CipherLab
User Guide

ReMoCloud

For Android 6.0 or later with GMS Certificated

RS31
RS35
RS36
RS51
HERA51
RK25
RK26
RK95

Version 1.17

CIPHERLAB

CIPHERLAB CO., LTD.

Website: http://www.CipherLab.com

RELEASE NOTES

Version	Date	Notes
1.17	Apr. 15th, 2024	· Add **Section 2.7** "Advanced Settings". · Add **Section 3.3** "Zero-touch Enrollment". · Update **Section 5.3** "Device Information". · Add **Section 5.3.2** "File Management" and **3.2.3** "Device Logs". · Remove Section **5.2.6 Upload Log**. · Add **Section 5.4.5** "Enable Webkey Remote Control (Selected)", **5.4.6** "Enable Webkey Remote Control (All)", **5.4.7** "Device Transfer", and **5.4.8** "Assign Geofence Setting" · Add **Section 7.2.4** "Account Sharing". · Update figures.
1.16.1	Nov. 9th, 2023	· Revise **Section 2.4.1** and **2.5.1** and add **Appendix V.**
1.16	Aug. 17th, 2023	· Update all chapters and the related figures · Add **Section 1.3.3** "ReMoCloud Online Support," **section 1.3.5** "Logout Timer," and new section "Site" to **Chapter 6** "Group Management". · Revise Appendix III. · Add Appendix IV.
1.14	Nov. 24th, 2022	· Update all chapters and the related figures. · Add **Section 5.3.1** "Push Notification," **section 5.3.3** "Enroll by pre-User Defined," **section 5.3.9** "Sync with Google," and **section 5.3.11** "Search Box & Quantity per Page" to **Chapter 5.3** "Device Setting Buttons". · Delete **Appendix III** "Create URL of ADC.zip on Google Drive" · Modify **Section 9.3.2** "Create a ZIP file & URL".
1.13	Aug. 22nd, 2022	· Update figures. · Update all chapters. · Modify 1.1 **Section 1.1.5** "Forget Password". · Add the description about CAI Service.
1.10	March 15th, 2022	· Update Feature of Introduction. · Add new section "Important Notice" to **Section 1.1.2** "Log on to Bind ReMoCloud Account with Managed Google Play Account". · Add new section "Overview" to **Chapter 6** "Sub Account". · Add new section "Child Account Enroll Page" to **Section 6.3.1** "Login". · Modify **Section 6.2** "Sub Account Management (Only Available for Parent Account) " & **Section 6.3** "Child Account View. · Update **Section 9.5** "License Information". · Update all the related figure.

1.09	Jan. 25th, 2022	·	Update **Section 1.1.2** "Log on to bind ReMoCloud Account with Managed Google Play Account".
		·	Add new section "Two-factor Authentication" to **Section 1.1** "Login for the First Time".
		·	Update the description about "Release Note" of **Section 1.3.1** "Header Navigation Buttons".
		·	Update the brief introduction of **Chapter 9** "Edit Account".
		·	Add new sections "Google Key" & "License Information" to **Chapter 9** "Edit Account".
		·	Update all the related figure.
1.08	Jan. 5th, 2022	·	Update "Issue Report and Suggestion" to **Section 1.3.1** "Header Navigation Buttons".
		·	Update "Profile Edit Time Overview" to **Chapter 2** "Dashboard".
		·	Add the description about "Filter Devices" to **Section 3.3.2** "Assign a Profile to a Device".
		·	Add the description about "Remote Control" to **Section 3.5.1**
		·	"Functionality," **Section 5.4** "Device Management," and **Appendix III**.
		·	Update all the related figures.
1.0.7	Dec 9th, 2021	·	Add "Release Note" to Help part of **Section 1.3.1** "Header Navigation Buttons".
		·	Add "App" to **Section 1.3.2** "Main Menu (Sidebar Menu)".
		·	Add description about "CipherLab Profile Information" & "Device Policy" to **Section 3.2.1** Add a Profile
		·	Add description about "App Auto Update Mode" to **Section 3.5.2** Permission, Appication, & Bluetooth
		·	Add description about password visibility of Wi-Fi Setting to **Section 3.5.4** Network
		·	Add description about "CipherLab Home Clear Cache Application Settings" to **Section 3.5.5** Lock Task
		·	Add "Validity" and "Renew" to **Section 4.1** Prerequisite.
		·	Update "Default Wi-Fi Setting" to **Section 4.1** Prerequisite.
		·	Update the enrollment process of **Section 4.2** and **Section 4.3**.
		·	Add new section "Introduction of Monitor" to **Chapter 5** Monitor
		·	Update **Section 5.2** Preset/ Add/ Delete/ Assign Group
		·	Add new section "Enroll by Pre-group" to **Section 5.2** Preset/ Add/ Delete/ Assign Group
		·	Add description about "Move/ Show/ Hide Column" to **Section 5.4** Device Management.
		·	Add description about "Schedule Report" to **Section 5.4.2** Device Setting Buttons.
		·	Revise the description about "Report" to **Section 5.4.2** Device Setting Buttons.
		·	Update **Section 8.1.2** Other Settings.
		·	Update **Section 8.3** CipherLab ADC Module.

1.0.7	Dec 9th, 2021	·	Add new section "CipherLab Profile information," "CipherLab Home," & "Device Policy" to **Chapter 8**.
		·	Add note to **Appendix I**.
		·	Update Appendix II.
		·	Update all the related figures.
1.0.5	March 2nd, 2021	·	Update Section 1.3 "Main User Interface Introduction".
		·	Add new chapter "Dashboard".
		·	Update Section 3.5 "Edit a Profile—Device Settings".
		·	Add description about "Keyguard Disabled Features" to Section 3.5.1 "Functionality".
		·	Add description about "Always On Vpn App" to Section 3.5.2 "Permission, Applications, & Bluetooth".
		·	Add description about how to disable Bluetooth function for Android 6 and Android 7 devices to Section 3.5.2 "Permission, Applications, & Bluetooth"
		·	Add description about "Short Support Message & Long Support Message" to Section 3.5.3 "Use Setting, Wallpaper, Time Serring, & USB".
		·	Update Section 3.5.5 "Lock Task".
		·	Remove "Compliance Rule Action" from Section 3.5.6 "Security".
		·	Add the description about "Battery Plugged Mode" to Section 3.5.6 "Security".
		·	Update the description about "Refresh Data" of Chapter 5 "Monitor".
		·	Add the description about "Reset Password" of Section 5.3.2 "Device Setting Buttons".
		·	Update "User Log" of Section 6.2.1 "Login".
		·	Add "Sub Account Help Page" to Section 6.2.1 "Login".
		·	Update the description about "Refresh Data" of Section 6.2.3 "Group Management".
		·	Add "Search Log" to Section 7.2 "Search, Sort, & Filter Logs".
		·	Add "Other Settings" to Section 8.1 "CipherLab OEMConfig".
		·	Update Section 8.3.1 "Save the Project from Android Deploy Confugurator".
		·	Add description about "Greeting Message" to Section 9.1 "Change User Information".
		·	Add the description about ADC.zip file size limit to Appendix II.
		·	Update "Remote Control the Registered Device(s)" to Appendix III.
		·	Update all the related figures.

1.0.4	Nov. 18th, 2020	·	Support RS35 Mobile Computer.

1.0.4　　Nov. 18th, 2020　　·　Support RS35 Mobile Computer.

·　Update **Section 1.1.2** "Login".

·　Update **Section 1.1.3** "Remember Me".

·　Add new section "Request Account" to **Section 1.1** "Login for the First Time".

·　Add "Issue Report and Suggestion" to **Section 1.3.1** "Header Navigation Buttons".

·　Update **Section 2.2.1** "Add a Profile".

·　Add "Delete Installed App(s) in Unmanaged Mode" to **Section 2.4.4** "Delete Apps".

·　Add new sections "Block List Apps" & "Save a Roll-back Profile" to **Section 2.4** "Edit a Profile".

·　Update **Section 2.4.7** "Device Settings".

·　Update **Chapter 4** "Monitor".

1.0.3　　Sep. 9th, 2020　　·　Update all figures.

·　Add "User Log" to **Section 1.3** "Main User Interface Introduction".

·　Add new section "Scroll Back to Top Button" to **Section 1.3** "Main User Interface Introduction".

·　Add description about filtering by Last Edit Time to **Section 2.1.2** "Sort, Search, & Filter".

·　Add new section "Copy a Profile" to **Chapter 2** "Deployment: Profile Management".

·　Add description about WildCard setting button(s) in gray to **Section 2.4.3** "WildCard Setting".

·　Add description about "Wi-Fi Setting" to **Section 2.4.5** "Device Settings".

·　Add "Reservation Date & Time" to **Section 2.5.2** "Schedule".

·　Add description about "Schedule Profie Info" and "Back Button" to **Section 2.5.2** "Schedule".

·　Update "Default Wi-Fi Setting"of **Section 3.1.1** "On ReMoCloud".

·　Add "User-Defined" to **Section 4.2.1** "Group Device List" and **Section 4.3** "Device Management".

·　Add new chapter "User Log".

·　Add new section "WebKey" to **Chapter 8** "Edit Account".

1.0.0　　July 28th, 2020　　Initial release

TABLE OF CONTENTS

INTRODUCTION

ReMoCloud is a cloud-based web system designed for enterprise users to manage CipherLab mobile computers. It provides an efficient way for controlling employees' mobile devices and enables employees to use mobile devices and applications securely. With ReMoCloud, managing your fleet of devices has never been easier. ReMoCloud offers a comprehensive suite of features designed to streamline device provisioning, enhance productivity, and fortify your data against potential threats.

FEATURES

- Supports CipherLab Android 6, Android 7, Android 8, Android 9, Android 10, Android 11, and Android 12 mobile computers with GMS certificated.
    - RS31 Mobile Computer (Android 7)
    - RS35 Mobile Computer (Android 10 & Android 11)
    - RS36 Mobile Computer (Android 12)
    - RS51 Mobile Computer (Android 8)
    - HERA51 Mobile POS (Android 8)
    - RK25 Mobile Computer (Android 7 & Android 9)
    - RK26 Mobile Computer (Android 12)
    - RK95 Mobile Computer (Android 9 & Android 12)

- Fully control your CipherLab mobile computers.
- Easy to install Apps on your enrolled devices.
- Supports multiple sub-accounts with different authorities of access and management.

Chapter 1

CHAPTER 1. GETTING STARTED

This chapter guides the users who sign in ReMoCloud for the very first time to complete registration. Also, it provides the introduction of ReMoCloud's user interface and specifies how to create the first profile for a new user.

IN THIS CHAPTER

1.1 LOGIN FOR THE FIRST TIME

1.1.1 PREREQUISITES

The requirements for logging in to **ReMoCloud**:

REMOCLOUD ACCOUNT & PASSWORD

Please contact the local sales representative for account application and fill out the request form. First, click "New account registration" on the login page to enter the request form.

ReMoCloud Login Page: https://remocloud.cipherlab.com/login

For more details about "**ReMoCloud Account Request Form**," refer to **Request Account**.

GOOGLE CHROME BROWSER, SAFARI, FIREFOX, INTERNET EXPLORER 11, OR MICROSOFT EDGE

It is highly recommended to access ReMoCloud with Google Chrome.

To download Google Chrome browser:
https://www.google.com/chrome/

MANAGED GOOGLE PLAY ACCOUNT

ReMoCloud allows users to manage Apps for their organizations through "**Managed Google Play**," the Google Play Store for enterprises. Therefore, Managed Google Play account of your organization is required. If the user needs to further manage the company's own private Apps, it is suggested to subscribe your Managed Google Play account and to bind the accounts of ReMoCloud and **Google Play Console** together.

For more information on the registration of the Google Play Developer account, refer to How to use the Play Console and Managed Google Play Account.
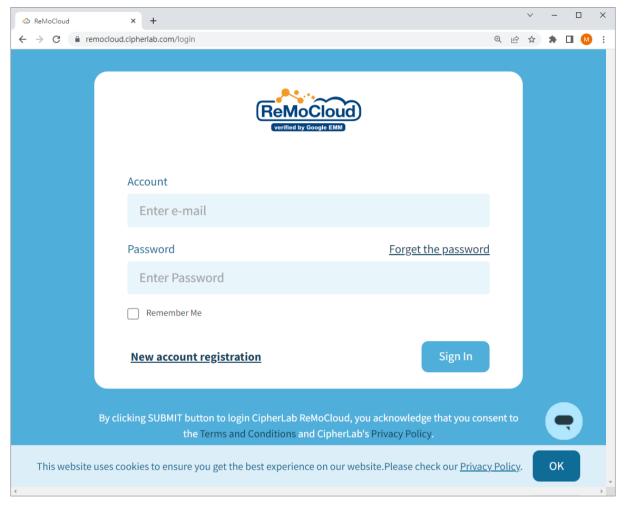
CIPHERLAB MOBILE COMPUTER

ReMoCloud supports the CipherLab mobile computers running on Android 6.0+ with GMS certification as below:

- RS31 (Android 7)
- RS35 (Android 10 and Android 11)
- RS36 (Android 12)
- RS51 (Android 8 and Android 11)
- RK25 (Android 7, Android 9, and Android 11)
- RK26 (Android 12)
- RK95 (Android 9 and Android 12)
- HERA51 (Android 8 and Android 11)

1.1.2 LOG ON TO BIND REMOCLOUD ACCOUNT WITH MANAGED GOOGLE PLAY ACCOUNT

For the first time to access **ReMoCloud**'s website (https://remocloud.cipherlab.com/login), please input your account(e-mail address) and password, and click "**Sign In**" to log in to **ReMoCloud**.

Clicking "**Sign In**" signifies the user's agreement to CipherLab's **Terms and Conditions** and **Privacy Policy**.

For more details, refer to:

▪ Terms and Conditions:

https://remocloudregister.cipherlab.com.tw/static/Terms%20and%20Conditions.pdf
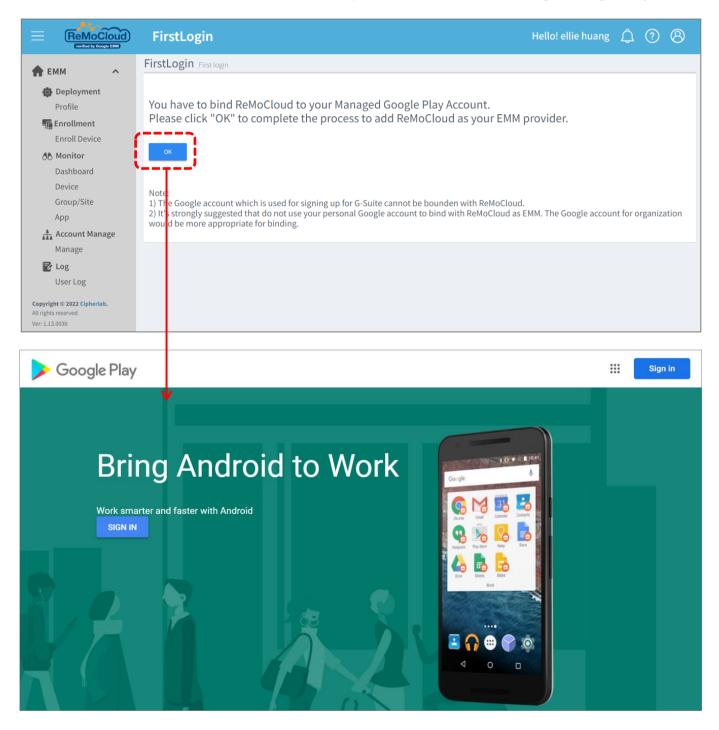

▪ Privacy Policy:

https://www.cipherlab.com/en/a4-10996/Privacy-Policy.html

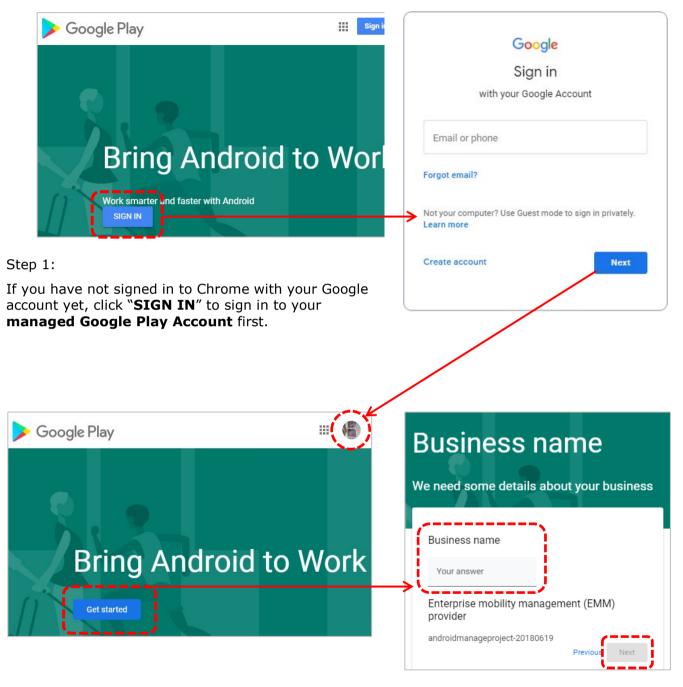Note: The password can be changed in **Edit Account** after you log in.

After logging in, the user will be required to complete binding the ReMoCloud account with the Managed Google Play account:

1) After logging in, the user needs to sign in to **managed Google Play** with their super administrator account. Click "**OK**". The page will be redirected to **managed Google Play.**

2) For those who have already signed in to Chrome with your Google account, please click "**Get Started**" to continue. Else, click "**Sign In**".

Step 1:

If you have not signed in to Chrome with your Google account yet, click "**SIGN IN**" to sign in to your **managed Google Play Account** first.

Step 2:

Click "**Get Started**" to continue the registraction process.

Step 3:

Click "**Next**" after entering the Business name.

3) In **Contact details** page, fill out the necessary information, click on the checkbox of **Managed Google Play agreement**, and click "**Confirm**" to complete the setup.

4) Click "**Complete Registration**". The page will be redirected to **ReMoCloud**.

IMPORTANT NOTICE
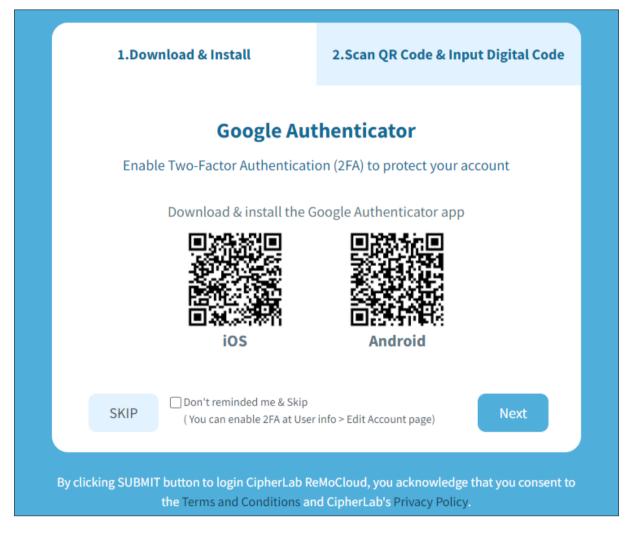
New users should pay attention to the following matters:

1) One Google Play account only allows one Enterprise Mobility Management (EMM) provider for Android management. Therefore, before using ReMoCloud as your EMM provider, please remove other EMM providers from your Google Account in advance.

2) Your Google Account used for signing up for G-Suite cannot be bound with ReMoCloud.

3) It is highly recommended that users avoid using your personal Google Account to bind with ReMoCloud as EMM. Your Google Account for organization would be more appropriate.

1.1.3 TWO-FACTOR AUTHENTICATION (2FA)

ReMoCloud offers **2FA**(**two-factor authentication**). It is the security process to enhance the access security by two different authentication factors, and to verify the user's identity. Whenever one tries to sign in to the user's ReMoCloud account, they will only gain access by providing evidence, other than the password, to verify the identity.

After completing the account binding process, the user will be asked to set up **2FA**(**Two-Factor Authentication**) the next time they log in by their ReMoCloud account and password. The pop-up window "**Google Authenticator**" appears after the user enters and submits the account and password.

Note:
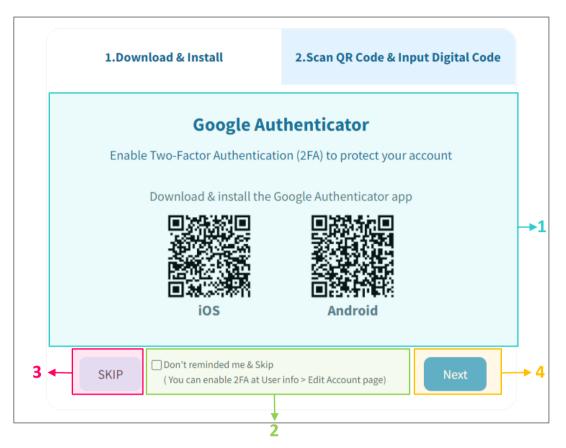
For more details about the binding process, refer to **Log on to Bind ReMoCloud Account with Managed Google Play Account**.
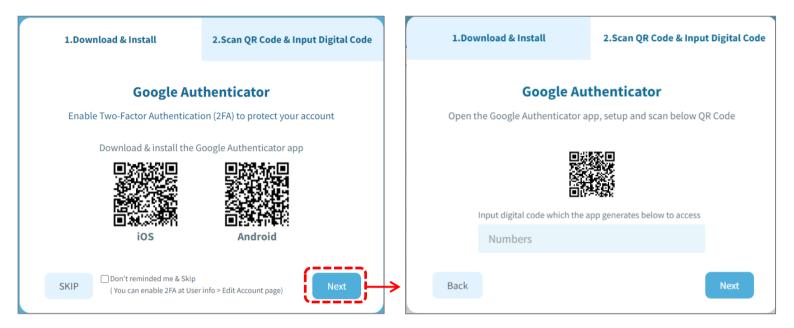
The items on the pop-up window "**Google Authenticator**" are:

Item	Description
1	The on-screen instruction about **2FA** setup and the additional authentication step to access your ReMoCloud account. Follow step 1 to download the application "**Google Authenticator**". Click the button "**Next**" at the bottom right of the popup to continue to step 2, carrying out the identity verification for this login.
2	By checking the box "**Don't remind me & skip**" on the login page, the pop-up "**Google Authenticator**" will no longer show up during the login process. This setting can be changed on **Edit Account** page.
3	Click the button "**Skip**" to close the pop-up "**Google Authenticator**" and skip **2FA** for one time. The user will directly log in to ReMoCloud with just their account and password.
4	Click the button "**Next**" to proceed to step 2 "**Scan QR Code & Input digital code**".

GOOGLE AUTHENTICATOR
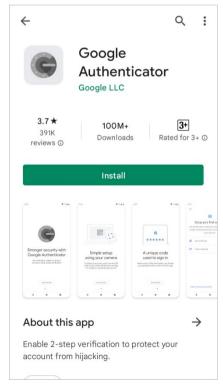
To reinforce the security of the ReMoCloud account, it is highly recommended that users enable **2FA** to protect their accounts from being compromised.

DOWNLOAD & INSTALL
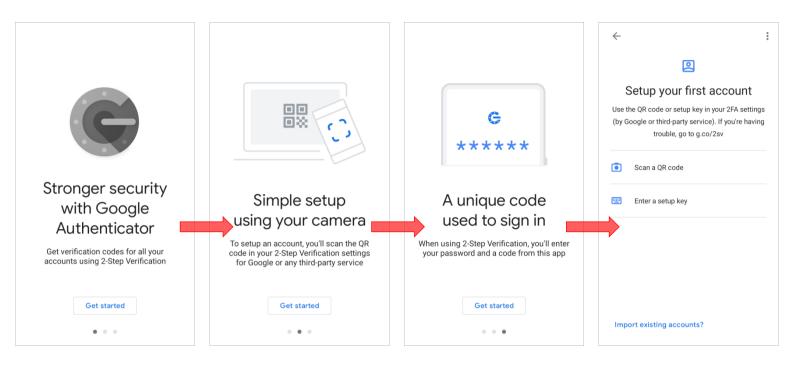
Step 1 "**Download & Install**" presents the QR code, linking to the download page of the App "**Google Authenticator**".

Use an own mobile device that is able to connect to the Internet. Scan this QR code and install "**Google Authenticator**".
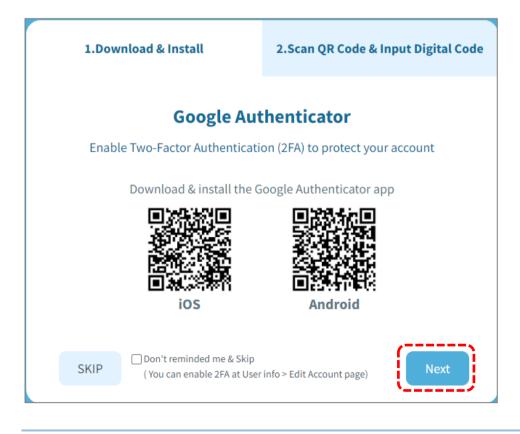
When launching the App "**Google Authenticator**," users will enter "**Setup your first account**" page after the introduction pages.

The user can proceed to step 2 "**Scan QR Code & Input digital code**" by clicking the "**Next**" button on the "**Google Authenticator**" pop-up window.

SCAN QR CODE & INPUT DIGITAL CODE
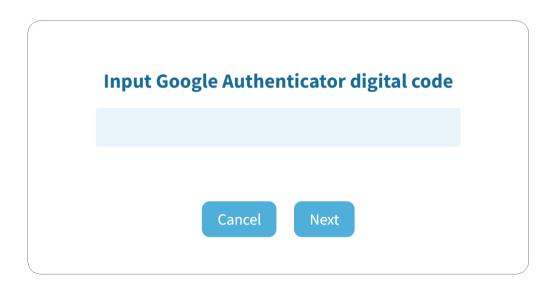
Step 2. There will be another QR code presented on the pop-up window. Please launch the App "**Google Authenticator**" and choose "**Scan a QR code**" to scan this QR code.

Make sure to turn on camera access for "**Google Authenticator**".

Enter the digital code received from "**Google Authenticator**" into the filed "**Numbers**" and submit it. For example:

So far, users have completed setting up **2FA** for ReMoCloud. Next time the user logs in, they will be required for the digital code that only belongs to the account holder. As shown:
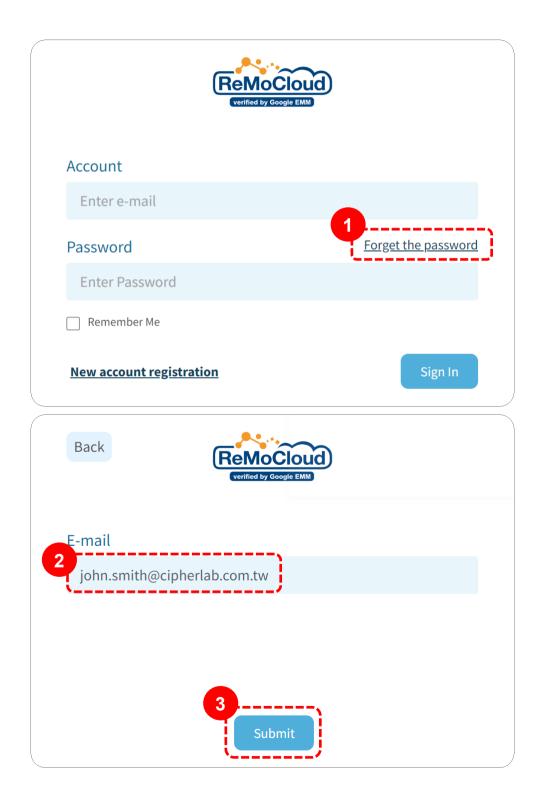
1.1.4 REMEMBER ME

If the user logs in to ReMoCloud with the box "**Remember Me**" checked, the user's account will stay signed in for 14 days with the same browser on the same PC.
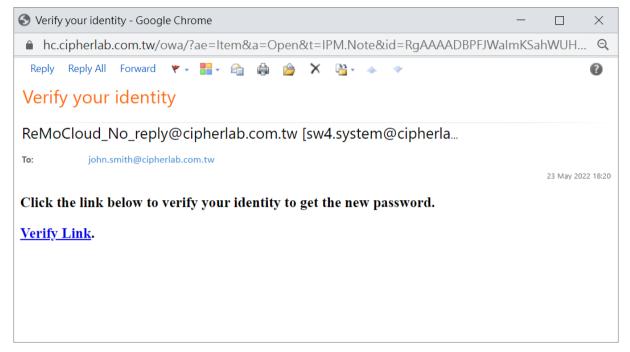
1.1.5 FORGET PASSWORD

To recover the forgotten password, click "**Forget the password**" and enter the e-mail address used for enrolling the ReMoCloud account to reset the password.

The user will receive an e-mail from ReMoCloud to confirm their identity after submitting. Follow the instruction to complete the verification. The user will receive another e-mail informing them of the new password. As shown:

Use the new password to log in. The user may change the password in **Edit Account** part after logging in.

1.1.6 NEW ACCOUNT REGISTRATION

To apply for a ReMoCloud account, click "**New account registration**" to enter "**ReMoCloud Account Request Form**" page, fill out all fields, and submit the request. The local sales representative will contact the user soon afterwards.

1.2 CREATE A PROFILE

After completing your Google account's registration, you will be redirected to the "**Profile**" page of **ReMoCloud**. You may create your first profile by clicking the "**Add**" button.

While the pop-up window "**Please input profile name**" is for creating a new profile, it offers the following functions:

Item	Description
Profile Name	Enter a name for this new profile. This field is required.
Cancel	Stop the creating process and close the pop-up window.
Submit	Click "**Submit**" to create this new profile.

Fill out the necessary fields and click "**Submit**" to proceed. A pop-up window will show up promptly to notify the user of the completion.

The newly created profile will be listed on the "**Profile**" page with its status shown as "**Inactivated**":

To activate the profile, the user should assign an enrolled device to this profile.

For more details about how to enroll a device, refer to Enroll Device.
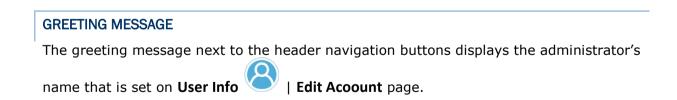
For more details about profile management, refer to Deployment.

1.3 MAIN USER INTERFACE INTRODUCTION

Whenever you log in to ReMoCloud after completing the **managed Google Play Account** settings, you will enter the "**Dashboard**" page.

Greeting Message

Header Navigation Buttons

Main Menu (Sidebar Menu)

GREETING MESSAGE

The greeting message next to the header navigation buttons displays the administrator's

name that is set on **User Info** | **Edit Acoount** page.

After the user changes the name of the administrator, the greeting message will be changed next time the user logs in to ReMoCloud as well.

1.3.1 HEADER NAVIGATION BUTTONS

There are 3 navigation buttons in the header:

MESSAGE

The "**Message**" button 🔔 shows the system messages from ReMoCloud. Click to expand the message box and read the text:

Alert [Clean Messages]

Unread   **Read**

Notification
Reboot of Device Successfully(SN :
FW120A0002230).
2022/11/23 15:26

Notification
Lock Screen of Device Successfully(SN :
FW120A0002230).
2022/11/23 15:22

The "**Message**" button displays a number 🔔¹ to show the unread message counts. When the user clicks the "**Message**" button to expand the message box, the number icon disappears at the same time.

In the Message Notification box, there are 2 sections: "Unread" and "Read".

To manage your messages, follow these steps:

1. Click "Clean Messages".

2. Select the messages from either section and click the "Delete" button to eliminate the messages.

3. Alternatively, click "Cancel" to undo the action and keep the messages.

HELP

Click "**Help**" button   to enter "**Help Page**".

REMOCLOUD TECHNICAL SUPPORT CENTER

Click on "**ReMoCloud technical support center**" to get help with any issues or problems you are experiencing with ReMoCloud.

CREATE API KEY

If you want to use an application programming interface (API) key to send your data from ReMoCloud to other system or database, please contact CipherLab Support.

For more details, refer to ReMoCloud API Service

USER INFO

Click "**User Info**" button to show the drop-down menu.

> **John Smith**
>
> Account
>
> License Information
>
> Log Out

The drop-down menu displays the user's name and three options, the link to the "**Edit Account**" page, the link to the "**License Information**" page, and "**Log Out**".

ACCOUNT

Click "**Account**" to enter the "**Edit Account**" page.

For more details, refer to "Change User Information".

LICENSE INFORMATION

"**License Information**" page lists the current status of all ReMoCloud accounts, including the admin account, the parent account, and the child account.

For more details, refer to License Information.

LOG OUT

Click "**Log Out**" to directly exit ReMoCloud and return to the login page.

1.3.2 MAIN MENU (SIDEBAR MENU)

Main Menu (Sidebar Menu)

The main menu, sidebar menu, is on the left side.

Click the menu items to enter specific pages.

EMM (ENTERPRISE MOBILITY MANAGEMENT)

As the "**EMM**" (**Enterprise Mobility Management**) provider, ReMoCloud allows the user to control devices and mobile Apps in an efficient way by:

- Deployment

Item	Description
Profile	For profile management, such as add/delete Apps.
Advanced Settings	To access proprietary functions developed by CipherLab.

- Enrollment

Item	Description
Enroll Device	To create a QR code of a profile for your CipherLab mobile computers to enroll.

- MONITOR

Item	Description
Dashboard	A collection of graphical reports that conveys profile and device information.
Device	Provides a list of enrolled devices for ReMoCloud administrators to manage and organize.
Group	For group management.
Site	For site management.
App	Provides a list of both "**User Installed Apps**" and built-in third-party apps from all enrolled devices.

- Management

Item	Description
Account Management	To create the sub-accounts that belong to the ReMoCloud account and give the child account the limited permission to access certain functions.

- Log

Item	Description
User Log	The user's operation record.

AGILITY INTELLIGENCE

Click "**Agility Intelligence**" to enter the "**User Info**" page of **CipherLab Agility Intelligence Service** (https://cai.cipherlab.com/) in a new tab.

For more details, refer to Agility Intelligence.

VERSION INFORMATION

The version information is displayed at the bottom of the main menu.

er44747

1.3.3 REMOCLOUD ONLINE SUPPORT

ReMoCloud's Online Support provides help when you have trouble with ReMoCloud's service. Through the Live Chat, you can have real-time, back-and-forth conversations with the live agent. Tell us your problem, and the live agent will get you the right help and support.

Click the [icon] icon in the bottm right corner to open the Live Chat window.

1. First, provide us with your information, including your name, company name, your country/state/zip code, telephone phone number, and e-mail address.
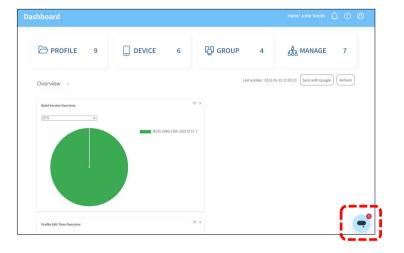
2. Tell us what we can help with.

   If necessary, click the ⬭ icon in the bottom left corner of the Live Chat window to attach files.

3. When the live agent replies, the icon displays a number to show the unread message counts.

4. The Live Chat history will be stored for 4 days.

Click the icon to view the chat history.

Note:
The live agent's office hours are from 9 a.m. to 12 a.m. UTC+8, excluding holidays.

1.3.4 SCROLL BACK TO TOP BUTTON

When scrolling down the page, the "**Back-to-Top**" button ⬆ appears in the bottom right corner and allows users to quickly navigate to the top of the page.
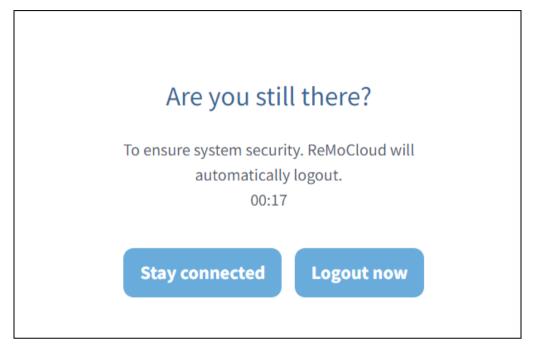
Click "**Back-to-Top**" button to return to the top of the page.

Back-to-top Button

1.3.5 LOGOUT TIMER

To ensure system security, the auto-logout timer will appear for 30 minutes of inactivity. Click "Stay connected" to close the timer, or click "Logout now" to log out of ReMoCloud.

Upon completion of the countdown, the system will initiate an automatic log out, accompanied by a notification sent to the user.

SETTINGS FOR REMOCLOUD LOGOUT TIMER

Click "**User Info**" button to show the drop-down menu. As shown:

John Smith

Account

License Information

Log Out

Click "**Account**" to enter the "**Edit Account**" page.

For "System logout time," click to expand the menu. For the options, you can select the duration of inactivity that will trigger the logout timer.

Select "None" to disable the logout timer.

Make sure to click "Save" in the top right corner to carry out the changed settings.

Chapter 2

CHAPTER 2. DEPLOYMENT: PROFILE MANAGEMENT

This chapter carries the introduction of how to create a profile, add/delete applications to profiles, manage profile device settings, and save or schedule to carry out the changed settings.

