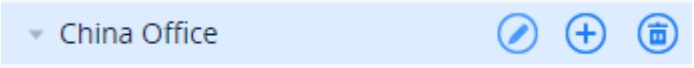
Note:

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 GDMS platform.

1. Click on the button next to the desired site.



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

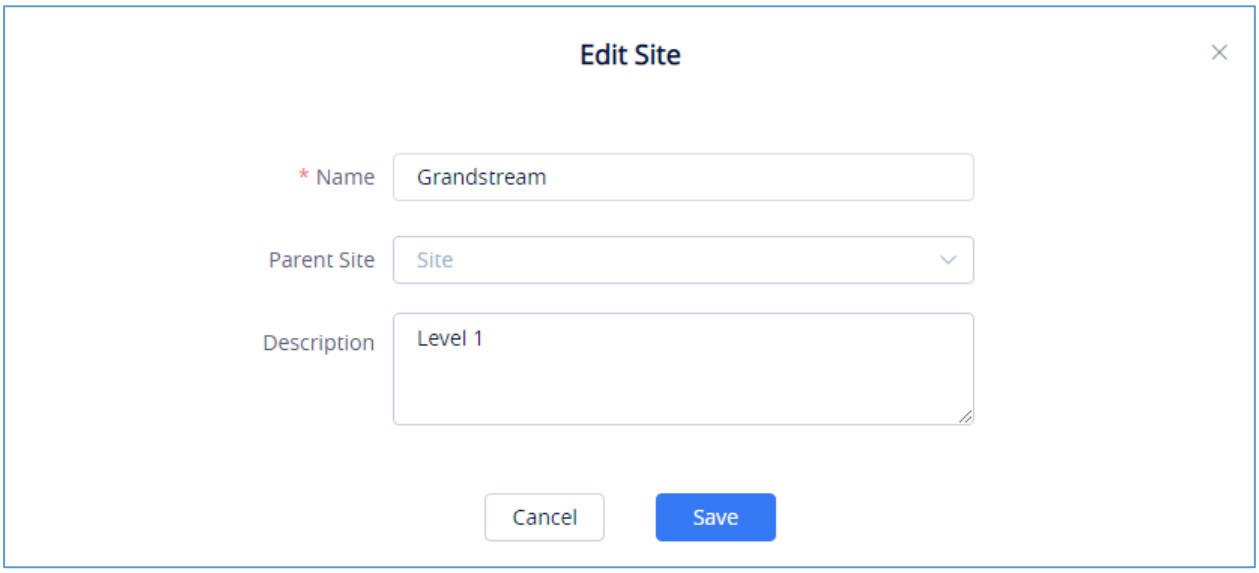


Figure 119: Edit Site

Delete Site

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

Note:

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.

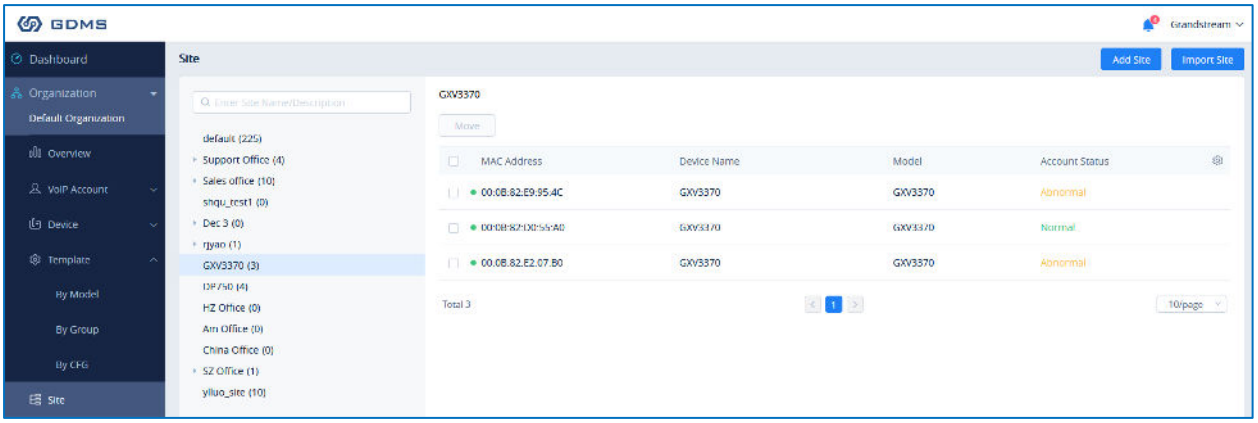


Figure 120: View Devices

Transfer Site

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

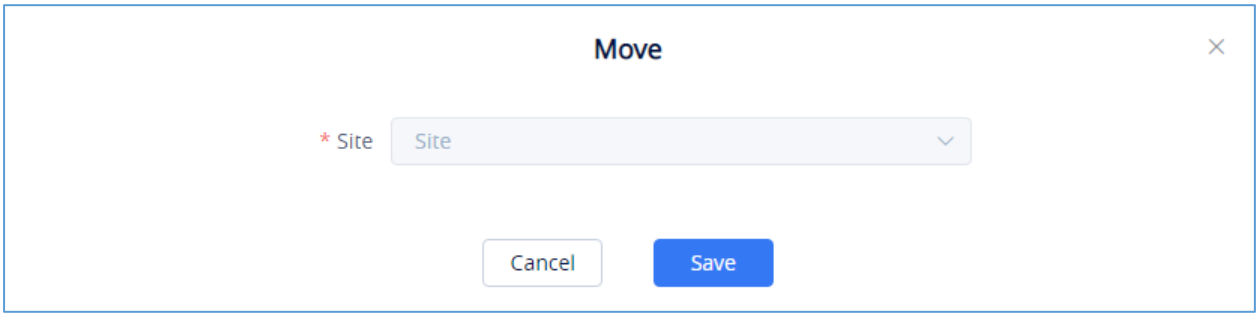


Figure 121: Transfer Site

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.

Add Task

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

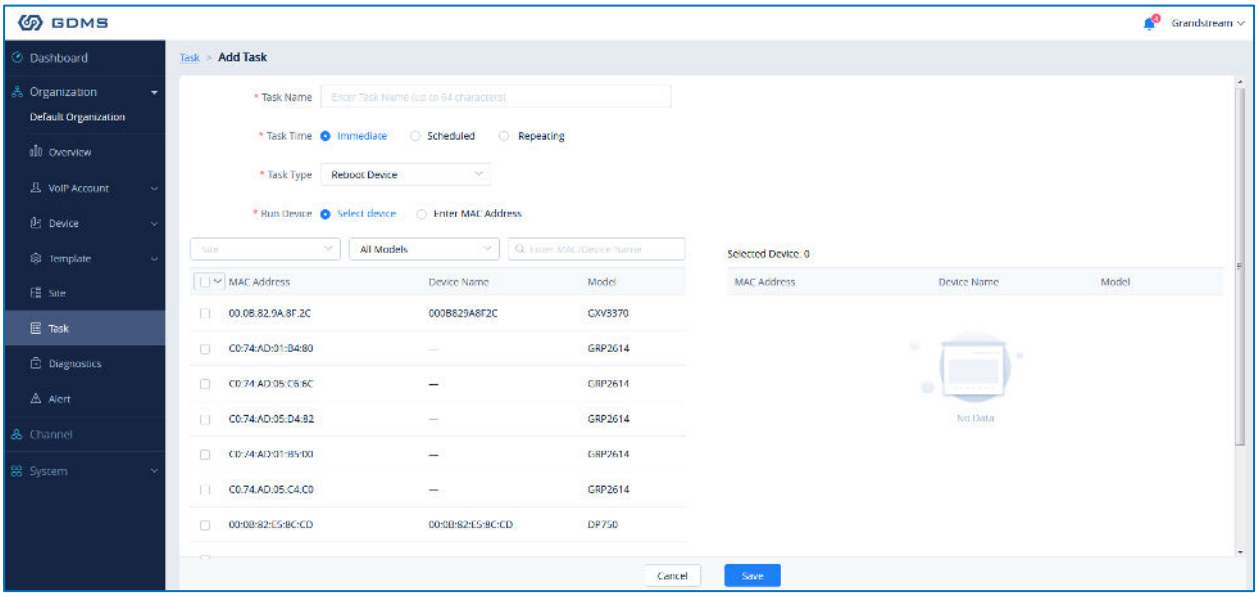
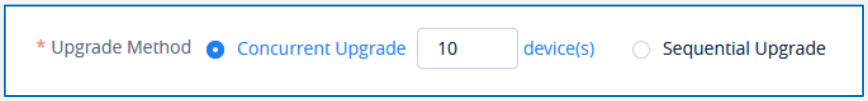


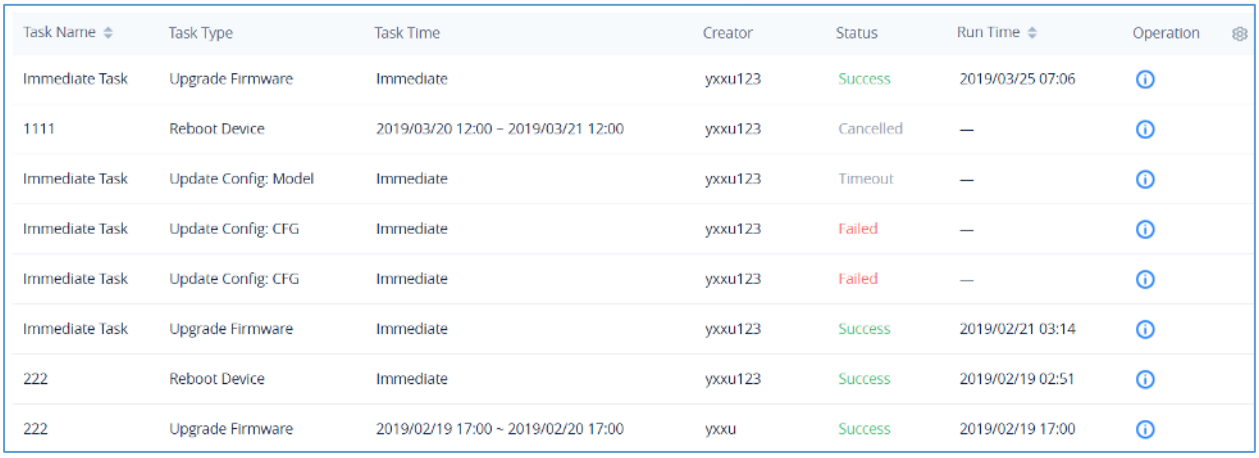
Figure 122: Add Task

Table 27: Add Task

Task Name	Enter the name of the task.
Task Type	• **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. • **Repeating**: Users could reserve the recurring tasks such as daily, weekly, monthly, Nth week of each month, and perform a certain task.
Task Contents	• **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	This option is available only when **Upgrade Firmware** is selected as the Task Type. • **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 the network quality, the user can also limit the maximum number of concurrent devices, such as upgrading 10 devices at the same time. 
Version Requirement	This option is available only when **Firmware Upgrade** is selected as the Task Type. Devices will be upgraded only if they meet certain requirements: • **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 ≤ x ≤ Highest firmware version) will be upgraded.
Execution Device	Select the devices to run this task for. Users can search for devices by their model, assigned site, or MAC address.

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	
1111	Reboot Device	2019/03/20 12:00 – 2019/03/21 12:00	yxxu123	Cancelled	—	
Immediate Task	Update Config: Model	Immediate	yxxu123	Timeout	—	
Immediate Task	Update Config: CFG	Immediate	yxxu123	Failed	—	
Immediate Task	Update Config: CFG	Immediate	yxxu123	Failed	—	
Immediate Task	Upgrade Firmware	Immediate	yxxu123	Success	2019/02/21 03:14	
222	Reboot Device	Immediate	yxxu123	Success	2019/02/19 02:51	
222	Upgrade Firmware	2019/02/19 17:00 ~ 2019/02/20 17:00	yxxu	Success	2019/02/19 17:00	

Figure 123: Task Management List

Notes:

- 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.

View Task Status

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

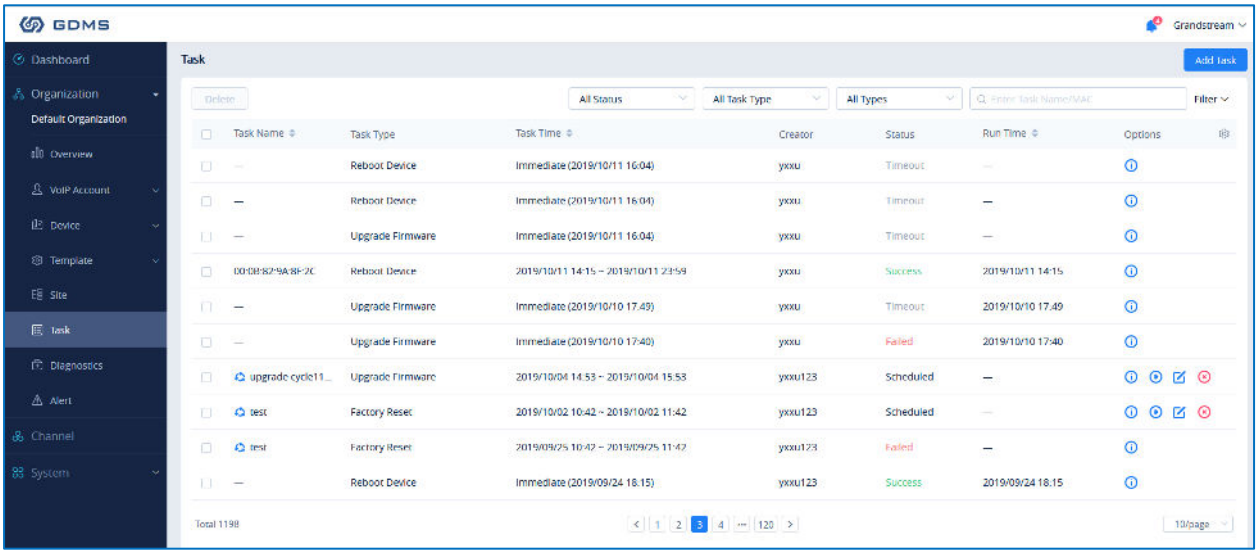


Figure 124: View Task Status

Table 28: Task Status Description

Pending	The task has not been executed yet.
Executing	The task is currently in progress.
Success	The task has completed successfully.
Failed	The task has failed.
Canceled	The task was cancelled.
Timeout	The task was not executed when it arrives 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.

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.

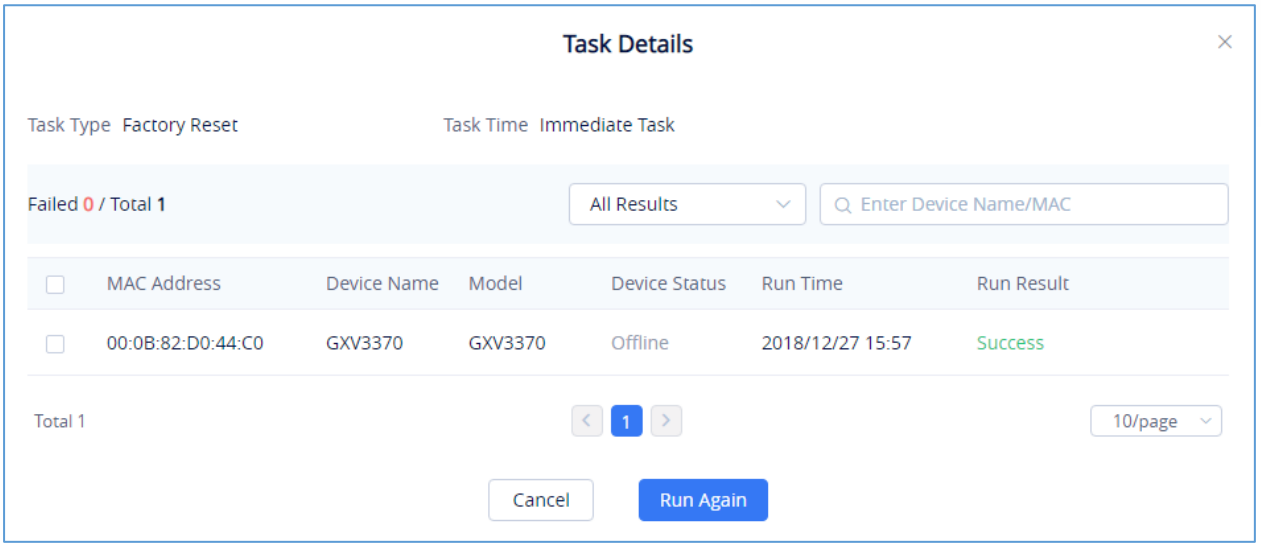


Figure 125: Task Status

Table 29: Task Status Detailed Description

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.

Users could re-create tasks for the executed failed devices, or all devices. If the user re-creates tasks for some 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 a recurring task, 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.

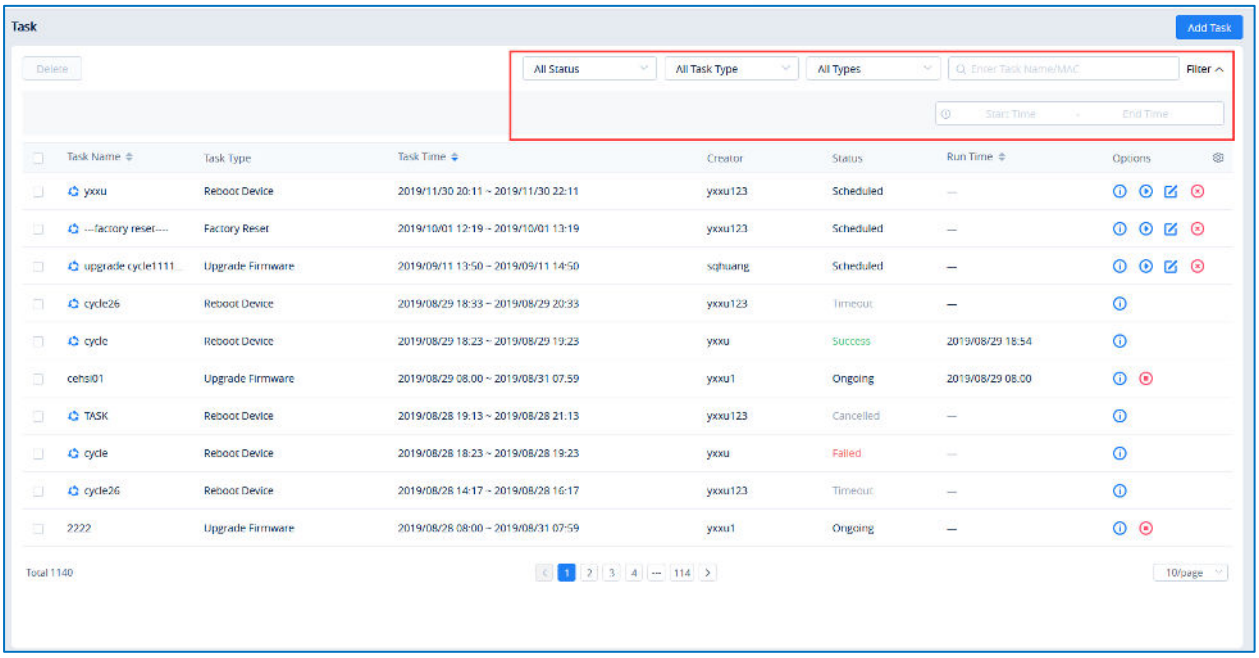


Figure 126: Search Task

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.

Note:

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.

Note:

Support to diagnose VoIP devices and UCM devices.

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.

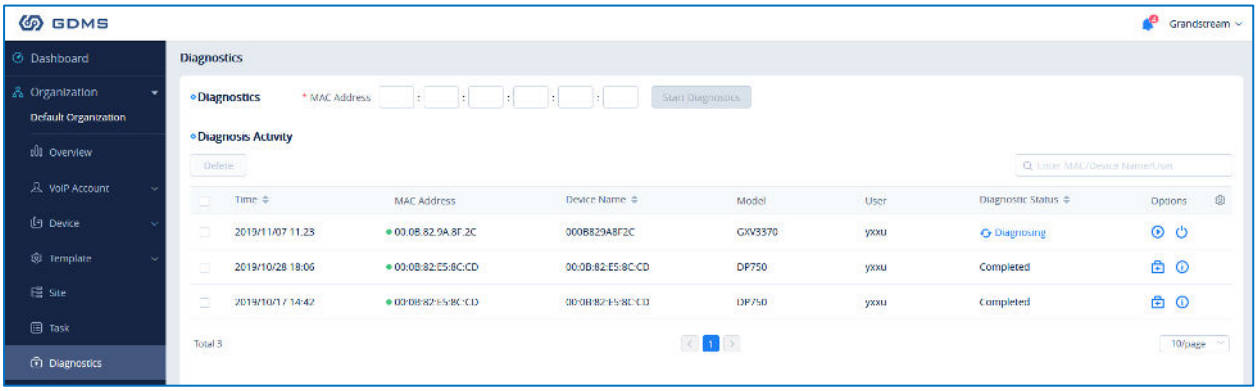


Figure 127: Device Diagnostics

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

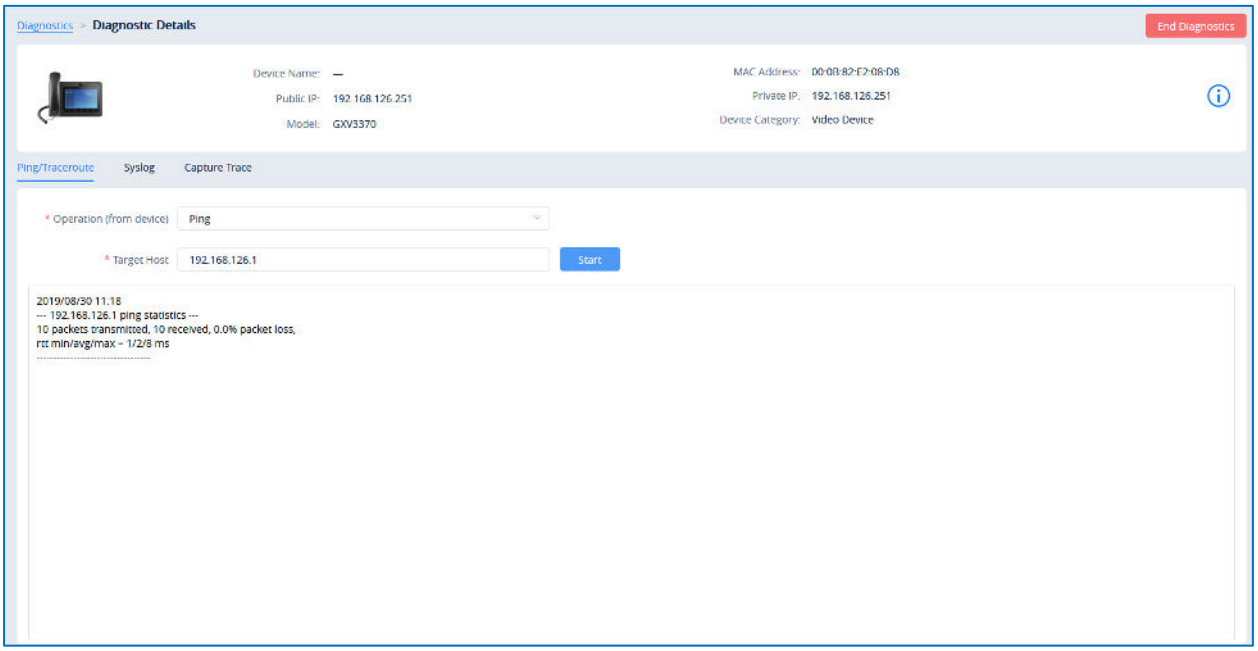


Figure 128: View Diagnostics Details

Notes:

- If the device is offline, users cannot diagnose this device on 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.

