The Guide Book of Unified Management System

UROVO TECHNOLOGY CO., LTD.

Catalogs

1 Summary

Agent management platform is a platform designed for agents to manage equipment, which provides one-stop solution for equipment management, application management, business tenant management.

2 System Overview

Agent management platform is provided for direct agent to use. Agents can invite their customers to register account for their application issuance and device management. Agents can upload applications, and can be found in the U-store without being subject to internal revives by partner connect platform. Its main function includes application management, management of devices by batch, equipment monitor and account management.

3 Register and Login

3.1 Register

Users can set up account and password via email register agents. Upon registration, users can use their account (E-mail registered) to login partner connect platform, followed by company information registration and the Company’s review, after which the platform is available for use.

Figure (3.1.1)

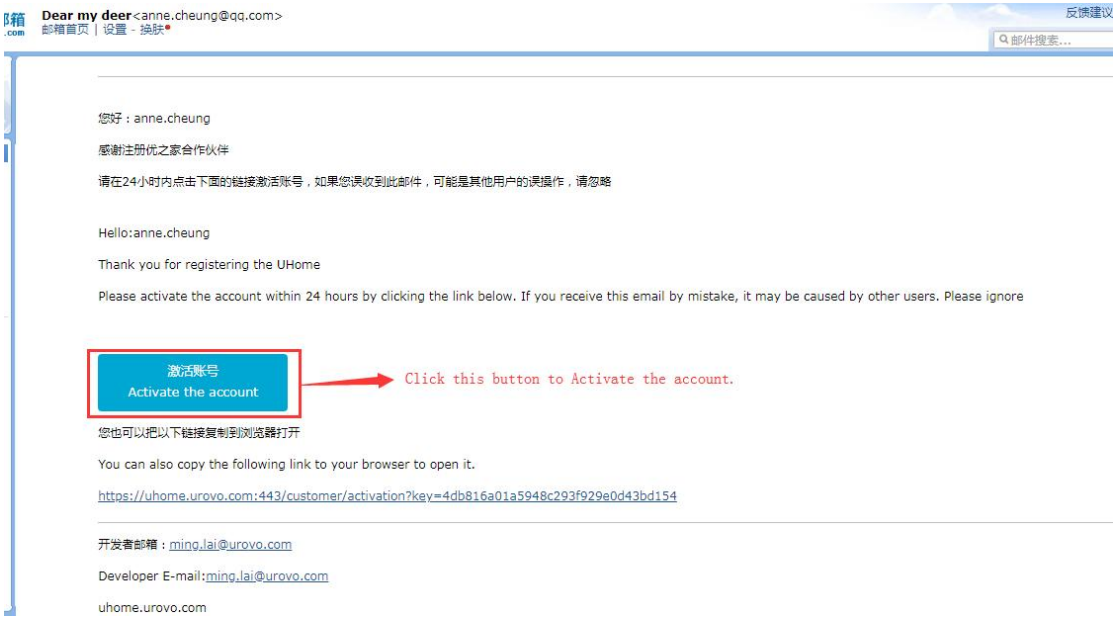


Figure (3.1.2)

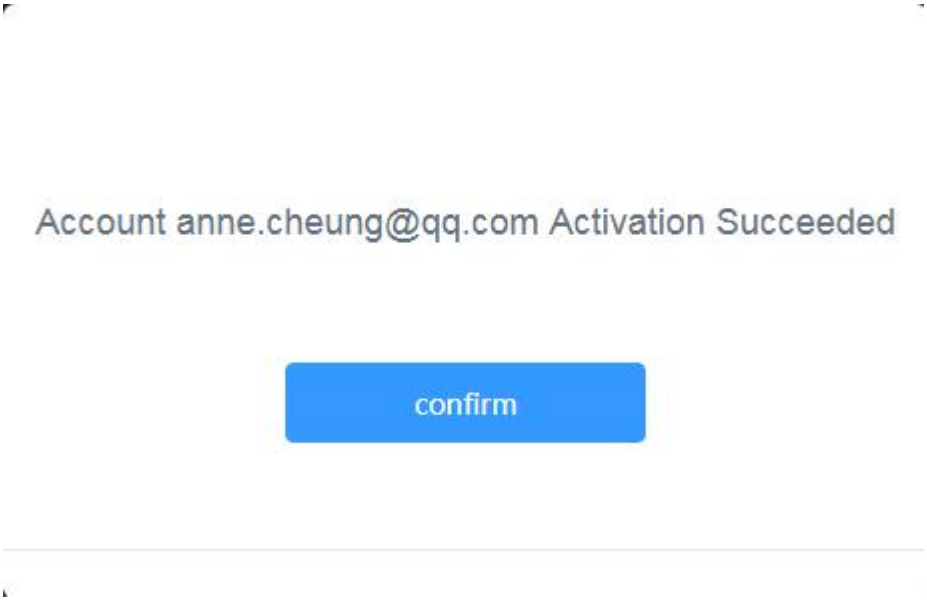


Figure (3.1.3)

1. Open the browser and at address field enter：https://uhomeov.urovo.com/customerui/login.
2. If you are **Agents account**, select [Sign Up], then enter the account and password, Click [Register Now]. After registration, the registered e-mail will receive an email for activation, as shown in the Figure (3.1.2);

   Click [Activate account] upon receipt of the email. Then, the account can be logged in after activation, as shown in the Figure (3.1.3). During the initial login, company information needs to be uploaded pending for review by Urovo. Users can use the system once Urovo approved.
3. If you are **customer of Agents account**, you will be the sub-account of a **Agents account**, who will invite you to register an account and send you an e-mail. You just need to login in through the account and password of the e-mail, and upload company information, as Figure (3.2.1) shows. Then wait for the review. Users can use the system once Urovo approved.

3.2 Login

Upon activation completed, users use the registered e-mail account and password to login the agent management platform, loaded in system then need to upload your company information, after checking it can use this device system, as shown in the

Figure below：

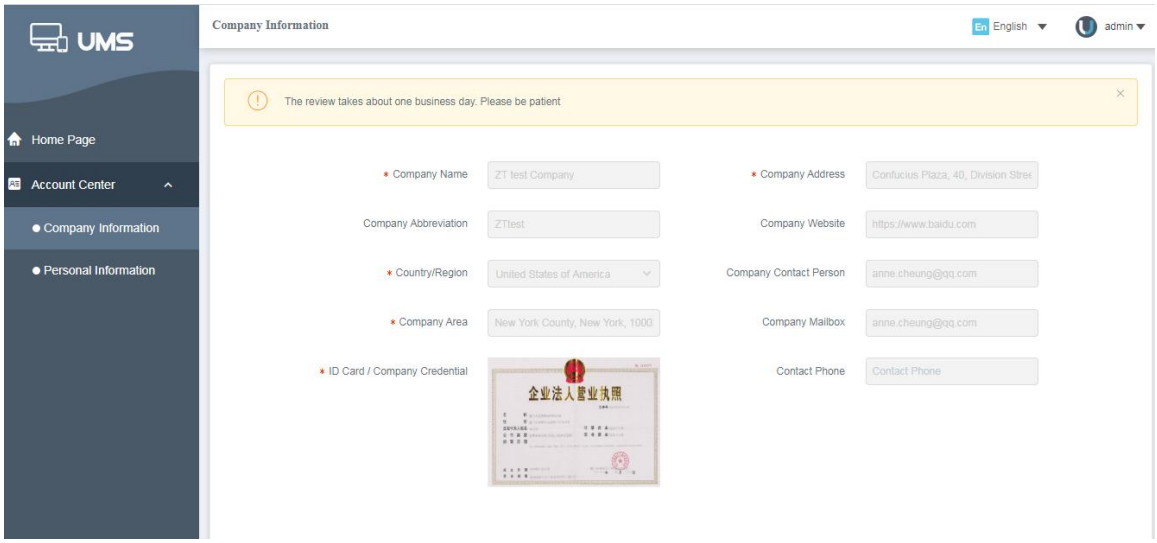


Figure (3.2.1)

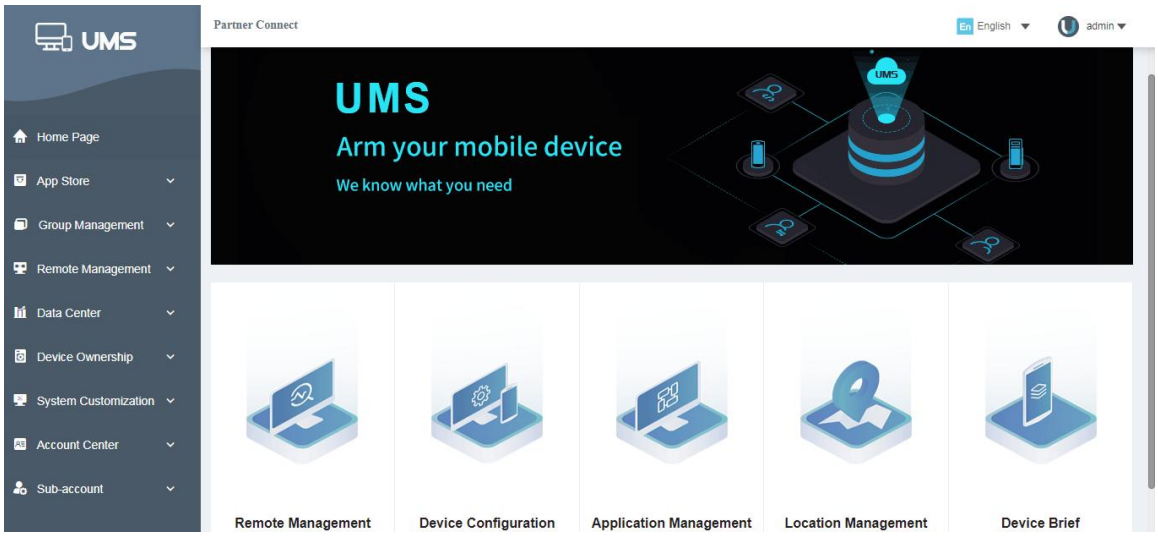


Figure (3.2.2)

1. After the initial login, company information, including company name, address and business licenses, should be uploaded pending for review by Urovo, as shown in the Figure (3.2.1). Once Urovo approve login the system again for use.
2. Enter user name (registered e-mail) and password after company information approved so as to use the system. After login, enter the main page of system where you find Urovo's product introduction and then click for details. You can exit and switch language in the upper right side. And on the left page side is a menu bar as shown the Figure (3.2.2).

3.3 Dashboard (new function)

After the company information is approved, input the username and password again to enter the

[Dashboard] on the home page. By clicking the menu page on the left to enter the [Dashboard], the [Device Overview], [Device Abnormal Status], [Warning Log], [Device Map] and [Flow Usage] will be displayed, as shown in the Figure below:

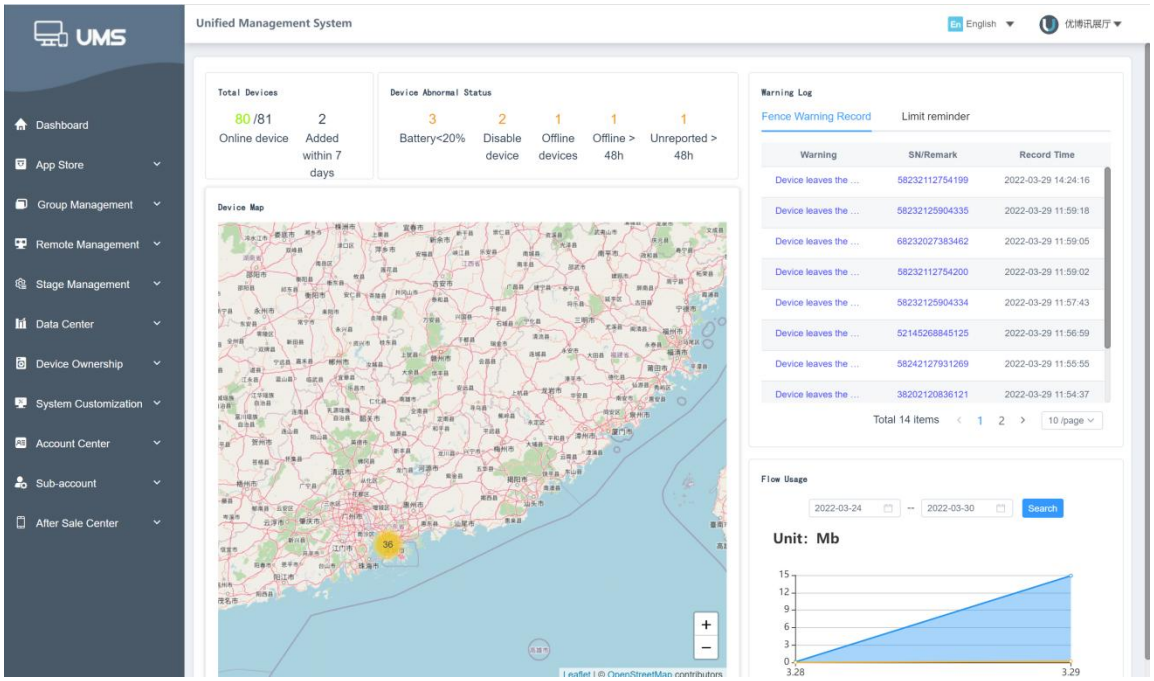


Figure (3.3.1)

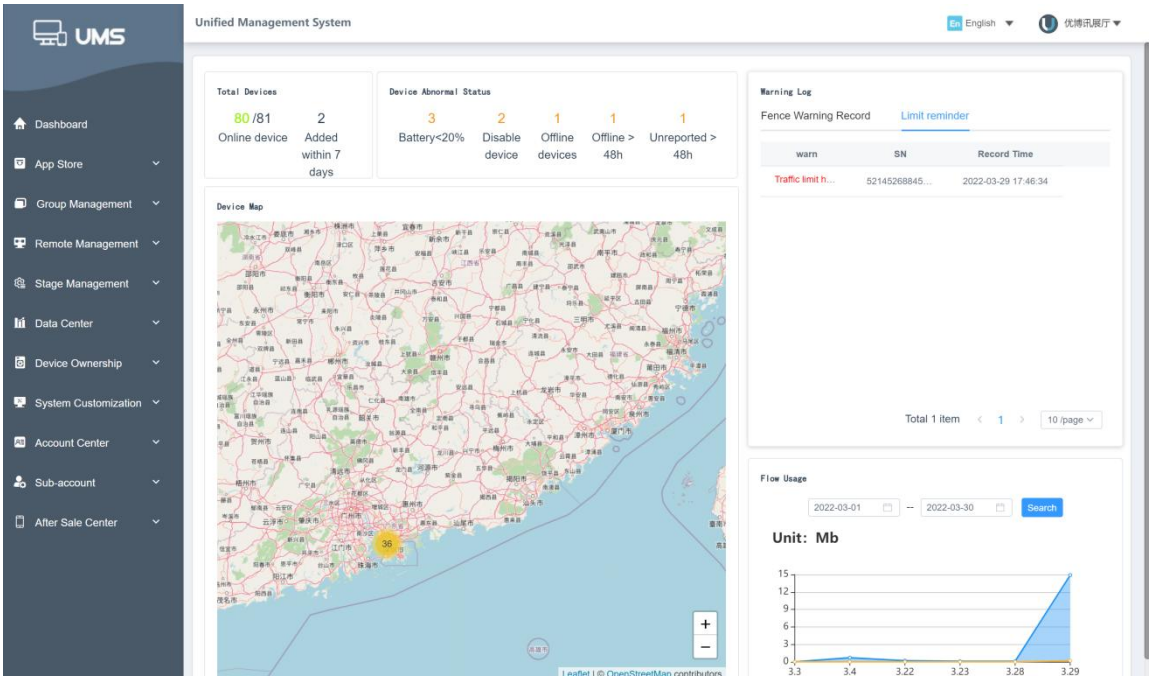


Figure (3.3.2)

1. Device Overview:

(1) Online devices/total devices: Dynamic display. Update data every time the page is refreshed.

(2) Added within 7 days: The number of activated devices within 7 days before 00:00 today in dynamic update.

2. Device Abnormal Status:

(1) Devices that need to be charged (less than 20%) : Dynamic display. The number of devices whose current battery is less than 20%, device SNs, and their groups to which the devices belong; Click the pop-up window to display all SNs and groups, which can be exported.

(2) Disable device: Dynamic display. The total number of devices in disabled status, device SNs, and groups to which the devices belong; Click the pop-up window to display all SNs and their groups, which can be exported.

(3) Offline devices: Dynamic display. The total number of devices in offline status, device SNs, and their groups to which the devices belong; Click the pop-up window to display all SNs and groups, which can be exported.

(4) Devices not online within 2 days: The total number of devices that are not online within 2 days (that is, 48 hours before 00:00 today), device SNs, and their groups to which the devices belong; Click the pop-up window to display all SNs and groups, which can be exported.

(5) Device information not reported within 2 days: The total number of devices whose information is not uploaded within 2 days (that is, 48 hours before 00:00 today), device SNs, and their groups to which the devices belong; Click the pop-up window to display all SNs and groups, which can be exported.

Figure (3.3.3)

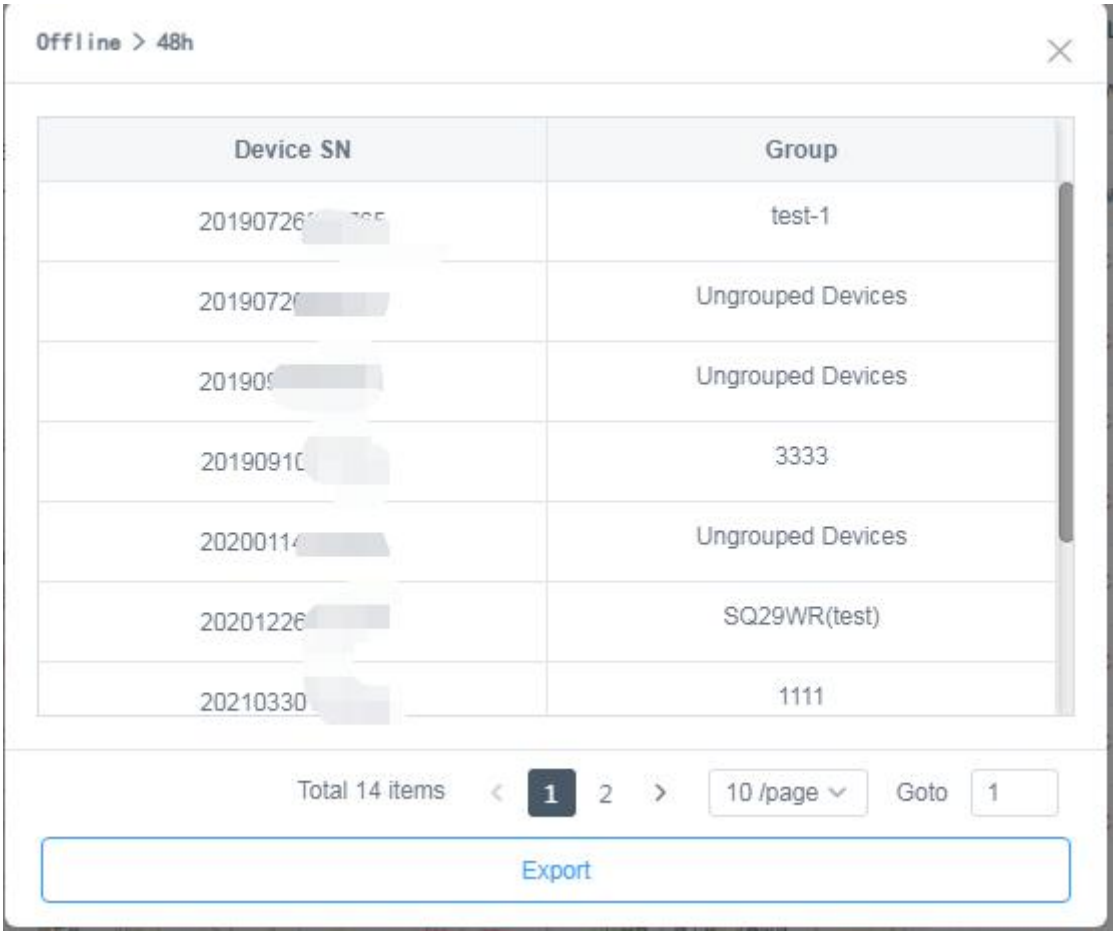


Figure (3.3.4)

3. Warning Log:

Geo-fence warning/limit reminder: record the warning types, SNs, device remarks, and record time.

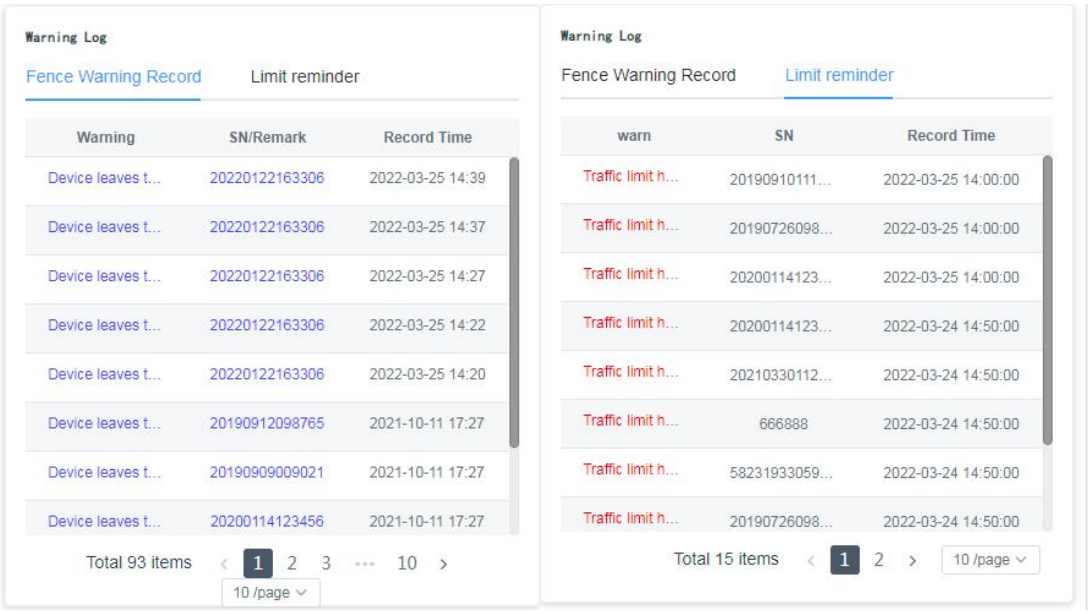


Figure (3.4.5)

4. Device Map:

The device distribution map under this account is displayed, and the scale of the map can be controlled through the mouse wheel.

5. Flow Usage:

It is consistent with the flow manager chart.

4 Application Functions

4.1 Data Center

For the purpose of monitor by agents, Data Center displays all devices information, including subordinate account, application information regarding the devices, equipment distribution and activation status.

4.1.1 Device Brief

Urovo helps agents bind all devices owned by them when the review is completed. After binding, users see their list of devices from[Data Center] - [Device Brief], as shown in the Figure below：

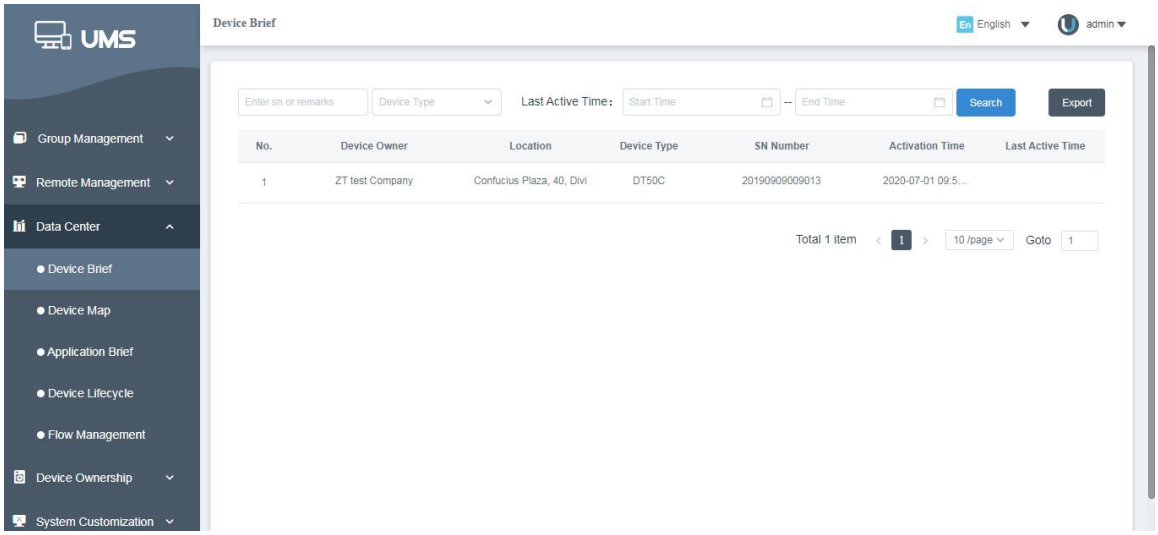


Figure (4.1.1.1)

1. Click the menu bar [Data Center]-[Device Brief] to find devices information owned by the logged account and all of sub-account information, including: number, Device owner, Location, and Device Type, SN number, the time of first and last time enter into system.
2. Enter the SN above and choose Device type, input the last activated time as the enquiry condition, to obtain corresponding device information.
3. Click [Export] button, users can turn the obtained device information in EXCEL format.

Tips:

If you have devices not bound in the UMS Platforms, please provide **Serial number (S/N)**, **Devices type** shows in the Setting Page, and **E-mail of account** to the agent or Technical supporters of Urovo. They will bind devices to your account.

Example:

A	B	C	D
TUSN	**DeviceType**	**Account**	**Remarks**
20195545646415	I9100	anne.cheung@qq.com	
20195545646416	I9100	anne.cheung@qq.com	
20195545646417	I9100	anne.cheung@qq.com	

4.1.2 Device Map

Click the [Data Center] and [Device Map] from the menu bar, users can find the distribution of company that owns the devices and related device distributions, Click switching button, and it shows the real time of location information uploaded by devices, as shown the Figure below:

1. The map of user location, click [Data Center]-[Device Map], system will show up the registered company location and the number of devices.

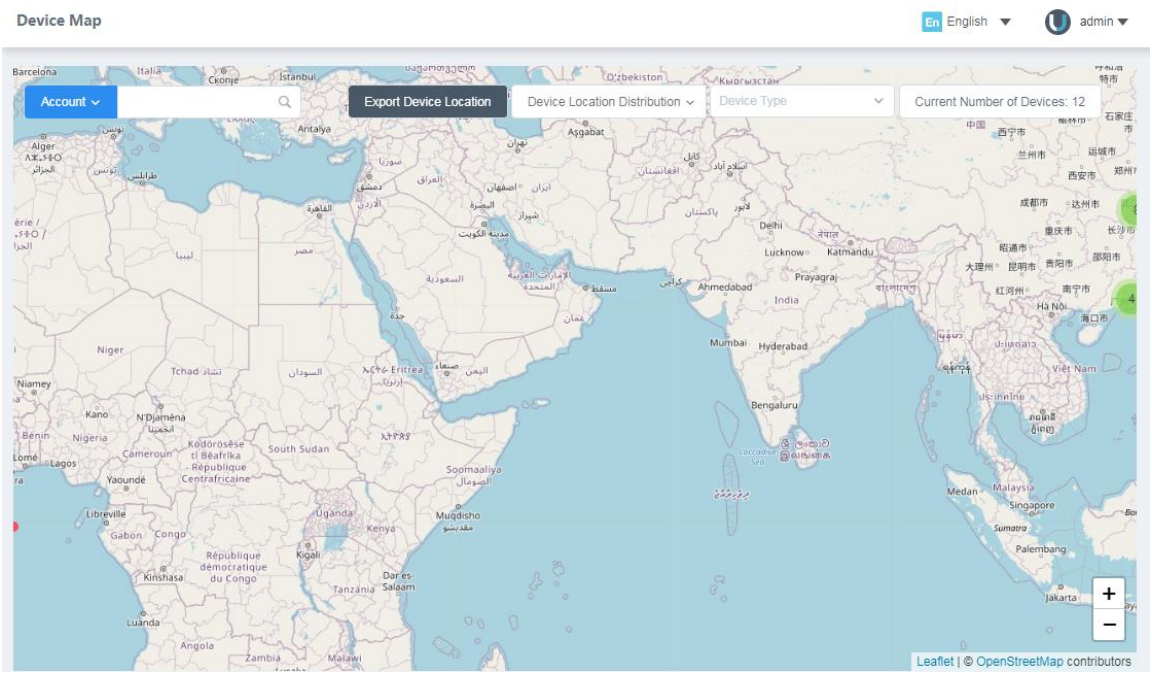


Figure (4.1.2.1)

2. The map of this device location, click switching button, it will show up this account and all of its sub-user, uploaded device location and GPS. Click location spot will show SN number, put your mouse on it then you will see the type of this device and where it from.

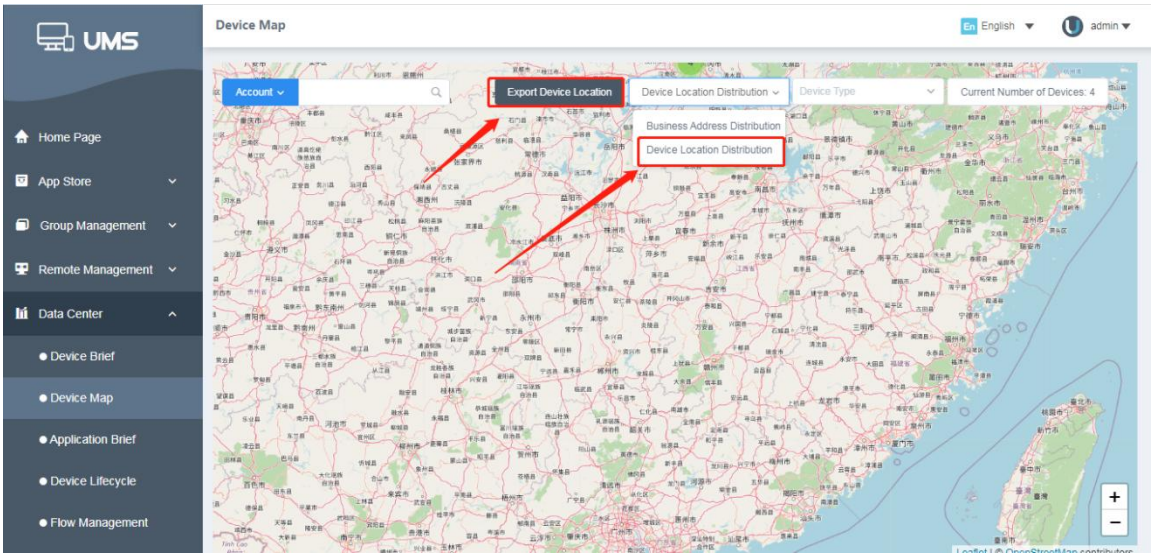
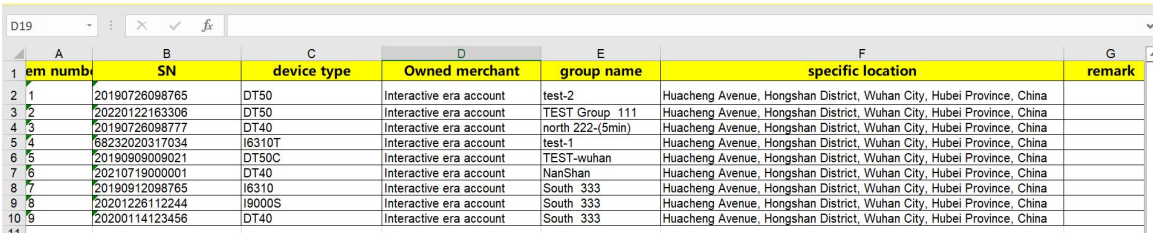


Figure (4.1.2.2)



em numb	SN	device type	Owned merchant	group name	specific location	remark
1	20190726098765	DT50	Interactive era account	test-2	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
2	20220122163306	DT50	Interactive era account	TEST Group 111	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
3	20190726098777	DT40	Interactive era account	north 222-(5min)	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
4	68232020317034	I6310T	Interactive era account	test-1	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
5	20190909009021	DT50C	Interactive era account	TEST-wuhan	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
6	20210719000001	DT40	Interactive era account	NanShan	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
7	20190912098765	I6310	Interactive era account	South 333	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
8	20201226112244	I9000S	Interactive era account	South 333	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	
9	20200114123456	DT40	Interactive era account	South 333	Huacheng Avenue, Hongshan District, Wuhan City, Hubei Province, China	

Figure (4.1.2.3)

Note：

(1) The map of tenant location distribution (Figure 4.1.2.1) shows the location indicating the address of subordinate company that owns the device, instead of the location information of device.

(2) Click [Switch] on the upper right of map, change to [Device Location Distribution] mode, you can find location information uploaded by the device in real time.

(3) If there are more than 10 devices under sub-account in the page, a group of figures are displayed and click to look for the total number and modes of devices.

(4) There are query conditions on the upper side of Map. Enquire can be made by tenant name and SN number on the left side and by device type on right side.

(5) After switching to the Device Location Distribution mode, click the [Export Device Location] button to export the location information table of the device, as shown in Figure (4.1.2.3);

4.1.3 Application Brief

Click [Data Center]-[Application Brief] in the menu bar to find third-party application of all devices under this account, Click [Export] button to see query results.

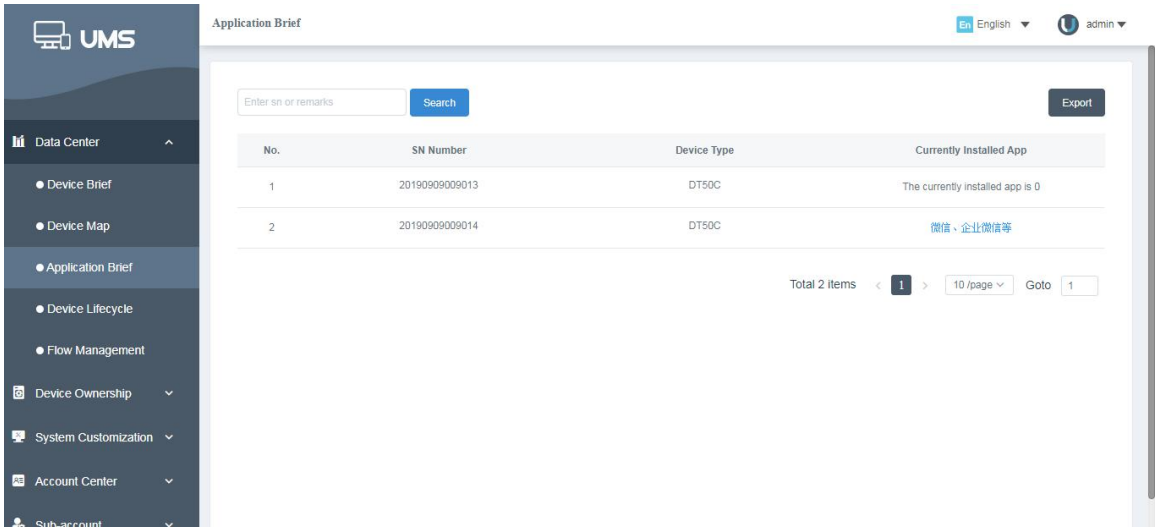


Figure (4.1.3.1)

4.1.4 Device Lifecycle

Click [Data Center]-[Device Lifecycle], to find delivery and activation status of all devices under this

account.

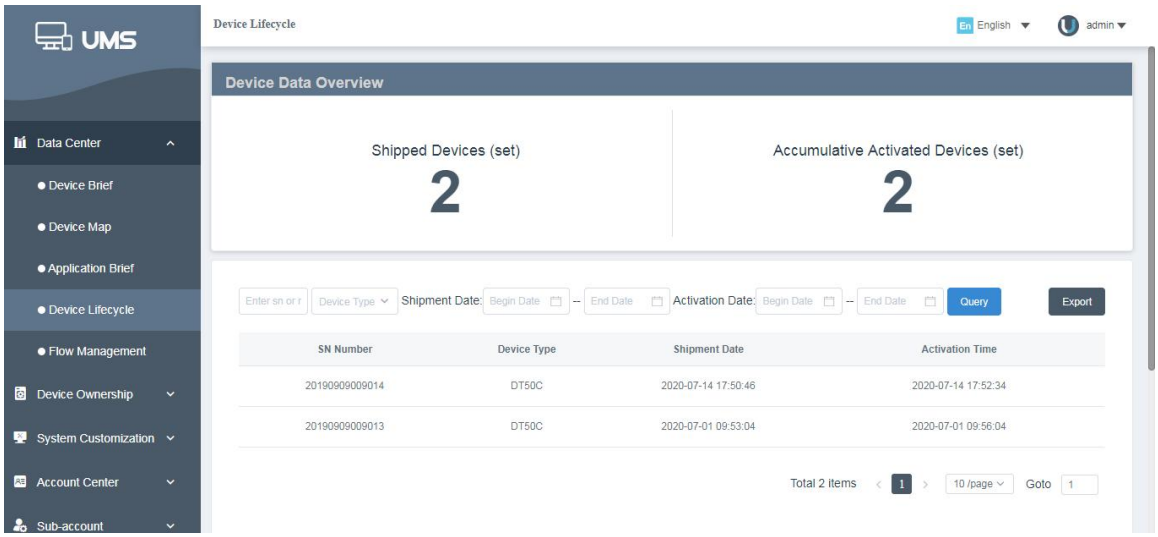


Figure (4.1.4.1)

1. The upper side shows the statistics regarding the device delivered and the ones activated, and the list shows all of the Device's SN, Device Type, time of delivery and activation.
2. On the upper side enter the SN, Device Type, delivery date, activated date, Click [Query] to find relevant device information.

3. Click [Export] to find information of device delivery and activation, and export such information in Excel format and save it to user's computer.

4.1.5 Flow Manager (new function "Limit Reminder")

Click the menu bar [Data Center]-[Flow Management], the data consumption of the devices under the account will be displayed. By default, it displays the total mobile data consumed by the device in the last week (excluding the WIFI traffic consumed by the device). The application ranking can query the traffic consumed by each application under a single device, and the group ranking can query the data traffic consumed by each grouped device by group.