IN THIS CHAPTER

2.1 OVERVIEW OF DEPLOYMENT MAIN PAGE

On the "**Deployment**" main page, you will find "**Profile**" and "**Advanced Settings**" sections. The "**Profile**" page displays a list of profiles created by the ReMoCloud administrator, along with a search box and 5 setting buttons.

The "Advanced Settings" page provides proprietary functions developed by CipherLab. For further information, please refer to Section **2.7 Advance Settings**.

Search Box

Setting Buttons

Profile List

The functions of the 5 setting buttons are:

Setting Button	Description
Add	To create a new profile.
Import	To import a .rmc file for creating a profile with the exported settings.
Assign	To assign profiles to groups and devices.
Copy	To copy an existing profile and make changes if necessary.
Delete	To eliminate the selected profiles. Note that you can only delete the inactivated profiles.

2.1.1 PROFILE LIST

The header row items shown on the profile list deliver the following information:

Header Row Items

	Profile ∨		User-Defined	Enroll Device Number ∨	Status ∨	Version ∨	Last Edit Time ∨
☐	Creat_Profile_Test	✎		0	Inactivated	0	
☐	DTS	✎		1	Activated	18	2023/05/24 11:27
☐	HCT	✎		0	Inactivated	46	2023/02/21 17:34
☐	Profile_1	✎		2	Activated	3	2023/05/24 11:27
☐	Profile_2	✎		0	Inactivated	0	

- Profile Name:

The profile name entered in the pop-up window "**Please input profile name**" when creating this profile.

Click the columns under "**Profile Name**" to enter its profile page for further settings.

For more details, refer to "Edit a Profile: APP" and "Edit a Profile: Device Setting".

- User-Defined:

The field for the user to put a mark on the profile.

- Enroll Device Number:

The amount of the devices that apply to the profile.

- Status:

An "**Activated**" profile means that it is applied by enrolled devices, while an "**Inactivated**" profile means it is not being applied by any enrolled devices.

To activate a profile, the users should apply an enrolled device to the profile. To details about enrolling a device, refer to Enroll Device.

- Version:

The revision number of the profile. Whenever the user makes any changes to the profile, the version number increases. Blankness means that the profile is still unedited.

- Last Edit Time:

The last time the profile was modified.

2.1.2 SORT, SEARCH, & FILTER

The header row items allow the profile list to be displayed sequentially by filtering.

- Sorting:

Click the sort button ∨ ∧ at the header row to display the profiles in ascending or descending order.

- Filtering:

Click the filtering button ▼ at the header row to expand "**Filter**" field for further searching.

SORTING YOUR PROFILES

Profiles may be sorted by "**Profile Name**," "**Enroll Device Number**," "**Status**," or "**Last Edit Time**". Click the button ∨ to display the profiles in ascending order. After that, click it again to display the profiles in descending order.

- Ascending (click once) ∧

	Profile ∨	▽ User-Defined	Enroll Device Number ∧ ▽	Status ∨ ▽	Version ∨ ▽	Last Edit Time ∨
☐	Creat_Profile_Test	✏	0	Inactivated	0	
☐	HCT	✏	0	Inactivated	46	2023/02/21 17:34
☐	RounDDay	✏	0	Inactivated	6	2023/05/03 15:47
☐	test_import1	✏	0	Inactivated	1	2023/05/04 10:40
☐	DTS	✏	1	Activated	18	2023/05/24 11:27
☐	Testing	✏	1	Activated	5	2023/05/24 11:28
☐	Profile_1	✏	2	Activated	3	2023/05/24 11:27
☐	RK25	✏	2	Activated	41	2023/05/24 11:27
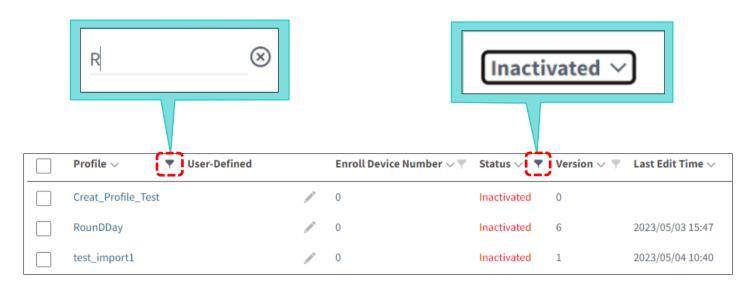
- Descending (click twice) ∨

	Profile ∨	▽ User-Defined	Enroll Device Number ∨ ▽	Status ∨ ▽	Version ∨ ▽	Last Edit Time ∨	▽
☐	Profile_1	✏	2	Activated	3	2023/05/24 11:27	
☐	RK25	✏	2	Activated	41	2023/05/24 11:27	
☐	DTS	✏	1	Activated	18	2023/05/24 11:27	
☐	Testing	✏	1	Activated	5	2023/05/24 11:28	
☐	Creat_Profile_Test	✏	0	Inactivated	0		
☐	HCT	✏	0	Inactivated	46	2023/02/21 17:34	
☐	RounDDay	✏	0	Inactivated	6	2023/05/03 15:47	
☐	test_import1	✏	0	Inactivated	1	2023/05/04 10:40	

SEARCHING & FILTERING YOUR PROFILES

"**Filter**" ▼ buttons help doing a quick search. The user may set multiple filter criteria to refine the results.

	Profile ⌄ ▼	User-Defined	Enroll Device Number ⌄ ▼	Status ⌄ ▼	Version ⌄ ▼	Last Edit Time ⌄
☐	Creat_Profile_Test	✎ 0		Inactivated	0	
☐	RounDDay	✎ 0		Inactivated	6	2023/05/03 15:47
☐	test_import1	✎ 0		Inactivated	1	2023/05/04 10:40

BY PROFILE NAME, ENROLL DEVICE NUMBER, OR VERSION

1) Click the filter button ▼ to expand "**Filter**" field.

	Profile ⌄ ▼	User-Defined	Enroll Device Number ⌄ ▼	Status ⌄ ▼	Version ⌄ ▼	Last Edit Time ⌄	▼
☐	Creat_Profile_Test	Filter ⊗	0	Inactivated	0		
☐	DTS	✎	1	Activated	18	2023/05/24 11:27	
☐	HCT	✎	0	Inactivated	46	2023/02/21 17:34	
☐	Profile_1	✎	2	Activated	3	2023/05/24 11:27	
☐	RK25	✎	2	Activated	41	2023/05/24 11:27	
☐	RounDDay	✎	0	Inactivated	6	2023/05/03 15:47	
☐	Testing	✎	1	Activated	5	2023/05/24 11:28	
☐	test_import1	✎	0	Inactivated	1	2023/05/04 10:40	

2) In "**Filter**" field, enter the keyword to make the matching profiles appear.

BY PROFILE STATUS

For the header row item "**Status**," a drop-down menu will appear after clicking the filter button . Select the preferred profile status to see the matching results.

BY LAST EDIT TIME

Click the filter button from "**Last Edit Time**" to show the drop-down menu and the datepicker for designating the date range:

1) Click the filter button ⏷ to display the drop-down menu and select the duration:

Duration	Description
None	Set for nothing.
Before	Set for an earlier duration lasts until the selected date
Specify	Set for a specific date.
After	Set for a later duration since the selected date
Between	Set for a date range from start date to end date.

2) Click the calendar button 📅 to expand the datepicker and select the date.

August 2020 ▾					↑	↓
Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	**13**	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today

After

mm/dd/yyyy 📅

For the filter "**Between**," select the start date and end date.

Between ▾

⧗ mm/dd/yyyy 📅 ⟶ **Start Date**

⧗ mm/dd/yyyy 📅 ⟶ **End Date**

3) The matching results will be displayed as shown:

Profile Name ⬍ ▼	Enroll Device Number ⬍ ▼	Status ⬍ ▼	Version ⬍ ▼	Last Edit Time ⬍ ▼
☐ Profile3	0	Inactivated	2	2020/09/01 15:50
☐ Testing	0	Inactivated	5	2020/08/30 12:00
☐ Testing_2	2	Activated	8	2020/08/28 07:26

Note:
The current date and time of the timepicker is in accord with **Time Zone's** setting on User Info page.

2.2 ADD/ DELETE/ COPY A PROFILE

On the main page of **Profile** from **Deployment**, the user may add or delete profiles.

2.2.1 ADD A PROFILE

To create a new profile:

1) Click "**Add**" on the **Profile** page.

2) In "Please input profile name" pop-up window, enter the profile name and "Submit".
Click "**Cancel**" to close the pop-up window.

3) When the profile is successfully created, a pop-up window will appear promptly to notify the user of the completion.

4) The newly-created profile will be listed on the profile list with its status shown as "**Inactivated**". The user may edit the profile by clicking the name to enter the information page.

Note:

1.To make an "Inactivated" profile "Activated," please **assign an enrolled device to this profile**.

2.For more details about profile editing, refer to "**Edit a Profile: APP**" and "**Edit a Profile: Device Setting**".

Click the profile's name to enter the "**Profile Information**" page. The default Apps are listed here. Note that the default Apps that only runs in the background will not show on the enrolled device.

▪ CipherLab OEMConfig:

A default App that helps ReMoCloud administrator configure the enrolled devices applying to the profile. It may work with "**ADC Module**" to deploy the ADC Project Settings to the enrolled devices through ReMoCloud. Also, it may work with another CipherLab default App, "**LogCollection**," to retrieve the enrolled device logs.
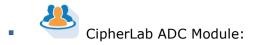
▪ CipherLab Device Health:

Checking the enrolled devices' battery health.

▪ CipherLab LogCollection:

A default App that works with "**CipherLab OEMConfig**" to upload the logs of the enrolled devices to the user's designated PC where the FTP server is installed.

- CipherLab ADC Module:

A default App that works with "**CipherLab OEMConfig**" to deploy the ADC(Android Deployment Configurator) Project Settings to the user's enrolled devices.

- CipherLab Profile Information:
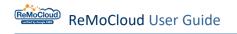
A default App that demonstrates the profile and the version the device applies to. It lists the default Apps installed on the device as well.

- Device Policy

This default App is developed by Google. It is designed to control and synchronize the Android devices managed by EMM(Enterprise Mobility Management).

The default Apps will be installed on the enrolled devices that apply to the profile after "Saved" or "Scheduled". If the profile does not include those Apps, click "**Add App**" to add them into the profile from the "**App Management**" page.

For more details, refer to **Default Applications**.
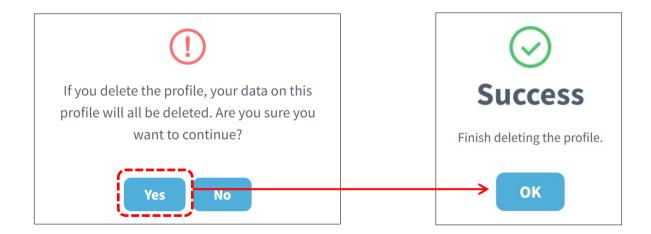
2.2.2 DELETE A PROFILE

Select the profiles and click "Delete".

A warning message appears after clicking "Delete". Click "**Yes**" to continue deleting.

Next, click "**OK**" to close the pop-up window that notifies the profile is successfully deleted.

The profile is successfully deleted as shown:

Note:

"Activated" profiles cannot be deleted.

2.2.3 COPY A PROFILE

"**Copy Profile**" is to reproduce an existing profile.

1) Click "Copy" to make the pop-up "Select a profile and input profile name" appear.

2) Select the profile for copying.

3) Enter a new name for the new profile and "**Submit**".

4) The new profile is successfully created. Click the profile name to enter and make changes if necessary.

2.3 ASSIGN A PROFILE

"**Assign**" is to designate an existing profile to the certain group or device. Therefore, the user needs to create groups in advance.

For more details about creating a group, refer to **Create a New Group**.

2.3.1 ASSIGN A PROFILE TO A GROUP OR A DEVICE

To assign a profile to groups and devices:

1) In the top left corner, click to select the profile to be assigned.

2) In the "**Group/Device**" list, the group's original assigned profile and the device's serial number will be demonstrated. Click to select a group or device.

3) Click ❮ and the selected group or device will move to the left section, suggesting it will apply to the profile you selected in step 1.

4) Click "**Save**" to finish the assignment and carry out the changed settings.

Note: The assigning process will fail if the selected group contains no device.

After completing the assigning process, the devices belong to the group will apply to the designated profile immediately. The user may check the group information by accessing "**Group**" page from "**Group/Site**" and clicking the group's name.

For more details about group management, refer to "Group Management".
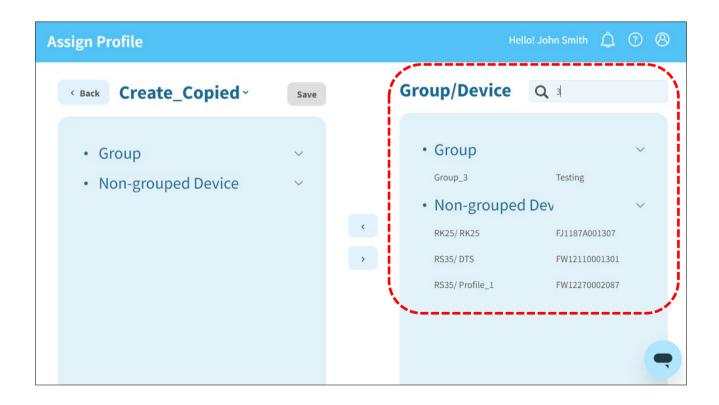
The device will apply to the assigned profile after the completing the process. Go to "**Device"** page for checking the designated devices' profile and profile status.

SEARCH BOX

On "Assign Profile" page, the search box is in the top right corner. You may enter the keyword to narrow down the matching results of groups and devices.
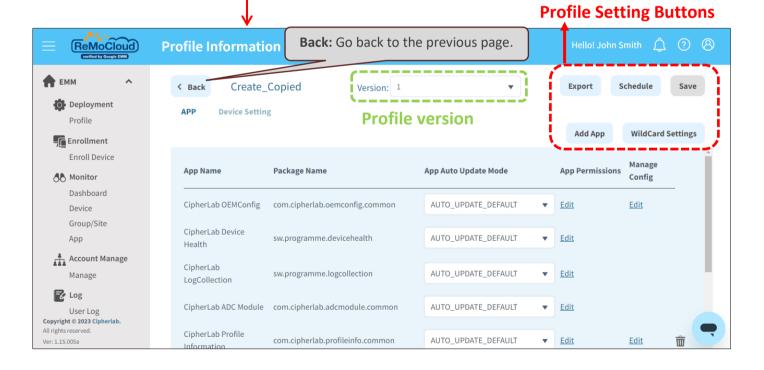
2.4 EDIT A PROFILE: APP

In "**Profile,"** click the profile's name to enter the "**Profile Information**" page for editing.

Profile Setting Buttons

Back: Go back to the previous page.

Profile version

The functions of the profile setting buttons on the **Profile Information** page are:

Button	Description
Export	To export the profile's settings into a .rmc file
Schedule	To make a plan for carrying out the profile's changed settings
Add App	To add Apps to the profile
WildCard Settings	To set multiple e-mail addresses to the e-mail App

The profile information page includes "**APP**" and "**Device Setting**" tab pages.

For "**APP**" page, you may add Apps or delete Apps from the profile.

For "**Device Setting**" page, you may change the device system's settings for the enrolled devices that apply to the profile.

▪ "APP" Tab Page:

Note:

Click the "Back" button [< Back] to return to the previous page.

▪ "Device Setting" Tab Page:

For more details, refer to "**Edit a Profile: Device Setting**".

2.4.1 ADD APPS

On "**APP**" tab page, click "**Add App**" button to enter the "**App Management**" page.

Here, you can add Apps by the mode you set from Functionality.
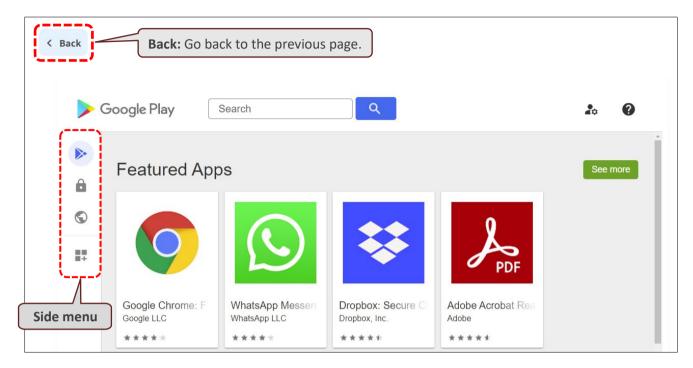

Apps added to the "**Activated**" profile will be simultaneously added to the enrolled devices that apply to the profile after clicking "Save" or "Schedule".

GOOGLE MANAGEMENT MODE

In Google Management Mode, you can add a new App from Google Play Store:
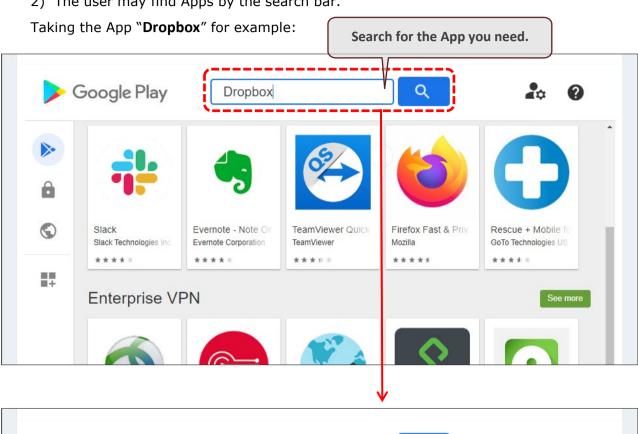
1) Click "**Add App**" button to enter the "**App Management**" page:

The side menu offers:

	Item	Description
	Search Play store	To discover or find Apps from Google Play Store.
	Private Apps	To publish private Apps. Google Play Developer account is not required. Refer to https://support.google.com/googleplay/work/answer/9146439.
	Web Apps	To create web Apps. Refer to https://support.google.com/googleplay/work/answer/9147423.
	Organize Apps	To arrange the user's approved Apps.
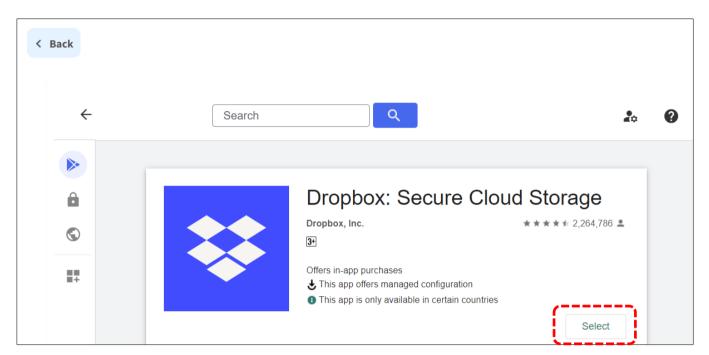
2) The user may find Apps by the search bar.

Taking the App "**Dropbox**" for example:

Search for the App you need.

Click to enter the App's detail page.

3) On the App's detail page, click "**Select**" to add this App to the profile.

4) The App is added to the profile. As mentioned above, Apps added to the activated profile will be simultaneously added to the enrolled devices that apply to the profile after "Save" or "Schedule".

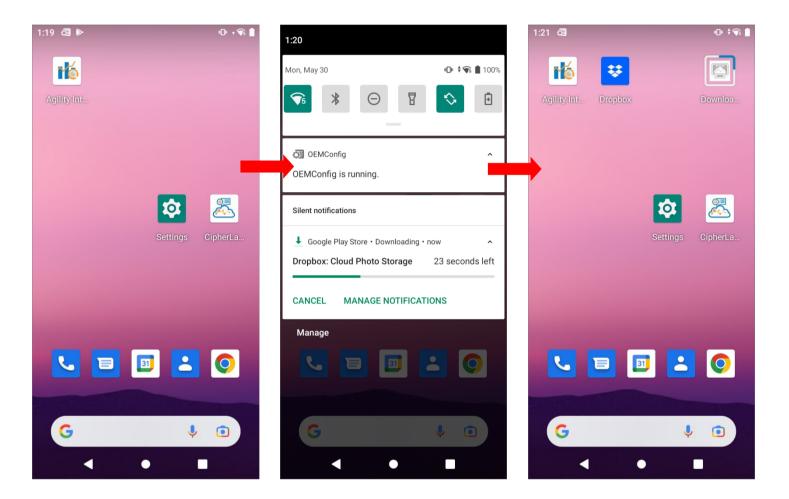When the profile's changed settings are carried out, the enrolled devices start to download and install the newly-added App.

PRIVATE APPS

"**Private App**" is an internal App made for the user's organization and products. It is only available for enterprise users.

The user should upload their own private Apps through "**Private Apps**" before adding them to a ReMoCloud profile. The uploaded private Apps are exclusive to the Managed Google Play account. Namely, other users will not find them in Google Play Store.

To upload private Apps and add them to the profile:

1) Click "Add App" to enter "**App Management**" page.

2) Select "Private **apps**" 🔒 from the side menu.
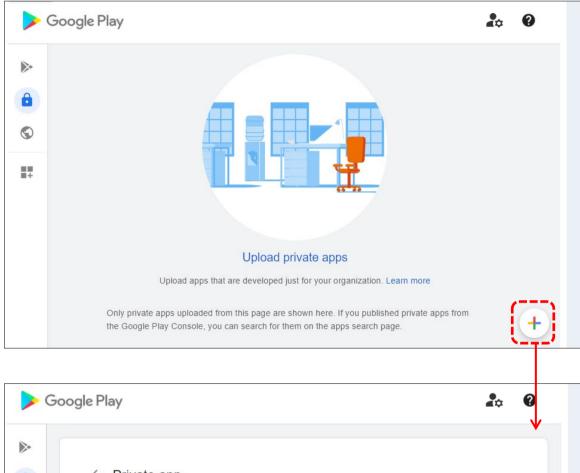
3) Click the add button ⊕ in the bottom-right corner. Enter a title and click "**Upload APK**" to select the App from the PC.
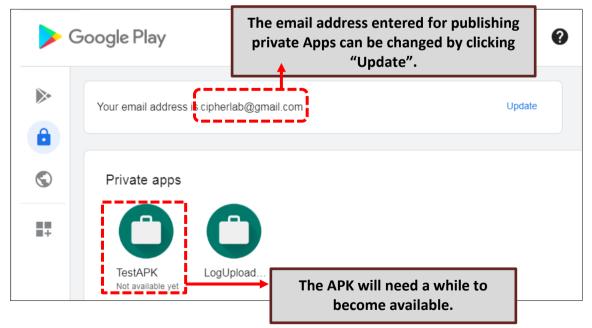
Note: The package name of the uploading private App must be unique. Else, cannot be published.
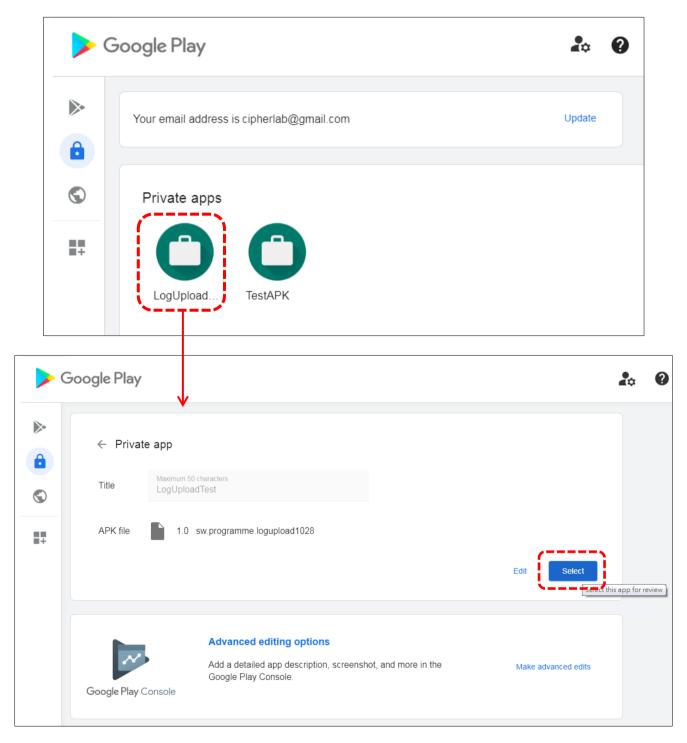
4) Click "Create" to upload the APK. If it is the user's first time to publish a private App, they need to enter the email address for receiving notifications from the Play Console.

5) When the APK is successfully uploaded, it will take a while to become available for adding to the profile. Users are free to go to other web pages before the process is completed.

6) When the APK is available, click it to enter its detail page. Next, click "**Select**" to add it to the profile.

7) The private app is successfully added to the profile.

Make sure to "Save" or "Schedule" the changed settings.

Note:

1. Please be cautious about uploading private Apps. Successfully uploading a private App means that the App's package name is unique in Google Play store. Thus, other APKs with the same package name cannot be uploaded to Google Play store, while the uploaded private Apps can only be accessed by the Google account set for uploading.

2. For more information on uploaing private Apps, refer to:
https://developers.google.com/android/management/apps#private-apps_1
https://support.google.com/googleplay/work/answer/9146439
https://support.google.com/googleplay/work/answer/9496237?hl=en&ref_topic=9496238

3. More details about the functions for editing private Apps in Manage Google Play that are only available for the Google Play Developer account. Refer to the "Register for a Google Play Developer account" part of "**How to use the Play Console**".

CIPHERLAB MANAGEMENT MODE

CipherLab Management Mode serves as an alternative to Google's application management capabilities and provides cloud storage that better optimizes the deployment of private applications for ReMoCloud users.

Follow the steps to activate CipherLab Management Mode:

1. Update the CipherLab OEMConfig App to version 1.0.0.36.1 or above.

2. Access Profile Information > Device Settings > App Management Mode

   and select "CipherLab Management Mode"

3. Install the App Manager Service by using OEMConfig Deploy from ZIP and enter the following URL:

https://asset.cipherlab.com/remocloud-download/download?token=Jzv3fJbZMVOrbqyUpi SQFucvBPMFtmFLH7FryFjd971qs44uXWQ0rq5BeD6PuzAcUX34KBB

4. Make sure to "Save" or "Schedule" the changed settings.

To add a new App in CipherLab Management Mode:

1. Click "**Add App**" button to enter the "**App Management**" page.

2. Select "CipherLab" to enter CipherLab Management Mode.
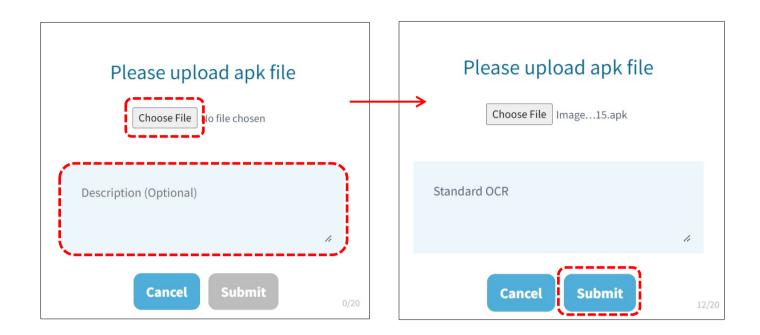
CipherLab Management Mode	
Item	Description
1. Mode Switching Buttons (Google Play / CipherLab)	Click to switch between Google Management Mode and CipherLab Management Mode.
2. Search Box	To search for specific Apps by keywords.
3. Storage Usage Progress Bar	Displaying how much storage space is used and how much space is available.
4. Upload APK File	To upload Apps by .apk files.
5. Add Selected Apps	To add the selected Apps to the profile.
6. App List	Displaying the detailed information about the uploaded Apps.

3. Click "Upload APK File" to open the "Please upload apk file" pop-up window.

4. Click "Choose File" to select the .apk file and click "Submit" to upload it.

The description field allows the user to add 20-word notes for the uploaded App, making it easily distinguishable from others. Else, click "Cancel" to close the pop-up window.

5. When successfully uploaded, the App will be displayed on the list. Select the App and click "Add Selected Apps" to add it to the profile.

Make sure to "Save" or "Schedule" the changed settings.

Note:

Please avoid simultaneously updating the App Manager Service and adding new apps.

2.4.2 EDIT APPS

Apps listed in the profile can be edited by:

APP PERMISSIONS

Click "**Edit**" under "**App Permissions**" to enter App permissions page.

Change the permission settings by selecting items, including "**None**," "**PROMPT**," "**GRANT**," and "**DENY**," from the drop-down menu.

Click "**OK**" to save the changed settings.

The available permission settings are:

Item	Description
None	to work in default mode
PROMPT	the App will prompt the window with question to set permissions
GRANT	allow the required access permissions
DENY	forbid the access permissions.

Return to "**Profile Information**" after editing permission settings.

"**Save**" or "**Schedule**" to carry out the changed settings before leaving this page.

Be sure to "Save" or "Schedule" the changed settings before leaving the "Profile Information" page.

MANAGE CONFIG

Click "**Edit**" under "**Manage Config**" to enter the App's configuration page. The configurable items vary depending on the Apps.

For example, the different configurable items of **Dropbox** and **Gmail** are as shown:

Make sure to "Save" or "Schedule" the changed settings before leaving "**Profile Information**" page.

2.4.3 WILDCARD SETTINGS

"**WildCard Settings**" is for the administrator to centrally manage Apps' information settings, such as email address or user name. For users who would like to have their employees' information set up to the enrolled mobile devices with designated Apps, using "**WildCard Settings**" will be the better method than setting each mobile computer individually.

The possible required information depends on different Apps, mostly including email address and user name. Take "**Gmail**" for example:

1) Go to "**Profile Information**" page. Add "**Gmail**" to the App list, referring to "<u>Add Apps</u>". Click "**Edit**" under "**Manage Config**" to enter Gmail configuration page.

2) Enter $emailaddress$ into "**Email Address**" field, and $username$ into "**Username**" field.

3) Click "**OK**" to save the changed settings before leaving "**Manage App Config**" page.

4) Go back to "**Profile Information**" page and click "**WildCards Settings**" to proceed.

If the user did not correctly enter $emailaddress$ into "**Email Address**" field and $username$ into "**Username**" field, the system would answer "You don't have any setting by using wildcards" after clicking "**WildCard Settings**".

5) Else, click "**Import**" to upload the **.csv** file that contains the required information, e-mail address, of all the employees.

For more details, refer to How to Create a .csv File for WildCard Settings.

WildCard

Hello! John Smith

< Back

Import   Export   Delete

| Serial Number | User Name | Email Address |

There are 3 setting buttons on "**WildCard**" page:

Setting Button	Description
Import	To import .csv files to WildCard Setting and set e-mail addresses with designated e-mail Apps.
Export	To export the e-mail address information listed on WildCard Setting page and save it as .csv files.
Delete	To delete all email address information from WildCard Setting page.

Gray setting buttons are unavailable. To make them available, save the changed settings on "**Profile Information**" page and return to **WildCard Setting** page to proceed.

6) In "**Please select csv file.**" pop-up window, click "**Choose File**" to select the .csv file and click "**Submit**" to upload it.

Click "**Cancel**" to close the pop-up window.

Please select csv file.

Choose File   No file chosen

Cancel   Submit

7) All the required e-mail addresses will be listed on the WildCard Setting page after successfully uploaded.

Make sure to "Save" or "Schedule" before leaving "**Profile Information**" page to carry out the changed settings.

Note:

1. The user may only upload one .csv file to a profile. Delete the original .csv file to upload another one if necessary.

2. When there are multiple Apps using wildcards $emailaddress$ or $username$ in "Manage App Config," they will all be set by the uploaded .csv file.

EXPORT

To export the email address information, click "**Export**" and enter the file name.

Click "**Submit**" to download it.

Click "**Cancel**" to close the pop-up window.

DELETE

Click "**Delete**" and "**Yes**" on the warning window to confirm deleting. All the e-mail addresses listed on **WildCard** page will hence be removed. The e-mail App's settings for the enrolled devices will also be deleted after "Save" or "Schedule".

HOW TO CREATE A .CSV FILE FOR WILDCARD SETTINGS

The **.csv** file should contain the information:

- the device serial number
- user name
- user's email address

The user may create a **.txt** file to input the required information as shown:

The device serial number, user name, and the email address are separated by commas but any white-space characters between them.

Save the **.txt** file and change its filename extension from **.txt** to **.csv**:

1) Click "**File**" and select "**Save As…**".

2) The "**Save As**" window appears. Select "**All Files (*.*)**" for "**Save as type**".
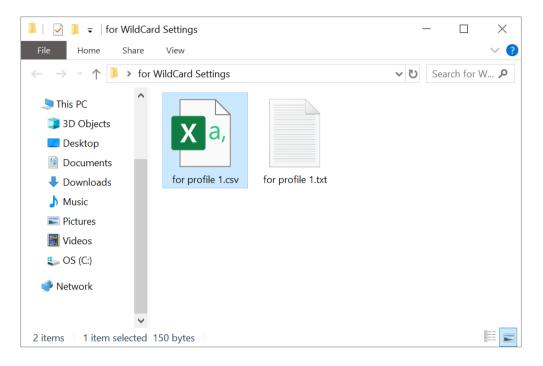
3) Manually change the filename extension to **.csv** in "**File name**" field.

4) Set "**UTF-8**" for "**Encoding**" and click "**Save**".

100

5) The **.csv** file is created and available for uploading to ReMoCloud "**WildCard Settings**".

Note:

When there are multiple Apps using wildcards $emailaddress$ or $username$ in "Manage App Config," they will all be set by the uploaded .csv file.

2.4.4 APP AUTO UPDATE MODE

There are three options for "App Auto Update Mode". Click to select.

App Name	Package Name	App Auto Update Mode	App Permissions	Manage Config
CipherLab Device Health	sw.programme.devicehealth	AUTO_UPDATE_DEFAULT ▲	Edit	
		AUTO_UPDATE_DEFAULT		
CipherLab LogCollection	sw.programme.logcollection	AUTO_UPDATE_POSTPONED	Edit	
CipherLab ADC Module	com.cipherlab.adcmodule.common	AUTO_UPDATE_HIGH_PRIORITY	Edit	

	Control the auto update mode for the Apps.		
App Auto Update Mode	AUTO_UPDATE_DEFAULT	Apps will be automatically updated with low priority to minimize the impact on the user. By default, Apps are automatically updated when the following constraints are met: ▪ The device is not actively used. ▪ The device is connected to a Wi-Fi network. ▪ The device is charging. The device will be notified within 24 hours after a new update is published by the developer. After an App is added to the queue, it wull be updated the next time the constraints above are met.	
	AUTO_UPDATE_POSTPONED	The App will not be automatically updated during 90 days after the App first became out of date. After the 90-day period, the latest available version of the App is automatically installed with the default update behavior. After the App is updated to the latest version, a new 90-day postponement period will begin the next time the developer publishes a new version of the App. The user can still manually update the app from the Play Store at any time.	
	AUTO_UPDATE_HIGH_PRIORITY	When using the High Priority mode, the app is updated, as soon as possible, after the developer publishes the new version.	

2.4.5 DELETE APPS

Click the dustbin button 🗑 to delete Apps.

Click "**Yes**" on the warning window to confirm deleting.

Click "**No**" to cancel.

Note that Apps installed on the enrolled devices applying to the profile will also be removed after "Save" or "Schedule".

DELETE INSTALLED APP(S) IN CIPHERLAB MANAGEMENT MODE

After clicking the dustbin button 🗑, the user will have to further confirm moving the deleted App to "**Block List Apps**" if "App Management Mode" is set to be "CipherLab Management Mode".

The App will be deleted from "**Installed Apps**" and moved to "**Block List Apps**" if clicking "**Yes**" on the pop-up confirming window "**Woud you like to move this app to 'Block List Apps'?**"

Make sure to "Save" or "Schedule" to carry out the changed settings.

2.4.6 BLOCK LIST APPS

"**Block List Apps**" conceals Apps from Google Play store and prevents the enrolled devices' users from installing them. Set "**App Management Mode**" as "**CipherLab Management Mode**" to access "**Block List Apps**".

ENABLE BLOCK LIST APPS

To enable the profile to access "**Block List Apps**" on the Profile Information page:

1) Enter the profile and enter its "**Device Setting**" tab page.

2) On "Device Setting" tab page, click "Functionality" to find "App Management Mode" and select "CipherLab Management Mode".

3) Return to "**App**" tab page. "**Block List Apps**" will appear.

Make sure to "Save" or "Schedule" to carry out the changed settings.

> Be sure to "Save" or "Schedule" the changed settings before leaving the "Profile Information" page.

After setting "App Management Mode" as "CipherLab Management Mode," "App" tab page will be divided into "Installed Apps" and "Block List Apps":

Item	Description
Installed Apps	Apps installed on the enrolled devices that applied to the profile.
Block List Apps	Apps hidden from Google Play store on the enrolled devices that applied to the profile.

ADD APPS TO BLOCK LIST APPS

To add Apps to "**Block List Apps**":

1) Enter "Block List Apps" tab page and click "Add App by Google" to enter "Managed Google Play Block List" page.

