

Grandstream Networks, Inc.

Manage SoftwareUCM Services Through GDMS



INTRODUCTION

SoftwareUCM is an on-premises solution that provides businesses with complete control over their telephony systems and offers many advantages, such as scalability by expanding storage capacity, flexibility in integrating with third-party applications, and security within the internal network.

GDMS Unified Communication, on the other hand, is a cloud-based solution that provides a user-friendly interface to manage and monitor devices before, during, and after deployment. GDMS organizes systems into separate product lines, specifically Unified Communications and Networking Solutions, for simplified management.

This guide explains how to remotely manage SoftwareUCM using GDMS Unified Communications, enabling efficient monitoring and control from any location.

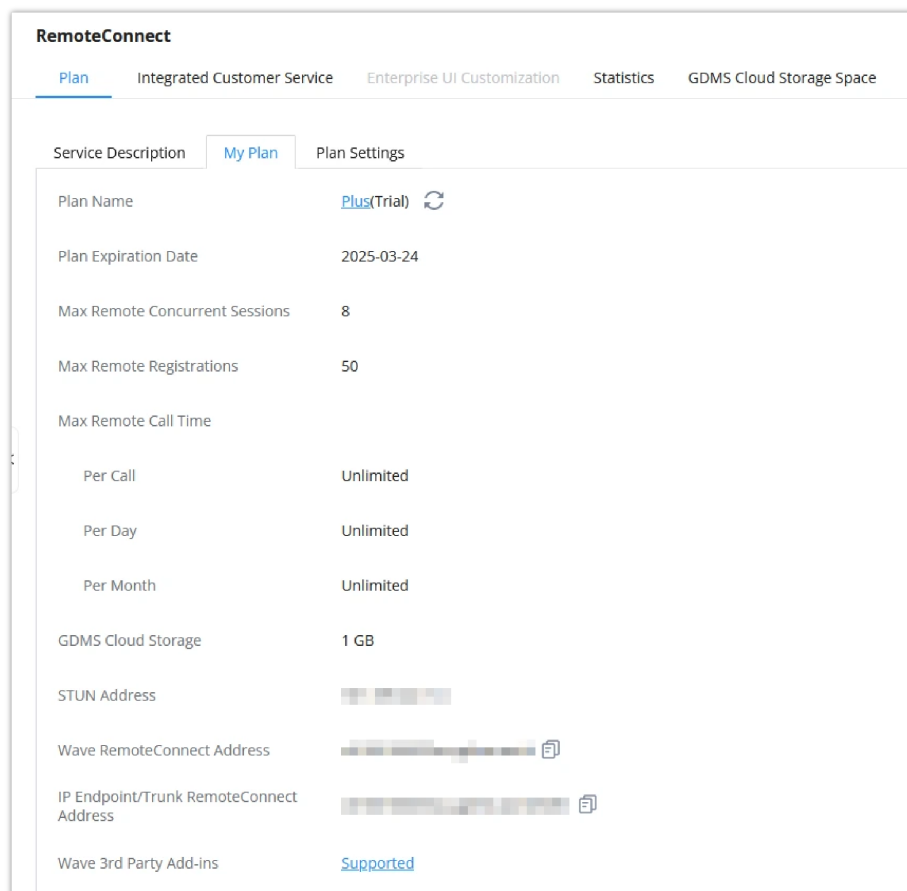
ADDING SOFTWAREUCM TO GDMS

UCMRC (UCM RemoteConnect) allows users to remotely access and configure SoftwareUCM through GDMS.

Note:

To learn more about UCM RemoteConnect plans, please refer to the following link: <https://ucmrc.gdms.cloud/plans>

1. Before connecting SoftwareUCM with GDMS, ensure that the RemoteConnect information is displayed on SoftwareUCM **web GUI→RemoteConnect→Plan→My Plan** page.

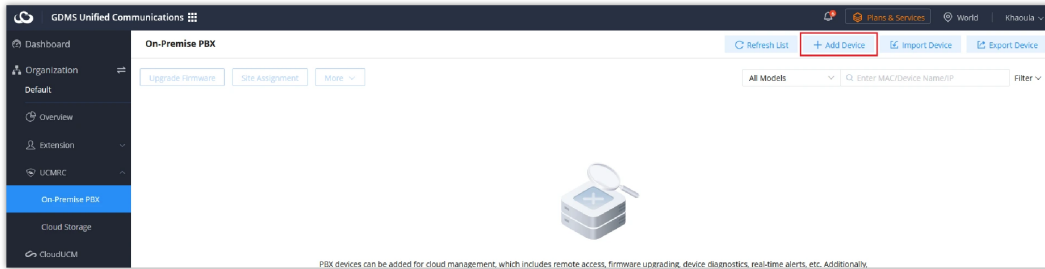


SoftwareUCM RemoteConnect Page

2. In order to use the service, please log in to your GDMS account. (If you do not have a GDMS account, please sign up here and then log in: <https://www.gdms.cloud/login>)

Add a single SoftwareUCM

1. On the GDMS platform, sign in and go to **UCMRC→On-Premise PBX** page, click on “**Add Device**”.



GDMS On-Premise PBX Page

2. Enter the MAC Address of the SoftwareUCM, which can be found on the **Web UI→System Status→System Information**.

Adding Software UCM MAC Address

3. Choose a **name** for your SoftwareUCM, assign it to the desired **site** and enter the **Serial Number** (located under **Web UI→System Status→System Information**).
4. If the “Activate UCMRC Free Trial Plan (Plus)” option is selected, the **UCMRC Plus** plan will be automatically activated after adding the SoftwareUCM. If it is not selected, the **Basic plan** will be applied instead.

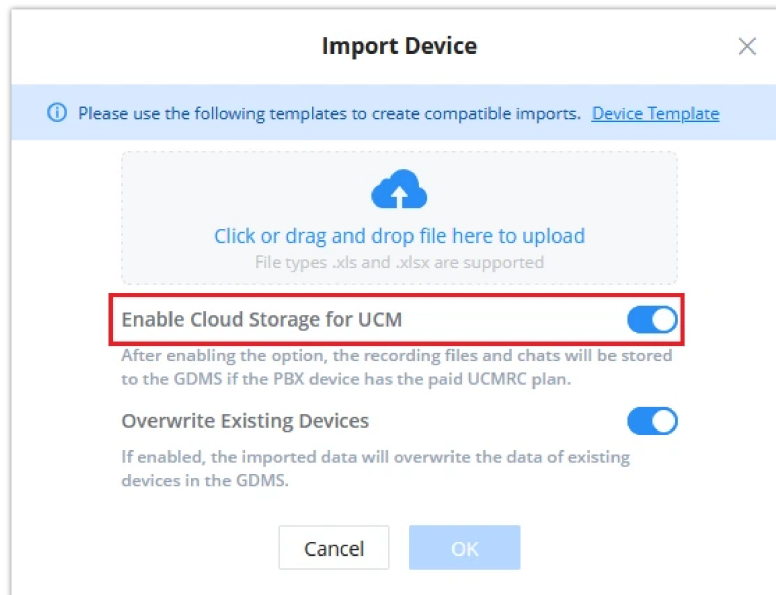
Adding SoftwareUCM Information

5. Once all of the information is filled correctly, click the **Save** button to add SoftwareUCM to the corresponding site.

Batch SoftwareUCM Import

1. On the GDMS platform, sign in and go to **UCMRC→On-Premise PBX** page, click on “**Import Device**”.

2. On the import device window, choose whether or not to store recording files and chats on GDMS Cloud storage by enabling/disabling the “**Enable Cloud Storage for UCM**” option. (This only applies to paid UCMRC plans)



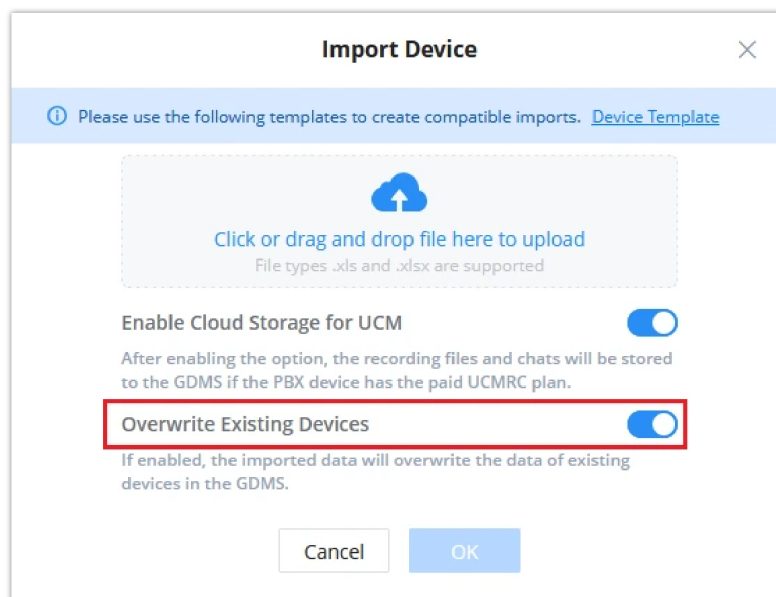
The screenshot shows the 'Import Device' dialog box. At the top, there is a blue header bar with the title 'Import Device' and a close button. Below the header, a light blue bar contains an information icon and the text 'Please use the following templates to create compatible imports. [Device Template](#)'. The main area has a dashed box for file upload with a cloud icon and the text 'Click or drag and drop file here to upload' and 'File types .xls and .xlsx are supported'. Below this, the 'Enable Cloud Storage for UCM' toggle is highlighted with a red rectangle and is turned on. Below it, the 'Overwrite Existing Devices' toggle is also turned on. At the bottom are 'Cancel' and 'OK' buttons.

Enable Cloud Storage for UCM

Note:

GDMS Cloud Storage is only available for SoftwareUCMs with paid UCMRC plans.

3. Select “**Overwrite Existing Devices**”, if you wish to import a SoftwareUCM that is already added to your GDMS account.



This screenshot is similar to the previous one, showing the 'Import Device' dialog box. In this instance, the 'Overwrite Existing Devices' toggle is highlighted with a red rectangle and is turned on. The 'Enable Cloud Storage for UCM' toggle is also turned on. The layout and other elements are identical to the previous screenshot.

Overwrite Existing Devices

4. Click on “**Device Template**” to download the Excel import file template.

Import Device

Please use the following templates to create compatible imports. [Device Template](#)



Click or drag and drop file here to upload

File types .xls and .xlsx are supported

Enable Cloud Storage for UCM

After enabling the option, the recording files and chats will be stored to the GDMS if the PBX device has the paid UCMRC plan.

☒

Overwrite Existing Devices

If enabled, the imported data will overwrite the data of existing devices in the GDMS.

☒

Cancel
OK

Download Device Template

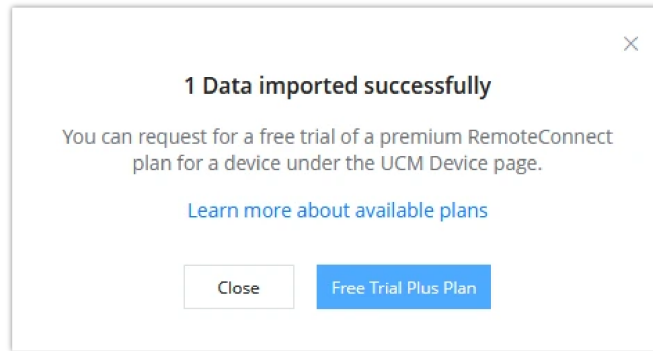
5. Open the downloaded file and complete the fields listed in the table below.

	A	B	C	D
1	Instructions: 1. Fields marked with * are required and cannot be empty. 2. MAC Address: Valid characters are 0-9, A-Z, hyphens (-), and colons (:) (e.g. 00-15-65-1A-2B-3C, 00:15:65:1a:2b:3c, 0015651a2B3c, etc.). If users want to assign accounts to multiple devices, they must enter the MAC addresses in multiple lines. 3. Password: Required if users want to add new devices to GDMS. Only alphanumeric characters allowed. 4. Device Name: The maximum allowed number of characters is 64 characters. 5. Site Name format: 1st Level Site/2nd Level Site/.../New Site. Users must enter the names starting from the 1st Level Site. If the higher level sites do not exist, they will be created automatically. If no higher level site name is entered, this site name will be used by default to fill in missing site names. The maximum allowed number of characters is 64 characters.			
2	*MAC address	*Password	Device Name	Site Name
3				
4				
5				
6				
7				

Device Template File

MAC Address	(Required) Enter the MAC address of SoftwareUCM. The valid characters (0-9, a-z, A-Z) can be entered either consecutively or separated by colons (:) or hyphens (-). Examples: ● 0015651a2B3c ● 00:15:65:1a:2b:3c ● 00-15-65-1A-2B-3C
Password/SN	(Required) Input the serial number of SoftwareUCM in this field.
Device Name	(Optional) Set the name of the SoftwareUCM. The maximum allowed number of characters is 64 characters.
Site Name	(Optional) Select the site to which the SoftwareUCM will be assigned. The maximum allowed length is 64 characters. Notes: ● 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 higher level sites do not exist, they will be created automatically ● If this field is left blank, SoftwareUCM will be added to the default site.

6. Save the template file, and upload it on the **Import Device** window.
7. A confirmation prompt will appear once the SoftwareUCM has been imported successfully.



Device Template Uploaded Successfully

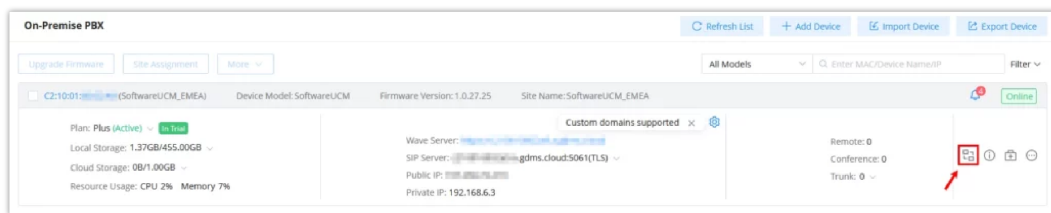
8. Close the window or select the option to activate the Free Trial for the RemoteConnect Plus plan.

SOFTWAREUCM GDMS FUNCTIONS

Remote Access to PBX

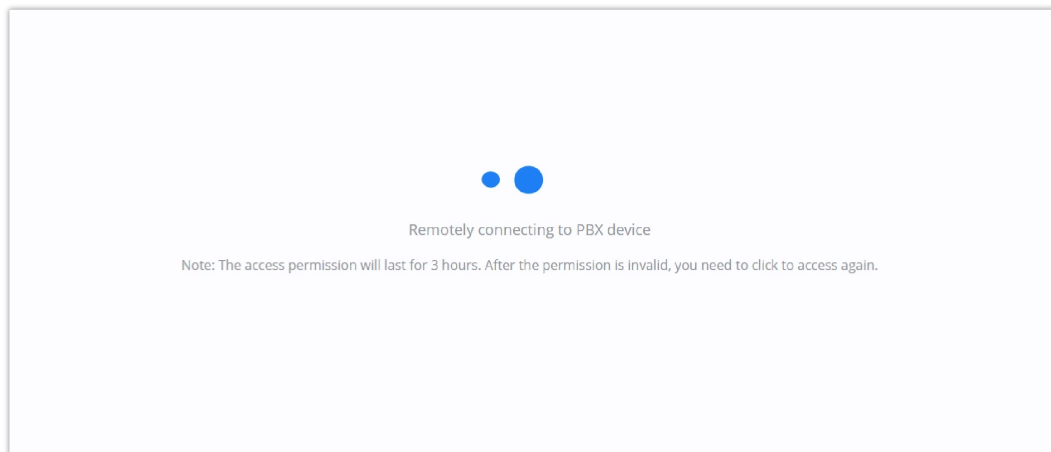
To access SoftwareUCM remotely, please follow the steps below:

1. Go to **GDMS Unified Communications→UCMRC→On-Premise PBX** and click on the icon shown in the image below.



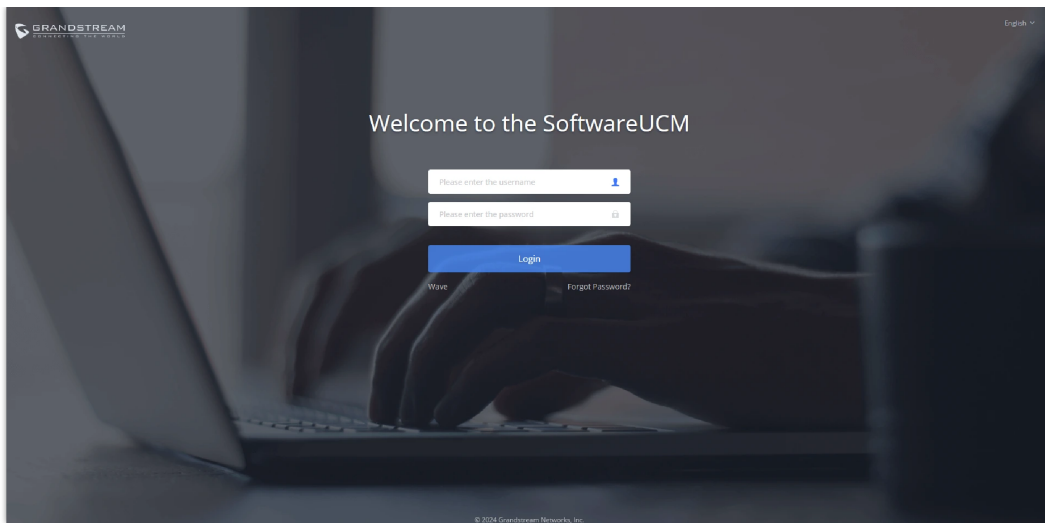
Remote Access to SoftwareUCM

2. After being redirected to this page, please wait for the connection time to complete. Access permissions are valid for only three hours, so once they expire, users will need to click the **"Remote Access to PBX"** button again to regain access.



Remote Access Redirect Page

3. Enter your **username** and **password** to remotely login to SoftwareUCM's Web UI.

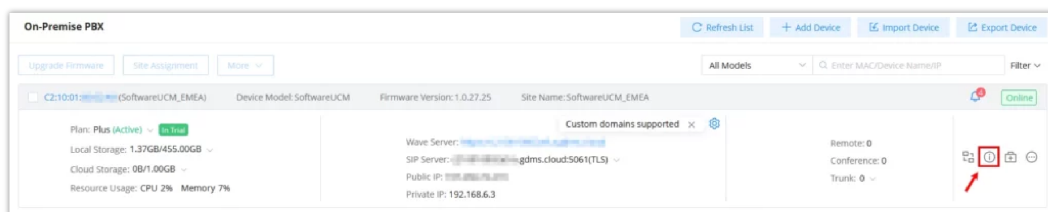


SoftwareUCM Login Page

Device Details

The **Device Details** tabs offer users access to various SoftwareUCM information, including device details, plan information, and statistical reports. This section describes the function of each tab.

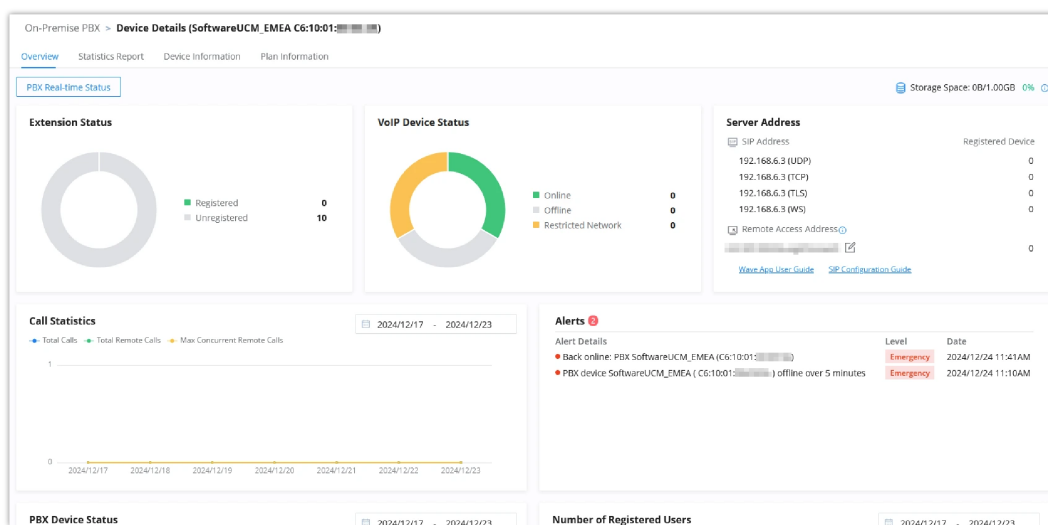
To access Device Details, first click on the icon highlighted in the image below:



SoftwareUCM Device Details

Overview

The Overview Page provides a comprehensive view of key system information, including the Extension Status, VoIP Device Status, and Server Address. It also displays Call Statistics, Alerts, PBX Device Status, and the number of registered users, offering users a quick and clear view of the system's current performance and health.