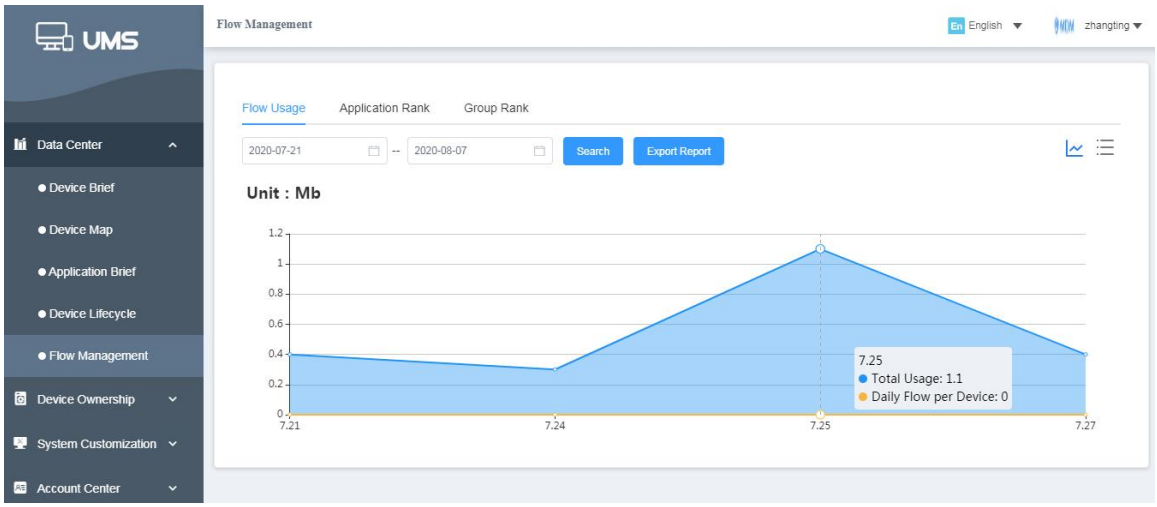


Figure (4.1.5.1)

1. Data usage:

By default, the total mobile data traffic consumed by the device in the last week is displayed. You can change the query date to query, click the icon on the right, you can switch to list style, and click icon to switch to line graph style. Click [Export Report] to export the query results to a table.

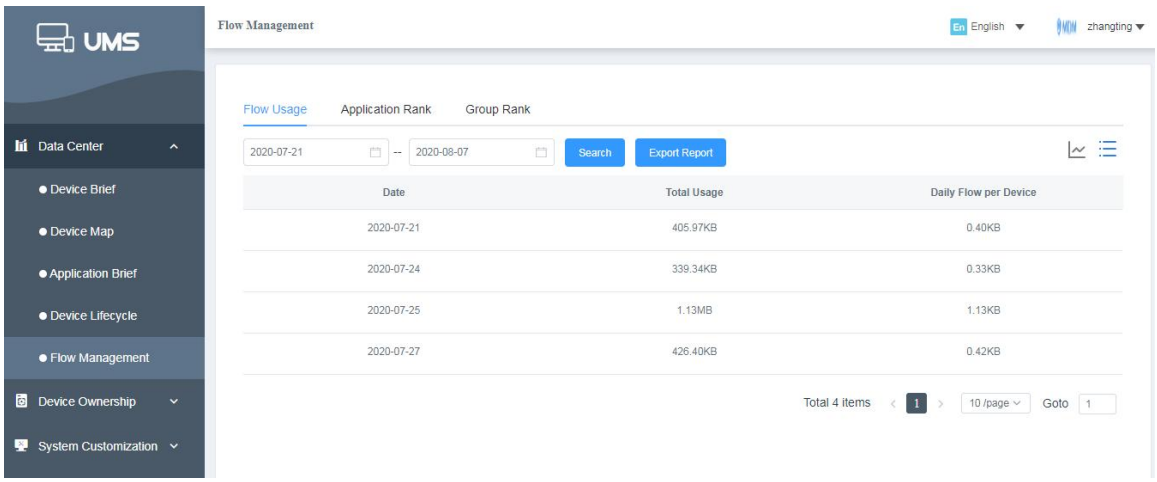


Figure (4.1.5.2)

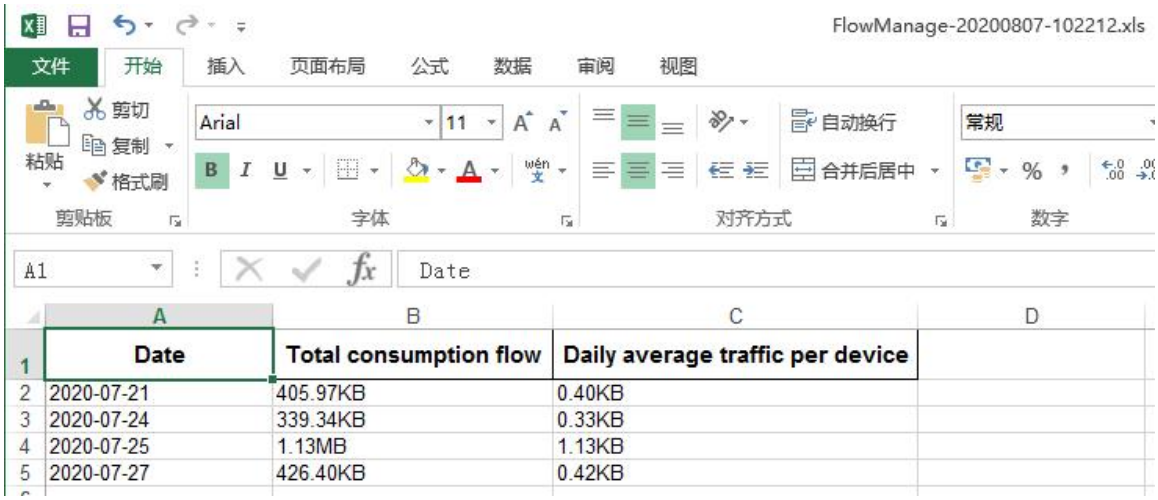


Figure (4.1.5.3)

Notes:

(1) Total consumption flow: the mobile data traffic consumed by all devices during the query time;

(2) Daily flow per device: total consumption flow/(number of devices * number of query days).

2. Application Rank:

Displays the application traffic consumption of a single device. The default query date is today, and the query date can be changed. Enter the SN number, click [Query], the total traffic consumed by the device during this period and the average daily traffic consumption are displayed in the middle. The list below shows the data consumption of the applications of the device, sorted by the highest to the lowest, and only shows the

data consumption of the top 20 applications. Click [Export Report] to export the query result as a table.

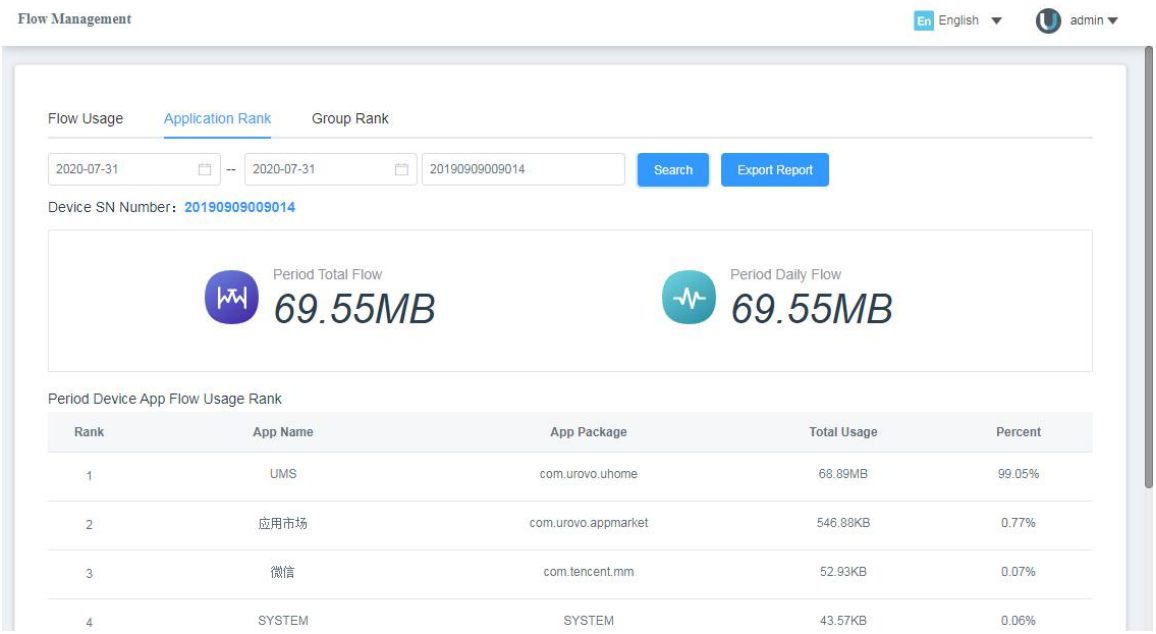


Figure (4.1.5.4)

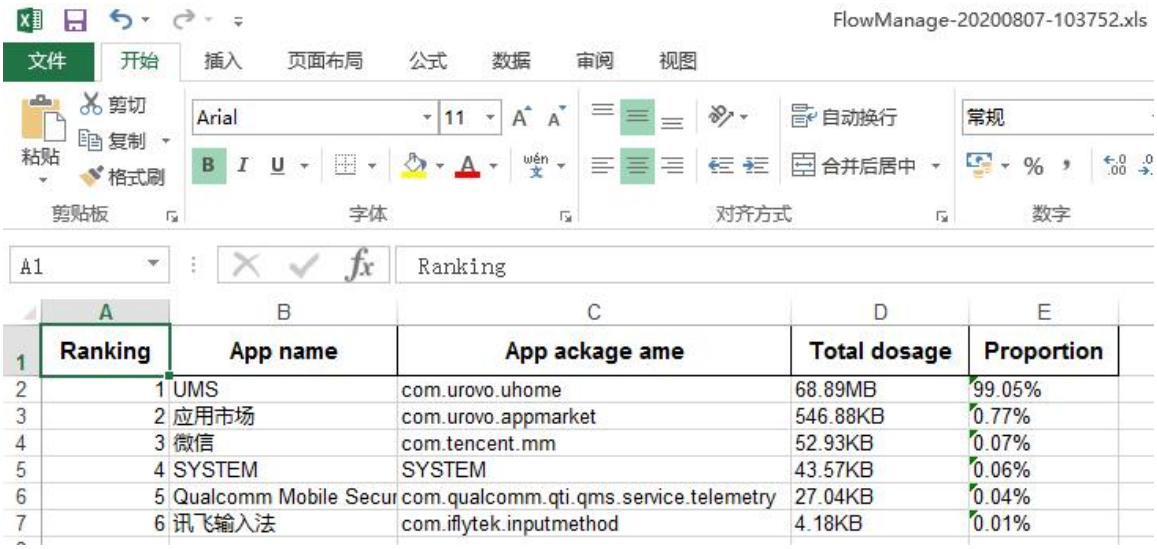


Figure (4.1.5.5)

Notes:

(1) Total traffic during the period: the total mobile data traffic consumed by the query device during the query time;

(2) Average daily flow during the period: total flow during the period/number of query days.

3. Group Rank

Displays the data consumption of devices in multiple groups. The default query date is today, and the query date can be changed. Select multiple groups, click [Query], the average daily traffic consumed by the selected group during this period of time and the average daily traffic consumed by each device are displayed in the middle. The list below shows the traffic consumption of each group of the device, sorted by traffic from high to low. Click [Export Report] to export the query result as a table.

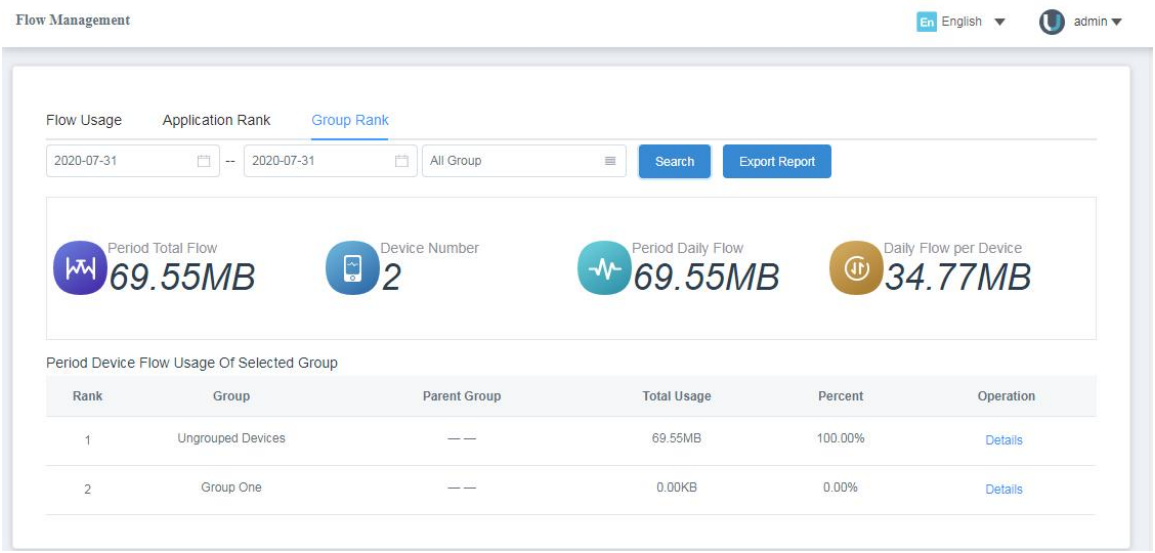


Figure (4.1.5.6)

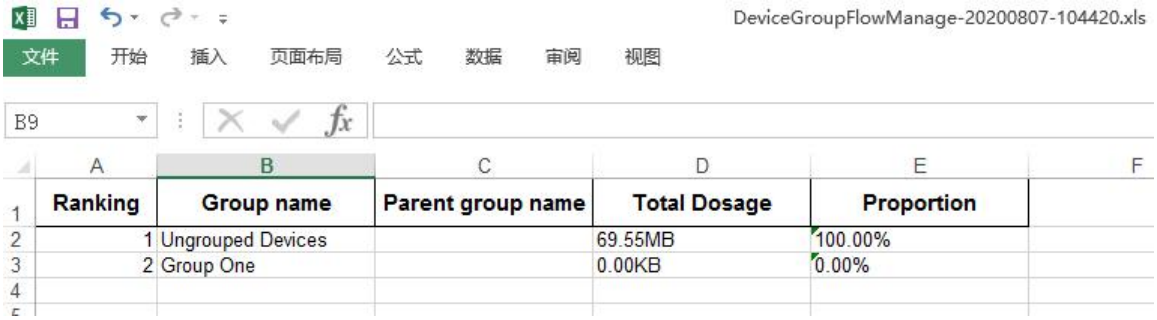


Figure (4.1.5.7)

Notes:

(1) Total traffic during the period: query the total mobile traffic consumed by all devices under the group;

(2) Number of devices: query the number of all devices in the group;

(3) Average daily flow during the period: total flow during the period/number of query days;

(4) Average daily flow of each device: total flow during the period/(number of days to query * number of devices).

Click [Details] in the operation bar in the list to query the traffic consumption of all devices under the selected group, including: total traffic during the query period, number of devices, average daily traffic during the period, and daily average traffic per device. Click [Export Report] to export the query result into a table.

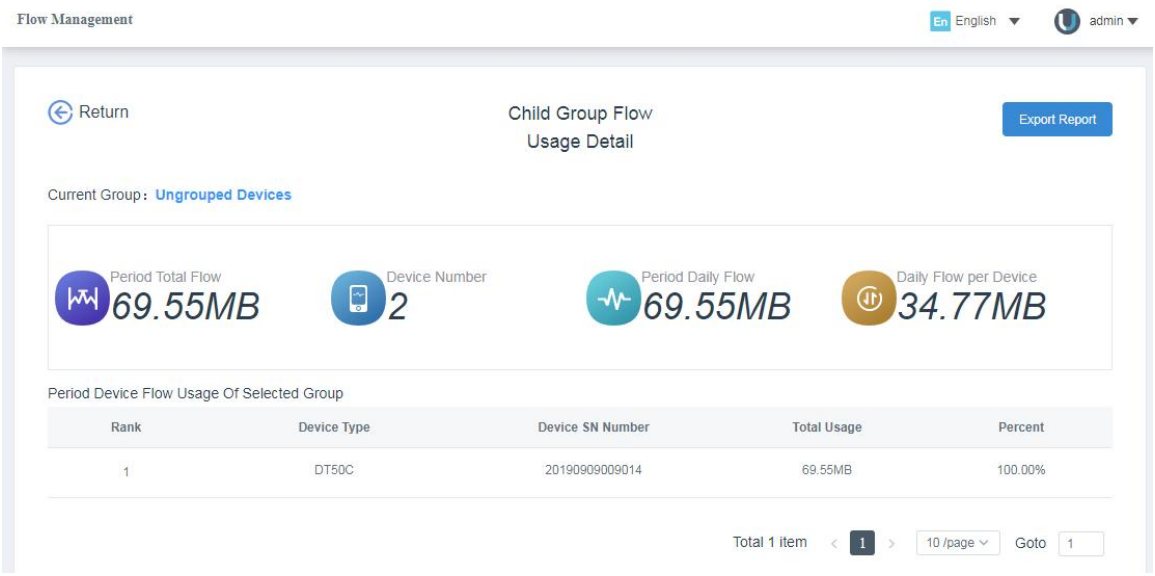


Figure (4.1.5.8)

Figure (4.1.5.9)

4. Limit Reminder

Remind customers of flow usage. When the consumption flow of the day exceeds the limit value, remind the user to avoid flow loss:

1. Click [Limit Reminder] to display a popup window.

2. Enter the limit of the day, which can be customized in an integer ranging from 1 to 9999; Compare the amount of traffic data uploaded in a polling mode and the limited amount. If the amount of traffic exceeds the limited amount, it will be recorded on the page to record the time and

consumption value;

3. Select the time to send the daily report. By default, no email is sent. You can send the daily report, send the warning email at 17:00 Beijing time, collect the data of yesterday and send the report

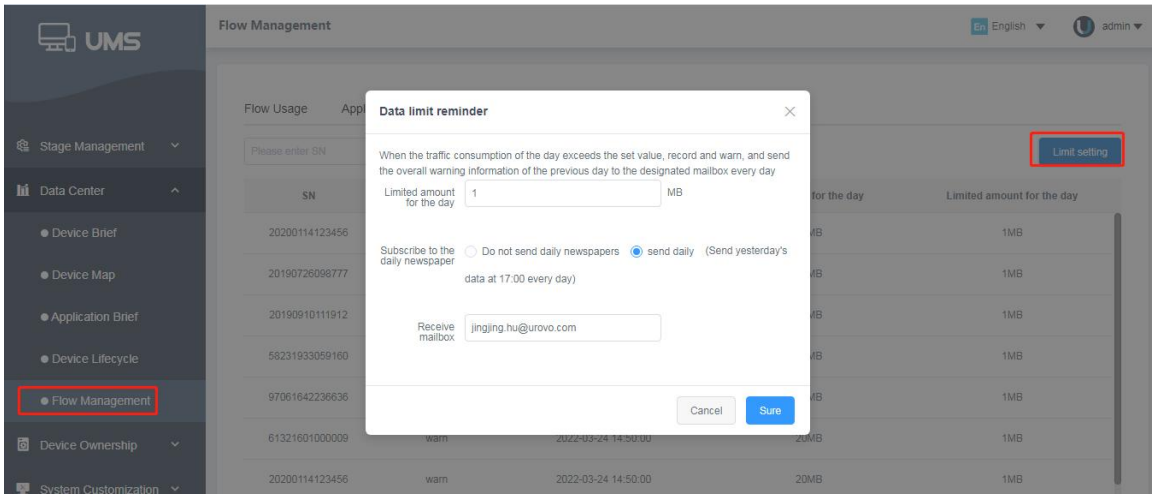


Figure (4.1.5.10)

Notes:

When the limit is exceeded, the flow usage of the device on the current day is recorded on the page for multiple polling and data coverage. (only one record is displayed on the same device on the same day).

4.2 Group Management

Group management page have all group information of customer, after setting group management and APP ,only have one group of unclassified in system, it can make to add ,delete, and arrange group, also can batch import system to group, associate and mobile device with others.

4.2.1 Group Management

Click menu group management, entering this page , only showing up one unclassified group device, all device belonging to this group, as the Figure shows :

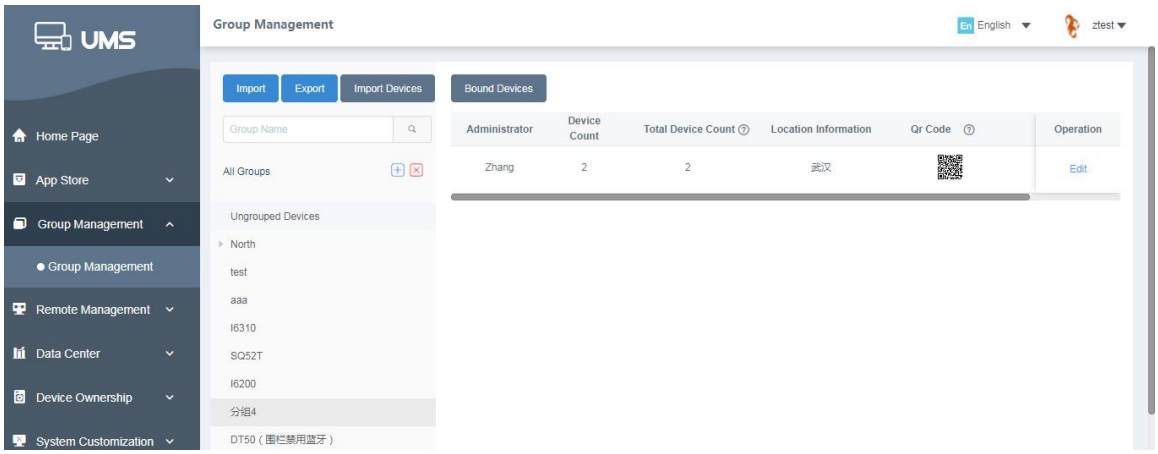


Figure (4.2.1.1)

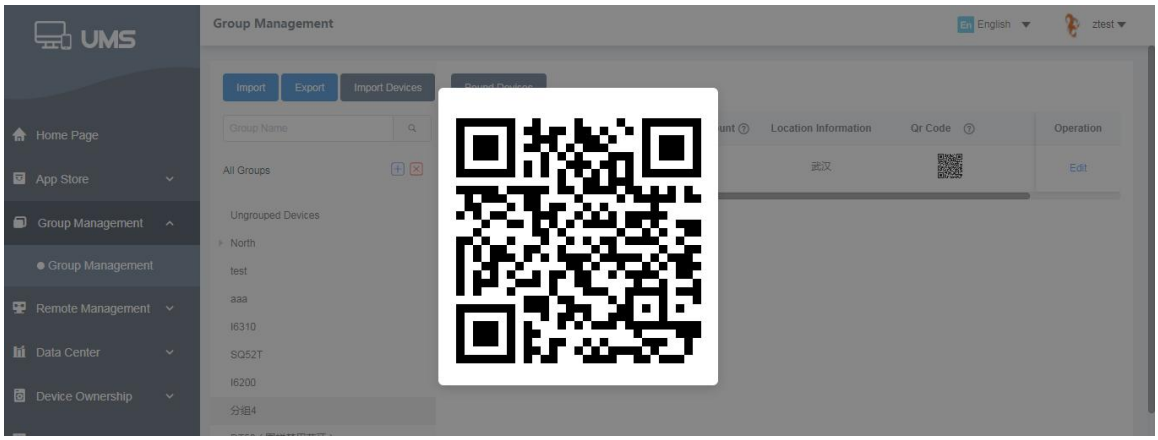


Figure (4.2.1.2)

Notes：

1. Device count：Device quantity under this group.
2. Total device count：Total device included this group and subgroup.
3. Group QC code: Click the QR Code to view its large image. Use a terminal to scan this QC code to move the device under current account to this respective group.

4.2.1.1 Add Group

It has two modes, one is adding manually, another is batch adding group.

(1) On the page of group management clicking the right adding button of all group, will have a windows of adding group (Figure 4.2.1.1.1),enter group name, location, manager name ,contact way ,and back up information, then click confirm button, will add a new group finally.

(2) If you want to setting batching group, click batching button, will show up a Figure like 4.2.1.1.2 , first click download excel ,then open the excel which you download, then adding group name ,rage of group,(if they are one group do not do this), manager, contact way, location, and backup information like 4.2.1.1.3, save template, put it adding batching group, if you tag the button of deleting all group, after batching group, it will delete all group.

(3) After adding or batching group, pop-up window will close, on the left page of group management will show up adding group

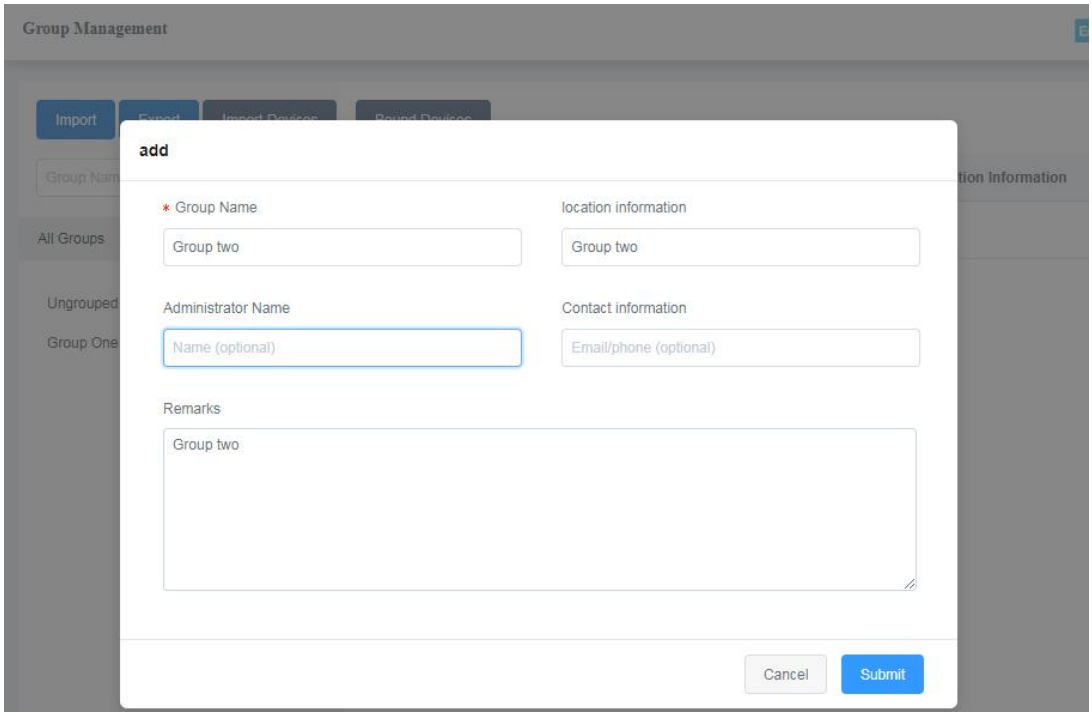


Figure (4.2.1.1.1)

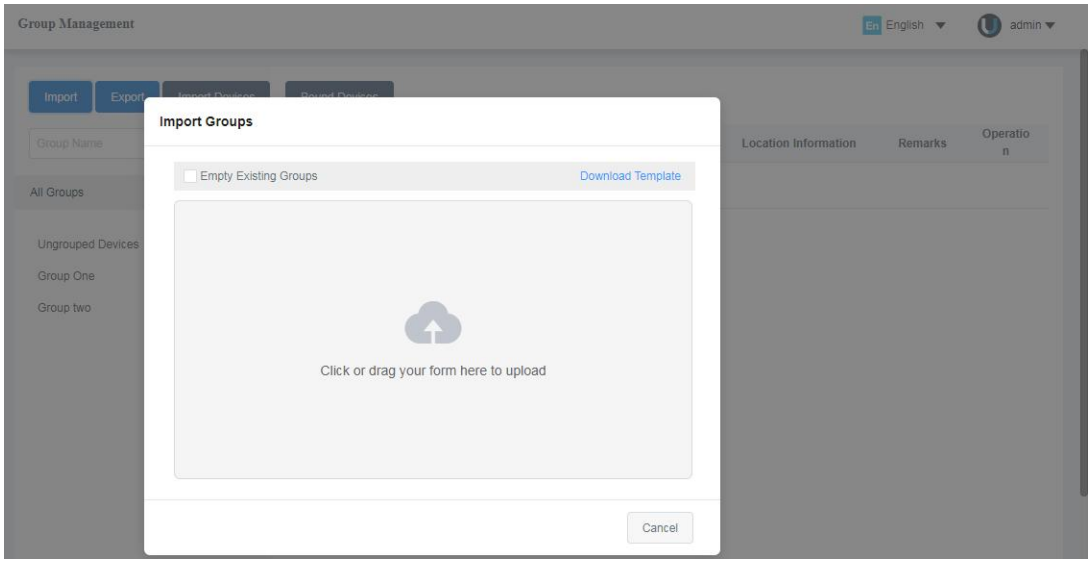
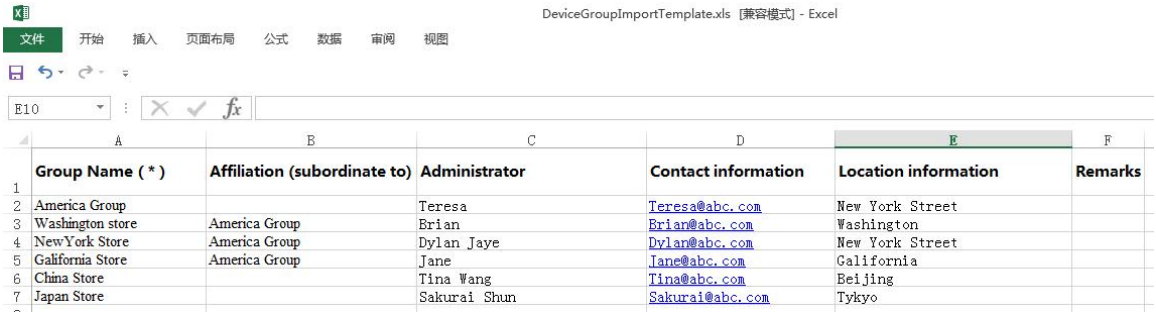


Figure (4.2.1.1.2)



	A	B	C	D	E	F
1	**Group Name (*)**	**Affiliation (subordinate to)**	**Administrator**	**Contact information**	**Location information**	**Remarks**
2	America Group		Teresa	Teresa@abc.com	New York Street	
3	Washington store	America Group	Brian	Brian@abc.com	Washington	
4	NewYork Store	America Group	Dylan Jaye	Dylan@abc.com	New York Street	
5	Galifornia Store	America Group	Jane	Jane@abc.com	Galifornia	
6	China Store		Tina Wang	Tina@abc.com	Beijing	
7	Japan Store		Sakurai Shun	Sakurai@abc.com	Tykyo	

Figure (4.2.1.1.3)

Notes：

- the name of group (must be write ,up to 30 characters)
- location information (optional, up to 100 characters)
- manager name (optional ,up to 30 characters)
- contact way (optional, up to 100 characters)
- remarks (optional ,up to 100 characters)

4.2.1.2 Edit Group

Edit group, it can revise the group name, location, and manager name, contact way.

On the page of this group management, making optional group, on the list will show up this group information, like figure 4.2.1.2.1, click the button of edit, on this windows icon to revise the name of group, and location, manager name, and contact way ,click [Submit] button, it have done to revise group management information, such as Figure 4.2.1.2.2

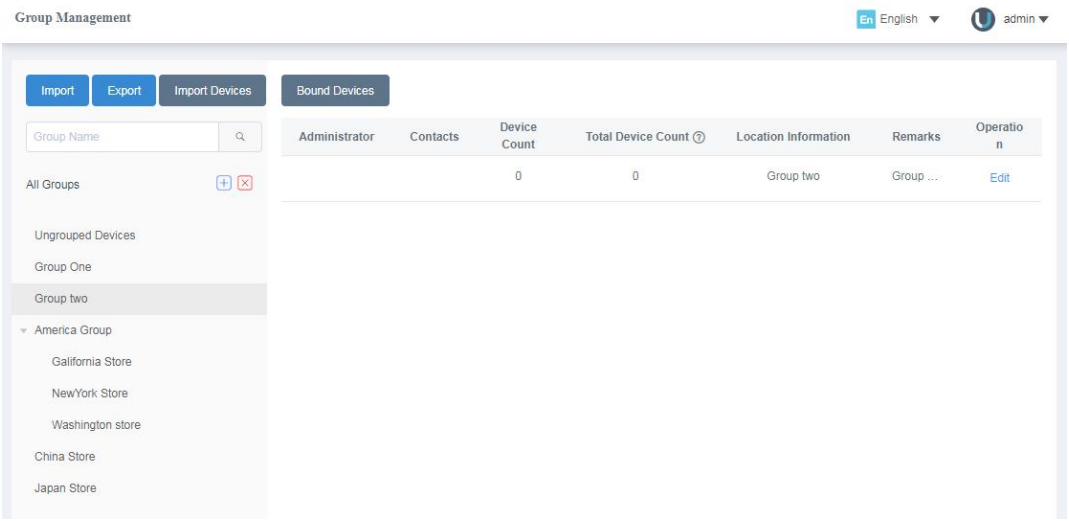


Figure (4.2.1.2.1)

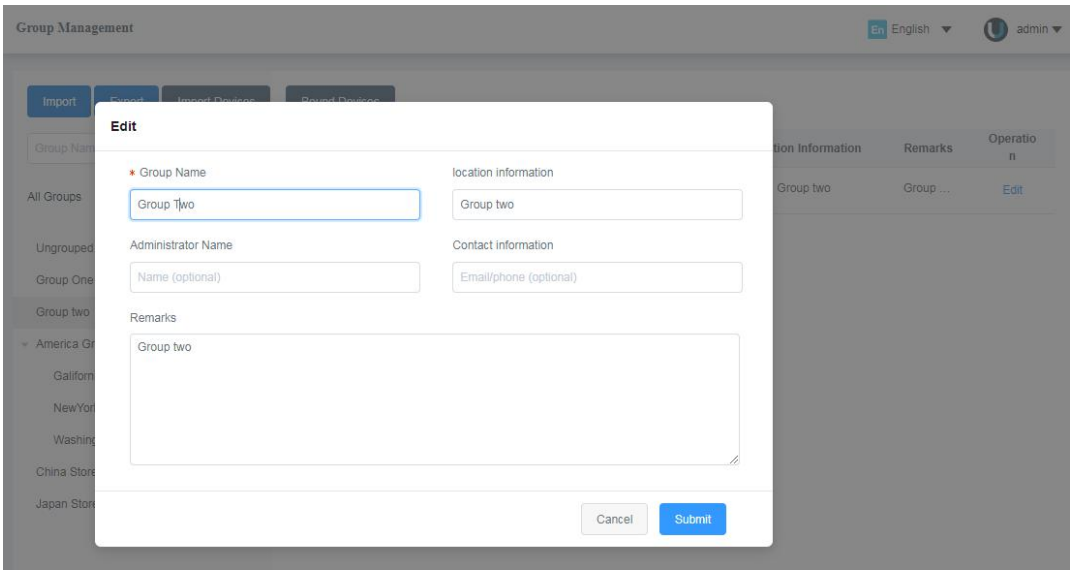


Figure (4.2.1.2.2)

4.2.1.3 Delete Group

Delete group will delete the group which do not have Subgroup, if this group have the device, this device will move to the group "ungrouped". On the page of group management, choose the certain group, click the button of left-side group list of all, choose the right button of this logo , it will show up the Note of “whether delete” (Figure 4.2.1.3.1), click the button of [Submit] will delete this group; otherwise, if click the button of [Cancel] will do not delete group. If it has Subordinate grouping, it will warn you “Subgroup under this group” (Figure 4.2.1.3.2), and it will not be deleted.

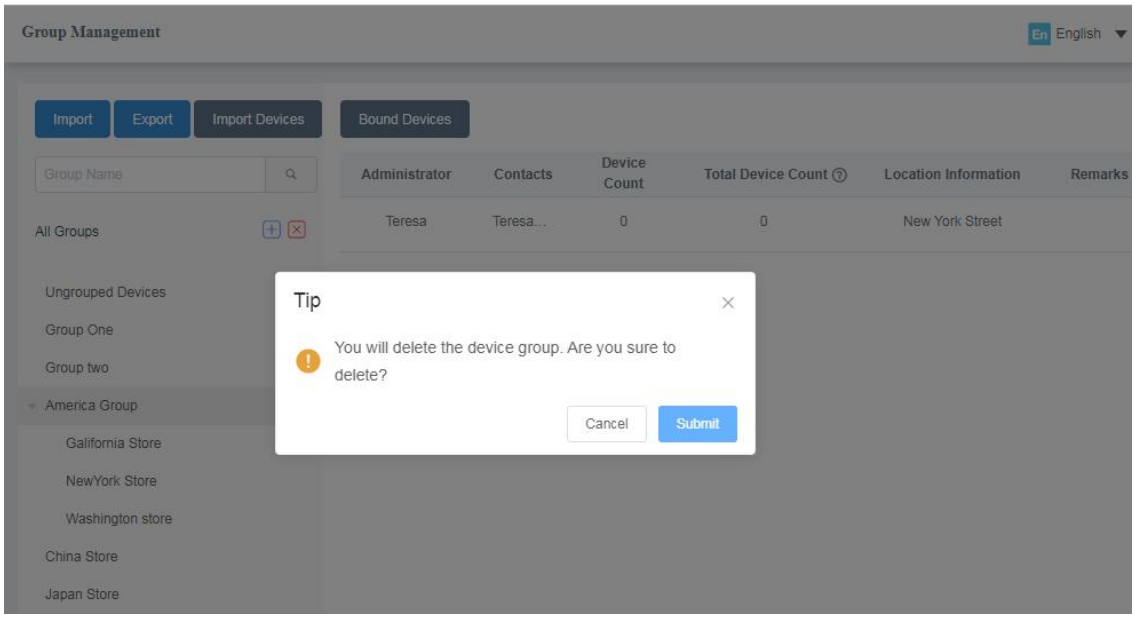


Figure (4.2.1.3.1)

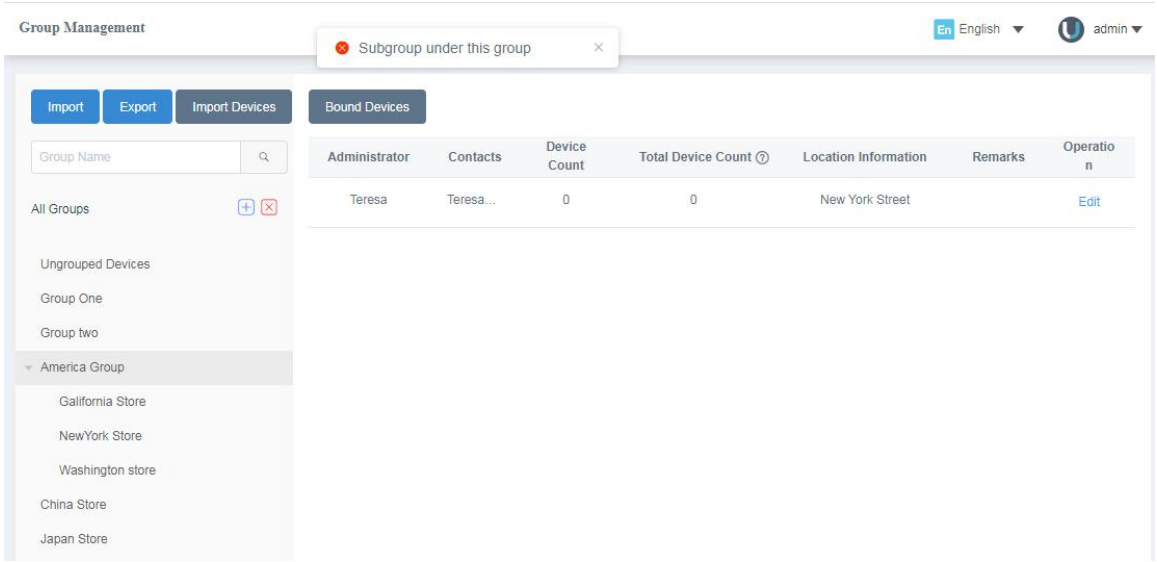


Figure (4.2.1.3.2)

4.2.1.4 Export Group

Export group can export as an Excel File of all group in this account, to check the information conveniently. Click the button of [Export], it will download the Excel automatically, open this Excel will look through the group information.