2) In "**Managed Google Play Block List**," enter the App's detail page and click "**Select**" to add it to "**Block List Apps**".
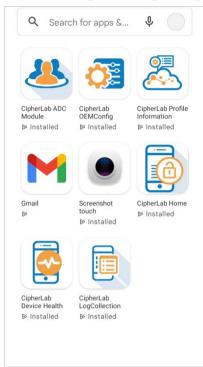
3) After the App is added to "**Block List Apps**" of the profile, make sure to "Save" or "Schedule" to carry out the changed settings.
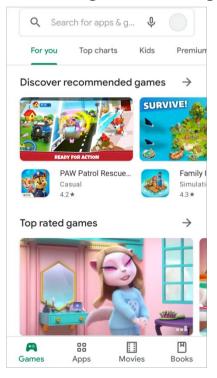
GOOGLE PLAY STORE ON THE ENROLLED DEVICE(S)

Check Google Play store on the enrolled devices after the changed settings are carried out. The normal UI allows users to search for and install Apps except for the blocked Apps.

- **The Main Page of Google Play on the Device (Google Management Mode):**
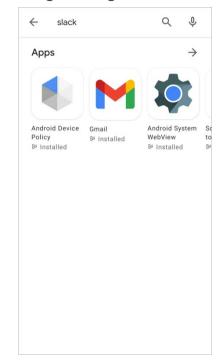
- **The Main Page of Normal Google Play on the Device (CipherLab Management Mode):**
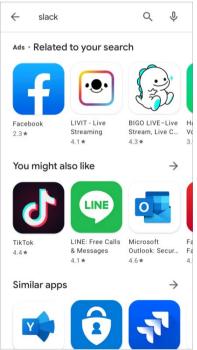
In Google Management Mode, only Apps installed by ReMoCloud will be displayed when searching Google Play store on the enrolled devices.

- **Search for Apps in Google Management Mode:**
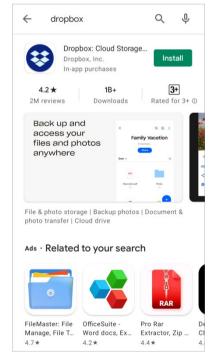
In CipherLab Management Mode, all Apps, execept for the blocked ones, will be available for searching and installing.

- **Search for the blocked App in CipherLab Management Mode**

- **Search for the unblocked App in CipherLab Management Mode**

ADD INSTALLED APPS TO BLOCK LIST APPS

To add the installed Apps to "Block List Apps," click "Add App by Google" on "Block List Apps" tab page to enter "Managed Google Play Block List".

Find the installed App and click "**Select**".
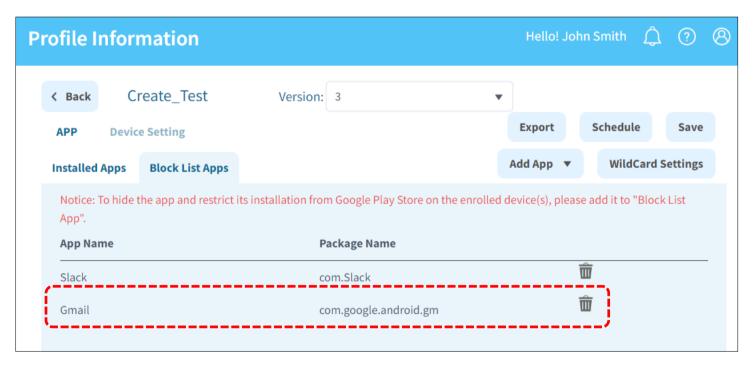
A pop-up window appears to confirm moving the selected installed App from "**Installed Apps**" to "**Block List Apps**".

Click "**Yes**" to proceed. Click "**No**" to cancel.

Make sure to "Save" or "Schedule" the profile to carry out the changed settings to the enrolled devices.

DELETE APPS FROM BLOCK LIST APPS

Click the dustbin button 🗑 to delete Apps from Block List Apps.

Clicking "**Yes"** on the pop-up warning window to confirm deleting.

Make sure to "Save" or "Schedule" the profile to carry out the changed settings.

2.4.7 SAVE A ROLL-BACK PROFILE

Saving a roll-back profile is to access a profile's previous version and save it as a new one.

Enter the profile and find "**Version**" next to the profile's name.

1) Click to select the version to be copied from the drop-down menu.

2) The roll-back version of the profile will be shown. Note that the user may only be able to check the details of profile setting but edit them.

3) Click "**Save As**" to save the previous version as a new profile.

Enter a name for the new profile and "**Submit**".

The roll-back profile is created. Enter the profile to edit if necessary.

Profile

Hello! John Smith

	Profile ∨	User-Defined	Enroll Device Number ∨	Status ∨	Version ∨	Last Edit Time ∨
☐	Create_Test	✏	1	Activated	3	2023/06/19 13:26
☐	DTS	✏	1	Activated	18	2023/05/24 11:27
☐	HCT	✏	0	Inactivated	46	2023/02/21 17:34
☐	Profile_1	✏	2	Activated	7	2023/06/14 16:31
☐	RK25	✏	1	Activated	41	2023/05/24 11:27
☐	RounDDay	✏	0	Inactivated	6	2023/05/03 15:47
☐	Testing	✏	1	Activated	5	2023/05/24 11:28
☐	Testing_for_rollback	✏	0	Inactivated	1	

Add Import Assign Copy Delete

Profile Information

Hello! John Smith

‹ Back   Testing_for_rollback   Version: 1

Export Schedule Save

APP   Device Setting

Add App   WildCard Settings

App Name	Package Name	App Auto Update Mode	App Permissions	Manage Config
CipherLab OEMConfig	com.cipherlab.oemconfig.common	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	Edit
CipherLab Device Health	sw.programme.devicehealth	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	
CipherLab LogCollection	sw.programme.logcollection	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	
CipherLab ADC Module	com.cipherlab.adcmodule.common	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	
CipherLab Profile Information	com.cipherlab.profileinfo.common	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	🗑
Android Device Policy ⓘ	com.google.android.apps.work.clouddpc	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	
CipherLab RemoteService	com.cipherlab.remoteservice	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	🗑
CipherLab Remote Control	com.webkey	AUTO_UPDATE_HIGH_PRIORITY ▾	Edit	🗑

EMM — Deployment, Profile, Enrollment, Monitor (Dashboard, Device, Group/Site, App), Account Manage (Manage), Log (User Log), Agility Intelligence

2.5   EDIT A PROFILE: DEVICE SETTING

"**Device Setting**" is for configuring system settings for the enrolled devices applying to the profile.

The information icon next to every setting option tells the details about the settings.

2.5.1 FUNCTIONALITY

Item	Description
Allow Screen Capture	Select whether the device is allowed to capture screenshots.
Allow Camera	Switch to enable or disable the camera on the device
Allow Adjust Volume	Select whether the volume can be adjusted or not.
Allow Mount Physical Media	Enable or disable the device to connect the external hard drive.
Allow Cell Broadcasts Config	Select whether to allow messages to be broadcast to all devices within a designated geographical area.
Allow Credentials Config	Select whether to allow configuration and credential files.
Allow Outgoing Beam	To enable or disable sending data to App through NFC.
Allow Outgoing Calls	To enable or disable dialing out.
Allow Share Location	To enable or disable sharing the device location to others.
Allow SMS	To enable or disable sending and receiving SMS.
Allow Unmute Microphone	To enable or disable mute or adjust the microphone volume
Allow Data Roaming	To enable or disable data roaming.
Allow Skip First Use Hints	To enable or disable the instruction when launching an App for the first time.

App Management Mode	Select the mode on the "App management" page:

Google Management	To add new Apps to the profile from Google Play Store.
CipherLab Management	Offers an alternative to Google's application management capabilities and provides cloud storage for uploading Apps.

Allow Keyguard	Switch to enable or disable the keyguard(lock screen).
Keyguard Disabled Features	Checked items will be hidden and unavailable when in keyguard mode.
Lock Screen Message	Enter the message to be displayed on the lock screen.

SERVICE

Item	Description
Sync Profile Information to Device	When this function is enabled, the default App "**CipherLab Profile Information**" on the enrolled devices will show the current profile information that the devices apply to. The App "**CipherLab Profile Information**" will not show any information till "**Sync Profile Information to Device**" is turned on. When "**Sync Profile Information to Device**" is turned on and the device is synced with ReMoCloud, "**CipherLab Profile Information**" will show the latest information that it acquires. When "**Sync Profile Information to Device**" is off, "**CipherLab Profile Information**" will show the information that the last time it synchronized.
Allow CipherLab Assistance Service	Enable or disable CipherLab Assistance Service for ringing the device and sending the push notification.
Allow Agility Intelligence Service	Allow or disallow installing the App "Agility Intelligence" which retrieves the device data for analyzing
Allow Remote Control	Switch to enable or disable remote controlling of the enrolled device(s). Please refer to Appendix III for details.

APP MANAGEMENT MODE
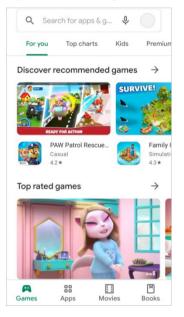
Follow the steps as "**Enable Block List Apps**" describes to set "**App Management Mode**" as "**CipherLab Management Mode**". For the details about hiding Apps from Google Play Store on the enrolled devices, refer to "**Add Apps to Block List Apps**".

After completing the steps, make sure to "Save" or "Schedule" the profile to carry out the changed settings on the enrolled devices. Check the App "**Google Play**" on the enrolled devices and the user may find the UI has changed:

UI of Google Management Mode   UI of CipherLab Management Mode
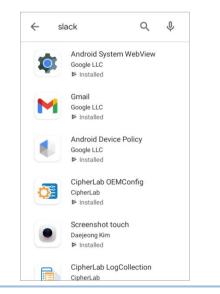
GOOGLE MANAGEMENT MODE
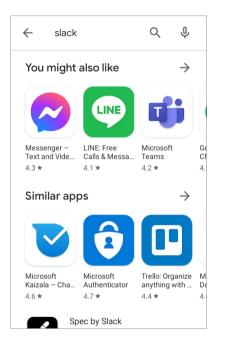
When searching for any Apps in Google Play Store on the enrolled devices, only Apps installed by ReMoCloud will be displayed.

122
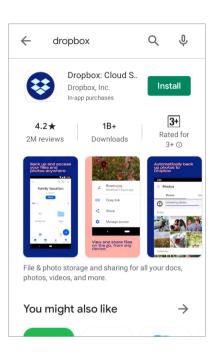
CIPHERLAB MANAGEMENT MODE

Apps in "**Block List Apps**" are concealed.

Other Apps, not in the block list, are displayed and available.

2.5.2 APPLICATIONS

Item	Description
Allow Install Apps	Switch to allow or disallow users to install Apps.
Allow Uninstall Apps	Switch to allow or disallow users to uninstall Apps.
Always On Vpn App	Setting an App to connect with VPN and making the VPN connection always-on to designated Apps. The user may check the designated App from **Settings**	**Network & internet**	**VPN** on the enrolled devices.

2.5.3   USER SETTING

Item	Description	
Default Permission	Set the access permission for all Apps in this profile.	
	None	To work in default mode
	PROMPT	The App will prompt the window with question to set permissions
	GRANT	Allow the required access permissions
	DENY	Forbid the access permissions.
Allow Modify Accounts	Allow or disallow to add or remove account to the device.	
Short Support Message	Set the warning message to be displayed on the pop-up for the forbidden functions on the enrolled devices. The length limit is 200 characters.	
Long Support Message	Set the detailed information for the "**Short Support Message**".	

APPEARANCE

Item	Description
Allow Set Wallpaper	Allow or disallow the user to set the wallpaper for this device.
Allow Set User Icon	Allow or disallow to change the user icon.

TIME SETTING
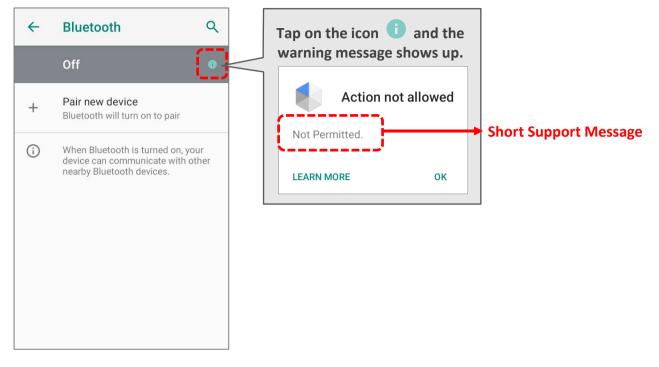
Item	Description
Allow Auto Time Required	Allow or disallow to automatically update time and date.

ReMoCloud User Guide

SHORT SUPPORT MESSAGE & LONG SUPPORT MESSAGE

To carry out the "**Short Support Message**" and "**Long Support Message**" settings, make sure to "Save" or "Schedule" this profile.

The enrolled device will show the warning message, the "**Short Support Message**" set by ReMoCloud administrator, to indicate that the function is unavailable if the user tries to access.

Click "**Learn More**" or "**More Details**" on the warning message to check the detailed information, namely, the "**Long Support Message**" set by ReMoCloud administrator.

2.5.4   NETWORK AND CONNECT

Item	Description
Allow Mobile Networks Config	Enable or disable the device to set up the mobile network.
Allow Tethering Config	Enable or disable sharing the Internet's connection for the device via tethering or hotspot.
Allow Vpn Config	Enable or disable the device to access a virtual private network.
Allow Wi-Fi Config	Allow or disallow the device to set Wi-Fi. Be cautious about disabling "Allow Wi-Fi Config" for the device. Wi-Fi will become totally unworkable and unconfigurable till a factory reset is performed on the device or the Wi-Fi function is restored by another profile.
Wi-Fi Setting	To set, edit, or delete the Wi-Fi networks that can be selected to apply on "**Enroll**"page.
Allow Network Reset	Allow or disallow the device to reset Wi-Fi.
Allow Network Escape Hatch	Switching on will allow the user to temporarily connect to a network to get the the device policy refreshed if a network connection can not be made at boot time. When "**Allow Network Escape Hatch**" is on, the enrolled devices will connect to a network if: ▪ There is no suitable networks in the last policy. ▪ The device boots directly into an App in lock task mode. ▪ Users are unable to reach the device settings. The temporary network will be forgotten after applying to the policy.

CONNECT

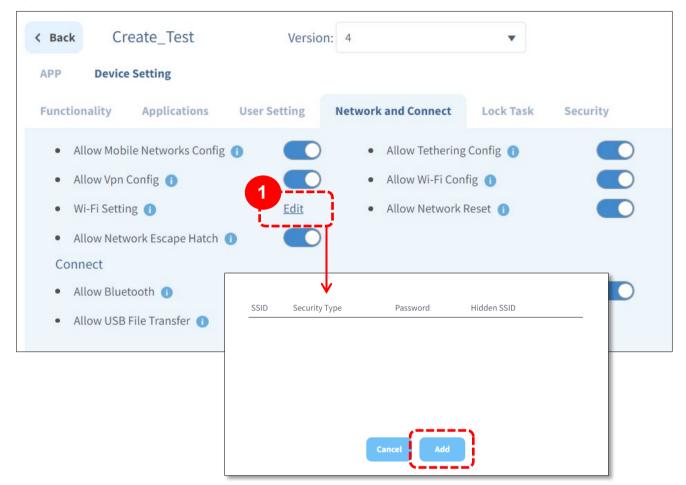| Item	Description
Allow Bluetooth	Enable or disable the bluetooth function of the device.
Allow Bluetooth Config	Allow or disallow the device to pair with other devices via bluetooth.
Allow USB File Transfer	Enable or disable sending files between the mobile computer and PC through USB.

Note:

To disable the Bluetooth functions for the Android 6 or Android 7 devices, please turn off both "Allow Bluetooth" and "Allow Bluetooth Config".

WI-FI SETTING

Follow the steps below to add a new Wi-Fi network:

1) Click "**Edit**" and "**Add**" in the pop-up window.

2) Fill out the network information in the pop-up window "**Please input Wi-Fi detail**" and "**Submit**".

For hidden SSID, select "**ON**":

Please input Wi-Fi detail

SSID:	Reliability
SECURITY_TYPE:	WPA-PSK ▼
PASSWORD:	•••••••• 🚫
Hidden SSID:	ON ▼

Cancel   Submit

3) Submit the Wi-Fi's detailed information. After completing the setting process, the Wi-Fi will be displayed on the setting list.

Repeat the above steps to add more Wi-Fi networks.

SSID	Security Type	Password	Hidden SSID		
Reliability	WPA-PSK	••••••••	ON	Edit	Delete

Cancel   Add

Button	Description
Edit	To modify the Wi-Fi network setting.
Delete	To delete the Wi-Fi network from the list.
Cancel	To close the Wi-Fi Setting window.
Add	To add a new Wi-Fi network to the list.

The user may choose to apply the Wi-Fi setting or manually enter a new one when setting up the defaulted Wi-Fi network for the Android 9 devices on "**Enroll**" page.

2.5.5   LOCK TASK

Item	Description
Lock Task Mode	Select the home screen setting for the devices.
	Null: No Apps will be pinned on the screen. The user will need to select either setting "**AppLock**" or "**Launcher3** (default)" as the home screen after completing the device enrollment.
	Single App: To pin an App on the screen. To select "**Single App**," the user will need to enter one App's package name in the field "**Lock task single App**" to pin it on the screen.
	Multi App: To allow or disallow Multi App mode on the device. The status bar cannot be revealed by swiping down when "**Multi App**" is selected.
	Cipherlab Home: To customize the user interface of the enrolled devices by setting limits to functions, making certain system resources available to users. Enable "**Cipherlab Home StatusBar Expansion Option Settings**" to reveal the status bar. For details, refer to "**CipherLab Home**".
Cipherlab Home Application Settings	This function will only be available when "**Lock Task Mode**" is set as "**Cipherlab Home**". It is for ReMoCloud administrator to customize the displayed Apps on the enrolled devices.
	Select an Existing App: To select the allowed Apps, including system Apps and installed Apps on the profile App list, from the drop-down menu.
	Input the Package Name: To designate an App, installed on the enrolled devices, to be shown by inputting its package name.
Lock Task Single App	Enter the App's package name to pin it on the screen. After completing the device enrollment and selecting the home screen, the device will start to download and install the applied profile's Apps. The designated App will be pinned on the screen after it is installed. This function will only be available when "**Lock Task Mode**" is set as "**Single App**".

These functions will only be available when"**Lock Task Mode**" is set as "**Cipherlab Home**"**.**

Item	Description
Cipherlab Home Clear Cache Application Settings	To clear the App cache. To function properly, the version of Google Chrome App should be 90 or later.
Cipherlab Home Background Settings	To set the enrolled devices' background by entering the URL of the designated wallpaper.
Cipherlab Home StatusBar Expansion Option Setting	The settings decide whether or not to let the status bar be expandable in "**User Mode**". The available settings are: <table><tr><td>Non-expandable</td><td>The status bar cannot be dropped down in User mode.</td></tr><tr><td>Expandable 1 layer</td><td>Users cannot drop the status bar down to check and manage system notifications or to open Quick Setting Panel.</td></tr><tr><td>Expandable 2 layers</td><td>Users cannot drop the status bar down to check and manage system notifications or to open Quick Setting Panel and Quick Setting Menu.</td></tr></table>
Cipherlab Home Custom Title Option	The options decide whether or not to show the title content on CipherLab Home's title bar. <table><tr><td>CipherLab Home</td><td>Shows "CipherLab Home" on the title bar</td></tr><tr><td>Serial number</td><td>Shows the device serial number.</td></tr><tr><td>WI-FI IP</td><td>Shows the device Wi-Fi IP address</td></tr><tr><td>WI-FI MAC</td><td>Shows the device Wi-Fi MAC address.</td></tr><tr><td>WI-FI SSID</td><td>Shows the Wi-Fi SSID that the device connects to.</td></tr><tr><td>Hostname</td><td>Shows the network hostname of the device.</td></tr><tr><td>Device name</td><td>Shows the device name.</td></tr><tr><td>Date (Month/date)</td><td>Shows the current date (format: MM/DD).</td></tr><tr><td>Custom title</td><td>Shows the content entered in "Cipherlab Home Custom Title String".</td></tr></table>

Item	Description
Cipherlab Home Custom Title String	Select "**Custom title**" for "**Cipherlab Home Custom Title Option**" to enter the content that will be displayed on CipherLab Home's title bar. Text characters are required for the string: English, Chinese, French, etc. The followings are optional for the string: ■ White-space ■ Digits: 0 to 9 ■ Symbols: !#$()*,-./:;?@[]_ {|}~ Note that the string might not be completely displayed on the device if it contains too many characters. The title may present multiple content options. For example, input {SN} into "**Cipherlab Home Custom Title String**" field to show the device serial number on CipherLab Home's title bar. That is, inputting "CipherLab {SN}" will make the CipherLab Home's title bar show "CipherLab FW12060011". The following list demonstrates the codes: ■ **{SN}** : Serial number ■ **{IP}** : Wi-Fi IP ■ **{MAC}** : Wi-Fi MAC ■ **{SSID}** : Wi-Fi SSID ■ **{HOSTNAME}** : Hostname ■ **{DEVICENAME}** : Device name ■ **{DATE}** : Month/date This function will only be available when "Lock Task Mode" is set as "Cipherlab Home," and "Cipherlab Home Custom Title Option" as "Custom title".
Cipherlab Home Admin Password	The password for CipherLab Home admin mode. When the user enters CipherLab Home admin mode, all the Apps will be displayed. The password can consist of text characters (English, Chinese, French, etc.), digits (0 to 9), and symbols (!#$()*,-./:;?@[]_{|}~). If this field is left blank, the password will be the default password "23058518". This function will only be available when "**Lock Task Mode**" is set as "**Cipherlab Home**".
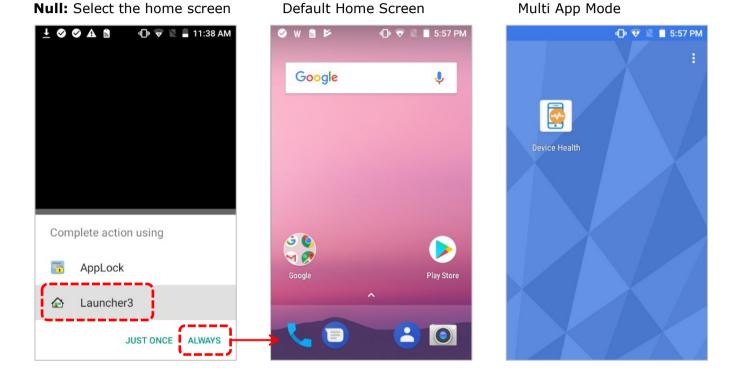
Item	Description
Cipherlab Home Enable Lock Device	To lock the devices. This function will only be available when "**Lock Task Mode**" is set as "**Cipherlab Home**".
Cipherlab Home Lock Device Background	When "**Cipherlab Home Enable Lock Device**" is enabled, the user may set the background by inputting the image's URL. The URL can consist of english letters; digits (0 to 9), and symbols (!#$&()*+,-./:;=?@_~). If this field is left blank, the default background will be "dark grey".
Cipherlab Home Lock Device Password	If "**Cipherlab Home Enable Lock Device**" is enabled, the user may input the password to manually unlock the device. If this field is left blank, the default password will be "**Cipherlab Home Admin Password**". The password can consist of text characters (English, Chinese, French, etc.), digits (0 to 9), and symbols (!#$()*,-./:;?@[]_{|}~).
Cipherlab Home Lock Device Message	When "**Cipherlab Home Enable Lock Device**" is enabled, the user may set text messages to be displayed on the lock device's screen. The default message is "**DEVICE LOCKED**". Note that the message must not be blank, and the limitation is no more than 50 characters. The message must consist of text characters: English, Chinese, French, etc. The followings are optional for the message: ▪ White-space ▪ Digits: 0 to 9 ▪ Symbols: !#$()*,-./:;?@[]_ {|}~
Cipherlab Home Lock Device Week	When "**Cipherlab Home Enable Lock Device**" is enabled, the user should select at least one day for a week to lock the devices.
Cipherlab Home Lock Device Time	When "**Cipherlab Home Enable Lock Device**" is enabled, the time must not be blank. Set the starting time to lock the devices. The time format should be HHMM (0000 - 2359). HH refers to hours (24-hour clock) while MM refers to minutes. For example, the starting time to lock the devices at 12:00 a.m.: 0000.

Item	Description
Cipherlab Home Lock Device Period	When "**Cipherlab Home Enable Lock Device**" is enabled, this field must not be blank. Setting the period is to lock the devices for 1 to 1440 minutes. The format: 1 - 1440.
Power Button Actions (Only support Android 9.0+)	To set the devices' behavior in kiosk mode when the user presses and holds (long-presses) the power button. This function will only be available when the devices OS are Android 9 or later, and when "**Lock Task Mode**" is set as " **Cipherlab Home**" or "**Multi App**".
App System Error Warning Actions (Only support Android 9.0+)	Specify whether the "system error" dialog for crashed or unresponsive Apps is blocked in kiosk mode. This function will only be available when the devices OS are Android 9 or later, and when "**Lock Task Mode**" is set as " **Cipherlab Home**" or "**Multi App**".
App System Navigation Actions (Only support Android 9.0+)	Specify what navigation features are enabled in kiosk mode, such as Home button and Overview button. This function will only be available when the devices OS are Android 9 or later, and when "**Lock Task Mode**" is set as " **Cipherlab Home**" or "**Multi App**".
App Status Bar Actions (Only support Android 9.0+)	Specify whether the system information and notifications are disabled in kiosk mode. This function will only be available when the devices OS are Android 9 or later, and when "**Lock Task Mode**" is set as " **Cipherlab Home**" or "**Multi App**".
App Devices Settings Actions (Only support Android 9.0+)	Specify whether the App "**Settings**" is allowed in kiosk mode. This function will only be available when the devices OS are Android 9 or later, and when "**Lock Task Mode**" is set as " **Cipherlab Home**" or "**Multi App**".

NULL & MULTI APP MODE

When setting "**Null**" for "**Lock Task Mode**," the user has to choose between "**AppLock**" or "**Launcher3** (default)" to be the home screen after completing the device enrollment.

Null: Select the home screen   Default Home Screen   Multi App Mode

SINGLE APP MODE

"**Single App**" mode is to pin an App on the device screen.

Enter one App's package name in the field "**Lock task single App**" to pin it on the screen. The package name must be the same with the system App or the installed App on the profile App list.

1. Select the home screen after enrollment.

2. It will automatically download the Apps the profile contains.

3. The designated App will be pinned on the screen after installation.

2.5.6   SECURITY

Item	Description
	Passcode settings.

None	No passcode.
Numeric	The passcode must include digits.
Numeric (Complex)	The passcode must not include repeating and sequential digits, such as 0000 and 1234.
Alphabetic	The passcode must include letters and symbols.
Alphanumeric	The passcode must include digits and letters (or symbols).
Complex	The passcode must include at least a digit, a letter, and a symbol.

If select other settings but "**None**," the user will be required to set:

Password Minimum Length	The minimum allowed password length. "None" refers to no restriction. It will only be required when the passcode is set as Numeric, Numeric (Complex), Alphabetic, or Complex.

Minimum Passcode Requirement

If select "**Complex**," the user will be required to set:

Minimum Letter Length	Minimum number of letters required in the password. Only required when the passcode is set as COMPLEX.
Minimum Lowercase Letter Length	Minimum number of lowercase letters required in the password. Only required when the passcode is set as COMPLEX.
Minimum Non Characters	Minimum number of non-letter characters, digits or symbols, required in the password. Only required when the passcode is set as COMPLEX.
Minimum Numeric Length	Minimum number of digits required in the password. Only required when the passcode is set as COMPLEX.
Minimum Symbol Length	Minimum number of symbols required in the password. Only required when the passcode is set as COMPLEX.
Minimum Uppercase Length	Minimum number of uppercase letters required in the password. Only required when the passcode is set as COMPLEX.

Item	Description
Password History Length	Setting the limit of the passcode length.
Maximum Number of Failed Attempts	Setting the limit of failed logins timer.
Battery Plugged Mode	Keep the device screen on when charging by the selected method. Note that setting as "**None**" is to disable "**Battery Plugged Mode**". Set "Max Time to Screen Lock (second)" as "None" to enable "Battery Plugged Mode".
Max Time to Screen Lock (Second)	Changing the screen timeout options to keep the device screen on for longer.
Allow Factory Reset	Decide whether or not to allow performing factory reset on the device.
Allow Install Unknown Apps	Decide whether or not to allow manually installing Apps.
Location Mode	Location access options: | User Choice	Location detection will be user-accessible
Enforced	Location detection will be enforced on the device.
Disable	Location detection will be disallowed.	
Compliance Rules Block After Days	If the devices break the security rules, Apps will be blocked after certain days.
Compliance Rules Wipe After Days	If the devices break the security rules, Apps will be wiped after certain days.
Allow Developer Settings	Decide whether or not to allow entering safe mode and debugging features.
Allow Google Play Protect Verify Apps	Decide whether or not to enable checking the potential threats brought by Apps.
Private Key Selection Enabled	Allow showing UI on the device for users to choose a private key alias.

2.6 SAVE/ SCHEDULE A PROFILE

2.6.1 SAVE

"**Save**" button is on both "**APP**" tab page and "**Device Setting**" tab page in a profile.

- On "APP" tab page:

- On "Device Setting" tab page:

Whenever the user makes changes to Apps or the settings for enrolled devices in a profile, the "**Save**" button changes its color to remind users that the changed settings are unsaved yet. Therefore, make sure to click the "**Save**" button to carry out the changed settings.

UNSAVED CHANGES WARNING

When the user leaves the **Profile Information** page without saving the changed settings, the warning popup appears to remind the user.

Click "**YES**" to save the changed settings and enter the page the user intended to reach

Click "**NO**" to directly leave the page.

2.6.2 SCHEDULE

The "**Schedule**" button on both "**APP**" tab page and "**Device Setting**" tab page is for planning the times at which each changed setting should happen or be done.

- On "APP" tab page

- On "Device Setting" tab page

Click the "**Schedule**" button to enter the updated profile task page after making changes to "**APP**" or "**Device Setting**" in a profile. The updated profile task page contains two tab pages, "**Schedule List**" and "**Schedule Record**".

Schedule List allows the user to create and manage all tasks. The device will automatically carry out the tasks at the time the user specifies.

Schedule Record allows the user to view and clear the task history.

SCHEDULE LIST

After making changes of **APP** or **Device Setting** in a profile, click the "**Schedule**" button to enter **Schedule List** tab page of "**Schedule**" for creating an updated profile task.

Schedule	Hello! John Smith
‹ Back Testing_for_rollback ⟳	**Add** **Update** **Delete**
Schedule List Schedule Record	

	Profile to be Updated	Scheduled Task Time	Last Edit Time	Change Task Execution Date & Time
☐	Create_Test	2023-06-29 13:00:00	2023-06-26 10:16:56	2023-06-29 00:00
☐	Testing_for_rollback	2023-06-30 10:30:00	2023-06-26 10:29:36	2023-06-30 00:00
☐	Create_Copied	2023-07-05 08:30:00	2023-06-26 10:29:04	2023-07-05 00:00

Setting Button	Description
⟳ (Refresh)	To reload the page and receive the latest status of all tasks.
Add	To make plans for the profile to be updated.
Update	Click "**Update**" to carry out the changes made to the existing tasks.
Delete	To delete the selected tasks.

A scheduled task contains the information and functions:

- Profile to be Updated:

The name of the profile to be updated.

- Scheduled Task Time:

The date and time that the task is scheduled to be executed

- Last Edit Time:

The date and time of when the scheduled task was edited the last time.

- Change Task Execution Date & Time:

Click "**Update**" to reschedule the date and time for the task to be executed. The user can select multiple tasks at a time to modify.
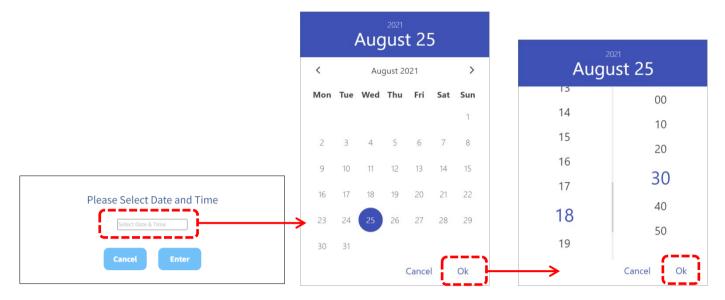
ADD A TASK IN SCHEDULE LIST

Click "**Add**" to schedule the date and time for the task to be executed. The user can schedule multiple tasks for one profile.

Click the "**Select date & time**" field to set the date and time.
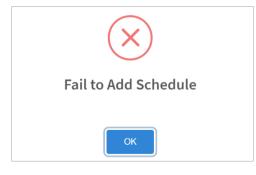
1. Click the "Select Date & Time" field.   2. Set the date and click "OK".   3. Set the time and click "OK".

4. Click "Enter" to complete the setting.   5. The task is successfully created.

Note that the date and time scheduled for the task should be later than the current time. Else, the task cannot be created.

After the task is successfully created, it will be listed on the **Schedule List**:

Note:

The current date and time of the timepicker will be in accordance with **Time Zone**'s setting in User Info page.

MODIFY/ DELETE THE PROFILE TASK(S)

The user can modify multiple tasks execution time at a time by ticking up the checkboxes and clicking "**Update**" or "**Delete**".

MODIFY THE PROFILE TASK(S)

To modify the tasks' execution date and time:

1. Click the "**Change Task Execution Date & Time**" field and select the date and time. Note that the date and time scheduled for the task must be later than the current time.

2. Tick the checkboxes of the tasks to be modified.

3. Click "**Update**" to save the changed settings.

DELETE THE PROFILE TASK(S)

Click "**Delete**" to eliminate the selectd tasks and click "**Yes**" on the warning pop-up window to confirm deleting.

ReMoCloud User Guide

## SCHEDULE RECORD

Schedule Record tab page lists the task histiory:

The information and functions on "**Schedule Record**" tab page are:

▪ Profile Name:

The name of the updated profile.

▪ Execution Date & Time:

The date and time that the task was executed.

▪ Reservation Date & Time:

The date and time for the ReMoCloud administrator to execute the task.

▪ Status:

Tells if the task is successfully updated to ReMoCloud or not.

▪ Delete :

Click "**Delete**" to delete the selected history log. The user can delete multiple task history logs at a time.

▪ Refresh :

Click the refresh button to reload the schedule record.

Note:

The Apps and device settings will not be updated and saved on the "Profile Information" page till the task is successfully executed at the scheduled date and time.

SCHEDULE PROFILE INFO

On both "**Schedule List**" and "**Schedule Record**" tab pages, click the profile's name to enter "**Schedule Profie Info**" page where the user can check the details.

Note that the profile's information is NOT editable on "**Schedule Profie Info**" page.

Click "**Check**" under "**App Permissions**" and "**Manage Config**" to enter the App's "**Schedule App Permissions**" page and "**Schedule Manage Config**" page. For these two pages, the detailed information is not editable as well.

2.7 ADVANCED SETTINGS

2.7.1 GEOFENCING

"**Geofencing**" is a security tool for administrators to manage devices using location-based rules. Alerts and notifications are triggered when devices enter or exit assigned geofences according to configured settings.

To create a Geofence Setting, navegate to the "**Advanced Settings**" page:
1. Customize the settings under "**Geofencing Settings**" to suit your requirements.
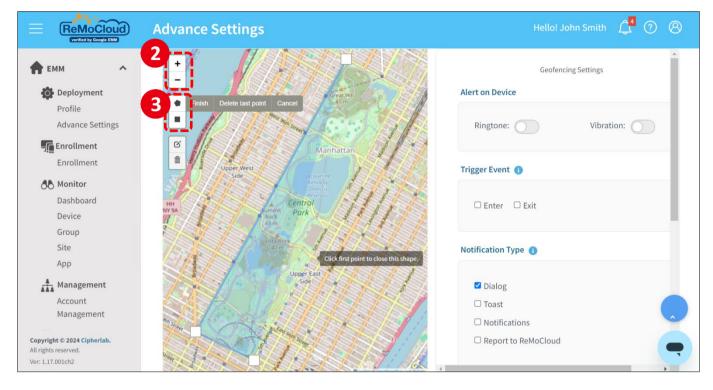
The table below lists the setting items and the descriptions for "**Geofencing Settings**":

Setting Item	Description
Alert on Device	Enable/Disable "**Ringtone**" or "**Vibration**" as alerts on the device.
Trigger Event	Configure alerts for entering/exiting geofences. Select "**Enter**", "**Exit**", or both.
Notification Types	Choose notification presentation: "**Dialog**", "**Toast**", "**Notificationa**", "**Report to ReMoCloud**" or multiple types.
Manual Stop	Allow the user to dismiss the alert on the device.
Text Messages	Define "**Title**" and "**Message**" for the alert shown on the device.

2. Navigate to the desired geographic area for creating a geofence by using the mouse scroll wheel or tapping the "**+**" and "**-**" buttons on the map.