SoftwareUCM Device Details – Overview

Statistics Report

The Statistics Report page provides detailed reports related to the SoftwareUCM (e.g. Device Storage, Total Calls, etc...) and allows users to configure an email address for receiving these reports at specified intervals, ensuring timely and efficient access to important system data.

On-Premise PBX > **Device Details (SoftwareUCM, EMEA C6:10:01:)**

Overview **Statistics Report** Device Information Plan Information

Email Notification Settings

Time Zone: (GMT+01:00) Casablanca, Monrovia

Statistics Time	Software Version	Device Storage	Cloud Storage	Total Calls	Total Remote Calls	Max Concurrent Remote Calls	Maximum number of PBX registration	Maximum number of local registration	Call Type
2024/12/16	1.0.27.25	445.08MB/23...	0B/0B	7	0	0	—	—	—

SoftwareUCM Device Details – Statistics Report

To receive these reports via email, click the “**Email Notification Settings**” button, then configure the desired sending interval and specify the recipient’s email address.

Email Notification Settings

Email Notification

Time Zone

(GMT+01:00) Casablanca, Monrovia

* Send Time

10:30

Interval

Daily

Every

Tuesday

Per month

24Day

Per month

Fourth

Tuesday

* Receiving Email Address

user@grandstream.com

Add Email Address

Cancel

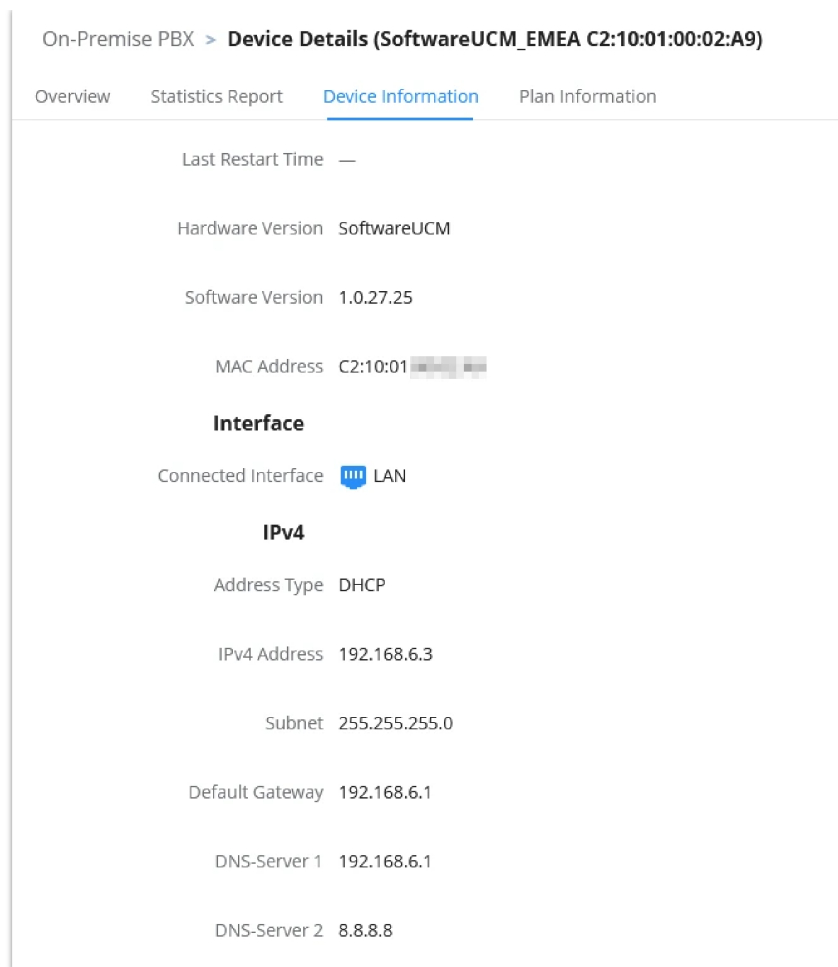
Save

Email Notification Settings

Device Information

The Device Information page displays essential details about the device, including the Last Restart Time, Hardware Version, Software Version, and MAC Address.

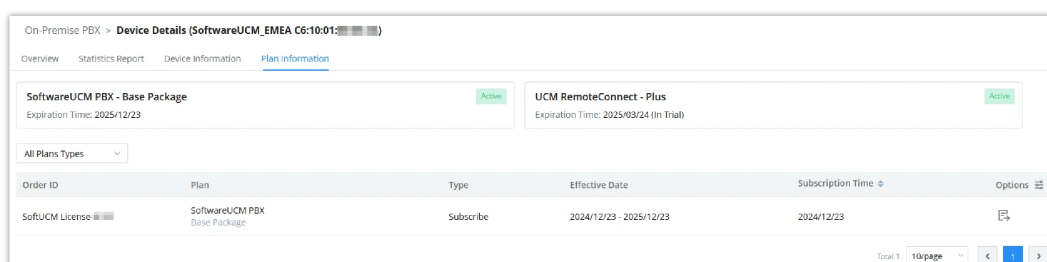
It also provides network information such as the Connected Interface, Address Type, IPv4 Address, Default Gateway, and IPv6 details, offering a complete overview of the device’s configuration and connectivity.



SoftwareUCM Device Details – Device Information

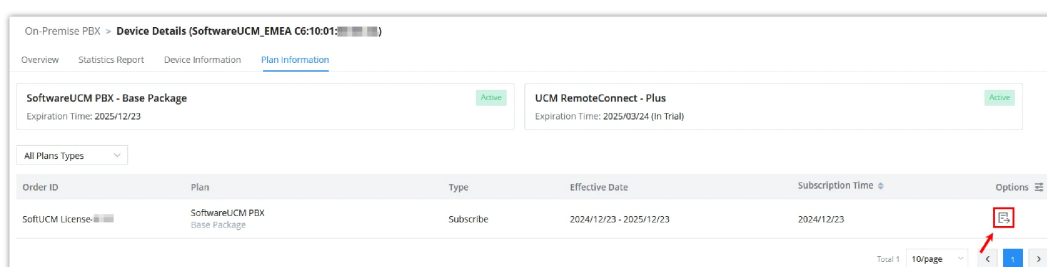
Plan Information

This tab provides comprehensive information about the activated plans for both UCMRC and SoftwareUCM, including details such as the plan type, and the expiration date of each.



SoftwareUCM Device Details – Plan Information

Additionally, users can view the SoftwareUCM license receipt by clicking the icon shown in the image below:

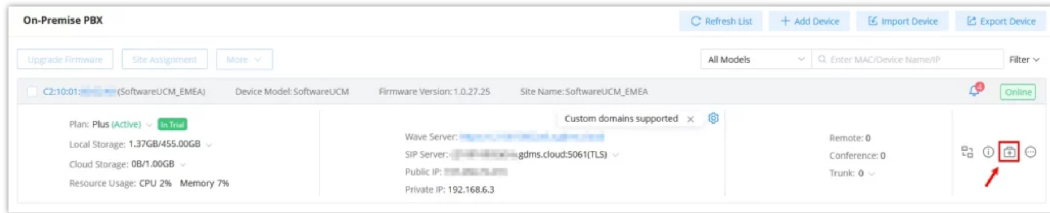


View SoftwareUCM Receipt

UCMRC Diagnostics

This feature provides users with the ability to troubleshoot and resolve any issues that may occur with SoftwareUCM. It offers different tools to identify potential problems, helping users to quickly diagnose, fix any errors and minimize downtime.

To access the diagnostics page, please click on the the icon shown in the image below:



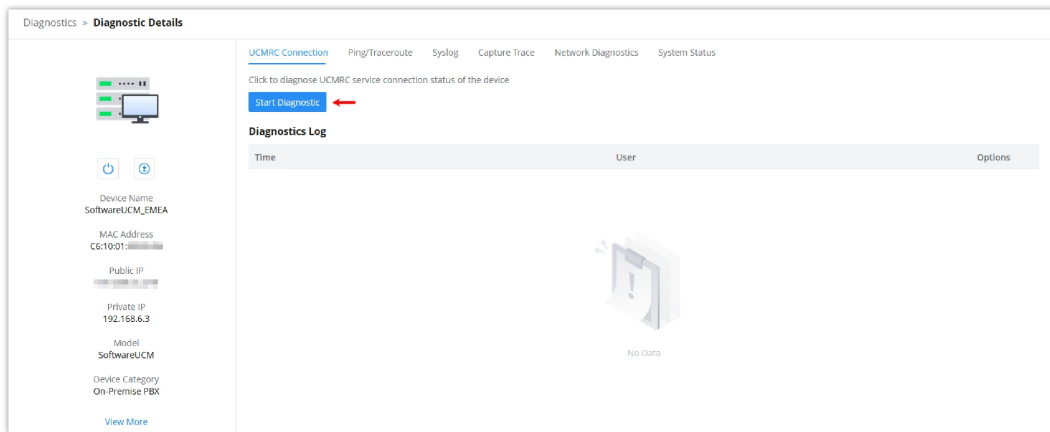
SoftwareUCM UCMRC Diagnostics

Note:

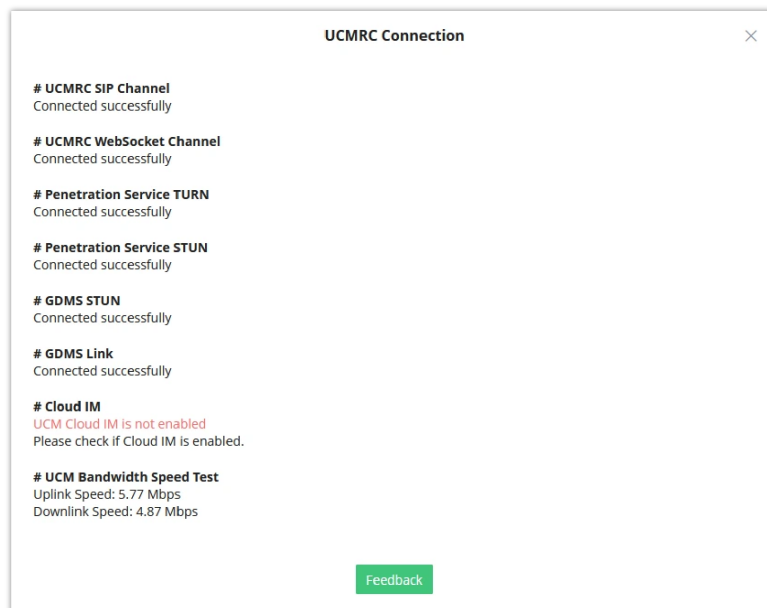
GDMS can only run one SoftwareUCM diagnostic at a time. If you attempt to start an additional diagnostic while another is already in progress, an error message will appear, informing you that the action cannot be completed. The message will read: "The device is currently busy with another task".

UCMRC Connection

This feature allows users to check the current status of the device's connection to the UCMRC service. By clicking on the **"Start Diagnostic"** button, users can initiate a diagnostic process that checks the health and status of the connection.



SoftwareUCM UCMRC Diagnostics – UCMRC Connection

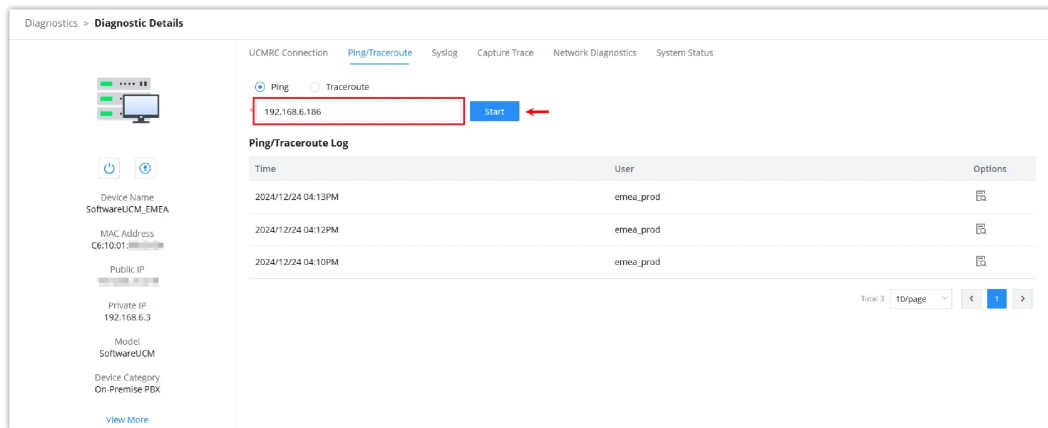


UCMRC Connection Diagnostic Results

Ping/Traceroute

The **Ping/Traceroute** diagnostic is a tool that allows users to remotely test and diagnose network connectivity related to the SoftwareUCM system. This can be useful to identify the cause of call drops and voice quality issues.

In order to run a Ping/Traceroute command remotely, please enter the target IP address and click on the **“Start”** button.

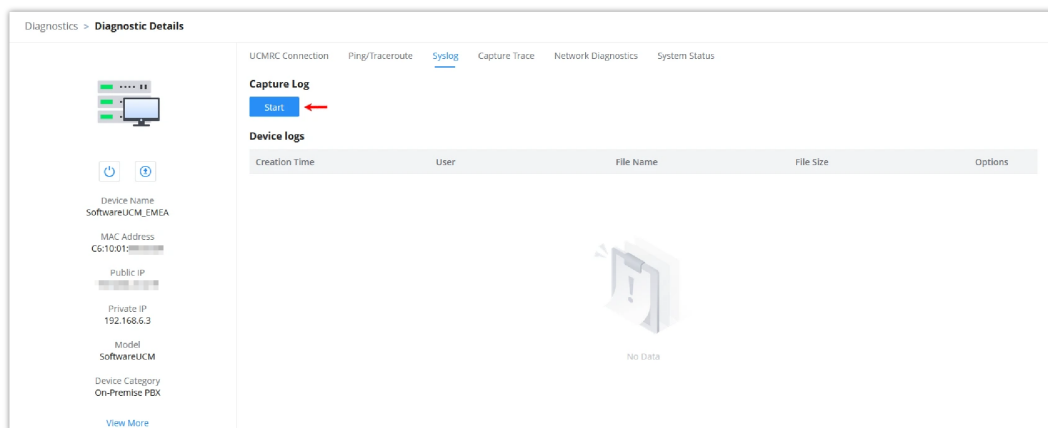


SoftwareUCM UCMRC Diagnostics – Ping/Traceroute

Syslog

The UCMRC **Syslog** diagnostic helps users retrieve and analyze logs generated by SoftwareUCM without the need for physical access. These logs can help to identify system failures, detect misconfigurations, and address call routing issues.

Click on the **“Start”** button to begin the syslog capturing process.



SoftwareUCM UCMRC Diagnostics – Syslog

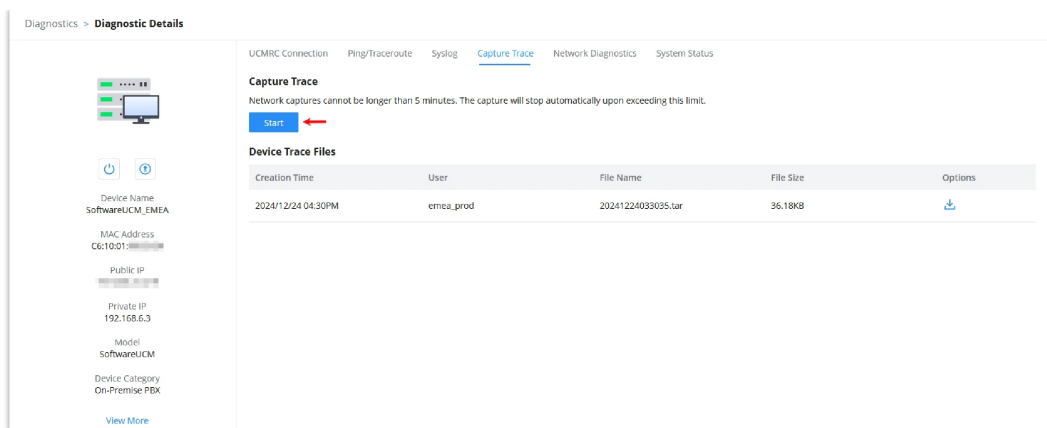
Capture Trace

UCMRC **Capture Trace** for SoftwareUCM is a diagnostic feature that enables users to remotely monitor and capture network traffic between endpoints and the IPPBX. This feature is essential for troubleshooting communications issues and ensuring reliable operation of IP-based telephony services.

Note:

Network captures cannot be longer than 5 minutes. The capture will stop automatically upon exceeding this limit.

To start the packet capture, please select **“Start”**.

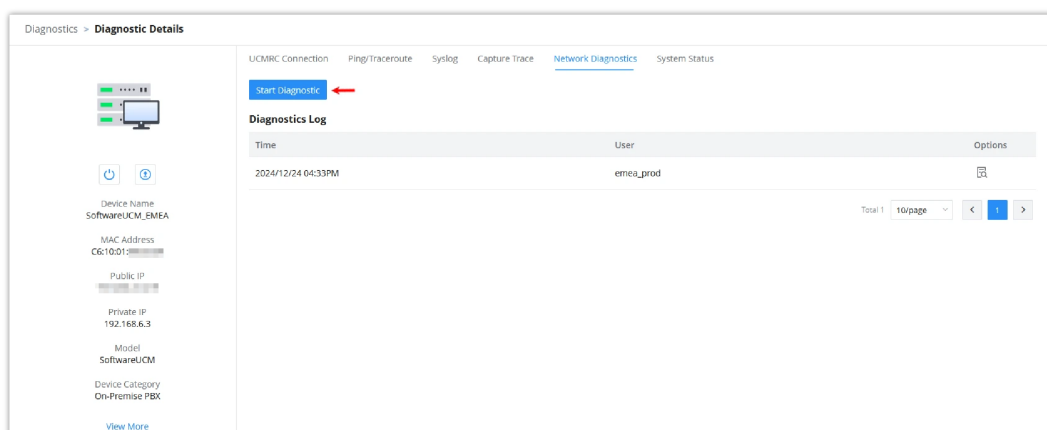


SoftwareUCM UCMRC Diagnostics – Capture Trace

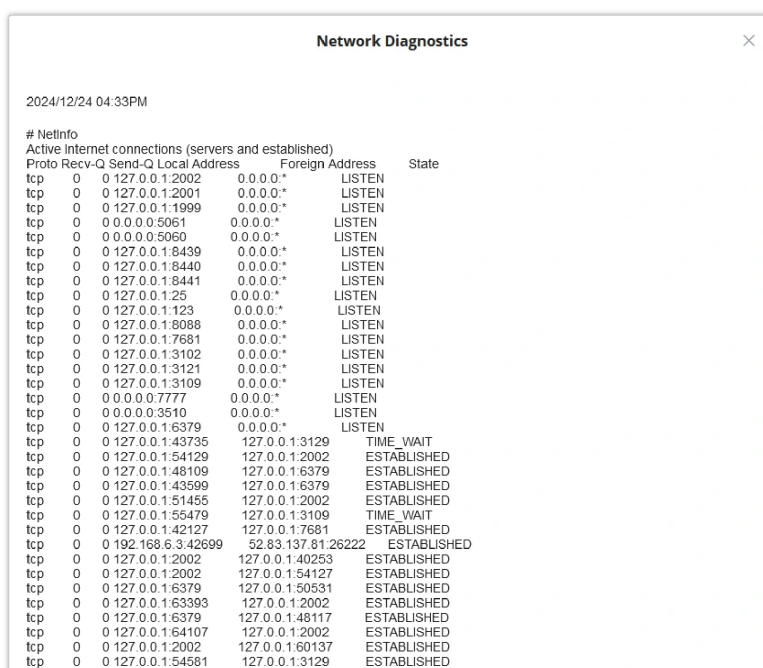
Network Diagnostics

The output from the Network Diagnostics provides a detailed list of active internet connections, including listening services, established connections on SoftwareUCM as well as additional information about the system's network interfaces and routing tables.

In order to use this feature, click on the **"Start Diagnostic"** button.