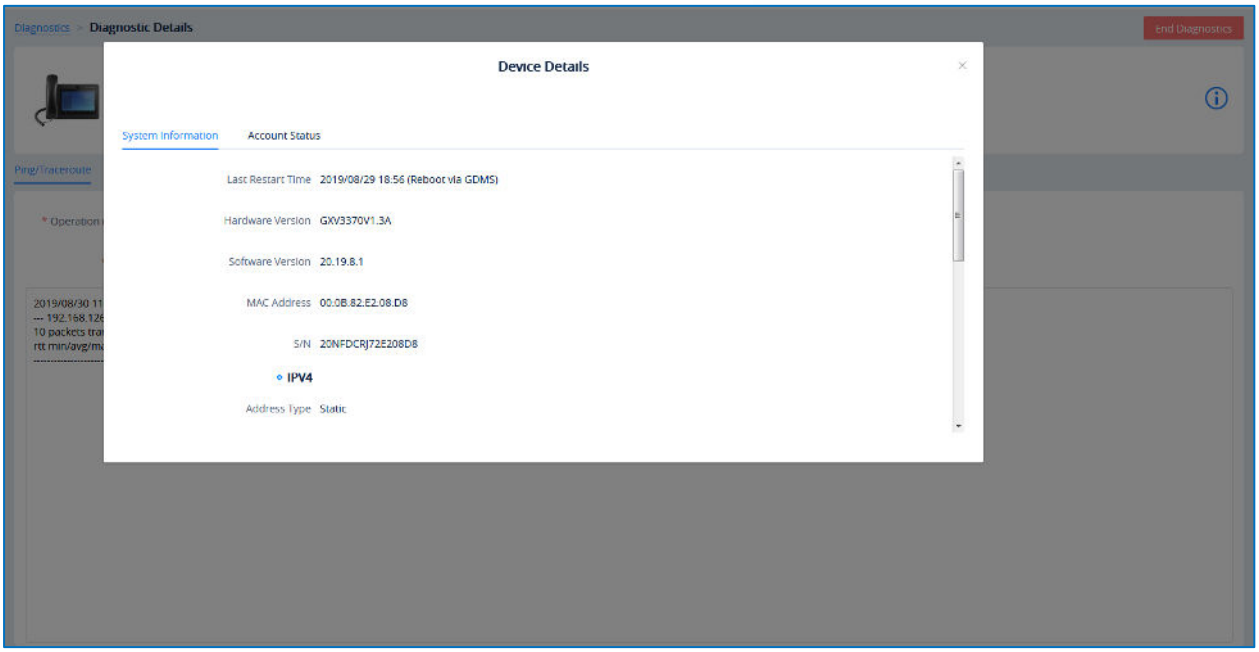


Figure 129: View Device Details

Ping/Traceroute

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

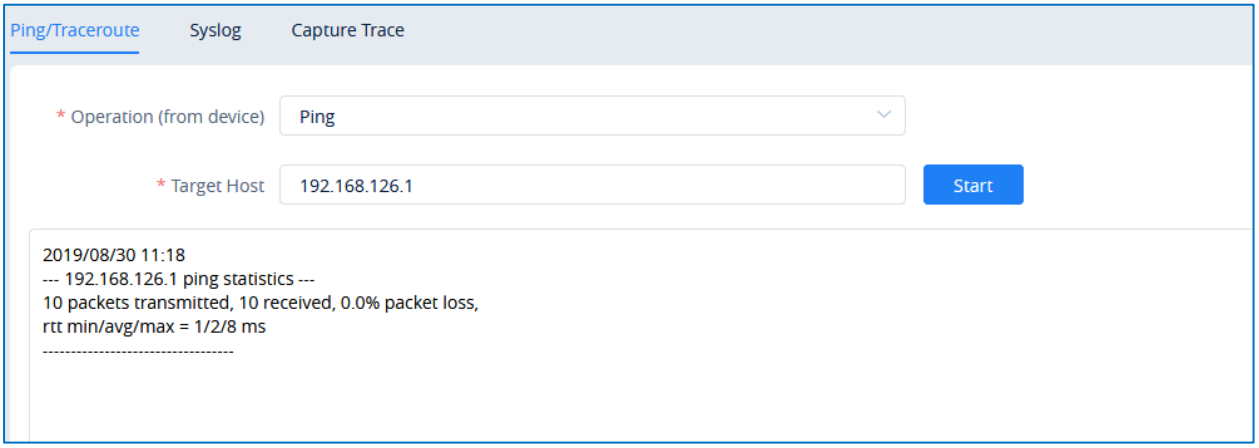


Figure 130: Ping/Traceroute

Table 30: Ping/Traceroute Options

Operation Method	• **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.

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

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

Note: To avoid cancelling 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.

Notes:

- An ongoing syslog capture will end automatically after 7 days.

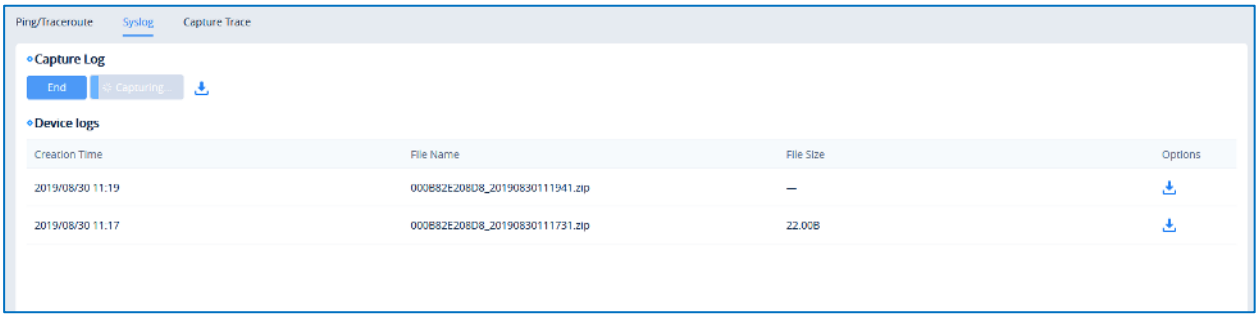


Figure 131: Syslog

- For UCM devices, syslog download function is temporarily not available.

Capture Trace

Users can get 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.

Notes:

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

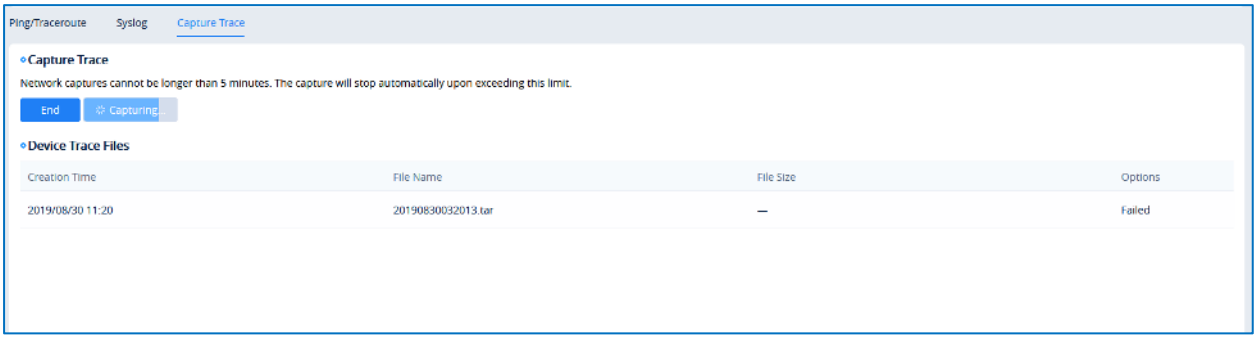


Figure 132: Capture Trace

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 "**Start Diagnostic**" button to start network diagnosis.

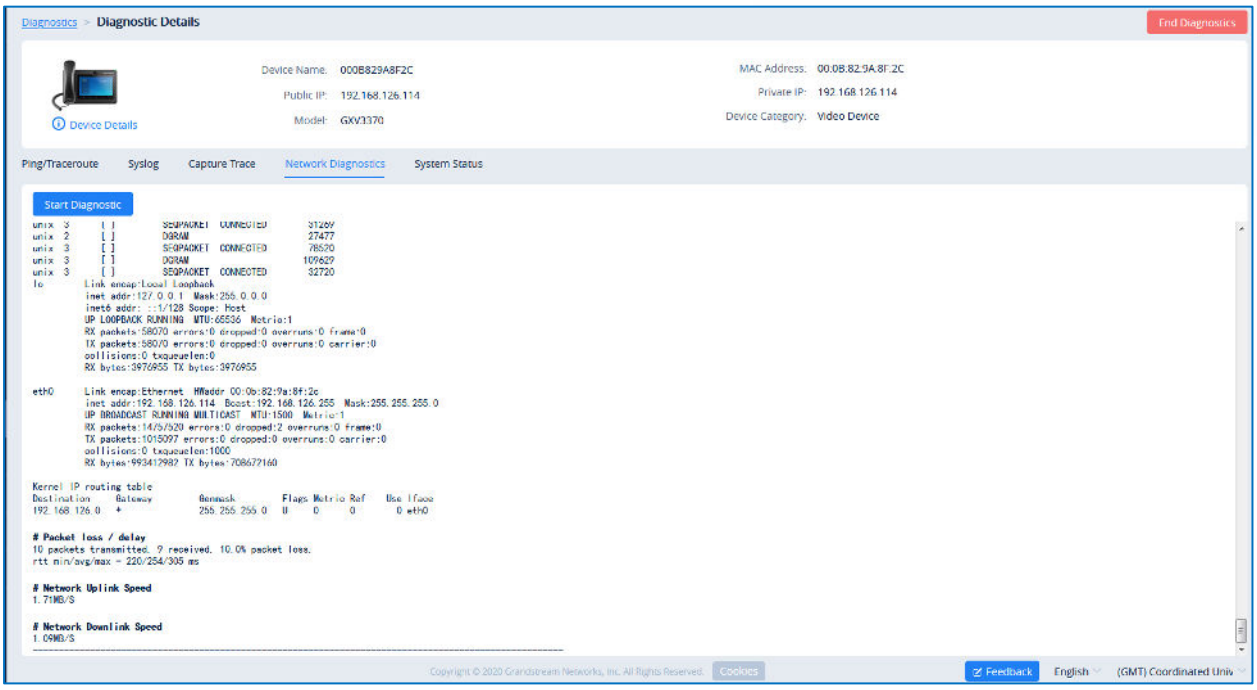


Figure 133: Network Diagnostics

System Status

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

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

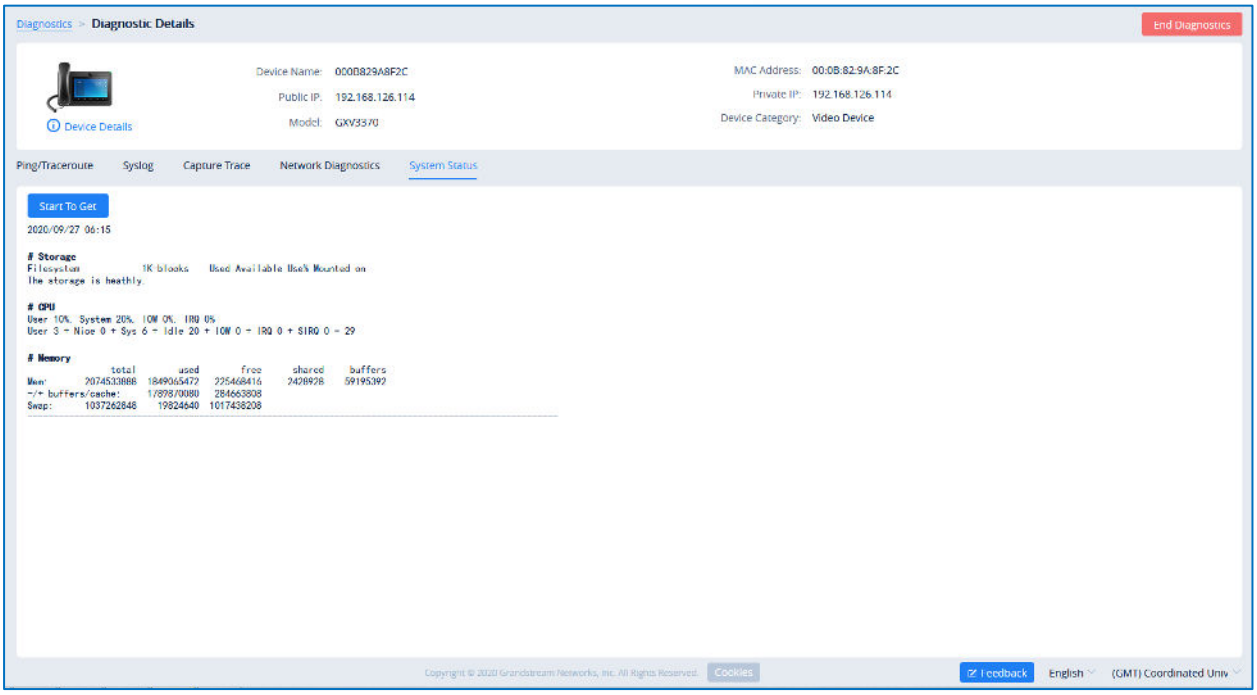


Figure 134: System Status

End Diagnostics

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

Note:

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.

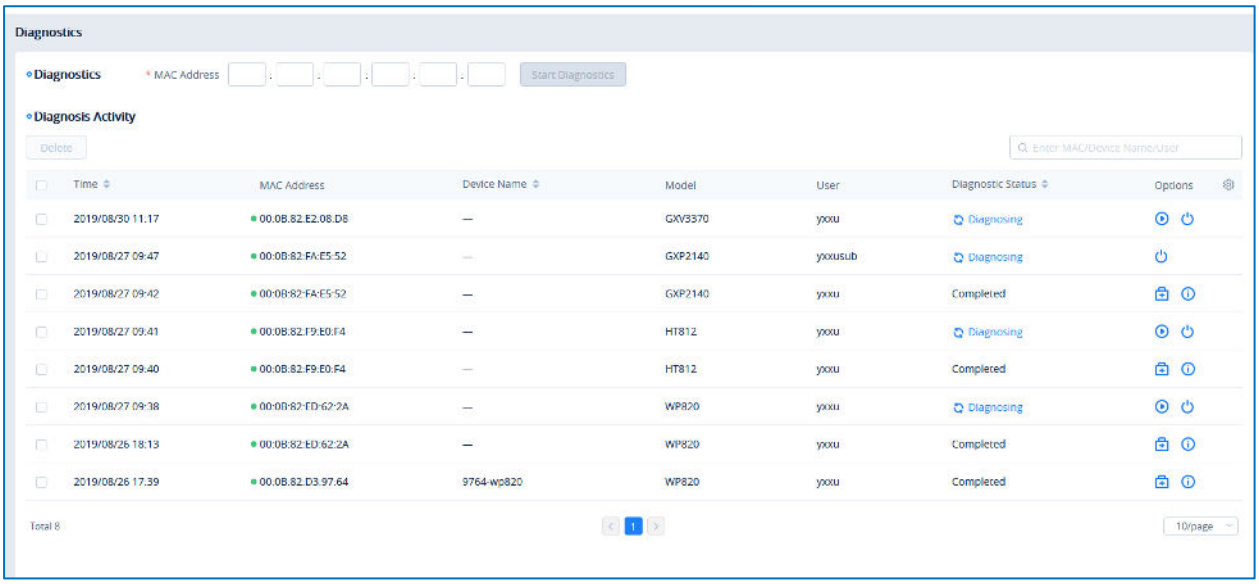


Figure 135: Diagnostics Records

1. If a device is currently being diagnosed, click on the button to continue diagnosing or the button to end it.

2. If a device has been diagnosed already, click on the button to start another round of diagnosis or the button to view the results.

3. View the diagnostic history of a specific device by using the search bar on top right of the **Diagnostic Records** page.

4. Users can delete records by selecting one or more items and clicking on the **Delete** button.

ALERT MANAGEMENT

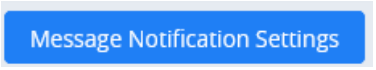
GDMS has an alert system that will trigger when certain conditions are fulfilled. There are 3 alert levels: High, Medium, and Low.

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.

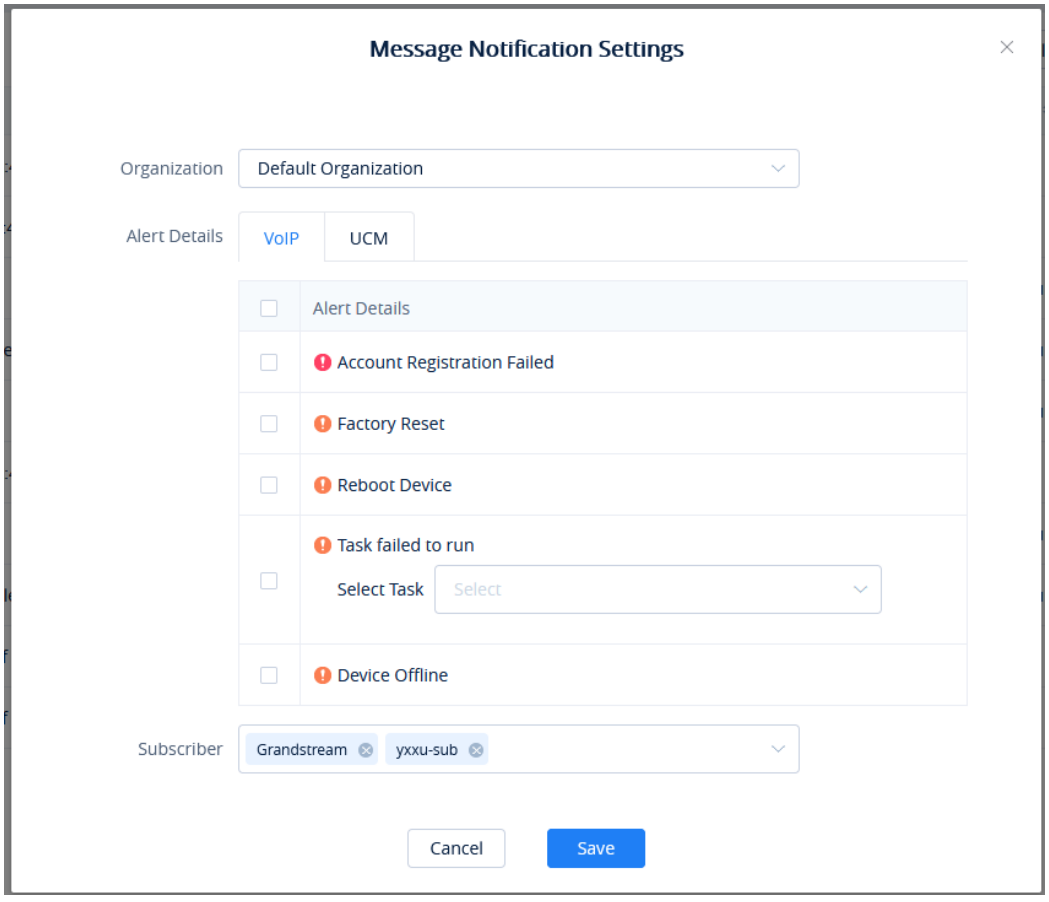


Figure 136: Message Notification Settings

Table 31: Message Notification Settings

Organization	Select the organization in question.
Alert Details	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: **High Level:** ▪ Account Registration Failure ▪ UCM cloud storage space is insufficient or full. **Medium Level:** ▪ Factory Reset ▪ Task Run Failure (users can specify the tasks they want notifications for) ▪ Device Offline ▪ Device Reboot **Note:** Only the UCM devices have UCM Remote Control 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 current user can be selected.

Note:

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.

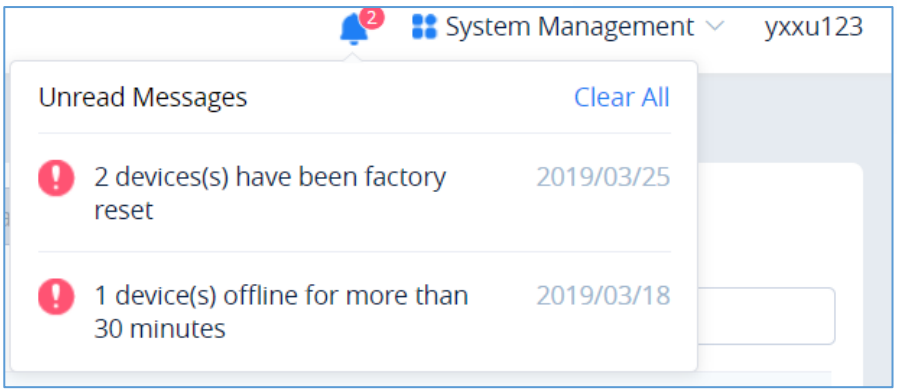


Figure 137: Unread Message Icon

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.

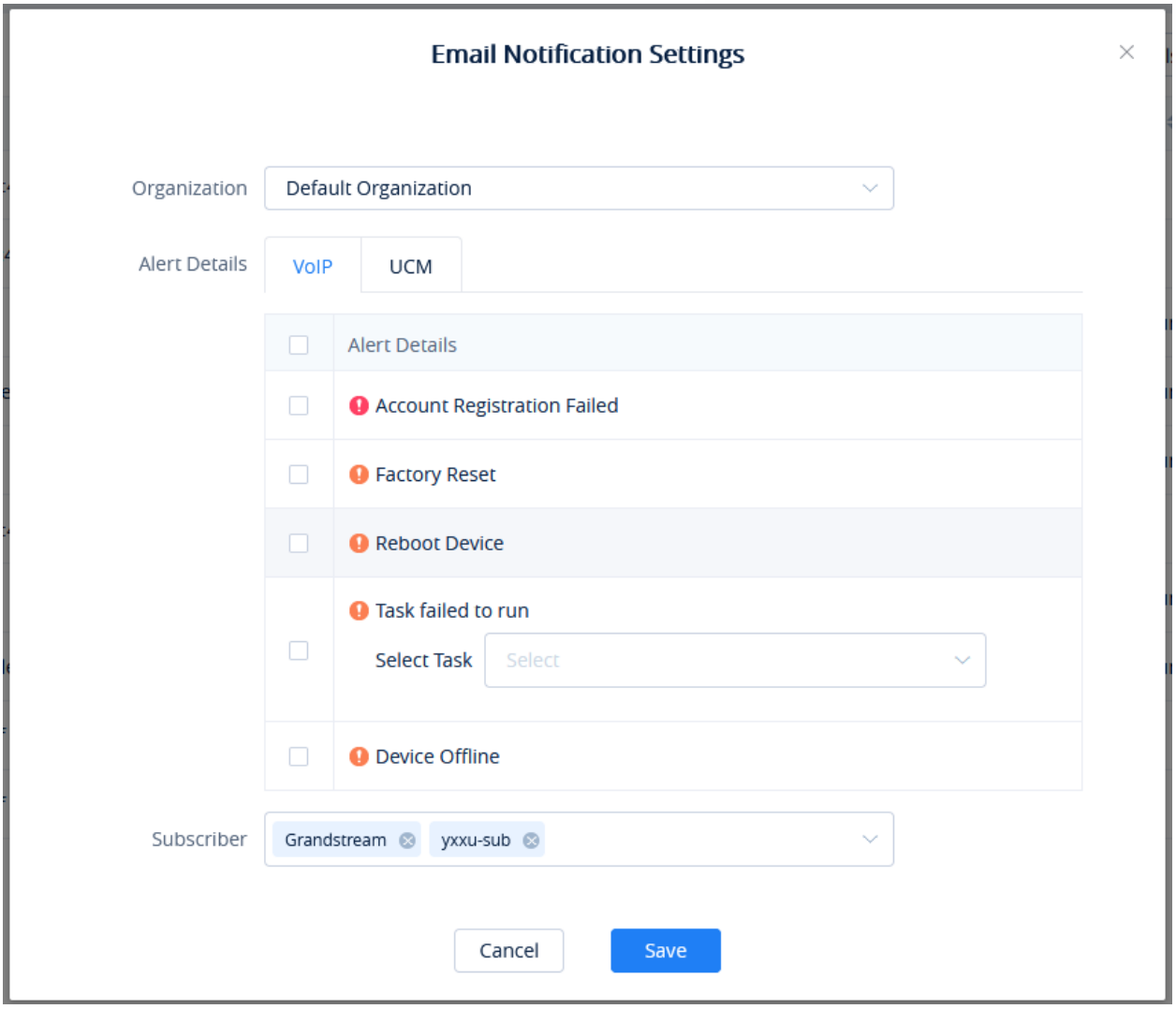


Figure 138: Email Notification Settings

Table 32: Email Notification Settings

Organization	Select the organization in question.
Alert Details	VoIP devices alert and UCM devices alert. Users can click Tab and select the alert contents, respectively.
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: **High Level:** ▪ Account Registration Failure ▪ UCM cloud storage space is insufficient or full.