3. Tap on the **pentagon** ⬠ or the **sqare** ◼ on the map to define the area.
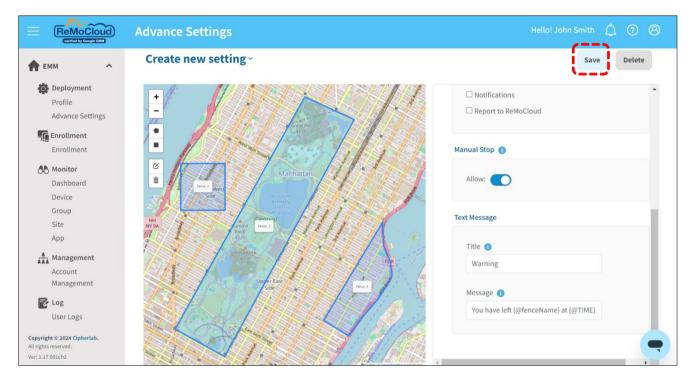
4. After drawing the shape, a pop-up window will appear. Enter a name for the geofence and click "**Submit**".

Users are allowed to draw multiple fences in one Geofence Setting.

5. After creating the geofences, tap "**Save**". A pop-up window will prompt you to name the setting.

6. Name the new setting and click on "**Submit**".

A pop-up window will appear to show the setting is added successfully.

Now you are ready to assign devices to the Geofencing Setting you created.
For further instructions, please refer to section 5.3.5 Assign Geofence Setting.

Note:

Upon assignment to a Geofence, devices are monitored every 3 minutes. The alert, whether ringtone or vibration is triggered, it will remain active until the user returns or leaves the fenced area or manually dismisses it.

Chapter 3

CHAPTER 3. ENROLL DEVICE
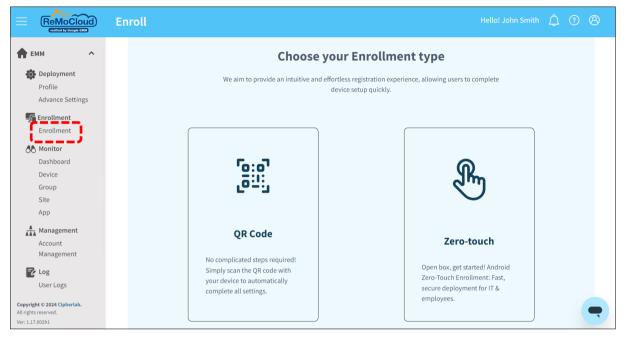
This chapter offers a step-by-step guide for enrolling CipherLab mobile computers, allowing users to choose between QR code or Zero-touch enrollment methods.

IN THIS CHAPTER

3.1 PREREQUISITE

Nevigate to "**Enrollment**" page where you will find two options for device enrollment:QR Code and Zero-touch. Tap to choose your preferred enrollment method.

To begin enrolling CipherLab mobile computers using either QR Code or Zero-touch, users must first create a profile.

Please note that for QR Code enrollment, the device's OS (Operating System) version should be Android 6.0 or later with GMS certification, while for Zero-touch enrollment, it should be Android 9.0 or later with GMS certification.

3.2 QR CODE ENROLLMENT

3.2.1 ON REMOCLOUD

Enter "**Enrollment**" page on ReMoCloud, and tap "**QR Code**" to enroll your devices.

Set up the default Wi-Fi network for the Android 9+ devices if necessary. After the completion, click "**Generate**" to receive the enroll code.

The **enroll code** (barcode/QR Code) will appear.

Click "Print" to print out the enroll QR Code.

Click "E-mail" to send the enroll QR Code, enroll code, and enroll barcode to the designated e-mail address.

Note:
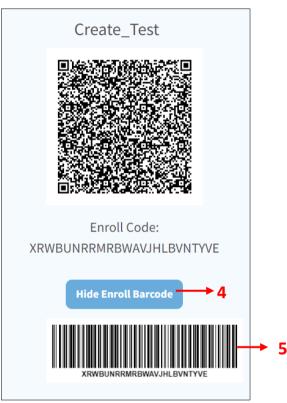
1. For more details about profile management, refer to "**Deployment**".

2. "Enable the default system Apps" will not be available for the devices enrolled by **manually inputting the "Enroll Code"**. All system Apps will be hidden even if the user chooses "Yes" for "Enable the default system Apps" on ReMoCloud.

FOR DEVICE WITH CAMERA

For step 3, the user should decide whether or not to allow the device's camera access during the enrollment. When the camera access is allowed, a QR Code will appear after clicking "**Generate**". As shown:
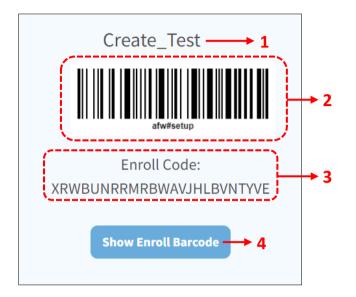
The items appear with the QR code:

No.	Item	Description
1.	Profile Name	The profile selected to generate the QR Code for device enrollment.
2.	QR Code	Provided to be scanned by the device's camera for enrollment.
3.	Enroll Code	Provided to be manually input to the devices for enrollment.
4.	Show Enroll Barcode/ Hide Enroll Barcode	Show or hide the barcode for the device's scanner but camera to scan.
5.	Enroll Barcode	Provided to be scanned by the device's scanner for enrollment.

FOR DEVICE WITHOUT CAMERA

When the camera access is disallowed in step 3, the **QR Code Generator** will create a set of barcode for the device's scanner.

The items appear with the Barcode:

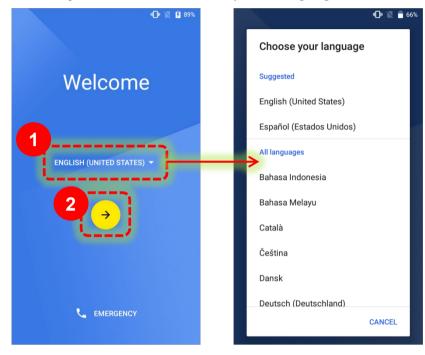| No.	Item	Description
1.	Profile Name	The profile selected to generate the QR Code for device enrollment.
2.	afw#setup barcode	Provided for Android 6.0+ devices for the step "Sign in" during enrollment.
3.	Enroll Code	Provided to be manually input to the devices for enrollment.
4.	Show Enroll Barcode/ Hide Enroll Barcode	Show or hide the barcode for the device's scanner but camera to scan.
5.	Enroll Barcode	Provided to be scanned by the device's scanner for enrollment.

Note:

1. The user can only enroll devices by inputting "Enroll Code" and scanning "Enroll Barcode" when the QR reader fails to download, or when the barcode "afw#setup" is used without tapping on the same spot for 6 times at the beginning.
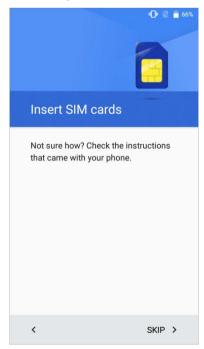
2. For more details about device enrollment, refer to:

- RS31, RS35, RS51, Hera 51, RK25, & RK95: **Enrollment for Device with Android 7.0+**.

- RS50: **Enrollment for Device with Android 6.0**.

DEFAULT WI-FI SETTING

The user can set the default Wi-Fi for the Android 9+ devices enrollment.

To set the default Wi-Fi network:

1. Complete step 1, selecting the profile for device enrollment, and step 2, deciding whether or not to enable system Apps.

2. In step 3, select "**Yes**" to enable the device camera.

3. In step 4, select "**No**" to disable mobile network. Else, the default Wi-Fi network will fail to be set in step 5.

4. In Step 5, select "**Yes**" to enable the default Wi-Fi network settings. Depending on different profiles, the "**SSID**" field may be a blank field or a drop-down menu displaying all the preconfigured Wi-Fi network settings from "**Device Setting**" tab page of the profile.
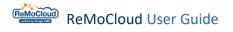
▪ The blank SSID field

For the blank SSID field, fill out the required information of the Wi-Fi network.

5. Fill out all the required information of the default Wi-Fi network settings. Note that if the user would like to hide the network ID, **"Hidden SSID"** must be set as "**ON**".

6. Step 6, click "**Generate**" to get the "**Enroll Code"** to be scanned by the device.

For more details about device enrollment, refer to Device with Android 9 or Later.

Note:

Selecting "No" in step 3 will make the default Wi-Fi settings unavailable.

3.2.2 ON YOUR MOBILE COMPUTER

If the mobile computer is not new, it needs to start with factory reset for enrollment.

To perform factory reset:

1. Access App Drawer (All Apps)>Settings ⚙ >Backup & reset ☁ >Factory data reset.

Note: Depending on different device models, the path to access "Factory data reset" may vary.

2. Confirm the action and input the verification code
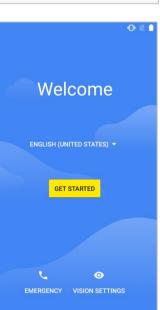
(please contact support@cipherlab.com.tw to obtain the verification code).

Click "**OK"** to perform factory reset.

3. After the factory reset, when the mobile computer boots up for the first time, the **Welcome wizard** appears.
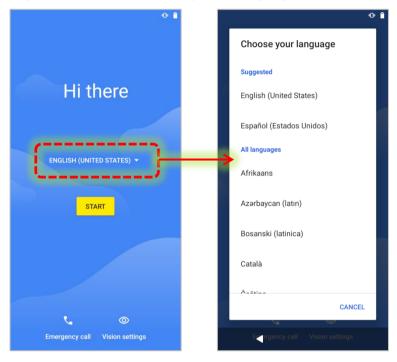
The following sections provide the enrollment introduction:

Enrollment for Device with Android 7.0+

Enrollment for Device with Android 6.0

ENROLLMENT FOR DEVICE WITH ANDROID 9.0+

For RK25, RK95 (Android 9.0), and RS35 (Android 10), the user can set the default Wi-Fi network in advance, and the device will automatically apply to the Wi-Fi setting during the enrollment.

- **Step 1:** Select the desired system language.

- **Step 2:** Tap on the same spot on the screen for **six times** to enter the QR code setup process.

▪ Step 3:
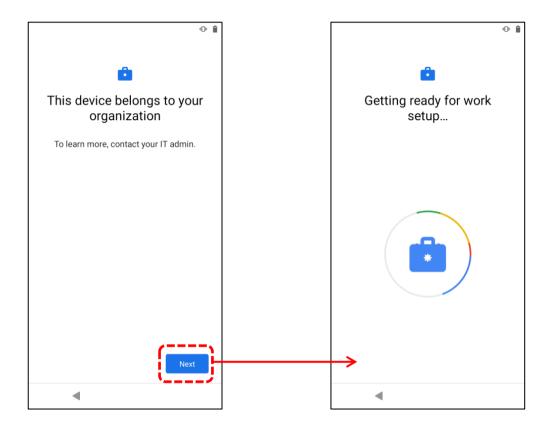
Use the mobile computer's camera to take aim at the QR code generated by ReMoCloud.
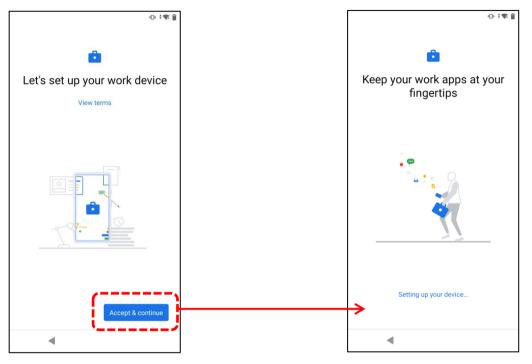
- **Step 4:**

Click "**Next**" to confirm that the device will be managed as a work device by the ReMoCloud administrator.

▪ **Step 5:**

Click "**Accept & Continue**" to proceed.

▪ **Step 6:**

Again, click "**Next**" to confirm that the device will be controlled by the ReMoCloud administrator.

▪ Step 7:

Choose the Google services that you would like to enable and click "**Accept**" to proceed.

▪ Step 8:

The enrollment process will take a while.

Click the "more button" ⋮ and select "**Reset Device**" to reset the device if necessary.

▪ Step 9:

When the enrollment is completed, the user will subsequently enter **the default home screen / CipherLab Home / Multi App Mode** previously set by the applied profile.

For more details about the related settings, refer to **Lock Task**.

Default Home Screen   CipherLab Home   Multi App Mode

The user may find the enrolled device listed on the "**Device**" tab page of "**Monitor**" on ReMoCloud. As shown:

Enrollment for Device with Android 7.0+

When **Welcome wizard** appears, instead of clicking the yellow button "**GET STARTED**," please follow the steps to enroll HERA51, RK25, RK95, RS31, RS35, or RS51 devices:

Note: Depending on different devices, the Welcome wizard may slightly vary. The following steps will take RK25 as example.

- **Step 1:** Select the desired system language.

- **Step 2:** Tap on the same spot on the screen for **six times** to enter the QR code setup process.

- Step 3:

When the QR code setup process starts, click "**Next**" to continue.

- Step 4:

Select the Wi-Fi network to connect.

▪ Step 5:

After connected to the Wi-Fi network, the system will automatically check for updates and install QR reader.

▪ Step 6:

Use the mobile computer's camera to take aim at the QR code generated by ReMoCloud.

- Step 7:

Click "**ACCEPT & CONTINUE**" to confirm that the device will be controlled as a work device by the ReMoCloud administrator.

The setup process will take a while.

- Step 8:

The enrollment is about to be completed.

Click the "more button" ⋮ and select "**Reset Device**" to reset the device if necessary.

The enrollment is done. The user will subsequently enter **the default home screen** / **CipherLab Home** / **Multi App Mode** previously set by the applied profile.

For the related settings, refer to **Lock Task**.

Default Home Screen	CipherLab Home	Multi App Mode

The device will start to install the Apps from the applied profile. Slide down the status bar to open the notification drawer and check the download progress.

For more details about the related settings of status bar, refer to **Lock Task**.

Note:

The status bar will be unavailable when "Multi App Mode" is enabled.

The user may find the enrolled device listed on the "**Device**" tab page of "**Monitor**" on ReMoCloud. As shown:

Note:

1. For more details about profile management, refer to **Deployment: Profile Management**.

2. For more details about enrolled device management, refer to **Device Management**.

3. The user can only enroll devices by inputting "Enroll Code" and scanning "Enroll Barcode" when the QR reader fails to download, or when the barcode "afw#setup" is used without tapping on the same spot for 6 times at the beginning.

ENROLLMENT FOR DEVICE WITH ANDROID 6.0

The steps to enroll the RS50 mobile computer (Android 6.0) through the **Welcome Wizard** process:

- **Step 1:** Select the desired system language and click the yellow button ⟶ to start.

- **Step 2:** Either insert the SIM card or directly "**SKIP**" to the next step.

■ **Step 3:**

Select the Wi-Fi network to connect.

■ **Step 4:**

Select "**NO thanks**" to not transfer data from other devices. Click "**Next**" to proceed.
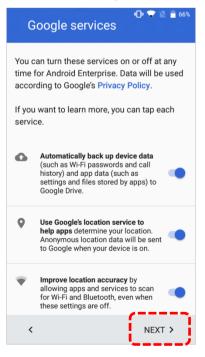
▪ **Step 5:**

Manually input "**afw#setup**" into the "**Email or phone**" field or scan the "**afw#setup**" barcode.

▪ **Step 6:**

Choose the Google services that you would like to enable and click "**Next**" to proceed.
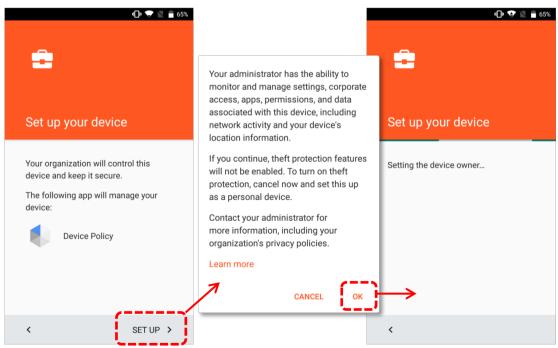
■ Step 7:

Click "**INSTALL**" to install the "**Android Device Policy**" App.

■ Step 8:
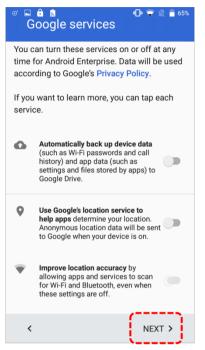
The ReMoCloud administrator will control the device through the "**Android Device Policy**". Click "**SET UP**" and "**OK**" to confirm that the device will be controlled as a work device by the ReMoCloud administrator.

185
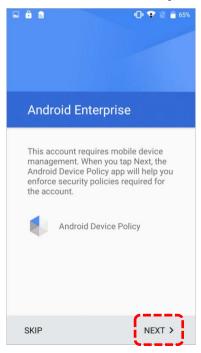
- Step 9:

Again, choose the Google services that you would like to enable and click "**Next**" to proceed.

- Step 10:

Again, confirm that the device will be controlled by the ReMoCloud administrator through "**Android Device Policy**". Click "**Next**" to proceed.
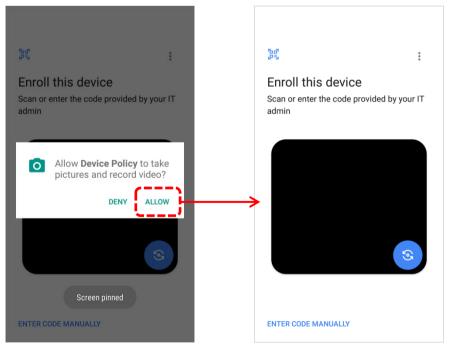
- **Step 11:**

It will take a while for the device to be updated.

- **Step 12:**
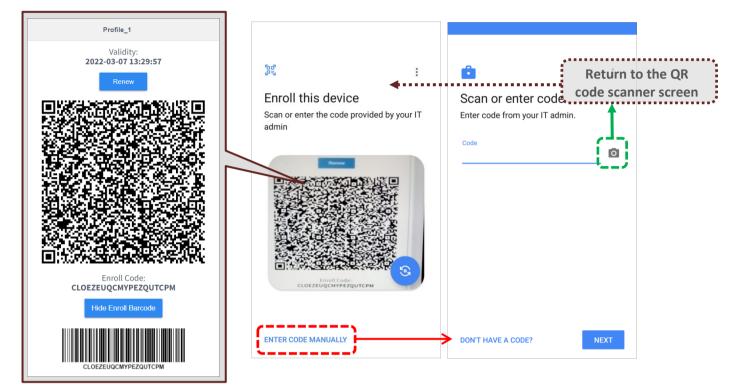
After the updating process is completed, click "**ALLOW**" to enable **Device Policy** using the device camera to scan the QR code for enrollment. The field for enroll code inputting will be offered later.
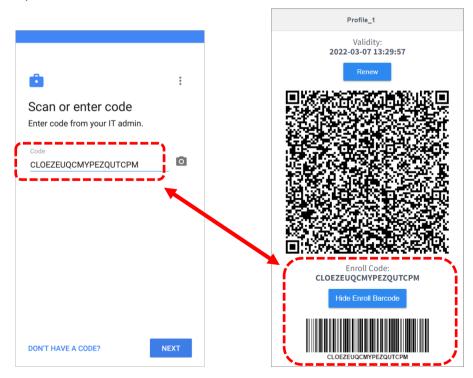
- Step 13:

Use the mobile computer's camera to take aim at the QR code generated by ReMoCloud.

Or click "**ENTER CODE MANUALLY**" to enter the "**Scan or enter code**" page. The user can either input the "**Enroll Code**" displayed under the QR code or scan the "**Enroll Barcode**" by the device's scanner.

- Step 14:

The enrollment process will take a while.

Click the "more button" ⋮ and select "**Reset Device**" to reset the device if necessary.

When the enrollment is completed, the user will subsequently enter **the default home screen / CipherLab Home** / **Multi App Mode** previously set by the applied profile.
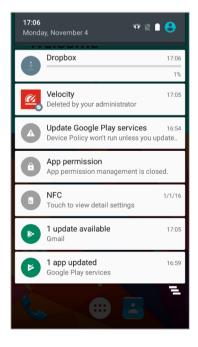
For more details about the related settings, refer to **Lock Task**.

The device will start to install the Apps from the applied profile. Slide down the status bar to open the notification drawer and check the download progress.

For more details about the related settings of status bar, refer to **Lock Task**.

Note:

The status bar will be unavailable when "Multi App Mode" is enabled.

The user may find the enrolled device listed on the "**Device**" tab page of "**Monitor**" on ReMoCloud. As shown:

Note:

1. For more details about profile management, refer to **Deployment: Profile Management**.

2. For more details about enrolled device management, refer to **Device Management**.

3. The user can only enroll devices by inputting "Enroll Code" and scanning "Enroll Barcode" when the QR reader fails to download, or when the barcode "afw#setup" is used without tapping on the same spot for 6 times at the beginning.

3.3 ZERO-TOUCH ENROLLMENT

Zero-touch enrollment provides a streamlined process for Android devices setup. Administrators can assign configurations to devices online, which will then be automatically detected by devices upon powering on. It simplifies online configuration and enables users for immediate use of the devices upon unboxing.

3.3.1 LINK ZERO-TOUCH ACCOUNTNOTE:

Before beginning the enrollment, please contact CipherLab to create your own Zero-touch account.

1. Nevigate to the "**Enrollment**" page and tap on "**Zero-touch**".

2. Select a profile you created and tap on "**Next**".

3. Copy the **DPC extras** for later use. Continue to tap on "**Copy & Link Zero-touch Account**".

4.Sign in to link your zero-touch account.

5.Select the account to link and tap "**Link**" and "**Next**" to proceed.
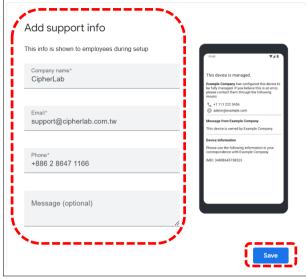
6. Fill the columns which will be shown to employees during setup, and tap "**Save**".

Now, you can view your zero-touch accounts and configuration information.

Tap on "**View devices in the zero-touch portal**" to view more information in the portal.

3.3.2 CREATE CONFIGURATIONS

1. Nevigate to "**Configuration**" page, and tap "**+**" to add a new configuration.

2. Fill in the columns.
Note to choose "**Android Device Policy**" for EMM DPC, and paste the **DPC extras** you previously copied.

Select "Android Device Policy".

Paste the "DPC extras" you previously copied.

3. Tap "**ADD**" to complete the configuration.

The created configuration will be listed on the page.

To change or delete the configuration, tap "**Edit**".

To set a default configuration:

1.Tap to choose one to apply to newly enrolled devices.

2.Tap on "**APPLY**".

The configuration will now apply to any new devices added to your account.

For more instructions about Zero-touch enrollment for IT admins, please refer to Android Enterprise Help.

Chapter 4

CHAPTER 4. DASHBOARD & APP
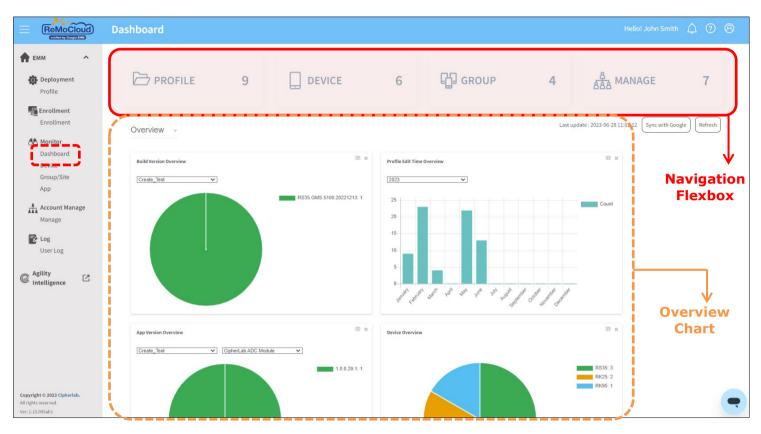
This chapter carries the detailed introduction of the functions offered by "**Dashboard**" and "**App**" on ReMoCloud.

IN THIS CHAPTER

4.1 DASHBOARD OVERVIEW

"**Dashboard**" is the page that presents a collection of graphical reports to give the user a full picture of the profile and device information.

1. Click the "**Home**" button 🏠 to expand the sidebar menu.
2. Click "**Dashboard**".

The "**Dashboard**" page includes two parts:
1. Four items in the navigation flexbox: Profile, Device, Site, and Manage.
2. Seven overview charts.
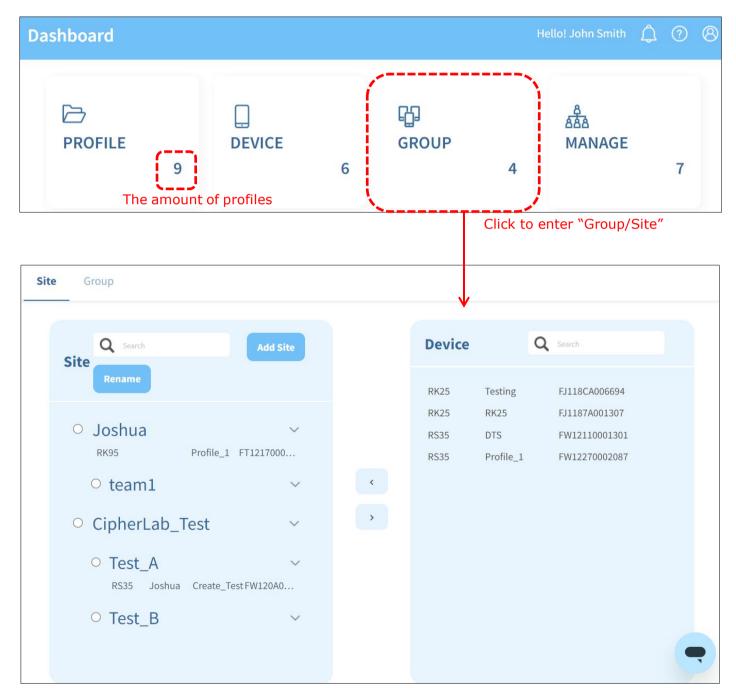
4.2 NAVIGATION FLEXBOX

The navigation flex container that includes the four items "**Profile**," "**Device**," "**Group**," and "**Manage**" is at the top of the "**Dashboard**" page.

The numbers under the items' titles respectively represent the amount of profiles, devices, groups, anb sub accounts.

Click on the flex items to enter the specific pages. As shown:

4.3   DASHBOARD OVERVIEW CHARTS

The overview charts visualize the general condition of the profiles, Apps, and devices on ReMoCloud. The 7 overview charts will all be displayed on the "**Dashboard**" page by default:

- App Version Overview:

Shows the proportion of a selected App's different versions in a selected profile.

- Build Version Overview:

Shows the proportion of the devices' build versions in a selected profile.

- Device Overview:

Shows the proportion of the enrolled devices' different models.

- Profile Edit Time Overview:

Shows the monthly edit counts of all profiles for the selected year.

- Application Analysis Overview:

The analysis and logs of the App's crash events.
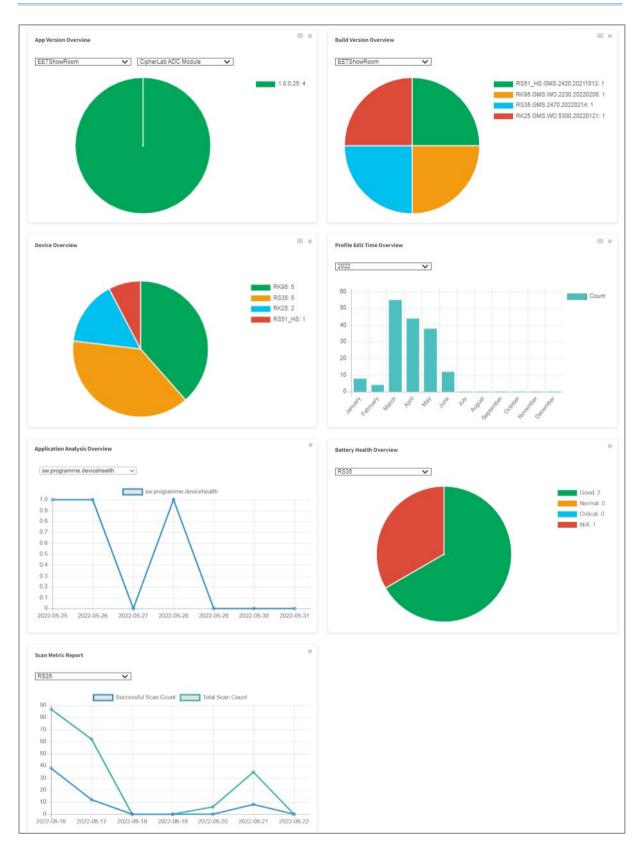
- Battery Health Overview:

The analysis of the device's battery health status.

- Scan Metric Report:

The statistical analysis of the device's barcode scanning records.

App Version Overview

EETShowRoom ▾   CipherLab ADC Module ▾

■ 1.0.0.25: 4

Build Version Overview

EETShowRoom ▾

■ RS51_HS.GMS.2420.20211013: 1
■ RK95.GMS.WO.2230.20220208: 1
■ RS35.GMS.2470.20220214: 1
■ RK25.GMS.WO.5300.20220121: 1

Device Overview

■ RK95: 5
■ RS35: 5
■ RK25: 2
■ RS51_HS: 1

Profile Edit Time Overview

2022 ▾

■ Count

Application Analysis Overview

sw.programme.devicehealth ▾

□ sw.programme.devicehealth

Battery Health Overview

RS35 ▾

■ Good: 2
■ Normal: 0
■ Critical: 0
■ N/A: 1

Scan Metric Report

RS35 ▾

□ Successful Scan Count   □ Total Scan Count

4.3.1   THE INFORMATION IN THE OVERVIEW CHARTS

The information about profiles, Apps, devices, and battery health will be summarized and visualized by the 7 overview charts.

APP VERSION OVERVIEW

There are two drop-down menus on "**App Version Overview**" for the user to select an activated profile and one of its "**User Installed Apps**". When the specific profile and App are selected, the pie chart will immediately show the proportion of the App's versions installed on all the enrolled devices in the profile.
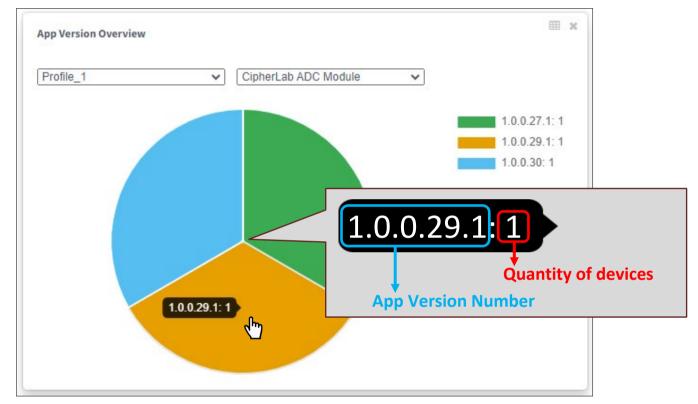
Note:

The access path for checking "User Installed Apps":

Device | Device Information (enter by clicking the device's model name) | Install App | User Installed Apps.

Move the cursor to the slice of the pie chart. It will demonstrate the quantity of the devices that apply to the App version.
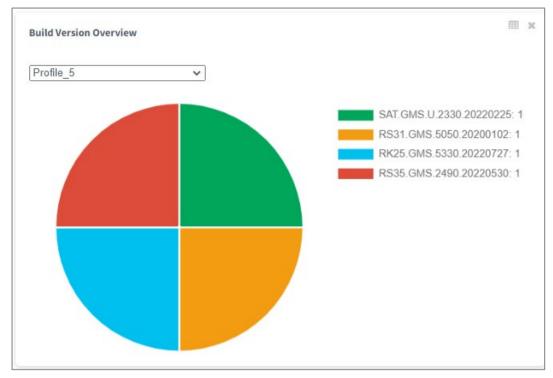
Click a slice to enter the "**Device of App**" page that lists the devices with their App versions.

BUILD VERSION OVERVIEW

After selecting a specific profile, the "**Build Version Overview**" pie chart will present the build version of all devices in the profile.

Move the cursor to the slice of the pie chart. It will demonstrate the proportion of the devices' build versions.

The build version and the quantity of devices will be displayed in the dialog box:
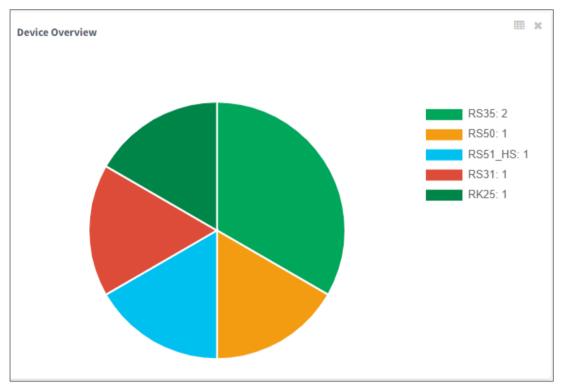
Click a slice to enter the device page that lists the devices with the same build version.

Note:

For more details about the functions of the listed devices on the device page, refer to "**Device Management**".

DEVICE OVERVIEW

The "**Device Overview**" pie chart offers the information about the proportion of different device models.

Each device model will be shown as a slice.
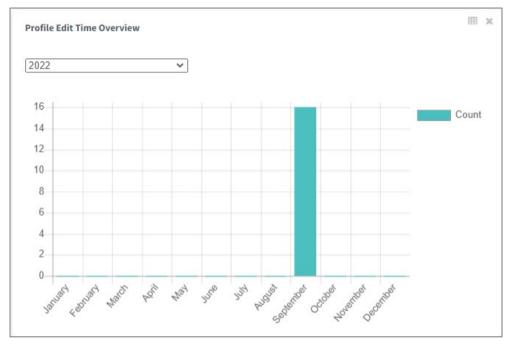
Click the slice to display all the enrolled devices with the same device model on the "device" page.

	Model Name	User Defined	Serial Number	Profile	Profile Current Ver	Build Version	Command Status
☐	RS35	Joshua	FW120A0002230	Create_Test	4	RS35.GMS.5100.20221213	
☐	RS35		FW12110001301	Profile_1	13	RS35.GMS.5100.20221213	
☐	RS35		FW12270002087	Profile_1	14	RS35.GMS.2530.20230322	
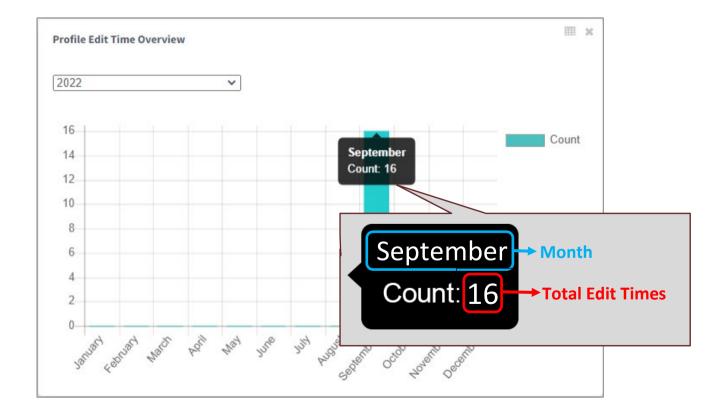
Device — Hello! John Smith

Search — Wipe | Delete | Lock | Reboot | Push Notification

Edit Column — 1 to 3 / Total Device(s) : 6 — Last update : 2023-06-29 11:20:55 — Sync with Google | Refresh

Note: For more details about the functions of the listed devices on the device page, refer to "**Device Management**".

PROFILE EDIT TIME OVERVIEW

"**Profile Edit Time Overview**" is the time series bar chart that demonstrates the editing data of all profiles.

Move the cursor on a specific bar to check the edit count of that month.
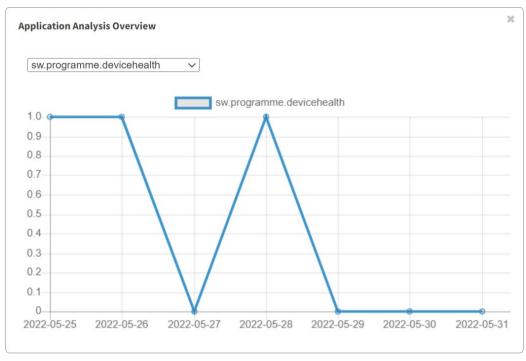
The user may also check the edit history by the following steps:

1) Enter the "Profile" page that lists the profiles with their **"Last Edit Time"**.

2) Click to enter the profile for checking.

3) Access the profile's previous version from the drop-down menu "**Version**" next to the profile name.
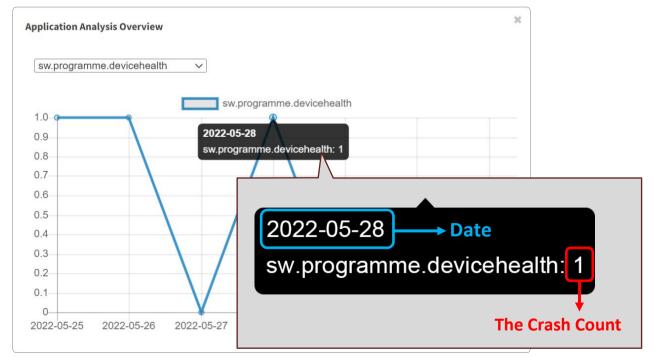
APPLICATION ANALYSIS OVERVIEW

"**Application Analysis Overview**" is the time series line chart with the horizontal axis representing date and the vertical axis representing crash count.