SoftwareUCM UCMRC Diagnostics – Network Diagnostics

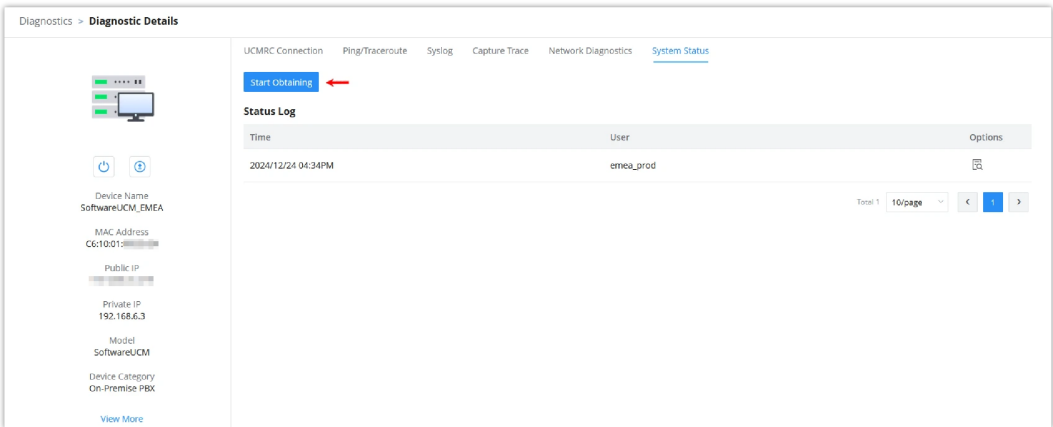


Network Diagnostics Results

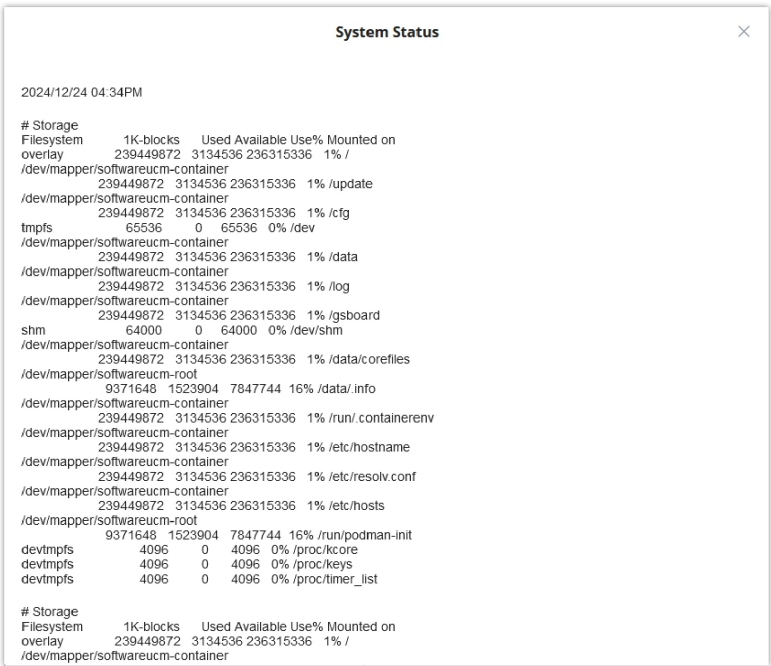
System Status

The System Status diagnostic provides insights into storage, CPU, and memory usage of SoftwareUCM. It allows users to ensure that the system has sufficient resources to operate efficiently and handle demanding tasks. This diagnostic tool is crucial for identifying potential performance issues, such as high CPU usage or low available memory.

To use this feature, click on the **“Start Obtaining”** button.



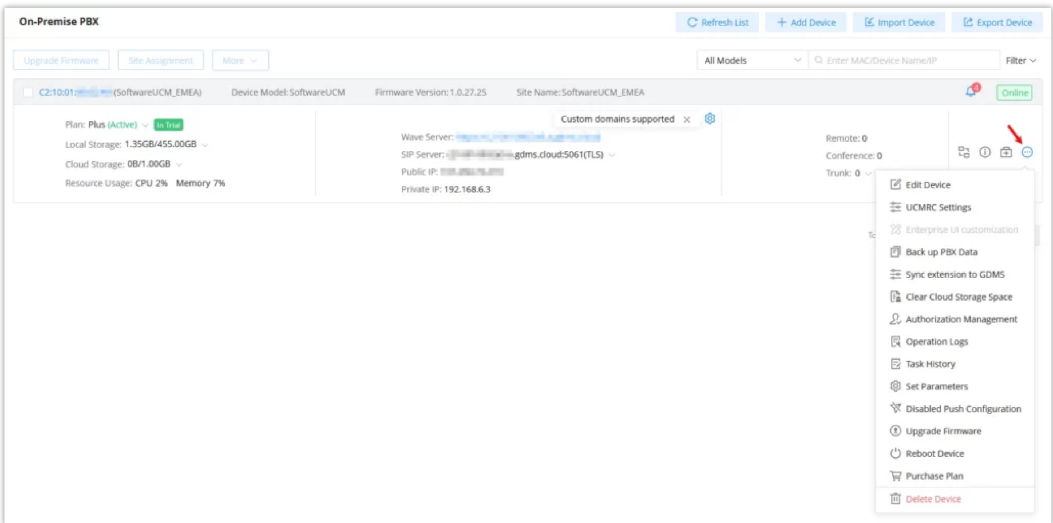
SoftwareUCM UCMRC Diagnostics – System Status



System Status Results

ADDITIONAL GDMS OPTIONS

GDMS offers some additional configuration options for SoftwareUCM, that can be found on the drop-down list shown below:



This section of the guide describes in detail each of the available options under this menu.

Edit Device

The **Edit Device** window allows users to configure the SoftwareUCM information related to GDMS mentioned in the table below.

Edit Device

MAC Address
C6:10:01:XXXXXX

Device Name
SoftwareUCM_EMEA

* Site
SoftwareUCM_EMEA

Remarks ⓘ
[Empty text area]

Access Server ⓘ ☒

Zone
Oregon

Default Server Address
XXXXXX

[Customize Personal URL](#) Or [Customize Domain](#) ⓘ

Cancel Save

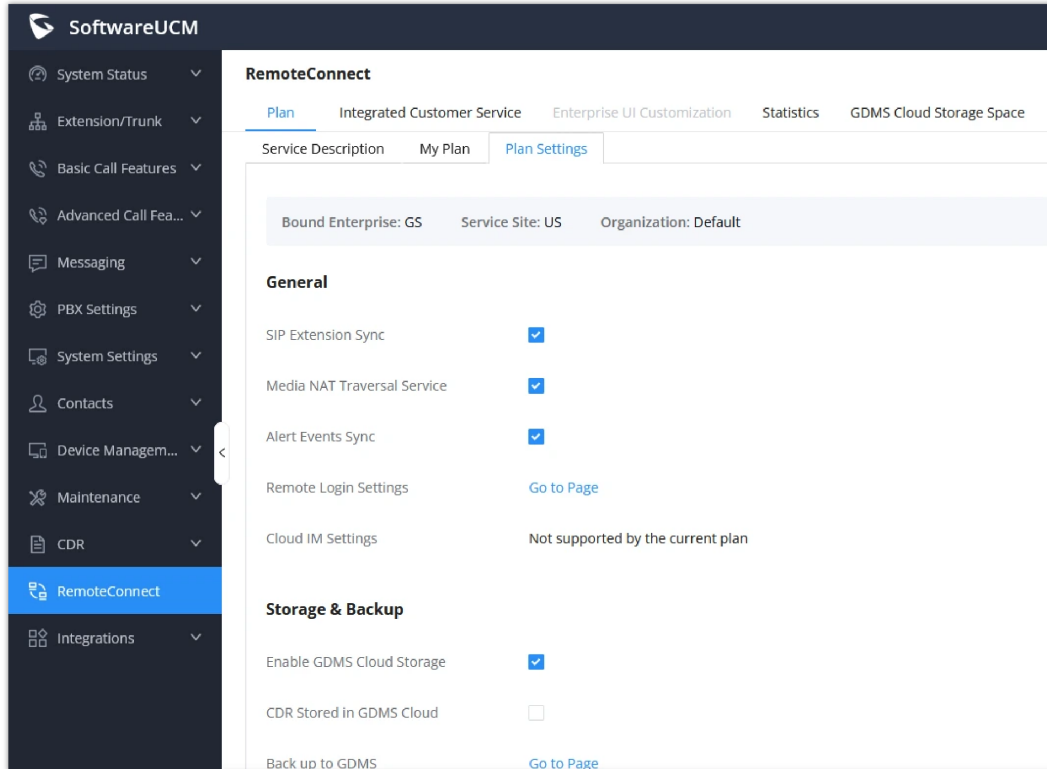
Edit SoftwareUCM Device

MAC Address	Shows the MAC Address of the SoftwareUCM.
Device Name	Configures the device name of the SoftwareUCM on GDMS.
Site	Allows users to choose the site to which this SoftwareUCM is assigned.
Remarks	Includes all relevant comments about this SoftwareUCM system. Note: This data is synchronized with the "Remark" field set locally in SoftwareUCM under System Status → System Information .
Access Server	Enables configuration of the remote access address for Wave.
Zone	Allows users to choose the zone for the remote Wave access address. Note: The server address will be changed after modifying this parameter.

Default Server Address	Shows the default remote Wave access address for SoftwareUCM.
Custom Server Address	Enables customization of the remote Wave access address.

UCMRC Settings

This can be used as a shortcut to remotely access SoftwareUCM's **RemoteConnect Plan Settings** page, which allows to configure the parameters presented in the table below.



SoftwareUCM RemoteConnect – Plan Settings

<i>General</i>	
SIP Extension Sync	This option enables users to automatically export the SIP extensions configured on SoftwareUCM to GDMS. This allows easy allocation and management of SIP extensions on end devices.
Media NAT Traversal Service	Enables/Disables NAT traversal service provided by GDMS. Notes: • If enabled, manual configurations for TURN servers and other NAT-related settings on UCM will not take effect. • This feature will not work unless "ICE Support" is enabled under PBX Settings→RTP Settings.
Alert Events Sync	Allows users to enable/disable synchronization of SoftwareUCM's alert information with GDMS.
Remote Login Settings	Redirects to SoftwareUCM's Remote Login page under Maintenance → Login Settings , which allows to configure trusted login locations.
Cloud IM Settings	Configures cloud-based instant messaging services for SoftwareUCM. Note: This feature is only included in the UCMRC Enterprise plan.

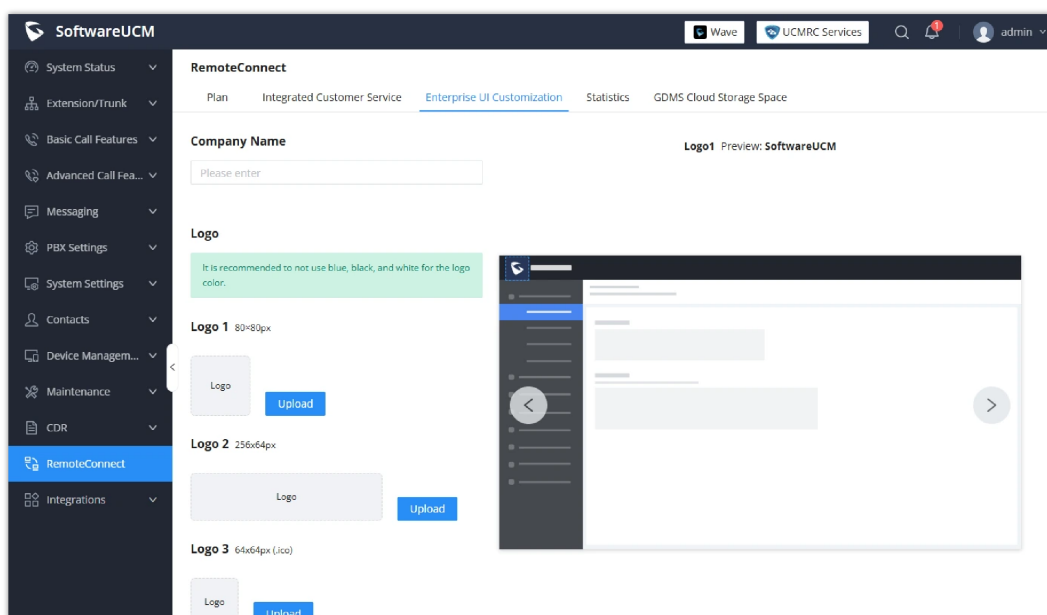
<i>Storage & Backup</i>	
Enable GDMS Cloud Storage	Configures whether or not to enable GDMS cloud storage. Note: if this feature is disabled, users will still be able to retrieve data/files stored on GDMS.
CDR Stored in GDMS Cloud	If enabled, SoftwareUCM CDR data will be synced to the GDMS server at 2 AM on the 1st of each month based on the SoftwareUCM's system time.
Back up to GDMS	Redirects to SoftwareUCM's Backup page under Maintenance , where users can start or schedule a backup with GDMS Cloud Storage configured as the destination.
Recordings Stored in GDMS Cloud	Redirects to SoftwareUCM's File Manager page under PBX Settings , where users can choose to store recording files on GDMS Cloud Storage.
Chat Data Cloud Storage	Redirects to SoftwareUCM's File Manager page under PBX Settings , where users can choose to store IM files on GDMS Cloud Storage.
<i>Passwordless Remote Access</i>	
Enable Passwordless Remote Access	This option allows users to remotely access SoftwareUCM using GDMS, eliminating the need for a login password.

Enterprise UI Customization

This option on GDMS enables users to remotely access SoftwareUCM's **RemoteConnect**→**Enterprise UI Customization** page, where organizations can modify the interface based on their preferences. It provides the ability to personalize elements such as the logos of SoftwareUCM and Wave, both on the Web UI and in emails sent by SoftwareUCM.

Note:

The Enterprise UI Customization is available only with the Business and Enterprise UCMRC plans.



SoftwareUCM RemoteConnect – Enterprise UI Customization

Back up PBX Data

The **Back up PBX Data** option redirects users to SoftwareUCM's **Maintenance**→**Backup** page, where users can perform or schedule system backups.

In order to create a new backup that will be stored in GDMS, please follow the steps below:

1. Click on the **"Backup"** button, and select **"GDMS Cloud Storage"** under **Choose Storage Location**.
2. Choose a Name for the backup file and the types of data that will be included.

Backup > Create New Backup

* Choose Storage Location: GDMS Cloud Storage

* File Name: backup_20241225_121620

Choose Backup Files:

- ☐ All ☒ Config File ☒ IM Message ☒ IM Files ☐ CDR Records ☐ Recording Files
- ☐ Video Recording Files ☐ Fax Files ☐ Voicemail ☒ Voice Prompt Files
- ☐ Queue Statistics Report ☒ ZeroConfig Storage ☐ Meeting Report

ⓘ Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

Cancel Backup

Create New Backup on SoftwareUCM

3. Click on **"Backup"** and wait for SoftwareUCM to complete the backup process.
4. To access the backup on GDMS go to UCMRC Cloud Storage

To schedule a backup from SoftwareUCM's web UI, please refer to the following instructions:

1. Click the **"Schedule Backup"** button and check the box to enable scheduled backups.
2. Select **"GDMS Cloud Storage"** under **Choose Storage Location**.
3. Choose the desired **Backup Time** for SoftwareUCM to schedule the backup.
4. Enter the **Backup Frequency** (in days), the valid range is 1 to 30.
5. Select the types of data that will be included in the backup and Click on **"Save"**

Backup > Schedule Backup

ⓘ SFTP server can be configured in the PBX Settings->Storage Device Management-> SFTP page.

Schedule Backup: ☒

* Choose Storage Location: GDMS Cloud Storage

* Backup Time: 10:00

* Backup Frequency: 1

Choose Backup Files:

- ☒ All ☒ Config File ☒ IM Message ☒ IM Files ☒ CDR Records ☒ Recording Files
- ☒ Video Recording Files ☒ Fax Files ☒ Voicemail ☒ Voice Prompt Files
- ☒ Queue Statistics Report ☒ ZeroConfig Storage ☒ Meeting Report

ⓘ Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

Cancel Save

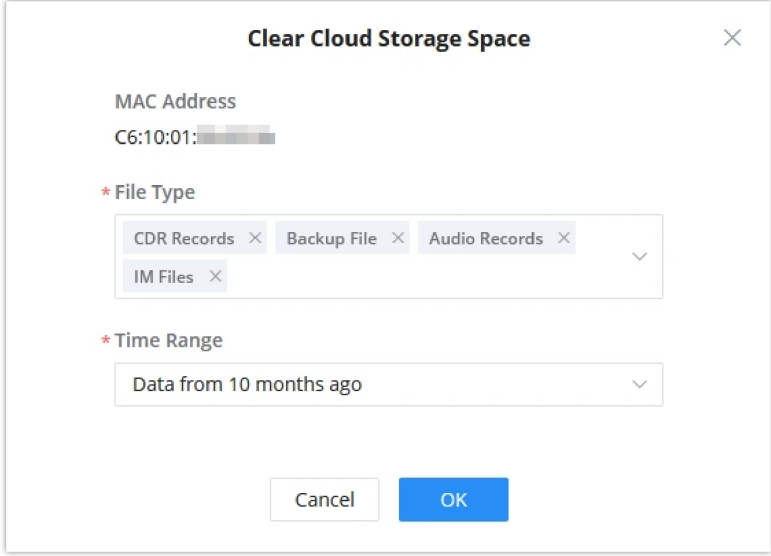
Schedule Backup on SoftwareUCM

Users can perform the following actions:

- Copy the file URL.
- Download the backup file.
- Rename the backup file.
- Delete the backup file.
- Restore the back up file to SoftwareUCM.

Clear Cloud Storage Space

Users can use this option to delete specific saved data in cloud storage, helping to free space and prevent unnecessary storage usage. To clear storage space, users can select the types of files to delete, as well as define the time range as shown in the image below:



The dialog box titled "Clear Cloud Storage Space" contains the following fields:

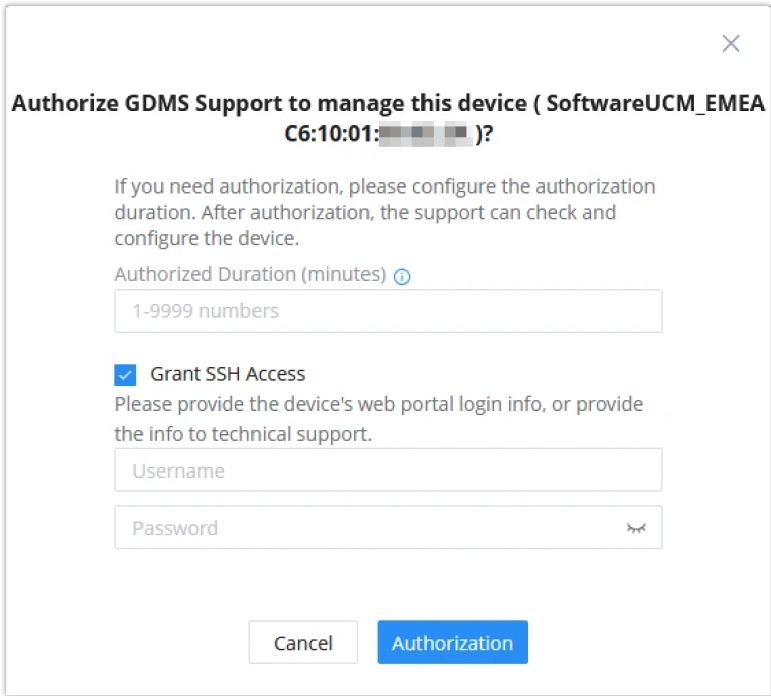
- MAC Address:** C6:10:01: [redacted]
- * File Type:** A multi-select dropdown menu with options: CDR Records, Backup File, Audio Records, and IM Files.
- * Time Range:** A dropdown menu with the selected option "Data from 10 months ago".
- Buttons:** "Cancel" and "OK".

Authorization Management

If assistance from Grandstream Support is needed to troubleshoot an issue, the user can enable Authorization Management to allow device management through GDMS Support.

To grant Grandstream Support authorization to manage the SoftwareUCM, please follow the steps below:

1. Select "**Authorization Management**" and enter the **authorization duration**, which can be set between 1 to 9999 minutes, according to the time required for troubleshooting.



The dialog box titled "Authorize GDMS Support to manage this device (SoftwareUCM_EMEA C6:10:01: [redacted])?" contains the following fields:

- Text:** "If you need authorization, please configure the authorization duration. After authorization, the support can check and configure the device."
- Authorized Duration (minutes):** A text input field with a help icon and the placeholder "1-9999 numbers".
- Grant SSH Access:** A checked checkbox with the label "Grant SSH Access".
- Text:** "Please provide the device's web portal login info, or provide the info to technical support."
- Username:** A text input field.
- Password:** A password input field with a toggle icon.
- Buttons:** "Cancel" and "Authorization".