	Medium Level: ▪ Factory Reset ▪ Task Run Failure (users can specify the tasks they want notifications for) ▪ Device Offline ▪ Device Reboot **Note:** Only the UCM devices have UCM Remote Control 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 current user can be selected.

Note:

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. In order 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.

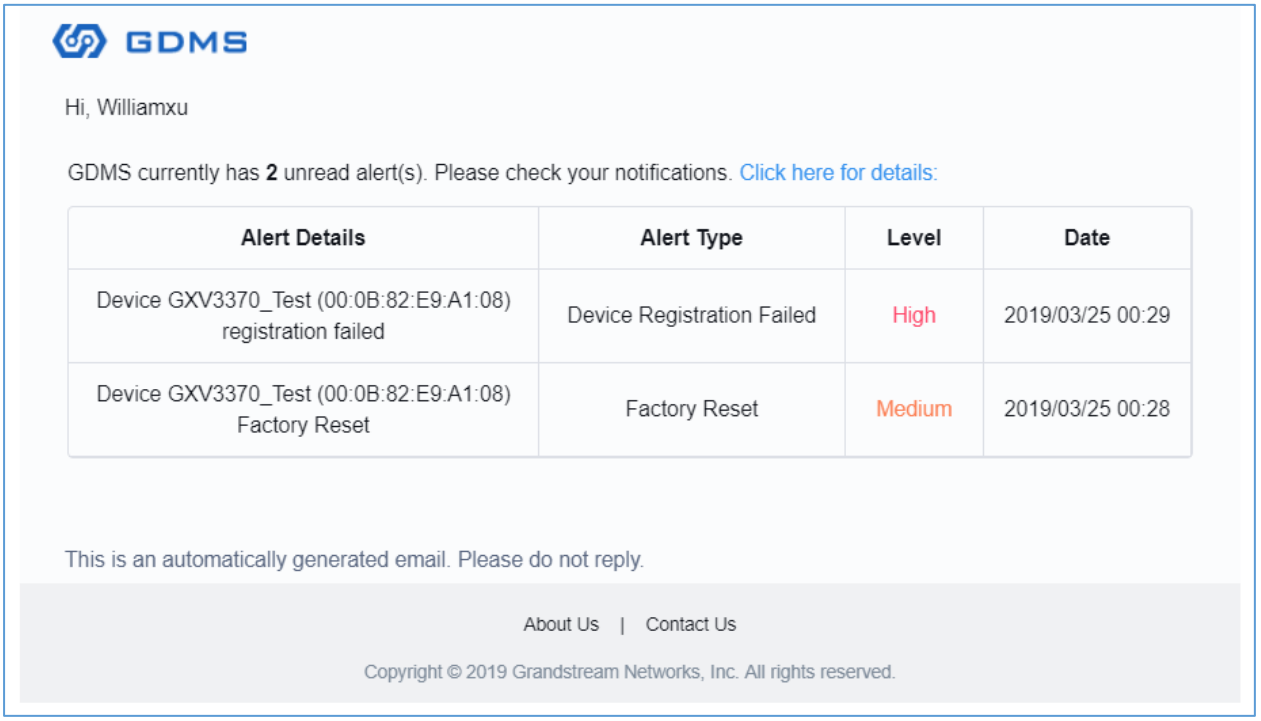
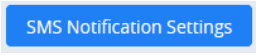


Figure 139: Email Alert Notification

SMS Notification Settings

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

1. To manage email alert notifications, click on the 

button on the top-right corner of the **Alert Management** page.

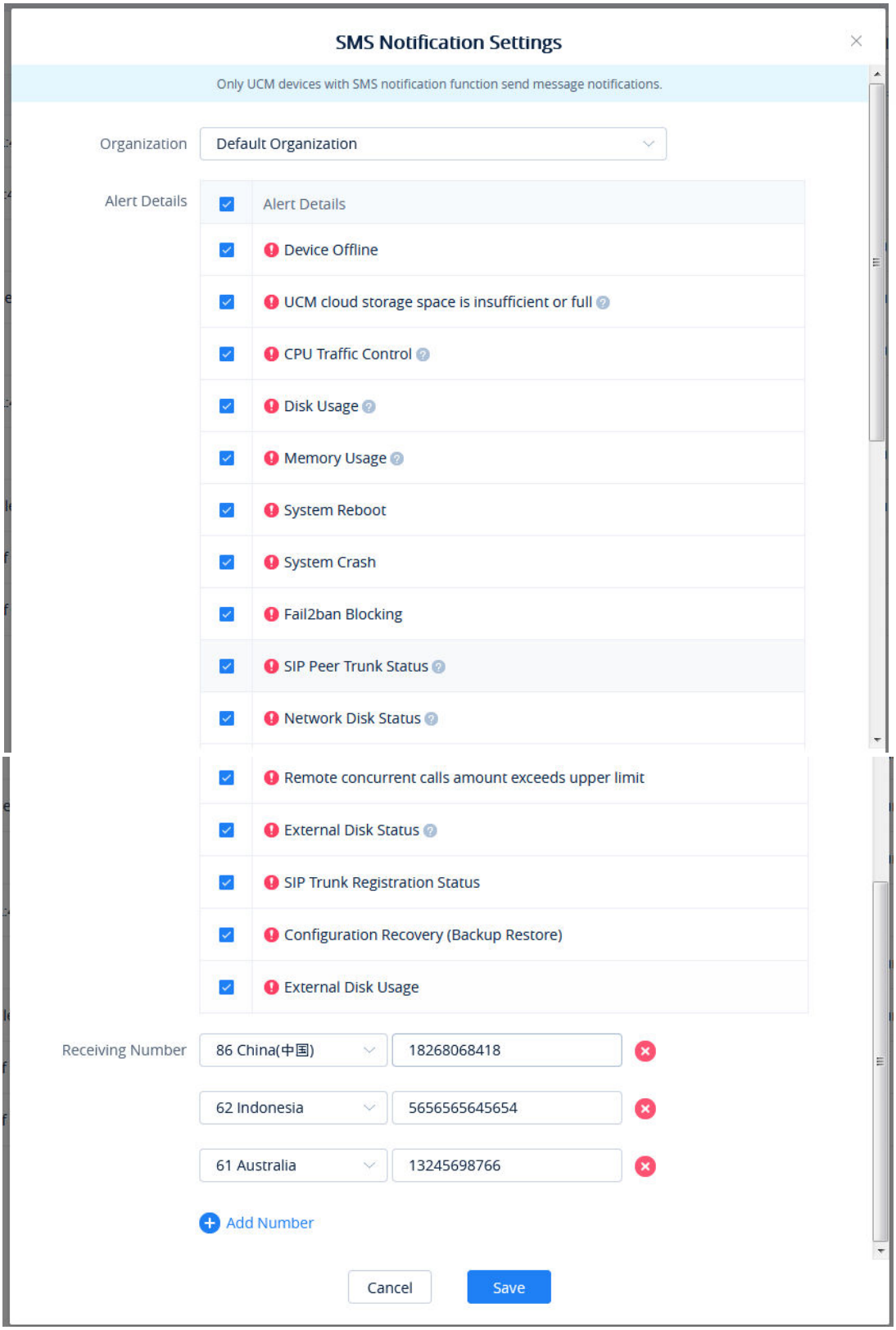


Figure 140: SMS Notification Settings

Table 33: Notification Settings

Organization	Select the organization in question.
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: **High Level:** ▪ UCM cloud storage space is insufficient or full. **Medium Level:** ▪ UCM Device Offline **Note:** Only the UCM devices have UCM Remote Control advanced plans can report the alert contents and send the alert notifications.
Receiving Number	Enter the phone numbers which will receive the notification message. The phone numbers can be added or deleted. When the number is entered, the user needs to click "**Send Captcha**" option and enter the received verification code to finish adding the receiving number.

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

View Alert Notification

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

Note:

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.

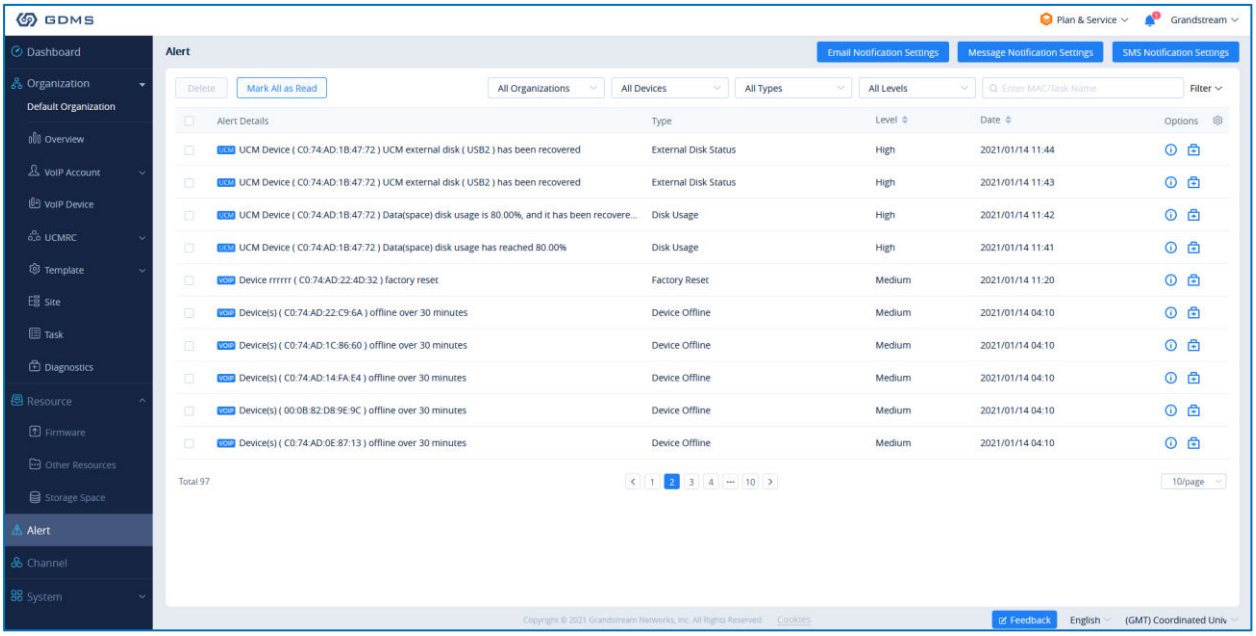


Figure 141: View Alert Notification

- **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 Mark All as Read 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.
- **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.

RESOURCE MANAGEMENT

Firmware Management

Custom Firmware

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

Note:

It is recommended to download the device's firmware from Grandstream Official website in order 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.

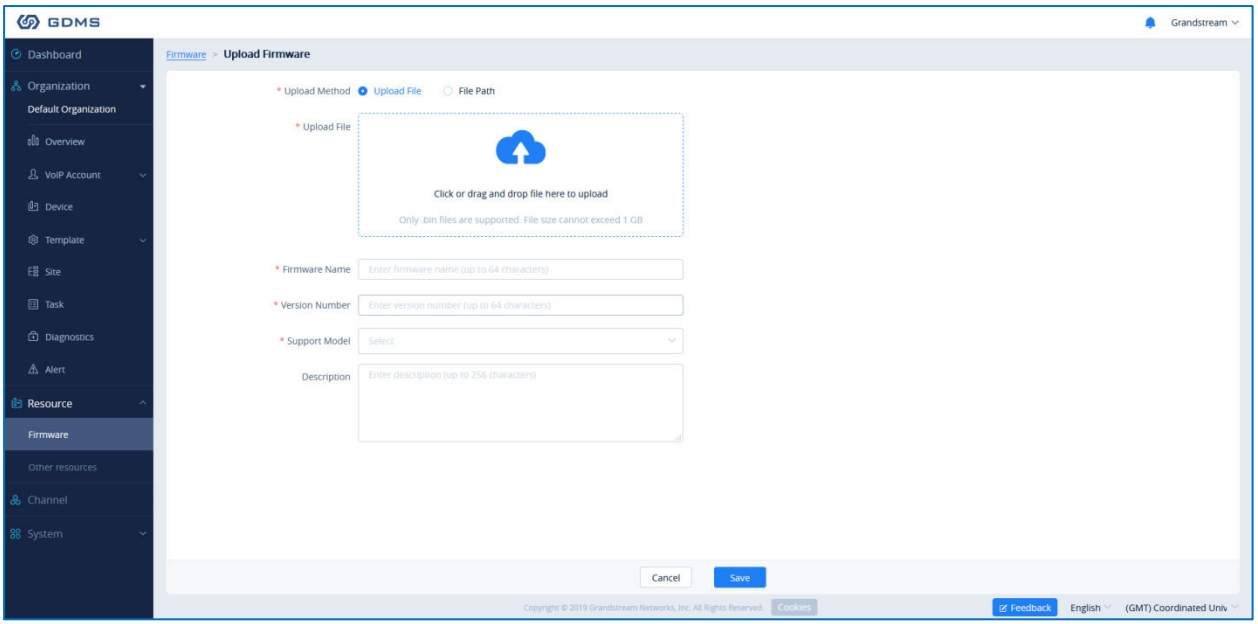


Figure 142: Custom Firmware

Table 34: Custom Firmware

Upgrade Path	• **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. Maximum character limit is 256.

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.

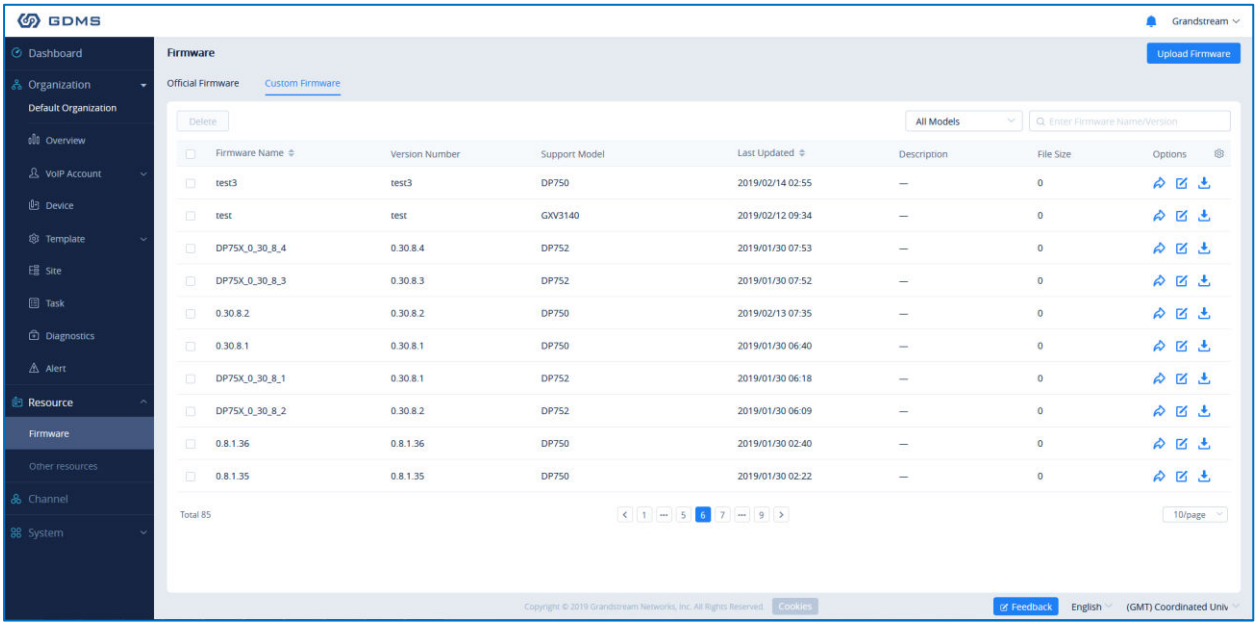


Figure 143: Finish Uploading Custom Firmware

Official Firmware

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

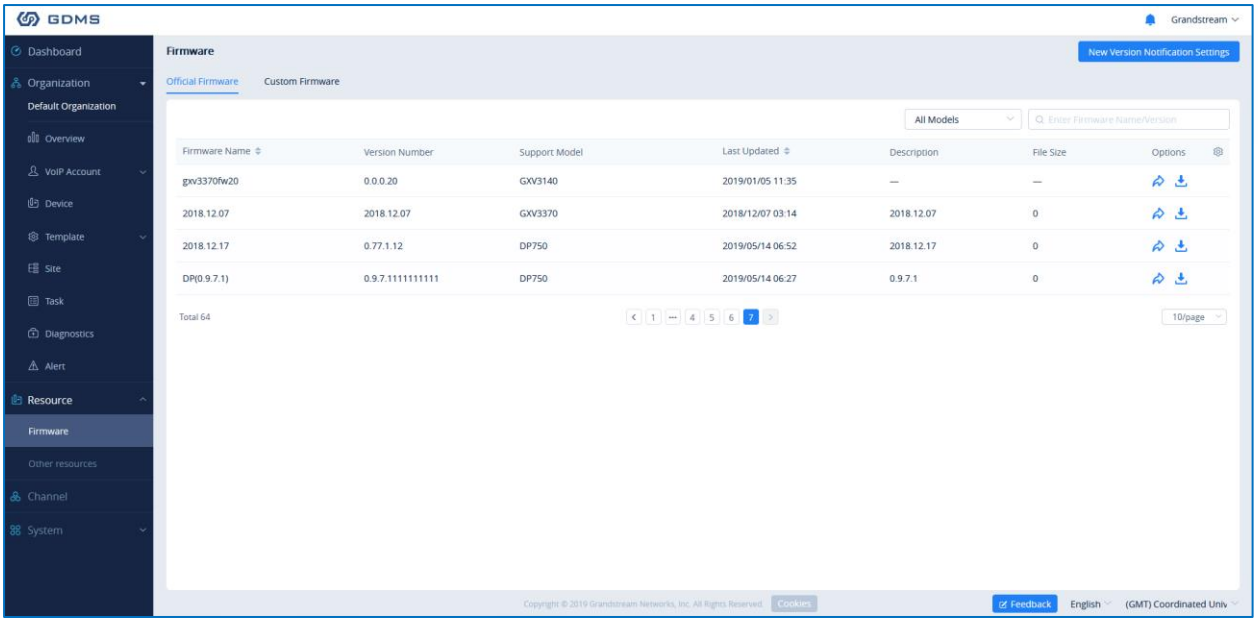


Figure 144: Official Firmware

Note:

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:

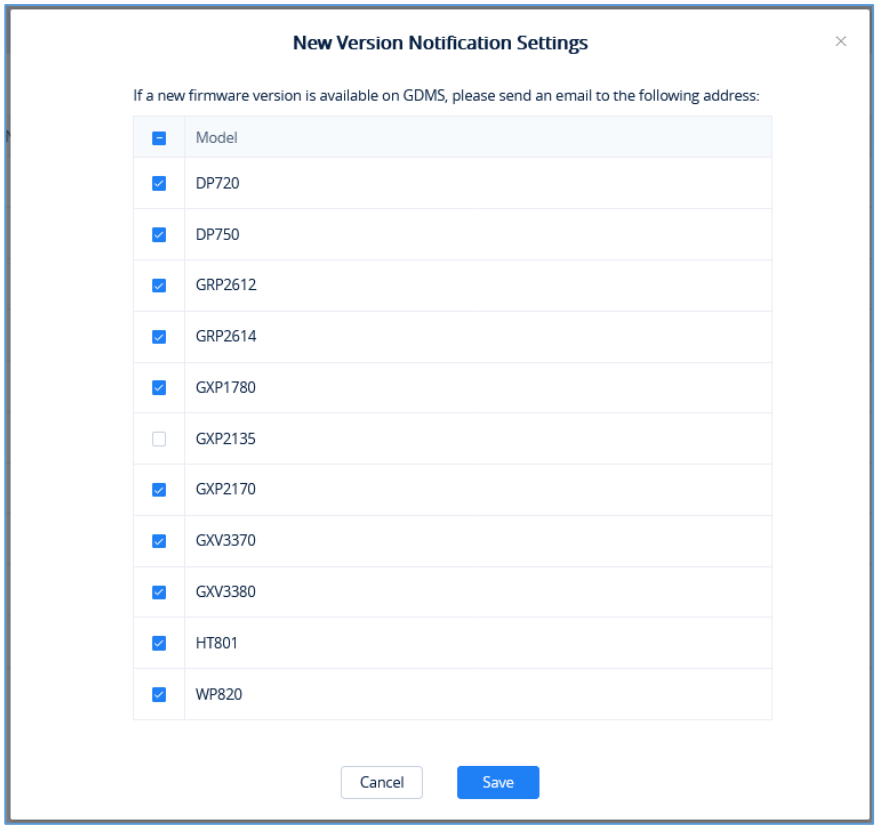


Figure 145: Firmware Update Notification Settings

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

Push to Upgrade Firmware

Users could push the upgraded firmware to the devices directly, or the devices in a range of firmware versions.