Select an App from the drop-down menu to present its crash events for the current week.
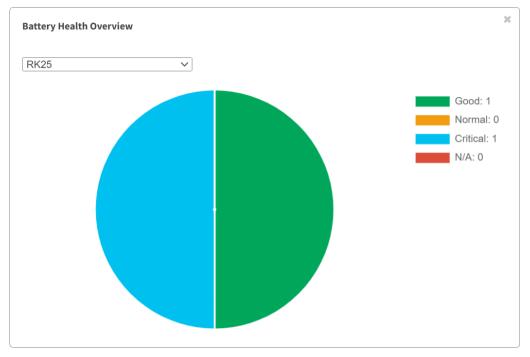
Move the cursor on a specific point to show the crash count of the day.
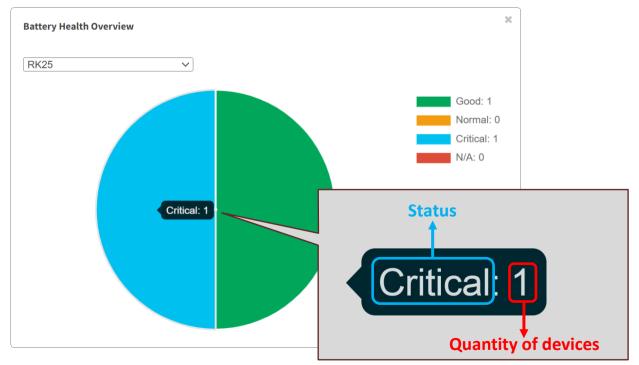
BATTERY HEALTH OVERVIEW

The "**Battery Health Overview**" pie chart represents the proportion of the enrolled devices' battery health status.

Select a device model from the drop-down menu to check the data.
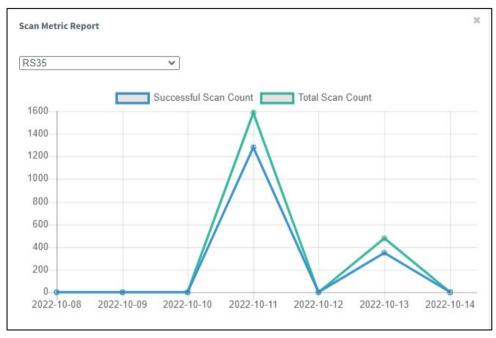
Move the cursor on a specific slice to show the quantity of devices for the certain battery health status.
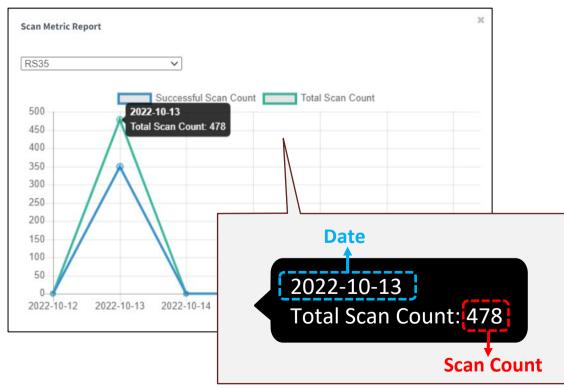
SCAN METRIC REPORT OVERVIEW

"**Scan Metric Report**" is the time series line chart that demonstrates the scan count data for the current week.

Select a device model from the drop-down menu to display its total scan count and successful scan count.

Move the cursor on a specific point to show the scan count of the day.

4.3.2   REVEAL & CONCEAL THE OVERVIEW CHARTS

In the top-left corner of the overview chart section, there will be a drop-down menu "**Overview**". Click to expand the menu. The checked items will be displayed as charts.
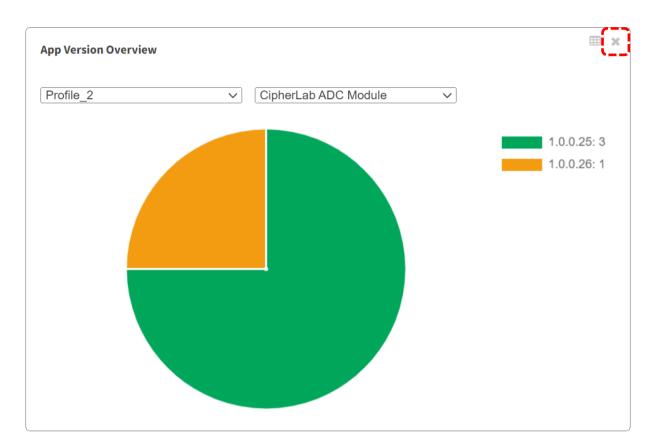
Uncheck the items to conceal the charts.
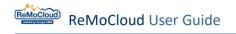
Check the items to reveal the charts.

ReMoCloud automatically saves the user's chart display settings.

Also, the user may conceal the chart by clicking the close button ✖ in its top-right corner.

App Version Overview

Profile_2   CipherLab ADC Module

1.0.0.25: 3
1.0.0.26: 1

4.3.3 ARRANGE THE CHARTS

Steps to arrange the charts:

1. Move the cursor to the chart. The cursor will change from arrow ⇖ to hand pointer ✋.

2. Drag and drop the chart onto the preferred place in the overview chart area.

ReMoCloud will automatically save the user's arrangement.
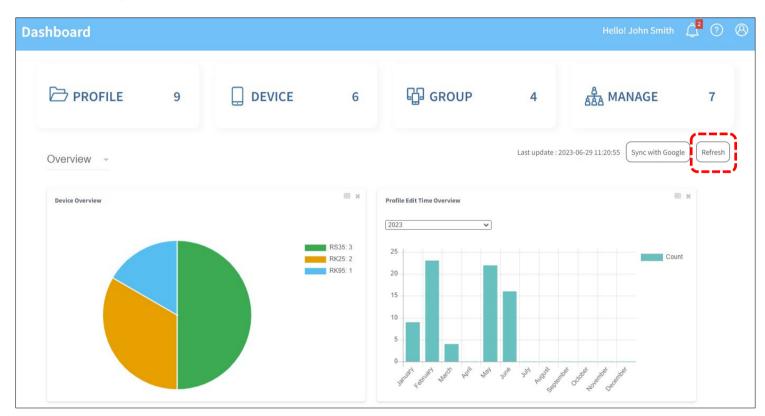
4.3.4 TO UPDATE THE DATA

In the top right corner of "Dashboard" page, there are two function buttons for updating the data, "**Sync with Google**" and "**Refresh**".

REFRESH

Click the "**Refresh**" button to update the data based on the condition for the last time ReMoCloud synchronized with Google system.Using this function will comparatively cause less system load.

SYNC WITH GOOGLE
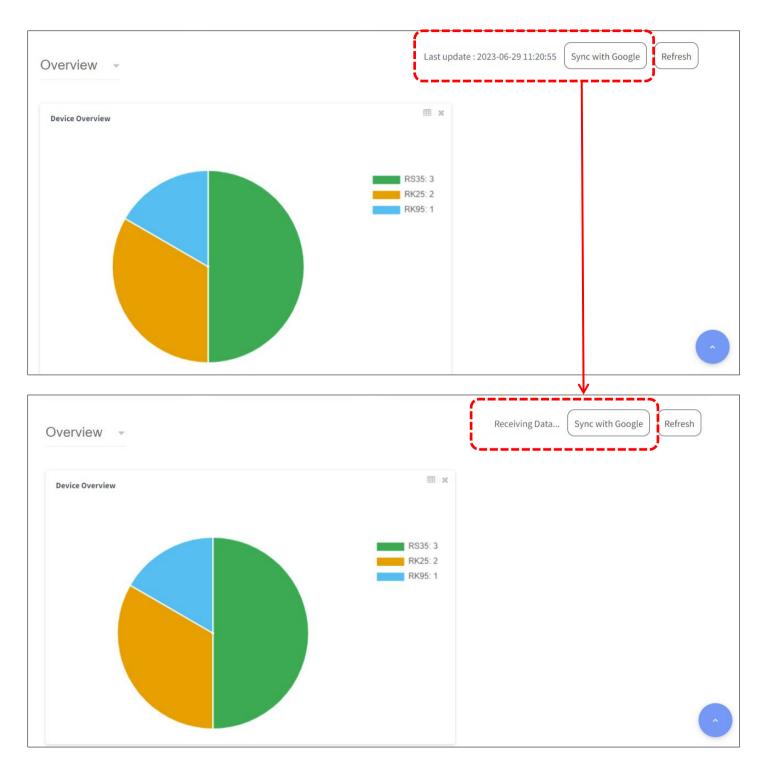
Click the "**Sync with Google**" button to update the data based on the most current conditions for all profiles and devices by synchronizing with the data from Google system.

While "**Sync with Google**" and "**Refresh**" are both for updating the data, "**Sync with Google**" will comparatively cause more system load.

After clicking "**Sync with Google**," it will take a while to receive and update data.
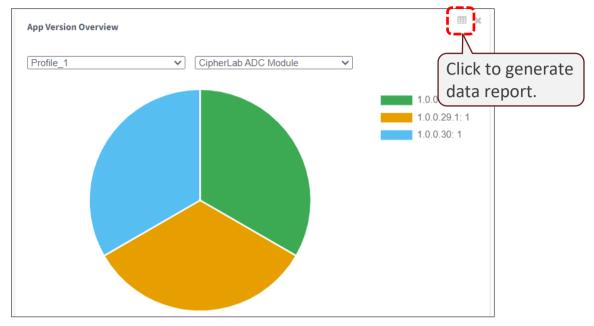
All group functions, such as profile assignment and wiping devices, will be temporarily unavailable during the data updating process.

When the status changes from "**Receiving Data…**" to "**Last update : YYYY-MM-DD HH:MM:SS**," the updating process is completed.

4.3.5 REPORT

Click the report button ⊞ to generate the data report in Excel format. The report file will be automatically downloaded on the user's PC.

APP VERSION OVERVIEW

The "**App Version Overview**" report will list all the activated profiles, the **user installed Apps**, the App versions of **user installed Apps**, and the quantity of devices that apply to the App version.

BUILD VERSION OVERVIEW

The "**Build Version Overview**" report will list all the activated profiles, the build versions of the devices that apply to the profiles, and the quantity of devices with the same build version.

DEVICE OVERVIEW

The "**Device Overview**" report will list all models of the enrolled devices and the quantity of devices for different models.

PROFILE EDIT TIME OVERVIEW

The "**Profile Edit Time Overview**" report demonstrates the monthly edit counts of all profiles for the selected year.

4.4 APPLICATION

The "**Application**" page lists all the "**User Installed Apps**" and the built-in third-party Apps on all enrolled devices.

The information provided by the **App** page includes:

- App Name

The App's name.

- Package Name

What allows the App to be uniquely identified on the devices and in Google Play Store.

- Profile Count

The number of the profiles that include the App.

- Device Count

The number of the devices that have the App installed.
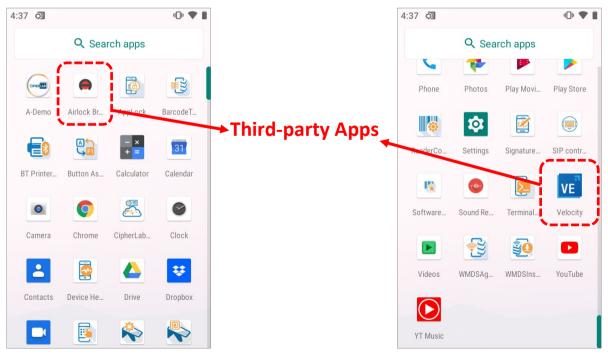
- Update required

"Yes" means that the app is in need of update. "No" means that the app is already updated to the latest version.

The user may check "User Installed Apps" through Device > Device Information > Install App > Managed Installed Apps.

Depending on different device models, third-party Apps may or may not be allowed for installation on the device. The figures below are the examples showing the third-party Apps installed on RK25.

225

4.4.1 PROFILE COUNT

Click the profile count of a specific App to enter its "**Activated Profile of App**" page. Profiles that contain the App will be listed on the page:

Click the profile's name to enter the "**Profile Information**" page for additional settings.

For more details, refer to "**Edit a Profile: APP**" and "**Edit a Profile: Device Setting**".

4.4.2 DEVICE COUNT

Click the device count of the App to enter the "**Device of App**" page. In this page, the user may check which devices have the App installed. Moreover, click the model name to enter "**Device Information**" page for checking this device's App and its setting information.

Chapter 5

CHAPTER 5. DEVICE MANAGEMENT

This chapter specifies the details of the enrolled devices' management, including unenrolling the device, locking the device screen, checking the enrolled device's information, and generating the device reports.

IN THIS CHAPTER

5.1 OVERVIEW

The "**Device**" tab page lists all the enrolled devices.

ENROLLED DEVICE LIST

The items for the "Edit Column" button in the top-left corner:

- Model Name:

The device model name.


- User Defined:

The field for the user to put a mark on the device. With the marks, the user is allowed to distinguish the devices from each other with the same model name.

- Serial Number

The serial number of the device.

- Battery Level

Move the cursor on the battery icon to display the percentage of remaining battery charge.

- Ring Device

To locate the device by making it ring.

▪ Group

The group to which the device belongs.

▪ Profile

The profile to which the device applies.

▪ Site

The site to which the device applies.

▪ Profile Current Ver

This column shows if the device applies to any designated profile.

If so, it will demonstrates the profile's version number. If not, it will show "Not Applied".

Item	Description
Green Version Number	The profile that this device applies to is the latest version.
Red Version Number	The profile that this device applies to is the old version.
Not Applied	The device does not apply to any designated profile.
0	The profile that this device applies to is unedited. 0 in green suggests that this profile is the latest version, while red suggests the old version.

▪ Profile Latest Ver

The latest version number of the designated profile.

▪ Build Version

The build number of the device.

▪ IMEI

The IMEI number of the device.

▪ Command Status

Showing the executing command, such as "**Locking**," "**Wiping**," and "**Rebooting**".

- Remote Control

The "**Remote Control**" buttons are for remote controlling the registered device. Note that there will be extra charges for activating the "**Remote Control**" functions.

For more details, refer to **Remote Control**.

- Status

Showing the executing command, such as "**Locking**," "**Wiping**," and "**Rebooting**".

DEVICE SETTING BUTTONS

The setting buttons on the "**Device**" page are:

Item	Description
Wipe	To restore the selected devices to their factory default settings and remove their data from ReMoCloud.
Delete	To remove the selected devices' data from ReMoCloud without restoring them to their factory default settings.
Lock	To turn off the selected devices' screens.
Reboot	To boot the selected devices again.
Push Notification	To pass text messages on to the selected devices.
Report (click ⋮ to show)	To generate the report about the selected devices.
Schedule Report (click ⋮ to show)	To make plans for automatically generating reports about all the enrolled devices. The reports will be sent to the designated e-mail address.
Reset Password (click ⋮ to show)	To set new passwords for the selected devices.
Pre-User Defined (click ⋮ to show)	To demonstrate the devices and their serial numbers as a list for more efficient reviewing.
Enable Remote Control (Selected) (click ⋮ to show)	To enable remote controlling of the selected devices. Please refer to Appendix III for details.
Enable Remote Control (All) (click ⋮ to show)	To enable remote controlling of all devices. Please refer to Appendix III for details.
Sync with Google	To update the data based on the most current conditions for all devices by synchronizing with the data from Google system. Using this function will comparatively cause more system load.
Refresh	To update the data based on the condition for the last time ReMoCloud synchronized with Google system. Using this function will comparatively cause less system load.

5.2 ENROLLED DEVICE LIST

The users are able to choose items to be displayed, to put marks on the enrolled devices, to sort and search from the device list, and to enter the "**Device Information**" page to check the devices' detailed settings.

5.2.1 MOVE/ SHOW/ HIDE COLUMN

Click "**Edit Column**" to unfold the drop-down menu for column items.
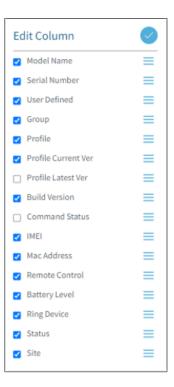
The user can display the list in the way they preferred by editing the columns.

Click "**Edit Column**" to unfold the menu and select the items to show on the header row of the list.

Click "**Edit Column**" again to fold the menu.

By clicking ☰, drag and drop to arrange the order of the header row items.
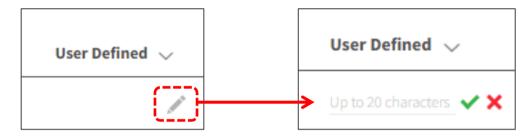
5.2.2   USER-DEFINED

The "**User Defined**" field is for the user to put marks on the devices. With the marks, the user is allowed to distinguish the devices from each other with the same model name.

To put a mark on the device:

1. Click the "**Edit**" button 🖊 of the device to make the editable field appear.

2. Including white-space and punctuation marks, the user is allowed to input no more than 20 characters.

3. Click ✔ to save. Or, click ✖ to exit the edit mode without saving.

.

To remove the mark:

1. Click the "**Edit**" button 🖊

2. Eliminate the mark and click ✔ to save.

Note:

The user defined information is only for the ReMoCloud administrator to check on ReMoCloud. It will not be displayed on the device.

5.2.3   SORTING THE ENROLLED DEVICES

In the "**Device**" tab page, the user may sort the displayed information by the header row items.

Click the sort button ⌄   of the header row item to display the device list in ascending order. Click it again to display the list in descending order. As shown:

▶   Ascending (click once)   ⌃

	Model Name ⌄	Serial Number ⌄	User Defined ⌄	Group ⌃	Profile ⌄	Profile Current Ver ⌄	Build Version ⌄	IMEI ⌄	Mac Address
☐	RK95	FT12170003374		Group_1	Profile_1	19	RK95.GMS.WO.2230.20...	None	00:d0:17:d0:90
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test	8	RS35.GMS.5100.20221213	354576110044584	00:d0:17:b9:11
☐	RK25	FJ118CA006694		Group_3	Testing	7	RK25.GMS.8130.20220930	354538090088288	00:d0:17:bc:96
☐	RS35	FW12260004001		None	Profile_1	19	RS35.GMS.S0071.20230...	354576110933083	00:d0:17:d2:19
☐	RK25	FJ1187A001307		None	RK25	44	RK25.GMS.WO.8110.20...	None	00:d0:17:be:e5
☐	RS35	FW12110001301		None	Profile_1	19	RS35.GMS.5100.20221213	354576110176006	00:d0:17:b9:44
☐	RS35	FW12270002087		None	Profile_1	19	RS35.GMS.2530.20230322	None	00:d0:17:d2:2e

Wipe | Delete | Lock | Reboot | Push Notification

Edit Column   1 to 7 / Total Device(s) : 7   Last update : 2023-07-11 10:21:32   Sync with Google   Refresh

▶   Descending (click twice)   ⌄

	Model Name ⌄	Serial Number ⌄	User Defined ⌄	Group ⌄	Profile ⌄	Profile Current Ver ⌄	Build Version ⌄	IMEI ⌄	Mac Address
☐	RS35	FW12260004001		None	Profile_1	19	RS35.GMS.S0071.20230...	354576110933083	00:d0:17:d2:19
☐	RK25	FJ1187A001307		None	RK25	44	RK25.GMS.WO.8110.20...	None	00:d0:17:be:e5
☐	RS35	FW12110001301		None	Profile_1	19	RS35.GMS.5100.20221213	354576110176006	00:d0:17:b9:44
☐	RS35	FW12270002087		None	Profile_1	19	RS35.GMS.2530.20230322	None	00:d0:17:d2:2e
☐	RK25	FJ118CA006694		Group_3	Testing	7	RK25.GMS.8130.20220930	354538090088288	00:d0:17:bc:96
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test	8	RS35.GMS.5100.20221213	354576110044584	00:d0:17:b9:11
☐	RK95	FT12170003374		Group_1	Profile_1	19	RK95.GMS.WO.2230.20...	None	00:d0:17:d0:90

Wipe | Delete | Lock | Reboot | Push Notification

Edit Column   1 to 7 / Total Device(s) : 7   Last update : 2023-07-11 10:21:32   Sync with Google   Refresh

5.2.4 FILTERING THE ENROLLED DEVICES

To search for the specific device from the device list:

1. Click the filtering button ▼ of the header row item to expand the editable "**Filter**" field.

	Model Name ⌄	Serial Number ⌄	User Defined ⌄	Group ⌄	Profile ⌄	Battery Level	Remote Control	Profile Current Ver ⌄
☐	RS35	FW120A0002230	Testing ✎	Group_2	Create_Test	🔋	👁	8
☐	RS35	FW12260004001	✎	None	Profile_1	🔋	👁	22
☐	RK25	FJ1187A001307	✎	None	RK25	🔋	👁	44
☐	RK95	FT12170003374	✎	Group_3	Testing	🔋	👁	7
☐	RS35	FW12110001301	✎	None	Profile_1	🔋	👁	22
☐	RS35	FW12270002087	✎	None	Profile_1	🔋	👁	22

2. Enter keywords to search from the column. The matching devices will be displayed.

The user may set multiple filter criteria to refine the results.

5.3 DEVICE INFORMATION

The **"Device"** page enables administrators to retrieve information and manage the content of enrolled devices. Additionally, administrators can access device logs for analysis or troubleshooting purposes. Click "**Device**" and then click on the "**Model Name**".

5.3.1 DEVICE AND SETTINGS OVERVIEW
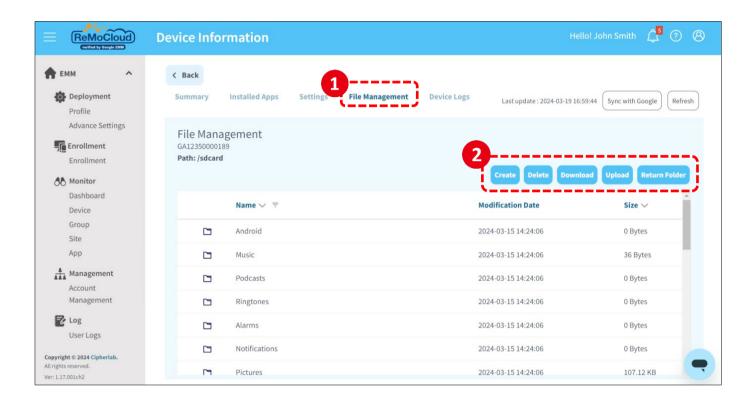
Click "**Summary**," "**Install App**," and "**Settings**" for more details about the device and its settings. Click "**Sync with Google**" or "**Refresh**" to receive the most recent data.

5.3.2 FILE MANAGEMENT

"**File Management**" enables administrators to perform actions such as creating, deleting, downloading, and uploading files from the PC to devices via ReMoCloud.

1. Click on "**Model Name**" on the "**Device**" page to enter "**Device Information**" page.
2. Tap "**File Management**" from the upper panel.
3. Manage the file by clicking buttons on the lower panel to perform desired actions.

CREATE
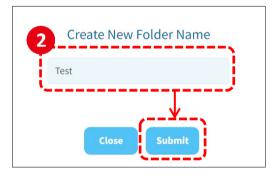
To create a folder on the device:

1. Tap "**Create**" in the chosen path.

A pop-up window will appear to prompt you to name the folder.

2. Enter the name and tap "**Submit**".

A pop-up window appears to show the folder is successfully added to the device.
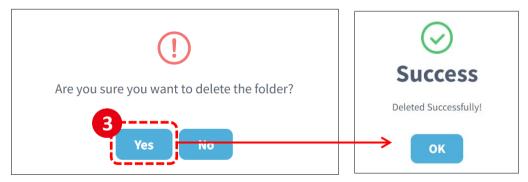
DELETE

To delete a folder or file on the device:

1. Select a folder or a file you would like to delete.

2. Tap "**Delete**".

3. A confirmation pop-up will appear. Tap "**Yes**" to proceed the action.

DOWNLOAD

To download a file from the device to the PC:

1. Find the file you want to download on the page.

2. Tap "**Download**".

A pop-up window will appear confirming the successful download of the file.

UPLOAD

To upload a file from your PC to the device:
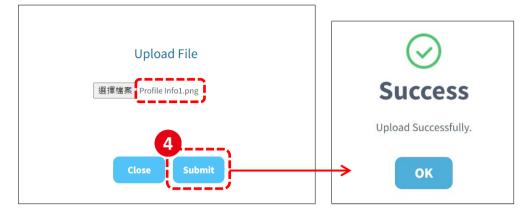
1. Locate the destination folder for your upload.

2. Tap "**Upload**" .

3. Select the file by tapping on the button 選擇檔案 .

After selecting the file, it will be displayed on screen.

4.Tap "**Submit**". A pop-up window will appear confirming the successful upload of the file.

RETURN FOLDER

To return a higher layer of the folder, tap "**Return Folder**".

5.3.3 DEVICE LOGS

The "**Device Logs**" function allows administrators to retrieve logs from the device. Administrators can download the logs which can then be uploaded to the cloud for examination. This allows for further analysis or troubleshooting as needed.

1. Tap "**Device Logs**" on the Device Information page.

2. Click on the "**Get Latest Logs**" button.

The screen will first display "**Getting Log**" in red. After some time, a pop-up window will appear to show that you got the latest log successfully.

3. Click on "**OK**", then tap the ZIP file displayed on screen to complete download device logs.

To delete the log, tap on the 🗑 icon.

A confirmation pop-up will appear. Tap "**Yes**" to proceed the action.
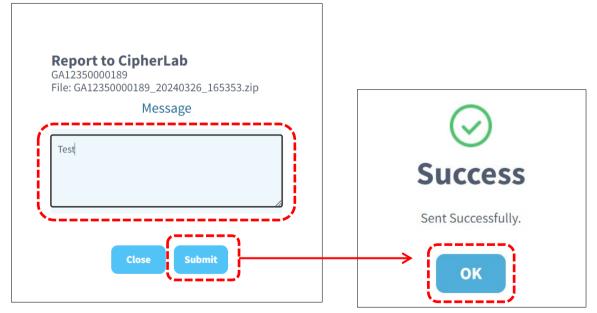
To receive further assistance from CipherLab:

1. Tap on "**Report**".

2. A pop-up window appears, prompting you to describe the problem you encountered. Type in the problem and tap "**Submit**" to proceed.

CipherLab Support will review your message and device log to offer further assistance.

5.4 DEVICE SETTING BUTTONS

In "Device" page, setting buttons offer the following functions for ReMoCloud adminstrators to manage the enrolled devices.

There are 13 settings buttons, including "Wipe," "Delete," "Lock," "Reboot," "Push Notification," "Report," "Schedule Report," "Reset Password," "Pre-User Defined," "Enable Remote Control(Selected)," "Enable Remote Control(All)," "Sync with Google," and "Refresh".

To use the functions "**Report**," "**Schedule Report**," "**Reset Password**", "**Pre-User Defined**," "**Enable Webkey Remote Control(Selected)**," "**Enable Webkey Remote Control(All)**," "**Device Transfer**," and "**Assign Geofence Settings**,"click ⋮ in the top-right corner to unfold the drop-down menu.

For "**Wipe**," "**Delete**," "**Lock**," "**Reboot**," "**Push Notification**," "**Reset Password**," "**Enable Remote Control(Selected)**," and more, the user has to select at least one device first before clicking the setting buttons.

248

Chapter 5. Device Management

5.4.1 REPORT

The user may generate a report to examine the information of the enrolled devices:

1) Click ⋮ to show the drop-down menu. Click "**Report**" to reveal the item selecting menu.

    By checking items, the user can create custom reports to obtain more specific data.

2) Click "**OK**" to export the report to an Excel .csv file and download it on the PC.

249

5.4.2 SCHEDULE REPORT

"**Schedule Report**" is to automatically generate a report that provides a list of dozens of devices details. This report will be sent to the designated e-mail address.

To set the e-mail address for receiving the report:

1. Click the "schedule report" button to enter the setting page.

Click "**Edit**" to make the pop-up window for e-mail address setting appear.

Click "**Add**" to continue.

2. Enter the e-mail address for receiving the report and click "Submit".

3. The e-mail address is successfully set. Click "**Add**" and repeat the same steps to set more e-mail addresses.

Click the toggle switch button to select the days on which the reports will be generated.

Make sure to save the changed settings before leaving this page.

As shown, the reports will be generated and sent to the designated e-mail address on the selected days.

5.4.3 RESET PASSWORD

Click ⋮ in the top-right corner to show the "Reset Password" button.

Select the devices for changing the password.

To reset the password of multiple devices at the same time, the selected devices must apply to the same profile.

▪ When the devices apply to different profiles, it will fail to reset. As shown:

1. Select the devices that apply to the same profile first, and click the "**Reset Password**" button.

Please enter your new password

Your new password must fulfil the value of "Password History Length" .

New password

Reset_Password_Testing 👁

Repeat password

Reset_Password_Testing 👁

Cancel   Next

2. Enter the new password that corresponds with the settings in "**Password History Length**".

Back

Please select the action

Select the action to be performed after the password is reset.

🔘 None

⭕ Lock the device(s) now

Cancel   Next

3. Select the action to be performed on the selected devices after changing their device password.

Click "**Next**" to proceed.

Back

Please enter your ReMoCloud login password

Enter your ReMoCloud login password to confirm the change of the device password.

••••••••

Cancel   Next

4. Enter the user's ReMoCloud login password to confirm changing the device password.

Click "Next" to proceed.

✓ Success

OK

5. The password of the selected devices is successfully changed.

Note that the devices will be locked right away if selecting "**Lock the device(s) now**" in step 3.

5.4.4   PRE-USER DEFINED

The "**Pre-User Defined**" function allows users to efficiently examine the devices and their serial numbers.

Note that the "**Pre-User Defined**" function exclusively supports importing .csv files. Therefore, it is important to know how to generate a .csv file to utilize this "Pre-User Defined" effectively.

HOW TO CREATE A .CSV FILE FOR PRE-USER DEFINED

The **.csv** file should contain the following information:
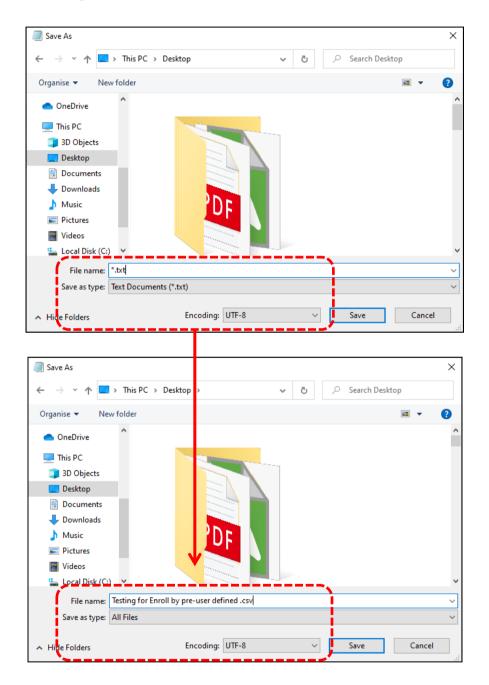
- Serial Number
- User Defined

Open a **Notepad** file. Input the devices' serial numbers and their user-defined marks in sequence, one device per row. The serial number and the user-defined mark are only separated by a comma without any other characters or symbols. For example:

After finishing inputting, click **"File"** and select "**Save As…**"

1) For the "**File name**" field, input a name and manually change the filename extension from **.txt** to **.csv.**
2) For the "**Save as type**" field, select "**All Files (*.*)**".
3) For the "**Encoding**" field, select "**UTF-8**".

The .csv file is successfully created and ready to be imported to the "**Enroll by pre-user defined**" setting page on ReMoCloud.

IMPORT, EXPORT, AND DELETE

On the "**Enroll by pre-user defined**" setting page, click the "**import**" button to upload the file.

Click the "**Choose File**" button to select the .csv file and click the "**Submit**" button to upload.

When the file is successfully imported, a pop-up window will appear to notify the user of the completion, and the imported .csv file will simultaneously be demonstrated as a list on the "Enroll by pre-User Defined" setting page.

After importing a .csv file, the "Export" button and the "Delete" button in the top-right corner will become available.

The user may click the "Export" button to export the list to an Excel .csv file for reviewing. After clicking "Export," a pop-up window will appear for the user to enter a name for the file. After inputting a name, click "Submit" to download the file on the PC. Or, click "Cancel" to undo.
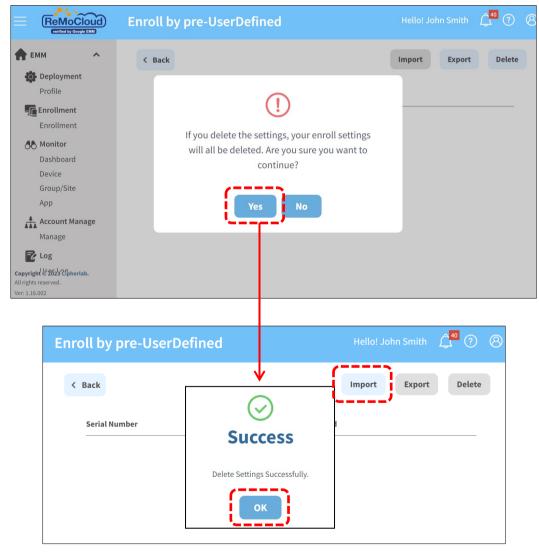
The exported file will be saved in the default download location.

Click the "Delete" button to eliminate the settings. Next, click "Yes" on the warning pop-up window to confirm deleting the settings on the "Enroll by pre-User Defined" page.

The user will be able to import new settings after deletion.

5.4.5 ENABLE WEBKEY REMOTE CONTROL (SELECTED)

To enable Webkey Remote Control to your selected devices, please nevigate to "**Device**" page:
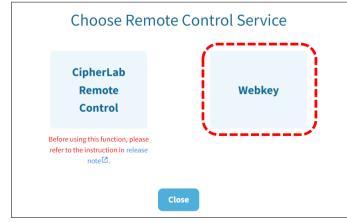
1. Select the device for remote control.

2. Click ⋮ in the top-right corner to tap "**Enable Webkey Remote Control (Selected)**".

3. A pop-up window appears reminding users to ensure the device is powered on and connected to a stable internet. Tap "**OK**" to continue.

4. Return to the device page, and click on the "**Remote eye**" button ◉. Webkey Remote Control is now available.

5.4.6 ENABLE WEBKEY REMOTE CONTROL (ALL)

To enable Webkey Remote Control to all enrolled devices at once, please nevigate to "**Device**" page:

1. Click ⋮ in the top-right corner to tap "**Enable Webkey Remote Control (All)**".

3. A pop-up window appears reminding users to ensure the device is powered on and connected to a stable internet. Tap "**OK**" to continue.

4. Return to the device page, and click on the "**Remote eye**" button . Webkey Remote Control is now available.

5.4.7 DEVICE TRANSFER

"**Device Transfer**" allows users to transfer the devices between different accounts. To transfer the device:

1. Navigate to the "**Device Page**" and select the devices for transfer.
2. Tap ⋮ then continue to tap on "**Device Transfer**".

3. Select the account to transfer to and tap "**OK**".

The device is successfully transferred to the selected account.

5.4.8 ASSIGN GEOFENCE SETTING

Geofencing helps admins manage devices with location-based rules. Utilize the "**Assign Geofence Setting**" function to set actions when devices enter or exit designated areas.

Note: Before assigning geofence settings to devices, make sure to create the desired Geofencing Setting in the "Advanced Settings" page.

1. Navegate to the "**Device Page**" and select the devices for geofence assignment.
2. Tap ⋮ then continue to tap on "**Assign Geofence Setting**".

3. Tap "**OK**" to complete the assignment after choosing your desired Geofence Setting from the dropdown list. A pop-up menu will confirm successful assignment of the Geofencing Setting to the devices.
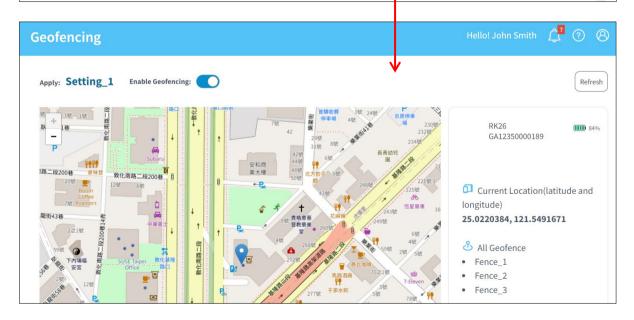
CHECK GEOFENCE ASSIGNMENT

After assigning Geofence Settings to the device, you are able to check the assignment on the Device page.

Click on the assigned geofencing to enter the Geofencing page.
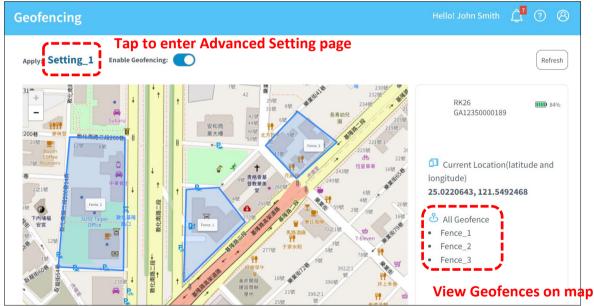
The Geofencing page shows the applied setting name, device location, and the created geofences. Users can toggle the geofencing function on or off as well.