SoftwareUCM Authorization Management in GDMS

2. Check the **Grant SSH Access** box, and enter the username and password of SoftwareUCM's web portal login.
3. Click on the "**Authorization**" button, to allow Grandstream Support to manage SoftwareUCM within the authorization period.

In case users wish to stop authorization before the configured period ends, they can select Authorization Management again and click the "**Stop Authorization**" button.

✕

Authorization Management

You have authorized GDMS Support to manage this device.

Authorization Time 2024/12/25 03:07PM-2024/12/25 03:09PM

Stop Authorization

Stop Authorization Management

Operation Logs

This feature helps users track the operations performed on SoftwareUCM through GDMS by providing a time-log. The records allow users to review the history of the changes made in order to monitor system activity.

On-Premise PBX > **Operation Logs (SoftwareUCM_EMEA C6:10:01:)**

View PBX Operation Logs

Emergency

All Operations

Q Enter Username

Filter

Time	Operator	Level	Details
2024/12/25 03:11PM	emea_prod	Emergency	Remote access to PBX
2024/12/25 03:08PM	emea_prod	Emergency	Device Stop Authorization
2024/12/25 03:07PM	emea_prod	Emergency	Device Authorization
2024/12/25 02:26PM	emea_prod	Emergency	Remote access to PBX: Back Up PBX Data
2024/12/25 12:40PM	emea_prod	Emergency	Backup Restore
2024/12/25 12:05PM	emea_prod	Emergency	Remote access to PBX: Back Up PBX Data
2024/12/25 10:45AM	emea_prod	Emergency	Remote access to PBX: UCMRC Settings
2024/12/25 09:57AM	emea_prod	Emergency	Remote access to PBX: Back Up PBX Data
2024/12/25 09:57AM	emea_prod	Emergency	Remote access to PBX: UCMRC Settings
2024/12/25 08:23AM	emea_prod	Emergency	Start Diagnostics

Total 3110/page1234

SoftwareUCM GDMS Operation Logs

Task History

The Task History page provides a detailed log of all the tasks performed on this SoftwareUCM. This includes the task type, time and status.

Task

+ Add Task

Delete

All Statuses

All Task Type

All Types

C6:10:01:

Filter

Task Name	Task Type	Task Time	Creator	Status	Run Time	Options
Rebooting SoftwareU...	Reboot Device	Immediate (2024/12/25 03:25PM)	emea_prod	Success	2024/12/25 03:25PM	

Total 110/page1

SoftwareUCM Task History in GDMS

Add a Task

To add a task for SoftwareUCM, navigate to the **Task** page and click on “Add Task”. The table below provides explanation of the parameters on this page.

Task > **Add Task**

* Task Name

Rebooting SoftwareUCM

* Task Type

Reboot Device

* Task Time

Immediate

Scheduled

Interval

* Target Device(s)

Select Devices

Enter MAC Address

Site

All Models

Q Enter MAC/Device Name

MAC Address

Device Name

Model

C6:10:01:

SoftwareUCM_EMEA

SoftwareUCM

C6:10:01:

SoftwareUCM

SoftwareUCM

Selected Device: 1

MAC Address

Device Name

Model

C6:10:01:

SoftwareUCM_EMEA

SoftwareUCM

Total 210/page1

Add a New Task in GDMS

Task Name	Enter the name of the task.
Task Time	● Immediate: The task will be run immediately. If the task is not run after 5 minutes, GDMS will automatically close it. ● Scheduled: Schedule the task to run at a specified time. The task will end at the specified end time, even if there are still devices queued up to run the task. ● Interval: Users could configure the recurring tasks such as daily, weekly, monthly, Nth week of each month, and perform a certain task. Specify the start date and time when the task will start, then specify the Duration of the task. If a device goes online during the duration of the task, the scheduled task will be performed as soon as the device goes online. If the device goes online after the task's duration, the task will not performed on that specific device. ● Permanent: This option applies only when the task type is Firmware Upgrade. Every time a corresponding device is added, the device will be upgraded. This is a reccurent task.
Task Type	● Reboot Device: VOIP device, SoftwareUCM, UCM6300 Series devices, and CloudUCM. ● Factory Reset: VOIP devices, SoftwareUCM and CloudUCM. ● Upgrade Firmware: Users will need to select the device model and firmware version to upgrade to. VoIP device and IPPBX device. ● Update Config: Model: Select the model template that will be used for the configuration update push. Applicable to VoIP devices and CloudUCM. ● Update Config: Group: Select the group template that will be used for the configuration update push. Applicable to VoIP devices and CloudUCM.
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 network quality, the user can also limit the maximum number of concurrent devices, such as upgrading 10 devices at the same time. * Upgrade Method ☒ Concurrent Upgrade 10 device(s) ☐ Sequential Upgrade
Current Firmware Range	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 $\leq x \leq$ Highest firmware version) will be upgraded.
Target Device(s)	● All devices of this model. ● Select Device. ● Enter MAC Address.

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

- If there are multiple tasks for one SoftwareUCM device, they will be queued up to run in order of their configured start time.
- If SoftwareUCM is offline, pending tasks will be run the next time the device is offline.
- Certain tasks and device setting changes can cause SoftwareUCM to reboot.
- Firmware upgrade tasks may require more time to run due to the size of some firmware files.

Task Status

Users can see the status of all completed and pending tasks by checking the **Status** column on the **Task** page.

Task							+ Add Task
Delete All StatusesAll Task TypeAll TypesEnter Task Name/MACFilter							
☐	Task Name	Task Type	Task Time	Creator	Status	Run Time	Options
☐	SoftwareUCM Reboot	Reboot Device	2024/12/25 04:41 PM ~ 2024/12/25 11:59 PM	emea_prod	Scheduled	—	⌚ ⏸ ⏹
☐	SoftwareUCM Factory...	Factory Reset	2024/12/25 04:39 PM ~ 2024/12/25 11:59 PM	emea_prod	Scheduled	—	⌚ ⏸ ⏹
☐	SoftwareUCM First Re...	Reboot Device	Immediate (2024/12/25 04:12 PM)	emea_prod	Success	2024/12/25 04:12 PM	⌚
Total 310/page							

Task Statues in GDMS

The following statuses are supported:

Scheduled	The task is scheduled at a future time.
Ongoing	The task is currently in progress.
Success	The task has been completed successfully.
Failed	The task has failed.
Cancelled	The task was canceled before its start time.
Stopped	The task was stopped while in progress
Timeout	The task was not executed once it has reached its ending time.

Search Task

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

Task							+ Add Task
Delete All StatusesAll Task TypeAll TypesEnter Task Name/MACFilter							
☐	Task Name	Task Type	Task Time	Creator	Status	Run Time	Options

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

To run the task again, click on **View Task Details**→**Run Again** for the desired task.

Stop Task

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

If the device has already completed the task (e.g., Reboot Device), it will finish the task. If not, the device will no longer execute the 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.

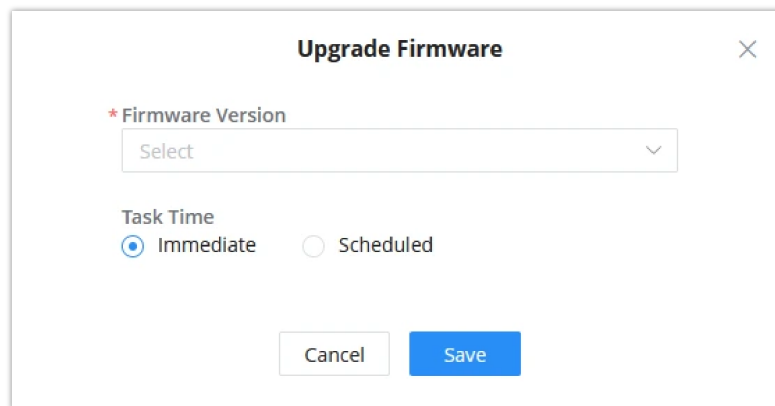
When deleting ongoing tasks, GDMS will automatically suspend and delete them. Any changes made before the task was suspended cannot be undone.

Upgrade Firmware

This option allows users to create a task to upgrade the firmware version of SoftwareUCM based on the latest release, or a specific upload.

To upgrade the firmware of SoftwareUCM, please follow the steps below:

1. Select “**Upgrade Firmware**” from the options menu on the **UCMRC→On-Premise PBX**. A window will appear to create a task for firmware upgrade.

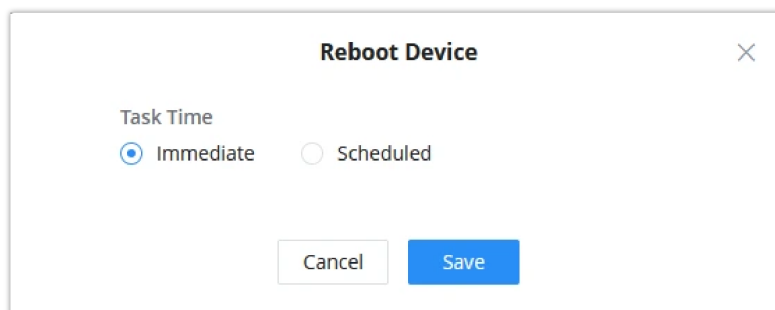


Firmware Upgrade Window

2. Choose the latest official firmware, or an uploaded version. (Firmware files can be added in GDMS under **Resources→Firmware→Custom Firmware**)
3. Schedule the time of the firmware upgrade, or choose to run it immediately then click on the **Save** button.
4. Go to the **Task** page, to check on the status of the firmware upgrade task.

Reboot Device

This option allows users to create a task to reboot SoftwareUCM. Users can choose whether to reboot the device immediately or schedule it at a later time.



Reboot Device Window

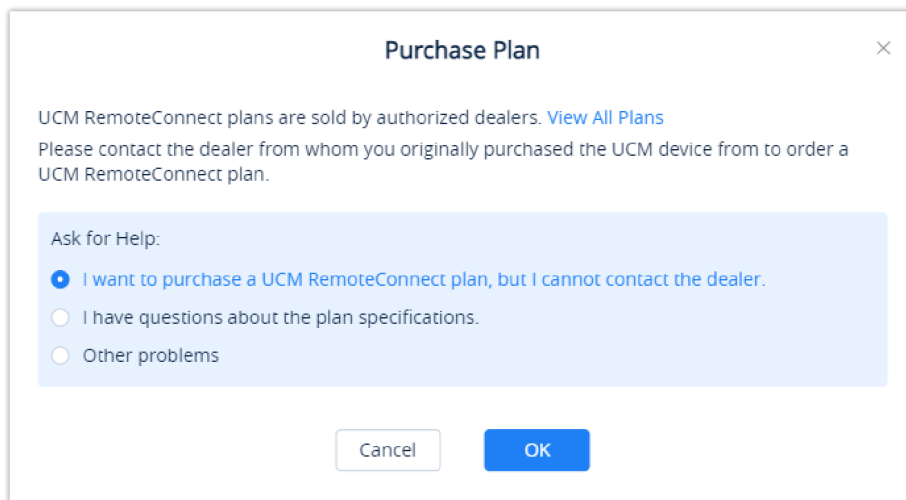
Purchase Plan

Users can purchase one or more UCM RemoteConnect plans and assign them to the corresponding SoftwareUCM instances. If the user wants to purchase a UCM RemoteConnect plan, they need to contact the device distributor.

Note:

The GDMS platform does not provide the purchasing service online.

If the user cannot contact the device distributor, they can use this option to notify the device distributor to contact them as soon as possible.



Purchase Plan [X]

UCM RemoteConnect plans are sold by authorized dealers. [View All Plans](#)

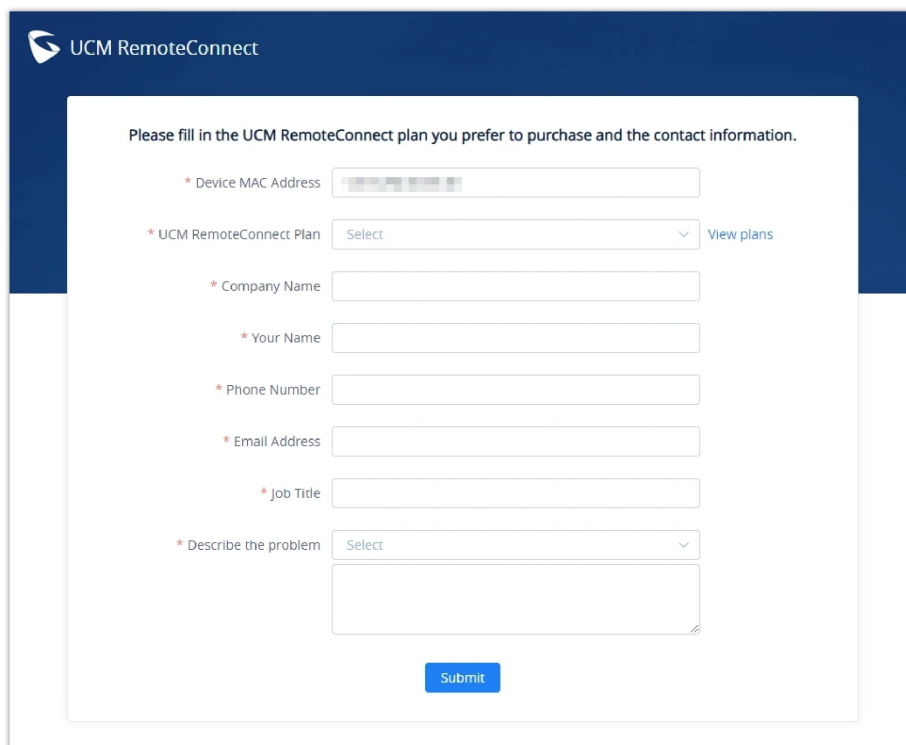
Please contact the dealer from whom you originally purchased the UCM device from to order a UCM RemoteConnect plan.

Ask for Help:

- ☒ I want to purchase a UCM RemoteConnect plan, but I cannot contact the dealer.
- ☐ I have questions about the plan specifications.
- ☐ Other problems

[Cancel] [OK]

Purchase Plan Window



UCM RemoteConnect

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

* Device MAC Address

* UCM RemoteConnect Plan [View plans](#)

* Company Name

* Your Name

* Phone Number

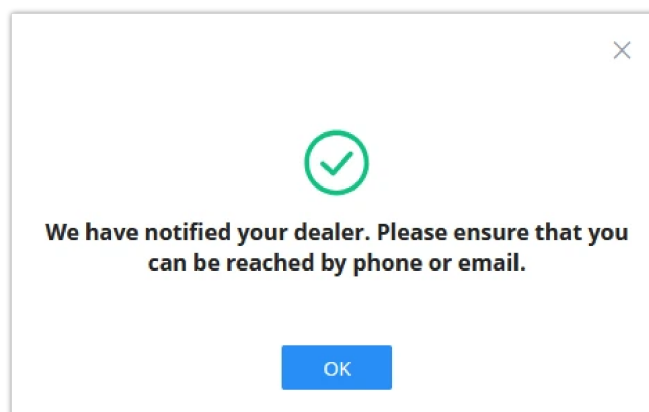
* Email Address

* Job Title

* Describe the problem

[Submit]

UCM RemoteConnect Form



[X]



We have notified your dealer. Please ensure that you can be reached by phone or email.

[OK]

Device Distributor Notified

If the user has questions about the plan specifications or encounters any issues, they will be directed to a window where they can report the issue to the support team.

Report an Issue

×

* Please enter your feedback

You can directly paste screenshots and web pictures here as attachments

+

(File type: zip, tar, rar, xls, xlsx, txt, docx, doc, jpeg, jpg, png, pdf, mp4, avi, wav, csv, gz)

* Feedback Category

UCMRC Plan

* Please enter your email address so that we can contact you in time.

@grandstream.com

×

+ Add Email

Cancel

Submit

Report an Issue

Delete Device

To delete SoftwareUCM from GDMS, please follow the steps below:

1. Go to **UCMRC→On-Premise-PBX** and select **"Delete Device"** from the SoftwareUCM options menu.
2. Choose a reason from the list then, click on **OK**

Delete the Device "C6:10:01: (SoftwareUCM_EMEA)?"

×

After deletion, all data of the device on GDMS will be cleared. If you decide to delete, we hope you can tell us the reason for the deletion so that we can improve the product. Thank you!

Delete Reason

☐ Remote management is not easy to use

☐ Remote calling is unavailable or difficult to use

☐ My UCM is only used in internal network, not in external network

☐ Cloud storage space is too small to use

☐ Security concerns

☐ Lack of functionality, such as

Please enter

☐ Other reason, such as

Please enter

Cancel

OK

Reason of Deletion

Note:

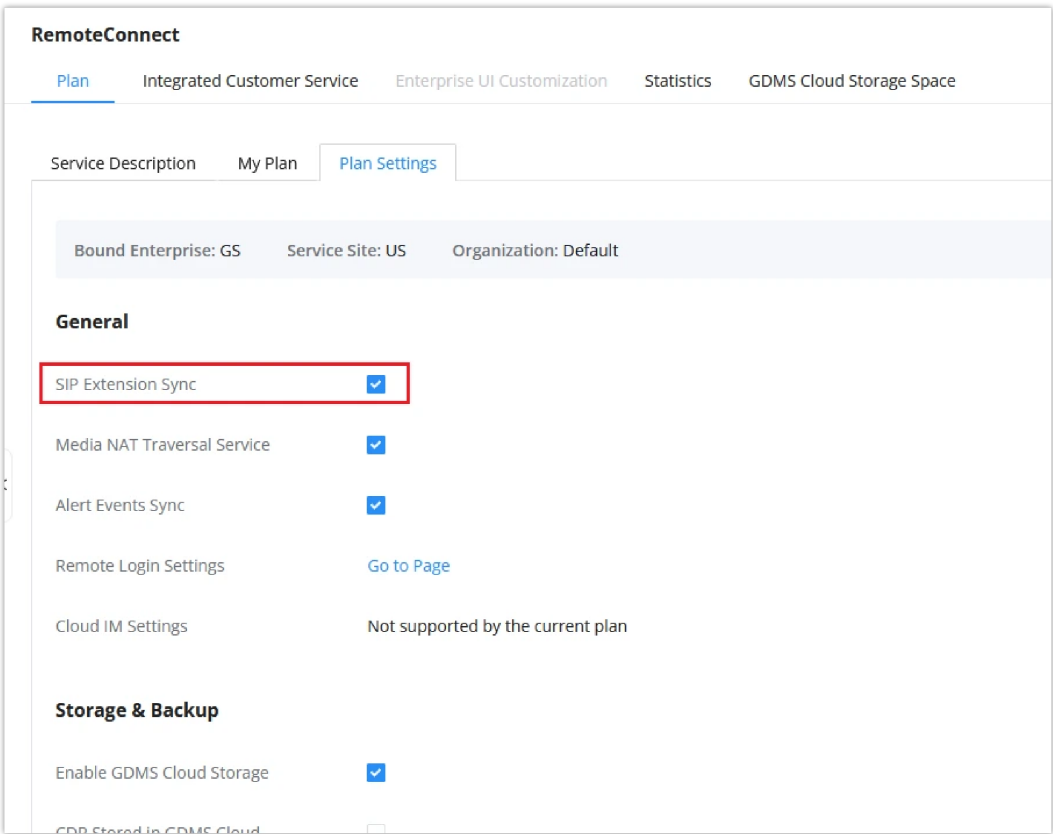
Once SoftwareUCM has been deleted, all data of the device on GDMS will be cleared.

SOFTWAREUCM EXTENSION MANAGEMENT IN GDMS

The extension section in GDMS allows users to manage SoftwareUCM extensions and assign them to existing SIP endpoints.

SIP Extension Sync

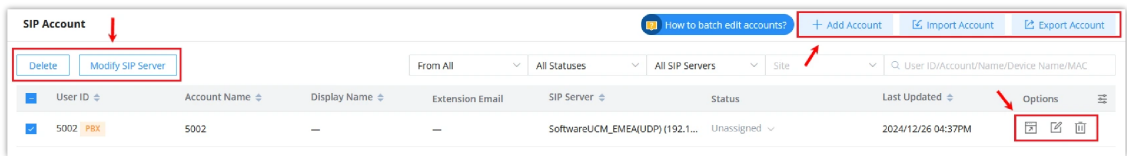
Users can enable the “**SIP Extension Sync**” option on SoftwareUCM under **RemoteConnect→Plan Settings**, which synchronizes the SIP extension created on the PBX with GDMS.