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

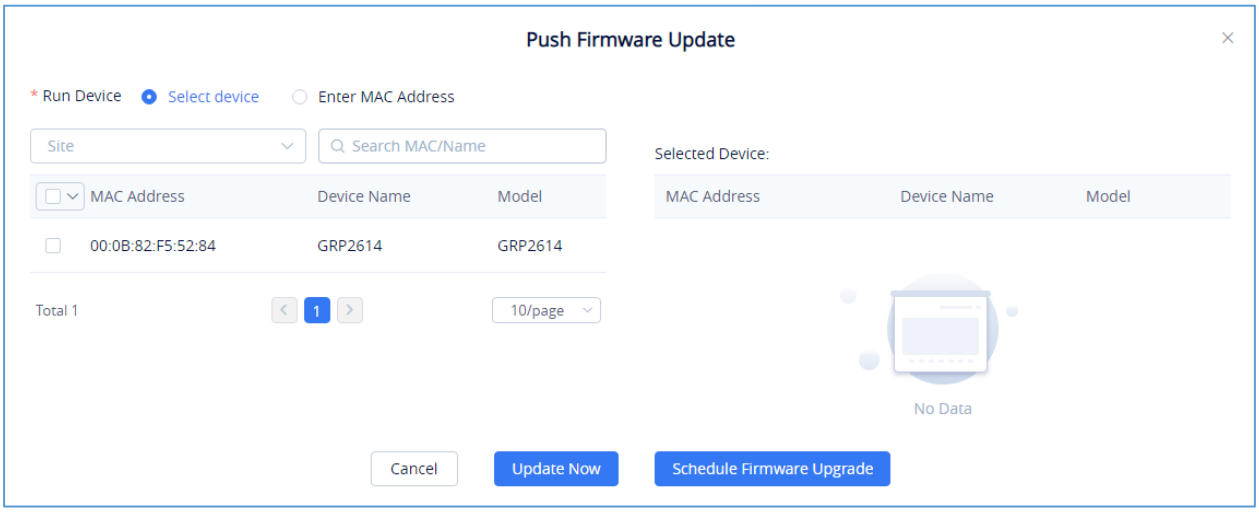


Figure 146: Push to Upgrade Firmware

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 in the **Task Management** page.

Edit Firmware

Users could edit the firmware name, firmware version, and other information on GDMS platform. Users could also re-upload the firmware into GDMS platform. Click on the button to access to the firmware editing page.

Note:

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.

Note:

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

Delete Firmware

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

Note:

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 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:

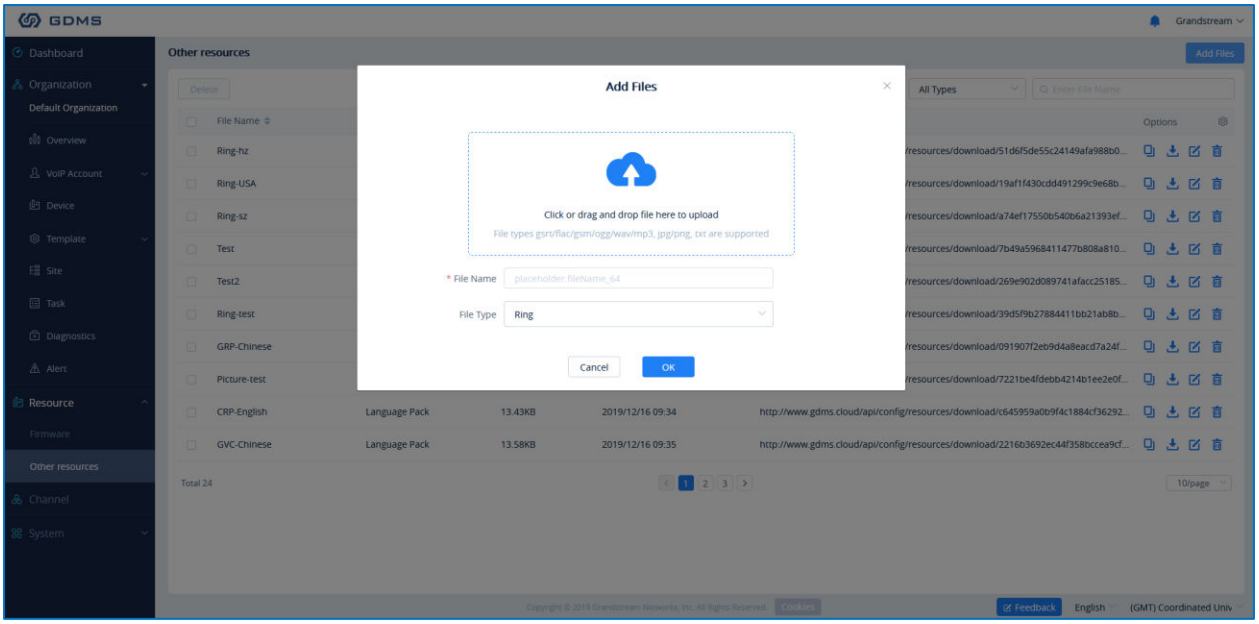


Figure 147: Custom Firmware

Table 35: Custom Firmware

File	Users could drag the file to the uploading area or click on the uploading area to select the file. 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. File size limit: Bin file/Ringtone – 128KB; Picture/Language pack – 500KB; Other – 5MB.
File Name	This is used to identify the file name. The limit is 1 - 64 characters.
File Type	This is used to identify the file type, such as ringtone, picture, language pack, and Others.

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

Notes:

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

View Resource List

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

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

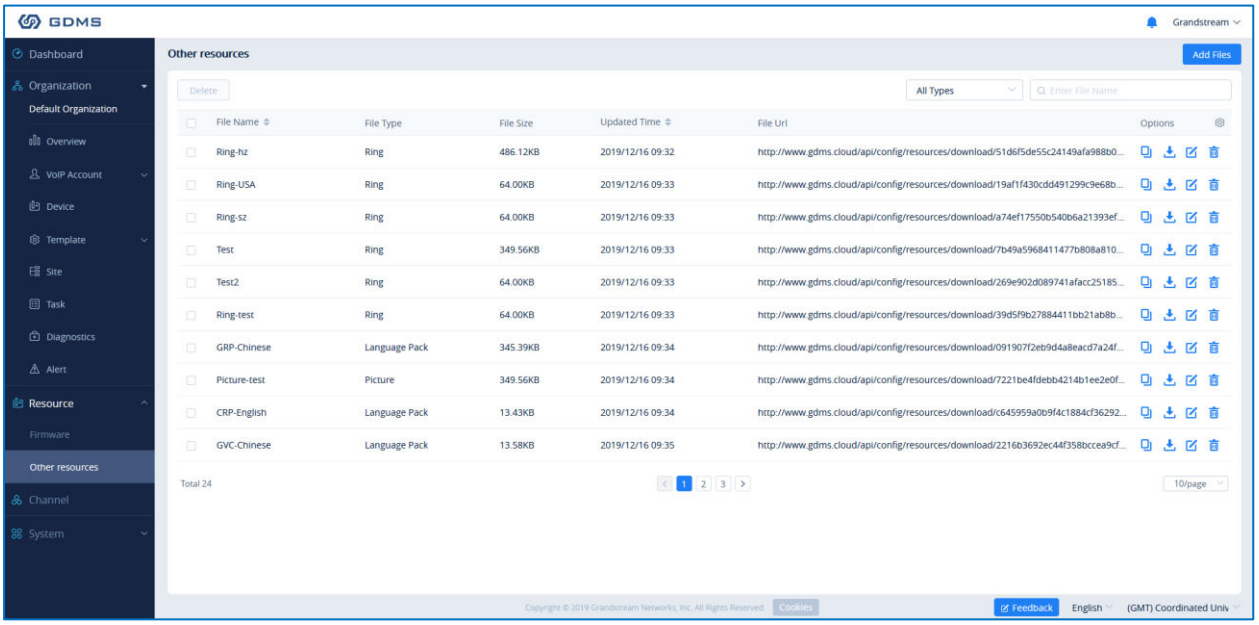


Figure 148: Other Resources

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.

Note:

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 GDMS platform.

Note:

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

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:

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

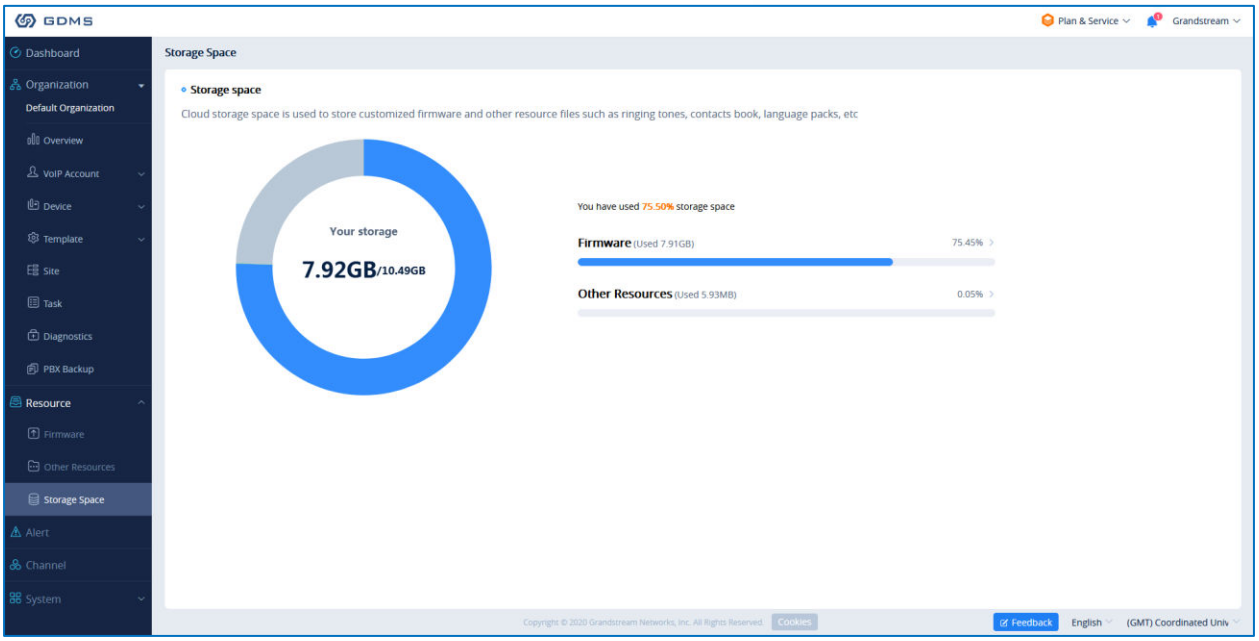


Figure 149: View Storage Space

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:

1. 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.

Note:

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 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:

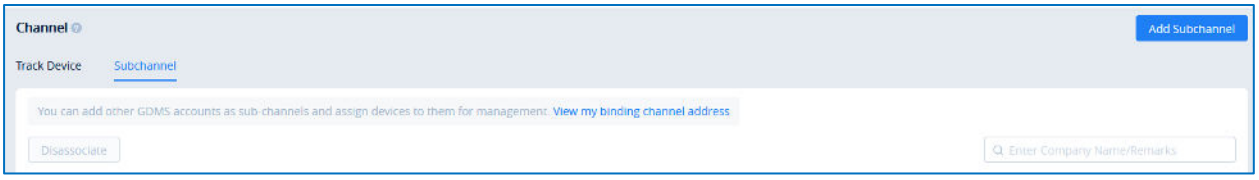


Figure 150: View My Binding Channel Address

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

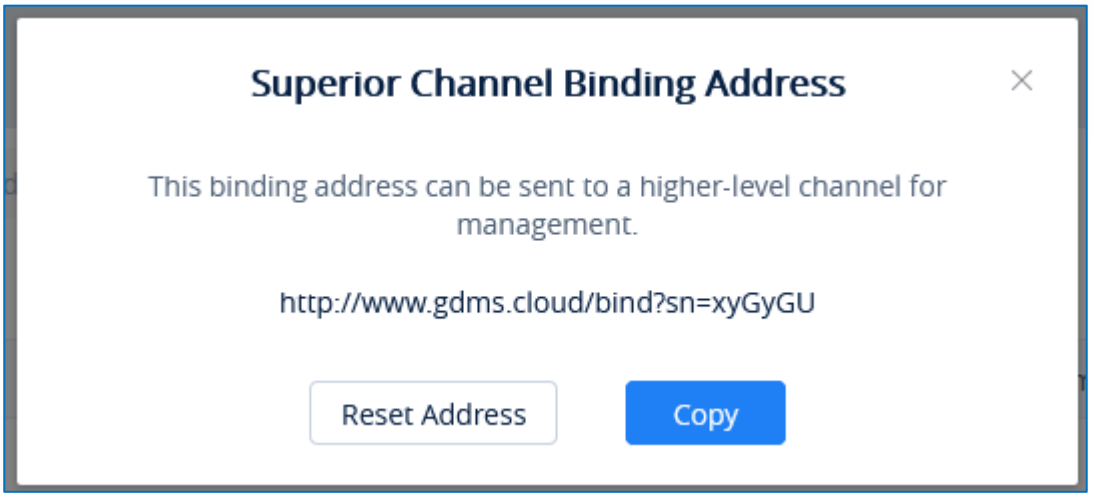


Figure 151: Superior Channel Binding Address

- **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' 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:

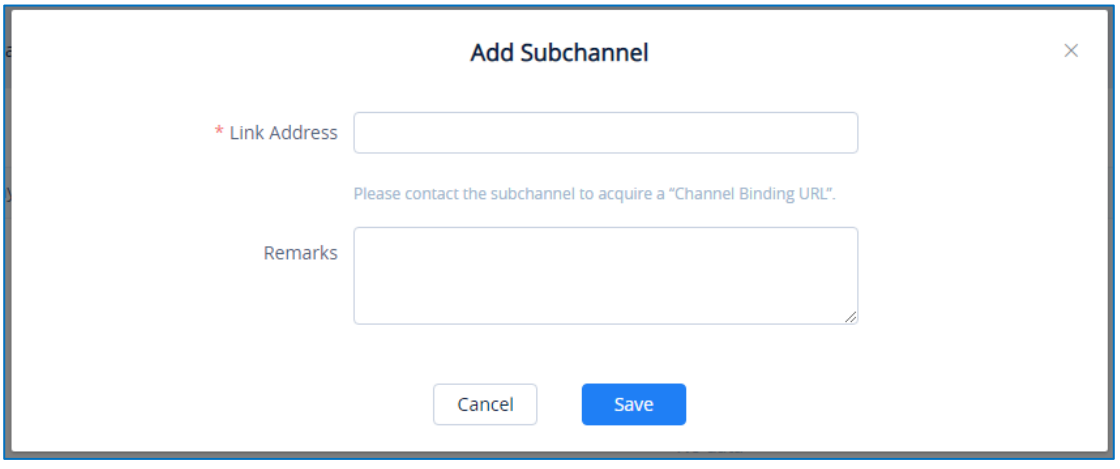


Figure 152: Link Address

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.

Notes:

- 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 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.

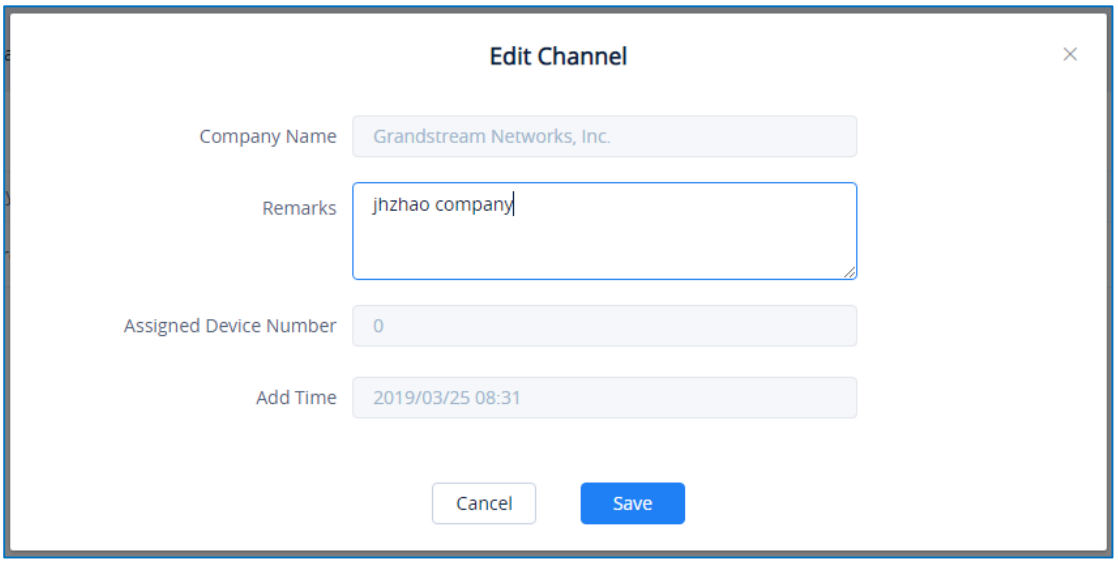


Figure 153: Add Remarks

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.

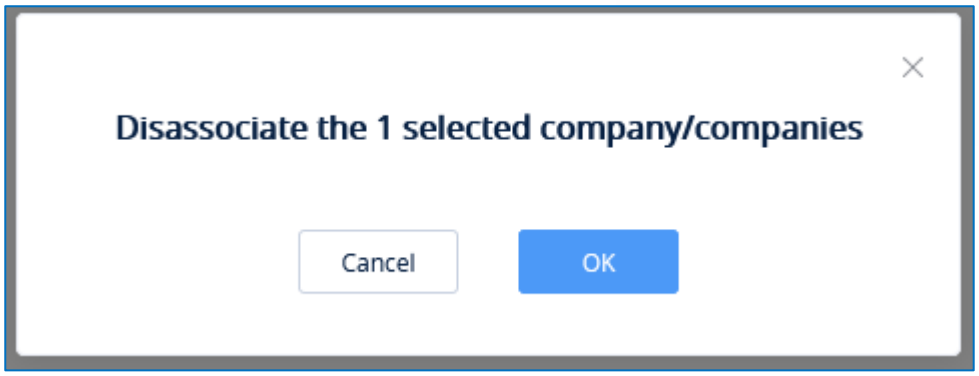


Figure 154: Disassociate Sub-channel

Track Device

View Device

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

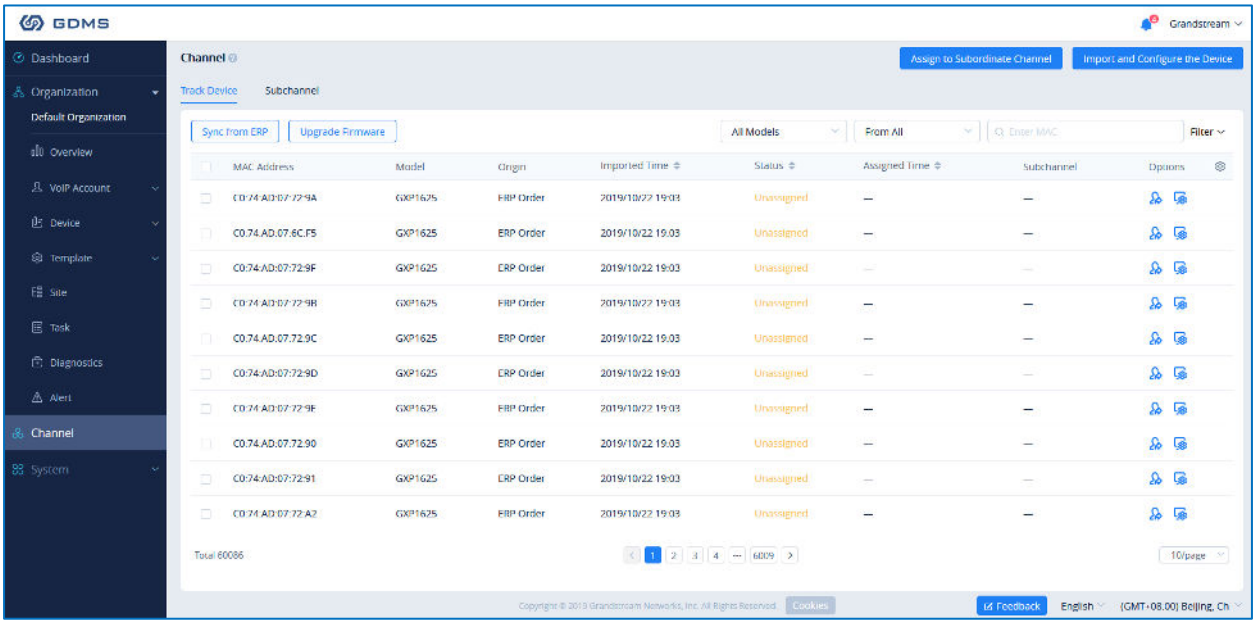


Figure 155: Track Device

Table 36: 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: • **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	**Allocated**: The device has been assigned to a sub-channel and cannot be assigned to other sub-channels. **Unallocated**: The device is not allocated to any sub-channel yet.
Outgoing Time	The date/time the device was assigned to a sub-channel. The company name of the sub-channel will also be displayed.

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

Note:

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 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:

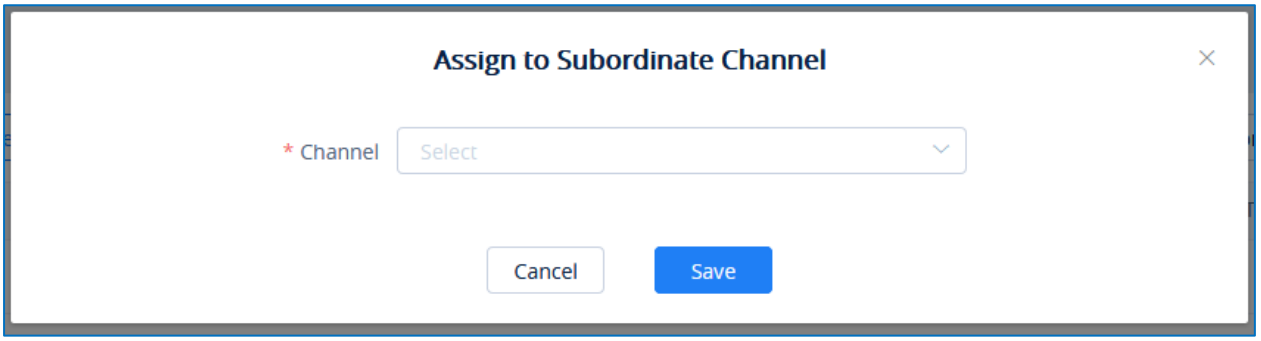


Figure 156: Assign Single Device to Subordinate Channel

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 **Track Device** page. The user will be redirected to the batch device assignment page.