4.2.1.5 Import Device

Input device function can put the device of “ungroup” batch binding with other group. Remark information will show in the page of remote management.

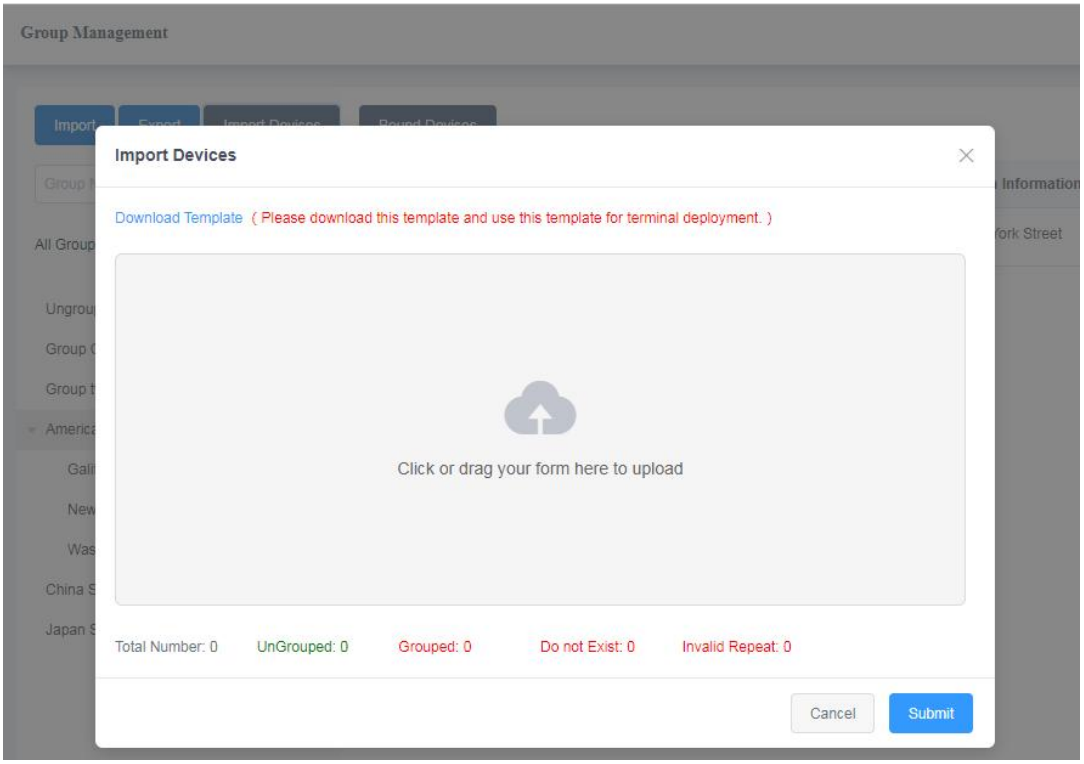


Figure (4.2.1.5.1)

Figure (4.2.1.5.2)

(1) Click [Import], it will show up this import devices interface, click then download Excel template, in this template input SN number and the name of group (Figure 4.2.1.5.2), conserve template.

(2) Click the interface of gray zone (Figure 4.2.1.5.1), after choosing template, it will show up the situation of all input devices, click confirmed it will batched binding successfully. Only have the “ungrouped” device, which can batch binding with other group.

Tips:

A. Ungrouped group: In this account the device of "ungroup", which can batch binding with others.

B. Grouped group: it mean that this account has connected with other group devices, which can not binding with other group.

C. Not existing account: the device which is not existing.

D. Invalid repetition: in this template the device which has been existed.

4.2.1.6 Bound Devices

Bound devices can binding one device or various “ungroup” devices into another group.

(1) On the page of group management (Figure 4.2.1.1) pick up one group, click [Bound Devices] will show up an icon, on the right of it input SN number, click [Add] it will show up the adding device situation downside, the situation will same as the import devices.

(2) Click [Submit] it can batch binding to a certain group successfully, only can “ungroup” device binding successfully.

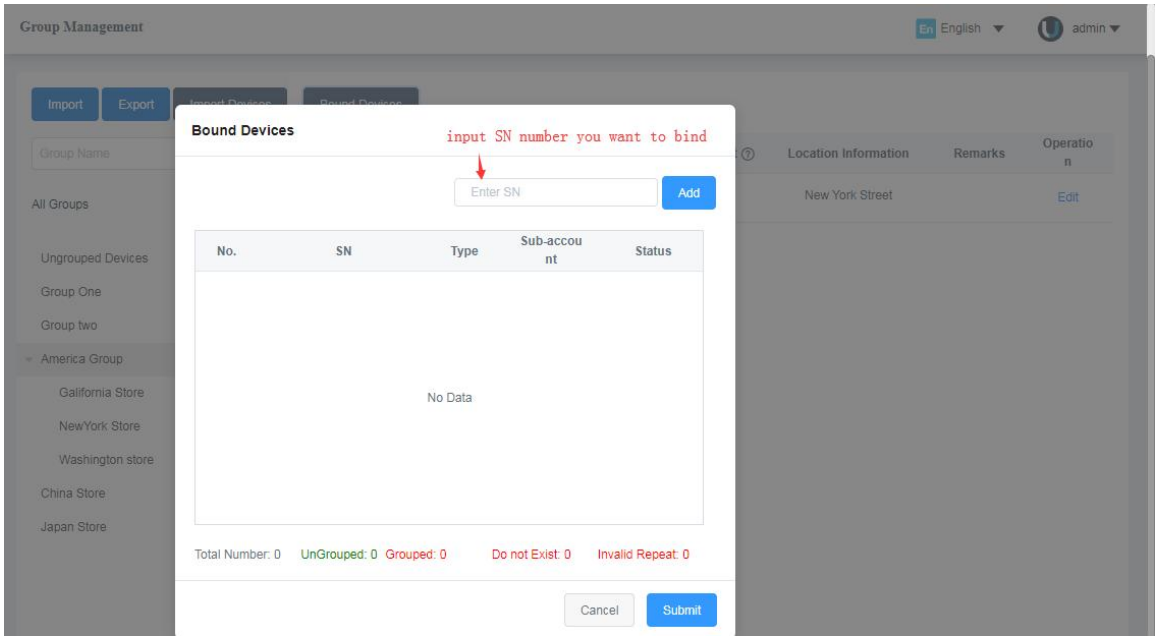


Figure (4.2.1.6.1)

4.3 App Store

The main function of application market uploading, launch application channels

device checking, download, install; upload “Banner” Figure which use for advertising.

4.3.1 App Upload（Upload Multiple Versions）

4.3.1.1 Add Apps

In the Figure (4.3), click [App Store]- [App Upload] on the menu bar to access the interface, as shown the Figure below：

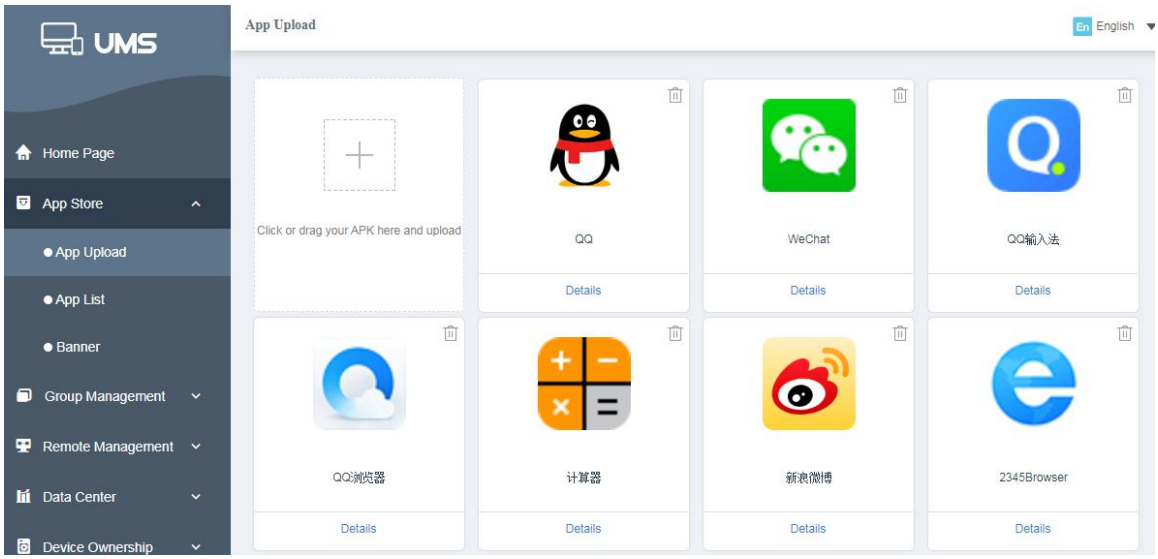


Figure (4.3.1.1.1)

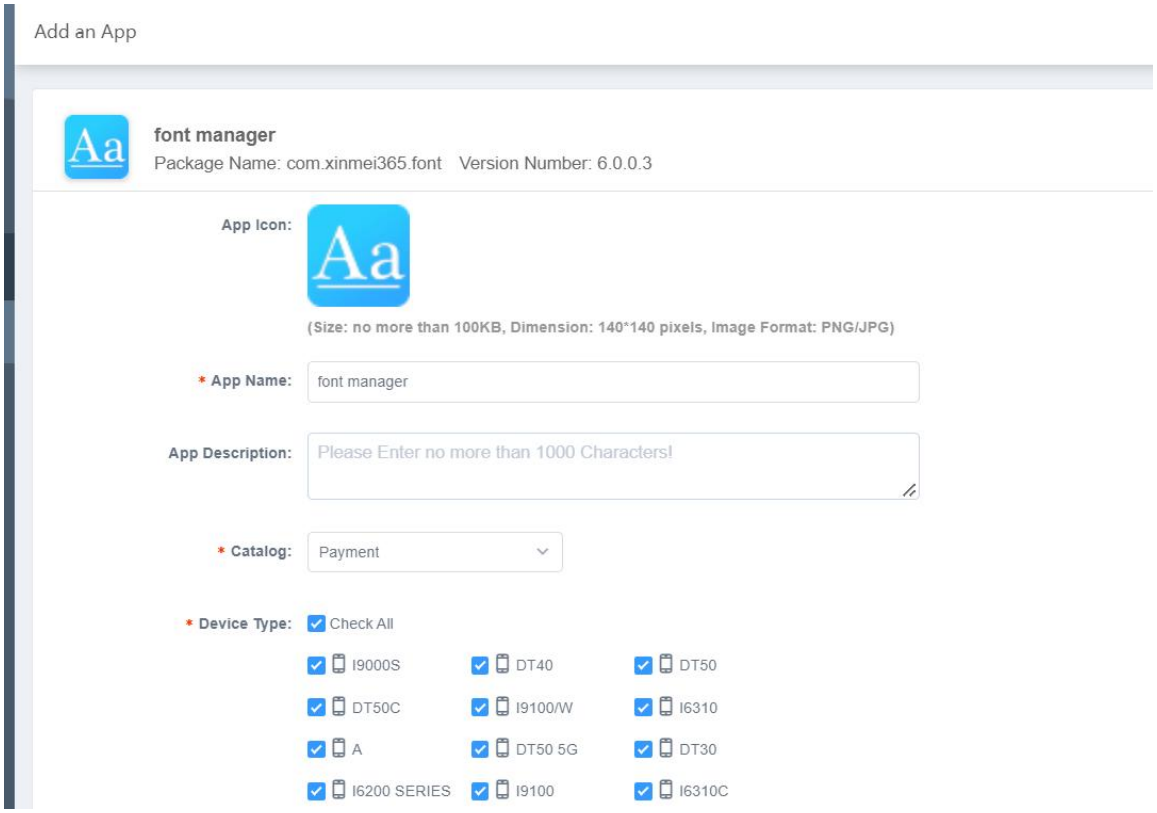


Figure (4.3.1.1.2)

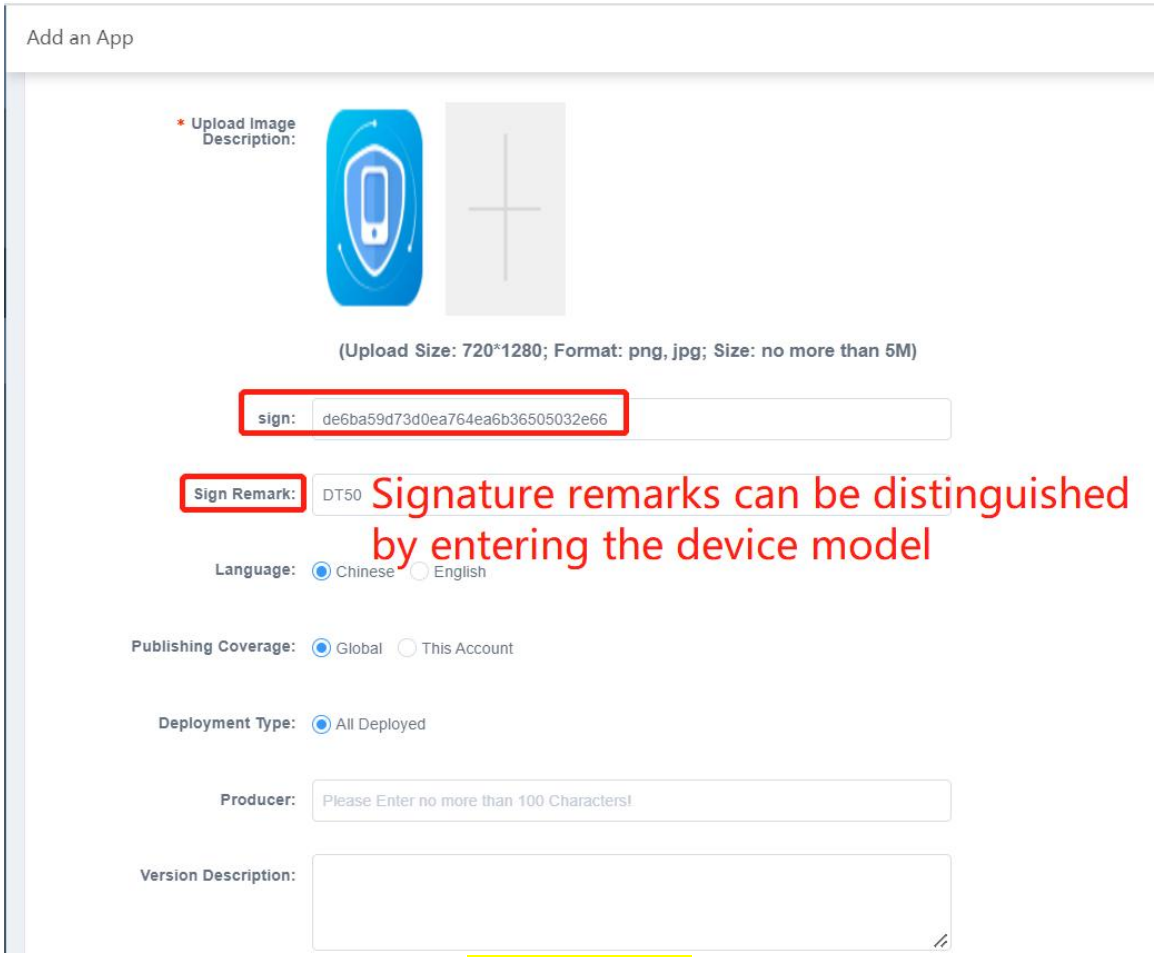


Figure (4.3.1.1.3)

1. Click the [Upload] button, select or drag the APK that needs to be upload in designated area, followed by entering application information and click [save], then the new application is added.

2. App Name: Required fields. They can be analyzed automatically or modified manually.

3. App Profile: Optional fields. User can look for profile after terminal detects the application is detected by terminals.

4. Classification of industry: Required fields. Terminal's users can look for applications by industry.

5. Device Types: Required fields. Such applicated can only be detected for the device of certain selected type.

6. Description of Figure: Required fields. The description for the design works of

uploaded apps can be seen after such app is detected by terminal.

7. Signature: Optional fields. It can be automatically parsed, and also can be manually modified;

8. Signature Remarks: Optional fields. After entered, users can view the signature version based on the remarks.

9. Release Channel: Required fields. If Omni-channel is selected, all of the agents and sub-accounts are able to display the app after it is reviewed; if this channel is selected, only the agents and sub-accounts under current channel can display apps.

10. Launch Mode: Required fields. Full launch means the application list under this account shows agents and sub-accounts of this channel. Gated Launch means the device that only adds SN can detect the apps, which is not shown in application list and usually used for limited-scale test.

11. Notes on manufacturer and version: Optional field. Users can find application details when app is detected.

12. P.S. Optional Fields. Urovo can internally conduct review based on notes when the app is submitted for review.

4.3.1.2 App Edit

Click [Detail]- [App Detail] in the page of application upload to edit the filled-in of basic application information, including application name and brief, industry classification, and device types.

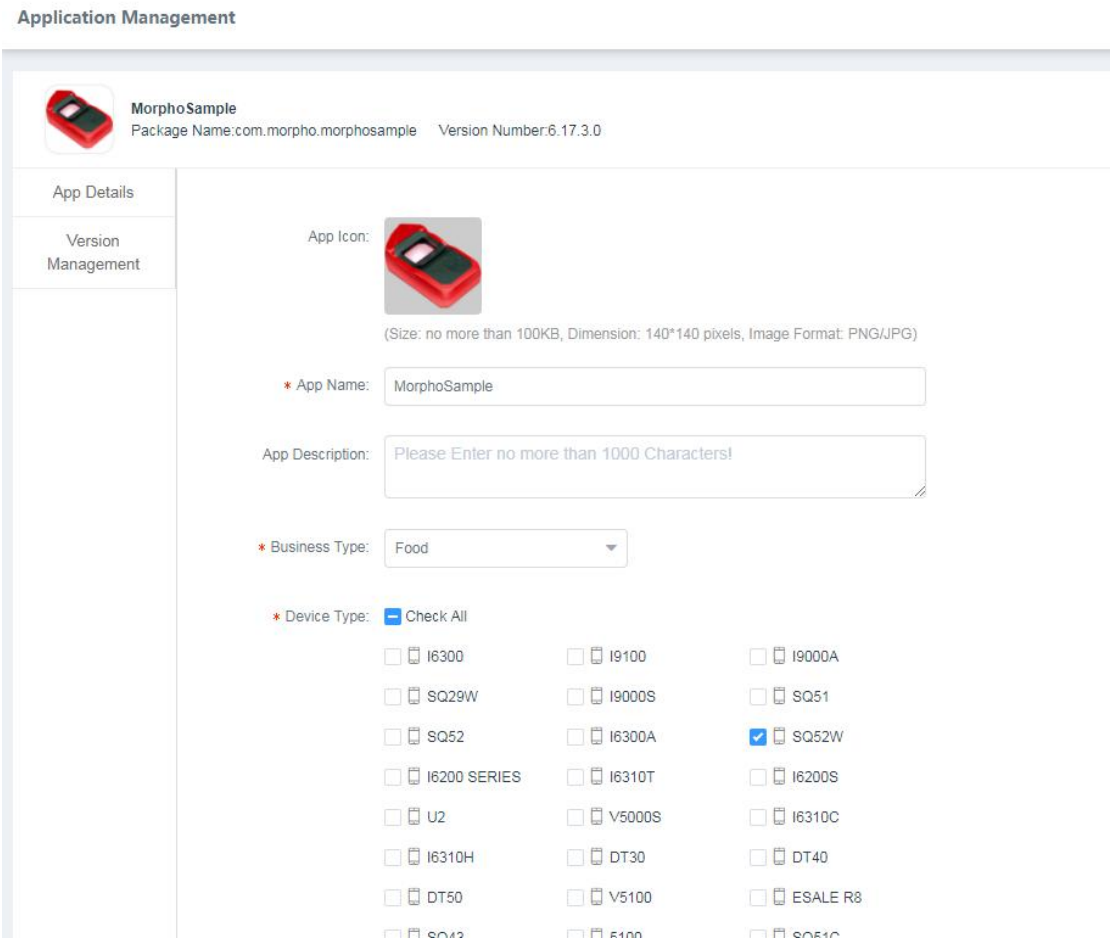


Figure (4.3.1.2.1)

Attention：

(1) Under gated launch, apps cannot be released in Omni-launch, but only in local channel.

(2) If the app is released under Omni-channel and approved, it cannot be switched to local channel;

4.3.1.3 App Upgrade

Click the [Detail]-[Version management]in the application upload page date to find uploaded version information, click [Upgrade] button to upload new version for update.

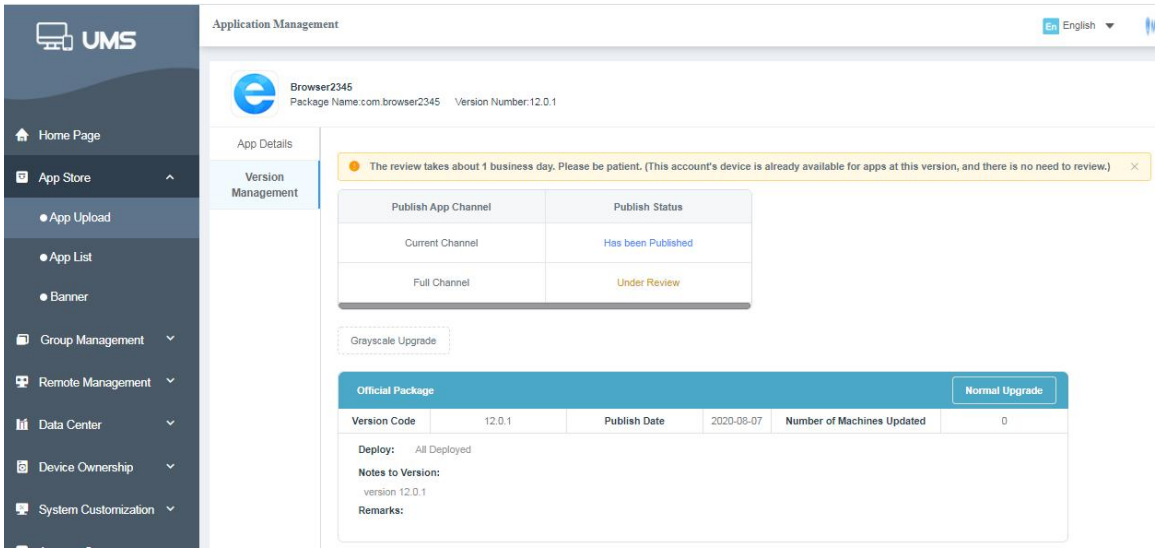


Figure (4.3.1.3.1)

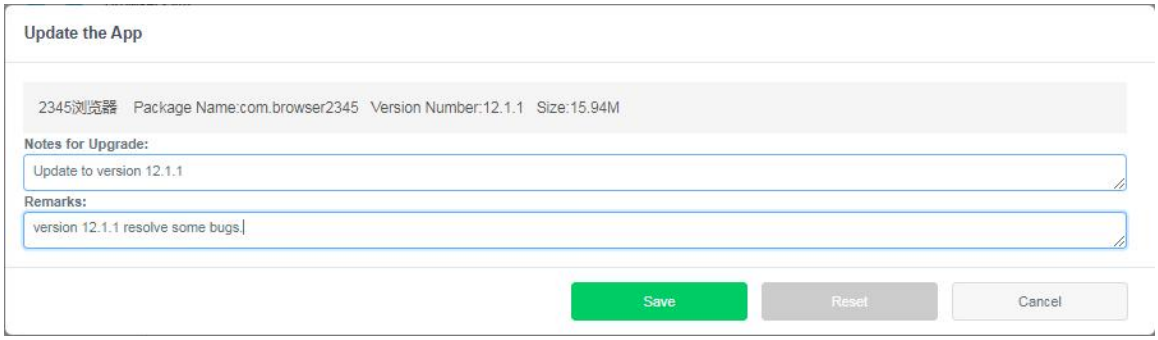


Figure (4.3.1.3.2)

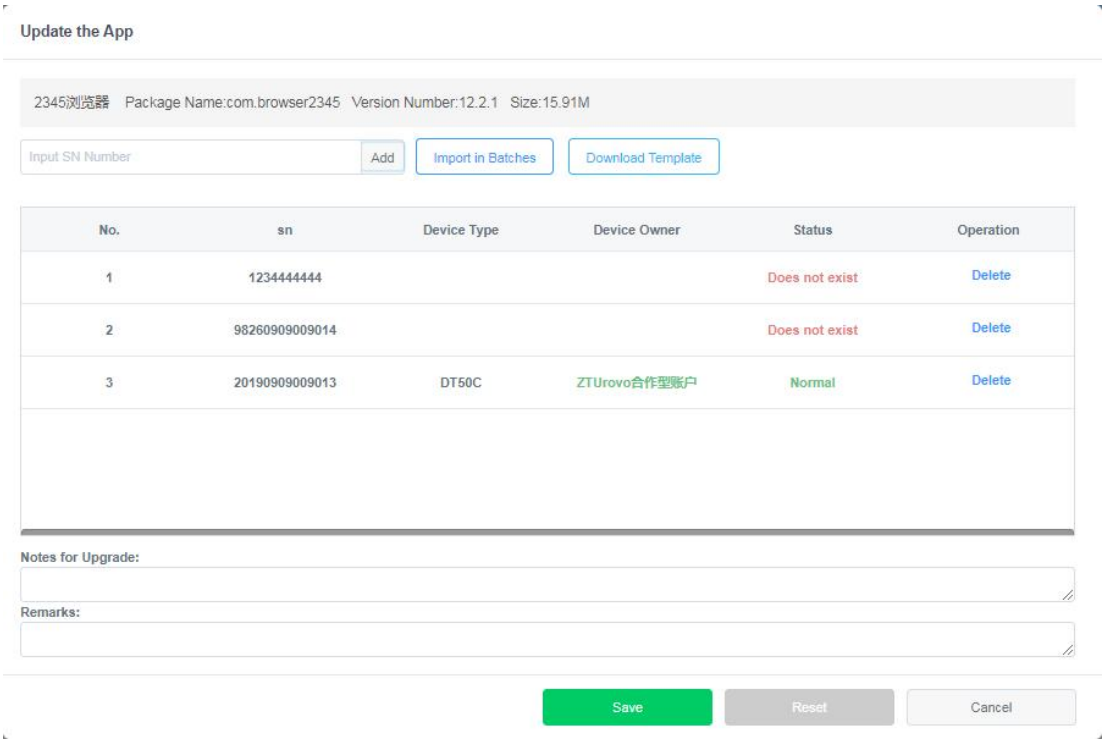


Figure (4.3.1.3.3)

1. If the old version are official version(meaning launch mode is full launch), there are two ways to upgrade：normal upgrade, gray scale upgrade.

(1) Normal upgrade: Click [Normal Upgrade], upload new version of APK, enter upgrade description and notes, then save it. So update is completed. After the update, the new version is official version as well (full launch). The application which detects the old version originally can spot the new version.

(2) Gray scale upgrade: Click [Gray upgrade] to upload the new version of APK, then set up the range of gated launch (specific SN), after adding the SN, enter upgrade description and notes, then save it to update is completed. After the update, the new version is grayscale version (gated launch). Only the devices that add to the gray SN list can spot the new version, and such function is used within small range.

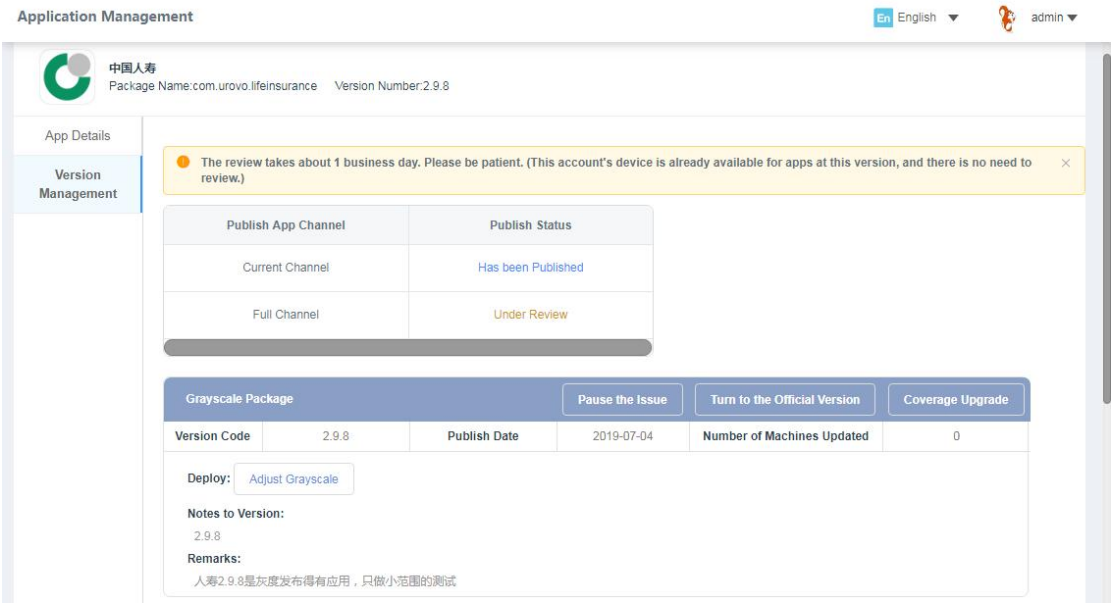


Figure (4.3.1.3.4)

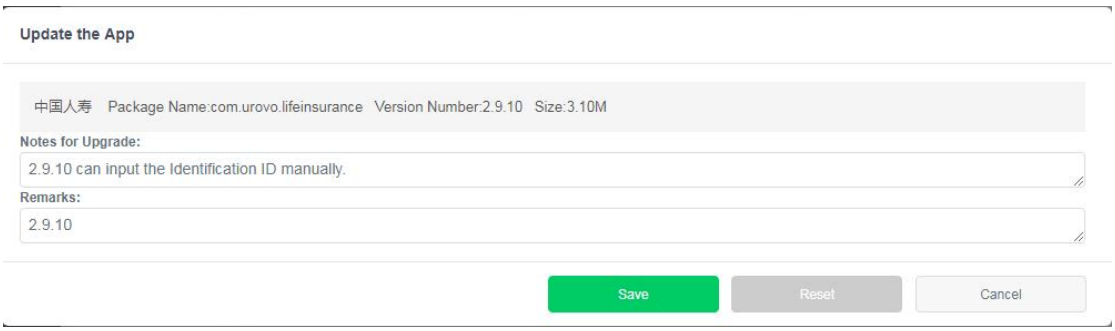


Figure (4.3.1.3.5)

2. If the old version is grayscale version (meaning launch mode is gated launch), there is

only one way to upgrade: overwritten upgrade；

overwritten upgrade: Click [Grayscale Upgrade], upload new version APK, enter upgrade description and notes, save it then updating is completed. After updating, the new version is grayscale version (gated launch), the grayscale coverage is the SN added by the old grayscale version. If there is need to edit the range of SN, click the [Adjust the grayscale range] from grayscale package below to see or edit the range of grayscale；

4.3.1.4 Suspension of application issuance

When the latest version of application is grayscale version, the issuance of such app can be suspended. After suspension, the device cannot detect this grayscale version.