To access the Advanced Setting page for editing, tap on the setting name.
To view geofences on the map, click on their names listed under "All Geofence".

5.4.9   WIPE

The function, "**Wipe**," is to restore the selected devices to their factory default settings and to remove their data from ReMoCloud.

Select the device and click the "Wipe" button.

Click "OK" on the pop-up warning window to proceed.

Enter the user's ReMoCloud password to confirm wiping the selected devices.

5.4.10 DELETE

The function, "**Delete**," is to remove the selected devices from ReMoCloud's device management list. Note that deleting a device does not "**Wipe**" or restore the device to its factory default settings.

Select the device and click the "Delete" button.

Click "OK" on the pop-up warning window to proceed.

Enter the user's ReMoCloud password to confirm deleting the selected devices.

5.4.11 LOCK

Select devices and click the "**Lock**" button to turn off their screens. The user will need to unlock the screen first if the screen lock is set on the device.

Select the device and click the "Lock" button.

A pop-up window will appear to remind the user that the selected device's screen is locked successfully.

5.4.12 REBOOT

The function, "**Reboot**," is to shut down and restart the selected devices.

Select the device and click the "Reboot" button.

A pop-up window will appear to remind the user that the selected device is successfully rebooted.

5.4.13 PUSH NOTIFICATION

"**Push Notification**" is to pass text messages on to the selected devices.

Before clicking the "Push Notification" button, the user should select at least one device. Namely, the user is allowed to send messages to multiple devices simultaneously.

After selecting devices, click the "Push Notification" button to make the "Message" pop-up window appear.

On the pop-up window, there will be a text area and two buttons, "Cancel" and "Submit".

Including digits, punctuation marks, and symbols, the user may input no more than 100 characters.

For example:

After entering the text, click "Submit" to pass the text on to the devices or click "Cancel" to undo. When the text is successfully sent, the process will be followed by another pop-up window notifying the user of the completion, and the text message will be displayed on the device. As shown:

5.4.14 SYNC WITH GOOGLE

Click the "**Sync with Google**" button to update the data based on the most current conditions for all devices by synchronizing with the data from Google system.

While "**Sync with Google**" and "**Refresh**" are both for updating the data, "**Sync with Google**" will comparatively cause more system load.

After clicking "**Sync with Google**," it will take a while to receive and update data.

5.4.15 REFRESH

Click the "**Refresh**" button to update the data based on the condition for the last time ReMoCloud synchronized with Google system.

While "**Sync with Google**" and "**Refresh**" are both for updating the data, "**Refresh**" will comparatively cause less system load.

	Model Name	Serial Number	User Defined	Group	Profile	Battery Level	Remote Control	Profile Current V
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test		👁	8
☐	RS35	FW12260004001		None	Profile_1		👁	23
☐	RK25	FJ1187A001307		None	RK25		👁	44
☐	RK95	FT12170003374		Group_3	Testing		👁	7
☐	RS35	FW12110001301		None	Profile_1		👁	23
☐	RS35	FW12270002087		None	HCT		👁	48
☐	RK25	FJ118CA006694		Group_3	Testing		👁	7

Wipe | Delete | Lock | Reboot | Push Notification

Edit Column | 1 to 7 / Total Device(s) : 7 | Last update : 2023-07-14 18:04:32 | Sync with Google | Refresh

5.4.16 SEARCH BOX & QUANTITY PER PAGE

In the top-left corner of the "Device" page, there is the search box for the user to search for specific devices.

Enter the keywords in the text area to search.

Search ⟶ Click to enter the keywords

Only the matching results will be displayed.

	Model Name	Serial Number	User Defined	Group	Profile	Battery Level	Remote Control	Profile Current V
☐	RK25	FJ1187A001307		None	RK25		👁	44
☐	RK25	FJ118CA006694		Group_3	Testing		👁	7

1 to 2 / Total Device(s) : 7 Last update : 2023-07-14 18:04:32

In the bottom-right corner, click the quantity box to unfold the menu.

By unfolding the menu, you can select the number for the devices to be displayed on a page.

The options include 50, 100, and 150.

	Model Name	Serial Number	User Defined	Group	Profile	Battery Level	Remote Control	Profile Current V
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test		👁	8
☐	RS35	FW12260004001		None	Profile_1		👁	23
☐	RK25	FJ1187A001307		None	RK25		👁	44
☐	RK95	FT12170003374		Group_3	Testing		👁	7
☐	RS35	FW12110001301		None	Profile_1		👁	23
☐	RS35	FW12270002087		None	HCT		👁	48
☐	RK25	FJ118CA006694		Group_3	Testing		👁	7

1 to 7 / Total Device(s) : 7 Last update : 2023-07-14 18:04:32

50
100
150
50 Quantity/Page

|< < 1 /1 > >|

Chapter 6

CHAPTER 6. GROUP MANAGEMENT

This chapter carries the detailed introduction of the functions offered by "**Group"** and **"Site**", especially specifying how to create a group and how to manage the enrolled devices in a group.
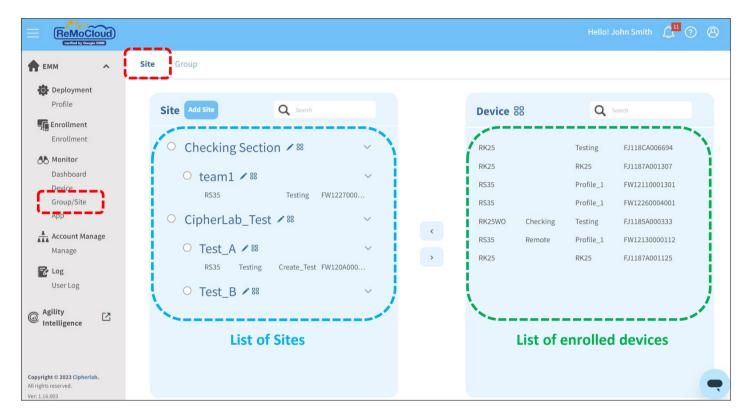
IN THIS CHAPTER

6.1 SITE

"**Site**" is for you to effectively categorize your devices, allowing you to organize the enrolled devices more efficiently.

Access "**Group/Site**" > "**Site**" :

The functions of the buttons on the "**Site**" page:

Button	Description
Add Site **Add Site**	To create a new site.
Add Sub Site ➕	To create a new site under a certain upper-level site.
Edit Site Name ✏️	To give the site a new name.
Select all ⊞	To select all the devices on the list or in the site.
Delete Site —	To eliminate the site.

6.1.1 CREATE A NEW SITE

Follow the steps to create a new site:

1. Click **Add Site** to open the "Add New Site Name" pop-up window.

2. Enter a name for the new site and click "Submit".

6.1.2 ADD A SUB SITE

Follow the steps to create a sub-site:
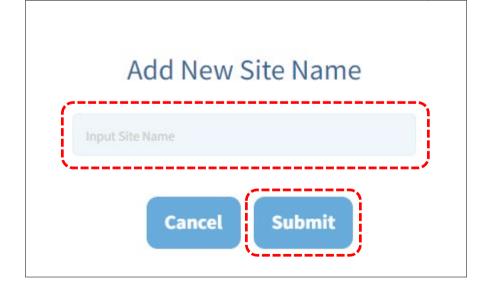
1) Make sure you have an existing site where you want to create a sub-site.

2) Move the cursor to the site. The function buttons ➕ and ➖ will appear.

3) Click ➕ to open the "Add New Site Name" pop-up window.

4) Enter a name for the new sub-site and click "Submit".

Note:

You are not allowed to add a sub-site under a sub-site.

6.1.3 EDIT SITE NAME

Follow the steps to edit the name of a site or a sub-site:
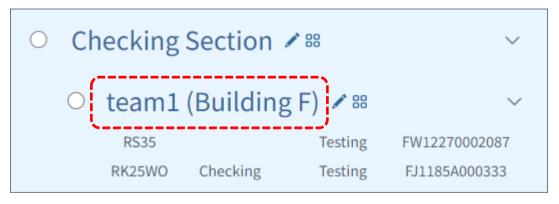
1) Click ✏ to open the "Edit Site Name" pop-up window.

2) Enter a new name and click "Submit".

3) The name is successfully changed.

6.1.4 DELETE A SITE

Follow the steps to delete a site or a sub-site:

1) Move the cursor to the site. The function buttons ✚ and ▬ will appear.
2) Click ▬.
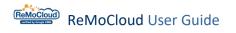
3) Click "OK" to eliminate the site.

4) The site is successfully deleted.

6.1.5 ASSIGN SITE

On the "Site" page, you can assign devices to sites.

On the right side, all devices without a site will be listed with their user-defined, applying profiles, and serial numbers on the "Device" section.
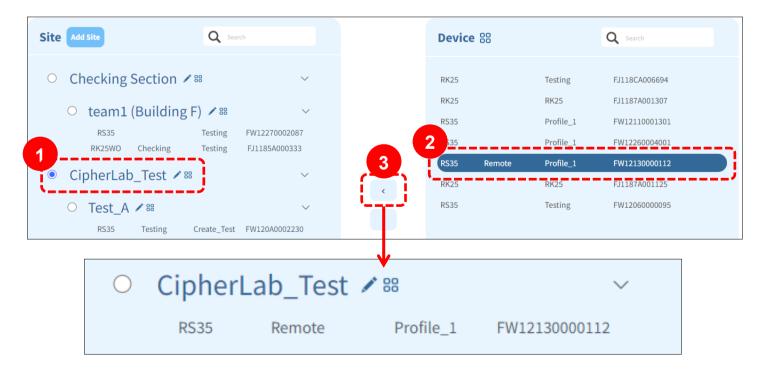
On the left side, the assignment list allows you to add devices to the selected site.

To assign devices to a site or a sub-site :

1. Click to select a site on the "Site" list. You can enter keywords in the search box to look for specific sites.

2. Click to select a device on the "Device" list. You can enter keywords in the search box to look for specific devices.

3. Click the left button 〈 to add the selected device to the selected site.

6.2 GROUP

"**Group**" helps the user manage devices. Create groups to organize the enrolled devices by different setting buttons.

Access "**Group/Site**" > "**Group**" :

The functions of the 5 setting buttons on the "**Group**" page:

Setting Button	Description
Add Group	To create a new group.
Assign	To assign a profile to the selected group. Devices from the selected group will hence apply to the assigned profile's settings.
Pre-Group	To import the .csv file for reviewing the device data in an efficient way.
Delete	To eliminate the selected groups.
Rename	To give a new name to the selected group.

6.3   PRESET / ADD / DELETE / ASSIGN GROUP

6.3.1   PRE-GROUP

The function, "Pre-Group," allows the user to more effectively examine the device serial numbers and the groups to which they belong.

SETTING BUTTONS ON THE "ENROLL BY PRE-GROUP" PAGE

Click the setting button "**Pre-Group**" in the top-right corner of the "**Group**" page to enter the "**Enroll by pre-group**" setting page.

Enroll by pre-group   Hello! John Smith

< Back   Import   Export   Delete

Serial Number   Group Name

The 3 setting buttons on the "**Enroll by pre-group**" page:

Setting Button	Description
Import	To upload the .csv file for setting.
Export	To export the list to an Excel .csv file for reviewing.
Delete	To eliminate the settings.

Note that the function, "Enroll by pre-group," only accepts .csv files for importing.
Hence, knowing how to create a .csv file for the "enroll by pre-group" function is essential.

HOW TO CREATE A .CSV FILE FOR "ENROLL BY PRE-GROUP"

The **.csv** file should contain the following information:

- The Device Serial Number
- The Group Name

1. Open a **Notepad** file.

2. Input the devices' serial numbers and the groups' names the devices belong to in sequence, one device per row.

The serial number and the group name are only separated by a comma without any other characters or symbols. For example:

3. After finishing inputting, click "**File**" and select "**Save As…**".
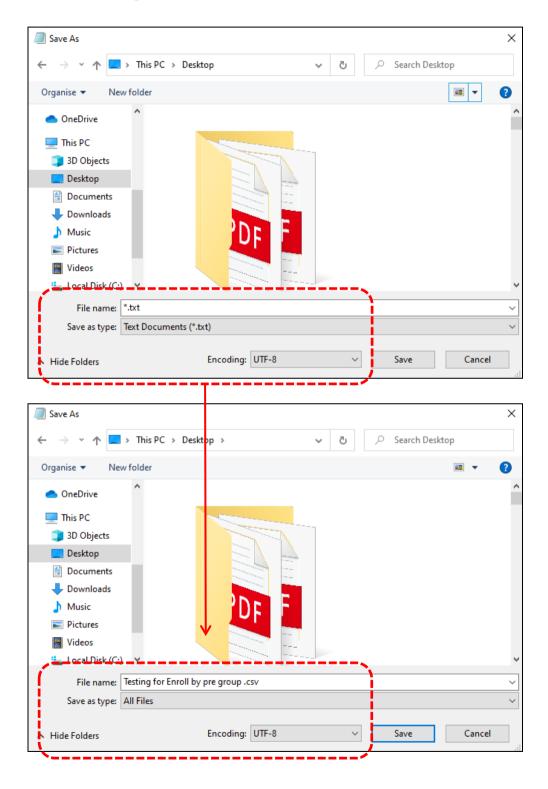
4. For the "**File name**" field, input a name and manually change the filename extension from **.txt** to **.csv.**

5. For the "**Save as type**" field, select "**All Files (*.*)**".

6. For the "**Encoding**" field, select "**UTF-8**".

The **.csv** file is successfully created and ready to be imported to the "**Enroll by pre-group**" setting page on ReMoCloud.

UPLOAD .CSV FILE FOR "ENROLL BY PRE-GROUP" SETTINGS

On the "**Enroll by pre-group**" setting page, click the "**Import**" button to upload the file.

Click the "**Choose File**" button to select the .csv file and click the "**Submit**" button to upload.

When the file is successfully imported, a pop-up window will appear to notify the user of the completion, and the imported .csv file will simultaneously be demonstrated as a list on the "Enroll by pre-group" setting page.

After importing a csv.file, the "Export" button [Export] and the "Delete" button [Delete] in the top-right corner will become available.

The user can upload only <u>one</u> .csv file to the "Enroll by pre-group" setting page. Click "Delete" to eliminate the original settings and import another one.

EXPORT "ENROLL BY PRE-GROUP" SETTINGS

The user may click the "Export" button to export the list to an Excel .csv file for reviewing. After clicking "Export," a pop-up window will appear for the user to enter a name for the file. After inputting a name, click "Submit" to download the file on the PC. Or, click "Cancel" to undo.

The exported file will be saved in the default download location.

DELETE "ENROLL BY PRE-GROUP" SETTINGS

Click the "**Delete**" button to eliminate the settings. Next, click "Yes" on the warning pop-up window to confirm deleting the settings on the "**Enroll by pre-group**" page.

The user will be able to import new settings after deleting.

GROUP THE DEVICE(S) BY FOLLOWING "ENROLL BY PRE-GROUP" SETTINGS

Even if the user had assigned a different profile for the device during the "enrollment," ReMoCloud will reassign the designated profile for the device according to the "Enroll by pre-group" settings.

Enroll by pre-group

Hello! John Smith

‹ Back   Import   Export   Delete

Serial Number	Group Name
FW120A0002230	Group_2
FW12260004001	None
FJ1187A001307	None
FT12170003374	Group_3
FW12110001301	None
FW12270002087	None
FJ118CA006694	Group_3

Device

Hello! John Smith

Search   Wipe   Delete   Lock   Reboot   Push Notification

Edit Column   1 to 7 / Total Device(s) : 7   Last update : 2023-07-14 18:04:32   Sync with Google   Refresh

	Model Name	Serial Number	User Defined	Group	Profile	Battery Level	Remote Control	Profile Current Ver	Profile Latest Ver
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test		👁	8	8
☐	RS35	FW12260004001		None	Profile_1		👁	23	25
☐	RK25	FJ1187A001307		None	RK25		👁	44	44
☐	RK95	FT12170003374		Group_3	Testing		👁	7	7
☐	RS35	FW12110001301		None	Profile_1		👁	23	25
☐	RS35	FW12270002087		None	HCT		👁	48	48
☐	RK25	FJ118CA006694		Group_3	Testing		👁	7	7

When the group listed on the "Enroll by pre-group" page has not been created yet, ReMoCloud will automatically create the group and assign the profile for the device.

Enroll by pre-group

Hello! John Smith

Back | Import | Export | Delete

Serial Number	Group Name
FW120A0002230	Group_2
FW12260004001	None
FJ1187A001307	None
FT12170003374	Group_3
FW12110001301	None
FW12270002087	None
FJ118CA006694	Group_3

Site | **Group**

Add Group | Assign | Pre-Group | Delete | Rename

Group	Number of Devices	Profile
Group_1	0	Profile_1
Group_2	1	Create_Test
Group_3	2	Testing
Test_for_Creating	0	HCT

6.3.2 CREATE A NEW GROUP

Use the following steps to create a new group:

1. Enter a name for the new group.

2. Select the profile from the drop-down menu.

3. the available enrolled devices that belong to no groups will be listed. Select the devices to add them to the new group.

The devices added to the group will automatically apply to the designated profile according to the group settings.

For more details about the "**Group Setting**" page, refer to Group Management.

4. Click the "**Back**" button in the top-left corner to return to the "List of Group" page. The created group will be listed here.

6.3.3 DELETE GROUP

On the "Group" page, the user can delete groups

Select the group and click the "**Delete**" button.

The warning pop-up window will appear for the user to confirm deleting the selected groups.

Click "**Yes**" to proceed. Or, click "**No**" to undo.

While the group is deleted, the devices from the group will not be deleted or wiped. The devices will still apply to the profile that was assigned by the deleted group.

You can check the device information on the "**Device**" page:

6.3.4 ASSIGN GROUP

The "**Assign**" function is to assign profiles to groups and ungrouped devices.

Click the "**Assign**" button to enter the "Assign Profile" page.

On the right side, all groups and the ungrouped devices will be listed with their original applying profiles and serial numbers on the "Group/Device" section.
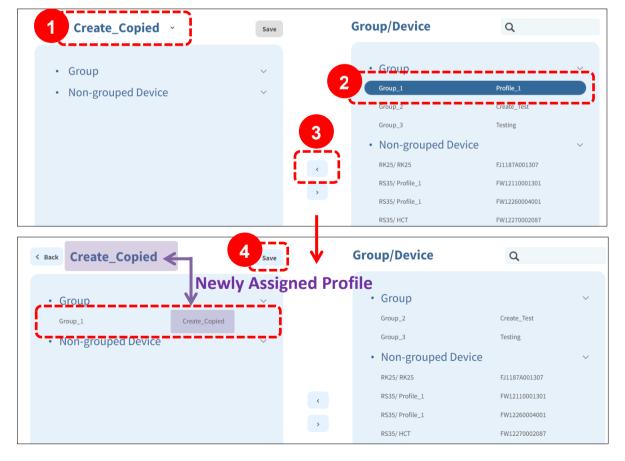
On the left side, the assignment list allows you to add groups/devices and select profiles.

To assign a profile to groups and devices :

1. Click to select a profile.
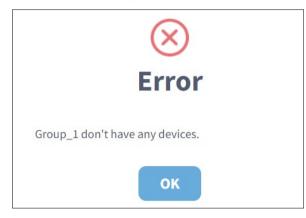
2. Select a group or device on the "Group/Device" list. You can enter keywords in the search box to look for specific groups or devices.

3. Click the left button to add the selected group or device to the assignment list.

295

4. Click "Save" to assign. (You can select multiple groups and devices for assignment.)

Note that the assignment will fail when there is no devices assigned to the selected group.

After the assignment is completed, the devices from the group will immediately apply to the designated profile.

6.4 GROUP MANAGEMENT

On the "**Group**" page, click the group's name to enter the "**Group Setting**" page.

The detailed information of the devices assigned to the group will be listed on this page.

Group Setting Buttons

Group Device List

6.4.1 GROUP DEVICE LIST

The header row items of the group device list:

- Model Name

The device model name.

- User Defined

The field for the user to put a mark on the device. With the marks, the user is allowed to distinguish the devices from each other with the same model name. For more details, refer to "User-Defined" of "Enrolled Device List".

- Serial Number

The serial number of the device.

- Group

The group to which the device belong.

- Profile

The profile to which the device applies.

- Profile Current Ver

This column shows if the device applies to any designated profile.

If so, it will demonstrate the profile's version number. If not, it will show "Not Applied".

Item	Description
Green Version Number	The profile that this device applies to is the latest version.
Red Version Number	The profile that this profile applies to is the old version.
Not Applied	The device does not apply to any designated profile.
0	The profile that this device applies to is unedited. 0 in green suggests that this profile is the latest version, while red suggests the old version.

- Profile Latest Ver

The latest version number of the designated profile.

- IMEI

The IMEI number of the device.

- Command Status

Showing the executing command, such as "**Locking**," "**Wiping**," and "**Rebooting**".

- Sorting:

Click the sort button ∧ ∨ at the header row to display the profiles in ascending or descending order.

- Filtering:

Click the filtering button ▼ at the header row to expand "**Filter**" field for further searching.

SORTING THE GROUP DEVICES

In the "Group Setting" page, the user may sort the displayed information by the header row items.

Click the sort button ∧ ∨ of the header row item to display the device list in ascending order.

Click it again to display the list in descending order. As shown:

- Ascending (click once) ∧

- Descending (click twice) ∨

FILTERING THE GROUP DEVICES

To search the specific device from the device list.

1. Click the ⛢ button of the header row item to expand the editable "**Filter**" field.

2. Enter keywords to search from the column. The matching devices will be displayed.

3. The user may set multiple filter criteria to refine the results.

6.4.2   GROUP SETTING BUTTONS

Above the group device list, there are 10 setting buttons:

SYNC WITH GOOGLE

Click the "**Sync with Google**" button to update the data based on the most current conditions for all devices by synchronizing with the data from Google system.

While "**Sync with Google**" and "**Refresh**" are both for updating the data, "**Sync with Google**" will comparatively cause more system load.

After clicking "**Sync with Google**," it will take a while to receive and update data. During this process, the setting buttons will be unavailable.

REFRESH

Click the "**Refresh**" button to update the data based on the condition for the last time ReMoCloud synchronized with Google system.

While "**Sync with Google**" and "**Refresh**" are both for updating the data, "**Refresh**" will comparatively cause less system load.

PUSH NOTIFICATION

"**Push Notification**" is to pass text messages on to the selected devices.

Before clicking the "**Push Notification**" button, the user should select at least one device. Namely, the user is allowed to send messages to multiple devices simultaneously.

After selecting devices, click the "**Push Notification**" button to make the "**Message**" pop-up window appear.

On the pop-up window, there will be a text area and two buttons, "**Submit**" and "**Cancel**".

Including digits, punctuation marks, and symbols, the user may input no more than 100 characters.

For example:

After entering the text, click "send" to pass the text on to the devices or click "cancel" to undo. When the text is successfully sent, the process will be followed by another pop-up window notifying the user of the completion, and the text message will be displayed on the device. As shown:

ADD

To add devices to the group:

1. Click the "**Add**" button on the "**Group Setting**" page. The available devices will be listed on the pop-up window.

2. Select the devices and click "**Add**" to add the device to the group. The added devices will apply to the designated profile that is displayed in the top left corner.
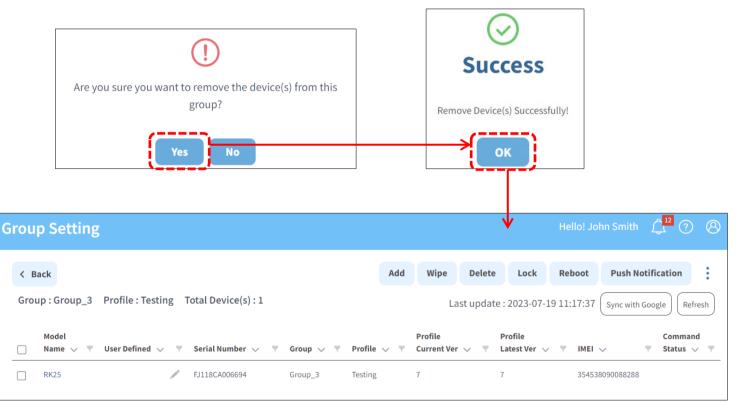
REMOVE

To use the function "Remove," click ⋮ to unfold the menu.

Select the device and click the "**Remove**" button to remove the device from the group.

Click "**Yes**" on the pop-up warning window to confirm removing the device.

Note that the removed device will not be "Wiped" or "Deleted" from ReMoCloud but removed from the group. Also, it will still apply to the profile designated by the group from which the device is removed.

ReMoCloud User Guide

MOVE
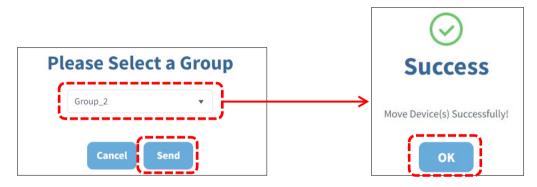
To use the function "Move," click ⋮ to unfold the menu.

Select the device and click the "**Move**" button to move the device to another group.

Select a group and click "**Send**".

The page will be redirected to the "Group Setting" page where the device is transferred to.

The moved device will apply to the profile designated by the new group.

WIPE

The function, "**Wipe**," is to restore the selected devices to their factory default settings and to remove their data from ReMoCloud.

Select the devices and click the "**Wipe**" button.

Click "**OK**" on the warning pop-up window and enter the user's ReMoCloud password to confirm wiping the selected devices.

The selected devices are successfully wiped.

DELETE

The function, "**Delete**," is to remove the selected devices from ReMoCloud's device management list. Note that deleting a device does not "**Wipe**" or restore the device to its factory default settings.

Select the device and click the "Delete" button.

Click "OK" on the pop-up warning window to proceed.

Enter the user's ReMoCloud password to confirm deleting the selected devices.

LOCK

Select devices and click the "**Lock**" button to turn off their screens. The user will need to unlock the screen first if the screen lock is set on the device.

A pop-up window will appear to remind the user that the selected device's screen is locked successfully.

REBOOT

Select devices and click the "**Reboot**" button to shut down and restart the devices.

A pop-up window will appear to remind the user that the selected device's screen is rebooted successfully.

Chapter 7

CHAPTER 7. ACCOUNT MANAGEMENT

This chapter carries the detailed introduction of the functions offered by "**Sub Account**". There are two kinds of sub accounts on ReMoCloud, "**Parent account**" and "**Child account**".

IN THIS CHAPTER

7.1 OVERVIEW

"**Management**" is ReMoCloud's function that allows the user to structure and organize their accounts using different levels of authority. The ReMoCloud account hierarchy consists of admin account, parent account, and child account. As the account owner, the admin account, the user can add multiple sub accounts.

When logging into ReMoCloud with either the admin or parent account, users with these account types gain access permission to the "**Account Management**" function, visible on the main menu.

Click "**Account Management**" under 👤 "**Management**" to enter the "**Account Management**" page.

7.1.1 USER ROLE TYPE

Every account type for logging into ReMoCloud—admin, parent, and child—is associated with the user's organization. When creating sub-accounts, users can specify access permissions for each sub-account, whether parent or child.

ADMIN ACCOUNT

The "**Admin account**" holds the highest position in the ReMoCloud account hierarchy. By default, it serves as the "**Main Account**", linked with the user's managed Google Play account.

With the admin account, the user can:

1. Create parent accounts and assign admin privileges.

2. Create child accounts and define their access permission.

3. Transfer its authority to a parent account.

Note that the admin account cannot be deleted or edited but only transferred.

PARENT ACCOUNT

The "**Parent account**" functions as a substitue for the admin account. However, the admin account retains ultimate authority and access permissions within ReMoCloud's account hierarchy.

The parent account is restricted to accessing devices solely from the groups assigned to its linked child account.

- The privileges that the parent account **does not** share from the admin account include:

  1. The parent account cannot review the data from other parent accounts on the Manage Account page.

  2. The parent account cannot create or edit parent sub accounts but only child accounts.

  3. The parent account cannot transfer the admin authority.

CHILD ACCOUNT

A "**Child account**," created by either the admin or parent account, has restricted access permissions. Positioned at the bottom of ReMoCloud's account hierarchy, the child account's access permissions are determined by its creator, the admin or parent account.

The definable configuration permissions for the child account are:

- Profile

The child account can only access the profiles from the assigned groups .

- Enroll Device

The child account's ability to perform device enrollment and the quantity of device enrolling are both decided by its creator.

- Group

The child account can only access the groups assigned by its creator.

- Edit Profile

The child account can only edit the profiles from the assigned groups.

- Wipe & Lock Group Device

The child account will be allowed to wipe and lock the device from the assigned groups when the creator selected "Write" for "Group Permission".

Note: Sub accounts will not be able to view the devices they newly enroll until the admin account adds these devices to groups.

7.1.2 ACCESS WITH ADMIN ACCOUNT FOR THE FIRST TIME

After logging in to ReMoCloud with the admin account, click the "**Account Management**" button under ![tree icon] "**Management**" to access the "**Account Management**" page.

For the first time accesing "**Account Management**" page with the ReMoCloud admin account, there will only be the admin account listed on the account list.

To add more sub accounts, refer to Create a Parent Account by Admin Account & Create a Child Account by Admin Account.

Note:

To create sub accounts, there must be at least one **group** in the admin account's settings on ReMoCloud.

SUB ACCOUNT LIST

The information provided by the account list:

- Account Name

The account names must be in the format of e-mail address.

- Account Type

The account types include "admin," "parent," and "child". For more details, refer to User Role Type.

- Build Time

The time and date when the account is built.

- Profile Permission

The permission type given to the child account for accessing profiles.

- Group Permission

The permission type given to the child account for accessing groups.

- Assign Group

The accessible group(s) for the child account.

- Enroll Permission

The permission type given to the child account for performing device enrollment.

- Assign License Type

The license type given to the child account. For more details, refer to License Information.

- Assign License Quantity

The total amount of the devices that the child account is allowed to perform device enrollment. The quantity is limited according to the user's license type.
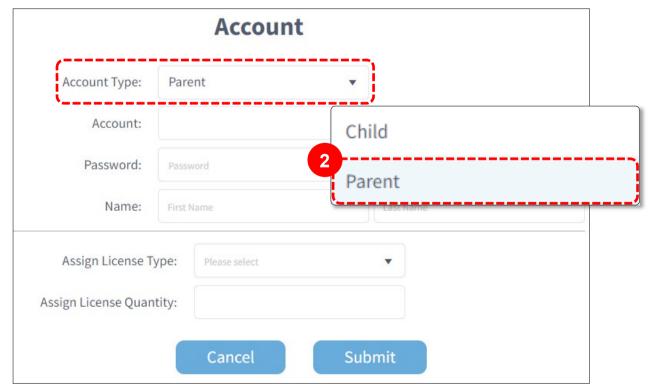
CREATE A PARENT ACCOUNT BY ADMIN ACCOUNT

Follow the steps to create a parent account:

1. Click the "**Add**" button.

2. On the "Account" pop-up window, select "Parent" for "Account Type".

319 of 436

3. Fill out the necessary information and click "Submit".

- **Sub account**

The account has to be in the format of an e-mail addresss.

Note that it will fail to create a new sub account if the e-mail address is already used by an existing ReMoCloud account. As shown:

- **Password**

The login password of the sub account.

- **Name**

The name you set here will be displayed as the greeting message next to the header navigation buttons when you log in to ReMoCloud with the sub account.

- **Assign License Type**
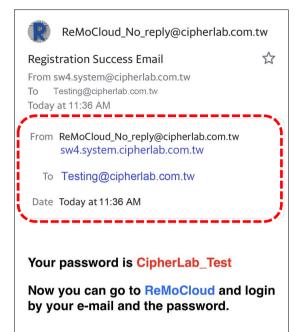
The available license type is decided by the user's ReMoCloud License. For more details, refer to License Information.

- **Assign License Quantity**

When defining the child account's license quantity for device enrollment, the quantity is limited by the remaining quantity that the user's ReMoCloud License allows.

4. After submitting, ReMoCloud will send an e-mail to notify the user of the completion, and the newly-created sub account will be listed on the "Account Management" page.

	Account Name	Account Type	Build Time	Profile Permission	Group Permission	Assign Group	Enroll Permission	Assign License Type	Assign License Quantity
☐	joshua.hsu@cipherlab.com...	Admin	2020/12/15 05:24						
☐	asd@cipherlab.com	Child	2022/12/20 11:21	Write	Write	Group_1;Group_2	disallow	Advance	50
☐	hh@gamil.com	Child	2023/01/16 16:57	Read	Write	Group_1;Group_2;Group_3	Allow	Advance	10
☐	qwe@cipherlab.com	Child	2022/11/23 14:24	Read	Read	Group_1;Group_2;Group_3	disallow	Advance	50
☐	zxc@cipherlab.com	Child	2023/03/08 18:07	Read	Write	Group_1	disallow	Advance	50
☐	Testing@cipherlab.com.tw	Parent	2023/07/20 11:36						

CREATE A CHILD ACCOUNT BY ADMIN OR PARENT ACCOUNT

Follow the steps to create a child account:

1. Click the "**Add**" button.

2. On the "Account" pop-up window, select "Child" for "Account type".

3. Fill out the necessary information and click "Submit".
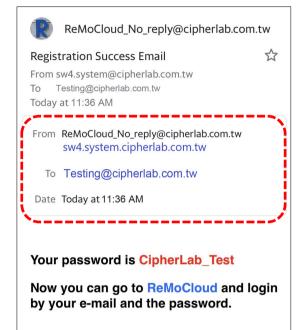
Note that the child account must be connected to a parent or the admin account.

4. After submitting, ReMoCloud will send an e-mail to notify the user of the completion, and the newly-created sub account will be listed on the "Manage Account" page.

THE REQUIRED INFORMATION FOR CREATING SUB ACCOUNTS

- Sub account & Password

The account has to be in the format of an e-mail addresss.

Note that it will fail to create a new sub account if the e-mail address is already used by an existing ReMoCloud account.

- Profile Permission

To define the child account's access permission for the profile settings.

Permission	Description
Read	The child account can only review the profiles.
Write	The child account can both review and edit the profiles.

- Group Permission

To define the child account's access permission for the group settings.

Permission	Description
Read	The child account can only review the group settings.
Write	The child account can both review and edit the group settings.

- Enroll Permission

To define this child account's access permission for performing device enrollment.

- Assign Group

To define this child account's permission for accessing groups.

- Assign License Type

The available license type is decided by the user's ReMoCloud License. For more details, refer to License Information.

- Assign License Quantity

When defining the child account's license quantity for device enrollment, the quantity is limited by the remaining quantity that the user's ReMoCloud License allows.

7.2 SUB ACCOUNT MANAGEMENT

Users with the "**parent**" role can create and manage "**child**" accounts' access and authority in profiles, groups, and device enrollment.

Parent accounts have fully authorization to control the changes to all child accounts, including the "Add", "Edit", and "Delete" functions on the "**Account Management**" page.

- Add

To create a new child account.

- Edit

To modify the selected child account's settings.

- Delete

To delete the selected child accounts. Please note that the parent account cannot deleted itself.

Also, when logging in with the admin account, all the accounts attached to your organization will be listed on "**Account Management**" page, and the function limitation for every account is indicated in the sub account list as followings:

- Account Name

The sub account format is e-mail address.

- Account Type

The account type this sub account is attributed.

Account Type	Description
Parent	Fully delegated, undeletable, and immutable.
Child	Restrictively authorized, deletable, and editable.

- Build Time

The time and date when the account was created.

■   Profile Permission

The permission that this child account is assigned to do with the profile(s).

Permission	Description
Read	The child account can only read the profile(s).
Write	The child account can edit the profile(s).

■   Group Permission

The permission this child account is assigned to do with the group(s).

Permission	Description
Read	The child account can only read the group(s).
Write	The child account can edit the group(s).

■   Assign Group

The group(s) this child account is permitted to access.

■   Enroll Permission

The permission or prohibition on enrolling device.

■   Assign License Type

The license type this child account is assigned. Please refer to License Information for details.

■   Assign License Quantity

The device amount this child account is allowed to carry out device enrollment.

7.2.1 TRANSFER THE ADMIN ACCOUNT'S AUTHORITY

While the admin account has the highest authority, it can transfer its authority to a parent account, resulting in an exchange of roles. After the transfer, the admin account becomes a parent account, and vice versa.

To transfer the admin account:

1. Click "Transfer" to open the **"Admin Transfer to Parent"** pop-up window.

2. Enter the admin account's password and select a parent account.

3. Click "Submit" to proceed.

4. After clicking "Submit," if the account is immediately logged out, it means that the admin account's authority is already successfully transferred.

5. Log in to ReMoCloud with the new admin account to check the account settings.

7.2.2 SUB ACCOUNT PERMISSION MANAGEMENT

The third setting button for account management is "Edit".

1. Select a child account and click the "Edit" button to open the "**Edit Account**" pop-up window

2. Redefine the sub account's settings for permission and license.

3. Click "**Submit**" to carry out the changed settings.

Please note that the fields "**Account Type**," "**Account**," "**Password**," and "**Name**" are uneditable.