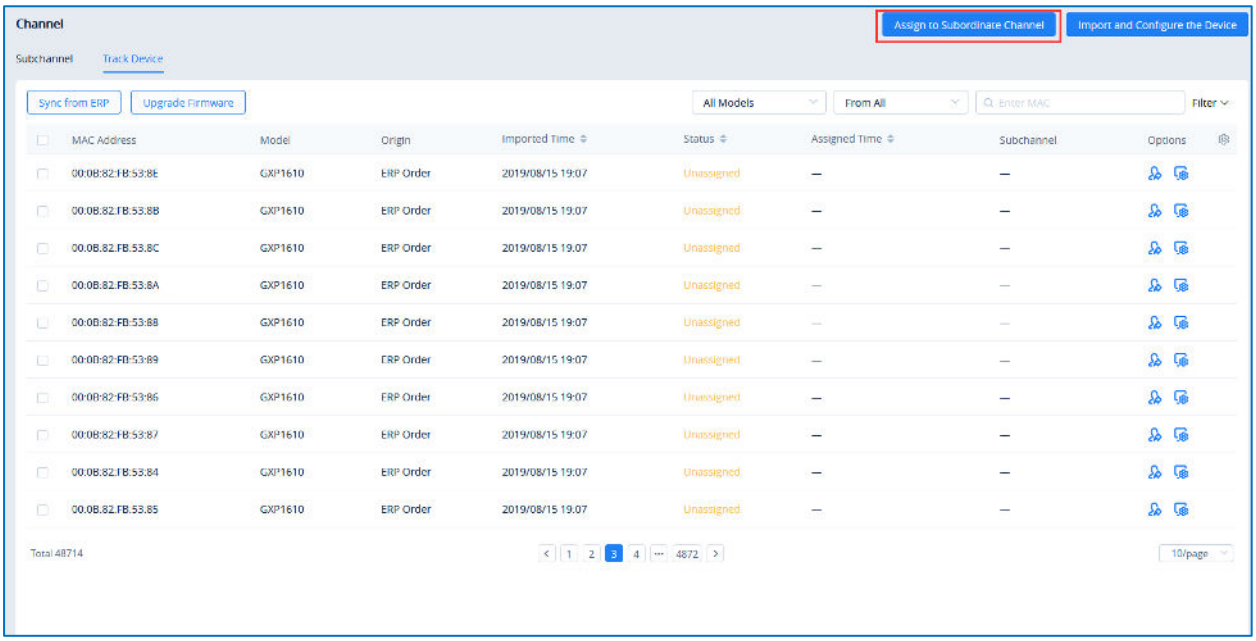


Figure 157: Device Operation Options

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

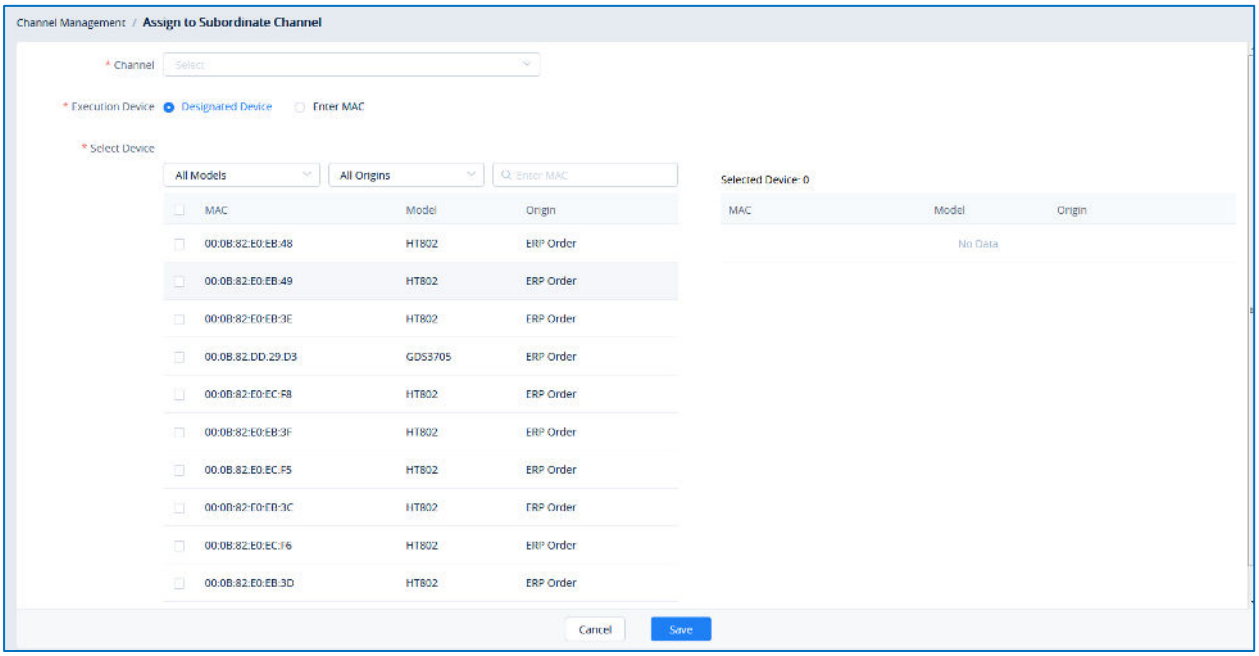


Figure 158: Assign Multiple Devices to Subordinate Channel

Table 37: Assign 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.

Figure 159: 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.

Notes:

- 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:

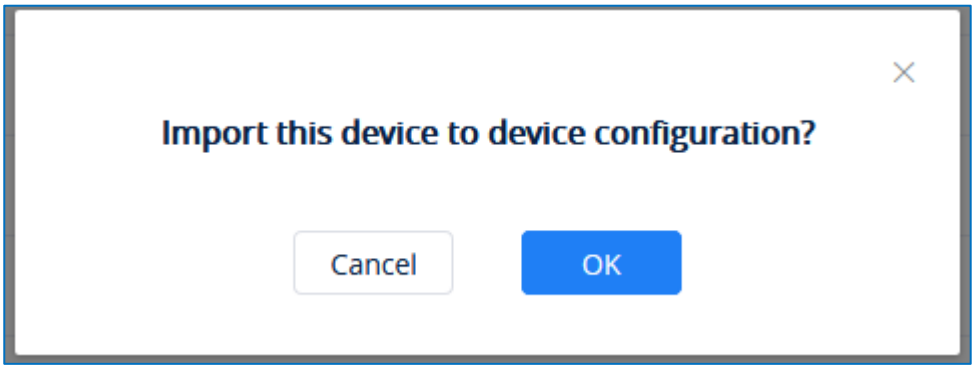


Figure 160: Import to Manage Device

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

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:

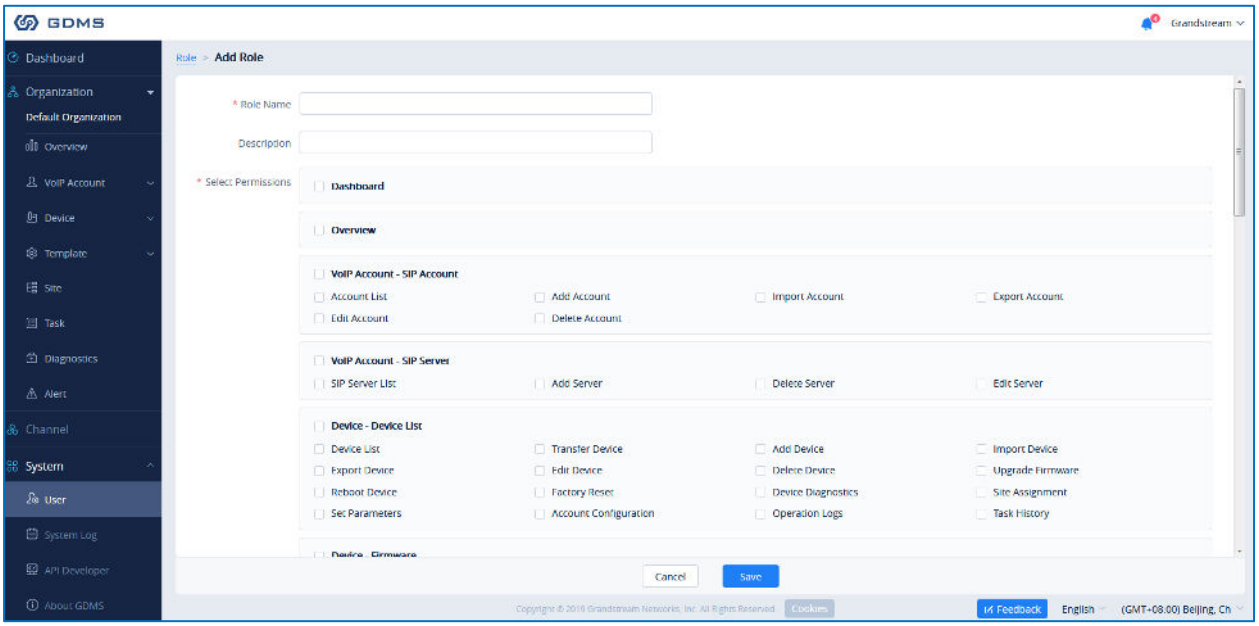


Figure 161: Add Role

Table 38: 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.

Note:

If a role does not have the privilege for a feature, 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.

Note:

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:

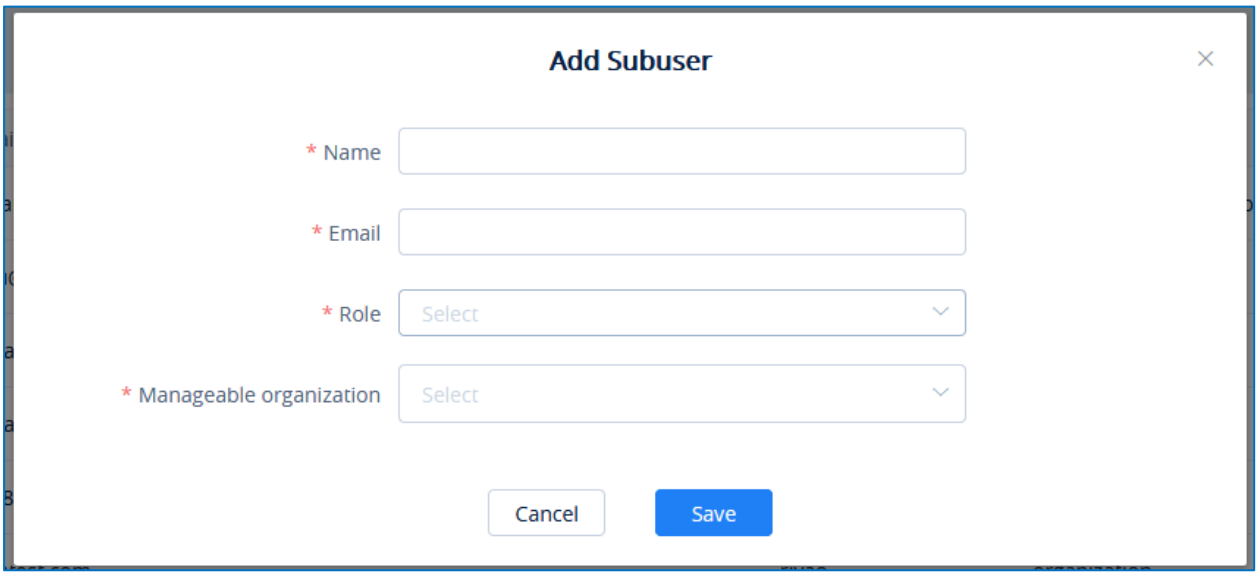


Figure 162: Add Sub-user

Table 39: 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.

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.

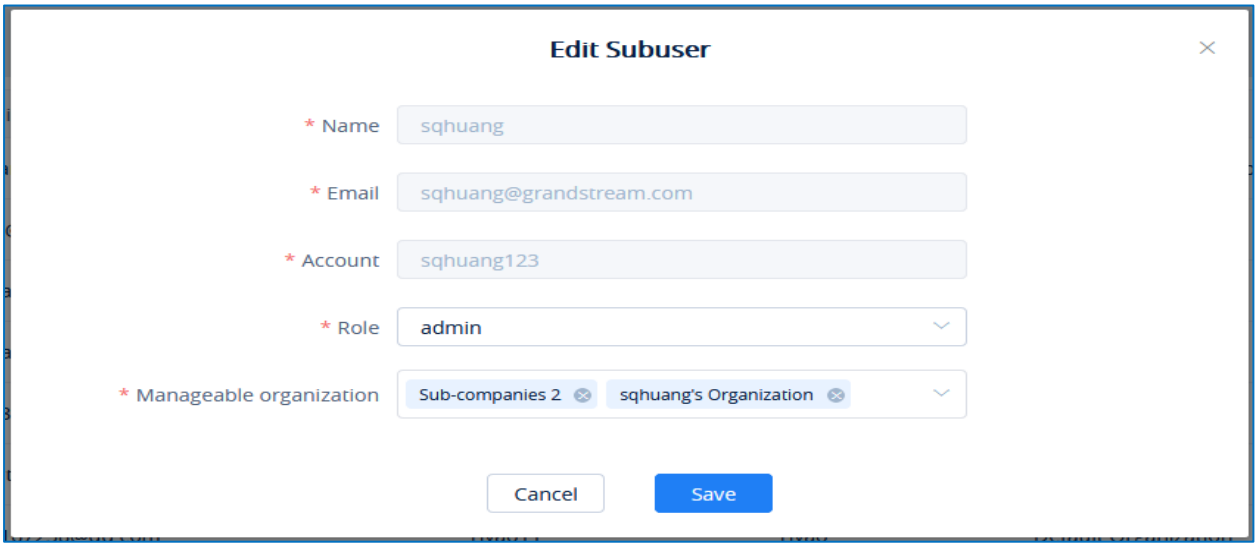


Figure 163: Edit Sub-user

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.

Figure 164: Edit Unverified Sub-user

Delete User

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

Personal Information

Users can view and edit their personal information on GDMS by clicking on their name in the top-right corner of the GDMS portal and clicking on **Personal Information**.

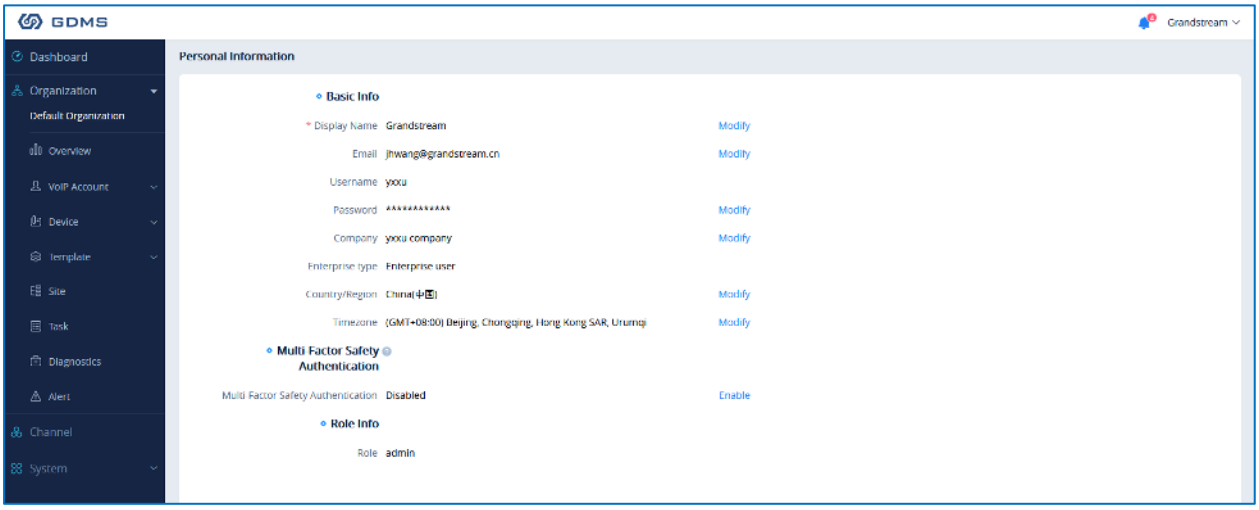


Figure 165: Personal Information

Table 40: Personal Information

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 cannot be modified.
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.
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 click **Sign Out**.

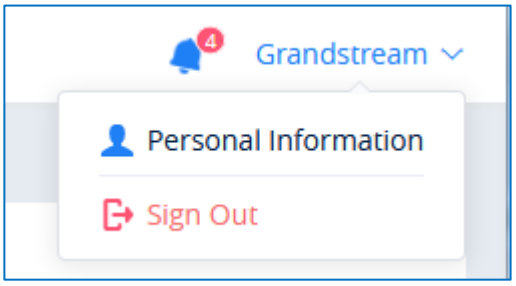


Figure 166: Sign Out

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.

Note:

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

1. Click "**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 "**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.

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 the permission.

All devices and data are in "**Default**" organization by default.

Multiple organizations and administrators:

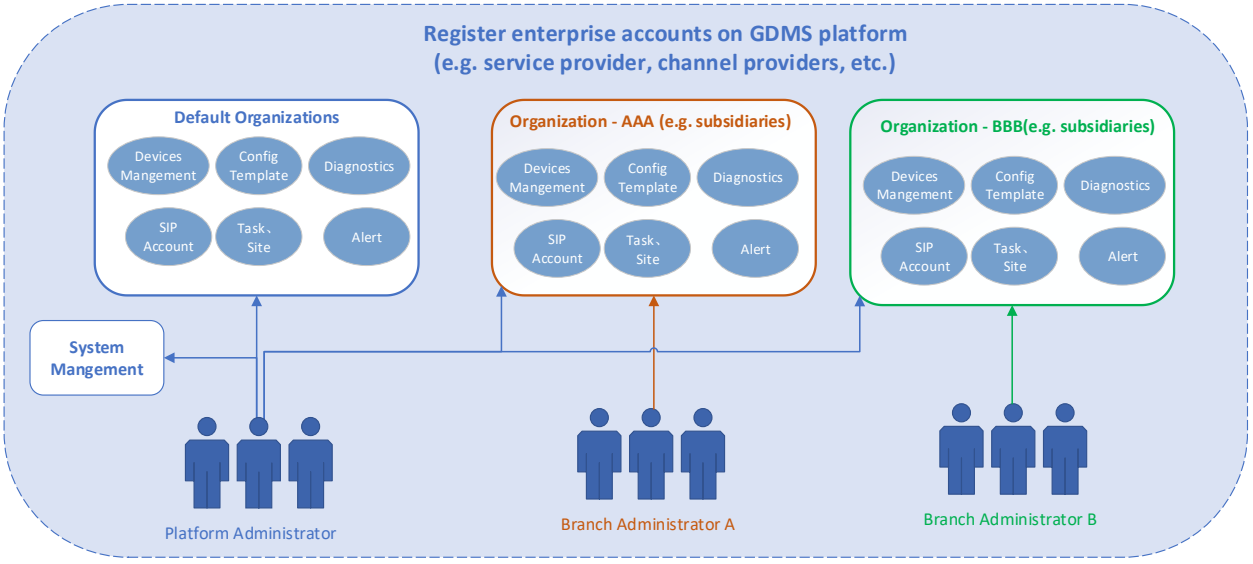


Figure 167: Multiple Organizations and Administrators

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.

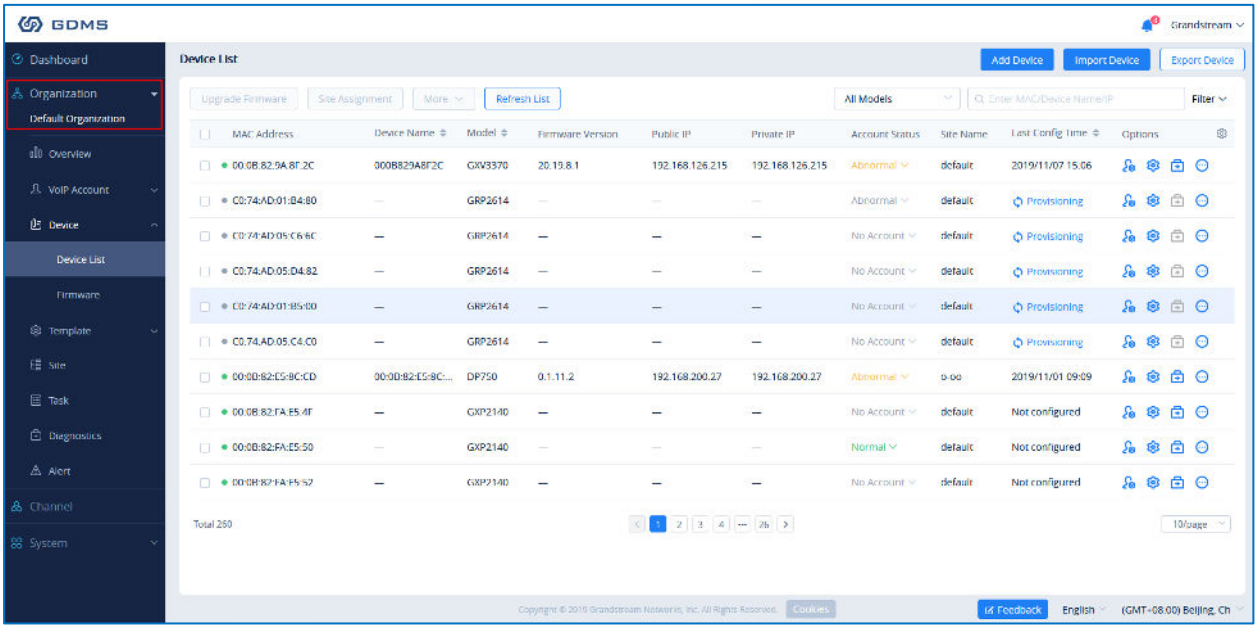


Figure 168: Switch Organization

Add Organization

The user could create an organization if the user has the 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:

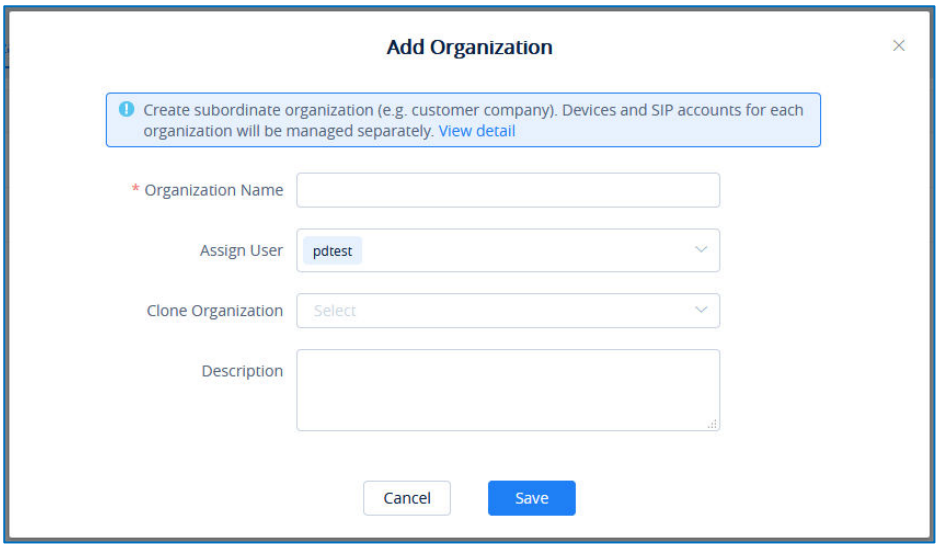


Figure 169: Add Organization

Table 41: Add Organization

Organization Name	Input the name of the organization.
Assign User	Select the users who will have the 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.
Description	Input the detailed descriptions of the organization.