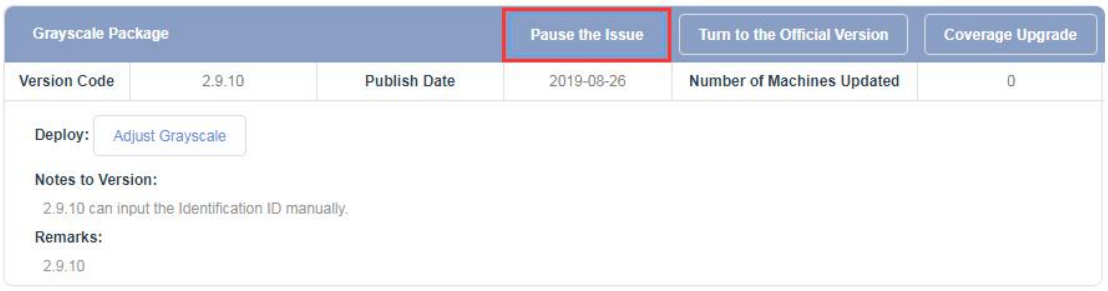


Figure (4.3.1.4.1)

Figure (4.3.1.4.2)

1. Click [Pause the Issue] in the right side of grayscale package, SN cannot detect this grayscale version within grayscale. With lower version for normal launch, the device will detect the lower version after issuance is suspended. With lower version for normal launch, the device cannot detect this application after issuance is suspended；

2. For the version suspended, Click [Restore the Issuance] can resume issuance of grayscale version, after resumption, the device within grayscale can detect this grayscale version；

3. [Turn to the Official Version]: that is, turn to the official release package, which can only be viewed in the application market after it is put on the application list (the original official package has been

put on the application list by default). If silent installation is required, application deployment is required to push the application

4. [Coverage Upgrade]: Update grayscale application

5. [Adjust Grayscale]: Device that can adjust the grayscale deployment again

Notes:

1. The version for grayscale release requires the device to manually download from the application market, and will not be automatically installed;

2. The grayscale version does not support application deployment push. Only the official version supports it

3. Do not add more than 10 devices in a grayscale release;

4.3.1.5 Upload Multiple Versions (new function)

Click "Normal Upgrade", and select "Coverage Upgrade" or "Upload Multiple Versions" in the displayed window;

1. "Coverage Upgrade": Only the higher versions with the same package name and signature can be uploaded; Each version of the coverage upgrade is included in the version list (historical version). The historical version can be "edited", "deleted", "downloaded" in the list;

2. "Upload Multiple Versions": Multiple versions can be uploaded. If the package name is the same, upload is allowed; After parsing the version number and signature, if one item is inconsistent with the one in the database, you can upload APK and enter the required remarks in the popover. The application can be "edited", "deleted" and "downloaded" in the multiple versions column list;

Notes:

1. If the application package name, signature, and version number are the same, the application cannot be uploaded;

2. If the application package name is consistent but the signature is inconsistent, the application can be uploaded. For example, the same application, if signed in different systems with different names, can be uploaded;

3. If the application package name is inconsistent, the application cannot be uploaded;

4. If you upload multiple versions, you need to upload the correct signature, so that the terminal can recognize it for normal installation. If the signature is scrawled, the application cannot be downloaded and installed successfully;

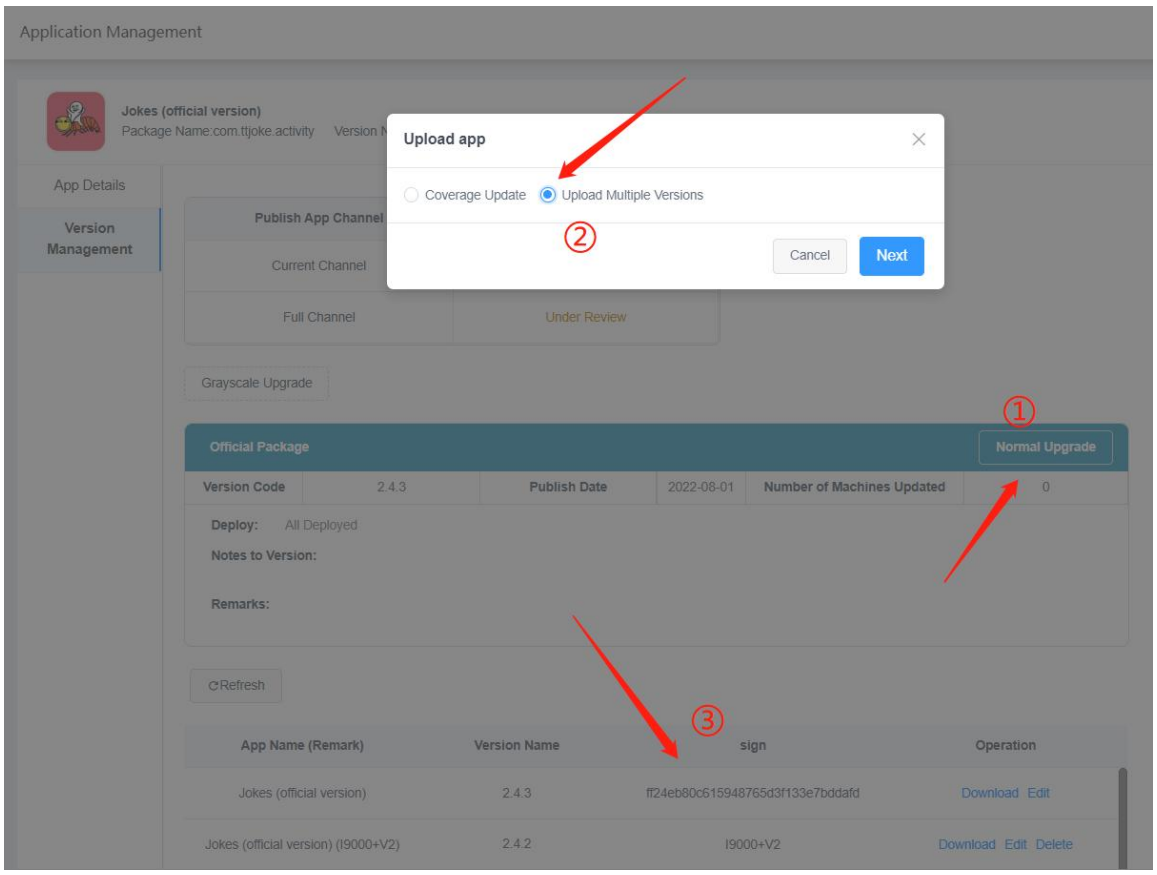


Figure (4.3.1.5.1)

1. Click Details in App Upload

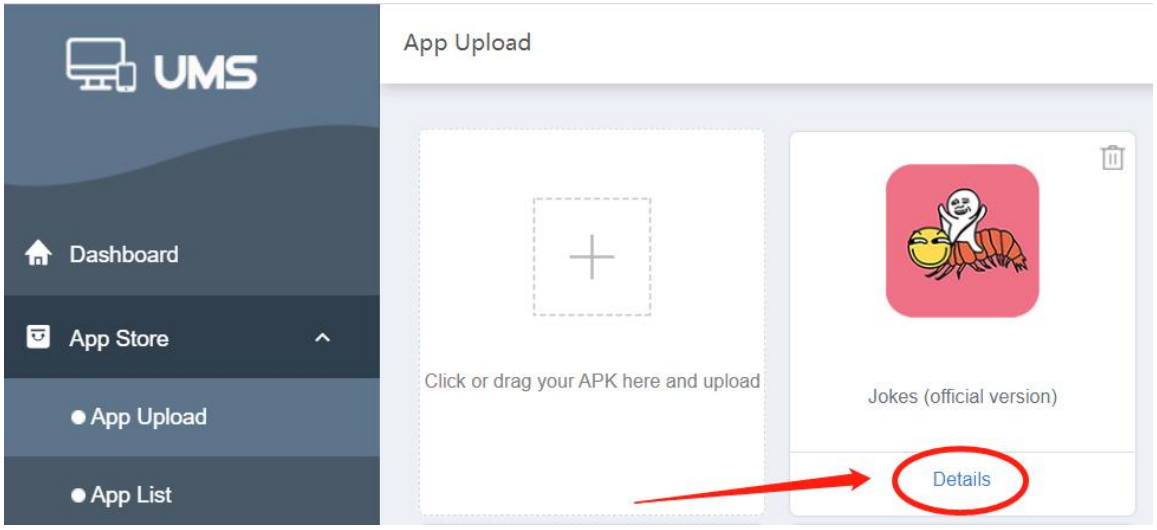


Figure (4.3.1.5.2)

1. Enter App Details and select Version Management

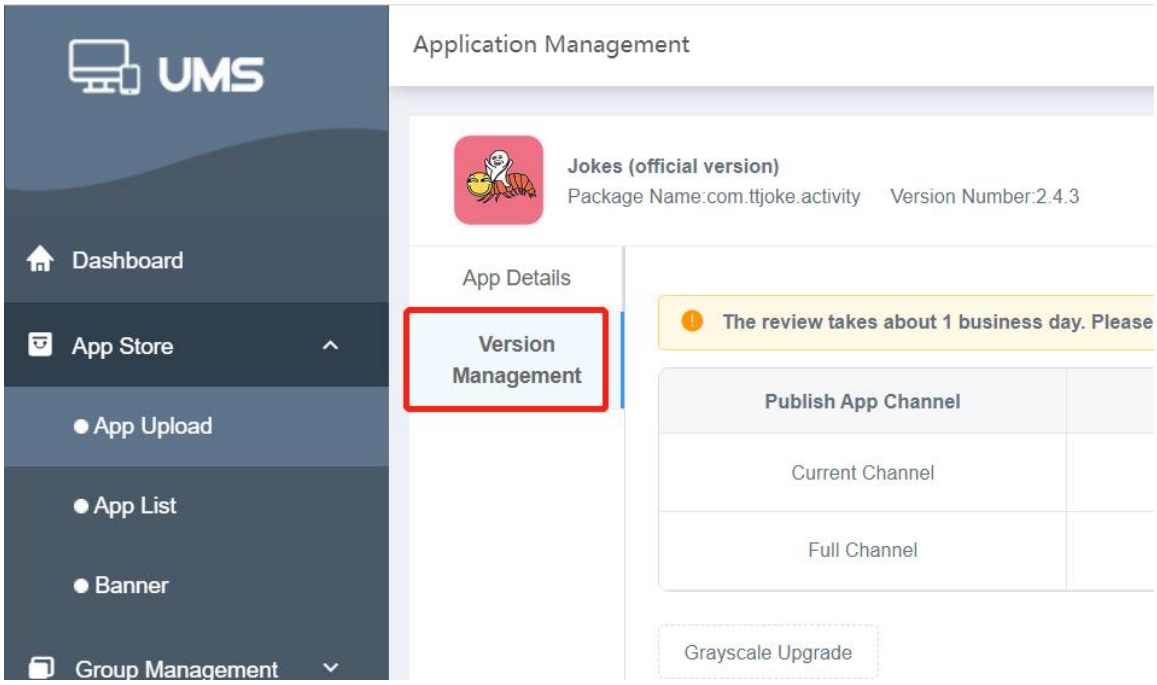


Figure (4.3.1.5.3)

2. Click Normal Upgrade - Upload Multiple Versions

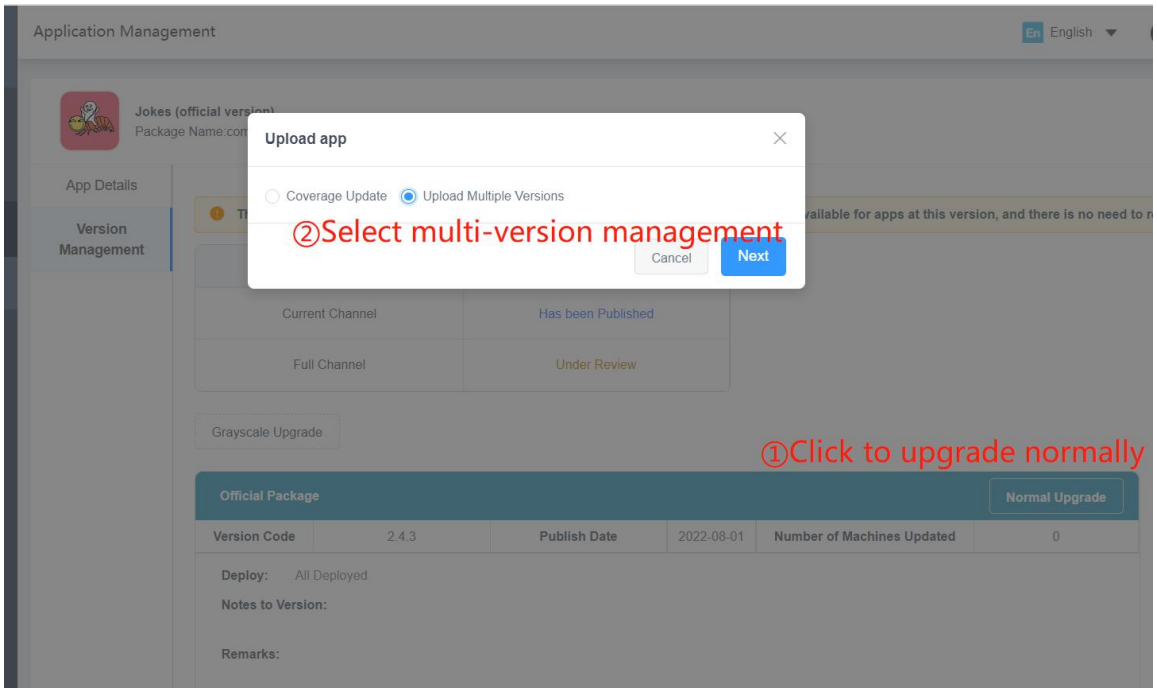


Figure (4.3.1.5.4)

3. Upload apk. Click or drag to upload

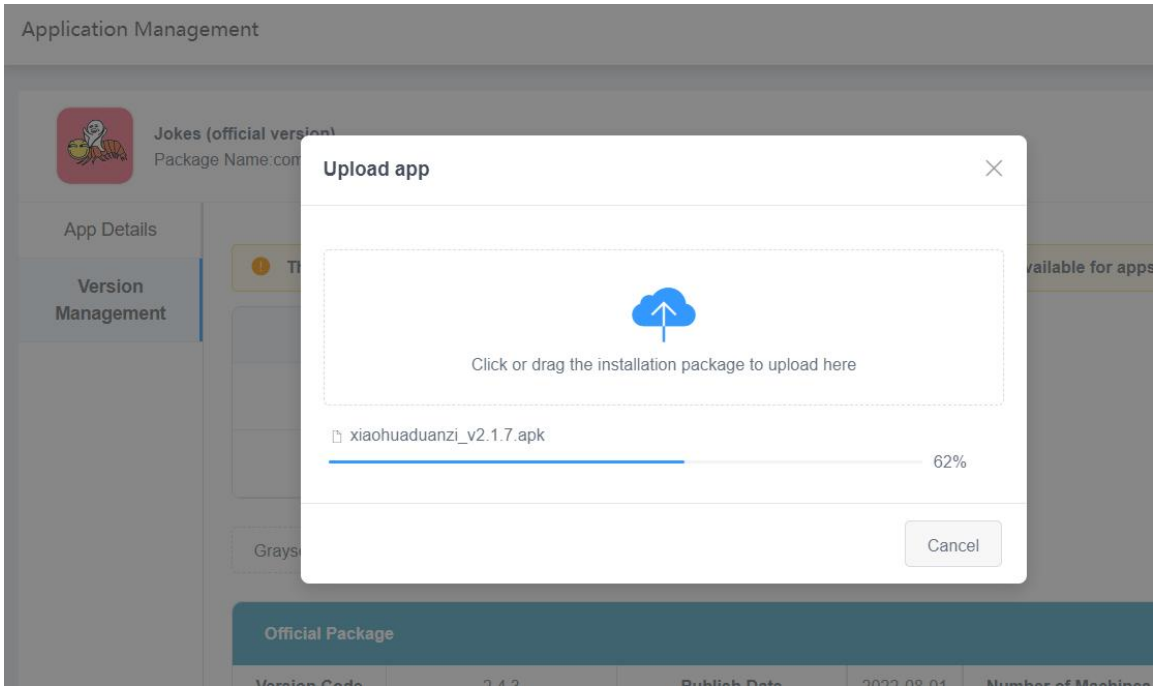


Figure (4.3.1.5.5)

4. After uploaded successfully, enter the signature and signature remark and click Submit (signature). The signature is usually automatically recognized. If the signature is not recognized, enter the model.

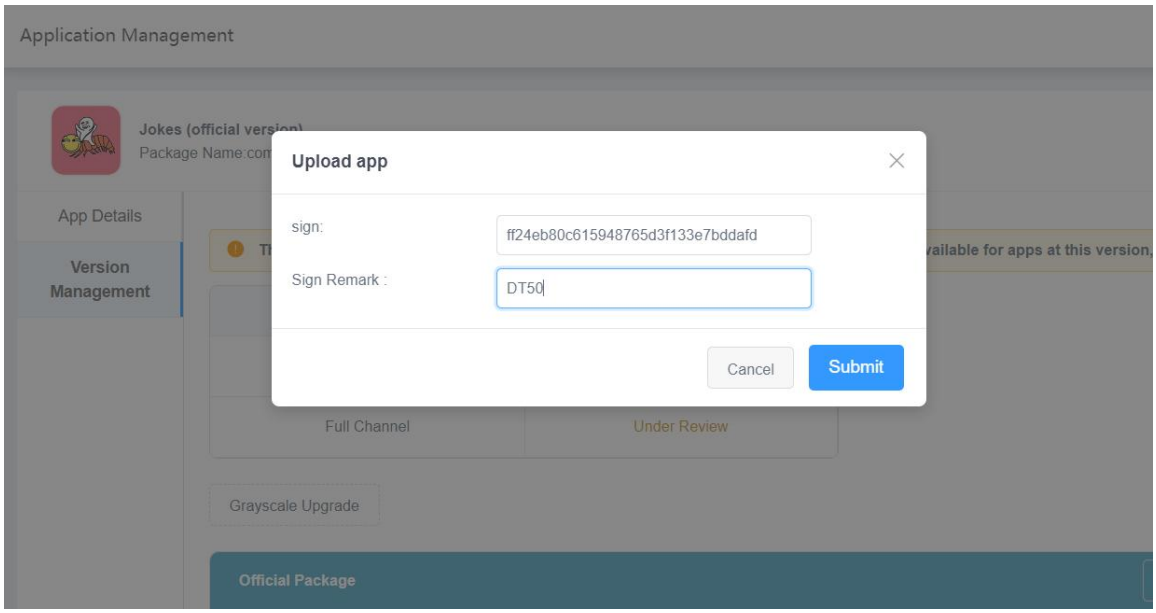


Figure (4.3.1.5.6)

5. After multiple versions are uploaded successfully, all versions are displayed in the lower part of the version update page

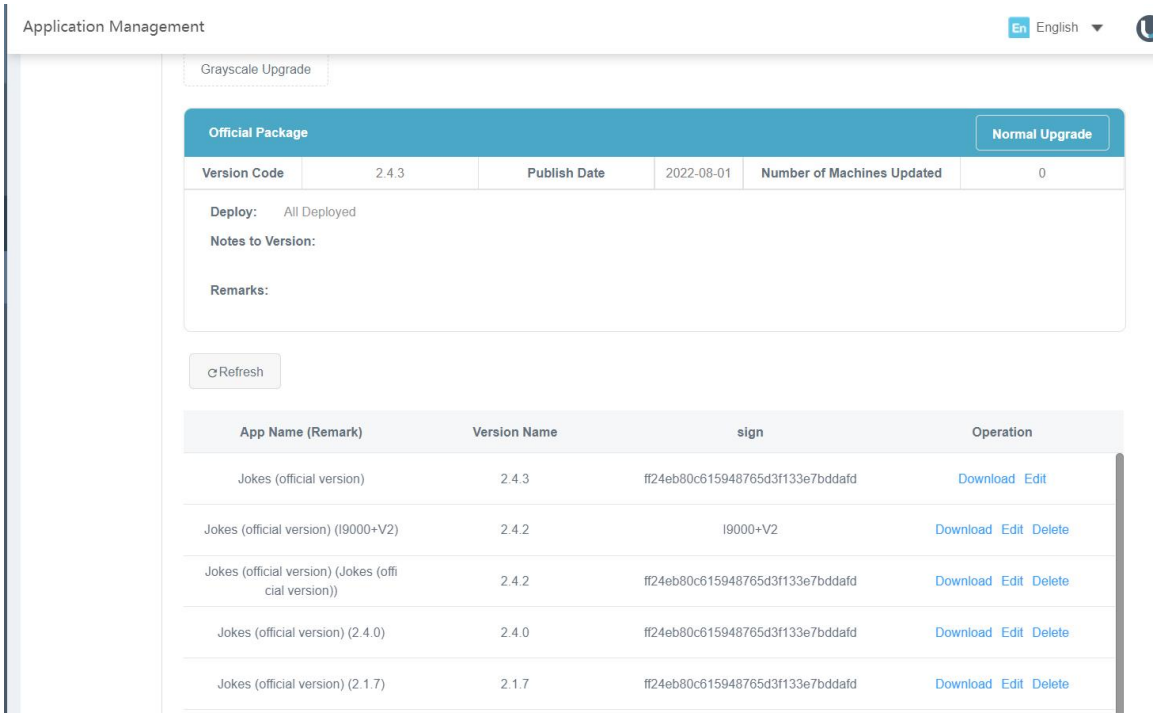


Figure (4.3.1.5.7)

6. As shown in the following figure, after multiple versions are uploaded successfully, all versions can be viewed by tapping the application in the application market to go to the Download Details page

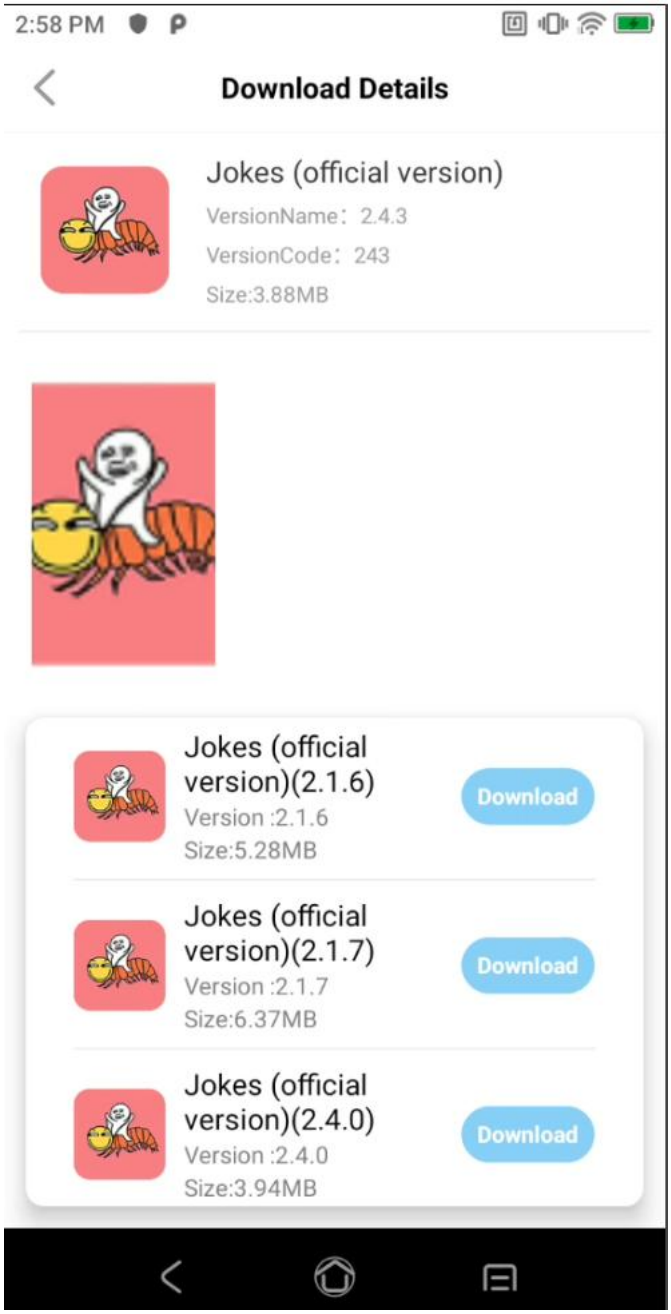


Figure (4.3.1.5.8)

4.3.1.6 Delete App

Click [Delete] button on the top right corner of application upload page, the application is deleted; the device cannot detect the app after its deletion.

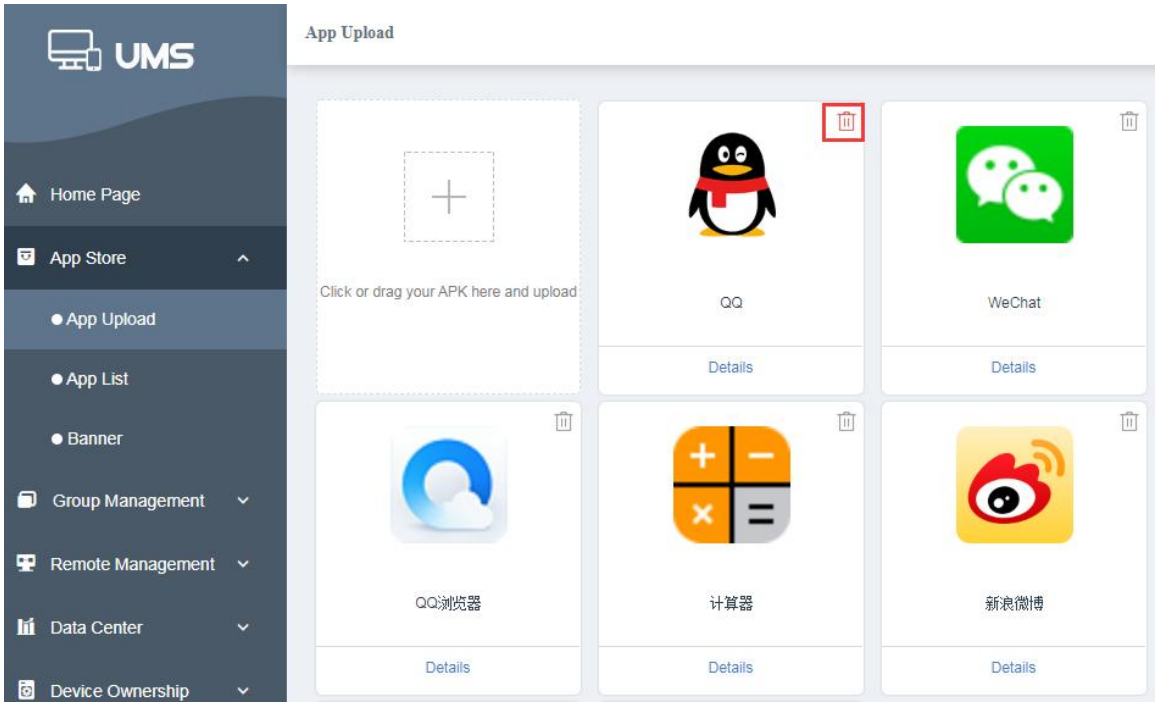


Figure (4.3.1.5.1)

Tips：

(1) Whether the app is on the shelf or not, all version of this application can be deleted. Then devices cannot find the app after its deletion. Once being deleted, the app cannot be restored.

(2) If the device had download and installed this application, Then delete it later, the application in the device will not be uninstalled and not appear in the page of application market.

4.3.2 App list

It shows the applications of registered account, including the official package uploaded from local channel, application uploaded under full launch with full deployment and grayscale package subject to review. The list which has been launched will show the available application. It can search corresponding application according to the device model or application name.

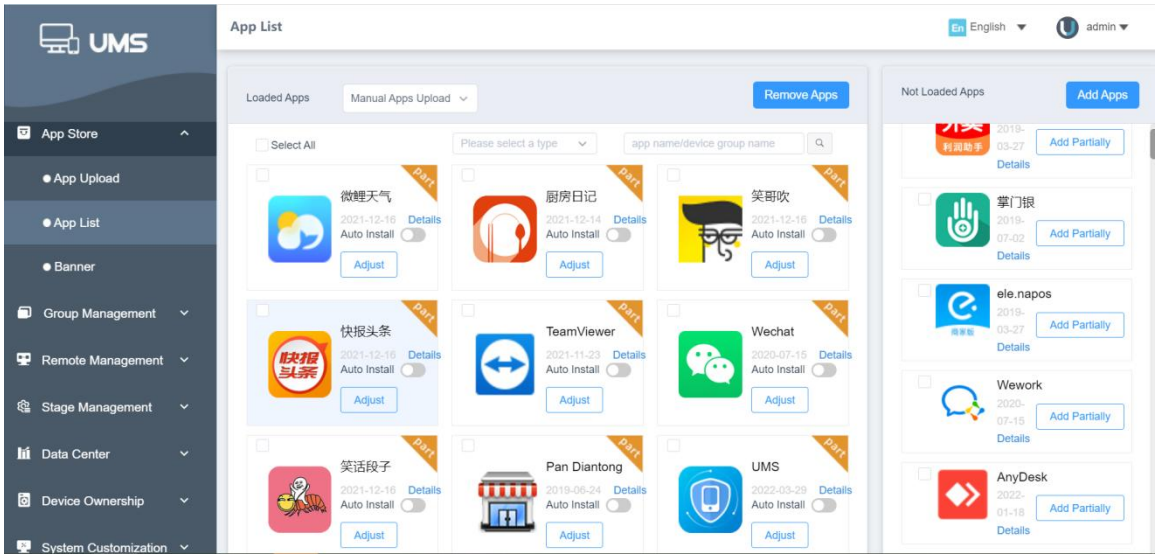


Figure (4.3.2.1)

1. App shelf：The list of apps will appear after being put on the store, the device of local account can detect this application, and there are two ways to put on apps, manual Upload and automatic Upload ；

(1) Manual Upload: Each application can launch manually, it include two ways: parts and all.

A : Add Partially: in the ungrouped list, click one application button of [Add Partially], it will show up a grouping launch interface, select the application group of needs to launch, click [OK], it will group launch successfully (Figure 4.3.2.2). After it , the application list which has been put away ,status bar will be" parts" or "all", application show up [Adjust] button, grouping device that has been tagged can detect the application.

Notes:

The application of grouping, after adding group, this application do not launched in this group, new adding group cannot detect this application. If you want the new group can find the App, you can click [Adjust], and then select the new group.

B: For all: in the list of ungrouped, select one or many application, then click the right upside button of [Add Apps], all selected application will on the shelf. After it launched successfully, application will input to all groups, launch application list status bar will be "all", and will not occur the button of "Adjust".

Notes:

All launched application, adding new group, the application will launch to the new group automatically, new adding group can detect this application.

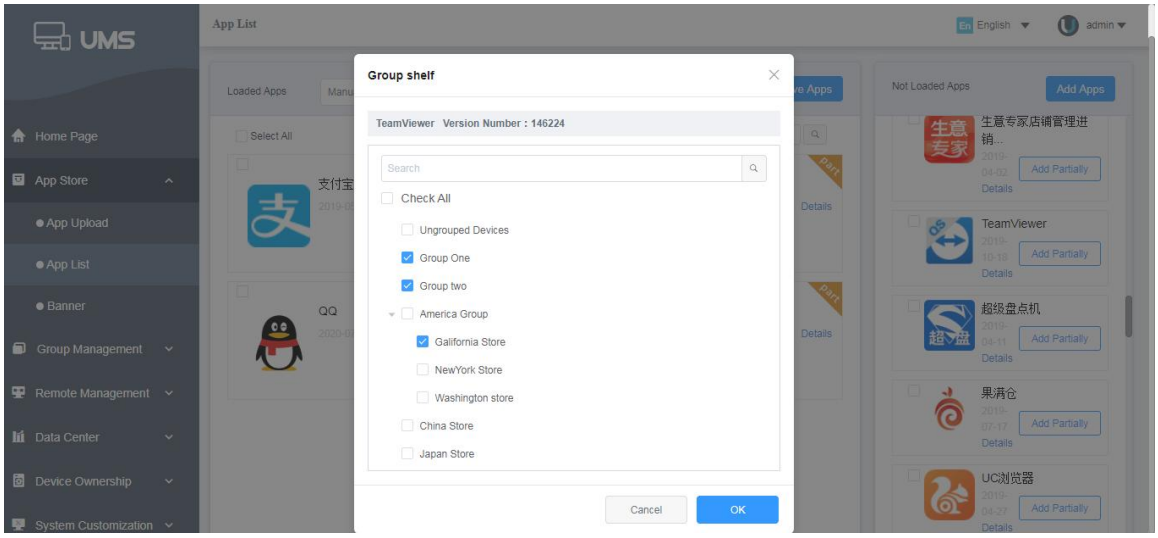


Figure (4.3.2.2)

(2) Automatic Upload: this model, all accounts will see all application launched , all groups' devices will detect all application uploaded, new adding group still can detect all application, and new applications uploaded will launch automatically.

Attention: if not necessary, don't use this function to upload apps, if you want to use it, please wait for a while and then operate other apps.

(3) Adjust: grouping application, on the list of launch will show up the button of [adjusting], click this button, it will show up this interface (Figure 4.3.2.3), you can cancel selected group before or adding new groups, click [confirm]. The devices of the groups you canceled cannot detect the application.

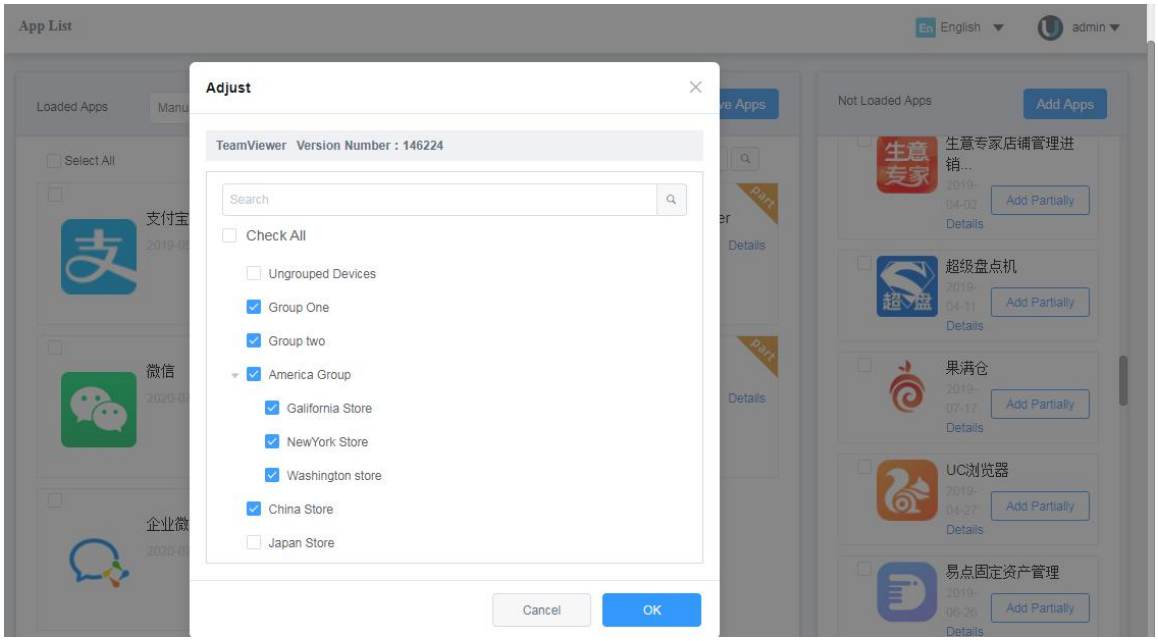


Figure (4.3.2.3)

2. App removal: select the app in displayed list, then Click [Remove Apps] to remove the application, device cannot detect the removed application.

3. Detail: Click the application detail to find information about app's name, version number, and check the device type, version description and Figure description;

Notes:

The display list will show the highest version of official package if multiple versions are uploaded;

4.3.3 Banner

The device will change Figures to carousel when Figures and link address are added on the banner. Click the Figure to enter relevant URL;

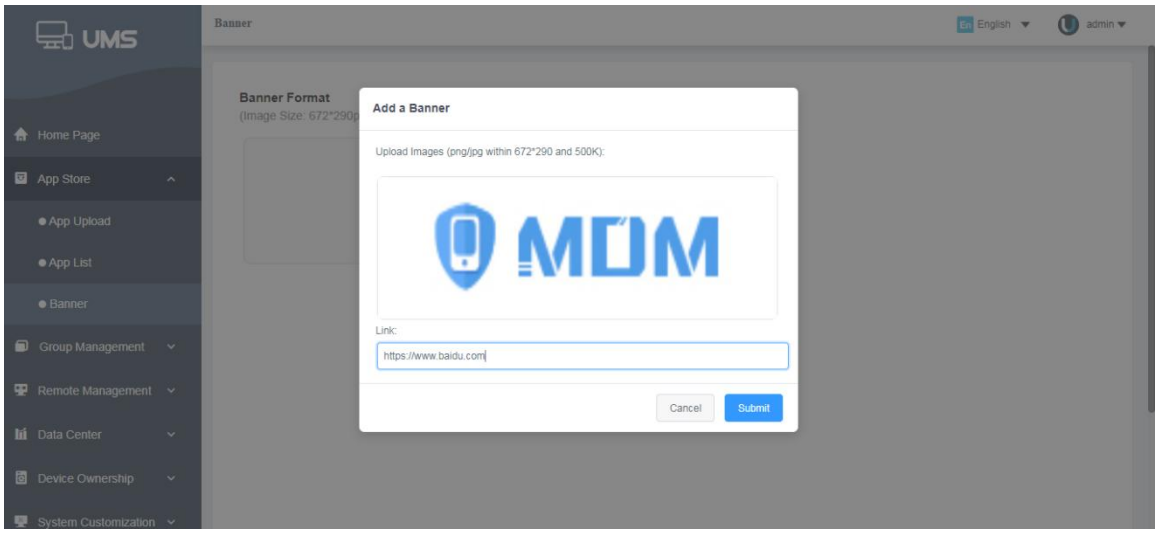


Figure (4.3.3.1)

1. Add Banner: Click [Add] button, upload Figure (less than 500KB, jpg/png format), terminal can detect this carousel after clicking the entered link.

2. Edit Banner: Click the added advertising Figure, then edit Figure and link, the edited carousel and links will be detected after device refreshes.

3. Delete Banner: Click the [Delete] button on advertise Figure, then delete this advertisement, and the device cannot detect this Figure link anymore；

Notes：no more than five carousels can be upload.

4.4 Remote Management

Remote collaboration is used for activated devices of different region or types by batch so as to monitor device status, and click the right side of the list to find regularly uploaded device information；

Remote management operates by batch and then sends instructions to terminals. Terminals can choose whether to execute them or not.

4.4.1 Remote Management

In the Figure (4.3), Click [Remote Management]-[Remote Management] in the list of menu bar to find information of activated device in the login account. It shows the device list of all devices, on the top of list will show the total amount of device and the amount

of online devices in the selected device group, as shown the Figure below 4.4.1.

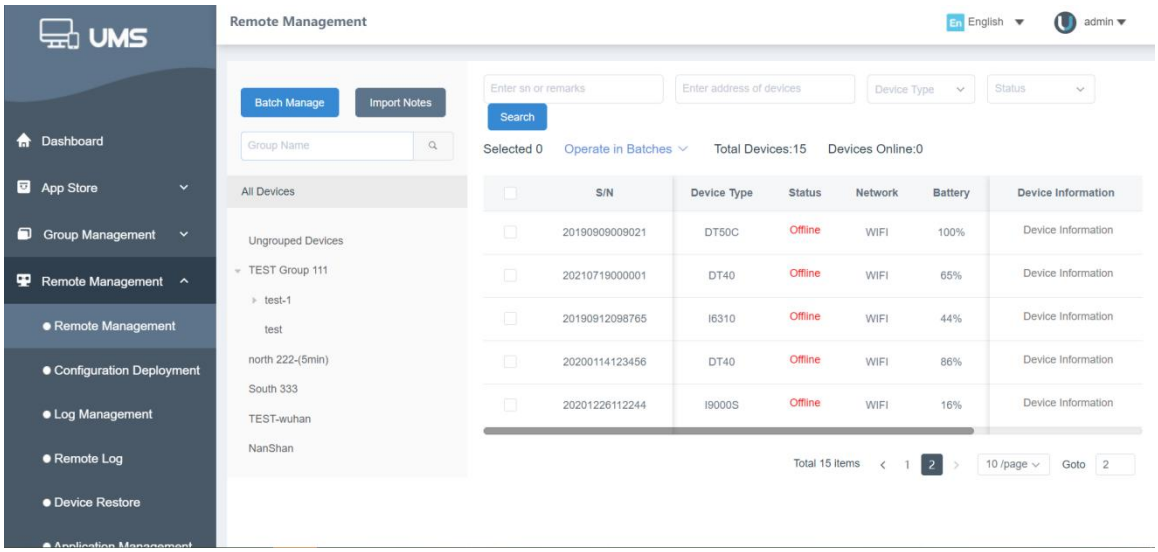


Figure (4.4.1.1)

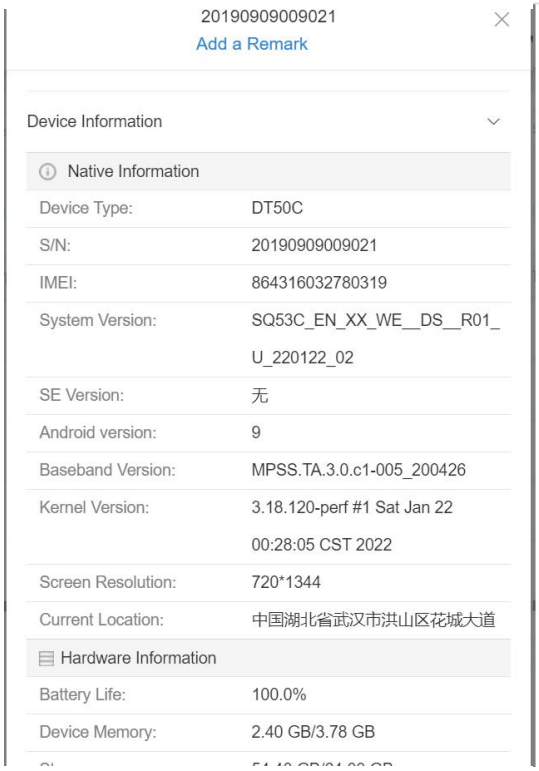


Figure (4.4.1.2)

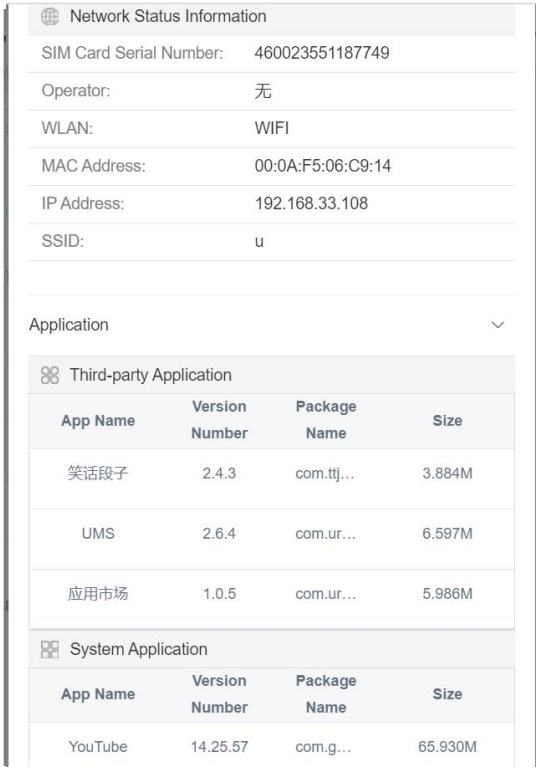
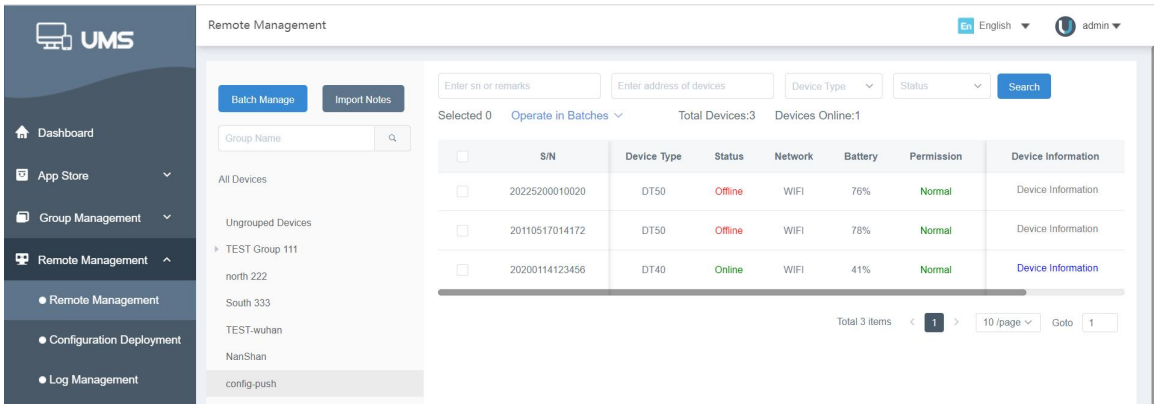


Figure (4.4.1.3)

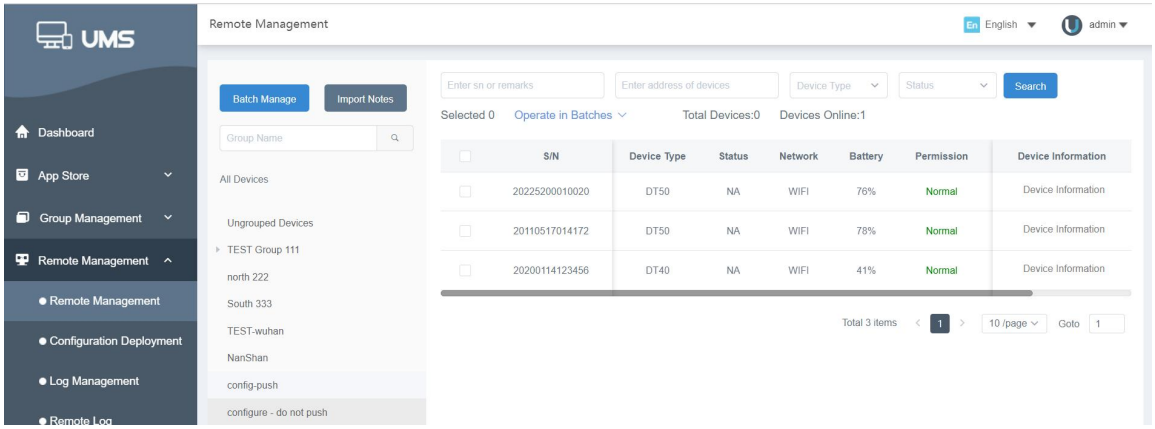
1. Enter SN number or choose model, Click [Search] to search relevant devices, Click [Device Information] on the list control bar to find regularly uploaded information regarding device and application;

2. Batch operation： Select one or multi-devices, Click [Batch Operation] to conduct remote management of devices by batch;

In remote settings - device configuration, custom mode, and push settings select "use", the online and offline display is normal (the device is online when connected to MQ, the device is disconnected or disconnected from the gateway, etc., offline after 2 minutes), please refer to the operation manual for the device. Configuration 4.4.8



In Remote Settings - Device Configuration, Custom Mode, and Push Settings, when "Not Use" is selected, NA is displayed both online and offline. For details, please refer to 4.4.8 of Device Configuration in the Operation Manual.