SoftwareUCM RemoteConnect Settings

SIP Account

On the **SIP Account** page, users can perform the following actions on an existing extension:



SIP Account Options

Delete	Select one or multiple extensions to delete from GDMS. Note: The extension not be deleted on SoftwareUCM's extensions page.
Modify SIP Server	Change the SIP Server of one or multiple selected extensions.
Add Account	Add a new SIP account to GDMS.
Import Account	Import one or multiple SIP account to GDMS using the corresponding provided template.
Export Account	Export an excel file containing all the SIP accounts on GDMS .
Go to PBX Web UI to edit extension	This option redirects users to the extension settings of this specific account on SoftwareUCM's Web UI.

Edit Account	Allows to edit the extension account name and assign it to a specific SIP endpoint on GDMS.
Delete Account	Delete this specific account from GDMS only. The extension will still remain on SoftwareUCM's extensions page.

SIP Account Status

The status of the SIP accounts in GDMS is summarized in the table below:

SIP Account									
How to batch edit accounts? + Add Account Import Account Export Account									
Delete Modify SIP Server									
From All All Statuses All SIP Servers Site Q User ID/Account/Name/Device Name/MAC									
☐	User ID	Account Name	Display Name	Extension Email	SIP Server	Status	Last Updated	Options	
☐	1002	1002	—	—	local_20241227110435_1735293...	Normal	2024/12/27 11:04		
☐	1003 PBX	1003	—	—	192.168.6.61:5060,c074ad453e4...	Abnormal Registration	2024/12/27 11:06		
☐	1002 PBX	1002	—	—	192.168.6.61:5060	Unassigned	2024/12/27 11:04		

Status	Description
Status	Normal: All devices using the account are registered, and the account is working normally. Abnormal Registration: 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 PBX	PBX This represents the SIP accounts are synchronized from the IPPBX device. If the user modifies the SIP accounts in IPPBX device, the updates will be synchronized to GDMS platform. The user can only edit SIP server, assign device, and cannot edit other information.
From CloudUCM	CloudUCM This represents the SIP accounts are synchronized from the CloudUCM. If the user modifies the SIP accounts in CloudUCM , the updates will be synchronized to GDMS platform. The user can only edit SIP server, assign device, and cannot edit other information.

Add SIP Account

To add a new SIP extension, click on the “Add Account” button under the SIP Account page, and fill the information mentioned below:

SIP Account > **Add Account**

Account Active ☒

Account Name

* SIP User ID

Authenticate ID

Authenticate Password

Name

Voice Mail Access Number

Outbound Proxy

* SIP Server

[Add Server](#)

Assign Device

Add New SIP Account in GDMS

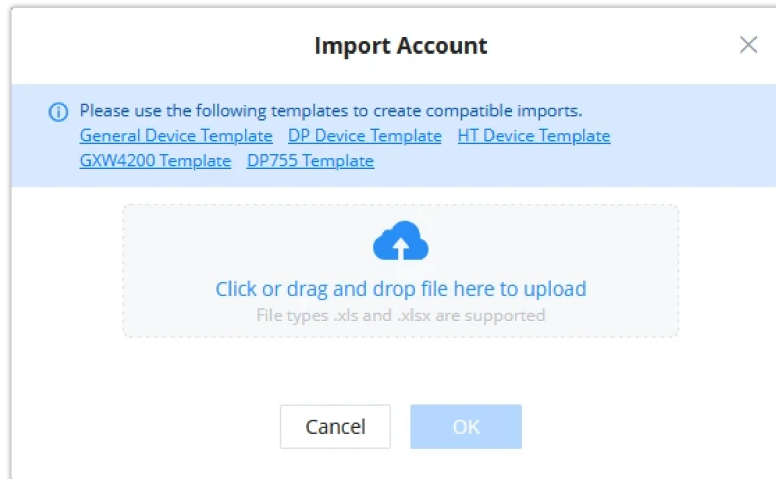
Account Active	Activates/deactivates the SIP account.
Account Name	This is a necessary option. Specifies an identity name for the SIP account.
SIP User ID	This is a necessary option. Configures user account information provided by your VoIP service provider (ITSP). It is usually in the form of digits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

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

Import SIP Account

The GDMS platform allows users to import a batch of SIP accounts and SIP servers to the system and allocate them to the devices via Excel files.

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



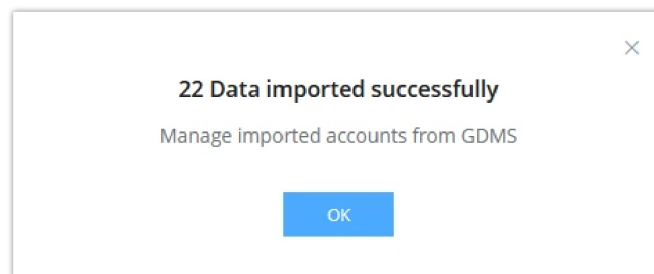
Import SIP Account Window

2. Download the SIP account templates based on the assigned devices, and fill in the information provided in the table below within the file:

Account Name	This is an optional option. Users need to set the identity name for the SIP account.
SIP Server	This is a necessary option. Users need to input the SIP server address. If the SIP server does not exist in the GDMS platform, the GDMS platform will create the SIP server in the system.
SIP User ID	This is a necessary option. Configures user account information provided by your VoIP service provider (ITSP). It is usually in the form of digits similar to a phone number or actually a phone number.
SIP Authentication ID	This is a necessary option. Configures the SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	This is a necessary option. Configures the account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purposes.
Display Name	Configure the display name of the SIP account. This option will be used for Caller ID display. The configured content will be included in the From, Contact, and P-Preferred-Identity headers of the SIP INVITE message.
Device MAC Address	(Required) Enter the MAC address of SoftwareUCM. The valid characters (0-9, a-z, A-Z) can be entered either consecutively or separated by colons (:) or hyphens (-). Examples: ● 0015651a2B3c ● 00:15:65:1a:2b:3c ● 00-15-65-1A-2B-3C

Account Index	Users need to select the account index to which the account will be allocated (e.g. Account 1 – Account 16). If the current account location has a configured account, the configured account will be replaced with the new account information.
Profile	For DP devices and HT devices only. Enter the profile that the account will use (e.g. Profile1, Profile2, etc.). If multiple different SIP servers use the same profile, the import will fail.
HS Mode	For DP devices only. Enter the HS mode for the account. Available options are “Circular”, “Linear”, “Parallel”, and “HSx”, where x can be 1 to 5.
HS1-HS5	For DP devices only. Users could configure the Line for each handset from Line 1 to Line 10. Each SIP account can be allocated to different handsets.
Port Type (FXS/FXO)	This option is valid only for HT devices . Input the port type which will be assigned to the device. Users could select FXO port type or FXS port type.
Port Serial Number	This option is valid only for HT devices . Input the port serial number which will be assigned to the device. Users could input the port serial number from Port 1 to Port 10.
Search Group	This option is valid only for HT devices . Users could select the search group between None (default), Active, and other port serial numbers beside their own.

- Once the template is filled out, drag, and drop the file to the upload window or select the file from your local device. Click on the **OK** button to confirm.
- A confirmation window will appear indicating that the SIP accounts were imported successfully. Click **OK** to close it.



SIP Account Imported Successfully

Export SIP Account

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

Allocate SIP Accounts to Devices

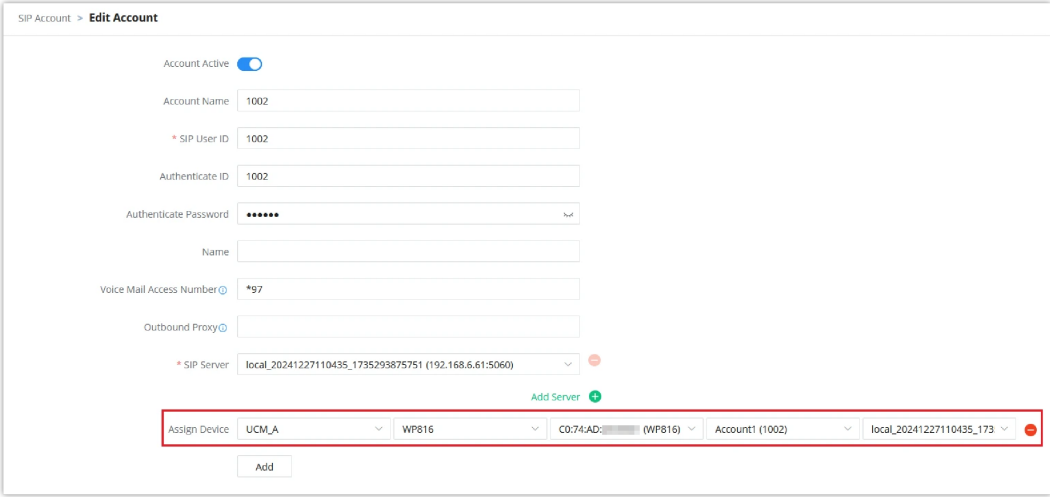
Users can allocate SoftwareUCM SIP accounts to the devices on GDMS. This can be done while editing SIP accounts, or importing a batch of SIP accounts to the GDMS platform using templates (as seen in the previous section).

Note:

Each SoftwareUCM SIP account can be assigned to multiple devices simultaneously.

To assign a SIP extension to a device in editing mode, please follow the steps below:

1. In GDMS, navigate to the **Extension→SIP Account** page and click the edit button  under the options for the desired SIP account.
2. Under the **Assign Device** section, enter the information provided in the table below:



Assign Device to SIP Account

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

Modify SIP Server

Users can modify the SIP server of one or multiple SIP accounts (e.g. Modify the SIP protocol of the SIP server from UDP to TCP)

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

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

2. Click on the **"Modify SIP Server"** button at the top of the interface.

SIP Account

Delete

Modify SIP Server

From All

	User ID	Account Name	Display Name	Extension Email
☒	5002 PBX	5002	—	—
☒	1009 PBX	1009	—	—
☒	1008 PBX	1008	—	—

Modify SIP Server

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

Modify SIP Server

When the SIP server address is modified, the new SIP server address will be assigned to the corresponding devices.

* SIP Server

Select

Cancel

Save

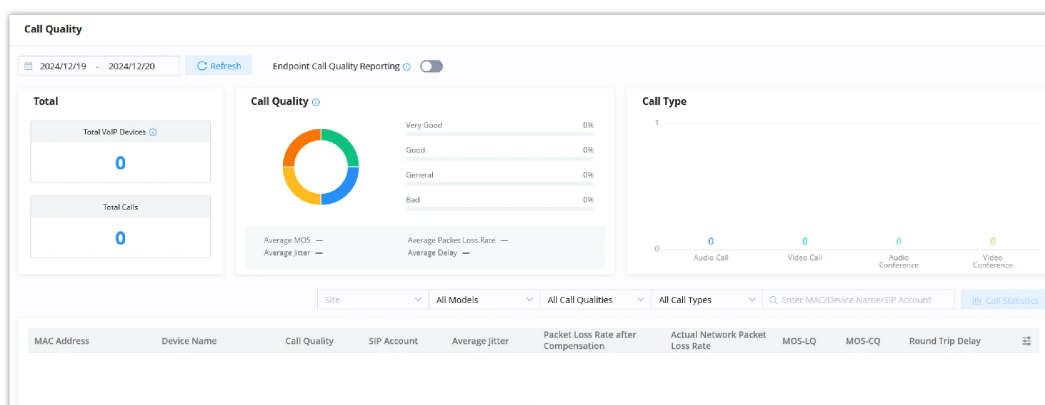
Choose New SIP Server

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

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

SOFTWAREUCM CALL QUALITY IN GDMS

The Call Quality page displays reports for calls made by SIP endpoints that are added on GDMS and registered to SoftwareUCM.



GDMS – Call Quality

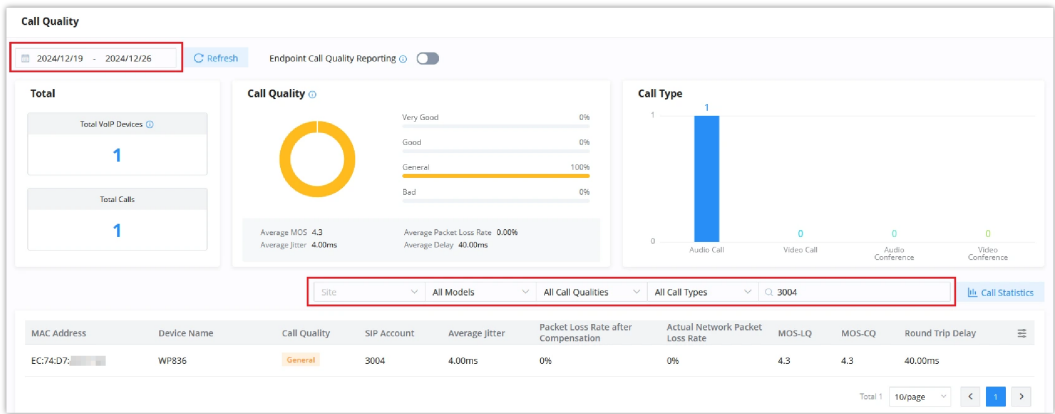
Note:

Call quality reports are only available for phones registered to a SoftwareUCM with the UCMRC Business or Enterprise plan enabled.

The call quality page shows the following information:

Total VoIP Devices	Displays the number of VoIP devices reported by the current organization.
Total Calls	Displays the number of calls reported by the current organization based on the time filter.
Call Quality	Displays the following values: ● Call Quality: The overall assessment of the call's quality, the ratings are: Very Good, Good, General, Bad. ● Average MOS: The numerical measure of the call quality on a scale from 1 to 5, with 5 being the highest quality. ● Average Jitter: The average variation in the delay of packets received during the call. ● Average Packet Loss Rate: The percentage of packets lost during transmission. ● Average Delay: The average time taken for packets to travel from the sender to the receiver during the call.
Call Type	Show the call types for the reported call history associated with the current organization. The available types are: ● Audio Call ● Video Call ● Audio Conference ● Video Conference

The GDMS platform supports filtering call quality records by date and searching for records by site, device model, call quality, call type, device MAC address, device name, and SIP Account.



Call Quality Search

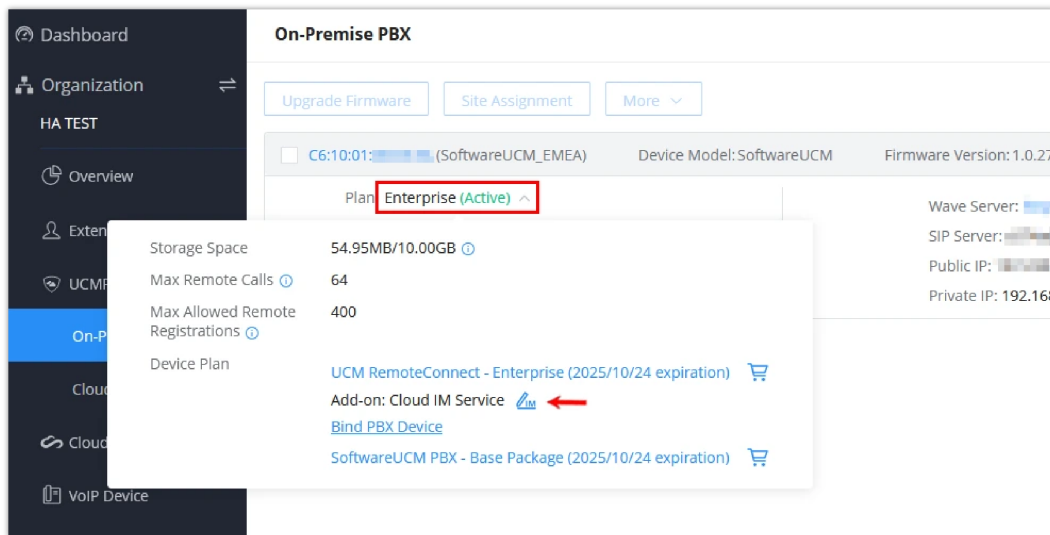
Users can toggle the “**Endpoint Call Quality Reporting**” option on this page to enable/disable call quality reports to GDMS.

SOFTWAREUCM CLOUD IM SERVICE IN GDMS

In order to benefit from SoftwareUCM’s Cloud IM service, users need to purchase a RemoteConnect plan that supports this feature. (Visit [this page](#) for more information regarding UCMRC plans)

After purchasing the UCM RemoteConnect plan which contains the Cloud IM for SoftwareUCM, the user can enable the service through GDMS. To do this, please follow the instructions below:

1. On the GDMS platform, navigate to **UCMRC→On-Premise PBX**, expand the plan information list for the desired SoftwareUCM and **"Edit Cloud IM"**.



SoftwareUCM Plan Details

2. Fill in the information mentioned in the table below:

Edit Cloud IM

Cloud IM

Region

EU Region

* Company Name for the Plan

Grandstream

* Cloud IM maximum storage space (MB)

50

Used 0MB

Available storage space is 10235 MB.

Message Read Receipt

* Chat File Limit (MB)

50

Cancel

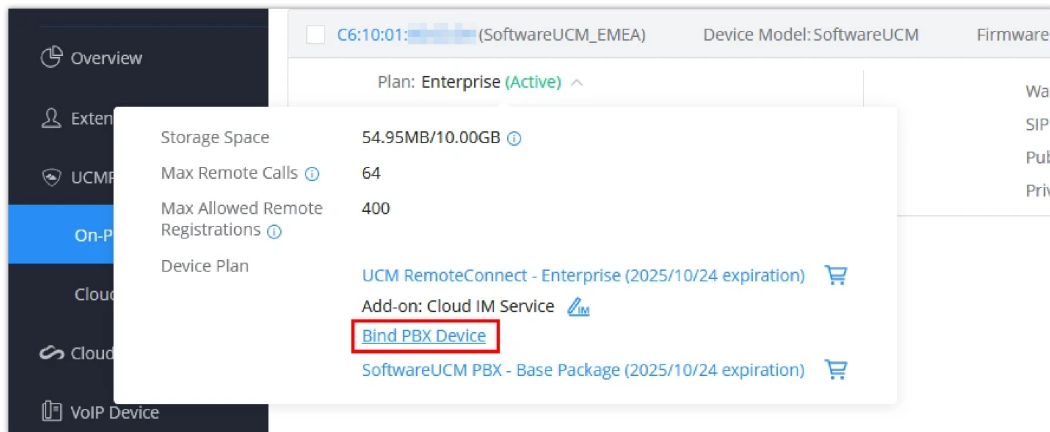
Save

Edit Cloud IM

Cloud IM	Toggle on/off Cloud IM service. Note: If the user wants to disable the Cloud IM service which is currently in use and will no longer use it, the data in the Cloud IM server will be cleared after disabling it.
Region	US Region / EU Region Note: - It is recommended to select the nearest region to the UCM device. - If the user switches to another region, the data in the Cloud IM server will be cleared.
Company Name For the Plan.	The user can customize the name of the company which will use the Cloud IM service.
Cloud IM Maximum Storage Space	The user can edit the maximum available storage space for the Cloud IM service. Note:

	• The user needs to allocate some space from the cloud storage space for Cloud IM service usage. • The configured storage space must be larger than the space currently used by the Cloud IM service and smaller than the available cloud storage space.
Message Read Receipt	When this option is toggled on, Wave clients will display that the message has been seen when the message is read by the recipient.
Chat File Limit (MB)	Set the limit of the chat file which can sent over Wave clients.

3. To bind the SoftwareUCM for the Cloud IM service, select “**Bind PBX Device**” from the UCMRC plan information.



Bind PBX Device

4. Fill in the information mentioned in the table below to bind the SoftwareUCM:

Bind PBX Device
✕

A Cloud IM plan supports binding multiple cross-region PBX devices, and can also be bound on the PBX device management platform.