7.2.3 DELETE A SUB ACCOUNT

To delete a sub account:

1. Select an account and click the fourth setting button "**Delete**" in the top-right corner.

2. Enter the admin account's password to confirm deleting and click "Submit".

7.2.4 ACCOUNT SHARING

"Account Sharring" facilitates the synchronization of sites and groups across multiple accounts in ReMoCloud. This enables administrators to efficiently view and apply changes, ensuring consistency and enhancing overall management.

ADD ACCOUNT SHARING

1. Navigate to the "**Account Management**" page, and tap "**Account Sharing**".

2. Tap "**Add Sharing**" in the upper-right corner.

3. Enter the Sharing Name, and proceed to select the accounts to be included in the sharing.

	Account Name	Account Type	Build Time
☐	aabctesting@cipherlab.com.tw	Parent	2023/07/20 11:36
☐	hsu@gamil.com	Parent	2023/01/16 16:56
☐	josh@cipherlab.com.tw	Parent	2023/07/14 17:54
☑	parent_1@gmail.com	Parent	2024/03/27 16:22
☑	parent_2@gmail.com	Parent	2024/03/27 16:23

Sharing Name: Sharing_1

Close   **Add**

A pop-up window will appear to show the "Sharing" is successfully added.

Success

Add Successfully!

OK

PARENT ACCOUNTS IN THE SAME ACCOUNT SHARING

Parent accounts within the same sharing group synchronize the same "Groups" and "Sites". Changes made in one parent account or their child accounts will be synchronized across other sharing accounts.

For instance, the account "parent_1@gmail.com" and "parent_2@gmail.com" belong to the same sharing goup,allowing them to share identical "Group" and "Site" pages. Furthermore, if one of these accounts or any of their child accounts edits a site page, synchronization occurs across both parent accounts and their respective child accounts.

"parent_1@gmail.com" account shares the same "Group" and "Site" pages with "parent_2@gmail.com"

"Group" page in "parent_1" account

"Group" page in "parent_2" account

"Site" page in "parent_1" account

"Site" page in "parent_2" account

CHILD ACCOUNTS IN THE SAME ACCOUNT SHARING

Child accounts within the same sharing group synchronize the same "Site" page but not the "Group" page. That is, if one of these accounts edits a site page, synchronization occurs across both child accounts and their respective parent accounts. However, child accounts can only view the group page of its own.

For instance, the accounts "child_1@gmail.com" and "child_2@gmail.com" belong to the same sharing group, allowing them to share identical "Sites" pages. However, they can only view their own "Group" page.

"child_1@gmail.com" account shares the same "Site" page with "child_2@gmail.comt".

"child_1@gmail.com" account doesn't share the same "Group" page with "child_2@gmail.com" account.

"Group" page in "child_1" account

"Group" page in "child_2" account

7.3 CHILD ACCOUNT'S POV

At the bottom of ReMoCloud's account ranking system, the child sub account's access for ReMoCloud's management functions is limited by its creator.

7.3.1 LOGIN

To log in to ReMoCloud with a child account:

Go to the login page https://remocloud.cipherlab.com/login.

Enter the child account (e-mail address) and the password for submitting.

For more details, refer to Login & Remember Me.

Note that sub accounts are not supported by the "**2FA**" service.

CHILD ACCOUNT GROUP LIST

After logging in, the child account user will enter the "**Group**" page.

The accessible groups for the child account will be listed here.

CHILD ACCOUNT PROFILE LIST

In addition to the "**Group**" page, the child account is also allowed to enter the "**Profile**" page. Yet, the ability to edit profiles will be decided by its creator's settings.

CHILD ACCOUNT DEVICE LIST

The child account is also allowed to enter the "**Device**" page, but not allowed to edit the settings.

CHILD ACCOUNT USER LOG

The "**User Log**" page lists all the activities of the child account.

Select the start month and end month from the drop-down menu to search for more data. Also, the logs can be sorted by "**Time**".

For more details, refer to **Search, Sort, & Filter Logs**.

CHILD ACCOUNT ENROLL PAGE

ENROLL PERMISSION

Select "Allow" for "Enroll Permission" to give the child account the ability of performing device enrollment. Otherwise, select "Disallow".

When given the permission, the child account will be allowed to perform device enrollment in the same way as the admin account and the parent account do.

For more details about permission settings, refer to Create a Sub Account.

When the creator selects "Disallow" for the child account's "**Enroll Permission**" setting, the "**Enroll Device**" **page** will not be displayed as an item on the main menu.

Use the setting button "**Edit**" on the "Account Management" page to change the "Enroll Permission" setting.

ENROLLMENT

When logging in with the child account, click "**Enroll Device**" under "**Enrollment**" on the main menu to enter the "**Enroll**" page.

For the detailed steps of performing device enrollment, refer to Enroll Device.

Note that only the profiles from the **Groups Assigned** are available for performing device enrollment.

Furthermore, since the device enrolled by the child account belongs to no groups, the child account will only be able to review the newly-enrolled device's data until it is assigned to a group accessible for the child account by either the admin account or a parent account.

7.3.2 PROFILE MANAGEMENT

Based on different permission settings, the child account may or may not edit the profiles when accessing the "Profile Information" page.

Only the profiles from the assigned groups will be listed.

Click the profile's name to enter its "Profile Information" page.

> ### READ
>
> With the permission setting "**Read**," the child account can only review but edit the profile's settings. As shown:

WRITE

With the permission setting "**Write**," the child account can both review and edit the profile's settings. As shown:

For more details, refer to "**Edit a Profile: APP**" and "**Edit a Profile: Device Setting**".

7.3.3   GROUP MANAGEMENT

Based on different permission settings, the child account may or may not edit the group settings when accessing the "Group" page.

Only the data of the assigned groups will be displayed on the list.

Click the profile's name to enter the "Group Setting" page.

READ

With the permission setting "**Read**," the child account can only review the group's settings.

Click "**Sync with Google**" or "**Refresh**" on the "Device Information" page to receive the latest status.

WRITE
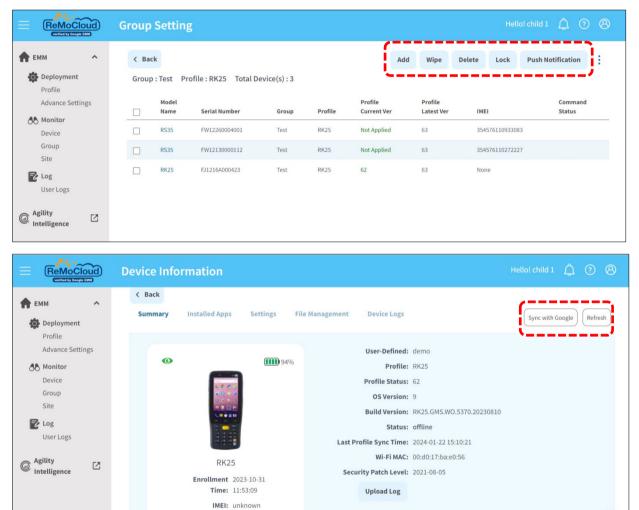
With the permission setting "**Write**," the buttons, "Wipe," "Delete," "Lock," and "Push Notification," in the top-right corner of "Group Setting" page will become available for the child account.

Click "**Sync with Google**" or "**Refresh**" on the "Device Information" page to receive the latest status.

Chapter 8

CHAPTER 8. USER LOGS

This chapter carries the introduction of the functions offered by "**Logs**" on ReMoCloud.

IN THIS CHAPTER

8.1 CHECK USER LOGS

The "**User Logs**" page lists all the activities and events of the account.

The "**User Logs**" page provides the information:

Item	Description
Time	The time and date when the activity was executed.
Arrive Page	The page where the activity was executed.
Description	The activity details.
By User	The account that executed the activity.

Click "**Export**" in the upper panel to download the user logs report as a CSV file.

8.2 SEARCH, SORT, & FILTER LOGS

The "**Search**" button on the "**User Logs**" page is for setting a date range to refine the results.

The user may also sort or filter the results by the "**Time**" column.

SEARCH THE LOGS

At first, the "**User Logs**" page only shows the logs for the current month.

1. Click to expand the drop-down menus and set the date range.

2. Click "**Search**" to display the logs for previous months.
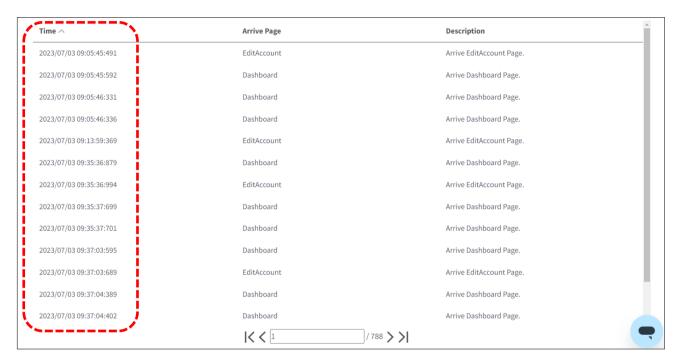
SORT THE LOGS

Click the sort button ⋀ ⋁ next to "**Time**" to display the logs in the ascending order. Click again to display the logs in the descending order.

- Ascending (click once) ⋀

Time ⌃	Arrive Page	Description
2023/07/03 09:05:45:491	EditAccount	Arrive EditAccount Page.
2023/07/03 09:05:45:592	Dashboard	Arrive Dashboard Page.
2023/07/03 09:05:46:331	Dashboard	Arrive Dashboard Page.
2023/07/03 09:05:46:336	Dashboard	Arrive Dashboard Page.
2023/07/03 09:13:59:369	EditAccount	Arrive EditAccount Page.
2023/07/03 09:35:36:879	Dashboard	Arrive Dashboard Page.
2023/07/03 09:35:36:994	EditAccount	Arrive EditAccount Page.
2023/07/03 09:35:37:699	Dashboard	Arrive Dashboard Page.
2023/07/03 09:35:37:701	Dashboard	Arrive Dashboard Page.
2023/07/03 09:37:03:595	Dashboard	Arrive Dashboard Page.
2023/07/03 09:37:03:689	EditAccount	Arrive EditAccount Page.
2023/07/03 09:37:04:389	Dashboard	Arrive Dashboard Page.
2023/07/03 09:37:04:402	Dashboard	Arrive Dashboard Page.

|< < 1 / 788 > >|

- Descending (click twice) ⋁

Time ⌄	Arrive Page	Description
2023/07/25 14:56:16:906	Save Settings	Save Profile Device Settings**...more**
2023/07/25 14:56:16:806	Profile Version Update	Testing_for_rollback;3;23
2023/07/25 14:55:06:268	Profile Info	Arrive Profile 'Testing_for_rollback' Page.
2023/07/25 14:54:59:893	Profile	Arrive Profile Page.
2023/07/25 14:53:40:420	DeviceList_new	Arrive Device Page.
2023/07/25 14:51:40:740	DeviceList_new	Arrive Device Page.
2023/07/25 14:51:40:717	DeviceList_new	Arrive Device Page.
2023/07/25 14:48:39:912	DeviceList_new	Arrive Device Page.
2023/07/25 14:46:40:233	DeviceList_new	Arrive Device Page.
2023/07/25 14:46:40:221	DeviceList_new	Arrive Device Page.
2023/07/25 14:43:40:049	DeviceList_new	Arrive Device Page.
2023/07/25 14:41:40:013	DeviceList_new	Arrive Device Page.
2023/07/25 14:41:39:964	DeviceList_new	Arrive Device Page.

|< < 1 / 788 > >|

Chapter 9

CHAPTER 9. DEFAULT APPLICATIONS

This chapter carries the detailed introduction of the functions offered by the default Apps.

IN THIS CHAPTER

9.1 CIPHERLAB OEMCONFIG

CipherLab OEMConfig is the hidden default App that helps the ReMoCloud administrator configure the settings of the enrolled devices.

9.1.1 MANAGE APP CONFIG PAGE

On the profile's App list, click "**Edit**" from the "**Manage Config**" column to enter **CipherLab OEMConfig**'s "**Manage App Config**" page.

On the "**Manage App Config**" page, the user can manage the advanced settings.

The significant settings on the "**Manage App Config**" page of CipherLab OEMConfig:

▪ DeployFromZip

Deploying the **ADC** (**Android Deploy Configurator**) project settings to the enrolled devices, the "**DeployFromZip**" settings must cowork with "**CipherLab ADC Module**".

▪ Log Collection

The "**Log Collection**" settings should cowork with "**CipherLab LogCollection**" for uploading the log data of enrolled devices to the FTP server.
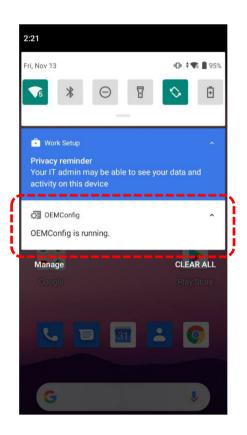
Switch on or off to enable or disable "Log Collection".

Make sure to click "OK" to save the changed settings before leaving the **"Manage App Config"** page.

"Save" or "Schedule" to carry out the changed settings on the **"Profile Information"** page.

While **"CipherLab OEMConfig"** will only be displayed in the App Drawer on the enrolled devices, it will be running in the background.

9.1.2 OTHER IMPORTANT SETTINGS

Other important settings of **CipherLab OEMConfig**:

SYSTEM UPDATE

1. Switch on or off to enable or disable update controls.

2. Click "Enable" or "Disable" to allow or disallow the enroll devices to perform an OTA system update.

An over-the-air (OTA) update is the wireless delivery of new software, firmware, or other data to mobile devices.

When the battery level of the device is below 50%, the OTA update cannot be performed. For this situation, have the enrolled device plugged into a power source to perform the OTA update.

SENT INTENT

"**Sent Intent**" is to perform an action on the device's screen, such as starting activities and services, or sending broadcasts and messages.

1. Switch on "Send Intent Controls".

2. Input the command in the required format into the "**Call activity manager (am)**" field.

For example:

Start SIPController

"ACTION:StartActivity, PKG:com.sw.android.sipcontroller, CLS:MainActivity"

Start SoftwareTrigger Icon

"ACTION:StartService, PKG:com.Cipherlab.SoftwareTrigger_Service, CLS:FlyBitch"

BUTTON ASSIGNMENT

"**Button Assignment**" is for the user to redefine the functions of the device's physical keys to trigger different actions.

Click the "**Add**" button to create new settings for redefining the action that occurs when clicking a button.

Click the "**Remove**" button to eliminate the most recently created setting, resetting the button settings to default.

By the function "**User-defined**," the user can map the key by entering the key code defined in the Android operating system:
https://developer.android.com/reference/android/view/KeyEvent

The package name and the class name for launching App settings:

Application	Package Name	Class Name
A-Demo	sw.programme.demos	sw.programme.demos.ui.activity.MainActivity
Airlock Browser	com.outcoder.ibrowser	crc643f80cb343b07773e.MainActivity
AppLock	sw.programme.applock	sw.programme.applock.SetHomeActivity
BarcodeToSetting	com.cipherlab.barcodetosetting	com.cipherlab.barcodetosetting.MainActivity
BT Printer Mate	▪ RK95/RS51: cipherlab.btprtmate ▪ RS35: com.cipherlab.btprtmate	▪ RK95/RS51: cipherlab.btprtmate.MainActivity ▪ RS35: com.cipherlab.btprtmate.MainActivity
Button Assignment	sw.programme.buttonassignment	sw.programme.buttonassignment.activity.ButtonAssignmentActivity
Calculator	com.android.calculator2	com.android.calculator2.Calculator
Calendar	com.android.calendar	com.android.calendar.AllInOneActivity
Camera	org.codeaurora.snapcam	com.android.camera.CameraLauncher
Chrome	com.android.chrome	com.google.android.apps.chrome.Main
Clock	com.android.deskclock	com.android.deskclock.DeskClock
Contacts	com.android.contacts	com.android.contacts.activities.PeopleActivity

Application	Package Name	Class Name
Device Health Dashboard	sw.programme.devicehealth .dashboard	sw.programme.devicehealth.dashboard.ui .DashboardActivity
Drive	com.google.android.apps.docs	com.google.android.apps.docs.app .NewMainProxyActivity
Duo	com.google.android.apps .tachyon	com.google.android.apps.tachyon .MainActivity
Enterprise Settings	com.sw.enterprisekeypadmode	com.sw.enterprisekeypadmode .MainActivity
EZConfig	sw.programme.ezconfig	sw.programme.ezconfig.MainActivity
EZEdit	sw.programme.ezedit	sw.programme.ezedit.MainActivity
Files/Downloads	▪ RS50: com.android.providers .downloads.ui ▪ Others: com.android.documentsui	▪ RS50: com.android.providers.downloads.ui .DownloadList ▪ Others: com.android.documentsui.LauncherActivity
File Manager	com.cyanogenmod.filemanager	com.cyanogenmod.filemanager.activities .NavigationActivity
Gallery	org.codeaurora.gallery	com.android.gallery3d.app.GalleryActivity
Gmail	com.google.android.gm	com.google.android.gm .ConversationListActivityGmail
Google	com.google.android .googlequicksearchbox	com.google.android .googlequicksearchbox.SearchActivity
HF RFID Configuration	sw.programme.hf	sw.programme.hf.ConfigPrefActivity
Keep Notes	com.google.android.keep	com.google.android.keep.activities .BrowseActivity
Maps	com.google.android .apps.maps	com.google.android.maps.MapsActivity

Application	Package Name	Class Name
Messages	com.google.android.apps.messaging	com.google.android.apps.messaging.ui .ConversationListActivity
Music	com.android.music	com.android.music.MusicBrowserActivity
Phone	▪ RK25N/RS50 com.android.dialer ▪ RK25P/RS51 com.android.dialer ▪ RS35 com.google.android.dialer	▪ RK25N/RS50 com.android.dialer.DialtactsActivity ▪ RK25P/RS51 com.android.dialer.app.DialtactsActivity ▪ RS35 com.google.android.dialer.extensions .GoogleDialtactsActivity
Photos	com.google.android .apps.photos	com.google.android.apps.photos.home .HomeActivity
Play Movie & TV	com.google.android.videos	com.google.android.youtube.videos .EntryPoint
Play Music	com.google.android.music	com.android.music.activitymanagement .TopLevelActivity
Play Store	com.android.vending	com.android.vending.AssetBrowserActivity
QTI Logkit-lite	▪ RS51 com.qualcomm.qti.logkit ▪ Others com.qualcomm.qti.logkit.lite	▪ RS51 com.qualcomm.qti.logkit.cActivity ▪ Others com.qualcomm.qti.logkit.lite.cActivity
Reader Config	sw.programme.readerconfig	sw.programme.readerconfig.MainActivity
SDLgui	com.zebra.sdl	com.zebra.sdl.SDLguiActivity
Settings	com.android.settings	com.android.settings.Settings
Signature Capture	sw.programme.signature	sw.programme.signature.MainActivity

Application	Package Name	Class Name
SIP controller	com.sw.android.sipcontroller	com.sw.android.sipcontroller.MainActivity
SoftwareTrigger	com.Cipherlab.SoftwareTrigger	com.Cipherlab.SoftwareTrigger.MainActivity
Sound Recorder	com.android.soundrecorder	com.android.soundrecorder.SoundRecorder
Terminal Emulation	sw.programme.terminalemulation	com.te.UI.MainActivity
Video	com.android.music	com.android.music.VideoBrowserActivity
Velocity	com.wavelink.velocity	com.wavelink.velocity.te.SplashActivity
Voice Search	com.google.android.googlequicksearchbox	com.google.android.googlequicksearchbox.VoiceSearchActivity
WMDSAgent	sw.programme.wmdsagent	sw.programme.wmdsagent.MainActivity
WMDSInstaller	sw.programme.wmdsinstaller	sw.programme.wmdsinstaller.MainActivity
Youtube	com.google.android.youtube	com.google.android.youtube.app.honeycomb.Shell$HomeActivity
YT Music	com.google.android.apps.youtube.music	com.google.android.apps.youtube.music.activities.MusicActivity

9.2 CIPHERLAB DEVICE HEALTH

The default App, "**CipherLab Device Health**," is for checking the battery level of the enrolled devices.

Having "**CipherLab Device Health**" installed on the enrolled devices, the user can check the devices' battery level on the "**Device Information**" page.

CHECK THE BATTERY INFORMATION ON REMOCLOUD

Access "Device" to check the battery information of the enrolled devices on ReMoCloud.

	Model Name	Serial Number	User Defined	Group	Profile	Battery Level	Remote Control	Profile Current Ver	Profile Latest Ver
☐	RS35	FW120A0002230	Testing	Group_2	Create_Test		⊙	12	12
☐	RS35	FW12260004001		None	Profile_1		⊙	29	29
☐	RK25	FJ1187A001307		None	RK25		⊙	48	48
☐	RS35	FW12110001301		None	Profile_1		⊙	29	29
☐	RK25WO	FJ1185A000333	Checking	Group_3	Testing		⊙	10	10
☐	RS35	FW12270002087		None	Testing		⊙	10	10
☐	RK25	FJ118CA006694		Group_3	Testing		⊙	10	10

Note:

The requirements must be fulfilled in advance to acquire the battery health status:

1. Update the device OS to the latest version.

2. Update the default Apps "CipherLab OEMConfig" and "CipherLab Device Health" to the latest version and reboot the devices.

9.3 CIPHERLAB ADC MODULE

The default App **CipherLab ADC Module** is a service that coworks with **CipherLab OEMConfig** to deploy the **ADC** (**Android Deploy Configurator**) Project Settings to the enrolled devices through ReMoCloud.

The following items are required:

- Android Deploy Configurator

Download **ADC** (**Android Deploy Configurator**) program installer from http://wmds.cipherlab.com/ to your PC and run it by following its on-screen instructions.

- SD Card or USB Disk

Plug in the SD card or the USB disk to your computer in advance.

Note:

For the details about _Android Deploy Configurator_, refer to the latest _ADC User Guide for Android_ that can be downloaded from **http://wmds.cipherlab.com/ADC/UserGuide/Latest**

The following sections provides the steps of deploying the ADC project settings to the enrolled devices through ReMoCloud.

9.3.1 SAVE THE PROJECT FROM ANDROID DEPLOY CONFIGURATOR

To save the project from ADC to the SD card or USB disk:

1. Execute **Android Deployment Configurator** and select an existing project or create a new one depending on the settings the user preferred to deploy.

2. On the main page of ADC, select the configuration items you need.

Click the App-launcher icon in the bottom-right corner to review more advanced settings.

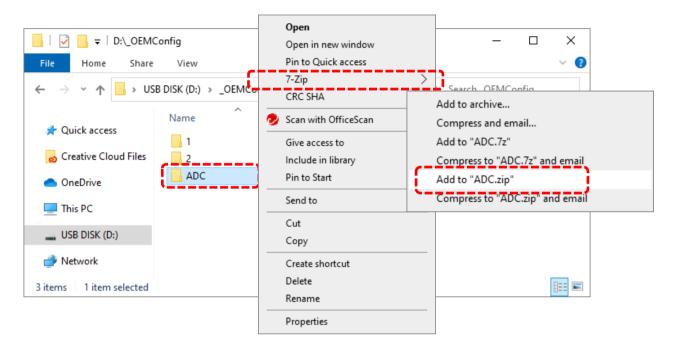3. After configuring the project settings, click "**Save current project to SD card**" to select the drive (SD card or USB disk) for saving the project.

9.3.2 CREATE A ZIP FILE & URL

1. Find the ADC project, a folder named "**ADC**," that you saved in the SD card or the USB disk.

2. Right-click the ADC folder to compress it.

3. Upload the zip file to a cloud storage platform to create and copy its link.

The following section takes Amazon S3 for example.

1. On Amazon S3, locate the zip file. Select the zip file and click "**Copy URL**".

2. A green notification tells that the URL is successfully copied.

3. Paste the URL into any file or field that allows you to edit it.

```
https://support-service.s3.ap-northeast-1.amazonaws.com/Android+Products/Software+User+Guide/ReMoCloud/CipherLab+ADC+Module/ADC.zip
```

4. Replace the first part, "…amazonaws.com," with "**d2b20xz24496kr.cloudfront.net**".

```
https://support-service.s3.ap-northeast-1.amazonaws.com/Android+Products/Software+User+Guide/ReMoCloud/CipherLab+ADC+Module/ADC.zip
                              ↓
        d2b20xz24496kr.cloudfront.net
```

5. Save the edited URL for CipherLab OEMConfig deployment.

```
https://d2b20xz24496kr.cloudfront.net/Android+Products/Software+User+Guide/ReMoCloud/CipherLab+ADC+Module/ADC.zip
```

9.3.3 HOW TO DEPLOY THE ADC PROJECT SETTINGS THROUGH REMOCLOUD

To deploy the ADC project settings:
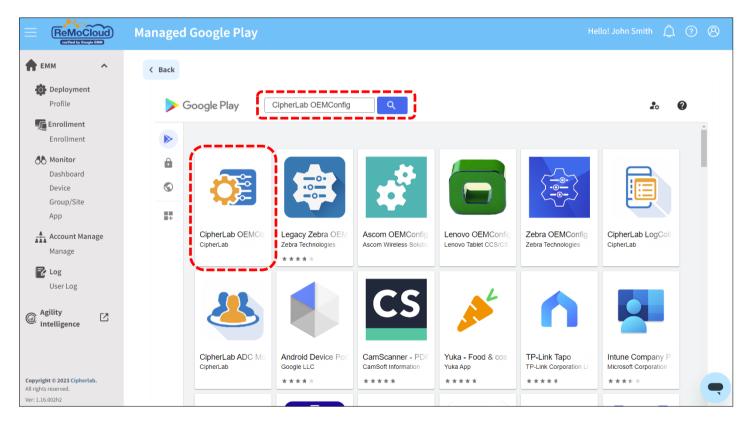
1. Access Profile>Profile name>Profile Information>App

2. Find the default App "**CipherLab OEMConfig**" from the App list. Click its "**Edit**" button from the "**Manage Config**" column.

If "**CipherLab OEMConfig**" is not included in the profile, click "**Add App**" to add it from the "**App Management**" page.

3. On the "**Manage App Config**" page, click to unfold the settings of "**DeployFromZip**".

Unfold other settings for more configuration if necessary.

The settings on the "**Manage App Config**" page:

(1)   DeployFromZip

(2)   Wireless

(3)   Wi-Fi Advanced

(4)   Cellular Data

(5)   System Setting

(6)   System Update

(7)   Log Collection

(8)   Send Intent

(9)   Button Assignment

(10)   Reader Config

(11)   Enterprise Settings

(12)   Cold Chain

(13)   SIP Controller

(14)   Software Trigger

(15)   Other Settings

Note that if the "**DeployFromZip**" settings' parameters and and other OEMConfig settings' parameters are in duplicate, the "**DeployFromZip**" settings have the highest priority to be applied.

4. Switch on "Deploy From Zip Control".

5. Input the link created from the cloud storage to the "**Deploy From Zip Control**" field.

6. Click on the "**OK**" button to save the changed settings before leaving this page.

7. Return to the "**Profile Information**" page, click "Save" or "Schedule" to carry out the changed settings.

For other settings, refer to **CipherLab OEMConfig** for more details.

Note:

The enrolled devices in the profile shoud be consistent with the device model from the ADC project to be deployed.

9.4 CIPHERLAB LOGCOLLECTION

The default App "**CipherLab LogCollection**" coworks with the App "**CipherLab OEMConfig,**" to upload the log data of the enrolled device to the designated PC.

Note that CipherLab LogCollection is concealed on the enrolled device.

9.4.1 PREREQUISITES
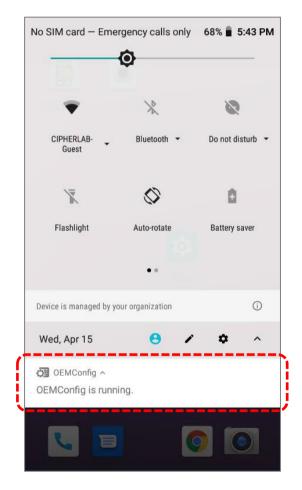
The requirements for uploading the device's log data to the designated PC:

1. Create a new profile or add all default Apps to an existing profile.

2. Enroll the device for log uploading to apply to the profile.

3. Make sure that "**CipherLab LogCollection**" and "**CipherLab OEMConfig**" are both installed on the enrolled device. Access the "**Device Information**" page to check if these two Apps are included in "**Install App**".

4. Make sure that the OEMConfig service is running. As shown:

9.4.2 LOG COLLECTION SETTINGS ON OEMCONFIG

1. Access the profile for setting. Click the "Edit" button of "**CipherLab OEMConfig**" from the "**Manage Config**" column.

2. On the "**Manage App Config**" page, switch on "Enable Log collection".

3. Unfold the settings of "**Log Collection**" and fill out all the necessary fields.

The necessary fields that must be filled in:

Item	Description
Server address	The FTP Server IP
Server port	The FTP port number
Upload path	The path to access the folder where the uploaded log will be saved. For root directory, input a slash " **/** ". Upload path /
Username	The user name for logging in to the FTP server from an FTP client
Password	The password for logging in to the FTP server from an FTP client

1. Click "**OK**" and return to the "**Profile Information**" page after completing the settings of **Log Collection**.

2. Make sure to "Save" or "Schedule" the changed settings before leaving the "**Profile Information**" page.

9.4.3 UPLOAD LOG

When the settings of "**Log Collection**" are completed, the "**Upload Log**" button will appear at the bottom of the **Device Information** page.
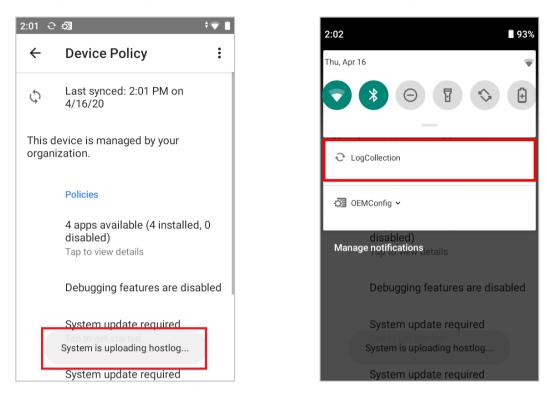
Click the "**Upload Log**" button and the log data of the device will immediately be uploaded to the FTP server.

The result of uploading log data will be displayed next to the "**Upload Log**" button.

After clicking "Upload Log," the device will start to upload the log data.

On the designated PC, access the folder that was set for saving the uploaded log data and locate the log file sent from the device.

The format of the log file's name will be "**SerialNumber_YYMMDD-HHMMSS_hostlog.zip,**" representing the device serial number, the date, and the time.

9.5 CIPHERLAB PROFILE INFORMATION

CipherLab Profile Information allows the user to review the profile's information on the enrolled device, including the profile's name, the profile version, the default Apps, and the installed Apps.
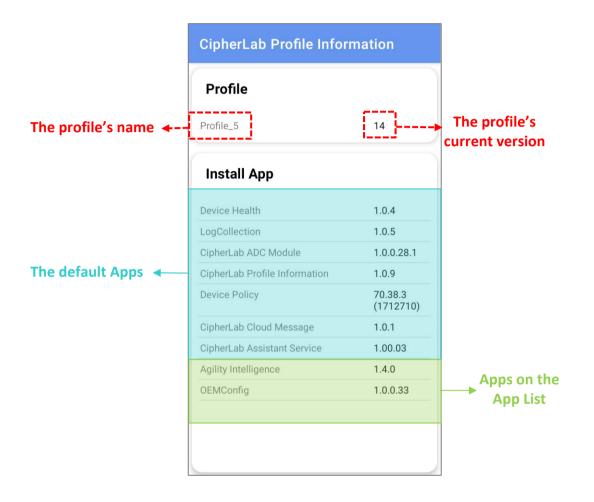
When the "**Sync Profile Information to Device**" function is never turned on, there will be no data on "**CipherLab Profile Information**".

Switch on "Sync Profile Information to Device" on the "Device Setting" page to review the data.

381

After the "**Sync Profile Information to Device**" is switched on, even if the user switches it off again, it will always show the information the last time it synchronized.

Make sure to save or schedule to carry out the changed settings.

The profile's name ←--

The profile's current version

The default Apps ←

Apps on the App List

CipherLab Profile Information

Profile

Profile_5   14

Install App

Device Health	1.0.4
LogCollection	1.0.5
CipherLab ADC Module	1.0.0.28.1
CipherLab Profile Information	1.0.9
Device Policy	70.38.3 (1712710)
CipherLab Cloud Message	1.0.1
CipherLab Assistant Service	1.00.03
Agility Intelligence	1.4.0
OEMConfig	1.0.0.33

9.6 CIPHERLAB HOME

"**CipherLab Home**" is the App that restricts user operation and customizes both the background and App settings.

By default, it will be installed on the enrolled device after setting "**CipherLab Home**" as the "**Lock Task Mode**". The App will not be uninstalled or removed even when switching the **Lock Task Mode** from **CipherLab Home** to other modes.

By enabling "**CipherLab Home**," the related functions will appear for further settings.

9.6.1 CIPHERLAB HOME APPLICATION SETTINGS

"**Cipherlab Home Application Settings**" determines what Apps will be available on the enrolled device.

Follow the steps to add Apps to CipherLab Home screen:

1. Click "**Edit**" to open the "CipherLab Home Application Settings" window.

2. Select the Apps from the "Application" list and click `+ Add`.

3. Or, input the App's package name and click `Add`.
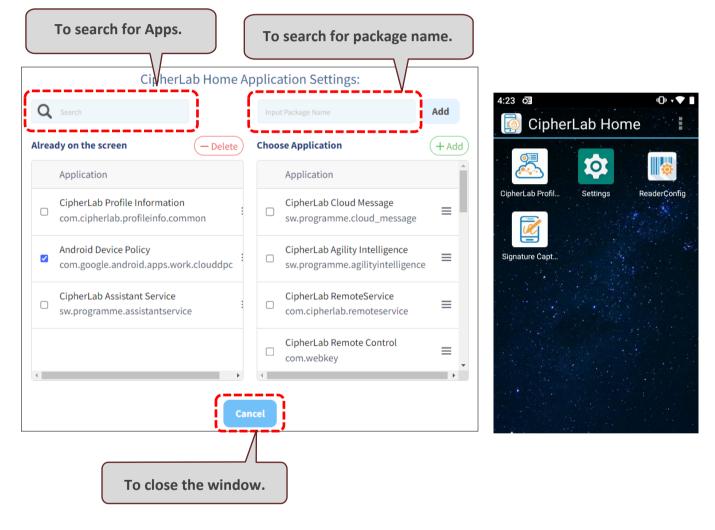
Note: Only the system built-in Apps or the installed Apps from the profile App list can be set for CipherLab Home screen.

4. The App added successfully will be on the "**Already on the screen**" list.

Make sure to Save or "Schedule" to carry out the changed settings. The enrolled devices that apply to the profile will change to CipherLab Home mode and display only the allowed Apps.

To remove the App from the "**Already on the screen**" list, select the App and click ⊖ Delete .

To search for Apps.

To search for package name.

To close the window.

9.6.2 CIPHERLAB HOME CLEAR CACHE APPLICATION SETTINGS
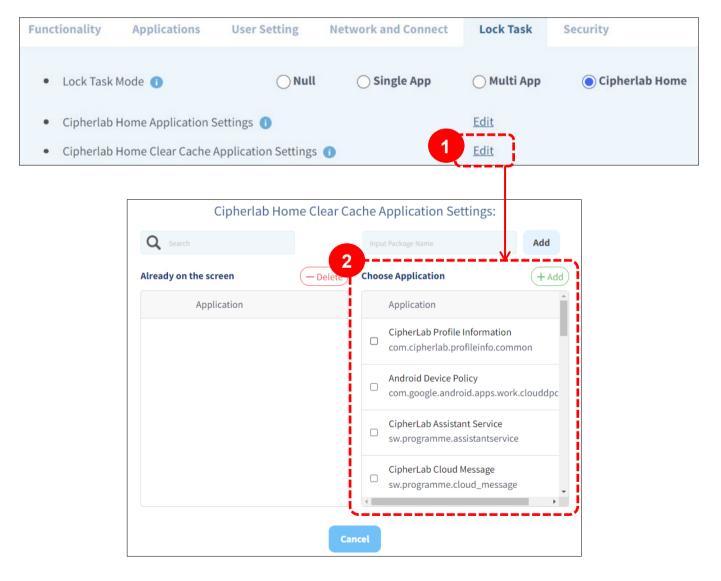
"**Cipherlab Home Clear Cache Application Settings**" clears the App cache, that is, removing all the temporary stored files the App uses.

To function properly, the version of Google Chrome App should be 9.0 or later.

SETTING CLEAR CACHE APPLICATION

Follow the steps to set Apps for clearing the cache:
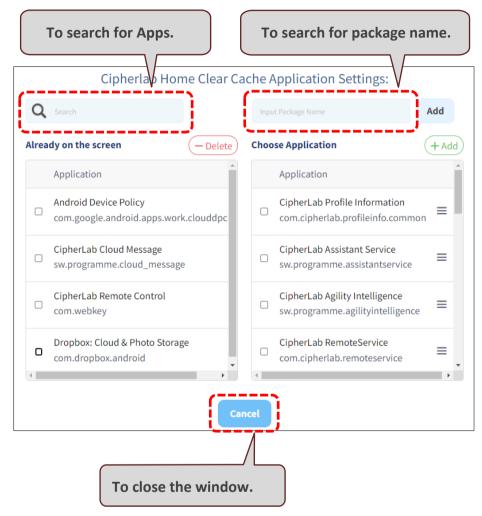
1. Click "**Edit**" to open the "Cipherlab Home Clear Cache Application Settings" window.