4.4.1.1 Operate in Batches

In the Figure (4.4.1.1), click the “Operate in Batches “to remotely manage the activated device. Click “All Devices” or “Device group below”, the list will show all of the devices or the device chosen in device group, then select the device in theist, click [batch operation] to operate all device or the device chosen in device group by batch.

1. Device Disabled/Unblocked：

Click [Disable Device]/[Enable Device] after the device is selected. Input the desired Notification Message in the pop-up window. Once the device receives the disable/enable command, those disabled will be blocked from use and have the afore notification message displayed on the device disabled screen. Contact the admin to re-enable such devices at back-end.

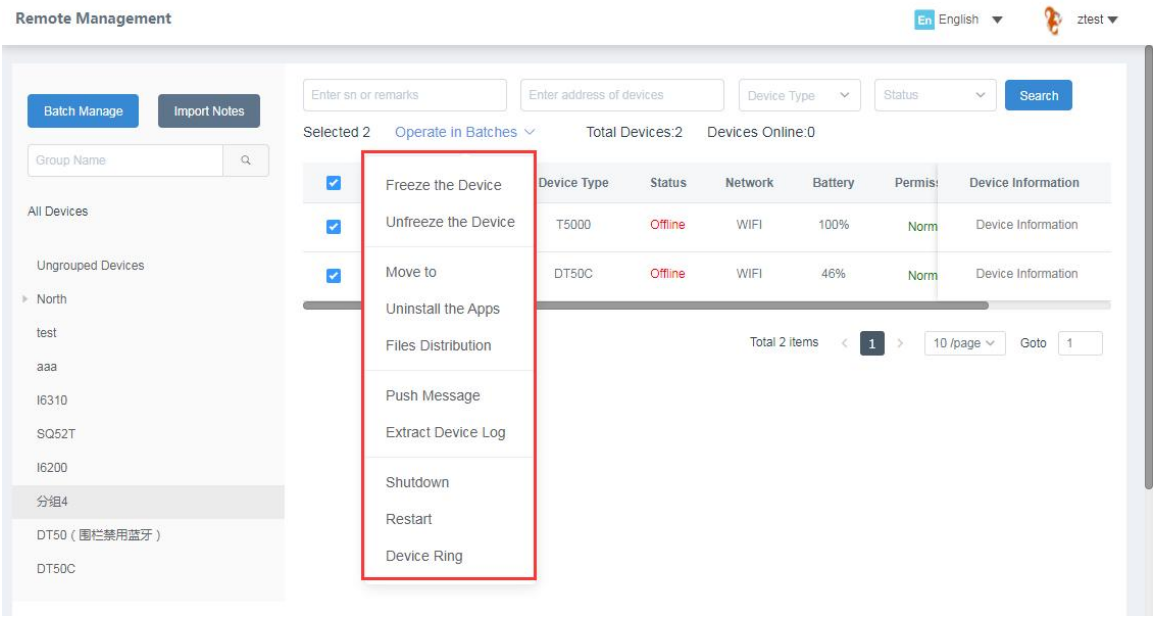


Figure (4.4.1.1.1)

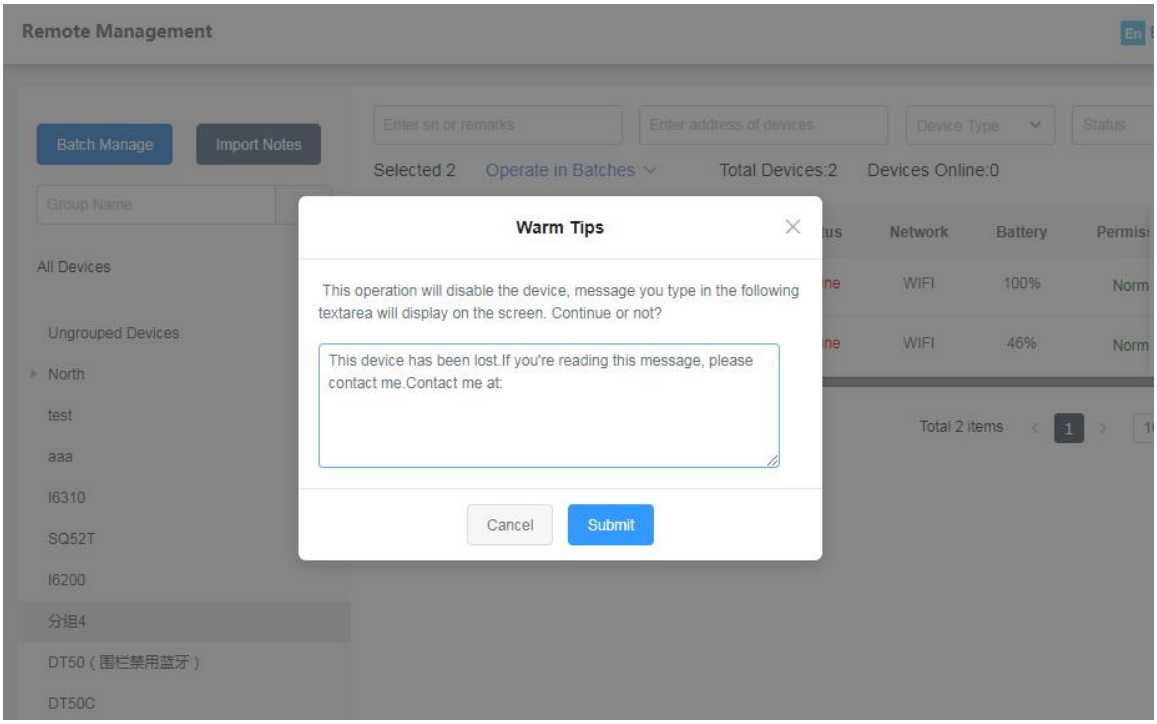


Figure (4.4.1.1.2)

2. Move to：

Click [Move to], move the same device of attribute to another group after check the

device then execute the same command for this group devices；

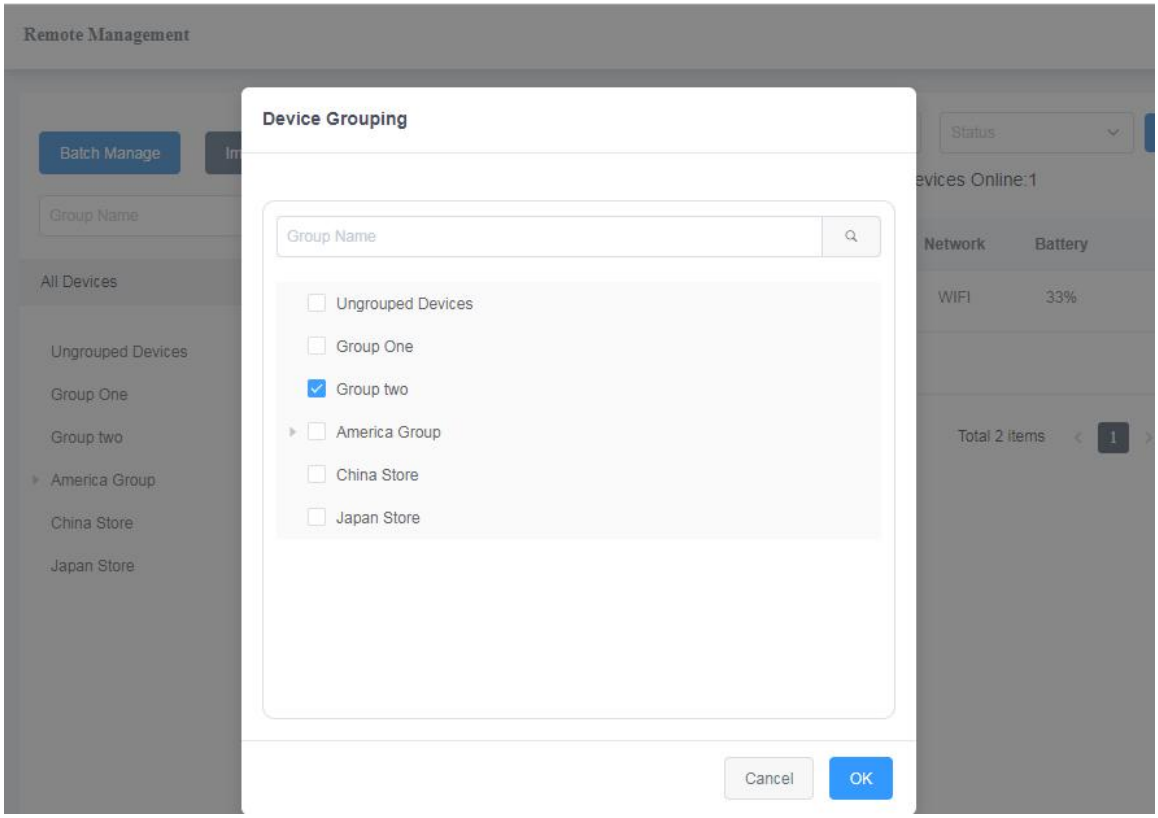


Figure (4.4.1.1.3)

4. Uninstall App：

Select a device and Click [Uninstall App] to find two ways to uninstall: uninstall by application name, uninstall by package name；

(1) Uninstall by application name: Choose application name or version to uninstall, then the device will uninstall this version only; uninstall fails if there is other version installed on the device.

(2) Uninstall by package name: Enter application package name and Click [Save], then all versions of this application under such package name are uninstalled from the device, as shown in the Figure (4.4.1.1.4).

Notes：The list of right side will appear an alarm clock for progress checking during task execution when batch operation is underway；

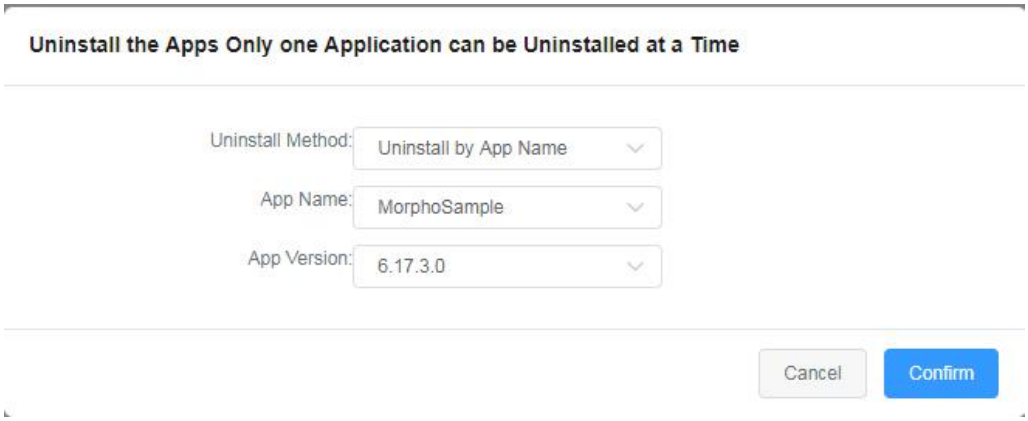


Figure (4.4.1.1.4)

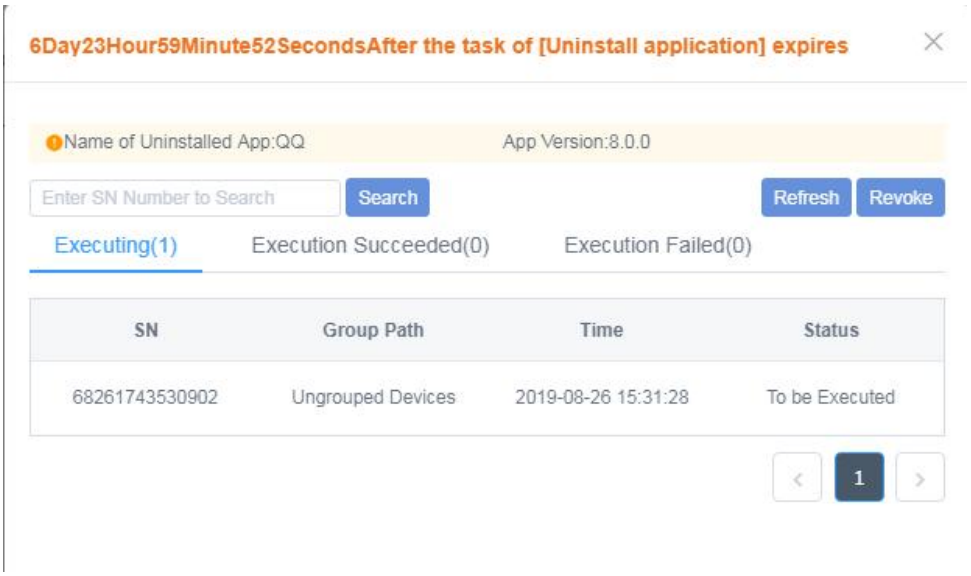


Figure (4.4.1.1.5)

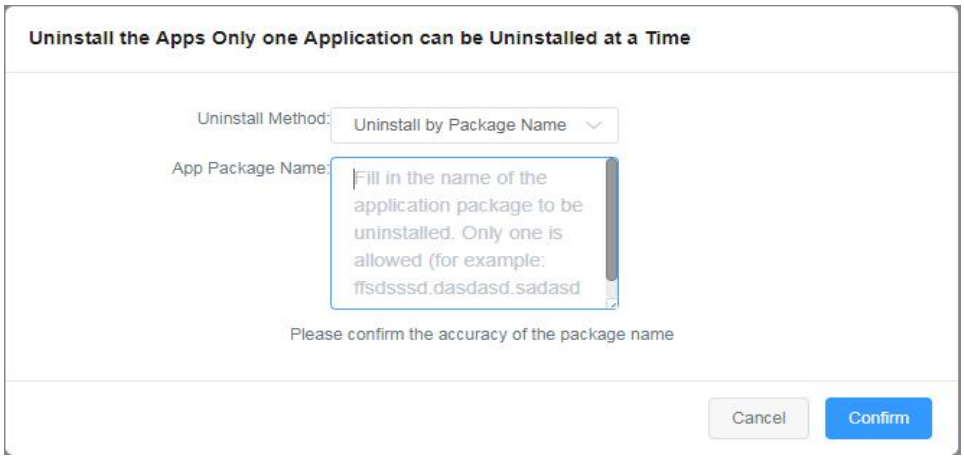


Figure (4.4.1.1.6)

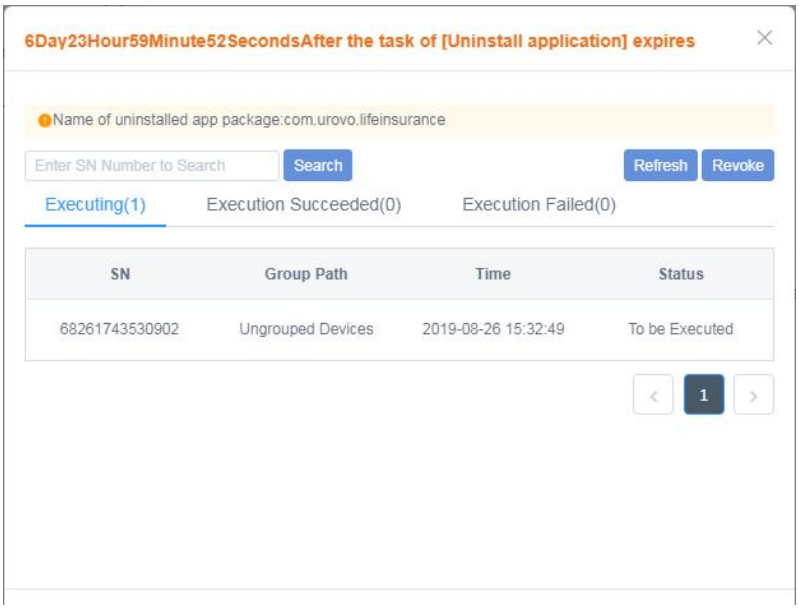


Figure (4.4.1.1.7)

4. File Distribution：

After selecting the device, click [File Distribution], upload the file (less than 100M), enter the target path, select the file rule, and click [OK] to complete the file distribution. After the device detects the file, it will download the file and store it in the target path.

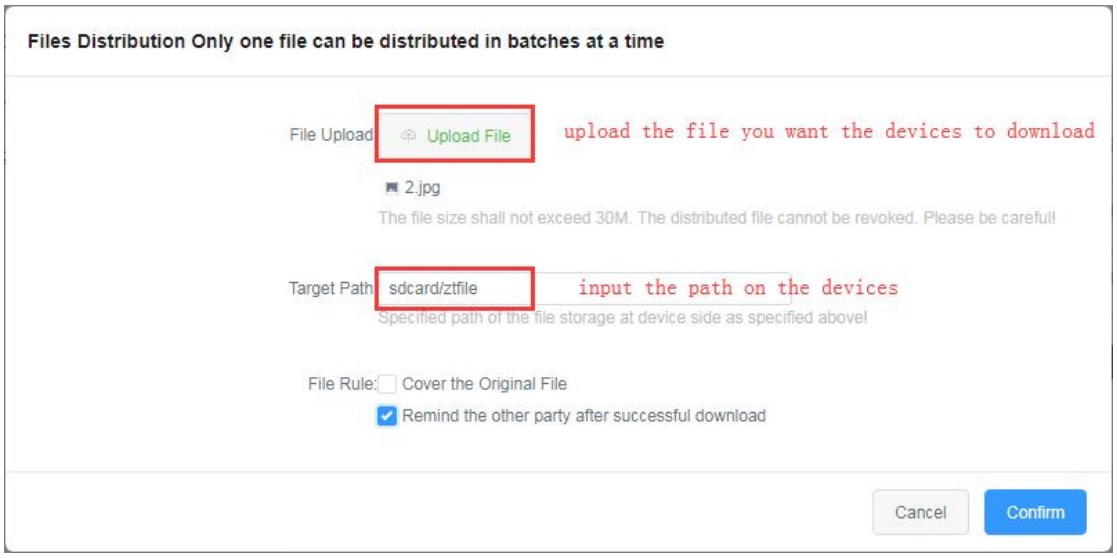


Figure (4.4.1.1.8)

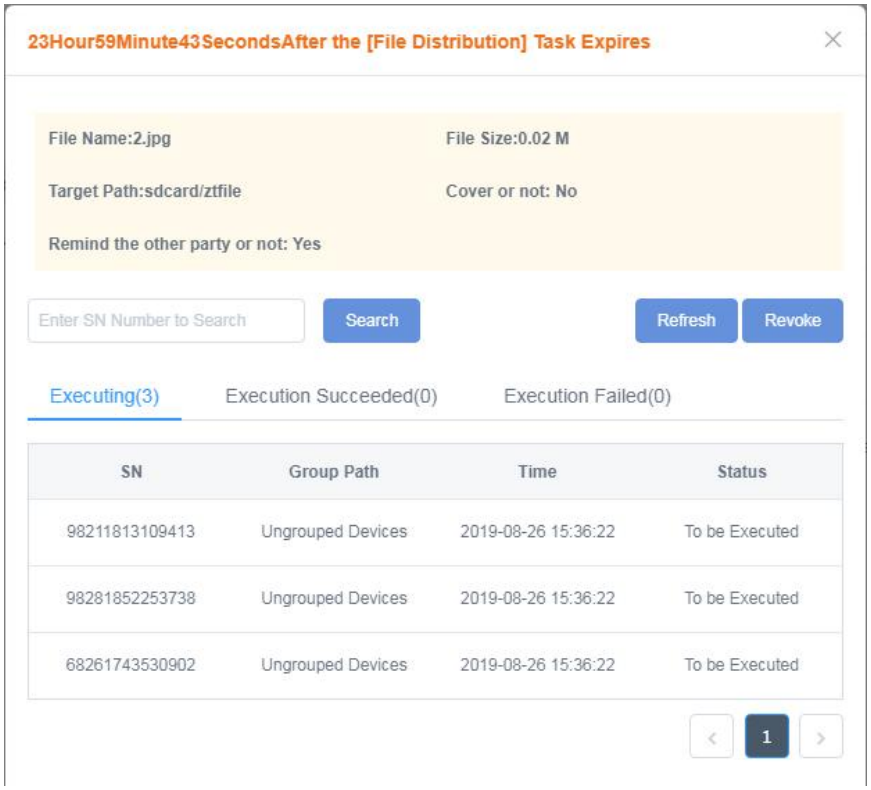


Figure (4.4.1.1.9)

5. Power off/Reboot：

Click [Power off/Reboot] after check the device, the device will execute the command of Power off/ Reboot when the device received the command；

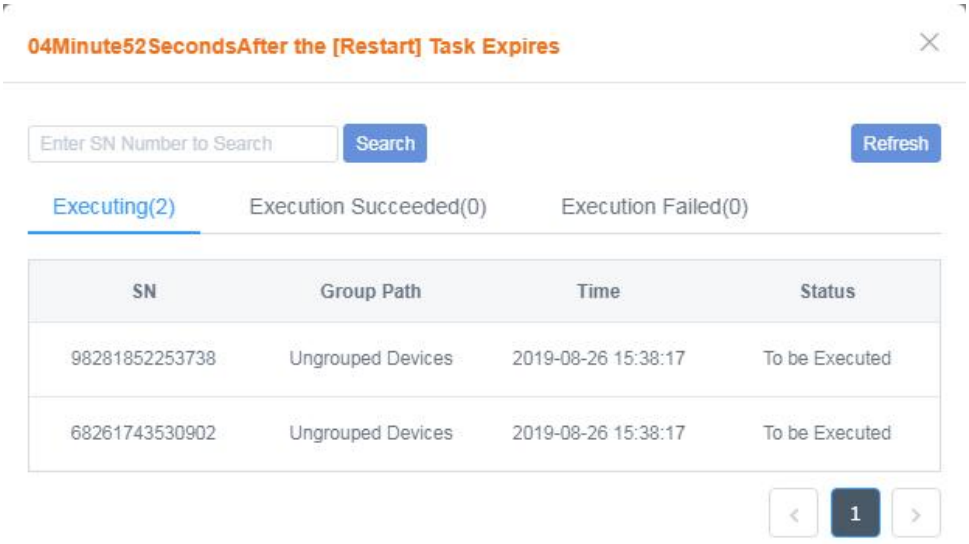


Figure (4.4.1.1.10)

6.Extract device log: Select a device then click [Extract device log]. Upon receiving the command, the device will upload its device log, which, if successfully uploaded, can be downloaded by clicking the

“View Log” in the Alarm Details pop-up window.

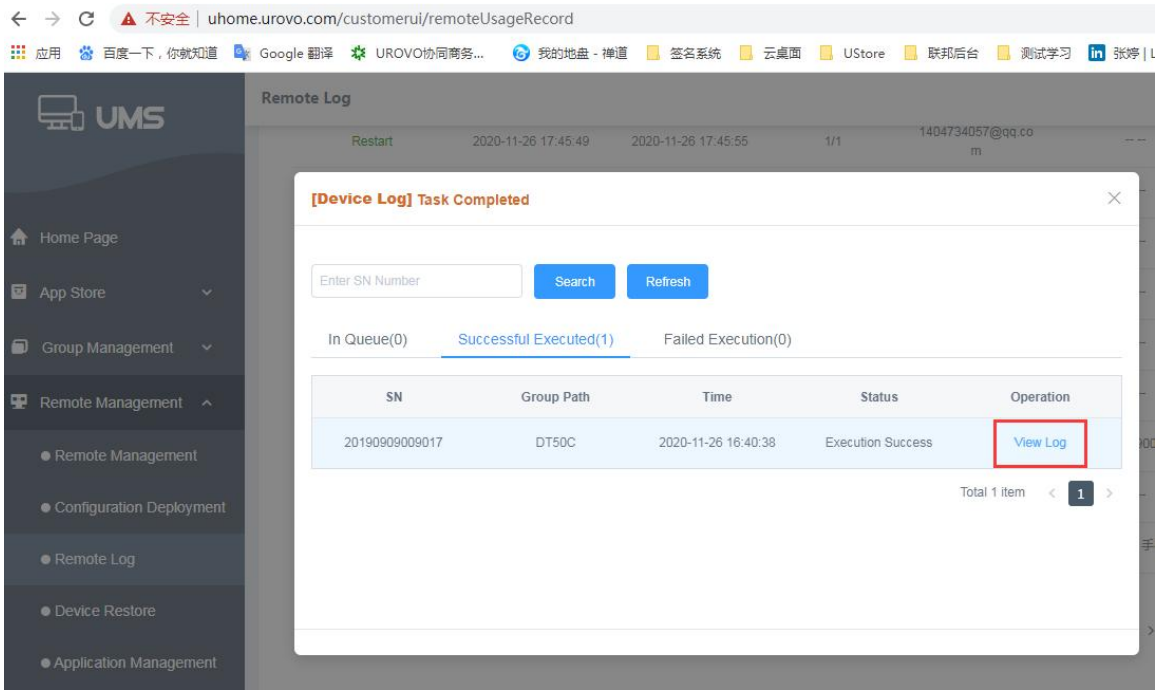


Figure (4.4.1.1.11)

7.Message push:

After selecting the device, click [Push Message], enter the message that needs to be pushed in the input box, and click [OK]. After the device receives the instruction, it will pop up a prompt message "New message received, do you want to check it? " , You can click [Open] or check it in the message list, each pushed notification is limited to 1000 words.

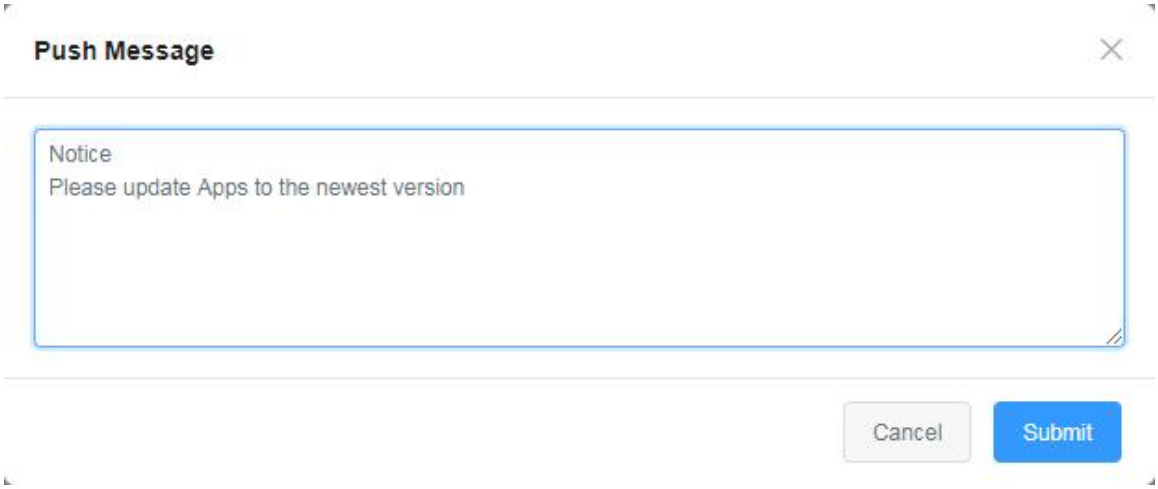


Figure (4.4.1.1.12)

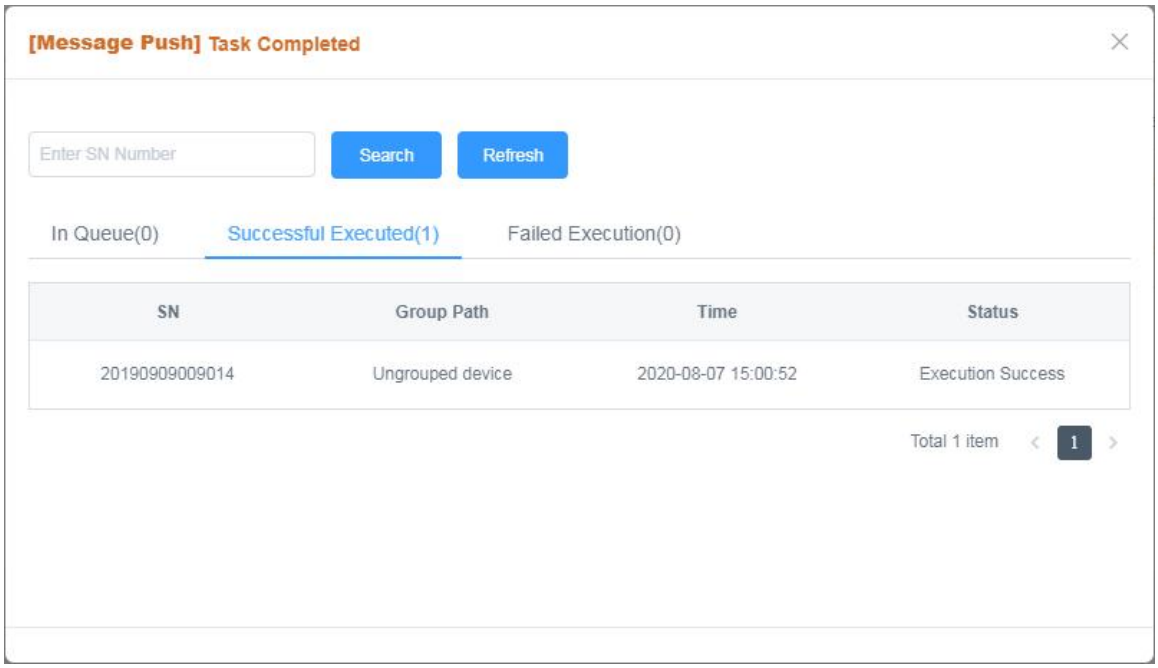


Figure (4.4.1.1.13)

8. Device ringing:

After selecting the device, click [Device Ringing] under the Batch Operation, and click the [Play] button in the confirmation pop-up window. After receiving the instruction, the device will ring with the maximum volume and the ringtone can be stopped only after shutting down/restarting the device. This function can be used to find nearby devices.

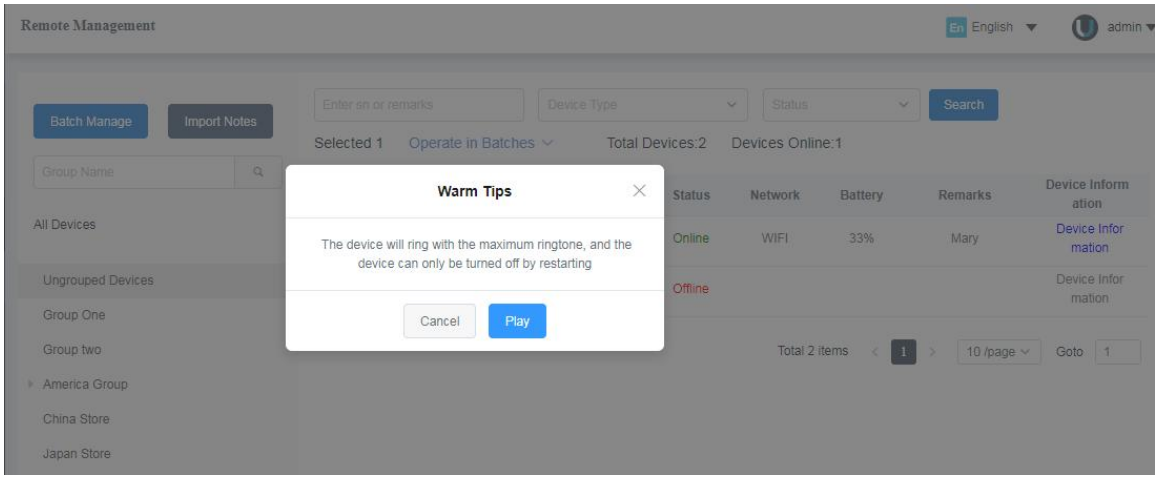


Figure (4.4.1.1.14)

4.4.1.2 Batch Manage

In the figure (4.4.1.2.1), click the "Batch Manage" button to perform remote batch operations on the devices in the group by group. The batch operation types include: Device Unforbidden/Unblock, Device Move To, Batch Uninstall App, Files Distribution,

Push Message, Extract Device Log, Shutdown/Restart, and Export Device Info.

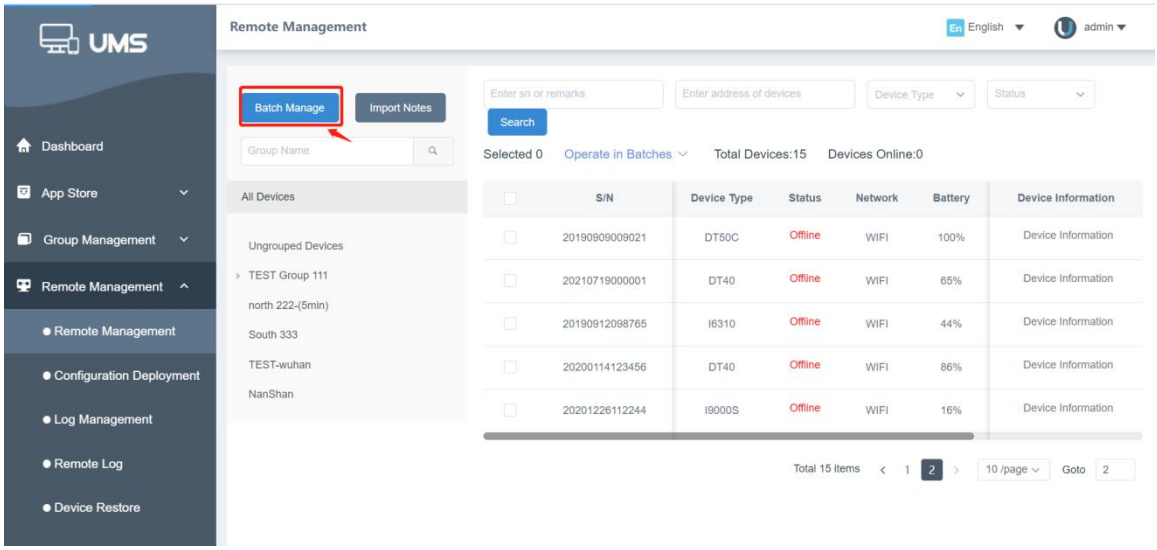


Figure (4.4.1.2.1)

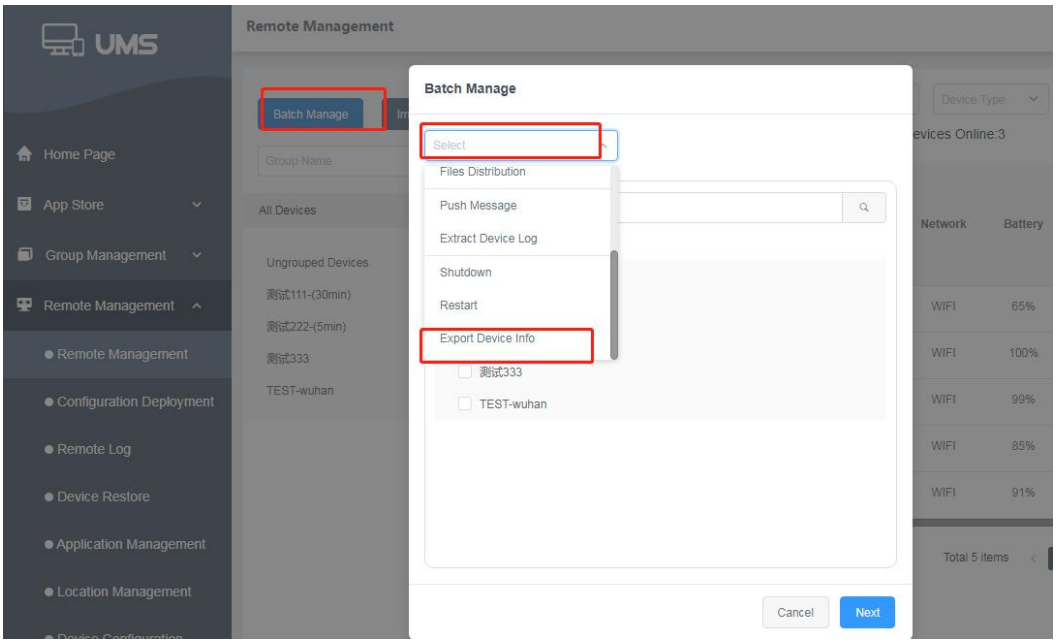


Figure (4.4.1.2.2)

(1) Click [Batch Manage], a batch management pop-up window appears, and the selection box of "Batch Operation" is displayed at the top (Figure 4.4.1.2.2), and the group information of this account is displayed at the bottom (Figure 4.4.1.2.1). After selecting batch operation, check the group requiring batch operations, and click [Next] to perform the relevant batch operation in the pop-up window corresponding to the next step (see 4.4.1.1 batch operation for each operation type), and then the devices in the

selected group will perform the corresponding operations.