Enter the department, MAC address of the device and the dial prefix ⓘ

Department1

(Softw: ▼

Dial Prefix

-

Add Device +

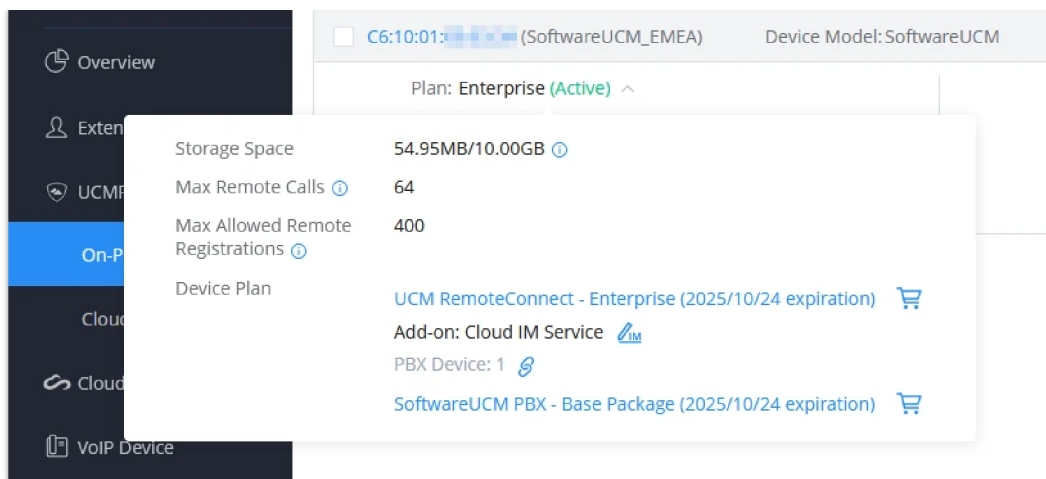
Cancel

OK

SoftwareUCM Binding Information

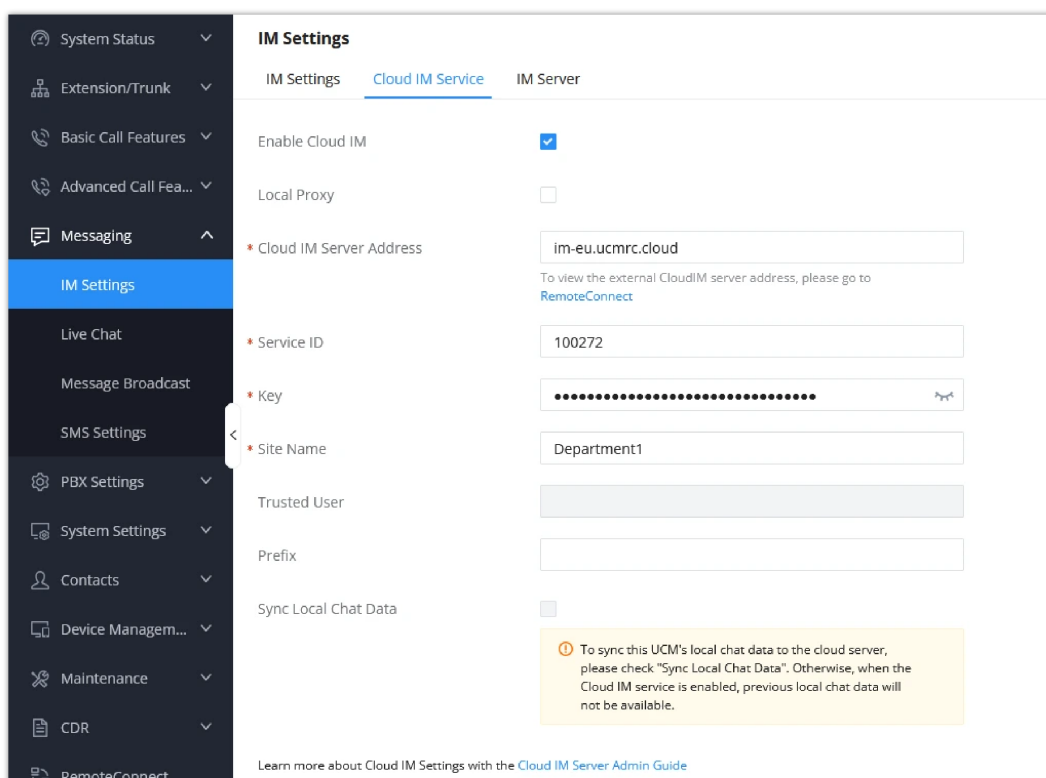
Department Name	Enter the name of the department using this SoftwareUCM so that the contact details in the Wave application can be viewed.
UCM MAC Address	Enter the MAC address of the SoftwareUCM that uses the Cloud IM service. It only supports the SoftwareUCM devices which have been associated with the GDMS platform.
Dial Prefix	Dial prefix: It must be consistent with the prefix configuration of the call trunk on the SoftwareUCM. It is not required and it supports special characters, letters and numbers.

5. Select **OK** to confirm, and verify the changes in the plan information.



SoftwareUCM Plan Information

Once these steps are completed successfully, the Cloud IM settings page on the SoftwareUCM will automatically populate with the Cloud IM server information:



SoftwareUCM Cloud IM Settings

Note:

If the SoftwareUCM Cloud IM service expires, Wave users will be unable to log in to their accounts, and the chat data will be deleted. Please make sure to renew the UCMRC Cloud IM service on time.

SOFTWAREUCM ALERT SYNC WITH GDMS

Users can synchronize certain SoftwareUCM alert events with GDMS, which are marked with the GDMS logo on the **System Events→Alert Events List** page on SoftwareUCM.

System Events

Alert Log

Alert Events List

Alert Contact

When alert events with the GDMS logo are triggered, alert information will be synced to GDMS.

Alert On

Alert Off

Email notification On

Email notification Off

HTTP notification On

HTTP notification Off

SMS Notification On

SMS notification Off

Event Name	Alert	Alert Contact				Options		
☐ SoftwareUCM plan	ON	Email	ON	SMS	OFF	HTTP	OFF	
☐ Fail2ban Blocking	OFF	Email	OFF	SMS	OFF	HTTP	OFF	
☐ Flood Attacks	OFF	Email	OFF	SMS	OFF	HTTP	OFF	
☐ Network Traffic Storm	OFF	Email	OFF	SMS	OFF	HTTP	OFF	
☐ User Login Banned	ON	Email	OFF	SMS	OFF	HTTP	OFF	
☐ Remote Login	ON	Email	OFF	SMS	OFF	HTTP	OFF	
☐ User Login Success	ON	Email	OFF	SMS	OFF	HTTP	OFF	
☐ User Login Failed	OFF	Email	OFF	SMS	OFF	HTTP	OFF	
☐ System Crash	ON	Email	OFF	SMS	OFF	HTTP	OFF	
☐ Restore Config	ON	Email	OFF	SMS	OFF	HTTP	OFF	

SoftwareUCM System Events – Alert Events List

In order to synchronize these alerts with GDMS, please ensure that the “**Alert Events Sync**” option is checked under **RemoteConnect—Plan Settings**.

RemoteConnect

Plan

Integrated Customer Service

Enterprise UI Customization

Statistics

GDMS Cloud Storage Space

Service Description

My Plan

Plan Settings

Bound Enterprise: GS Service Site: US Organization: Default

General

SIP Extension Sync ☒

Media NAT Traversal Service ☒

Alert Events Sync ☒

Remote Login Settings [Go to Page](#)

Cloud IM Settings Not supported by the current plan

Storage & Backup

Enable GDMS Cloud Storage ☒

CDR Stored in GDMS Cloud ☐

SoftwareUCM RemoteConnect – Plan Settings

Note

Please make sure that a RemoteConnect plan supporting this feature is enabled. (Visit [this page](#) for more information regarding UCMRC plans)

Configuring Alerts in GDMS

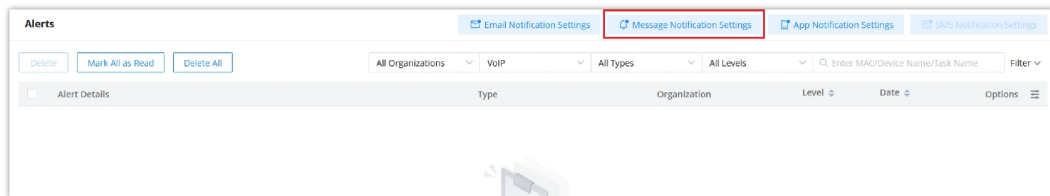
GDMS has an alert system that will trigger when certain conditions are fulfilled. There are 3 alert levels: **High**, **Medium**, and **Low**.

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 bell 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** page.



GDMS Alerts Page – Message Notification Settings

2. On the **Message Notification Settings** page, select **PBX** and fill the information included in the table below.

 A screenshot of the 'Message Notification Settings' page. At the top, it says 'Alerts > Message Notification Settings'. Below this is a blue banner with a warning icon and text: 'Please ensure the PBX device has enabled the corresponding alert options and purchased UCMRC advanced plan.' The page has three main sections: 'Organization' with a dropdown menu set to 'Default', 'Subscriber' with a dropdown menu set to 'emea_prod', and 'Notification time' with radio buttons for 'All day' (selected) and 'Custom'. Below these is the 'Alert Details' section, which has tabs for 'VoIP', 'PBX' (selected), and 'CloudUCM'. Under the 'PBX' tab, there is a list of alert types, each with a checkbox and a red circle icon: 'Alert Details', 'Device is back to online', 'Device Offline', 'PBX cloud storage space is insufficient or full', 'CPU Traffic Control', 'Local Disk Usage', 'Memory Usage', and 'Abnormal System Reboot'. All checkboxes are checked.

Message Notification Settings Page

Organization	Select the organization in question.
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected. The administrator can also add email addresses as subscribers instead of selecting the user account. This is a convenient feature when the email address is not linked to any GDMS user.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
PBX	
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: High Level: • Device is back online • Device Offline • UCM cloud storage space is insufficient or full • CPU Traffic Control • Local Disk Usage • Memory Usage • Abnormal System Reboot

- System Crash
- Fail2ban Blocking
- SIP Peer Trunk Status
- Network Disk Status
- Remote Concurrent Calls Amount Exceeds Upper Limit
- External Disk Usage
- TLS Certificate Expired
- Remote Login
- Network Port Traffic Alert
- High-frequency Outbound Call
- Flood Attack
- Outbound Trunk Call Duration Usage
- Outgoing Call Duration Limit Has been Reached

Medium Level:

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

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

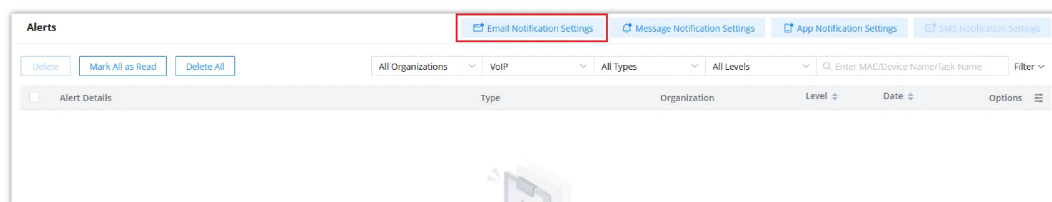
If a scheduled task fails to run, the alert notification will be sent only to the task creator.

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

Email Notification Settings

Alerts will be sent as emails to subscribers. The subscribers chosen can either be a GDMS sub-user or the administrator can directly enter an email address as a subscriber.

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



GDMS Alerts Page – Email Notification Settings

2. On the **Email Notification Settings** page, select **PBX** and fill the information included in the table below.

Organization	Select the organization in question.
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected. The administrator can also add email addresses as subscribers instead of selecting the user account. This is a convenient feature when the email address is not linked to any GDMS user.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
PBX	
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: High Level:

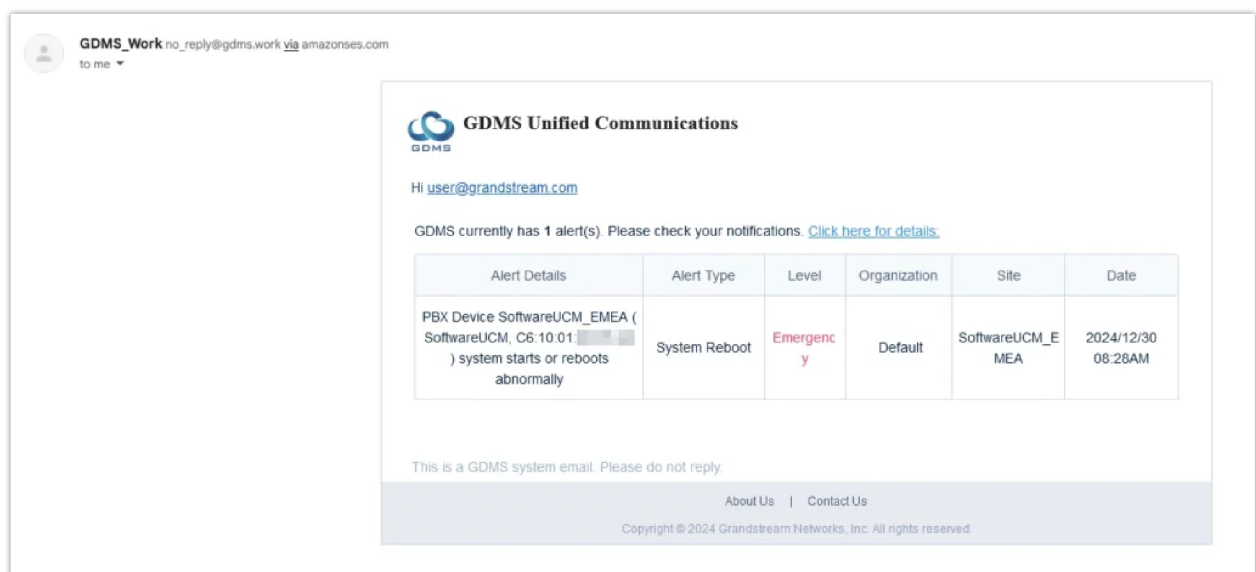
- Device is back online
- Device Offline
- UCM cloud storage space is insufficient or full
- CPU Traffic Control
- Local Disk Usage
- Memory Usage
- Abnormal System Reboot
- System Crash
- Fail2ban Blocking
- SIP Peer Trunk Status
- Network Disk Status
- Remote Concurrent Calls Amount Exceeds Upper Limit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

Medium Level:

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

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

3. With the email notifications successfully set up, users will receive an email for each configured event. The email will appear as follows:

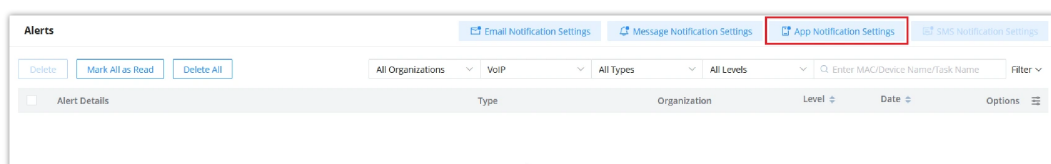


GDMS Alert Email

App Notification Settings

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

1. Select the “**App Notification Settings**” button to access the App notification settings interface.

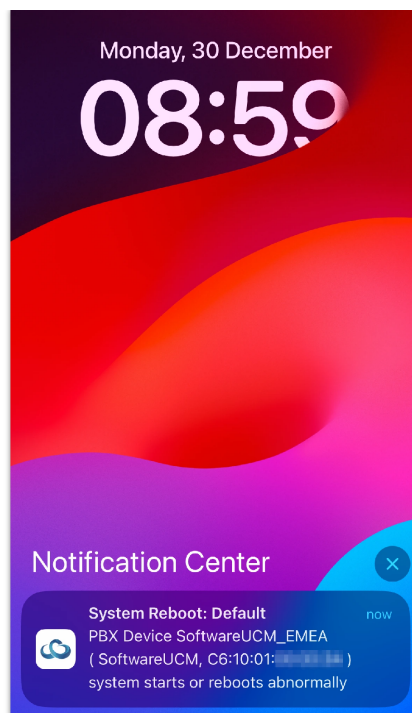


GDMS Alerts Page – App Notification Settings

2. On the **App Notification Settings** page, select **PBX** and fill the information included in the table below.

Organization	Select the organization in question.
Subscriber	Select the users that will be alerted. Only sub-users created by the current user can be selected. The administrator can also add email addresses as subscribers instead of selecting the user account. This is a convenient feature when the email address is not linked to any GDMS user.
Notification Time	Set the time for sending notifications. Only alerts that are generated during this time period will be sent as notifications.
PBX	
Alert Details	Users can specify what alerts to receive. The following alert priority levels are available: High Level: ● Device is back online ● Device Offline ● UCM cloud storage space is insufficient or full ● CPU Traffic Control ● Local Disk Usage ● Memory Usage ● Abnormal System Reboot ● System Crash ● Fail2ban Blocking ● SIP Peer Trunk Status ● Network Disk Status ● Remote Concurrent Calls Amount Exceeds Upper Limit ● External Disk Usage ● TLS Certificate Expired ● Remote Login ● Network Port Traffic Alert ● High-frequency Outbound Call ● Flood Attack ● Outbound Trunk Call Duration Usage ● Outgoing Call Duration Limit Has been Reached Medium Level: ● Failed to Run Task ● Modify Super Admin Password ● System Upgrade ● User Login Banned Note: Only the SoftwareUCM devices that have UCM RemoteConnect advanced plans can report the alert contents and send the alert notifications.

3. Once the app notifications are successfully set up, users will receive push notifications for each configured event as follows:



GDMS App Notification

SMS Notification Settings

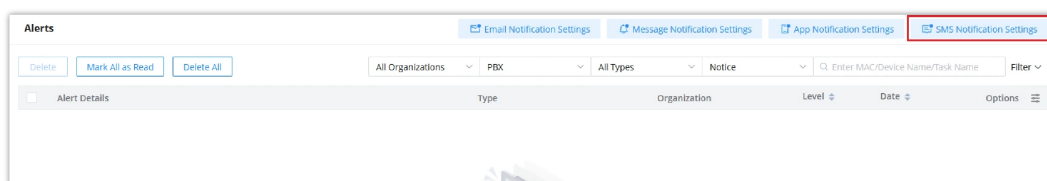
SoftwareUCMs with UCMRC plans can utilize the SMS Notification function to receive alert notifications. (Visit [this page](#) for more information regarding UCMRC plans)

Note:

Software UCMs with Pro plans and higher support the SMS notification feature, which is available only in the USA, Mexico, and Canada.

To configure SMS notifications, please follow the steps below:

1. On the GDMS **Alerts** page, select the “**SMS Notification Settings**” button.



GDMS Alerts Page – SMS Notification Settings

2. Choose **the organization**, set the **notification time**, and select the **alerts** to be sent via SMS. Then, enter a valid phone number and click “**Send Captcha**” to receive a verification code.

Alerts > **SMS Notification Settings**

ⓘ PBX with Pro plans and above supports the SMS notification feature (available in USA, Mexico, and Canada).

Organization: HA TEST

Notification time: ☒ All day ☐ Custom

Receiving Number: 1 United States

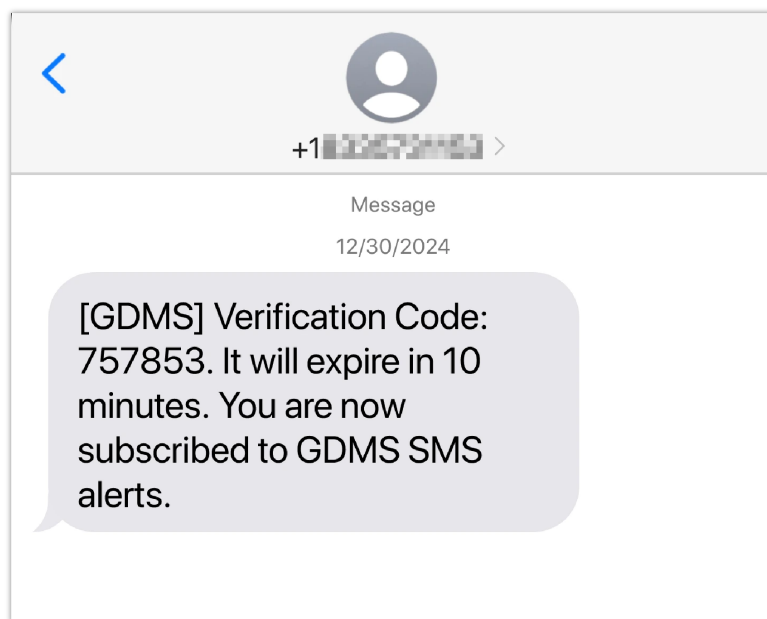
Alert Details

PBX

☒	Alert Details
☒	🔴 Device is back to online
☒	🔴 Device Offline
☒	🔴 Local Disk Usage ⓘ
☒	🔴 Abnormal System Reboot
☒	🔴 Remote concurrent calls amount exceeds upper limit
☒	🔴 External Disk Status ⓘ

SMS Notification Settings – Send Captcha

3. Check your SMS inbox, and copy the verification code received from GDMS.



SMS Verification Code

4. Paste the code into the "**Captcha**" field and click the **Save** button to apply the settings.

Alerts > **SMS Notification Settings**

ⓘ PBX with Pro plans and above supports the SMS notification feature (available in USA, Mexico, and Canada).

Organization: HA TEST

Notification time: ☒ All day ☐ Custom

Receiving Number: 1 United States 757853 Add Number +

Alert Details

PBX

Alert Details
☒ Device is back to online
☒ Device Offline
☒ Local Disk Usage ⓘ
☒ Abnormal System Reboot
☒ Remote concurrent calls amount exceeds upper limit
☒ External Disk Status ⓘ

SMS Notification Settings – Phone Number Verified

Viewing Alert Notifications

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

Users can be limited by their privileges on the alerts they can view on the Alerts page.