2. Select the Apps from the "Application" list and click 〔+Add〕.

3. Or, input the App's package name and click 〔Add〕.

4. The App added successfully will be on the "**Already on the screen**" list.

Make sure to Save or "Schedule" to carry out the changed settings. The enrolled devices that apply to the profile will change to CipherLab Home mode and display only the allowed Apps.

To remove the App from the "**Already on the screen**" list, select the App and click (− Delete).

Make sure to "save" or "Schedule" to carry out the changed settings.

Note:

Only the built-in Apps and the installed Apps will be available for **Cipherlab Home Clear Cache Application Settings**

HOW TO SET WEB APP AS CLEAR CACHE APPLICATION

To add web Apps to the clear cache list, the user needs to create the web App and add it to the profile App list in advance.

1. Click "**Add App**" on the profile information page to enter the "**App Management**" page.

2. Select "**Web Apps**" on the side menu.
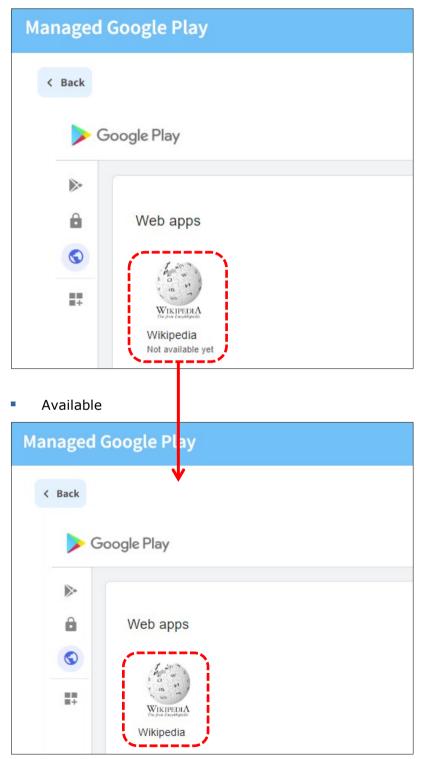
3. Click the add button ⊕ to create a new web App.

4. Fill out all the necessary information and click "**Create**".

5. The newly created web App will be listed on the "**App Management**" page. The created web App will become available in a while. When the web App has become available, click it to enter the "**Edit web app**" page.

▪ Not available yet

▪ Available

6. On the "**Edit web app**" page, click "**Select**" to add the web App to the profile's App list.

7. Now, the web App is allowed to be added to the clear cache App list.

For more details, refer to "**Setting Clear Cache Application**".

9.6.3 CIPHERLAB HOME BACKGROUND SETTINGS

To customize the background of the enrolled device:

1. Input the URL of the wallpaper into the "**Cipherlab Home Background Settings**" field.

2. Remember to save or schedule to carry out the changed settings.

The customized background is applied to the enrolled device as shown.
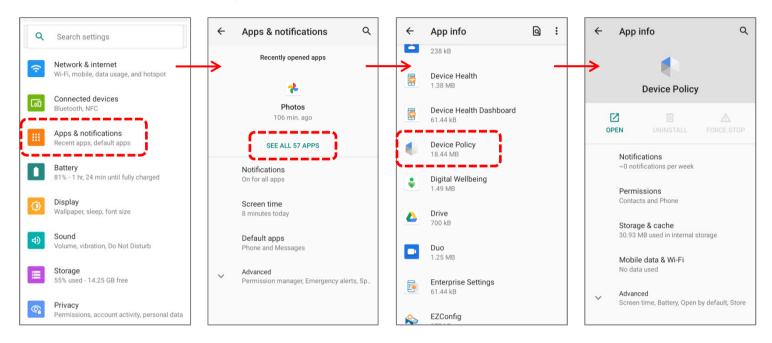
9.7 DEVICE POLICY

The default App "**Device Policy**" is developed by Google for the EMM administrator to remotely manage the enrolled device. It is concealed in the App Drawer on the device.
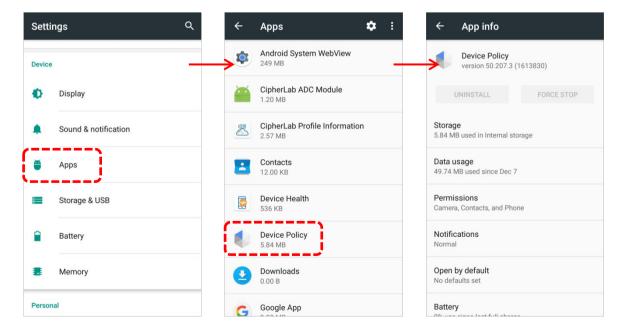
Access **Settings>Apps & notifications** or access **Settings>Apps** (depending on different device models) to check it on the device.

Take RS35 and RS50 for examples:

- RS35 Mobile Computer

- RS50 Mobile Computer

"Device Policy" is also listed on Device>Model Name>Install App>Managed Installed Apps on ReMoCloud.

To work properly, the App "**Device Policy**" on the enrolled device will automatically update itself to the latest version that Google released.

Chapter 10

CHAPTER 10. USER INFO

This chapter carries the introduction of the pages directed from the header navigation button,"**User Info**" .

IN THIS CHAPTER

ReMoCloud User Guide

10.1 CHANGE USER INFORMATION

Click the "**User Info**" button 👤 and click "Account" to enter the "**Edit Account**" page.

In this page, the user can check and change the information settings.

Make sure to "**Save**" before leaving the "Edit Account" page.

396

The editable sections of the "Edit Account" page are:

Item	Description
User Name	Enter your name. This section is allowed to be left blank.
Company	Enter the organization's name. This section is allowed to be left blank.
Phone	Enter your phone number. This section is allowed to be left blank.
Nation	Select the country from the drop-down menu.
Time	Set the time zone.
Language	Select to change the display language.
System Refresh Time	To schedule automatic refreshes of the device status.
System Logout Time	To set the logout timer to protect your data from unauthorized access.
Reset Password	To set the new password.
Google Authenticator	2FA (Two-factor authentication) setup settings.
Unenroll	To remove ReMoCLoud as the EMM provider from the user's Managed Google Play account.
Integration	To connect ReMoCloud to SATO Online Services.

10.2 USER NAME & GREETING MESSAGE

The first name and last name you set will be displayed as the greeting message next to the header navigation buttons.

After saving the changed settings, the greeting message will change accordingly.

10.3 ENABLE GOOGLE AUTHENTICATOR

"**Google Authenticator**" is the function that sets up **2FA** (**Two-factor authentication**) for the user's ReMoCloud account. More specifically, 2FA is the security process that enhances the access security by two different authentication factors. To reinforce the security of the ReMoCloud account, it is highly recommended that users enable 2FA to protect their accounts from being compromised.

2FA works by requiring the following two verification methods:
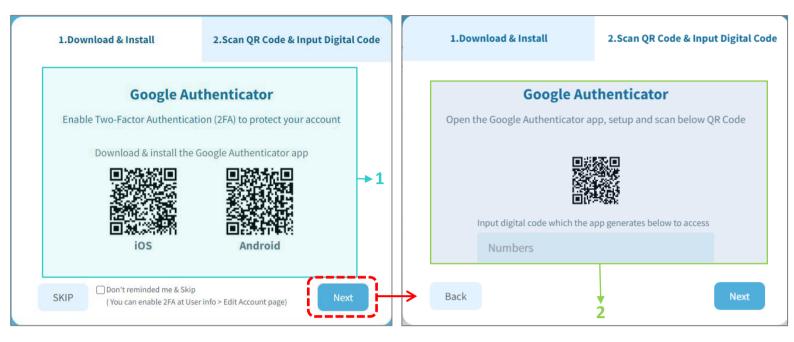
1) The password of the user's ReMoCloud account.

2) The code sent to the user's trusted device.

Click the "**Enable Google Authenticator**" button to open the "**Google Authenticator**" pop-up window. The user may tick the "**Don't remind me & skip**" checkbox to block the "**Google Authenticator**" pop-up window from the ReMoCloud login process.

The items on the "**Google Authenticator**" pop-up window are:
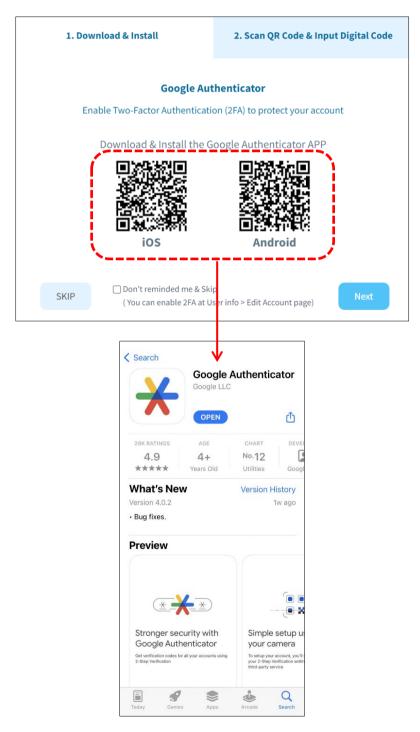
Item	Description
Step 1 (Download & Install)	Scan the QR code to download the App "Google Authenticator" on the user's trusted device. Click "Next" to proceed to step 2.
Step 2 (Scan QR Code & Input Digital Code)	Use the App's camera to scan the QR code. The digital code will be sent to the device. Input the digital code and click "Next" to activate 2FA.
Don't remind me & skip	Tick the "Don't remind me & skip" checkbox to block the "**Google Authenticator**" pop-up window from the ReMoCloud login process. The user may change this setting on "Edit Account" page.
Skip	Click "Skip" to pass over the "Google Authenticator".
Next	Click "Next" to proceed.

10.3.1 SET UP TWO-FACTOR AUTHENTICATION (2FA)

To set up **2FA** for the ReMoCloud login process:

DOWNLOAD & INSTALL

Scan the QR code to download the App "Google Authenticator" on the user's trusted device.

1. Click "**Next**" to proceed to Step 2.

2. Launch the App "**Google Authenticator**" on the device. Click "Get started".

3. Click "Add a code".

4. Click "Scan a QR code".

SCAN QR CODE & INPUT DIGITAL CODE

5. Enter the code generated by "**Google Authenticator**" on the device and click "**Next**" to activate **2FA** on ReMoCloud.
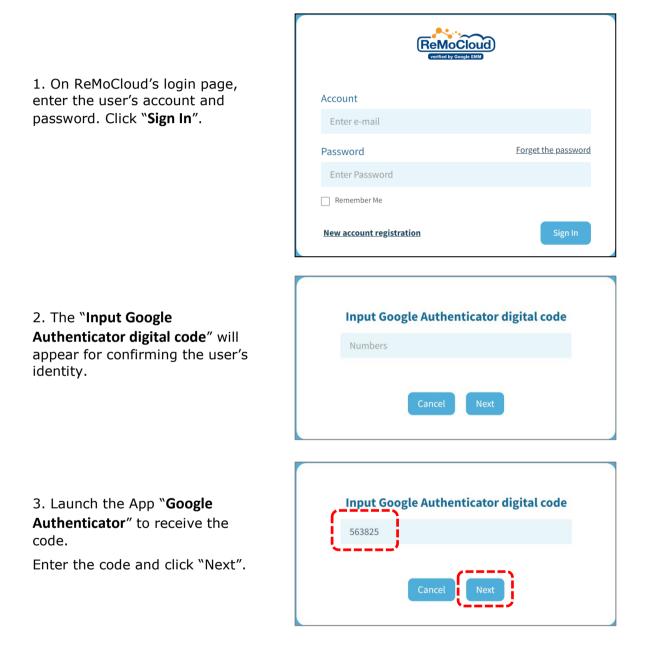
After **2FA** is activated, the "**Enable Google Authenticator**" button on the "Edit Account" page will become "**Disable Google Authenticator**".

10.3.2 2-STEP VERIFICATION

After activating **2FA** by following the steps "**Set up Two-Factor Authentication (2FA)**," the user will be asked to input the code generated by "**Google Authenticator**" whenever the user accesses ReMoCloud.

1. On ReMoCloud's login page, enter the user's account and password. Click "**Sign In**".

2. The "**Input Google Authenticator digital code**" will appear for confirming the user's identity.

3. Launch the App "**Google Authenticator**" to receive the code.

Enter the code and click "Next".

10.3.3 DISABLE GOOGLE AUTHENTICATOR

After 2FA is activated, the user can disconnect the authentication between the device and ReMoCloud:

1. Click the "Disable Google Authenticator" button on the "Edit Account" page to open "Input Google Authenticator digital code".

2. Enter the code sent from the App "**Google Authenticator**" and click "Next" to proceed.

When the **2FA** authentication is removed, the "**Disable Google Authenticator**" button will become "**Enable Google Authenticator**". The user may activate **2FA** again by following the steps "**Set Up Two-Factor Authentication (2FA)**".

10.4 CHANGE PASSWORD

To reset the password:

    1) Input the original password.

    2) Input the new password.

    3) Input the new password again for confirming.

    4) Click "Save" to carry out the changed settings.

10.5 UNENROLL

The "**Unenroll**" function is to remove ReMoCloud as the EMM provider from the user's Managed Google Play account. Performing "**Unenroll**" means that all the data on ReMoCloud will be eliminated. Also, the enrolled devices will be reset to factory settings.

1. Click the "**Managed Google Play**" button to make the pup-up window appear.
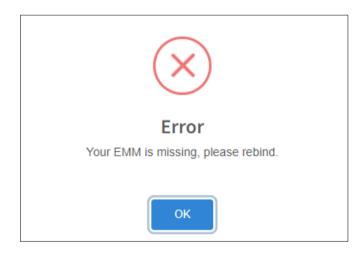
2. Click "**Yes**" to enter the "**Admin Settings**" page of **Managed Google Play**.

3. Click the more button ⋮ in the top-right corner of "**Organization information**"

4. Click "**Delete Organization**" and click "**Delete**" for confirming.

5. After returning to ReMoCloud, the "Error" pop-up window will appear when the user tries to use any function.

ReMoCloud User Guide

6. When the user logs in to ReMoCloud after deleting the organization information, the user will be asked to sign in to **Managed Google Play** with the super administrator account and to set ReMoCloud as the EMM provider.

For more details, refer to"Log on to Bind ReMoCloud with Managed Google Play Account".

FirstLogin First login

You have to bind ReMoCloud to your Managed Google Play Account.
Please click "OK" to complete the process to add ReMoCloud as your EMM provider.

[OK]

Note:
1) The Google account which is used for signing up for G-Suite cannot be bounden with ReMoCloud.
2) It's strongly suggested that do not use your personal Google account to bind with ReMoCloud as EMM. The Google account for organization would be more appropriate for binding.

7. The enrolled devices will be reset to factory settings after performing "**Unenroll**".

10.6 LICENSE INFORMATION

The "**License Information**" page displays the current status of all the user's ReMoCloud accounts, including the admin account, the parent accounts, and the child accounts.

Account Type	Account	License Type	Available	Purchased	In Used
Admin	joshua.hsu@cipherlab.com.tw		41	50	9
Parent	aabctesting@cipherlab.com.tw		1	10	9
Parent	hsu@gamil.com		1	10	9
Parent	josh@cipherlab.com.tw		41	50	9
Child	asd@cipherlab.com	Advance	50	-	1
Child	hh@gamil.com	Advance	10	-	3
Child	qwe@cipherlab.com	Advance	50	-	3
Child	zxc@cipherlab.com	Advance	50	-	0

For more details about the admin account and sub accounts, refer to **User Role Type** and **Sub Account**.

On the "**License Information**" page, the accounts' information will be listed as:

Account Type	Account	License Type	Available	Purchased	In Used
Admin	joshua.hsu@cipherlab.com.tw		41	50	9
		advance	2023/12/31	50	
Parent	aabctesting@cipherlab.com.tw		1	10	9
		advance	2023/12/31	10	
Parent	hsu@gamil.com		1	10	9
Parent	josh@cipherlab.com.tw		41	50	9
Child	asd@cipherlab.com	Advance	50	-	1

License Expiration Date

▪ License Type

The license type given to the account.

▪ Available

For **Main Accounts** (highlighted in blue), it represents the remaining device allocation for all accounts to use for device enrollment.

For child accounts, it represents the remaining device allocation specific to each child account for device enrollment.

▪ Purchased

The total number of devices purchased by the user for device enrollment.

▪ In Used

The amount of enrolled devices.

LICENSE TYPE

ReMoCloud offers three types of license.

Please contact the local sales representative for ReMoCloud license consultation.

Type	Description
Advance	Offering the advanced features.
Standard	Offering the basic features.
Trial	Offering the "**Advance**" level features within the validity period.

APPENDIX I

AGILITY INTELLIGENCE

"**CipherLab Agility Intelligence Service**"(CAI) is the analytic service for enterprise mobility. It works with ReMoCloud to demonstrate the analytical reports of enrolled devices.

Click "**Agility Intelligence**" on ReMoCloud's main menu to open the **CAI Service** page(https://cai.cipherlab.com/). ReMoCloud users can log in to **CAI Service** with their ReMoCloud account and password, including the admin account, the parent account, and the child account.

For more details, refer to CipherLab Agility Intelligence Service User Guide.

Note that the user can only review the data of the devices from the assigned profiles and groups when logging in to **CipherLab Agility Intelligence Service** with the child account.

413
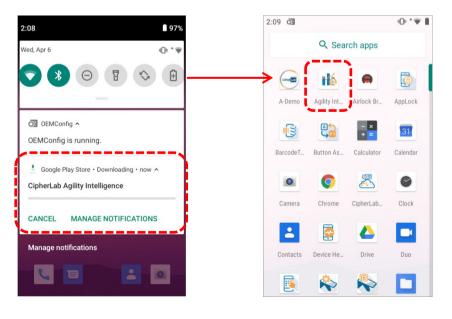
To enable **CAI Service** for group devices:

1. Access Profile Information>Device Setting>Functionality

2. Switch on the "**Allow Agility Intelligence Service**" item and click "**Save**" to carry out the changed settings.

3. The enrolled devices from the profile will automatically download "**Agility Intelligence**".

4. After successfully installed, launch the App "**Agility Intelligence**".
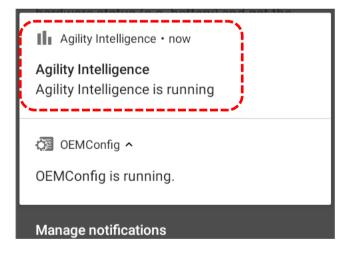
5. On the main screen, tap on the toggle button to activate "**Agility Intelligence**".

6. The user must accept CipherLab's "Terms and Conditions" to activate "**Agility Intelligence**".

After activated, "**Agility Intelligence**" will start to run in the background.
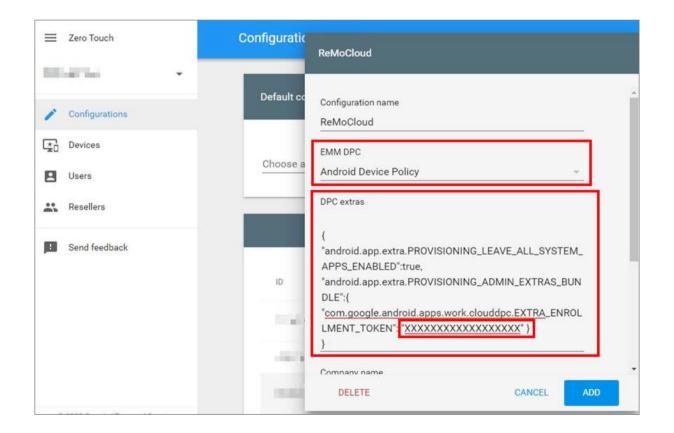
APPENDIX II

SETTINGS FOR ZERO TOUCH

Zero Touch portal link: https://partnerdash.google.com/zerotouch

For the "EMM DPC" field, select "Android Device Policy".

For the **DPC extras** field, input the following:

```
{
"android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true,
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{
"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":
"XXXXXXXXXXXXXXX" }
}
```


The "XXXXXXXXXXXXXXXX" part should be the enroll code generated by ReMoCloud. Hence, the device will apply to the corresponding profile during enrollment.

Note:The Zero Touch settings should be updated whenever the user generates a new enroll code.

APPENDIX III

REMOTE CONTROL ON REMOCLOUD

"**Remote Control**" allows the user to control the Android devices by the browser-based dashboard. More specifically, the "**Remote Control**" function enables the ReMoCloud administrator to remote control the enrolled devices.

"**Remote Control**" is only available for the users with advance license, please contact the local sales representative for activating "**Remote Control**" on ReMoCloud.

ENABLE "ALLOW REMOTE CONTROL"

To use the "**Remote Control**" function, the user should enable "**Remote Control**" from the "Device Setting" page in advance.

1. Access Profile Information>Device Setting>Functionality

2. Switch on "**Allow Remote Control**" and click "**Save**".

3. You can also enable "**Remote Control**" by [clicking the Device etting buttons](#).
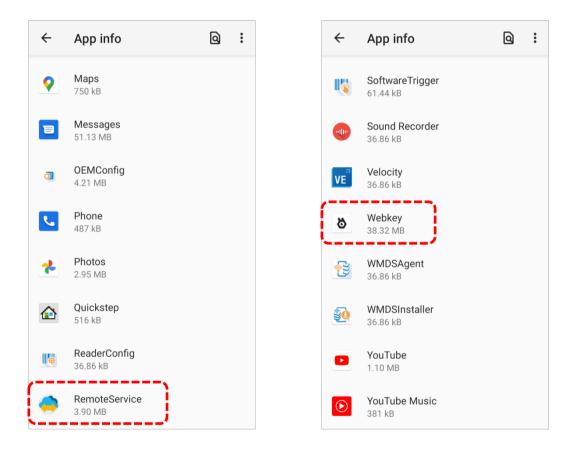
The enrolled devices will start to download and install "**CipherLab RemoteService**" and "**Webkey**" (**CipherLab Remote Control**).

⬇ Google Play Store · Downloading · now ⌃	⬇ Google Play Store · Downloading · now ⌃
CipherLab RemoteService	**CipherLab Remote Control** 17 seconds left
CANCEL MANAGE NOTIFICATIONS	CANCEL MANAGE NOTIFICATIONS

Note that "**RemoteService**" and "**Webkey**" (**CipherLab Remote Control**) must be successfully installed on the device. Otherwise, "**Remote Control**" will be unavailable.

▪ On the Enrolled Device:

Access App Drawer (All Apps)>Settings>Apps & notifications

Check and confirm that "CipherLab RemoteService" and "Webkey" are installed.

- On ReMoCloud:

1. Access Device > Model Name>Device Information>Install App>Managed Installed Apps
Check and confirm that "RemoteService" and "Webkey" are listed.

2. Access the "Application" page to check and confirm that "RemoteService" and "Webkey" are updated to the latest version.

REGISTER THE ENROLLED DEVICE(S)

The prerequisites for registering the enrolled devices:

1) The "**Remote Control"** function is successfully activated on the device.

2) The two Apps, "CipherLab RemoteService" and "Webkey" (CipherLab Remote Control), work properly.

3) The device's status is "**online**".

Note that the device amount for the user to register devices varies depending on different Remote license types.

To register the enrolled device:

CLICK THE DEVICE SETTING BUTTONS

1. On the "Device" page, select the "online" devices.

2. Click ⋮ to unfold the drop-down menu.

3. Click "Enable Remote Control(Selected)". Alternatively, you can click "Enable Remote Control(All) to enable Remote Control for all enrolled devices.

4. On the "Are you sure you want to continue?" window, click "OK" to proceed.

5. The registration process will take a while, less than 10 minutes.

After completing the registration process, the color of the "**Remote eye**" button will transition from grey 👁 to yellow 👁 to green 👁, indicating its availability.

The information about the "**Remote eye** 👁" button:

Button	Description
👁 Grey	Click to register the device for being controlled by Remote Control.
👁 Yellow	The registration process is still ongoing.
👁 Green	The device is successfully registered. Click to open the browser-based tool for remote controlling the device.
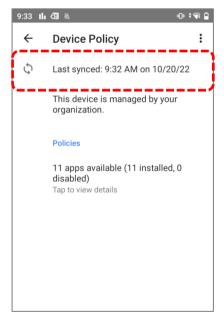
On the registered device, unfold the notification drawer to check the connection status, "Webkey is connecting" and "Webkey is active".

When the registration process takes too long, the user should:

(1) Reboot the device.

(2) On the device, access App Drawer (All Apps)>Settings>Google>Device Policy.

(3) Tap on ⟳ to manually synchronize the device with the settings on ReMoCloud.
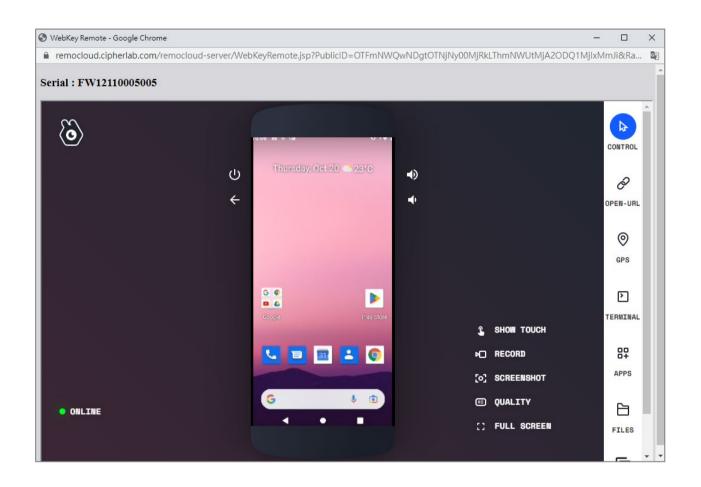
If the registration fails, the color of the "**Remote eye**" button will turn back to grey 👁.

Check if all the prerequisites mentioned in the previous section of this chapter are met, and then register again.

OPERATE THE DEVICE BY REMOTE CONTROL

To operate the registered device by remote control:

1. Find the device on the device list or enter its "**Device Information**" page.

2. Click the "**Remote eye**" button to open "**Webkey Remote**".

The functions of the buttons on Webkey Remote:

ON THE SIDEBAR

Item	Description
CONTROL	To open the control panel.
OPEN-URL	To enter the URL for the device to link.
GPS	To show the Global Positioning System(GPS) location of the device.
TERMINAL	To enable the real-time pseudoterminal access to the device.
APPS	The installed Apps on the device.
FILES	The internal storage of the device.
CLIPBOARD	Allow the user to copy and paste text to the device's input field.

ON THE CONTROL SCREEN
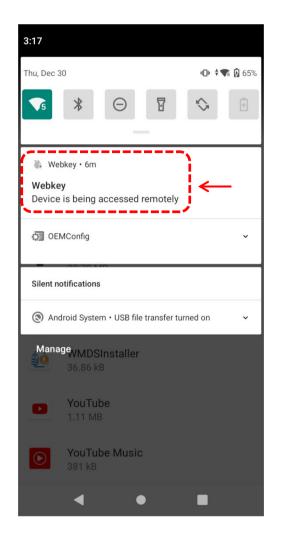
Item	Description
	The power button. Click once to turn on or off the device's screen. Click twice to turn the camera on. Long click to show the power menu.
	To return the user to a previously shown page.
	To increase the volume.
	To decrease the volume.
	To open the "More" menu for more functions.
	To be redirected to https://webkeyapp.com/ .

ReMoCloud User Guide

ON THE MAIN MENU

Item	Description
SHOW TOUCH / HIDE TOUCH	To enable or disable the touch pointer on the device display screen.
RECORD	To record the device's screen.
SCREENSHOT	To capture the image of the device display.
QUALITY	To change the streaming resolution settings.
FULL SCREEN	To maximize the device display screen.
EXIT FULL SCREEN	To exit the full screen mode.
◁	The navigation bar button "Back".
○	The navigation bar button "Home".
□	The navigation bar button "Recent".

On the controlled device, unfold the notification drawer to check the Webkey status, "Device is being accessed remotely".

APPENDIX IV

REMOCLOUD API SERVICE

The application programming interface (API) is for two different systems to share information and data. When an API calls another, it needs the API key to gain access because the API key serves as a secure password granting access between APIs.

Note that the ReMoCloud API service is currently only available for the users that have applied for this service. If you need the ReMoCloud API service, please contact CipherLab Support.
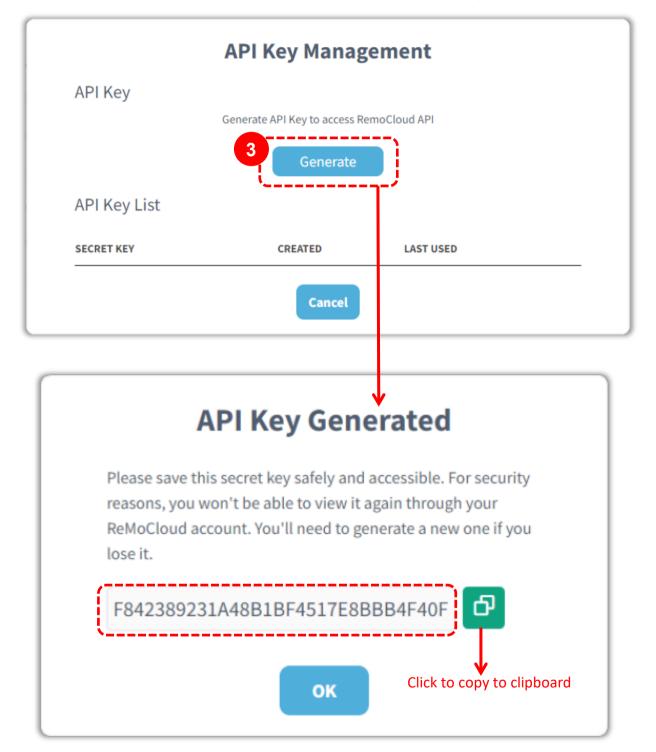
CREATE API KEY

Follow the steps to create the API key for accessing ReMoCloud API:

1. Click ⑦ in the top right corner to access the "Help Page".

2. Click "Create API Key".
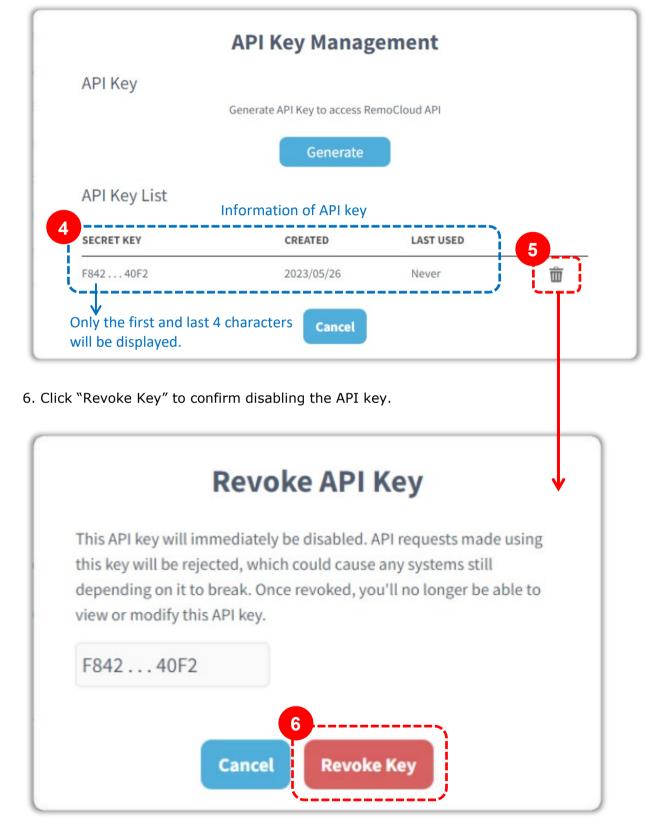
3. Click "Generate" on the "API Key Management" window to create and view the API key. Please note that ReMoCloud will display the API key only once upon its generation. Remember to securely store your API keys. If lost, you'll need to generate a new one.

API Key Management

API Key

Generate API Key to access RemoCloud API

3 Generate

API Key List

SECRET KEY	CREATED	LAST USED

Cancel

API Key Generated

Please save this secret key safely and accessible. For security reasons, you won't be able to view it again through your ReMoCloud account. You'll need to generate a new one if you lose it.

F842389231A48B1BF4517E8BBB4F40F

Click to copy to clipboard

OK

4. The information of the created API key will be displayed.

5. If necessary, click 🗑 to disable the API key.

API Key Management

API Key

Generate API Key to access RemoCloud API

Generate

API Key List

Information of API key

SECRET KEY	CREATED	LAST USED
F842...40F2	2023/05/26	Never

Only the first and last 4 characters will be displayed.

Cancel

6. Click "Revoke Key" to confirm disabling the API key.

Revoke API Key

This API key will immediately be disabled. API requests made using this key will be rejected, which could cause any systems still depending on it to break. Once revoked, you'll no longer be able to view or modify this API key.

F842...40F2

Cancel   Revoke Key

APPENDIX V

REMOCLOUD X SATO

Users are allowed to effortlessly integrate the S.O.S interface, SATO's renowned MDM software, directly into the ReMoCloud system.

This seamless integration provides users with a unified and comprehensive view of data from both systems, presenting critical information from both ReMoCloud and SATO's S.O.S interface in one place.
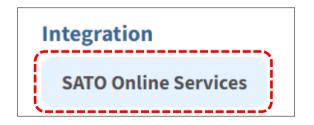
Note:

The special co-branding function is available exclusively for specific users. For more information, please contact your local sales representative.

Follow the steps to integrate SATO's S.O.S interface into ReMoCloud system:

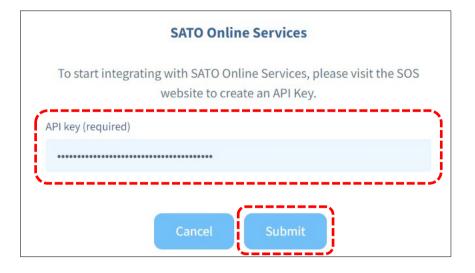1. Click the "**User Info**" button and click "Account" to enter the "**Edit Account**" page.

2. Click Integration > SATO Online Services.

3. On the "SATO Online Services" window, enter the API access token you created from S.O.S system and click "Submit".

Note:

For more details about creating the API key for integration, please contact SATO Online Services.

4. Once successfully integrated, the button will change to "SATO Online Services Connected," and the S.O.S system will appear on the sidebar menu as a new item.

5. Click SATO Online Services > Dashboard to enter the page that presents a collection of graphical reports to give the user a full picture of the printer information.
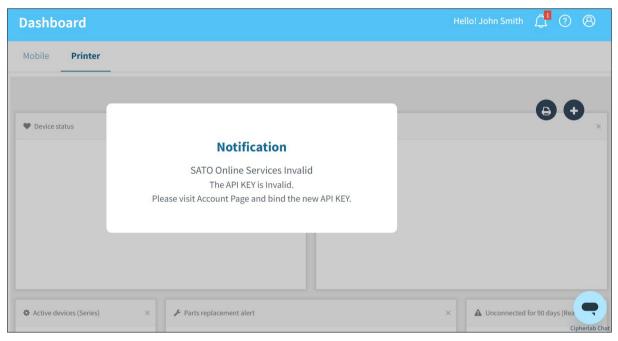

6. Click SATO Online Services > Device to enter the page that presents the devices you have registered with S.O.S system.
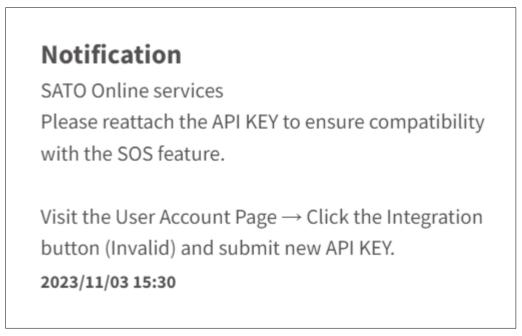
INVALID API KEY

If your API key is deleted or doesn't match, you will receive an "Invalid API Key" notification when accessing the "Dashboard" page.

Also, an alert message will instruct you to attach a new API key for restoring S.O.S interface integration.
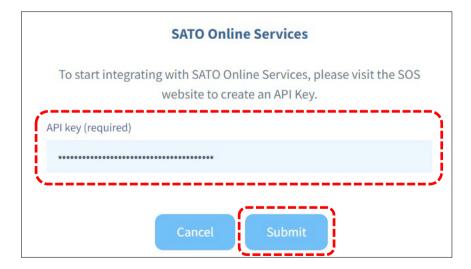
Follow the steps to reattach a new API key:

1. Click the "**User Info**" button , then click "Account" to enter the "**Edit Account**" page.

2. Click Integration > SATO Online Services (Invalid).

3. On the "SATO Online Services" window, enter the new API access token and click "Submit".

Note:

For more details about obtaining a new API key for restoring S.O.S interface integration, please contact your company's IT manager or SATO Online Services.

4. Once successfully integrated, the button will revert to "SATO Online Services Connected," and the "Dashboard" page will be restored.