4.4.2 Remote Configuration

In Figure (4.4), click [Remote Control/Remote Setting] in menu bar, can see WIFI deployment policy for all login account. After adding WIFI deployment policy, can push to device group. After that, device list will reflect total device count to be deployed. WIFI setting list shown as Figure 4.4.1.1：

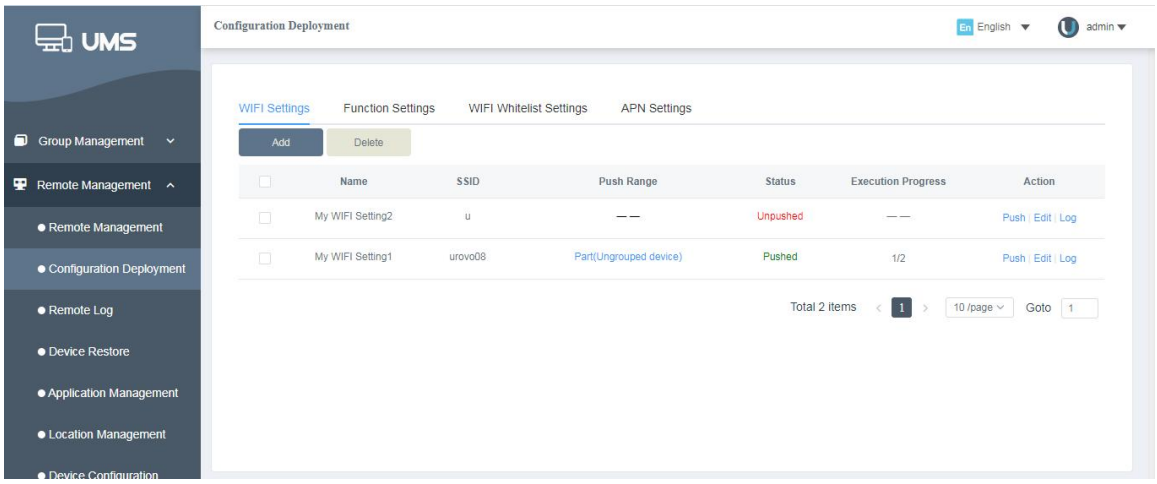


Figure (4.4.2.1)

4.4.2.1 WIFI Settings

1. Add WIFI deployment policy:

Click [Add] in WIFI deployment list, enter SSID, select security type, password in popup WIFI remote setting screen. Click [Confirm] to execute adding deployment. After that, the WIFI deployment policy will be shown in list and status is “Not pushed”.

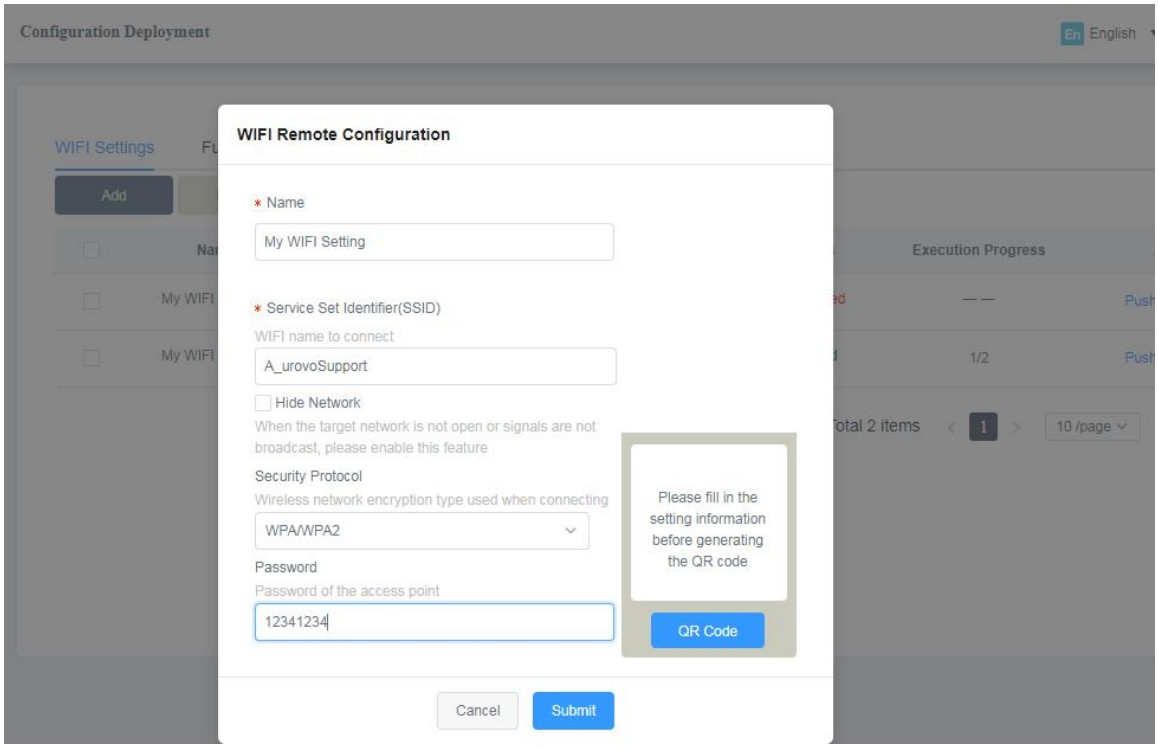


Figure (4.4.2.2)

Notes:

(1) If you select Hidden network, it can automatically connect to the hidden WIFI within the detection range of the device.

(2) The [Only allow this WIFI] option on the original WIFI setting page is removed, and now the WIFI displayed on the device is managed by the WIFI whitelist.

2. Push WIFI deployment policy

2.1 Group push

Click [Push] from the WIFI deployment list, popup “WIFI device push” message. You can select single or multiple group, then click [Next] to close the prompt. State of WIFI deployment policy will change to “Pushed”, progress is 0. Devices of selected group will connect the WIFI follow the WIFI deployment setting.

Progressing completing percentage will increasing when device start connecting to SSID. Progress percentage comes from success device / total push device count. After all device deployed success, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

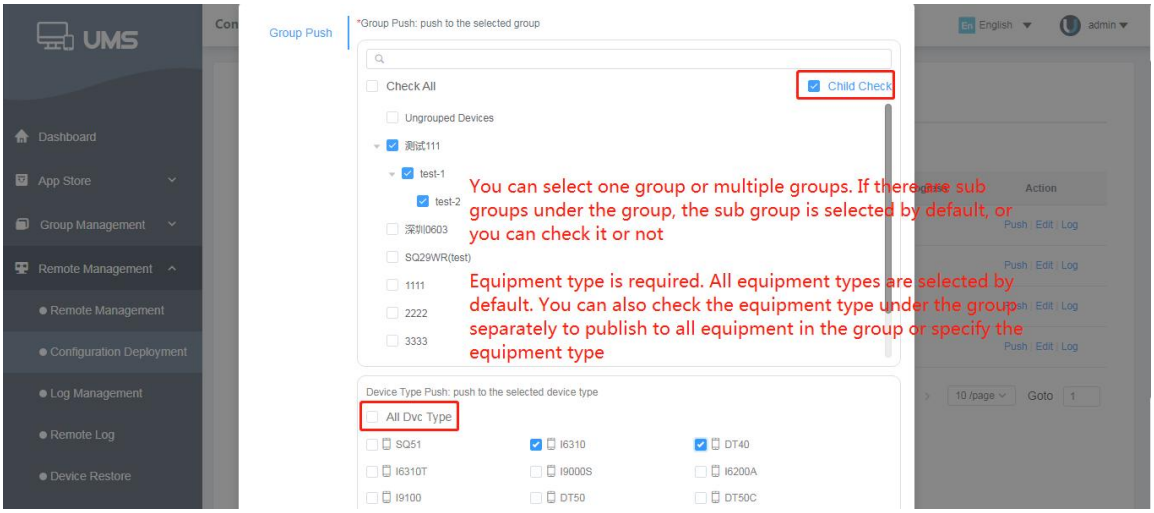


Figure (4.4.2.3)

2.2 SN push

Click [Push] in the operation bar of WIFI configuration list to pop up the window of "WIFI setting SN push". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, the pop-up window will close, and the state of WIFI configuration rule will change to “Pushed”, and the progress is 0/number of devices pushed. After receiving the command, the devices in the selected device group will execute this WIFI configuration rule, and connect to the configured WiFi.

If the devices in the pushed group receive the WIFI configuration command and try to connect to the published SSID, the progress of the rule will increase. The progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If all devices are connected to the WiFi, the number of successfully executed devices displayed in the progress bar is equal to the total number of devices.

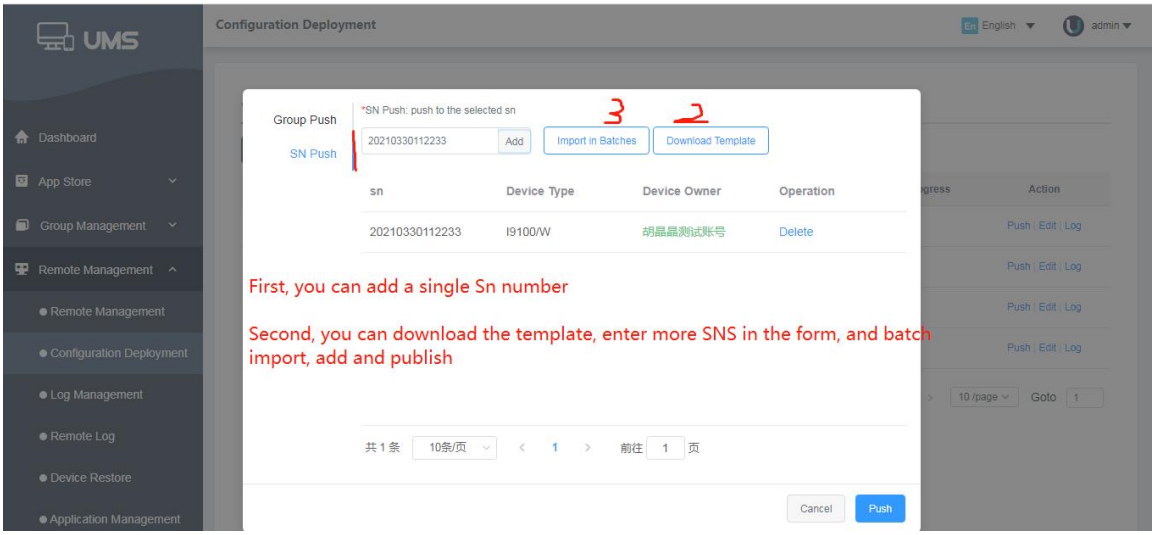


Figure (4.4.2.1.4)

Note:

1. If cancel selected group in push, WIFI deployment devices will disconnect and delete all WIFI deployment information (same result as delete WIFI deployment).
2. After push is executed, other devices which moved to this group will not execute the WIFI deployment policy.

3. Edit WIFI deployment policy

Click [Edit] of WIFI deployment menu, popup “WIFI remote setting”. Application policy can be modified here, included policy name, SSID, security, password…etc. After modified the policy, all policy will be pushed again and progress complete progress will start with 0.

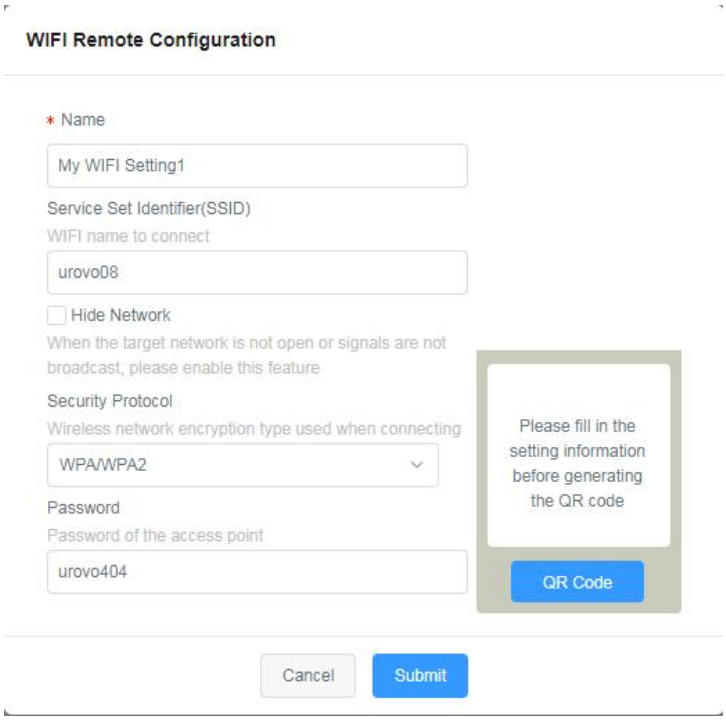


Figure (4.4.2.5)

4. Record

Click [Record] in WIFI deployment menu, deployment record will show up. Click [View push content], can check detail of WIFI remote deployment policy which pushed.

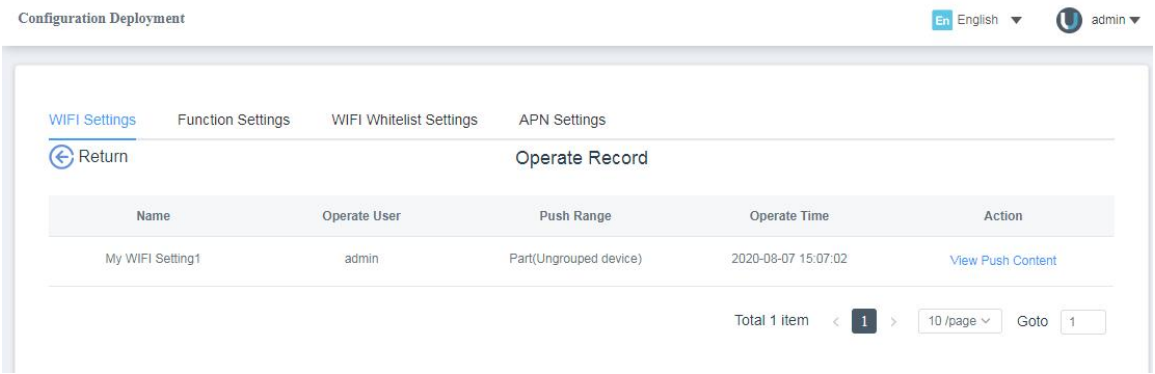


Figure (4.4.2.6)

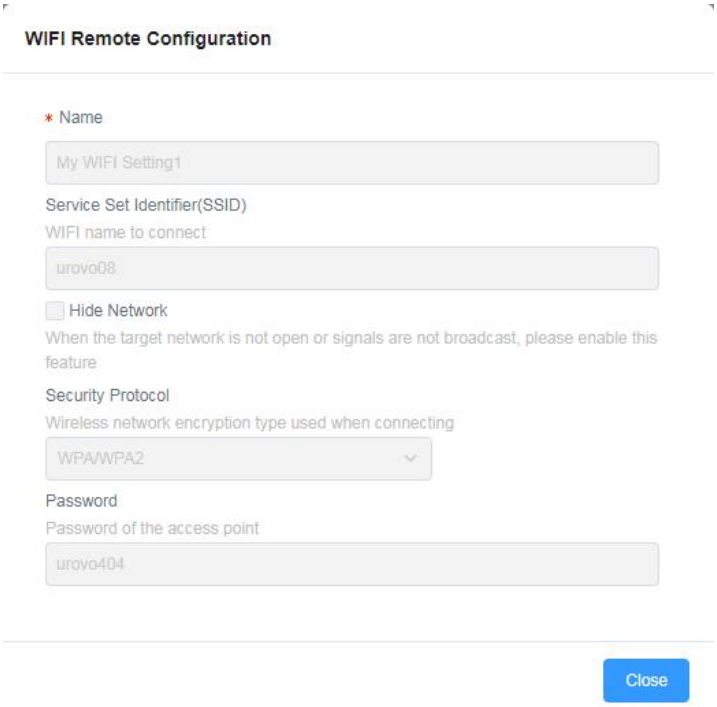


Figure (4.4.2.7)

5.Delete WIFI deployment policy

Click [Delete] from WIFI deployment menu, you can delete WIFI deployment policy to devices. After execution, the deleted policy will not show in deployment list and devices will follow up to disconnect the SSID and delete previous WIFI deployment information.

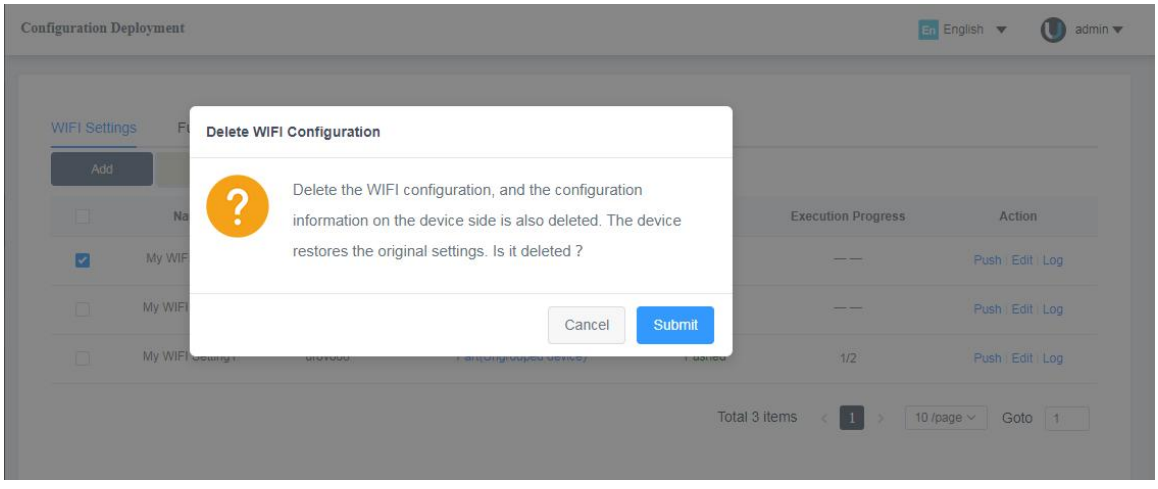


Figure (4.4.2.8)

4.4.2.2 WIFI Whitelist (new function)

On the remote setting page, click the "WIFI whitelist setting", the page will display the WIFI whitelist list. After adding the WIFI whitelist, push it to the device group. After the devices under the device group receive the WIFI whitelist command, only the detected whitelist WIFI will be displayed on the WIFI list page of the device. The WIFI whitelist list is shown in Figure 4.4.2.2.1:

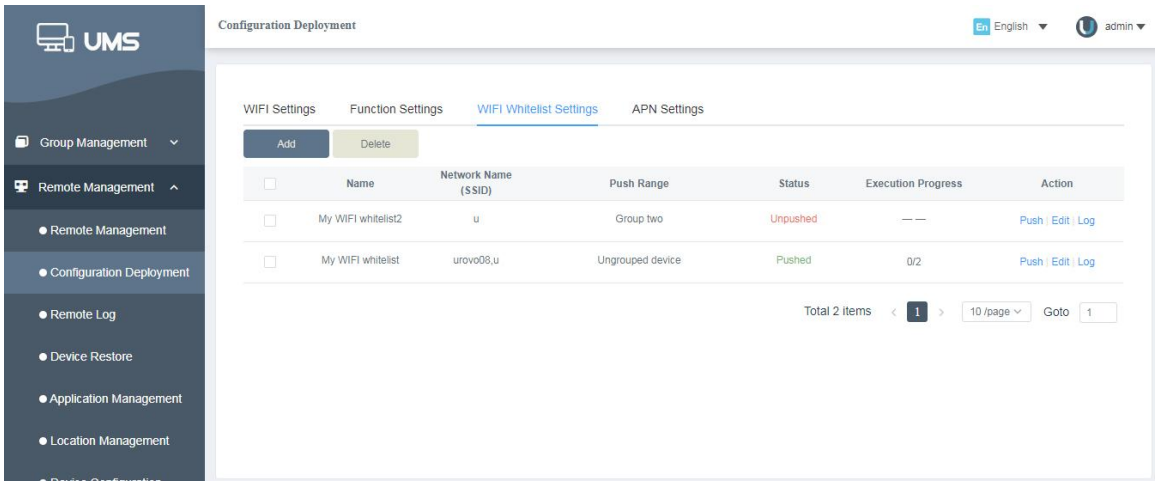


Figure (4.4.2.2.1)

1. Add WIFI whitelist rules

Click [Add] on the top of the WIFI whitelist page add a pop-up page to the WIFI whitelist, enter the name (default: My WIFI whitelist), select the push group (only one can be selected), the SSID of the WIFI pushed to this group will be shown under the whitelisted network name or we can add whitelist WIFI manually in the input box), and then click [Add], then the new rule is set up successfully. Finally, the WIFI whitelist rule will be displayed in the WIFI whitelist list, and the status is "Not Pushed";

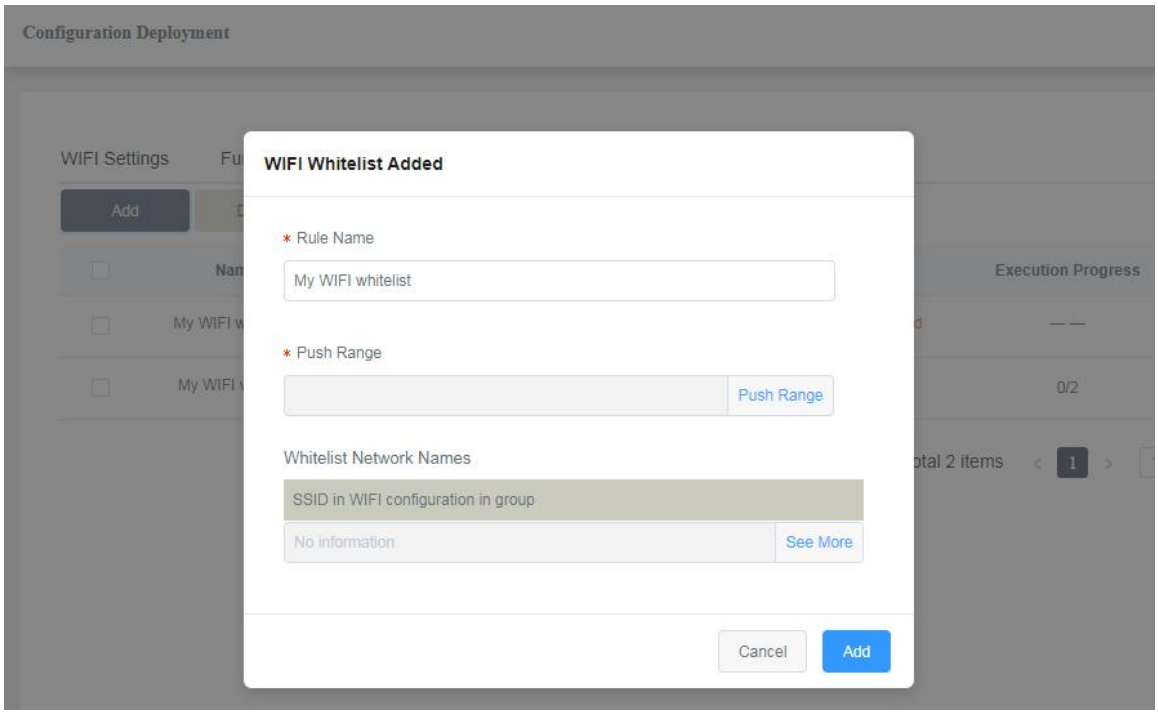


Figure (4.4.2.2.2)

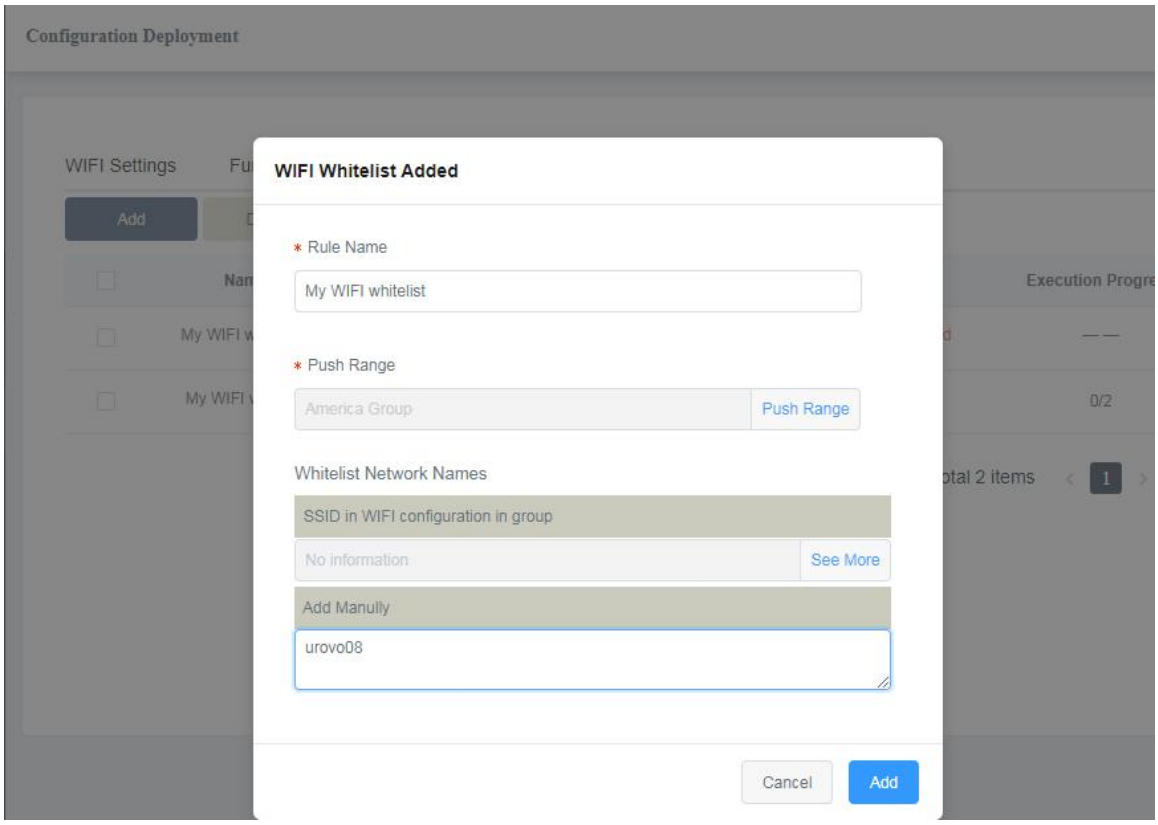


Figure (4.4.2.2.3)

Notes:

1. The rule name is my WIFI whitelist by default, and the rule name cannot be repeated;

2. A rule can only correspond to one group. After selecting the group, the "SSID in the

WIFI configuration in the group" below will display the WIFI pushed to this group in the "WIFI configuration";

2. Push WIFI whitelist rules

Click [Push] in the operation bar of the WIFI whitelist list, a pop-up window of "WIFI whitelist push" will pop up, click [OK] and the pop-up window will be closed, the status of this WIFI whitelist rule changes to "Pushed" and the progress is 0 /Total number of devices. The devices under the selected device group will execute this WIFI whitelist rule after receiving the instruction, and the WIFI list page of the device will only display the pushed whitelist WIFI.

If the device under the pushed group receives the WIFI whitelist command, after the device displays the detected whitelist WIFI, the progress of this rule will increase, and the progress will be displayed as: **number of successfully executed devices/total number of devices in the group pushed**. If all devices have finished executing the whitelist rules, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

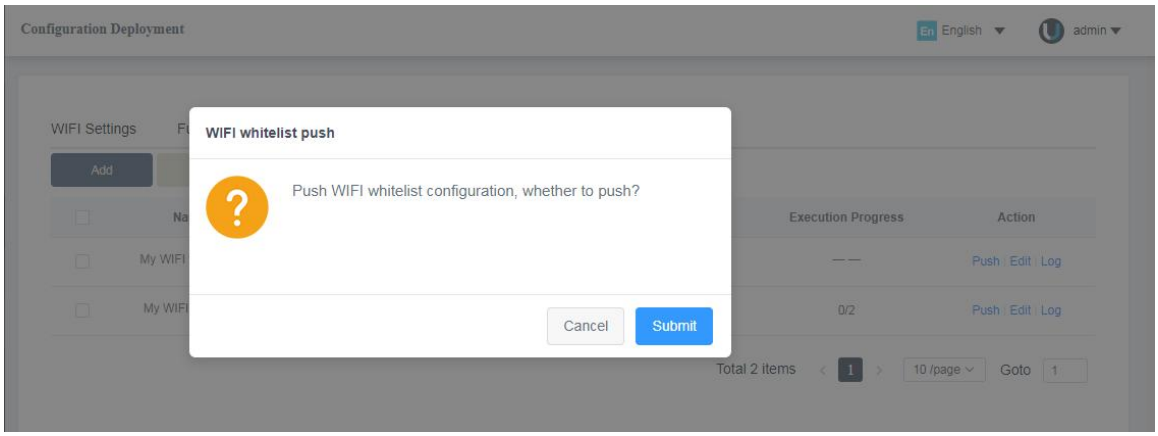


Figure (4.4.2.2.4)

3. Edit WIFI whitelist rules

Click [Edit] in the operation bar of the WIFI whitelist list, and a pop-up window of "WIFI whitelist setting modification" will pop up, and you can change the WIFI whitelist rule information. You can change the rule name, add the SSID of the whitelist WIFI

manually, etc. After the rule is modified, the previous rule will be pushed again. The progress bar for applying the rule will change to 0 again.

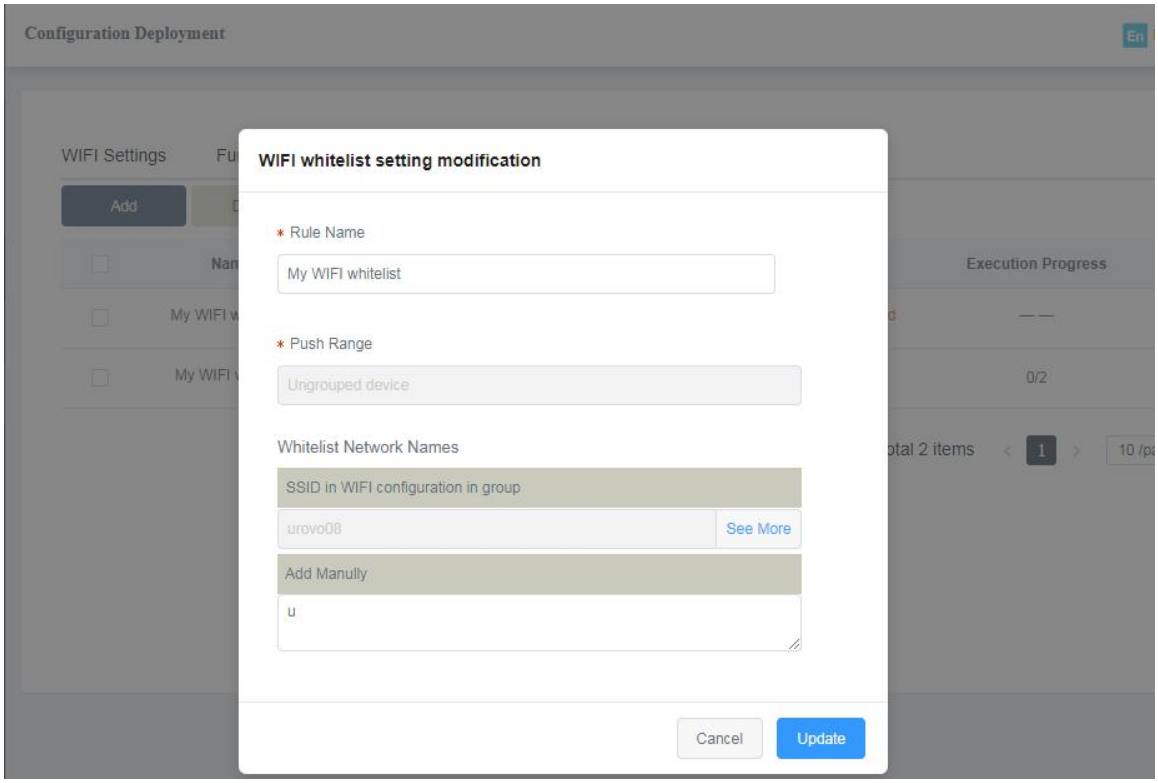


Figure (4.4.2.2.5)

Click the "View More" button in the WIFI whitelist setting modification pop-up window to check the SSID in the group WIFI configuration. These whitelist WIFI cannot be edited.

Figure (4.4.2.2.6)

4. Record

Click [Record] in the WIFI whitelist rule operation bar, and the push record table of WIFI whitelist rules will be displayed. Click [View Push Content] in the operation record table to view the details of the specific pushed WIFI whitelist rules.

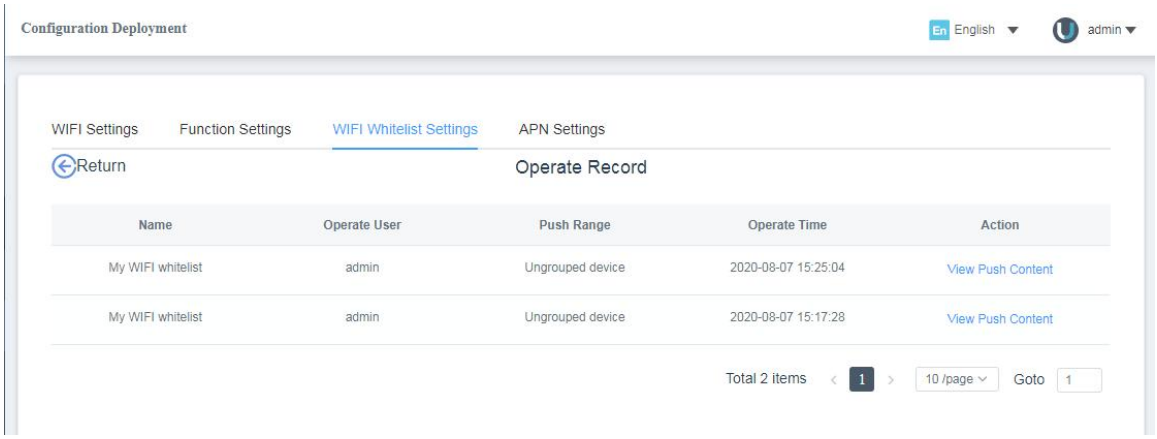


Figure (4.4.2.2.7)

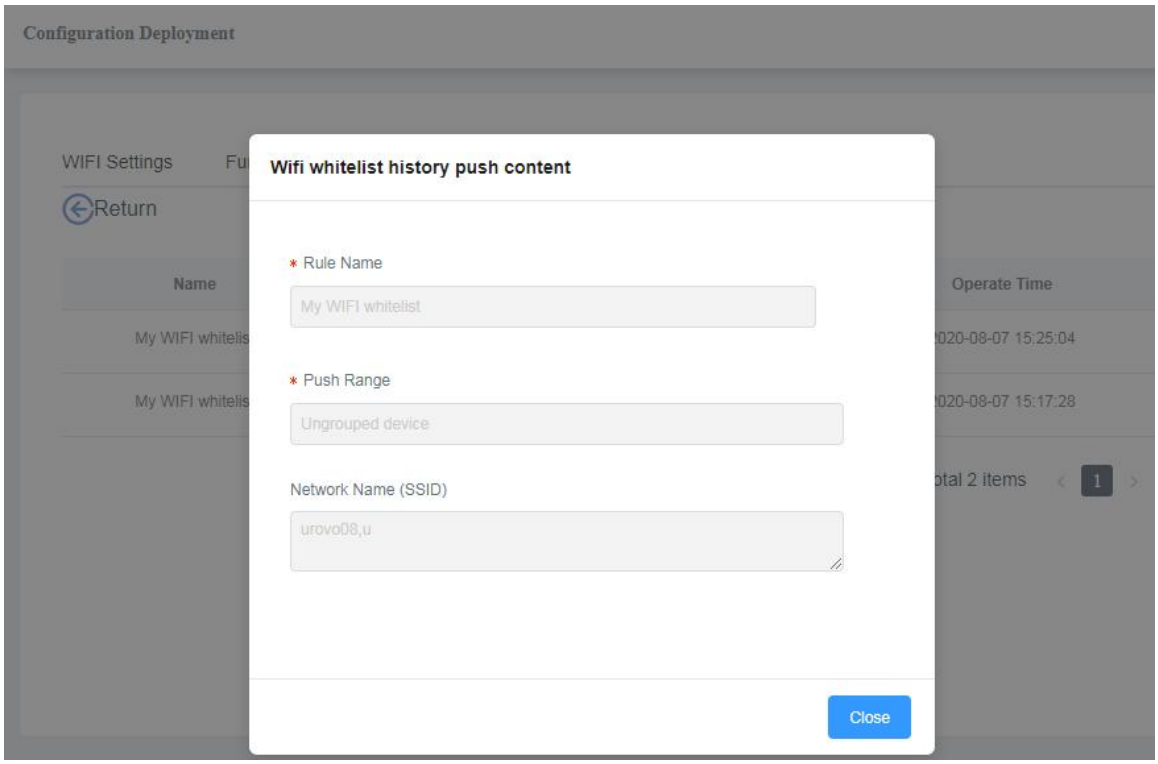


Figure (4.4.2.2.8)

5. Delete WIFI whitelist rules

Click [Delete] at the top of the WIFI whitelist list, and a delete instruction will be issued to the device. After the WIFI whitelist rule is deleted, it will not be displayed in

the WIFI whitelist list. The device will receive the delete instruction. After receiving the delete instruction, the device will change to Display all detected WIFIs.