Alerts Email Notification Settings Message Notification Settings App Notification Settings SMS Notification Settings

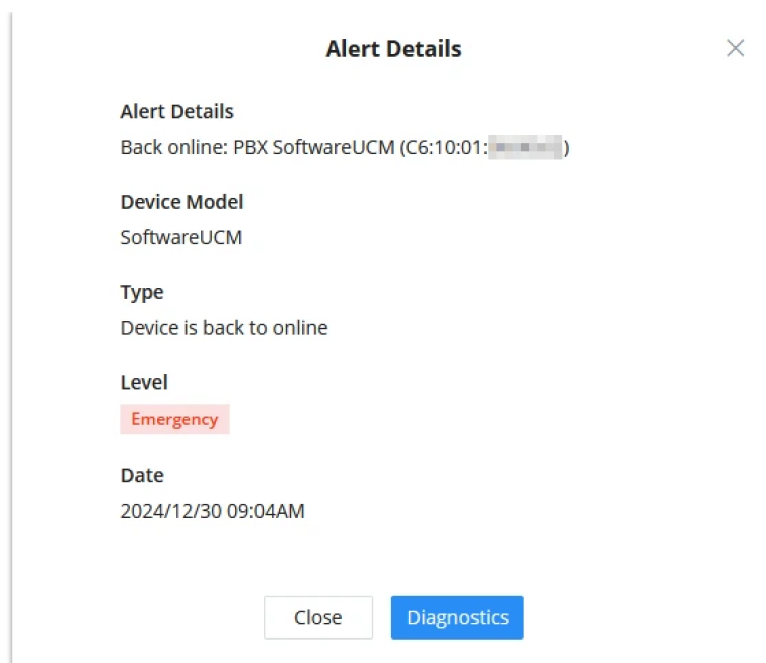
Delete Mark All as Read Delete All All Organizations All Devices All Types All Levels Enter MAC/Device Name/Task Name Filter

☐	Alert Details	Type	Organization	Level	Date	Options
☐	Back online: PBX SoftwareUCM (C6:10:01:)	Device is back to online	Default	Emergency	2024/12/30 09:04AM	 ⓘ
☐	PBX device SoftwareUCM_EMEA (C6:10:01:) system has booted up abnormally	Abnormal System Reboot	Default	Emergency	2024/12/30 08:58AM	 ⓘ
☐	Back online: PBX SoftwareUCM_EMEA (C6:10:01:)	Device is back to online	Default	Emergency	2024/12/30 08:29AM	 ⓘ
☐	PBX device SoftwareUCM_EMEA (C6:10:01:) system has booted up abnormally	Abnormal System Reboot	Default	Emergency	2024/12/30 08:28AM	 ⓘ
☐	PBX device SoftwareUCM_EMEA (C6:10:01:) offline over 5 minutes	Device Offline	Default	Emergency	2024/12/27 06:20PM	 ⓘ
☐	PBX device SoftwareUCM (C6:10:01:) offline over 5 minutes	Device Offline	Default	Emergency	2024/12/27 06:20PM	 ⓘ
☐	Back online: PBX SoftwareUCM_EMEA (C6:10:01:)	Device is back to online	Default	Emergency	2024/12/27 08:25AM	 ⓘ
☐	Back online: PBX SoftwareUCM (C6:10:01:)	Device is back to online	Default	Emergency	2024/12/27 08:25AM	 ⓘ
☐	PBX device SoftwareUCM_EMEA (C6:10:01:) system has booted up abnormally	Abnormal System Reboot	Default	Emergency	2024/12/27 08:24AM	 ⓘ
☐	PBX device SoftwareUCM_EMEA (C6:10:01:) offline over 5 minutes	Device Offline	Default	Emergency	2024/12/26 06:30PM	 ⓘ

Total 40 10/page 1 2 3 4

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 unread. Users could click on the **"Mark All as Read"** button to mark all unread notifications as "Read."
- **View Details:** Users can click the button ⓘ next to the alert notification to view its details. The red dot will disappear, indicating that the notification has been marked as "Read."

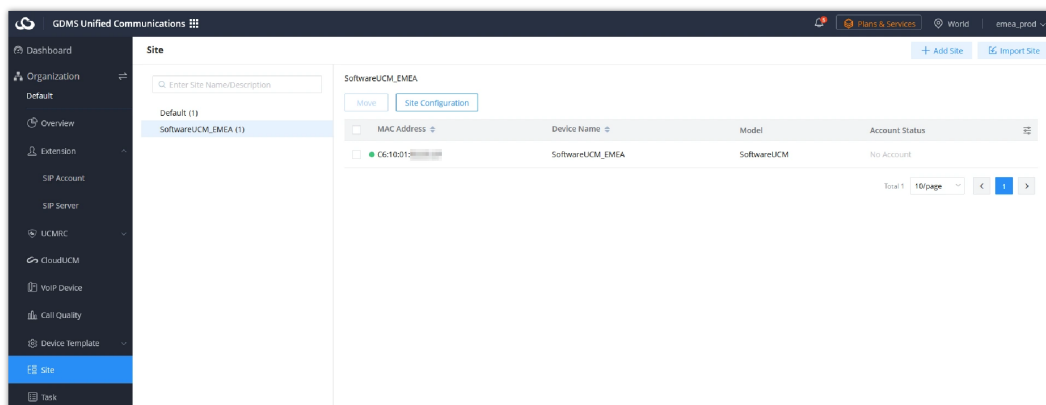


Device Alert Details

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

GDMS SITE MANAGEMENT

The GDMS **Site** page allows users to organize their devices, including SoftwareUCM, by sites and categories for easier management

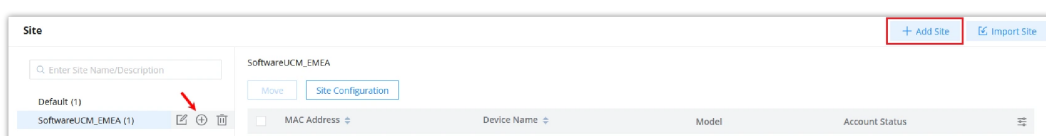


GDMS Site Page

Add Site

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

1. Click the **"Add Site"** button at the top-right corner of the **Site** page. To quickly add a site or sub-site, hover over an existing site and click the plus icon shown in the image below:



Add Site

Note:

Users can create a total of 7 different levels of sites.

2. Fill in the information mentioned in the table below:

Add Site

*

Name

Parent Site

Site

Description

Cancel

Save

Site Information

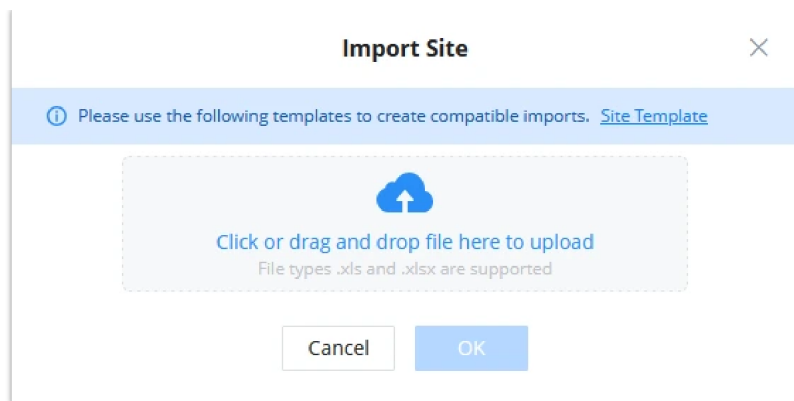
Site Name	(Optional) Select the site to which the SoftwareUCM will be assigned. The maximum allowed length is 64 characters. Notes: • If the site is under more than one level, all site levels must be included in the site name (e.g. first_level/second_level/.../new_site). • If the higher level sites do not exist, they will be created automatically • If this field is left blank, SoftwareUCM will be added to the default site.
Description	Enter the description of the site. The maximum allowed length is 256 characters.

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

Batch Import Sites

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

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



Import Site

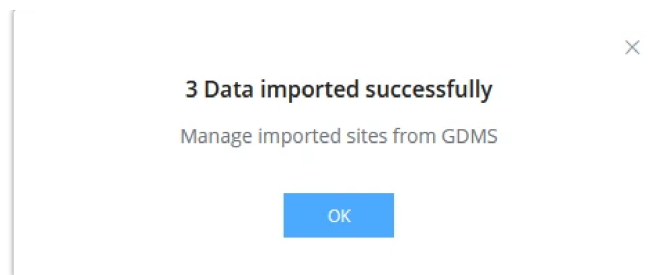
2. Click on the **Download** button to get a template that will be used to import site information.

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

Site Template

Site Name	(Optional) Select the site to which the SoftwareUCM will be assigned. The maximum allowed length is 64 characters. Notes: • 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 higher level sites do not exist, they will be created automatically • If this field is left blank, SoftwareUCM will be added to the default site.
Description	Enter the description of the site. The maximum allowed length is 256 characters.

3. Once the template is filled out, drag, and drop the file to the upload window or select the file from your local device. Click on the **OK** button to confirm the import.
4. A confirmation prompt will appear once the sites have been imported successfully.



Site Import Successful

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

Edit Site

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

1. Click on the  button next to the desired site.
2. Edit the desired fields and click on the **Save** button to finalize changes.

A white dialog box titled "Edit Site" with a close button (X) in the top right corner. It contains three form fields: a text input for "Name" (with a red asterisk) containing "SoftwareUCM_EMEA", a dropdown menu for "Parent Site" with "Site" selected, and a text area for "Description". At the bottom are two buttons: "Cancel" and "Save".

Edit Site

Delete Site

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

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

Transfer Site

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

A white dialog box titled "Move" with a close button (X) in the top right corner. It contains a dropdown menu for "Site" (with a red asterisk) showing "Site" as the selected option. At the bottom are two buttons: "Cancel" and "Save".

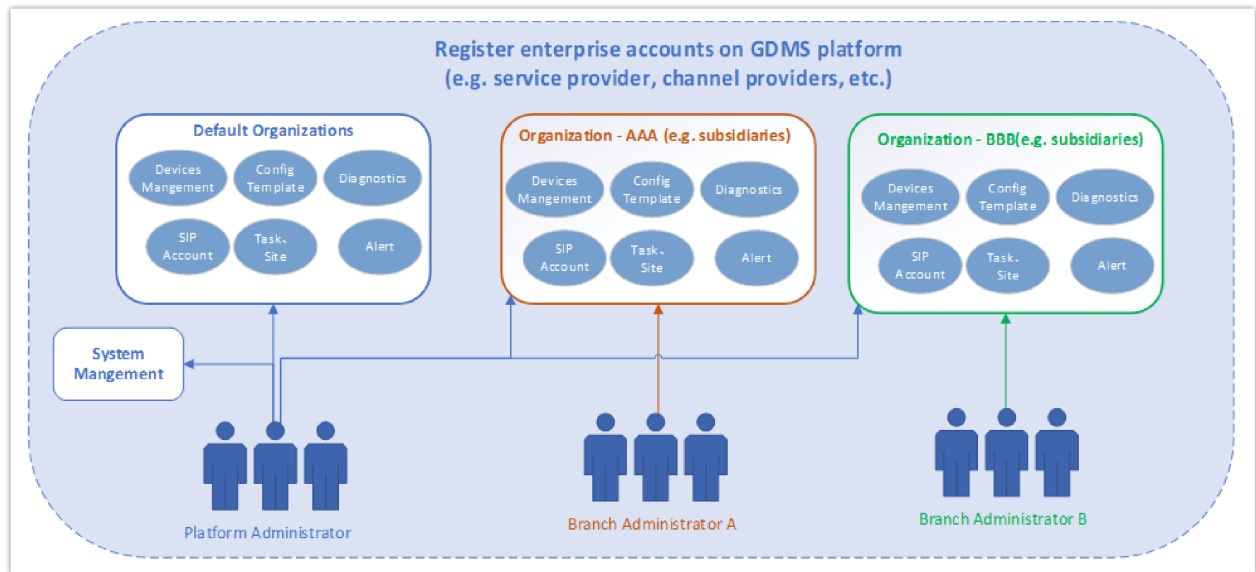
Clicking on the **Save** button will finalize the move to the specified site.

GDMS ORGANIZATION MANAGEMENT

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

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

Multiple organizations and administrators:

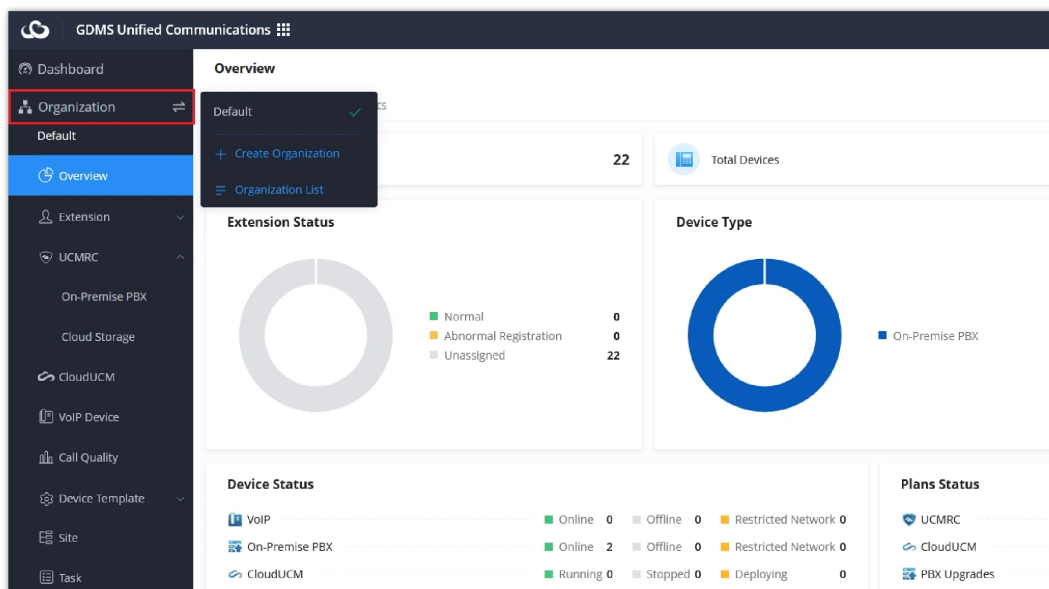


Multiple Organizations and Administrators

Switch Organization

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

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



Switch Organization

Add Organization

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

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

Add Organization

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

* Organization Name

Assign User

emea_prod

Clone Organization

Select

Description

Cancel

Save

Add Organization

Organization Name	Input the name of the organization.
Assign User	Select the users who will have permission to manage the organization.
Clone Organization	This is used to select to copy data from other organizations, the data include SIP accounts, model templates, group templates, sites, etc. When the organization is created successfully, the data under the specific organization will be copied to the current organization.
Description	Input detailed descriptions of the organization.

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

Edit Organization

Users can edit the organization’s information at any time.

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

✕

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

★ Organization Name

Assign User

emea_prod
▼

Description

Cancel

Save

Edit Organization

Delete Organization

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

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

Share Organization

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

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

Users					+ Add Organization
Users Role Organization Associated Company Account Security Settings SAML SSO					
Default Organization					Enter Organization Name/User/Description
Organization Name	Users	Description	Last Updated	Options	
Default	emea_prod	—	2024/12/30 11:35AM	✎ ✎ ✎	
EMEA	emea_prod	—	2024/12/30 11:34AM	✎ ✎ ✎	
Total 2					10/page

Users – Organization Page

Share

Organizations can only be shared between companies in the same region.

* Share Permission

Select

* Associate Company

Select

Cancel

Save

Share Organization

Share Permission	There are 2 methods of sharing permissions to another enterprise: Co-management and Authorized Management. Co-management: After sharing the organization, the user can manage the organization with the associated enterprise together. The associated enterprise can manage all devices in the shared organization and view the related data. Notes: • If the user sets to “Co-management”, the associated enterprise can manage the organization, but the associated enterprise cannot delete the shared organization. • If the user has shared the organization with one associated enterprise for management, the user cannot share the organization again with any other enterprise. Authorized Management: After sharing the organization to the associated enterprise, the user can fully authorize the management permissions to the associated enterprise for management, and the user does not have permission to manage this organization anymore. Note: • If the user sets to “Authorized Management”, the user cannot make any operation to this organization, and the organization information will be removed from the user’s “Organization” list. The data in the organization will be transferred to the associated enterprise for management. • After sharing the organization through the “Authorized Management” method, the associated enterprise can manage/edit/delete the organization. • After sharing the organization through the “Authorized Management” method, the associated enterprise can share the organization again with another associated enterprise.
Associate Enterprise	The user needs to select the associated enterprise with which the user wants to share the organization.

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

Share

Organizations can only be shared between companies in the same region.

* Share Permission

Select

* Co-management

You can manage the current organization along with the associated company.

Authorized Management

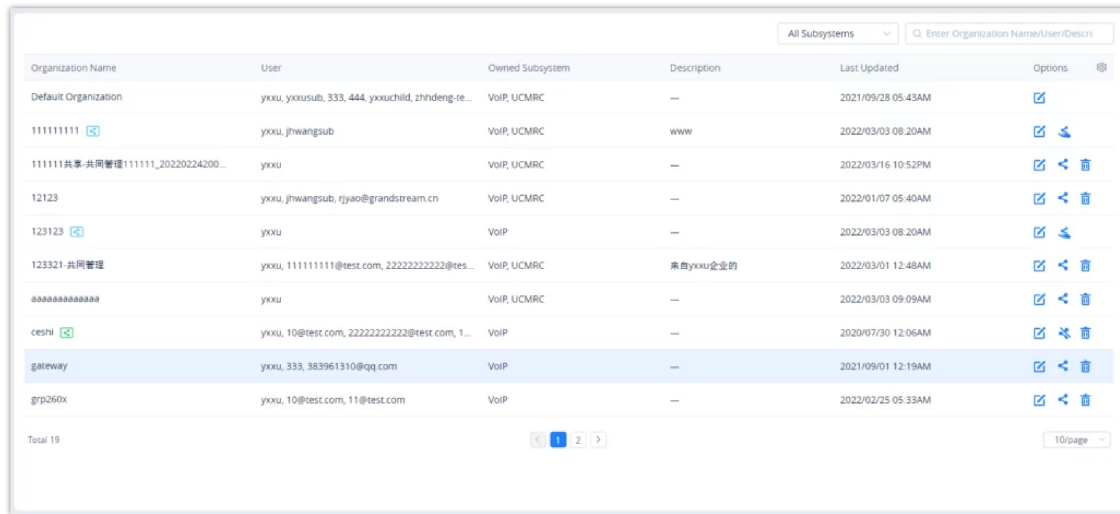
The current organization can only be managed by the authorized associated company. You are not allowed to manage it.

Share Permission

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

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

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



The screenshot shows a web interface for managing organizations. At the top, there is a search bar with the placeholder text "Enter Organization Name/User/Descr..." and a dropdown menu set to "All Subsystems". Below the search bar is a table with the following columns: Organization Name, User, Owned Subsystem, Description, Last Updated, and Options. The table contains several rows of data, including "Default Organization", "111111111", "111111111 共享-共同管理", "12123", "123123", "123321-共同管理", "aaaaaaaaaaaa", "ceshi", "gateway", and "grp26dx". Each row has an "Options" column with icons for editing, sharing, and deleting. The "gateway" row is highlighted in blue. At the bottom of the table, there is a pagination bar showing "Total 19" and "10/page".