3. Click Save button to save the organization in GDMS platform.

4. The system will switch to the new created organization by default, and the user could add devices to the new 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 to the editing page. The user could edit the organization name, the administrator of the organization, and descriptions, as the figure shows below:

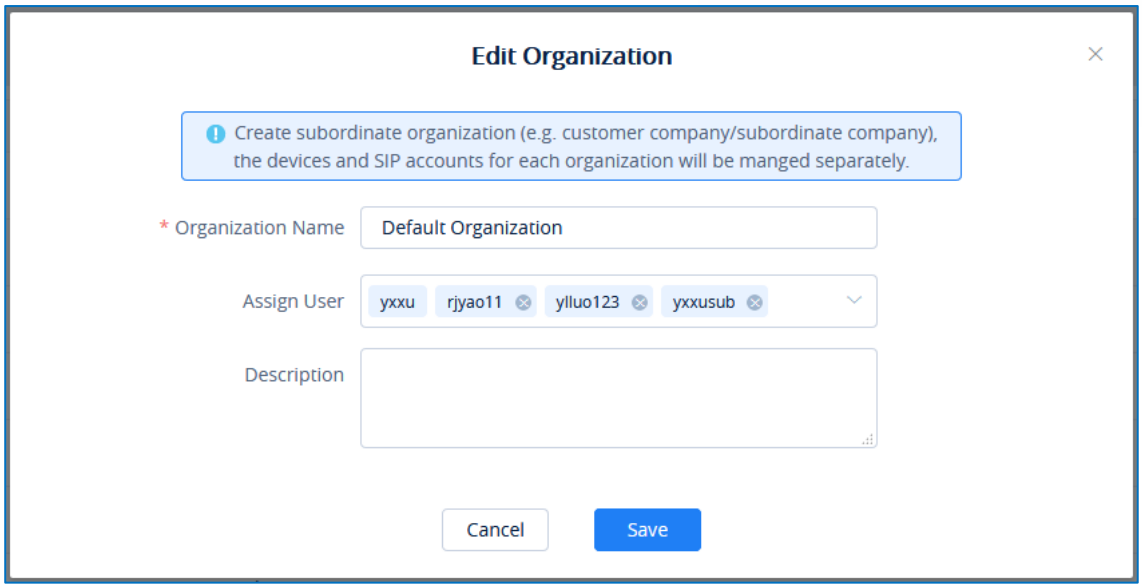


Figure 170: Edit Organization

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.

Note:

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

On 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.

Note:

Users could only view the system logs for the last 30 days.

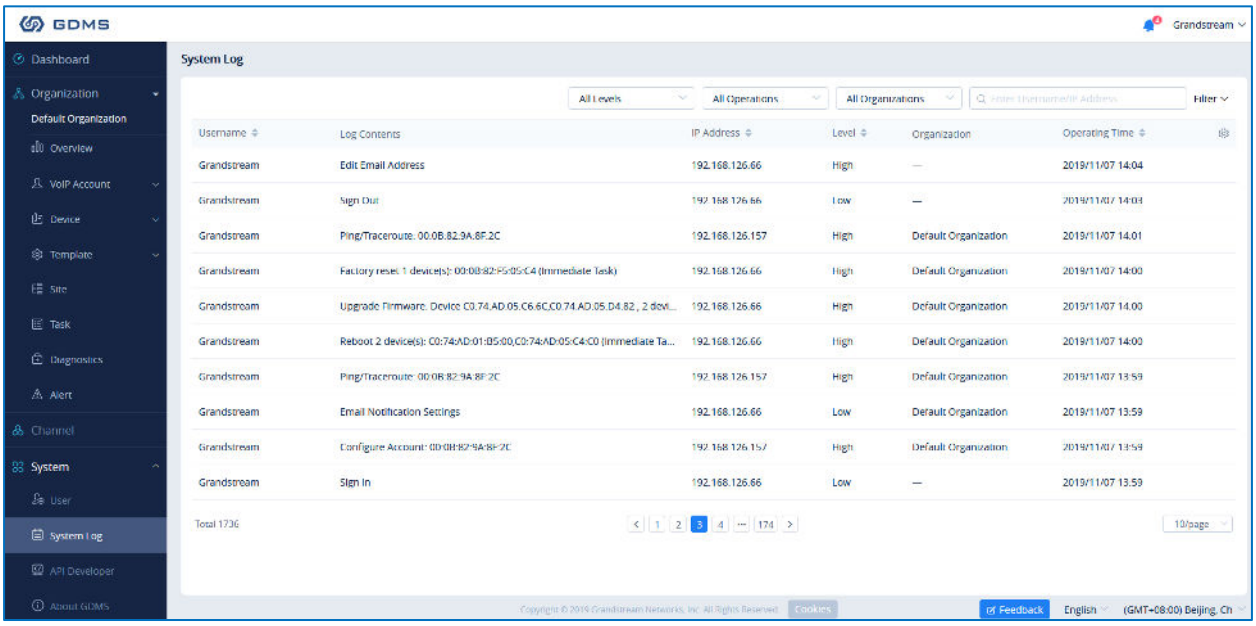
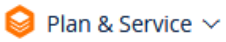


Figure 171: System Log

VALUE-ADDED SERVICES

Users can click on the button 

on the top right corner to view the value-added services provided by GDMS platform. The following two value-added services are available in GDMS platform:

UCM Remote Connect Plan

- Supports only for UCM63xx. When users add the UCM63xx device to GDMS platform, users will obtain the free trial plan.
- Complete NAT penetration mechanism. Users can use it directly without complicated configuration, so that it can ensure the remote communication requirements through external network (including GS Wave application in mobile phones/desktop clients for registration / communication through external network).
- **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.

Cloud Storage Space Plan

- The plan is used to store user profiles such as ringtones, language packs, firmware, and other resource files.
- As an additional plan of UCM device, this is used to expand the cloud storage space of UCM device, to backup configuration files and user data.

Note:

1. Users can check the plan details and price on official website.
2. Please refer to UCM63xx User Guide on official website for details about: Using remote call function on UCM/GS Wave application, backup files to GDMS cloud storage space, restoring backup files, and viewing the details of remote call records.

UCM CloudIM Plan

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.

Note:

1. Currently, users can only apply for trial plan. Each enterprise account can only apply for one UCM CloudIM plan.

2. After enabling 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.

3. 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.

4. If the UCM CloudIM plan expires, the Wave users cannot log in to the account. The chat data will also be deleted. Please renew the UCM CloudIM plan in time.

Trial Plan

1. Click on **Plan & Service** → **Services** interface on the right upper corner to access to **Services** interface.

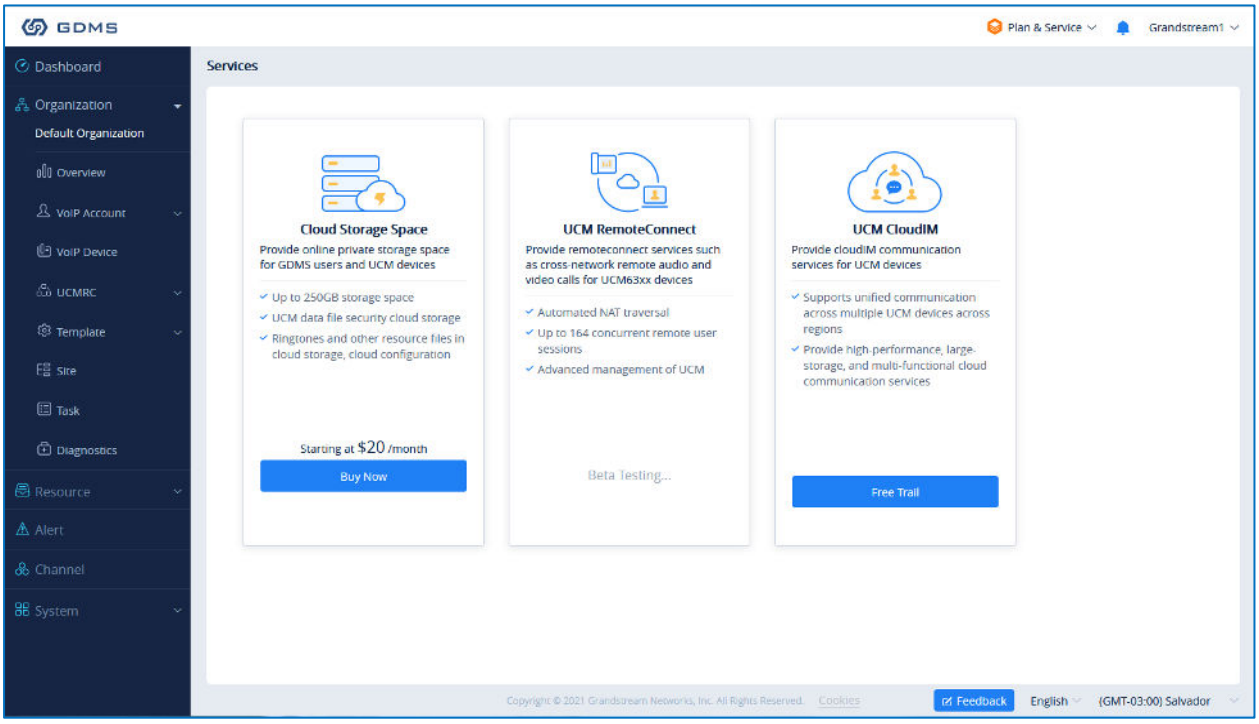


Figure 172: Services List Interface

2. Click "**Free Trial**" button at the bottom of "**UCM CloudIM**" service, select the CloudIM service region and enter the enterprise name for the plan. Please see the screenshot below:

   Note:

   It is recommended to select the nearest region to the UCM device.

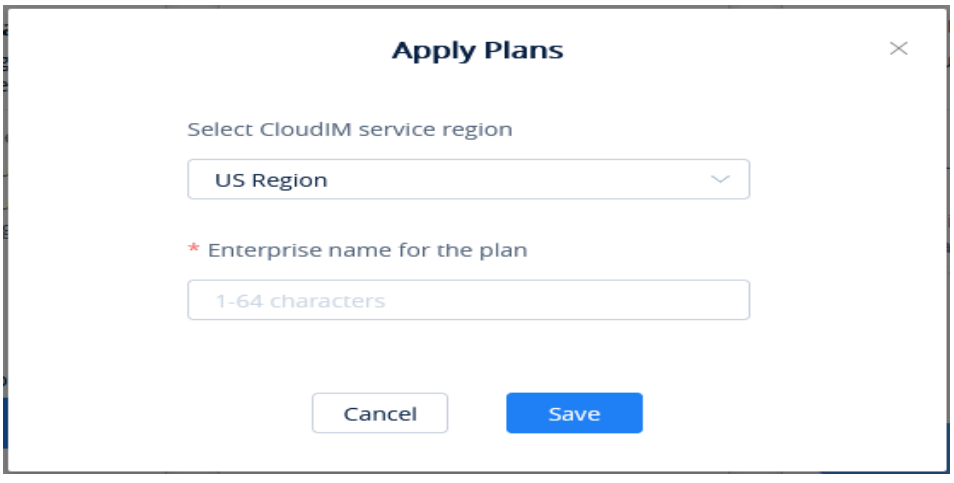


Figure 173: Apply Plans

3. Click "**Save**" button to get the UCM CloudIM plan, and the user can view CloudIM service domain name, service ID and Key.

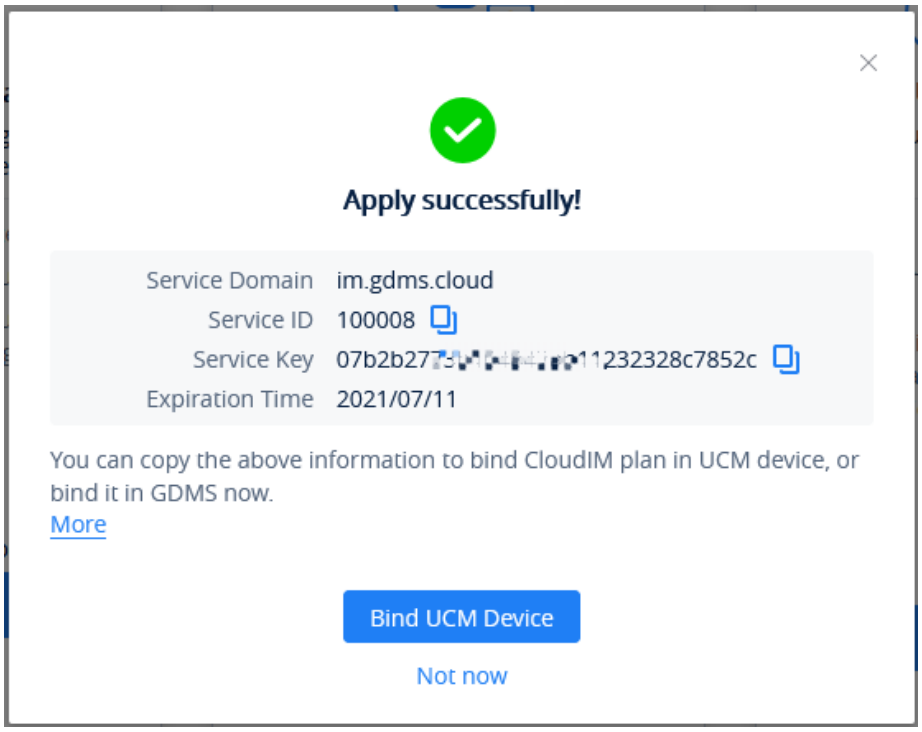


Figure 174: Finish Applying UCM CloudIM Plan

4. The user can quickly bind the UCM device for the UCM CloudIM plan so that the UCM device can quickly enable the UCM CloudIM plan.

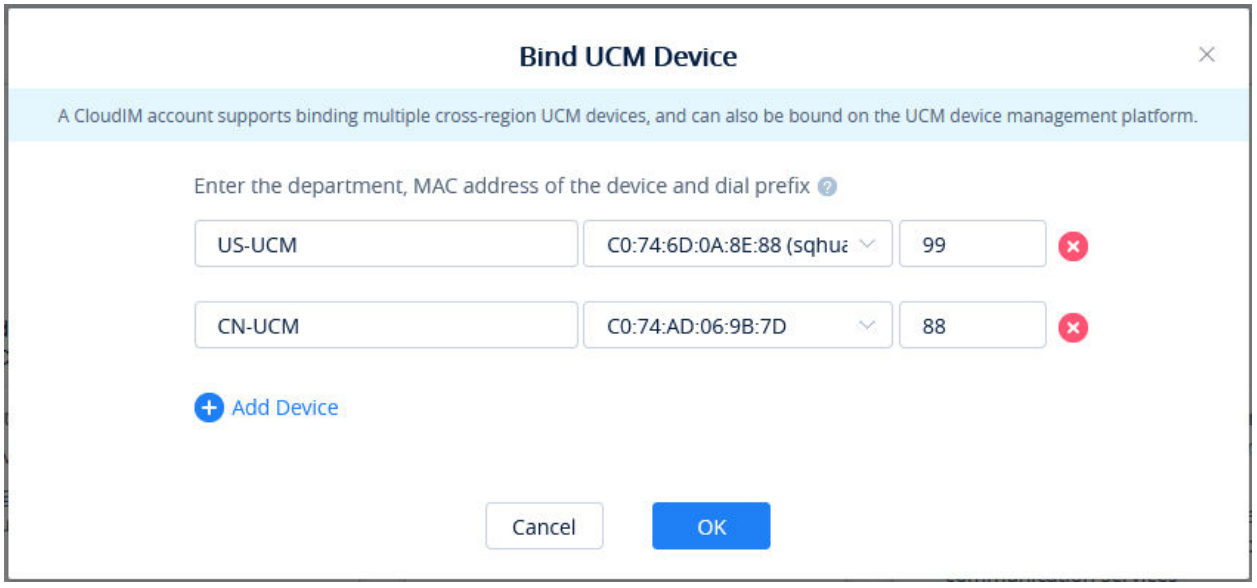


Figure 175: Bind UCM Device

Note:

The user can also copy the service ID and service key and bind the UCM device in the UCM device management platform. The user can go to **UCM Web UI → System Settings → CloudIM** interface and enter the CloudIM involved information in the blanks. The corresponding IM data are placed in the CloudIM external server.

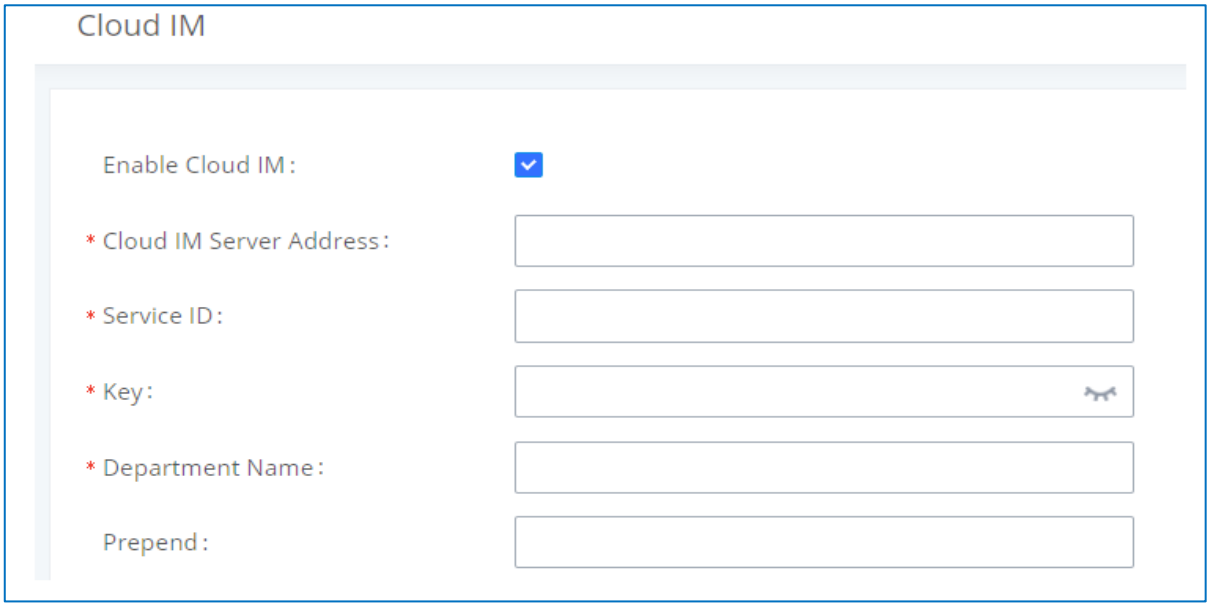


Figure 176: Bind UCM Device on Web UI

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.

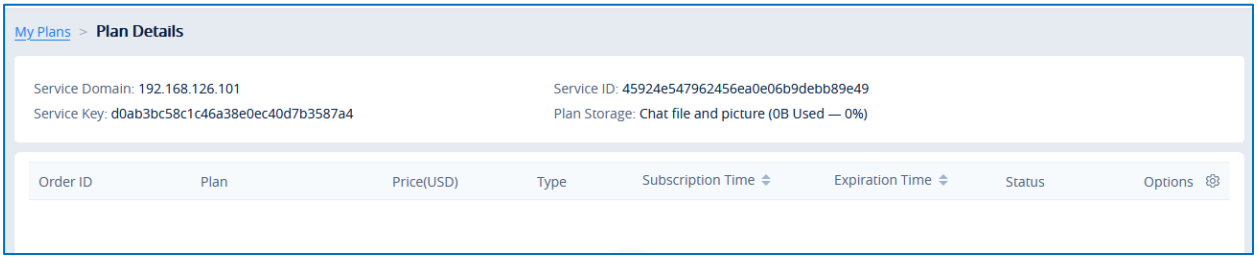


Figure 177: View Service ID and Key

Note:

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 .

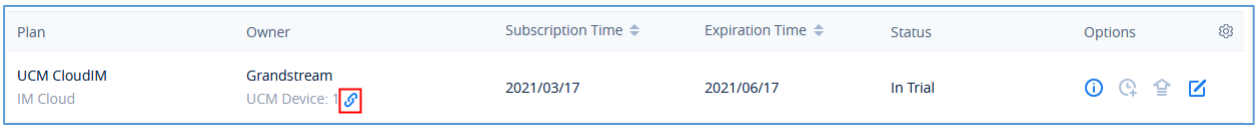


Figure 178: Find UCM CloudIM Plan

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:

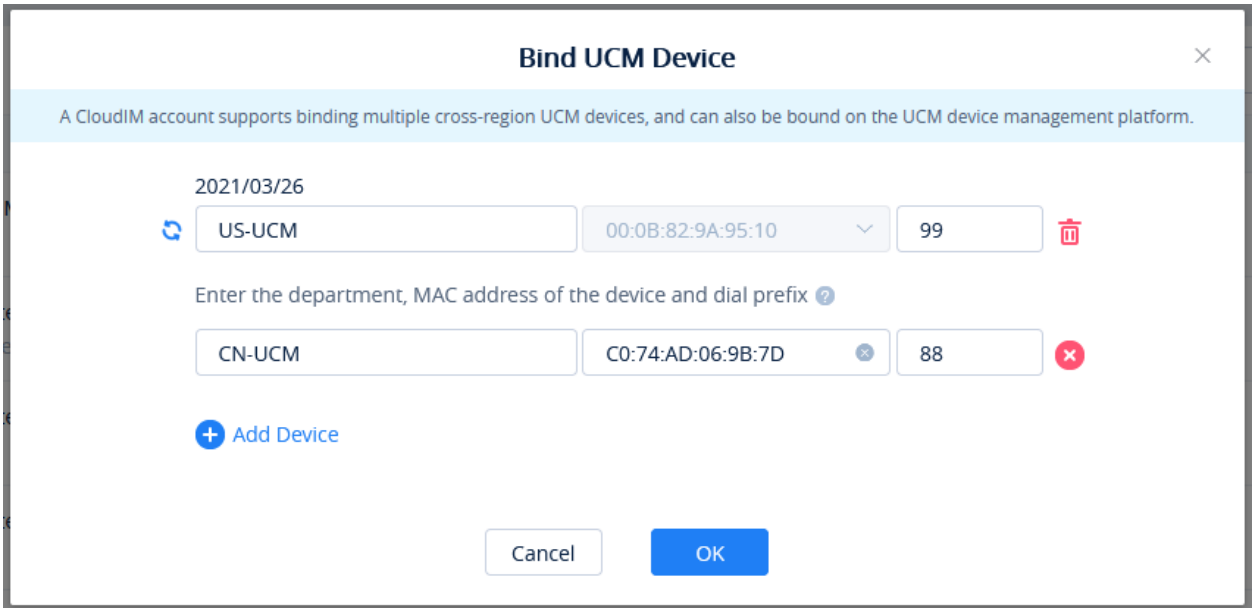


Figure 179: View Bound UCM Devices

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	Enter the MAC address of the UCM that uses the UCM CloudIM plan. It only supports the UCM devices which have been associated to the GDMS platform. **Note:** For the UCM devices which have been associated to the GDMS platform, the user can only log in to the UCM management platform to configure the CloudIM services.

Dial Prefix	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. 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.

Note:

If the user adds/deletes/edits department name, 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 .