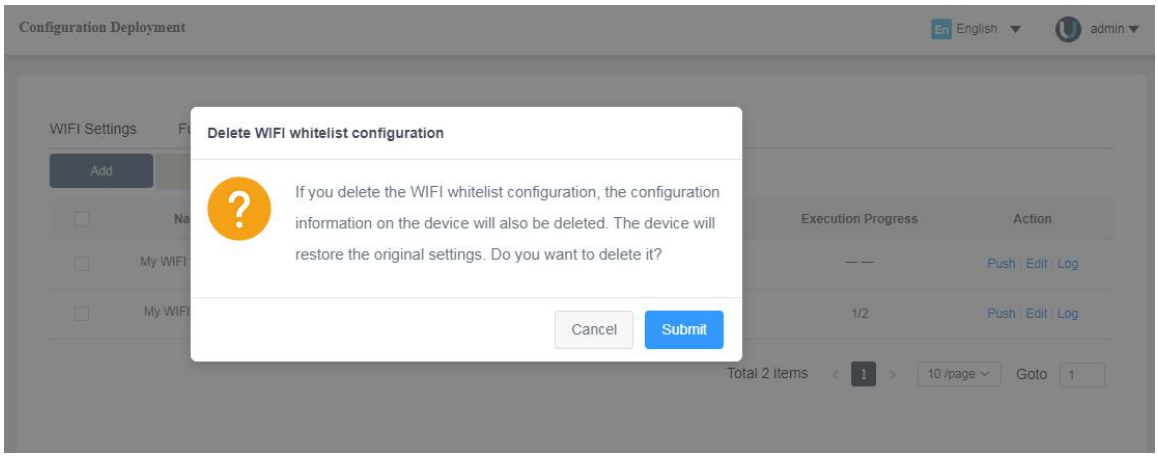


Figure (4.4.2.2.9)

4.4.2.3 Function Settings (new function)

click "Function Settings" at the top of the remote setting page, the page displays a list of function setting rules. After adding a function setting rule, push it to the device group. After receiving the function setting instruction, the devices under the device group will execute the rule to disable some items accordingly. The function setting list is shown in Figure 4.4.2.3.1:

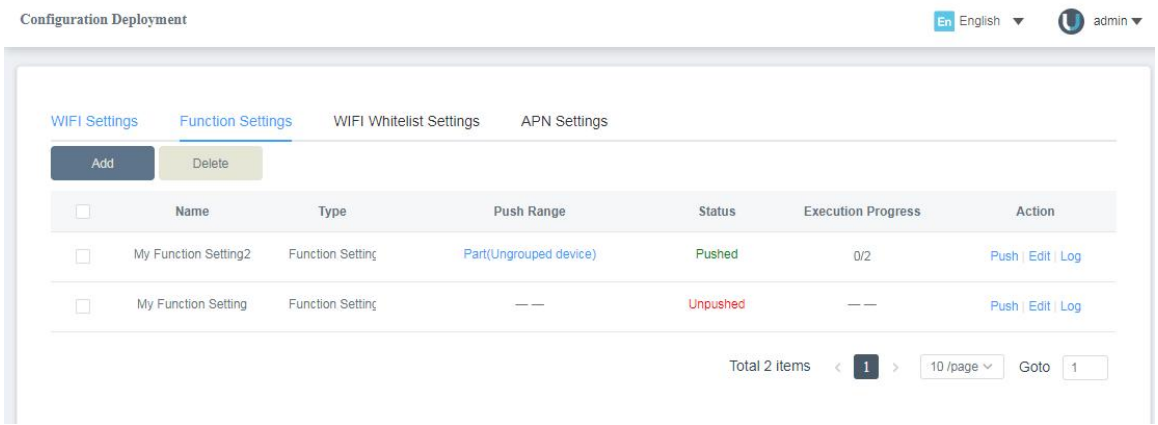


Figure (4.4.2.3.1)

1. Add function setting rules

Click [Add] above the function setting list, add the pop-up page in the function setting, enter the rule name (default: my function setting), select "Yes" for the items that need to be disabled, and then click [Add] to add deployment rules. After the rule is

successfully added, the function setting rule will be displayed in the function setting list, and the status is "not pushed";

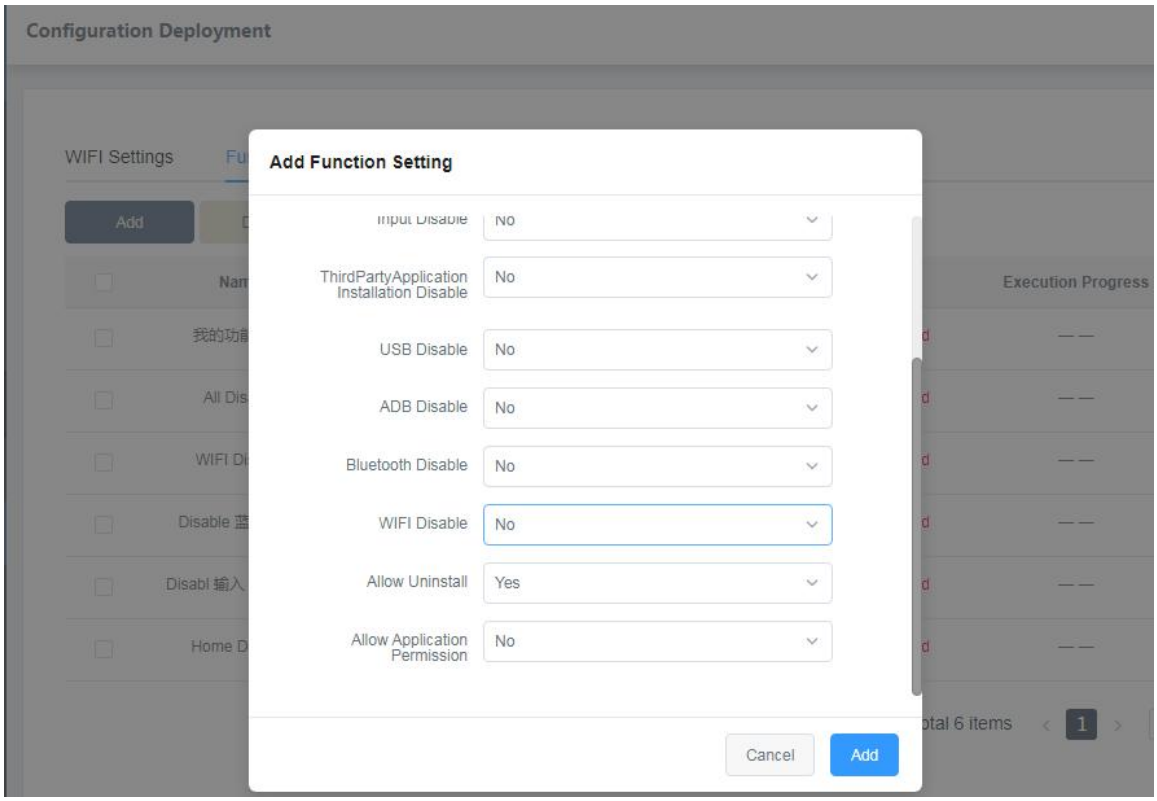


Figure (4.4.2.3.2)

Notes:

1. The rule name defaults to my function setting, and the rule name cannot be repeated;

2. When multiple function setting rules are pushed to a group, the devices under that group only apply the latest function setting rules, and the progress of the function setting rules pushed to the same group before will change to completed;

2. Push function setting rules

2.1 Group push

Click [Push] in the operation bar of the function setting rule list, a pop-up window of "Function setting push" will pop up, select the group to be pushed, and click [OK] to close the pop-up window, and the status of the function setting rule changes to "Pushed" ", the progress is 0/total number of devices. The device under the selected device group will execute this function setting rule after receiving the instruction, and the device will

correspond to the disabled item of the disabled setting.

If the device under the pushed group receives a function setting instruction, the device will display the detected function setting instruction and disable the set disabled items accordingly. The progress of this rule will increase, and the progress bar will display: Number of successfully executed devices/The total number of devices in the push group. If all the disabled function setting items are completed, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

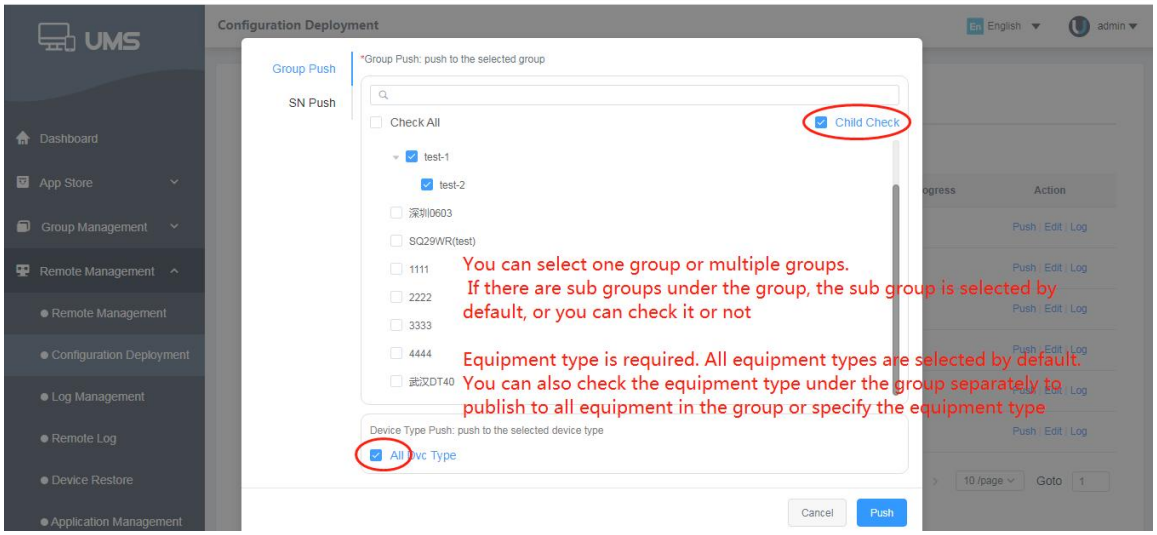


Figure (4.4.2.3.3)

2.2 SN push

Click [Push] in the operation bar of function setting rule list to pop up the window of "function setting SN push". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, the pop-up window will close, and the state of function setting rule will change to “Pushed”, and the progress is 0/number of devices pushed. After receiving the command, the devices in the selected device group will execute this function setting rule, and the devices will disable the disabled items accordingly.

If the devices in the pushed group receive the function setting command, the devices will display the detected function setting command and disable the disabled items, and the progress of the rule will increase. The progress is displayed as: Number of

successfully executed devices/Total number of devices in the pushed group. If all disabled function settings are complete, the number of successfully executed devices displayed on the progress bar is equal to the total number of devices.

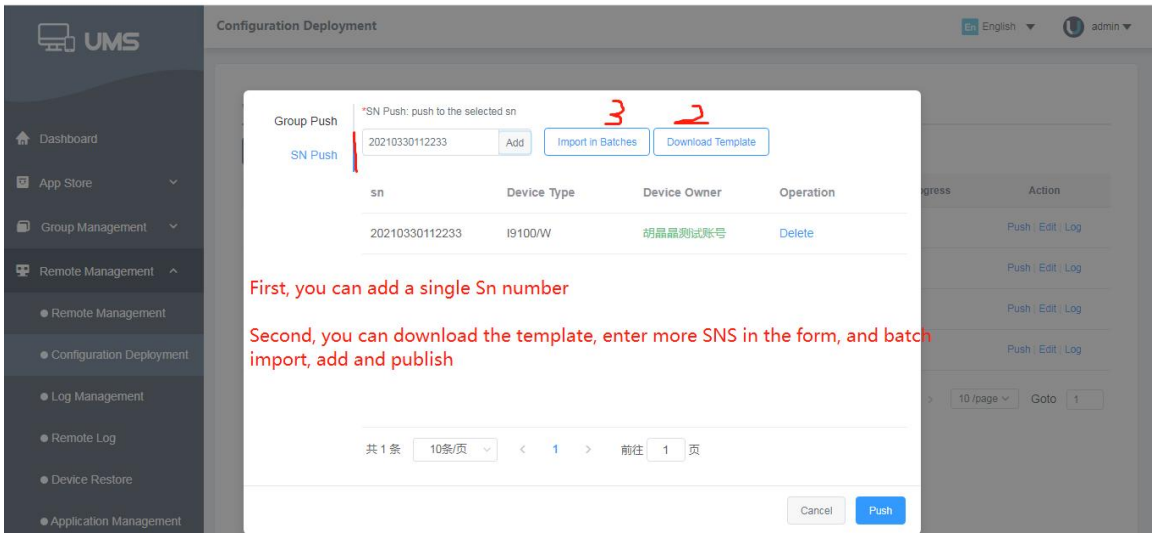


Figure (4.4.2.3.4)

3. Edit function setting rules

Click [Edit] in the operation bar of the function setting rule list, and a pop-up window of "Function Setting Modification" will pop up to change the function setting rule information. You can change the rule name, prohibited items, etc. After the rule is modified, the previous rule will be pushed again. The progress of applying the rule will become 0 again.

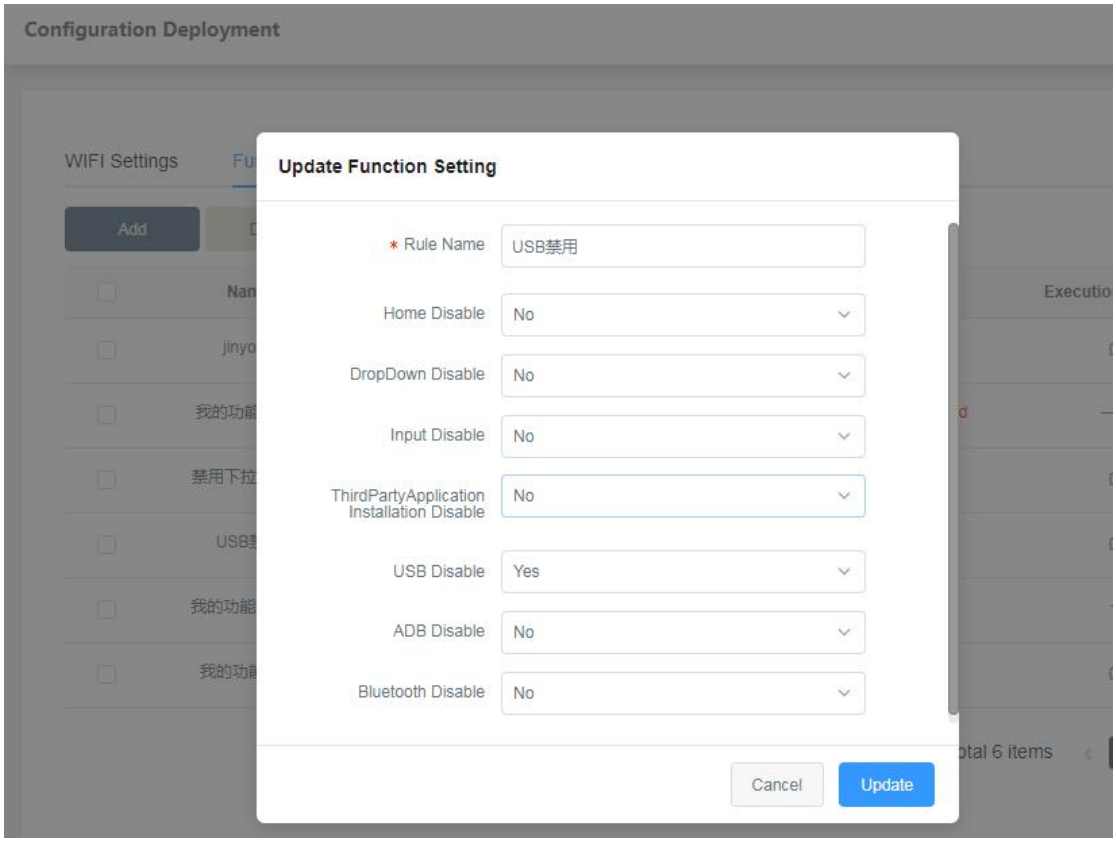


Figure (4.4.2.3.5)

4. Record

Click [Record] in the function setting rule operation bar, and the push record table of the function setting rules will be displayed. Click [View Push Content] in the operation record table to view the rules of specific push function settings.

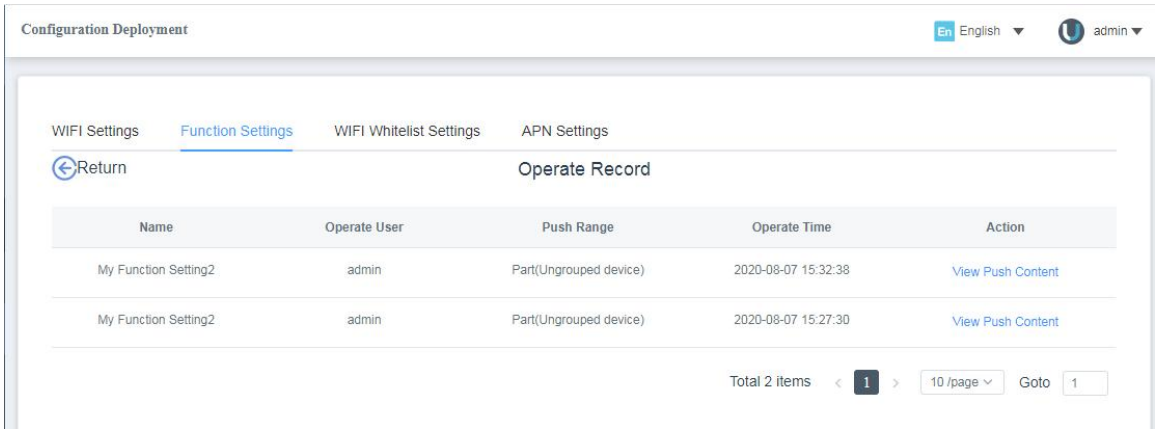


Figure (4.4.2.3.6)

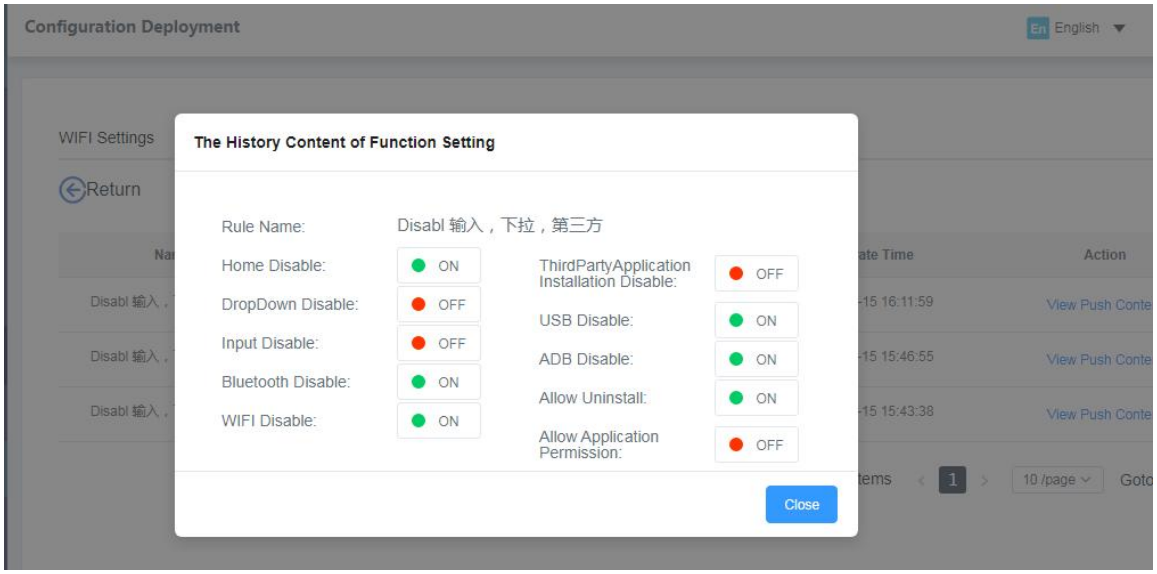


Figure (4.4.2.3.7)

5. Delete function setting rules

Click [Delete] on the top of the function setting list to issue a delete instruction to the device. After the function setting rule is deleted, it will not be displayed in the function setting list. The device will receive the delete instruction. After receiving the delete instruction, the device will not disable any disable items and restore default settings.

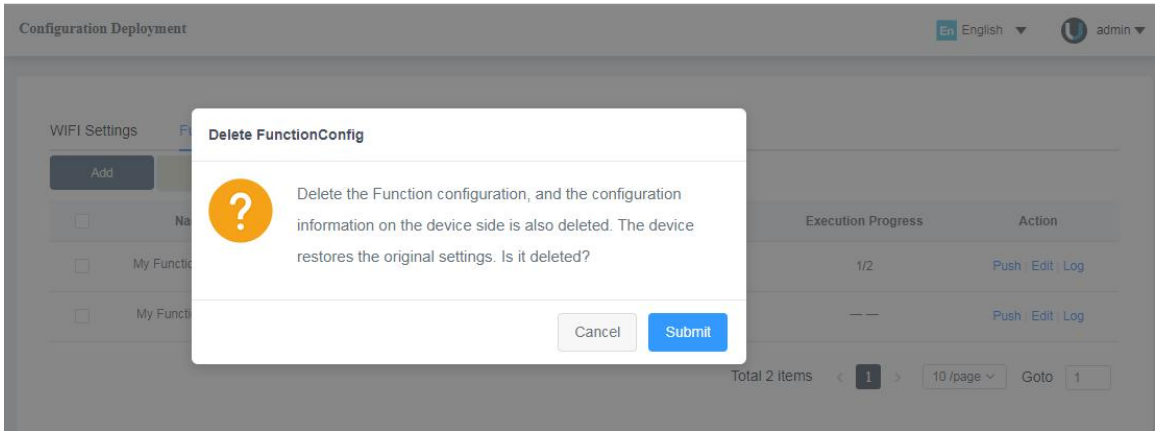


Figure (4.4.2.3.8)

4.4.2.4 APN Settings (new function)

Click “APN Settings” at the top of the remote setting page, the page displays a list of APN settings rules. After adding the APN setting rules, push it to the device group. After receiving the APN setting instruction, the devices under the device group will detect the

issued APN to save and connect. The APN setting list is shown in Figure 4.4.2.4.1:

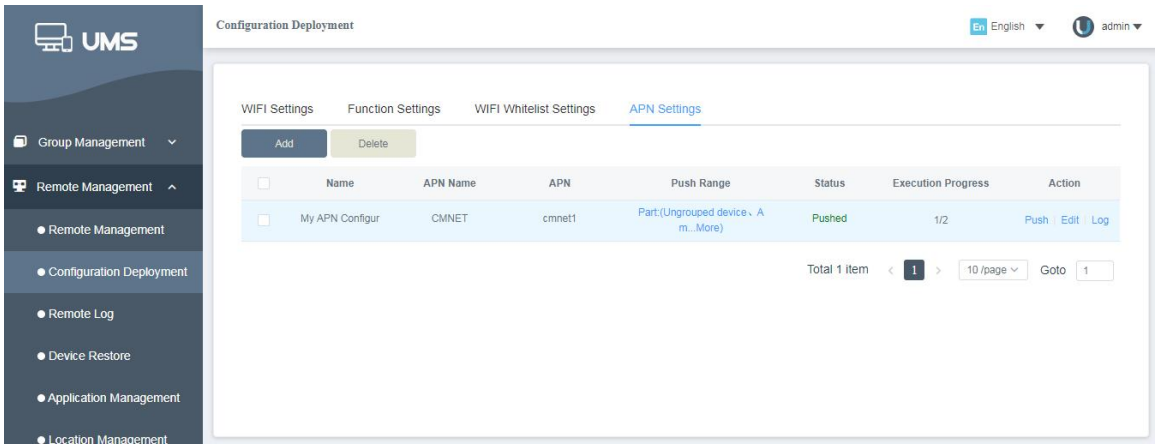


Figure (4.4.2.4.1)

1. Add APN setting rules

Click [Add] at the top of the APN settings list, in the APN settings add pop-up page, enter the rule name (default: My APN settings), APN name, APN, MCC, MNC, proxy, port, server, MMSC, MMS proxy , MMS port, authentication type, APN type, APN protocol and other information, and then click [OK], the deployment rule is added successfully, after the addition is successful, the APN setting rule will be displayed in the APN setting list, and the status is "Not Pushed";

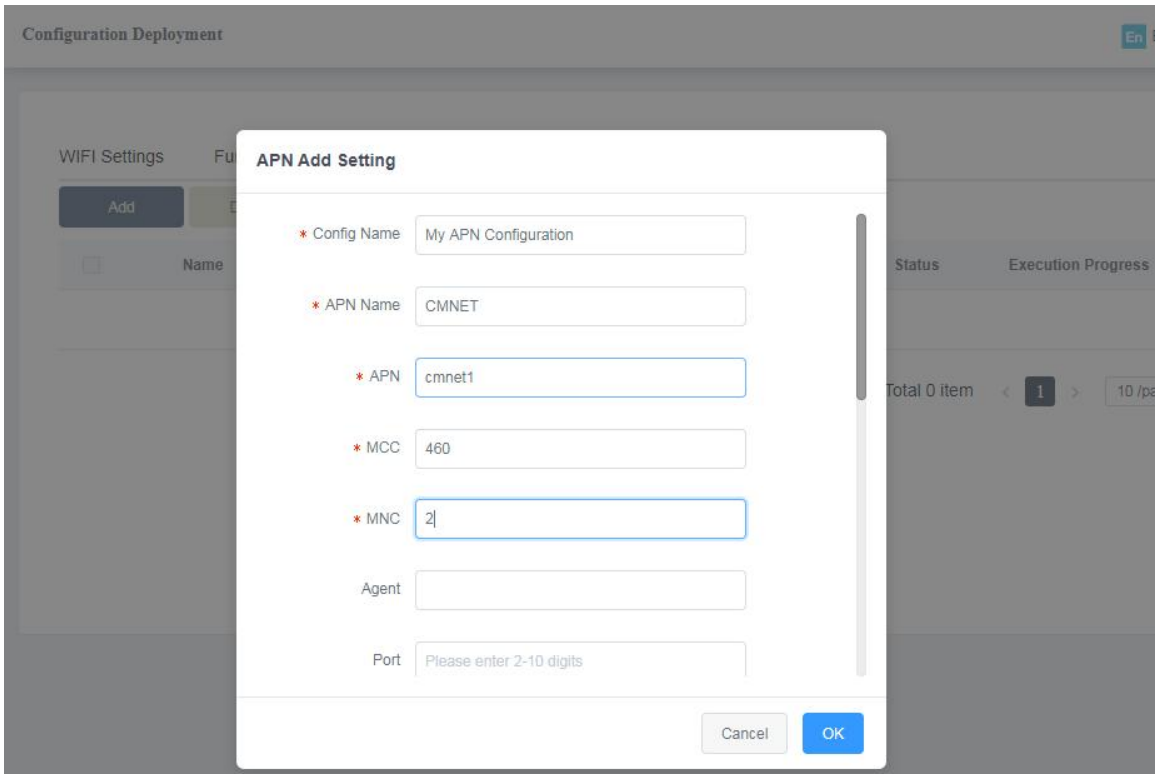


Figure (4.4.2.4.2)

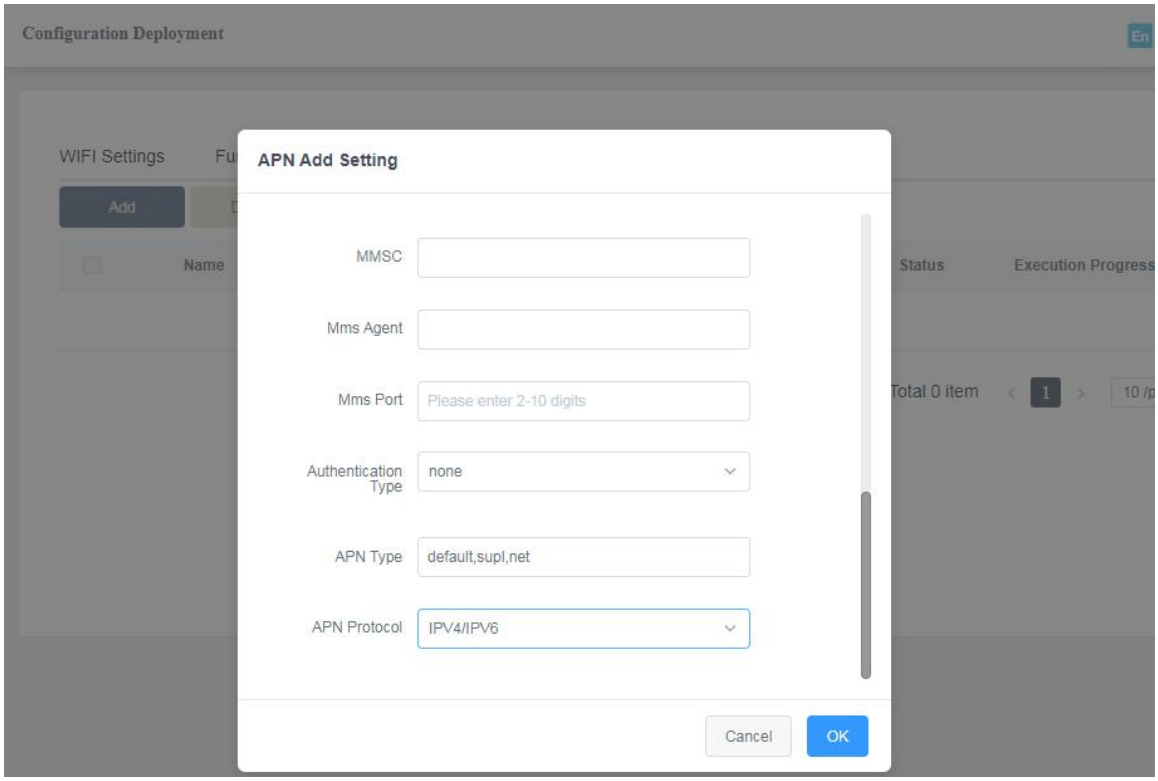


Figure (4.4.2.4.3)

Note:

1. The rule name defaults to "My APN Rule", and the rule name cannot be repeated;

2. When multiple APN setting rules are pushed to a group, multiple APNs will be saved in the APN list of the group device, but will be connected to the last executed APN;

2. Push APN setting rules

Click [Push] in the operation bar of the APN setting rule list, a pop-up window of "Select Push Range" will pop up, select the group to be pushed, click [OK], and the pop-up window will close, and the status of the APN setting rule will change to "Pushed" ", the progress is 0. The devices under the selected device group will execute this APN setting rule after receiving the instruction, and the device will save and connect after receiving the issued APN instruction.

If the device under the pushed group receives the APN setting instruction, the device will save the issued APN to the device's APN list, and connect to the latest issued APN, the progress of this rule will increase, and the progress will be displayed as: successfully executed device Number/Total number of devices of pushed groups. If the execution of

the rule is completed, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

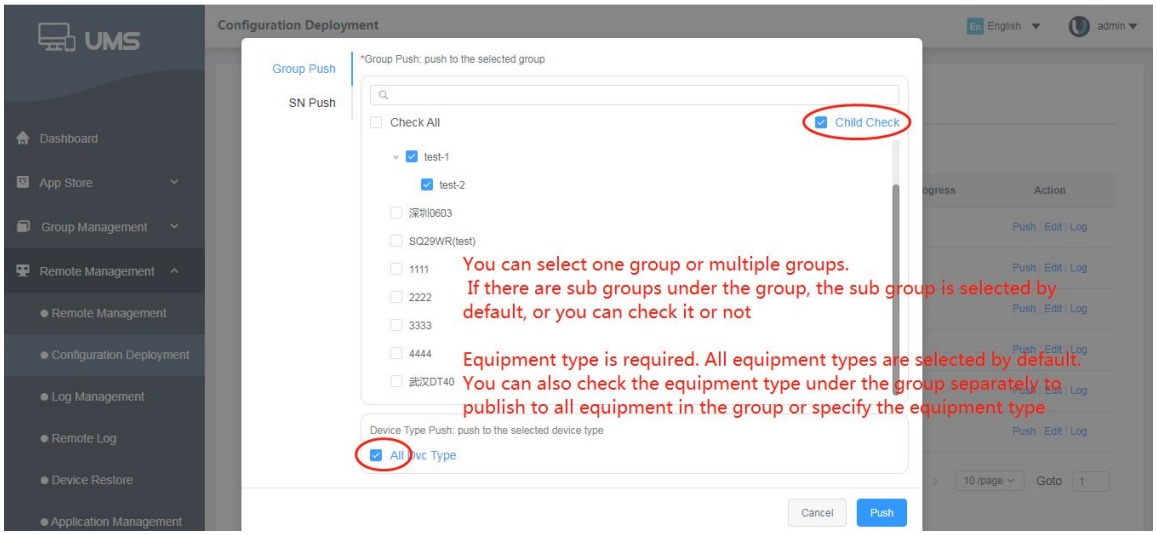


Figure (4.4.2.4.4)

2.2 SN publish and push APN

Click [Push] in the operation bar of APN setting rule list to pop up the window of "SN publish". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, The pop-up window will close, and the state of APN setting rule will change to "Pushed",and the progress is 0. After receiving the command, the devices in the selected device group will execute this APN setting rule. After receiving the APN command, the devices will be saved and connected.

If the devices in the pushed group receive the APN setting command, the devices will save the published APN to the APN list of the devices and connect to the latest APN, the progress of this rule will increase. The progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If the rule is executed, the number of successfully executed devices displayed in the progress bar is equal to the total number of devices.

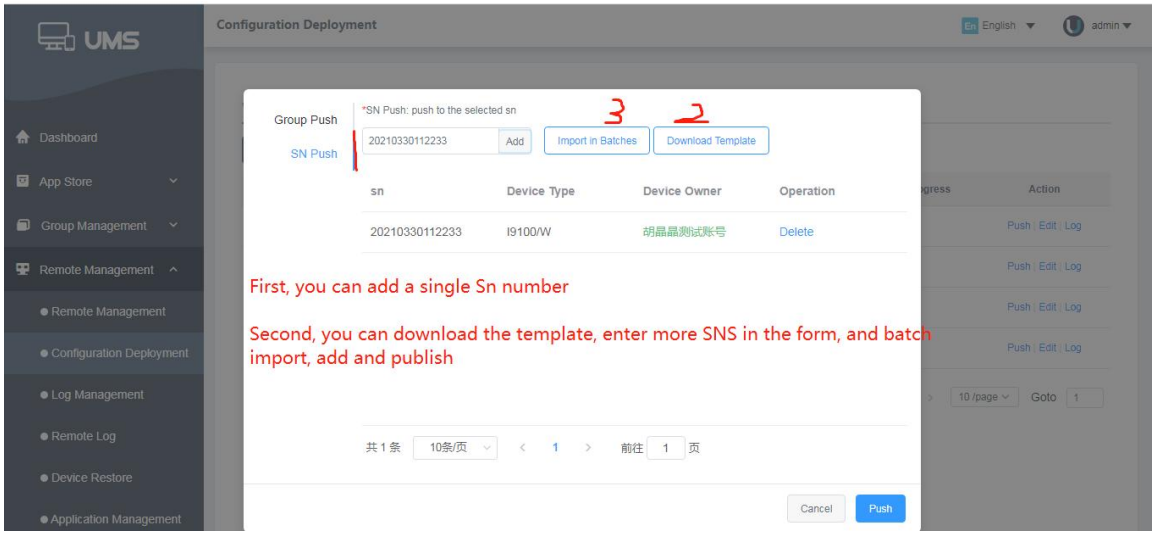


Figure (4.4.2.4.5)

3. Edit APN setting rules

Click [Edit] in the operation bar of the APN setting rule list, a pop-up window of "APN Setting Edit" will pop up, and you can change the APN setting rule information. You can change the rule name, input items, etc. After modifying the rule, the previous rule will be pushed again. The progress bar of the APN rule will change to 0 again.

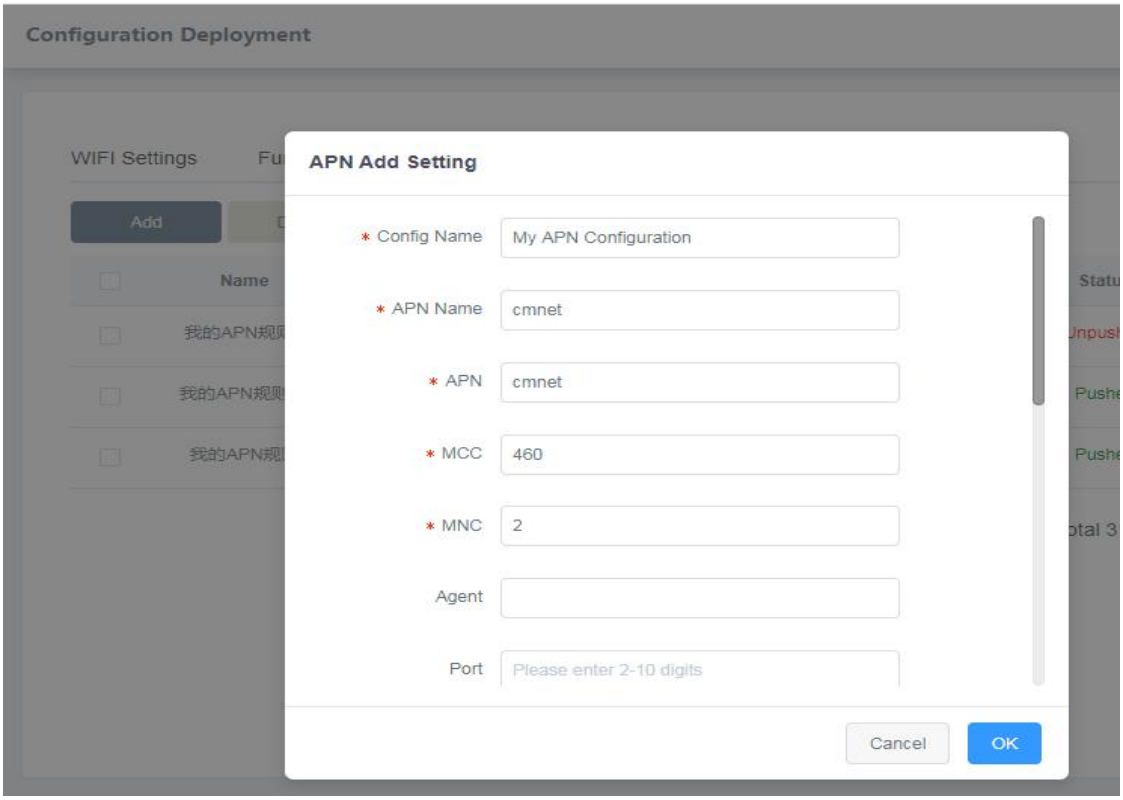


Figure (4.4.2.4.6)

4. Record

Click [Record] in the operation bar of the APN setting rule, and the push record table of the APN setting rule will be displayed. Click [View Push Content] in the operation record table to view the details of the specific push APN setting rule.