Organization Name	User	Owned Subsystem	Description	Last Updated	Options
Default Organization	yxku, yxkusub, 333, 444, yxouchild, zhndeng-te...	VoIP, UCMRC	—	2021/09/28 05:43AM	
111111111	yxku, jhwangsub	VoIP, UCMRC	www	2022/03/03 08:20AM	
111111111 共享-共同管理11111_20220224200...	yxku	VoIP, UCMRC	—	2022/03/16 10:52PM	
12123	yxku, jhwangsub, rjyao@grandstream.cn	VoIP, UCMRC	—	2022/01/07 05:40AM	
123123	yxku	VoIP	—	2022/03/03 08:20AM	
123321-共同管理	yxku, 111111111@test.com, 22222222222@test...	VoIP, UCMRC	来自yxku企业的	2022/03/01 12:48AM	
aaaaaaaaaaaa	yxku	VoIP, UCMRC	—	2022/03/03 09:09AM	
ceshi	yxku, 10@test.com, 22222222222@test.com, 1...	VoIP	—	2020/07/30 12:06AM	
gateway	yxku, 333, 383961310@qq.com	VoIP	—	2021/09/01 12:19AM	
grp26dx	yxku, 10@test.com, 11@test.com	VoIP	—	2022/02/25 05:33AM	

Organization List – Shared Organization

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

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

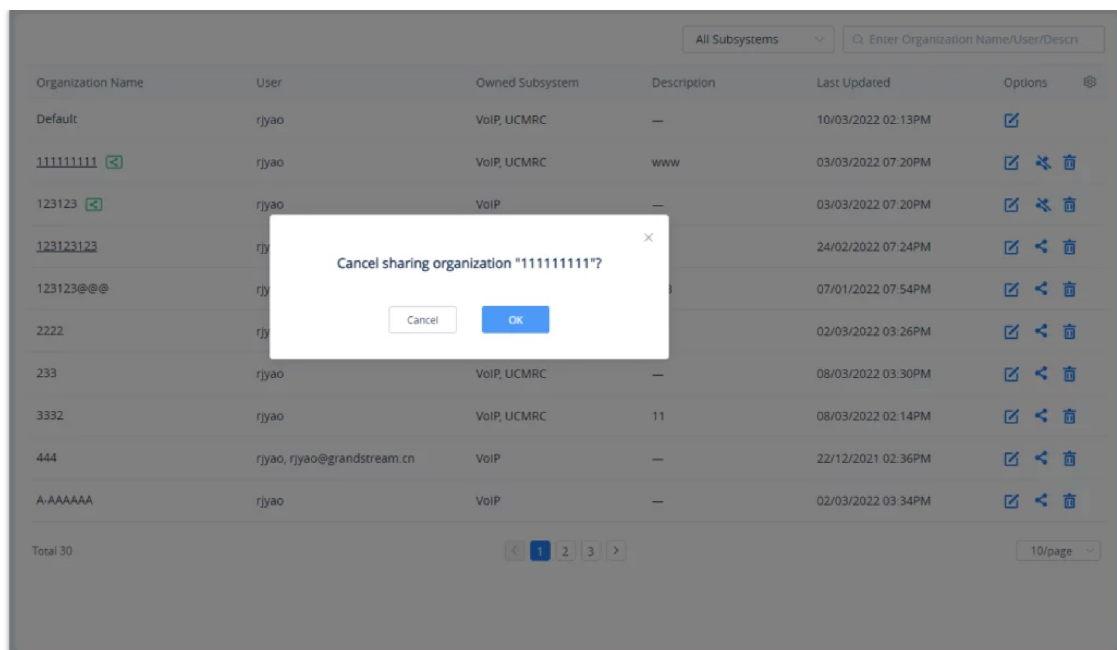
Notes

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

Cancel Sharing Organization

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

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



Cancel Sharing Organization

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

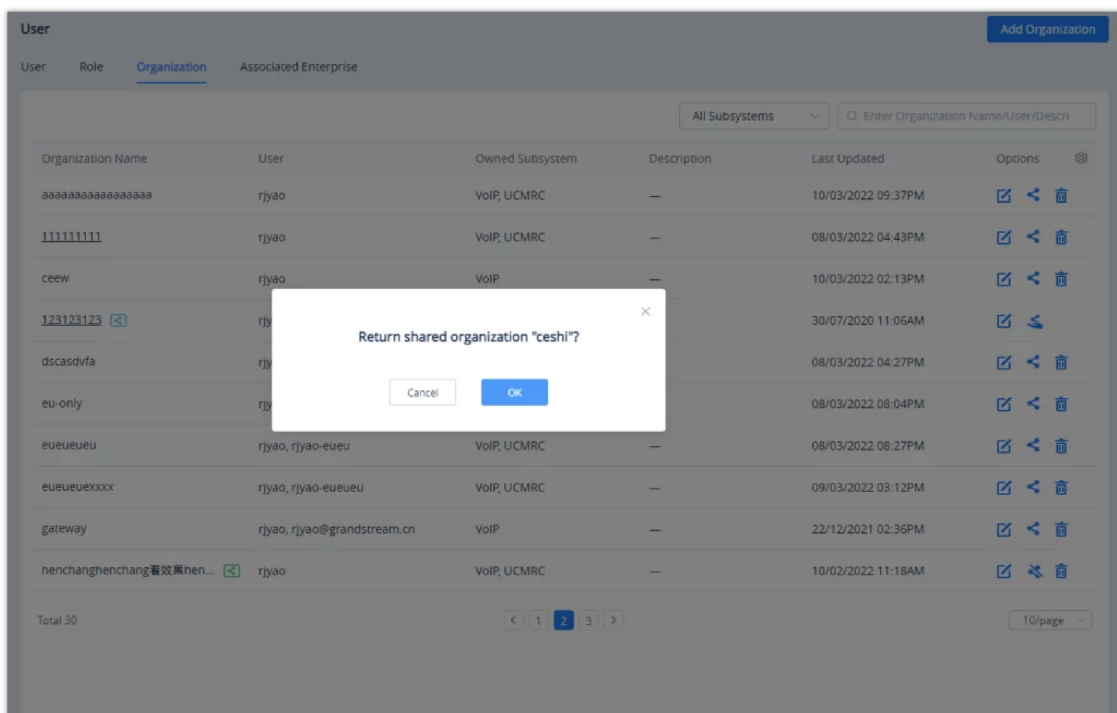
Notes

- After canceling sharing an organization, the user can share the organization again with another associated enterprise.
- The user can cancel sharing the organization only if the user sets the **"Co-management"** method when sharing the organization. If the user sets the method to **"Authorized Management"**, the user does not have any management permission after sharing the organization with the associated enterprise.

Return Organization

After receiving the shared organization, the associated enterprise can return the management permission to the user.

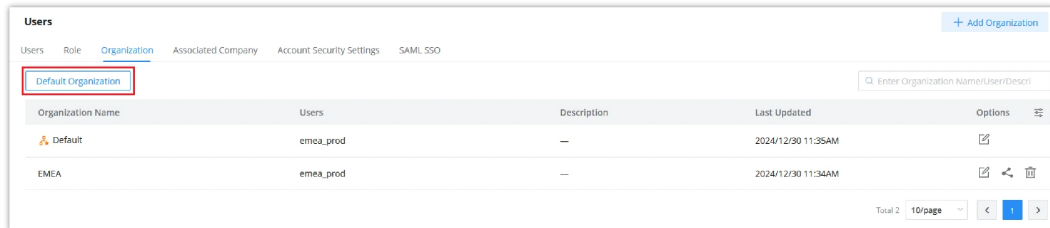
On the "Organization" list, the user can view the received shared organizations and select the organization to which the user wants to return it by clicking the button  as the screenshot shows below:



After returning the organization, the organization will be removed from the **"Organization"** list of the associated enterprise, and the associated enterprise will lose the management permission of the organization.

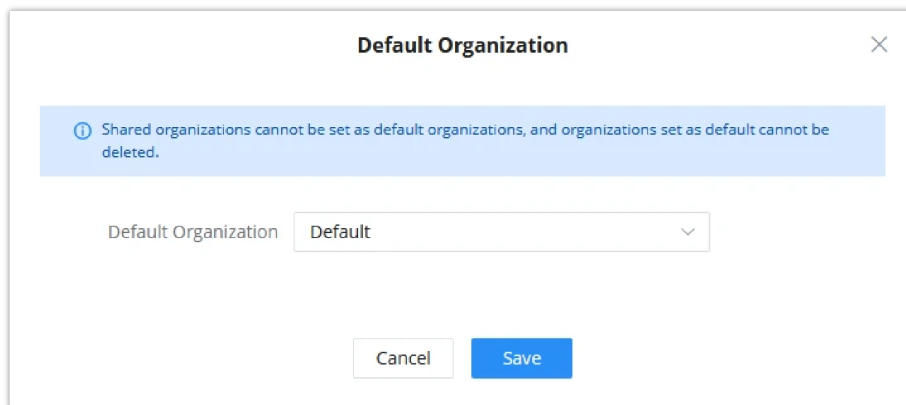
Default Organization

The user can select one organization to be the default organization. This organization will be selected by default when logging into the GDMS platform or when adding a new device. To set a specific organization as the default organization, please navigate to **Users→Organization**, the click on the button **"Default Organization"**.



Users – Organization Page

Then from the list of organizations, please choose the organization that you want to make as the default organization.



Default Organization

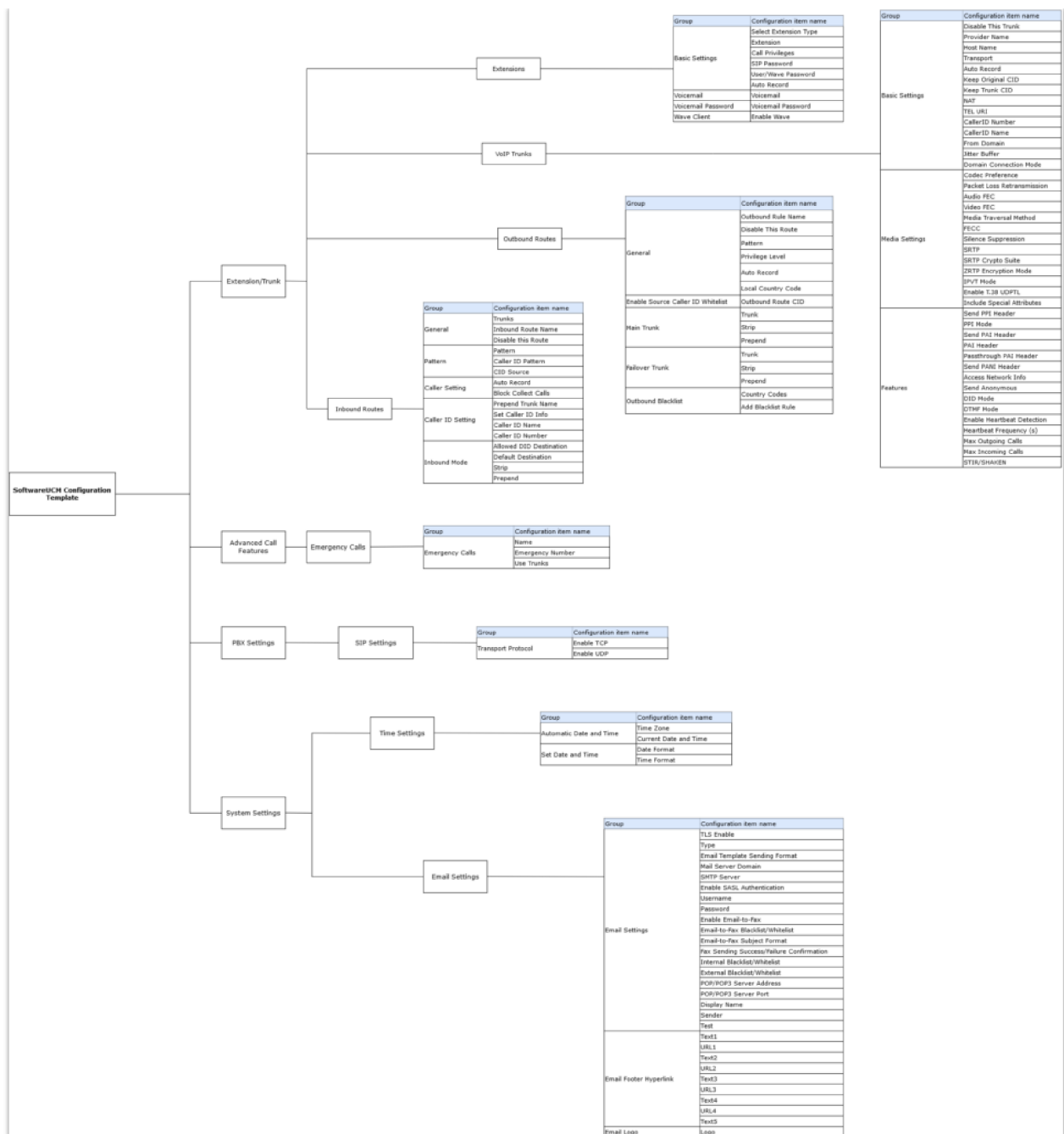
PROVISIONING SOFTWAREUCM THROUGH GDMS

SoftwareUCM supports configuration provisioning via GDMS, enabling users to configure a single SoftwareUCM instance or perform batch configurations using predefined templates to ensure consistency and increase efficiency.

This section describes in detail how SoftwareUCM leverages GDMS to facilitate efficient configuration provisioning for both individual devices and large-scale deployments.

Configuration Parameters

To give users a better understanding of the configuration possibilities, the following diagram outlines the key configuration parameters available in GDMS for SoftwareUCM.



SoftwareUCM Configuration Template Parameters

Creating SoftwareUCM Configuration Templates

SoftwareUCM supports provisioning using two types of templates:

Model Template

In order to add a SoftwareUCM Model template, please follow these steps:

1. Go to **Organization** → **Device Template** → **By Model** and click on [+ Add Model Template](#)
2. Enter a name for this template and select SoftwareUCM from the Model list.

Add Model Template

* Name
Configuration1

* Model
Select

- HT814V2
- HT818
- HT818V2
- WP820
- DP755
- GRP26X1
- CloudUCM
- SoftwareUCM**

Cancel Save

Adding New SoftwareUCM Model Template

- Choose whether to automatically push this template to a specific site, all sites or none. Users can also add a description for this template (optional).

Add Model Template

* Name
Configuration1

* Model
SoftwareUCM

* Auto Provision to Devices in

☒ All Sites ☐ Select Site ☐ None

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

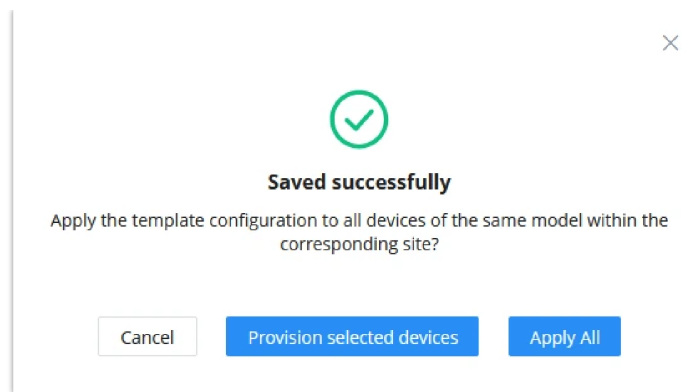
☐ Remember current selection

Description

Cancel Save

SoftwareUCM Auto Provisioning Sites

- Configure the model template parameters and click **Save**. A prompt will appear, confirming the change and offering the option to push the configuration to the entire site or to specific devices.



Success Prompt

Group Template

Users can configure a group of SoftwareUCM instances and apply settings to the entire group simultaneously by following the instructions below:

1. Under **Organization** → **Device Template** → **By Group**, click on [+ Add Group Template](#)
2. Name the group and choose the SoftwareUCM from the **Type** drop-down list. Writing a description is optional.

Add New SoftwareUCM Group Template

3. Select the target devices by checking the boxes or by entering their MAC Address.

Select Group SoftwareUCM Devices

4. Configure the group template parameters and select **Save**. Once this is done, the configuration template will be pushed to all the devices in the group.

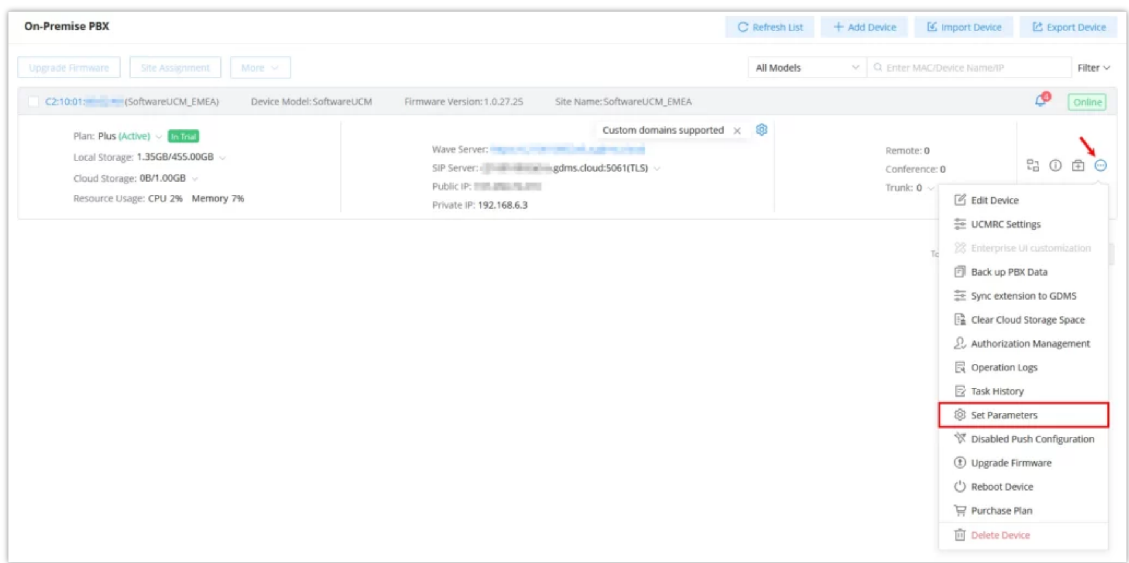
Pushing Configuration for SoftwareUCM

There are several methods available for users to push configurations to SoftwareUCM. This section will explain each method in detail, but first, it is important to highlight some important notes.

- All checked parameters on the configuration page will be pushed to the SoftwareUCM device, overwriting its local configuration.
- If a required configuration parameter fails (e.g. invalid voicemail password), the configuration will be considered unsuccessful.
- If a restart is needed, it will be performed immediately.
- When using a configuration template for a new SoftwareUCM, the setup wizard will still appear upon the first login and cannot be skipped.

Setting Parameters for a single SoftwareUCM

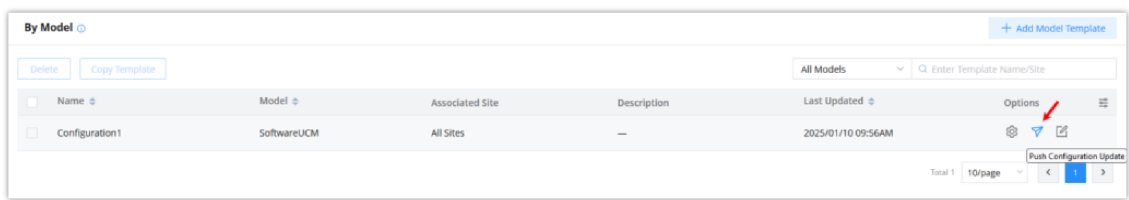
Users can edit the configuration for a single SoftwareUCM by going to **Organization → Device Template → Options** and selecting **Set Parameters**.



SoftwareUCM Set Parameters

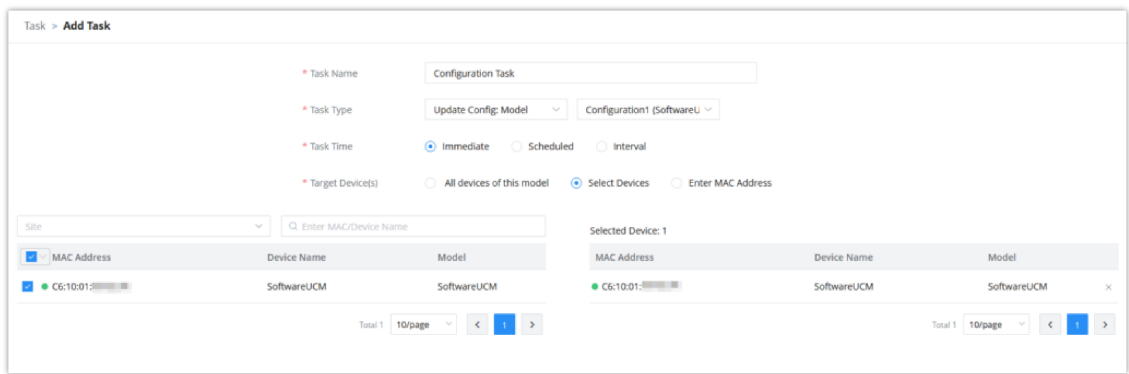
Configuring Multiple SoftwareUCM Devices

It is possible to manually push model configuration templates or group configuration templates to multiple SoftwareUCMs. This can be done by clicking on the **Push Configuration Update** icon that can be found under **Organization → Device Template → By Model/By Group**.



SoftwareUCM Push Configuration Update

Users can also manually create tasks to push model or group configuration templates. These tasks can be applied immediately, scheduled for a later time, or set at specific intervals.



SoftwareUCM Provisioning Task