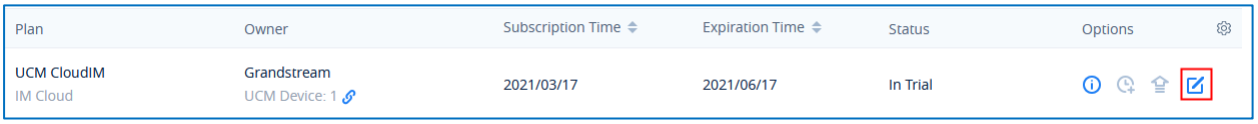


Figure 180: Find UCM CloudIM Plan

2. The user can modify the name of the enterprise, and the new name will be applied immediately.

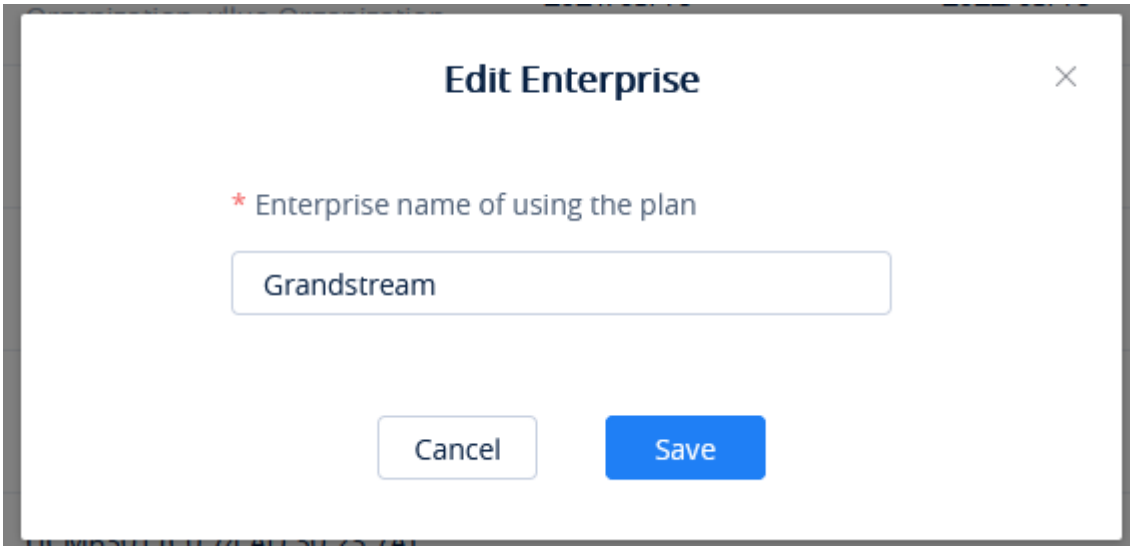


Figure 181: Edit Enterprise

Note:

Currently, the enterprise name is only used to remark the UCM CloudIM plan, and it will not be displayed elsewhere.

Purchase Service

Purchase UCM Remote Connect Plan（Pending）

Users can purchase one or more UCM Remote Connect plans and assign them to the corresponding UCM63xx devices.

Prerequisites: Users need to have a PayPal account before purchasing plans.

1. Click on **Plan & Service → Services** interface on the right upper corner to access to **Services** interface.

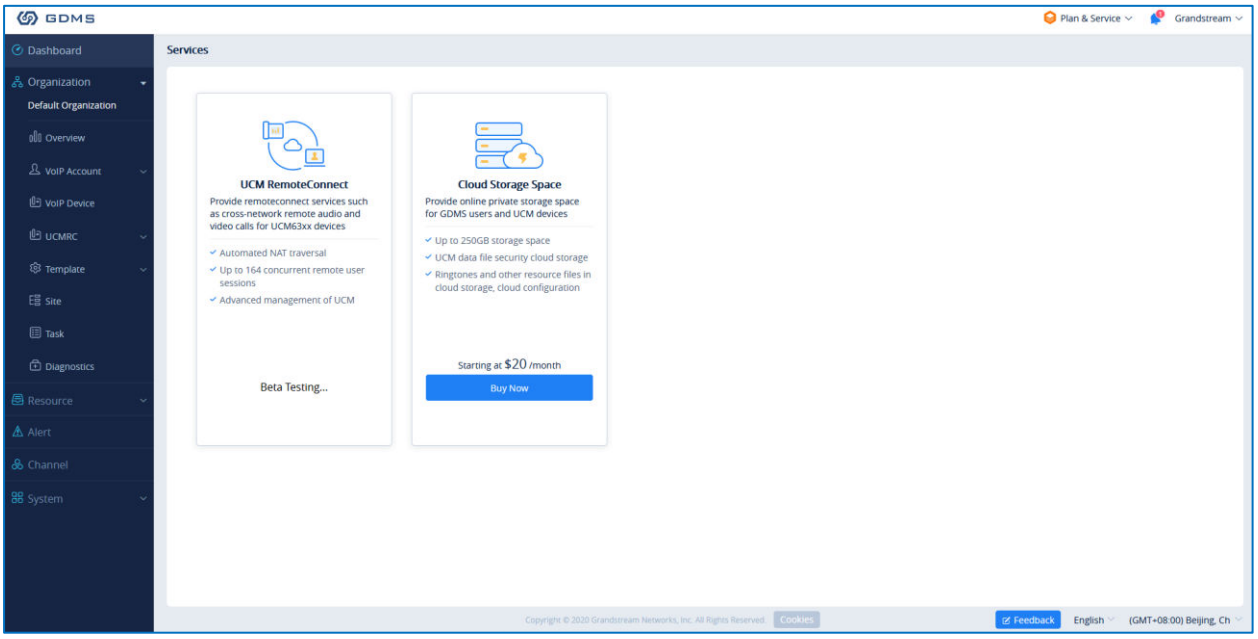
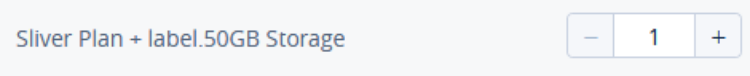


Figure 182: Services Interface

2. Select **UCM Remote Connect** plan and click on **Buy Now** button to purchase the plan. If the user never uses this plan in the UCM63xx device before, the user can click on "**Free trial for 3 months**" to get a free trial plan.

Table 42: Purchase Plan

Plan	(Required) Select the plan the user wants to purchase and click **More** button to view the plan details.

UCM Cloud Storage Add on Plan	(Optional)Purchase additional cloud storage space at the same time, the user can check this option and select the cloud storage space plan.
Billing Address	(Required) Fill in the user's actual address for invoice.
Amount	Please enter the number of the plans the user wants to purchase this time, the user can click "+" / "-" button to increase/decrease the amount, or directly enter the amount. 
Duration	Please select the duration of the plan to be purchased, e.g. 1 year.

3. View the total amount of the purchase order, including taxes.
4. Click the **Pay** button to enter the PayPal payment page and confirm the payment.
5. Once the payment is proceeded successfully, the purchased plan will be assigned to the associated UCM device immediately.

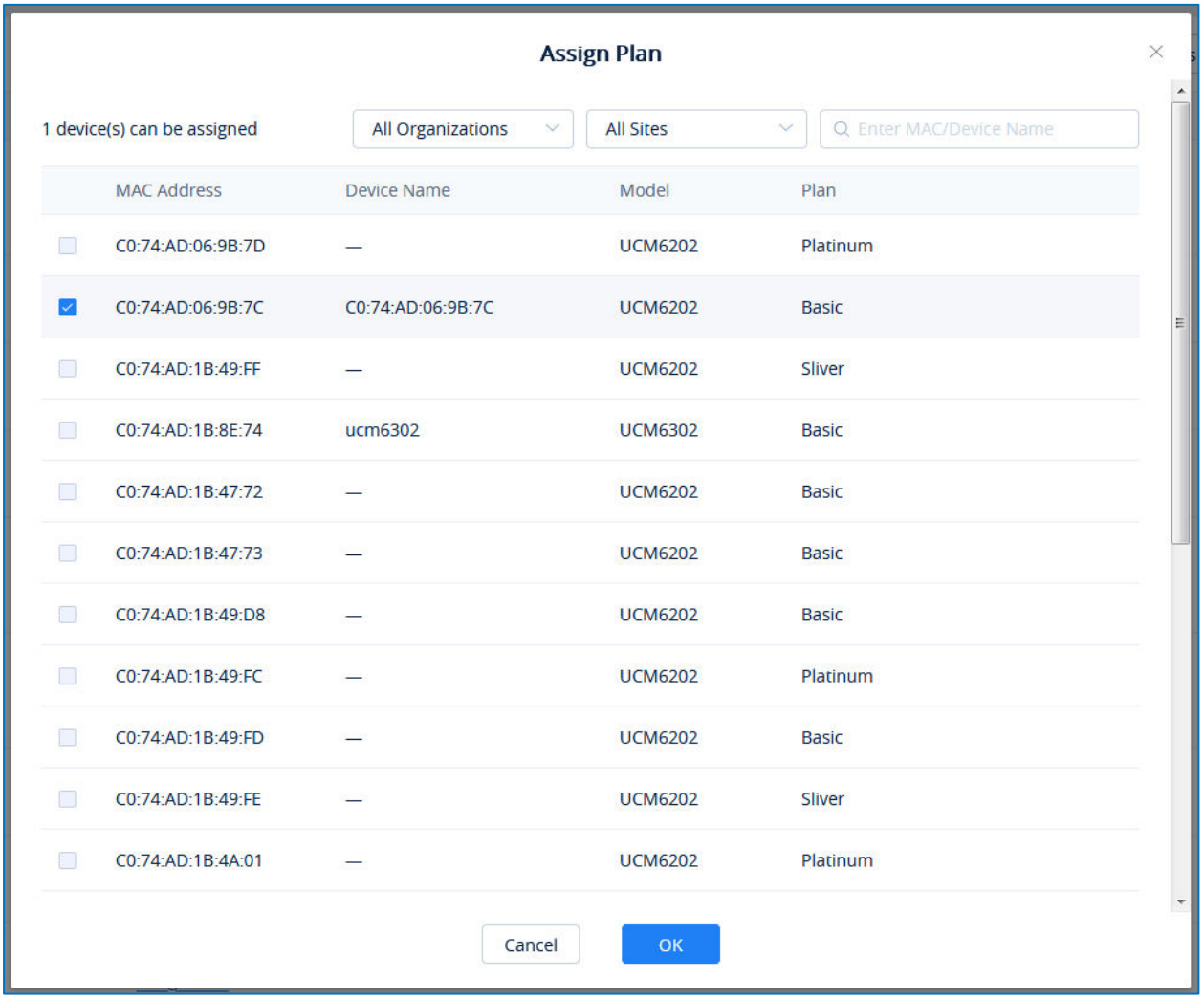


Figure 183: Assign Plan

6. When the user confirms to assign the plan to the UCM device, the user can view the purchased plan on **My Plans** interface, and view which device is using the purchased plan.

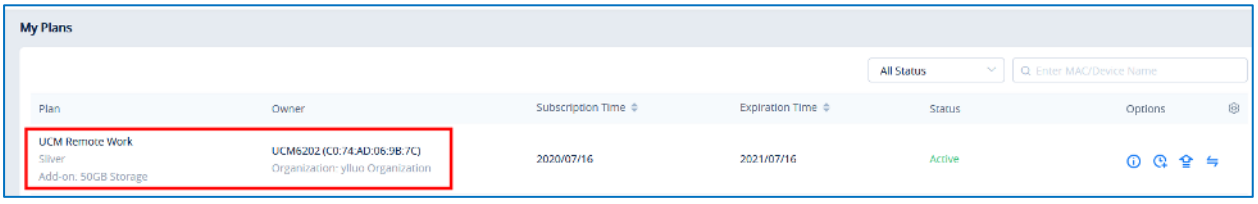


Figure 184: View Purchased Plan

Note:

Grandstream will review the order and contact the user if there is any problem. If the purchasing operation is failed, the user will receive an email.

Purchase UCM Cloud Storage Add-on Plan（Pending）

Prerequisites: The UCM device already has a paid UCM Remote Connect plan.

1. Go to **Plan & Service → Services** interface, select the **UCM Cloud Storage Add-on Plan** by clicking on **Buy Now → UCM Cloud Storage Add-on Plan**.

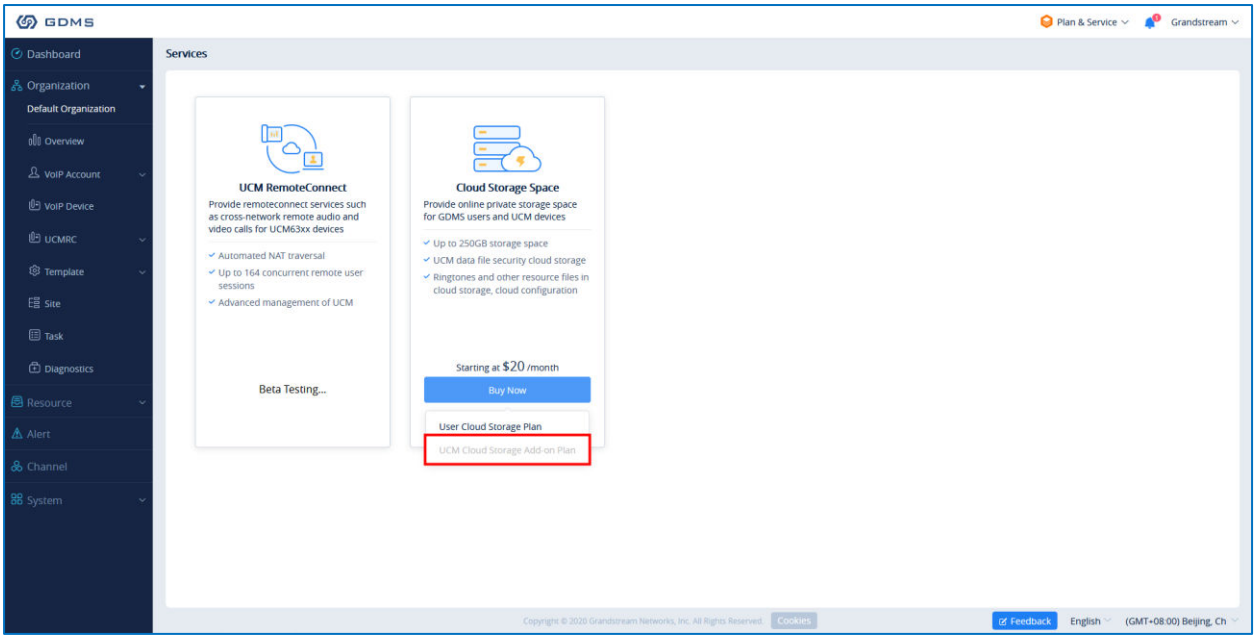


Figure 185: UCM Cloud Storage Add-on Plan

2. Select the UCM plan which the user wants to add the **UCM Cloud Storage Add-on Plan**.
3. Enter the plan purchase page and pay for the **UCM Cloud Storage Add-on Plan**.
4. When the payment is proceeded successfully, the user can view the **UCM Cloud Storage Add-on Plan** on **My Plans** interface.

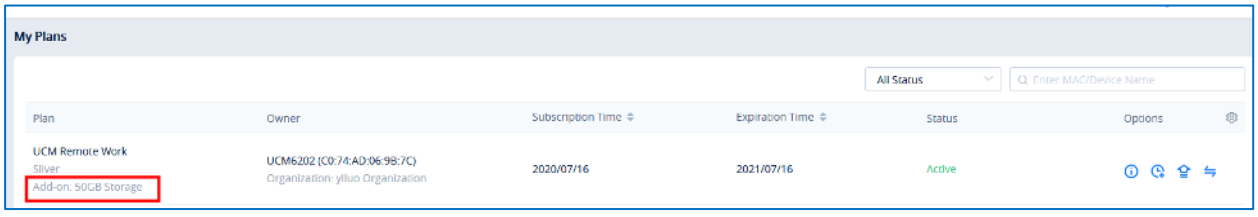


Figure 186: View Purchased UCM Cloud Storage Add-on Plan

Note:

Total Payment = the price of Cloud Storage Space plan * the remaining period of UCM Remote Connect plan. The purchased UCM Cloud Storage Add-on plan's expiration date must be the same as the UCM

Remote Connect plan.

Purchase User Cloud Storage Plan

User Cloud Storage space is the cloud storage space used by all the current enterprise users. It is mainly used to store resources files such as custom firmware, ringtones, language packs, etc.

Prerequisites: The enterprise account has not purchased any user cloud storage plans. If purchased, the administrator can renew or upgrade the current user cloud storage plan.

1. Go to **Plan & Service → Services** interface, select the **User Cloud Storage Plan** by clicking on **Buy Now → User Cloud Storage Plan**.

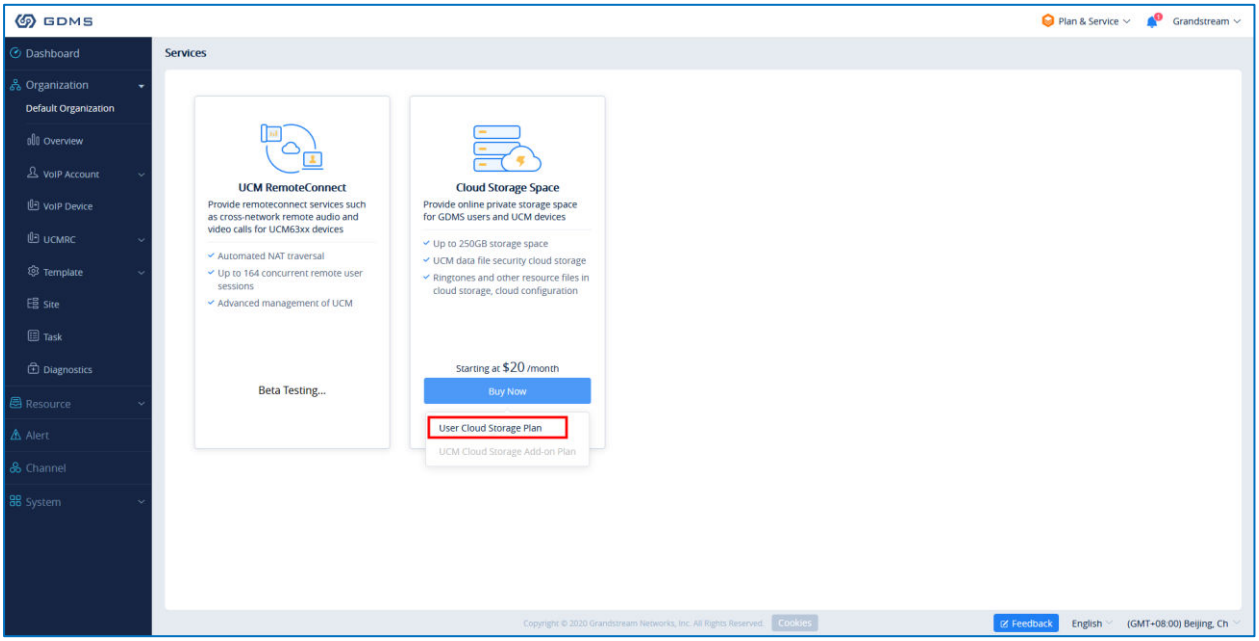


Figure 187: User Cloud Storage Plan

2. Enter the plan purchase page and pay for the **User Cloud Storage Plan**.
3. When the payment is proceeded successfully, the user can view this plan in **My Plans** interface. The user can also view the current usage on the **Resource → Storage Space** interface.

View My Plans

Click on the **Plan & Service → My Plans** on the upper right corner to access **My Plans** interface. This page displays all purchased plans by the current enterprise.

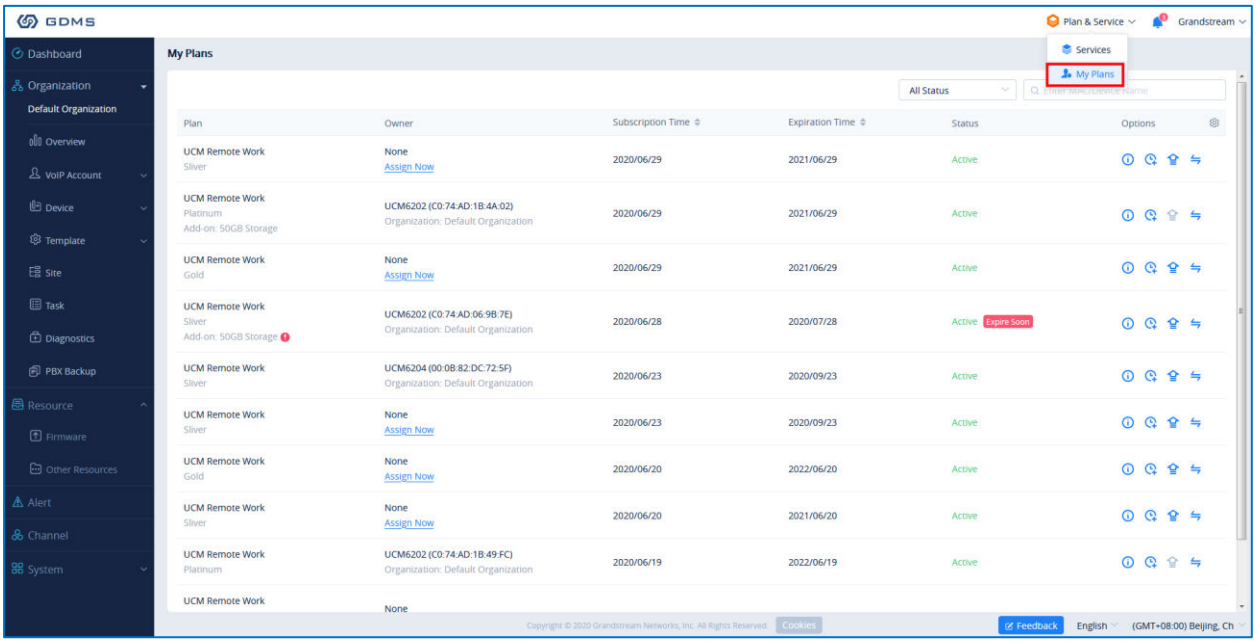


Figure 188: View My Plans

View all plans on the Plans menu. There are total three types of status:

- 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)

Note:

1. If the user can see icon , it means the UCM Cloud Storage Add-on Plan will expire soon. If the UCM Cloud Storage Add-on Plan has expired, this will not be displayed.

Figure 189: UCM Cloud Storage Add-on Plan Expiration

2. If the user can see 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 button to view all order history of this plan, including the additional plans.

- Users could check the order ID, purchase type (upgrade/renew/subscribe), current plans (including additional plans), total price, tax, and billing address.
- The user can view all the additional plans under the current plan, as well as the record of orders of the additional plans.
- If the payment status is "**pending"**, it means the payment is processed successfully, and the user could start to use the new plan. If the order cannot be processed, it will be regarded as "**Invalid**", and Grandstream team will contact the user.
- The user will receive an Email with the notification no matter the reviewing is successful or failed.

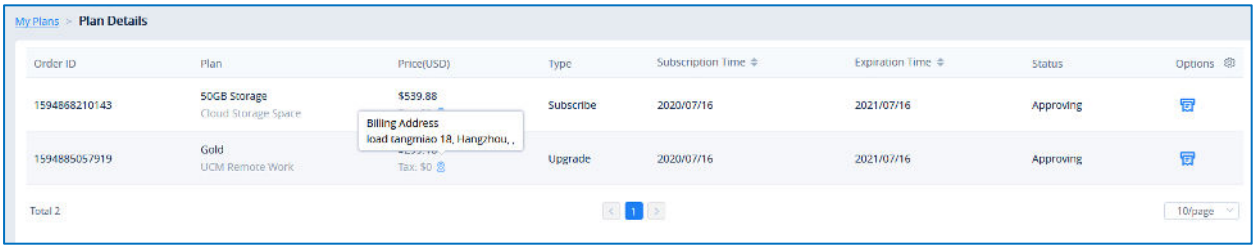


Figure 190: View Plan Details

Download Invoice

Users can download the invoices for all orders. If the purchasing behavior passes the verification, the user could download the invoice from IPVideoTalk Portal.

1. View all plans on the **My Plans** menu.

2. Select a specific plan, click icon to view all order history of the plan.

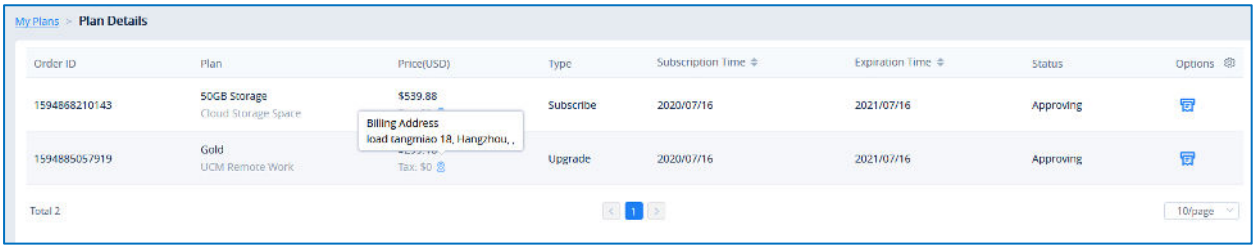


Figure 191: Download Invoice

3. Click button to download the invoice in PDF format.

Note:

- If the user purchases the plan from the distributor, please contact with the distributor to get the invoice.

Assign Plan to UCM

The user can assign the purchased UCM Remote Connect Plan to the specific UCM device.

1. On My Plans interface, select a specific plan and click on button or "**Assign Now**" option to assign the plan.

Figure 192: Assign Plan Options

Note:

If the plan has been assigned to the UCM device A, and the user assigns the plan to another UCM device B, the plan of UCM device A will be changed to Basic plan.

2. Select the device which the user wants to assign the plan to.

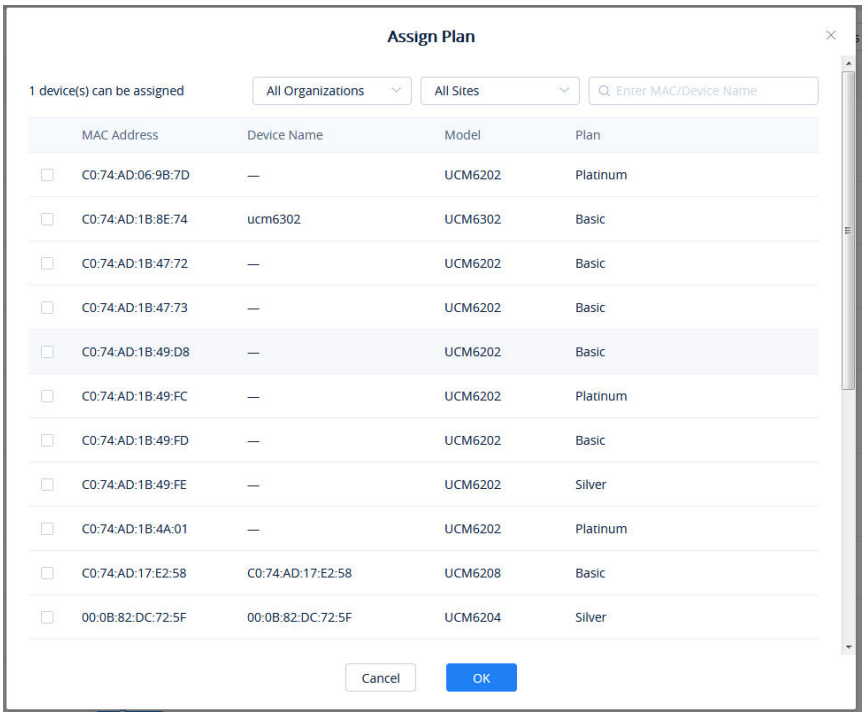


Figure 193: Assign Plan to UCM

Note:

If the user selects the UCM device which already has a plan, the plan of the UCM device will be updated to the new assigned plan, and the previous plan status will be "**Unassigned**".

3. Click "**OK**" button, the selected device can apply the selected plan immediately.

Note:

If the UCM device is not online, the plan cannot be applied on the UCM device until the UCM device is online.

Renew Plan

The user can renew the UCM Remote Connect Plan or Cloud Storage Space Plan at any time.

1. On **My Plans** interface, select a specific plan, click on button to access to the plan renewal interface.

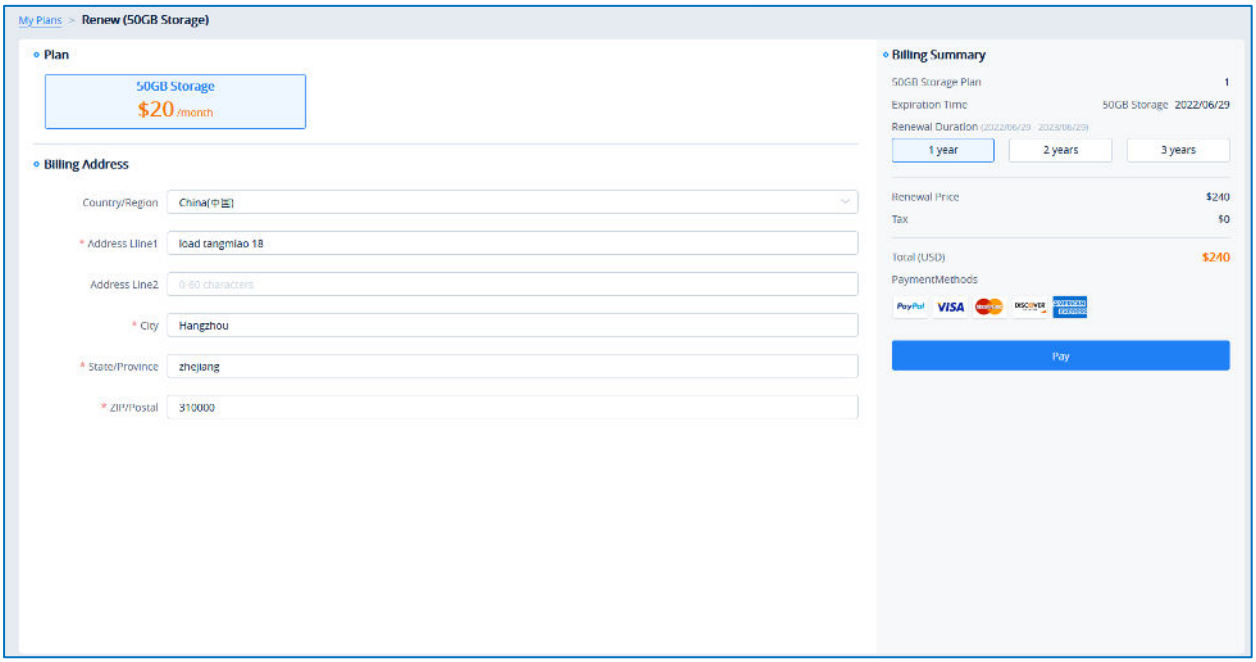


Figure 194: Renew Plan

2. On the plan renewal page, the user can only select to renew the current plan and the additional plan. The user can also select not to renew the additional storage plan at the same time.

3. Select the duration of the renewal, such as 1 year.

4. Fill in the billing address.

5. View the total amount of the purchase order, including taxes.

6. Click "**Pay**" button to enter the PayPal payment page and confirm the payment.

Notes:

- If the user wants to renew the **UCM Cloud Storage Add-on Plan**, the duration will be counted from current date to the expiration date of the UCM main plan.

- If the user wants to change plan, the user can click on button to upgrade plan.

- Grandstream will review the order and contact the user if there is any problem. If the purchasing operation is failed, the user will receive an email.

Upgrade Plan

The user can upgrade the UCM Remote Connect Plan or Cloud Storage Space Plan at any time.

1. On **My Plans** interface, select a specific plan, click on button to access plan upgrading interface.

If the UCM Remote Connect Plan has an additional Cloud Storage Space plan, the user can select to upgrade the specific plan.

2. Select the pre-upgraded plan on the purchase page. Users can only select the plan which is higher-level than the current plan.

3. When the user selects to upgrade the plan, the user can select to renew the plan at the same time and select the renewal duration.

4. If the current plan has expired, the user must check the option to renew the plan.

5. View the total amount of the purchase order, including taxes.

6. Click "**Pay**" button to enter the PayPal payment page and confirm the payment.

7. When the payment proceeded successfully, the upgraded plan will take effect immediately.

Notes:

Grandstream will review the order and contact the user if there is any problem. If the purchasing operation is failed, the user will receive an email.

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:

Figure 195: Plan Expiration Notice

Note:

- Once the plan expires, the files exceed the maximum storage space will be deleted after 7 days. Please download the files as soon as possible or renew in advance.
- Once the plan expires, if the user configures custom access server address for UCM device, the custom access server address will be deleted after 7 days.

MULTI-FACTOR AUTHENTICATION

GDMS Multi-Factor Authentication (MFA) is the simple and best security practice method that adds an 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 for 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 device 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 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 unsafe mobile device, it may not provide the same level of security as physical MFA device.

- **Physical MFA Device**

Physical MFA Device is a device can generate a six-digit code based on a one-time time-synchronized cryptographic algorithm.

When logging into 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

Table 43: 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 which supports open TOTP standards. It is recommended to use the devices from Microcosm manufacturer.
Function	Support multiple tokens on single device	The financial service institutions and IT enterprises use the same model of device.

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.

Table 44: Suitable Applications

Android	**Google Authenticator; Authy 2-Factor Authentication**
iPhone	**Google Authenticator; Authy**
Windows	**Authenticator**

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.

Enable Virtual MFA Device

Prerequisite: Users need to install virtual MFA application on the smartphone/tablet/PC before enabling 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:

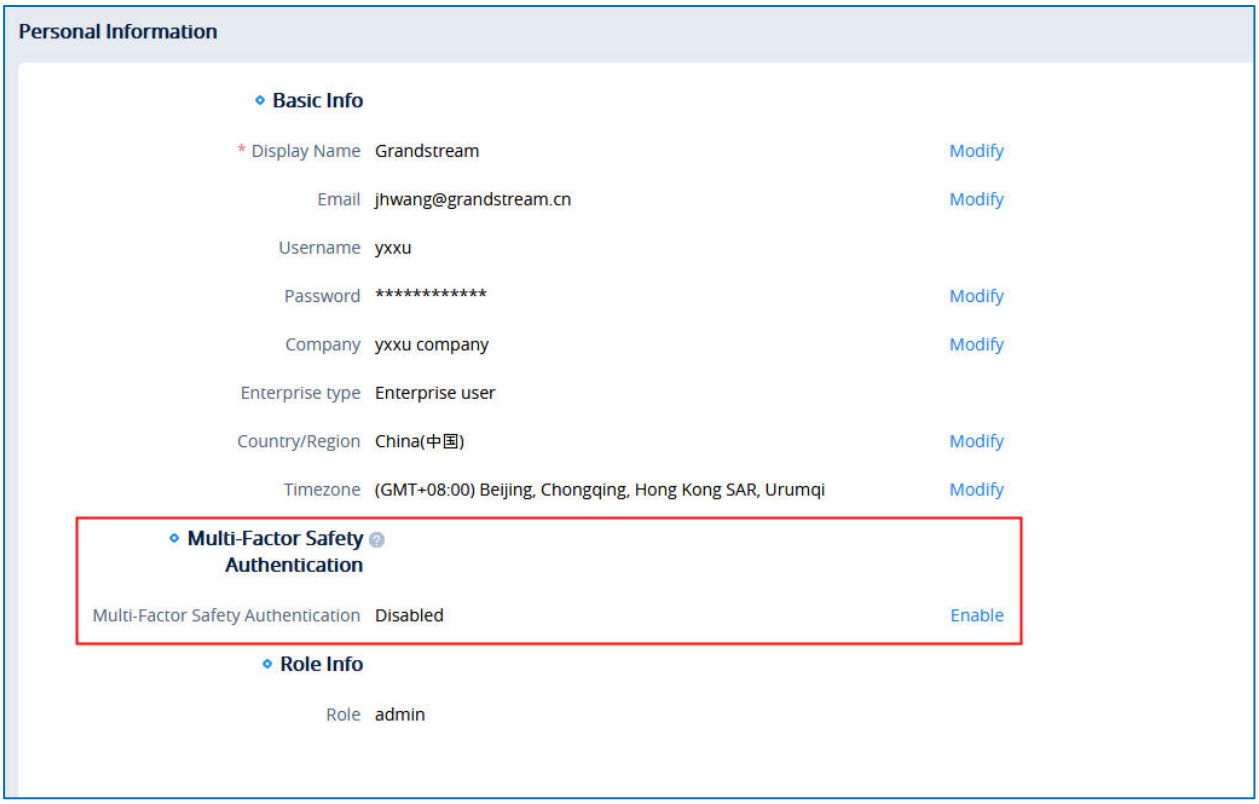


Figure 196: Access Personal Information Page

2. Click to enable "**Multi-Factor Safety Authentication**" option and select to use "**Virtual MFA Device**" on the pop-up window, then click "**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 virtual MFA device. Users can also input the secret key manually into the smartphone/tablet/PC in order to finish setting virtual MFA device if your smartphone/tablet/PC does not support to scan QR code.

Figure 197: Scan QR Code

4. Open virtual MFA application in your smartphone/tablet/PC, ensure that whether if the application in your smartphone/tablet/PC supports to scan QR code, and then perform one of the following actions below:

   a. If the MFA application in the smartphone/tablet/PC supports to scan 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.

   b. If the smartphone/tablet/PC does not support to scan QR code, the user can click on "**show secret key"** option and input the private secret key manually in the MFA application.

Note: 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.

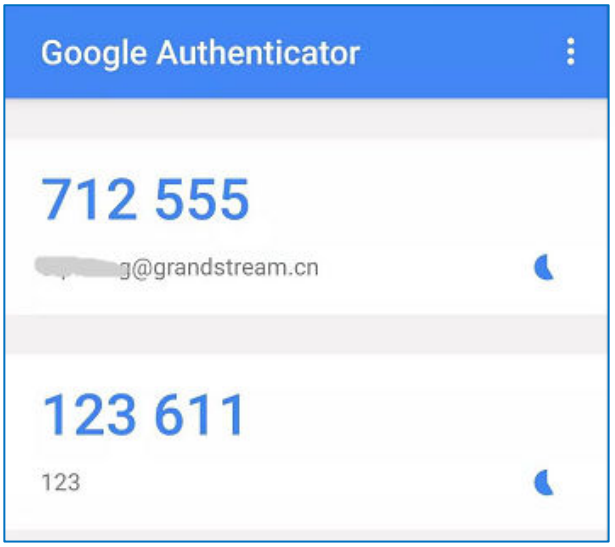


Figure 198: Input MFA Secret Code

6. Click on “Start Verification” option to start to verify the password. When the verification is pass, the GDMS account and the virtual MFA device has been bound successfully. When the user tries to log in the GDMS platform, the user must input the MFA device code.

Notes:

- 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 wait for 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.

Enable Physical MFA Device

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 “**Multi-Factor Safety Authentication**” option and select to use “**Physical MFA Device**” on the pop-up window, then click “**Next**” option to continue.
3. Enter the interface below to bind the physical MFA device with the GDMS account:

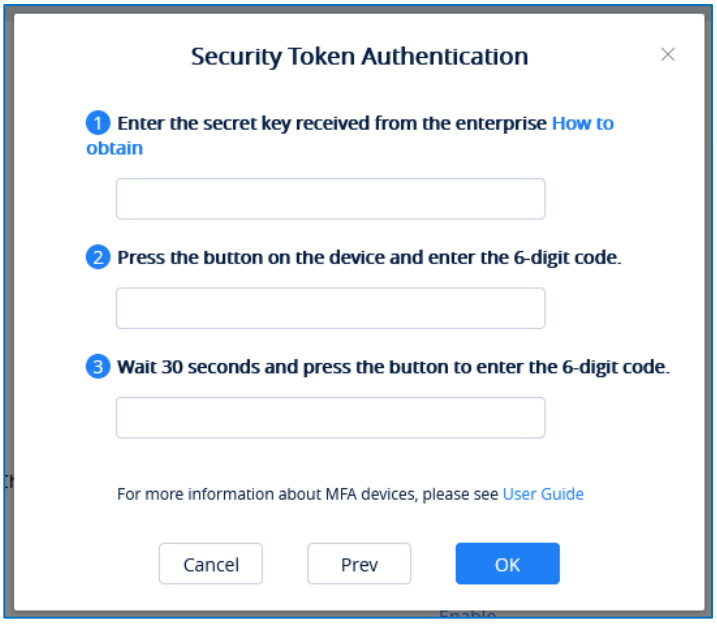


Figure 199: Hardware MFA Device Authentication

4. Input the secret key of the device. Please contact with the manufacturer for the secret key.

Note:

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.

Figure 200: Physical MFA Device

6. Click on “Start Verification” option to start to verify the password. When the verification is pass, the GDMS account and the physical MFA device has been bound successfully. When the user tries to log in the GDMS platform, the user must input the MFA device code.

Notes:

- 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 wait for 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.

Remove MFA Device

If the user does not need to proceed MFA verification, the user can remove the MFA device and restore 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 “**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 a 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.

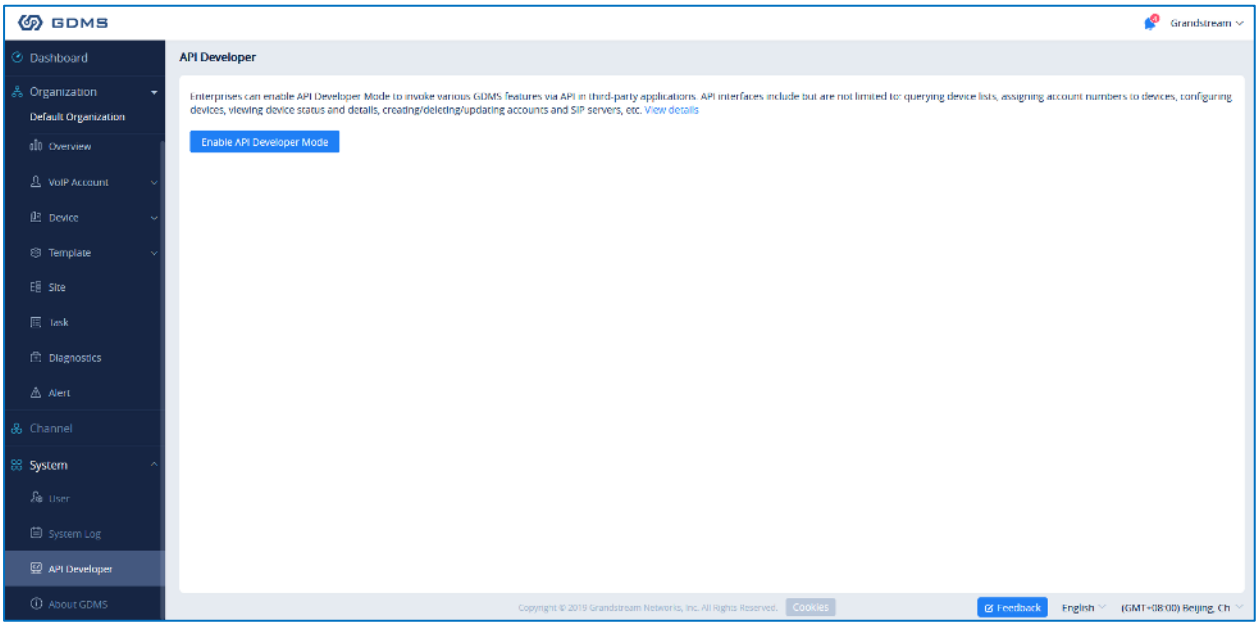


Figure 201: API Developer

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.

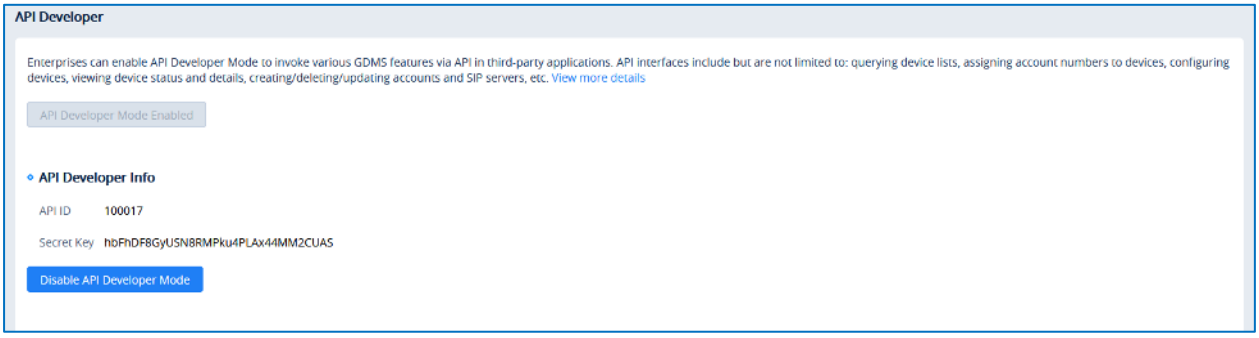


Figure 202: Apply for API Developer

3. If the user wants to disable 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 US region, the {gdms_domain} can be filled with www.gdms.cloud
- If your GDMS account is in 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 information, supported device models, and firmware requirements for device models by clicking on **System Management → About GDMS**.

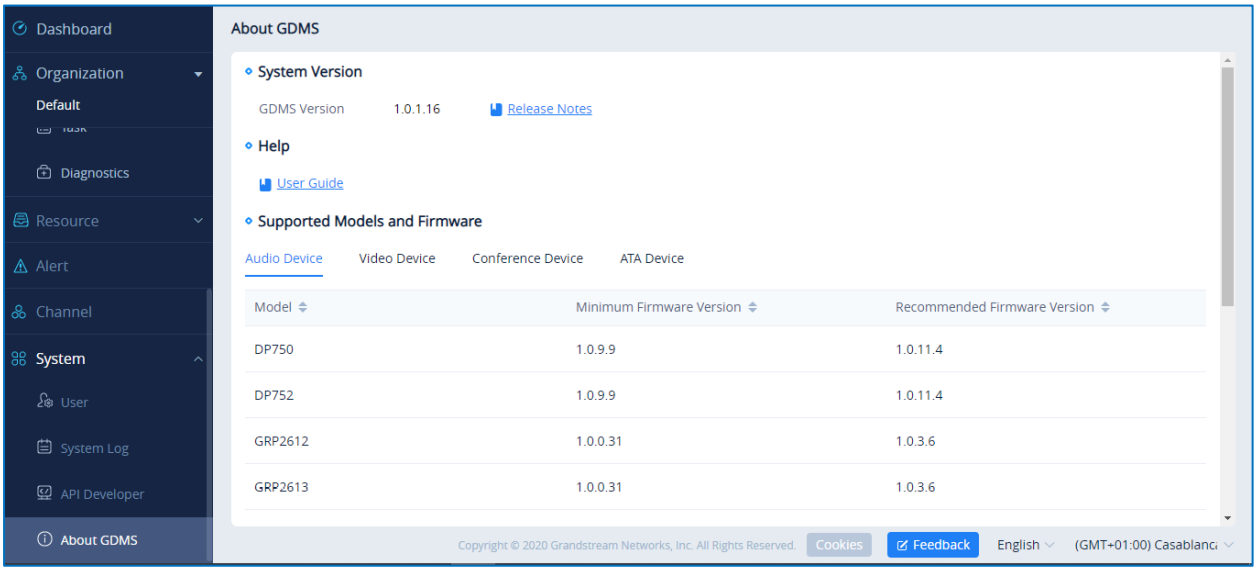


Figure 203: About GDMS

EXPERIENCING GDMS.CLOUD SYSTEM

Please visit our product website at https://www.grandstream.com for the latest release, features instructions, FAQs, latest documentations, and latest products information.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for using Grandstream GDMS system, it will be sure to bring convenience to both your business and personal life.