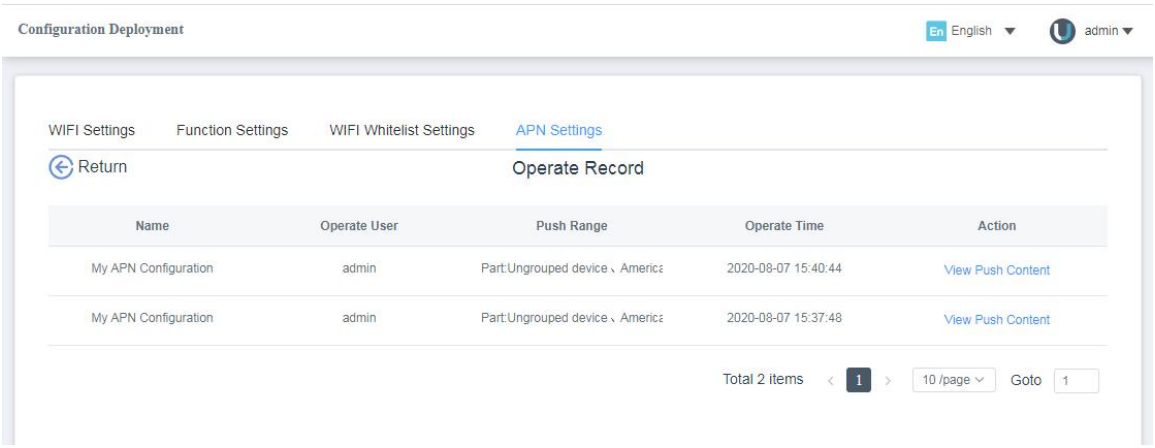


Figure (4.4.2.4.7)

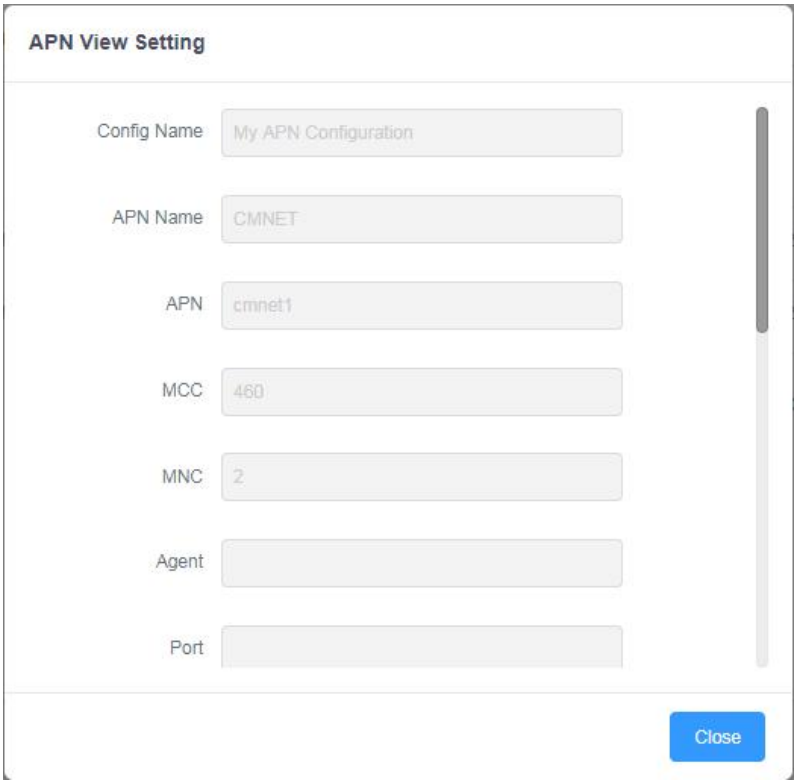


Figure (4.4.2.4.8)

5. Delete APN setting rules

Click [Delete] on the top of the APN setting list, and a delete instruction will be issued to the device. After the APN setting rule is deleted, it will not be displayed in the APN setting list. The device will receive the delete instruction. After receiving the delete

instruction, the device will delete those APN issued by this rule, and restore the connection of the default

APN.

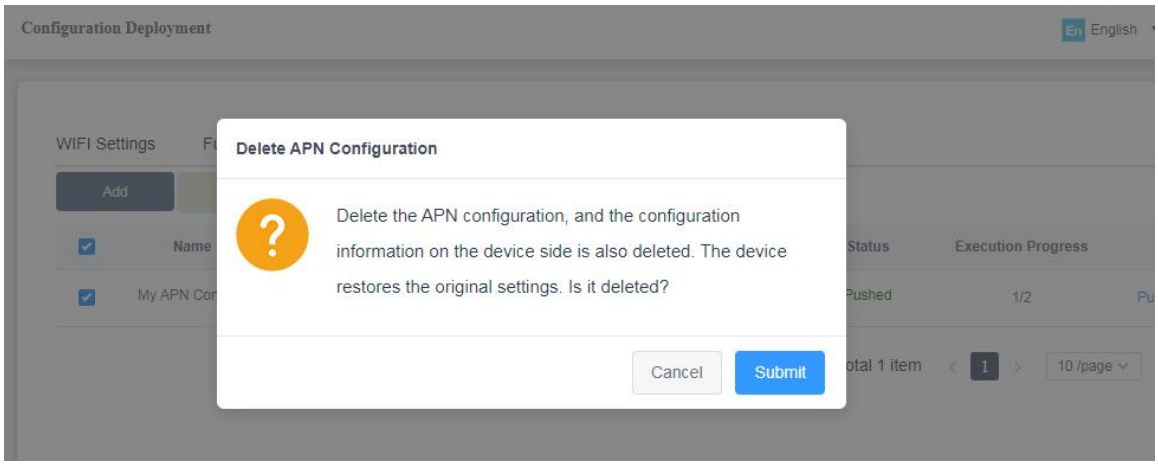


Figure (4.4.2.4.9)

Notes:

After deleting an APN, other APNs issued before will not be deleted;

4.4.2.5 Send script (new function)

Click "Send Script" at the top of the remote setting page to display the list of sending script rules. After adding the sending script rules, push it to the device group. After receiving the sending script instruction, the devices under the device group will execute the sending script rules and display it on the device page. The sending script list is shown in Figure 4.4.2.5.1.

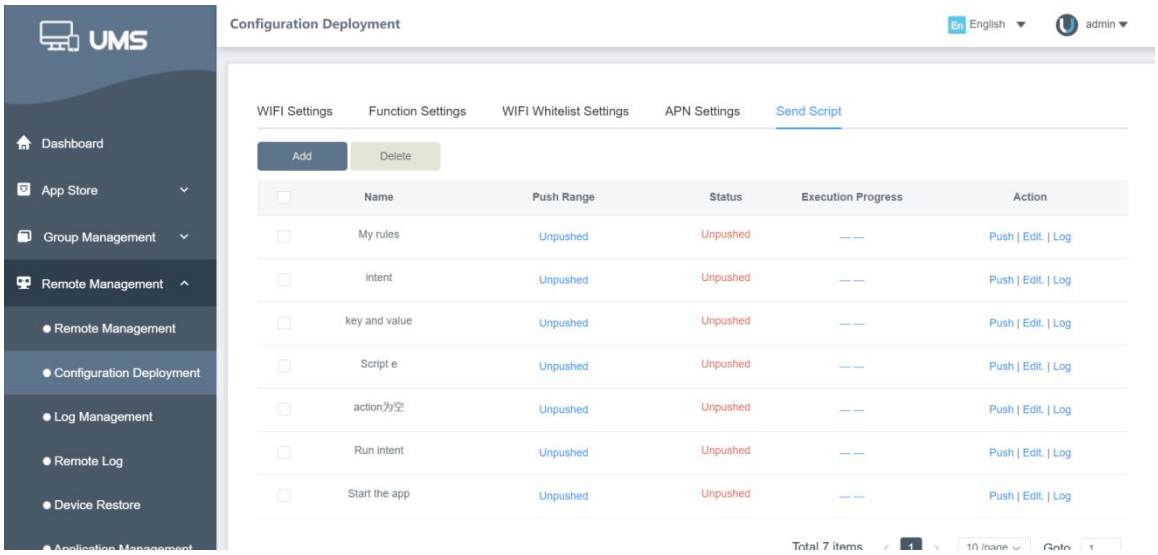


Figure (4.4.2.5.1)

1. Add sending script rules

Click [Add] at the top of the Sending Script list, add pop-up page on the Send Script, enter the rule name, select the Execute Script option (default: start application), enter the required Action or the application package name and application class name, and enter the script content (optional), and then click [Save] to add the sending script rules successfully. After adding successfully, the sending script rules will be displayed in the Send Script list with the status of "Un-pushed";

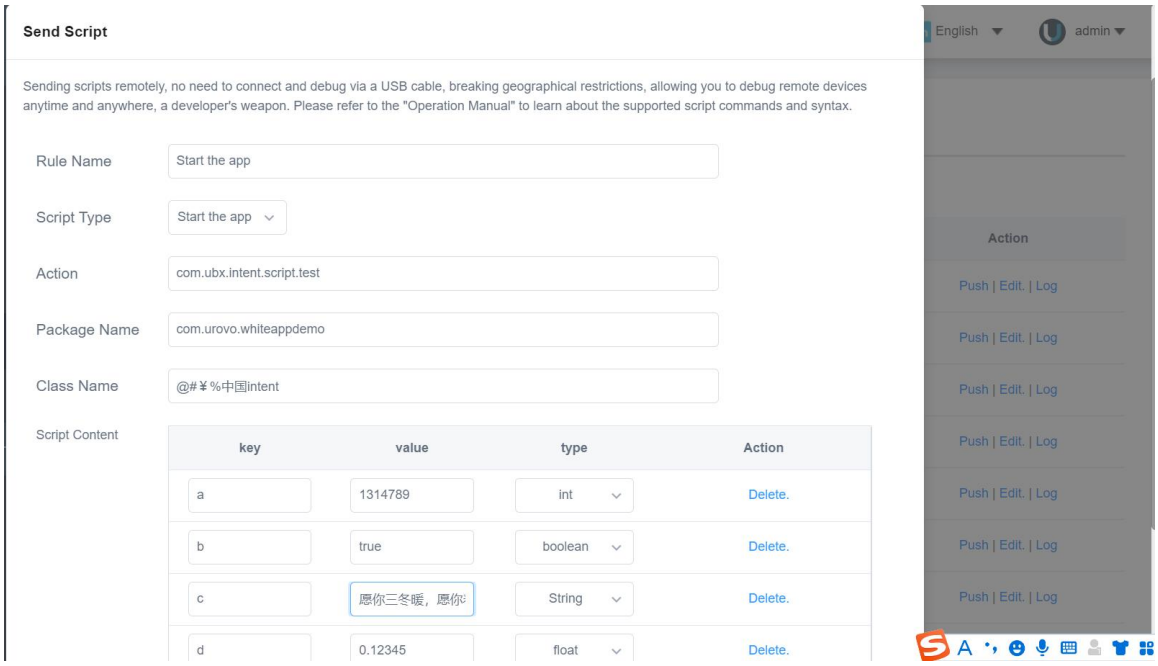


Figure (4.4.2.5.2)

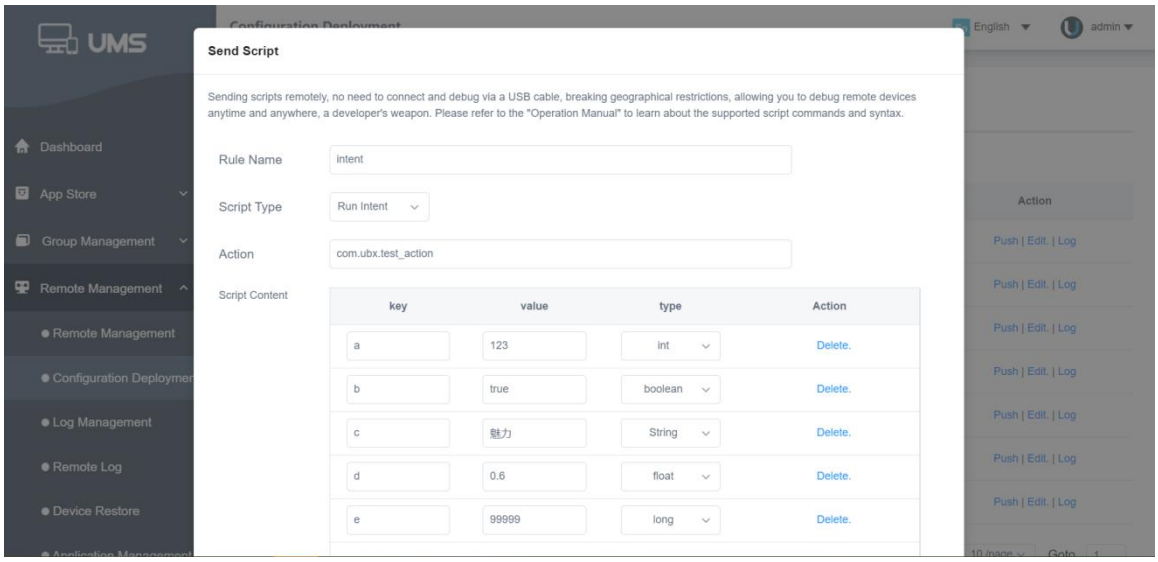


Figure (4.4.2.5.3)

Note:

1. Rule name cannot be repeated;

2. Execute Script options are: ①Start APP, ②Run intent;

3. Start APP is Action or (application package name, application class name), optional; Action in the running intent is required. The terminal will start the application only after the Action or (package name, class name) is written into the program. If it is not written into the program, the device will not start the application; running intent must register the broadcast on the page after the application is started, and the program that registers the corresponding Action can receive the corresponding message;

4. The script content can be filled in the values of Key and Value, and select the Type, for example

(①Key is a，value is 123，Type is int;

②key is b，value is true，Type is Boolean;

③key is c，value is motherland，Type is String;

④key is d，value is 0.888，Type is float;

⑤key is e，value is 11111111，Type is long)

Regardless of whether the script content is entered or not, the program will get it. If there is no corresponding parameter, there will be a default value.

2.Push the sending script rules

2.1 Group push

Click [Push] in the operation bar of the sending script rule list, a pop-up window of "Push Management" will pop up, check the group to be pushed, click [OK] to close the pop-up window. The status of the sending script rules will change to "Pushed", and the progress is 0/total number of devices. The device under the selected device group will execute this function setting rule after receiving the instruction, and the device will start the corresponding program.

If the device under the pushed group receives the sending script instruction, the terminal device will start the corresponding startup program after the device displays the detected sending script instruction, the progress of this rule will increase. The progress bar is displayed as: the number of devices successfully executed/the total number of devices in the pushed group. If the execution of the rule is completed, the number of devices successfully executed displayed in the progress bar will be equal to the total number of devices.

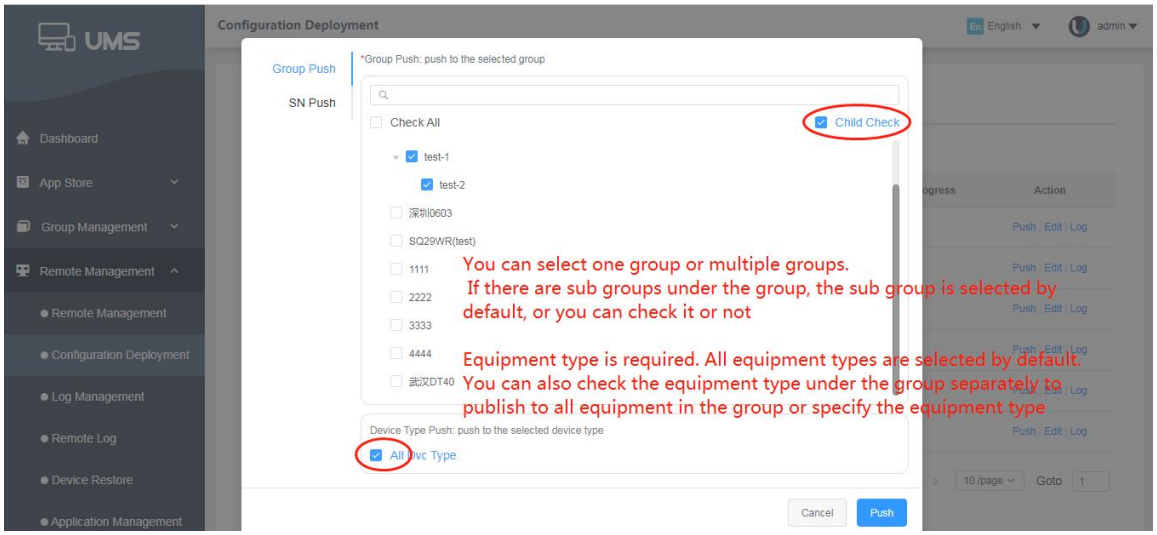


Figure (4.4.2.5.4)

2.2 SN publish and push APN

Click [Push] in the operation bar of APN setting rule list to pop up the window of "SN publish". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, The pop-up window will close, and the state of APN setting rule will change to "Pushed",and the progress is 0. After receiving the command, the devices in the selected device group will execute this APN

setting rule. After receiving the APN command, the devices will be saved and connected.

If the devices in the pushed group receive the APN setting command, the devices will save the published APN to the APN list of the devices and connect to the latest APN, the progress of this rule will increase. The progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If the rule is executed, the number of successfully executed devices displayed in the progress bar is equal to the total number of devices.

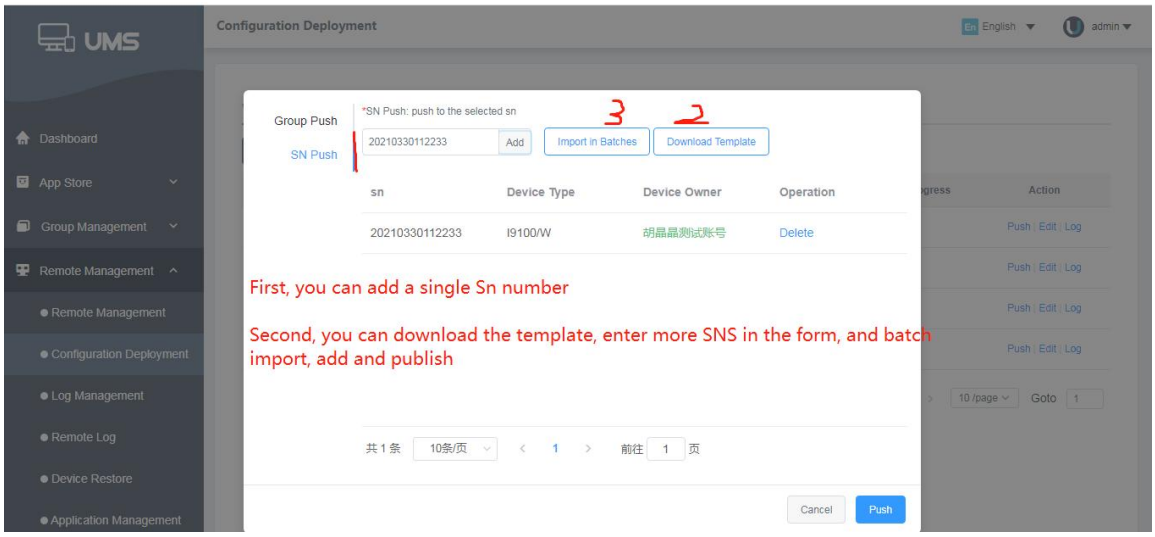


Figure (4.4.2.4.5)

3. Edit sending script rules

Click [Edit] in the operation bar of the sending script rule list, a pop-up window of "Edit the Sending Script" will pop up, where the sending script rule information can be changed. The Rule Name, Execute Script, Action and other input items, etc. can be changed. After the rule is modified, the previous rule will be pushed again. The progress bar of sending script rules will change to 0 again.

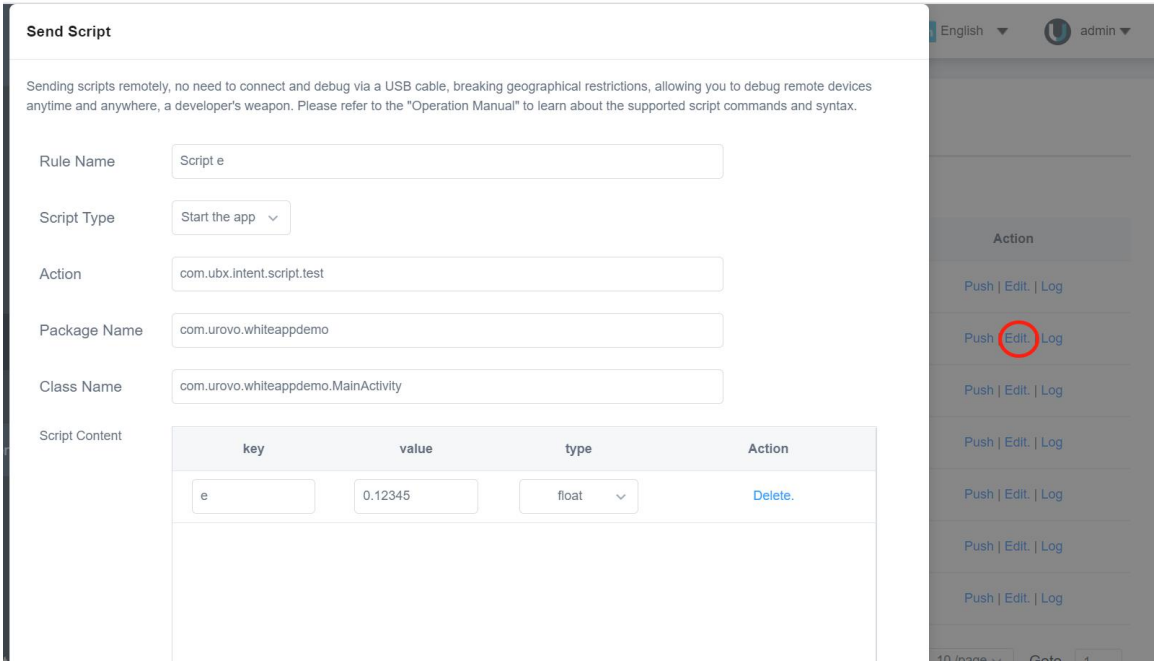


Figure (4.4.2.5.6)

4. Record

Click [Record] in the operation bar of the sending script rules, and the push record table of the sending script rules will be displayed. Click [View Push Content] in the operation record table to view the details of the specific push sending script rules.

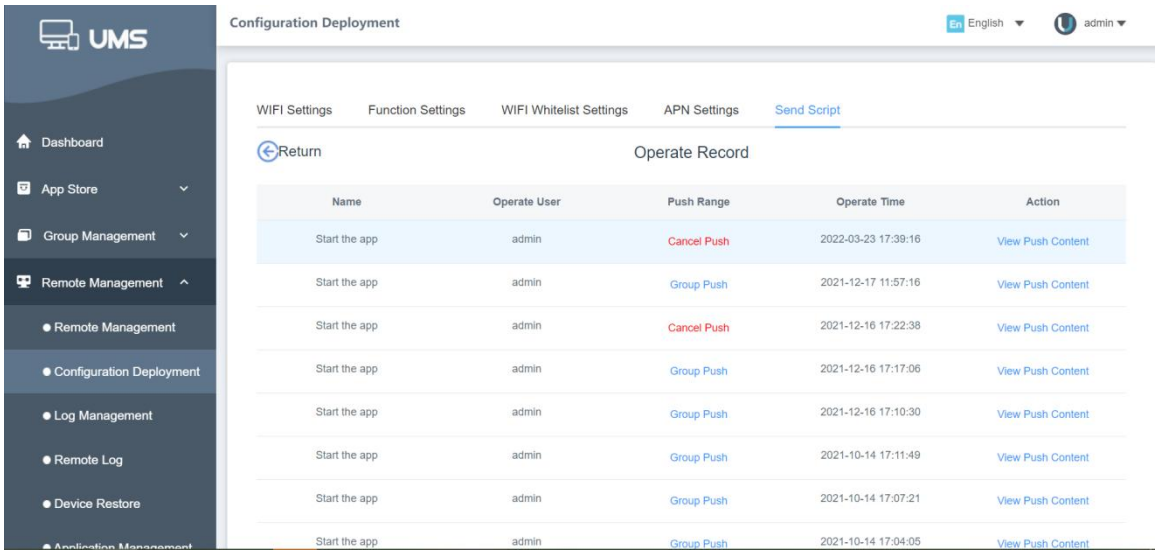


Figure (4.4.2.5.7)

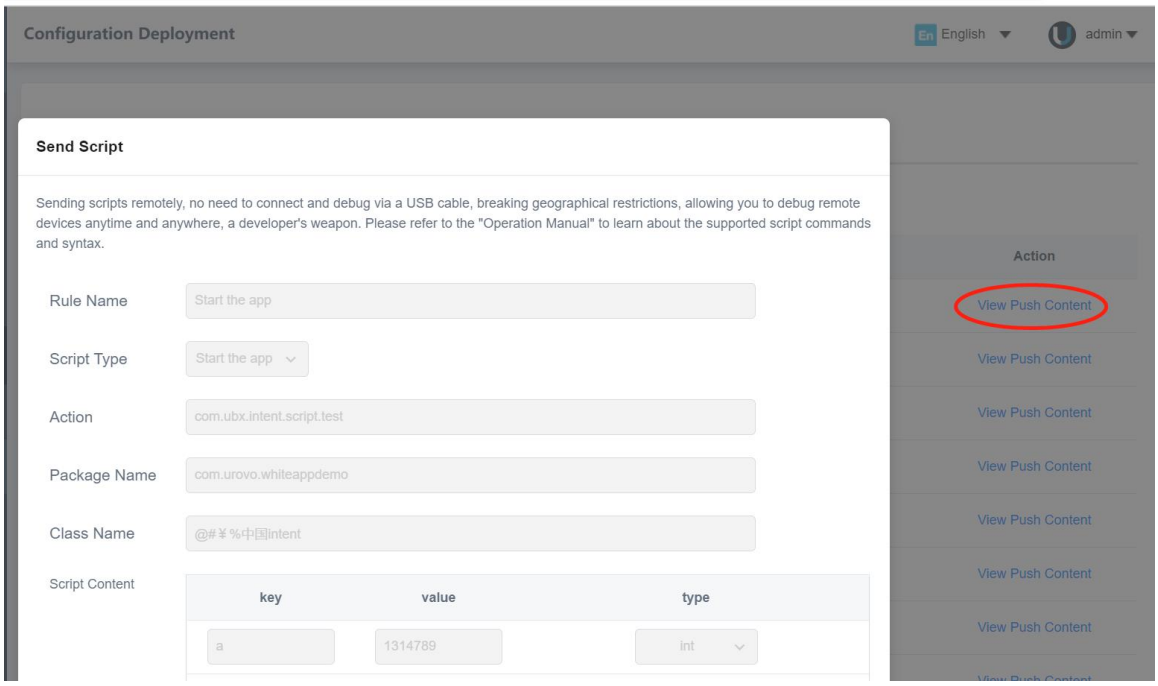


Figure (4.4.2.5.8)

5. Delete the sending script rules

Click [Delete] on the top of the sending script list, and a deletion instruction will be issued to the device. After the sending script rule is deleted, it will not be displayed in the sending script list. The device will receive the delete instruction. After receiving the delete instruction, the device will delete the sending script issued by this rule. The device page that has been pushed and executed will also display the sending script content, which cannot be restored and needs to manually return to the Android default desktop.

4.4.3 Log Management (new function)

Select [Remote Management] - [Log Management] on the menu bar to display the device log extraction rule list on the log management page. After adding a new log task, it is pushed to the device group. After receiving a new log task, the device in the device

group extracts logs from the new log task. The log management list is shown in Figure 4.4.3 below:

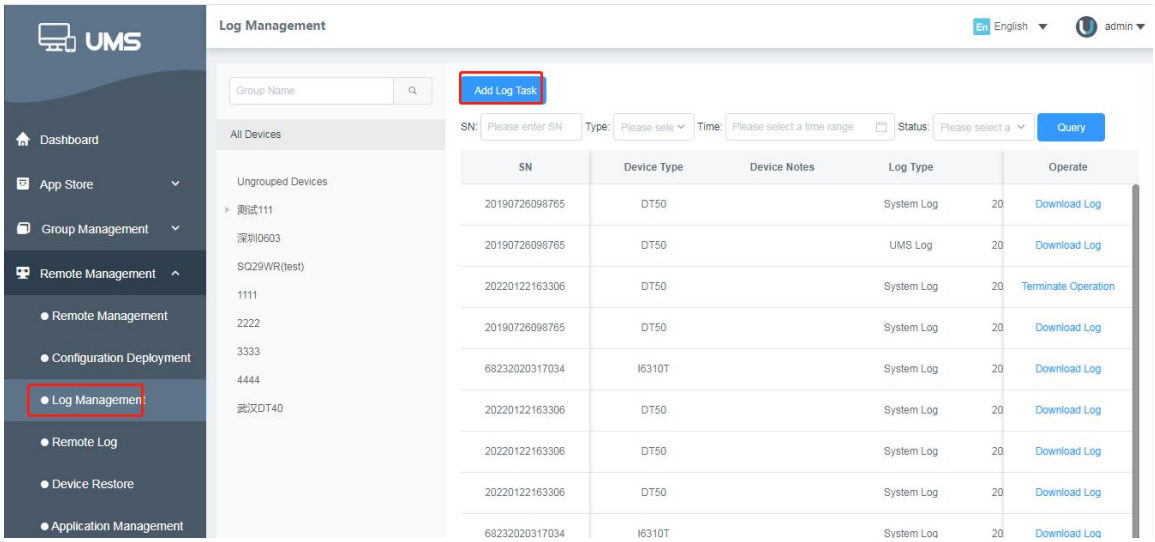


Figure (4.4.3)

New log task

On the log management page, you can select all devices or a group to perform [New Log Task]. Click [New Log Task] to pop up the window of [Extract Device Log], and select devices to add, as shown in the Figure below:

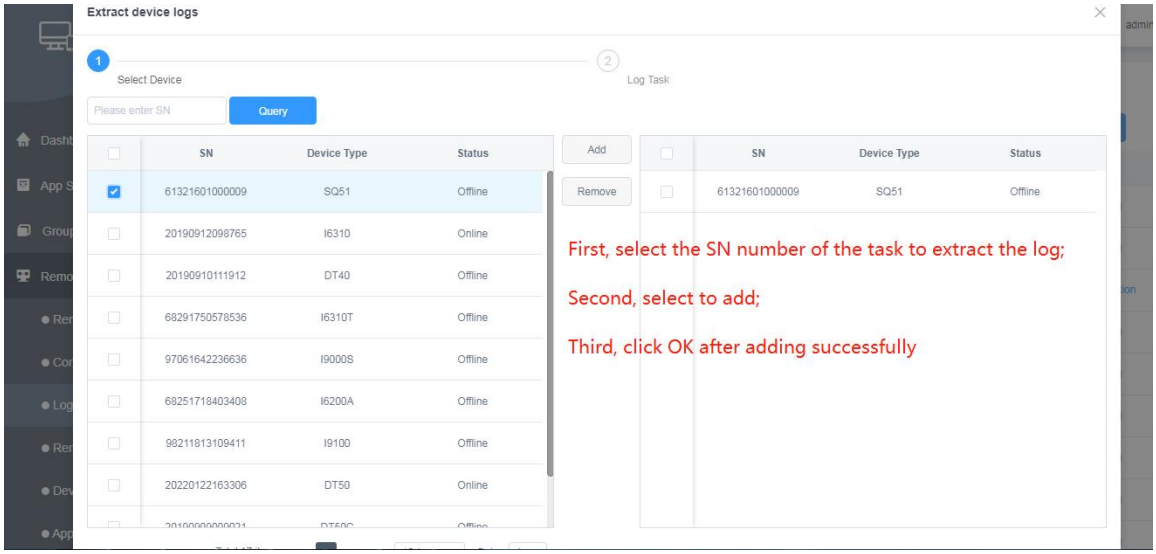


Figure (4.4.3)

1.1 Extract UMS log

Select a log type in the pop-up window. The default is UMS log. Click [OK] to extract the file under uhome/log and upload it to the "Log Management" list for users to download;

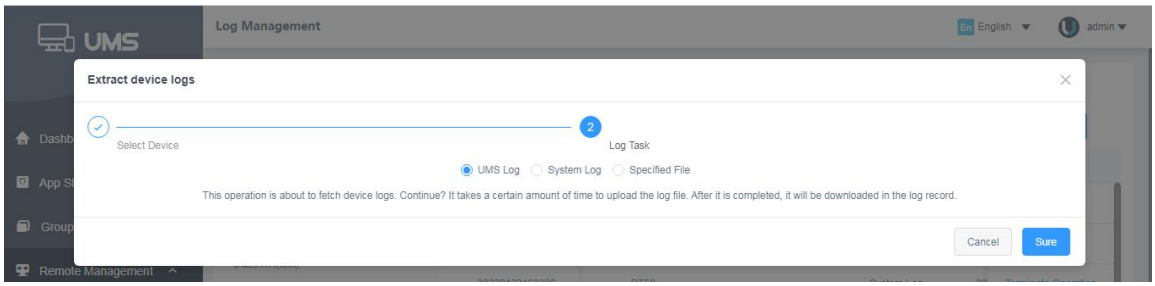


Figure (4.4.3.1)

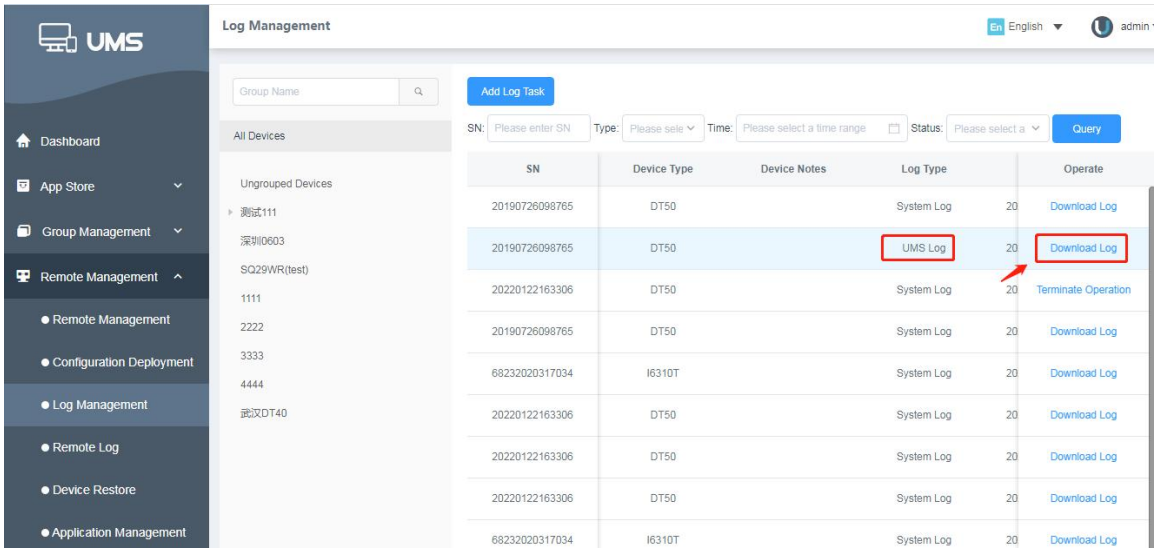


Figure (4.4.3.2)

1.2 Extract system log

Select a log type in the pop-up window. Select to extract the system log, click the time range, enter the duration, check the file rule, and then click [OK]. You can enable the system log function remotely and disable it periodically. Logs generated during this period are automatically uploaded to the background and uploaded to the "Log Management" list for users to download.

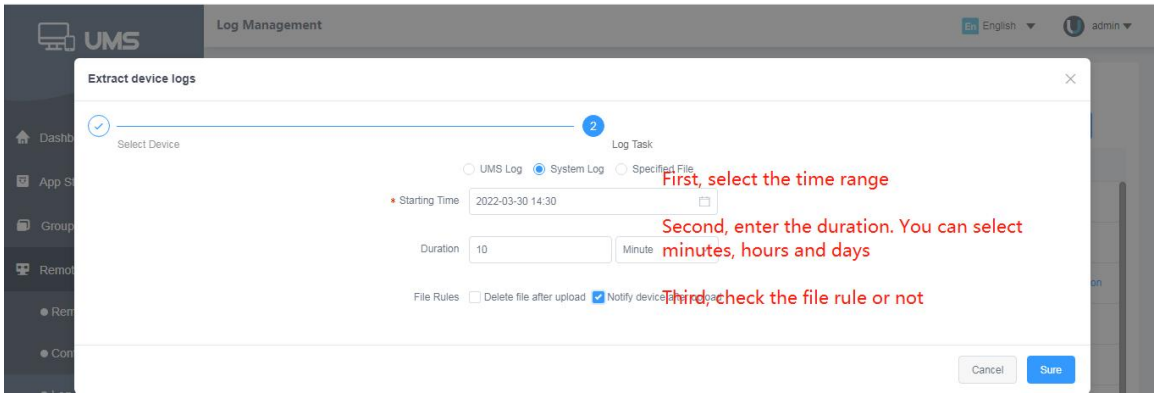


Figure (4.4.3.3)

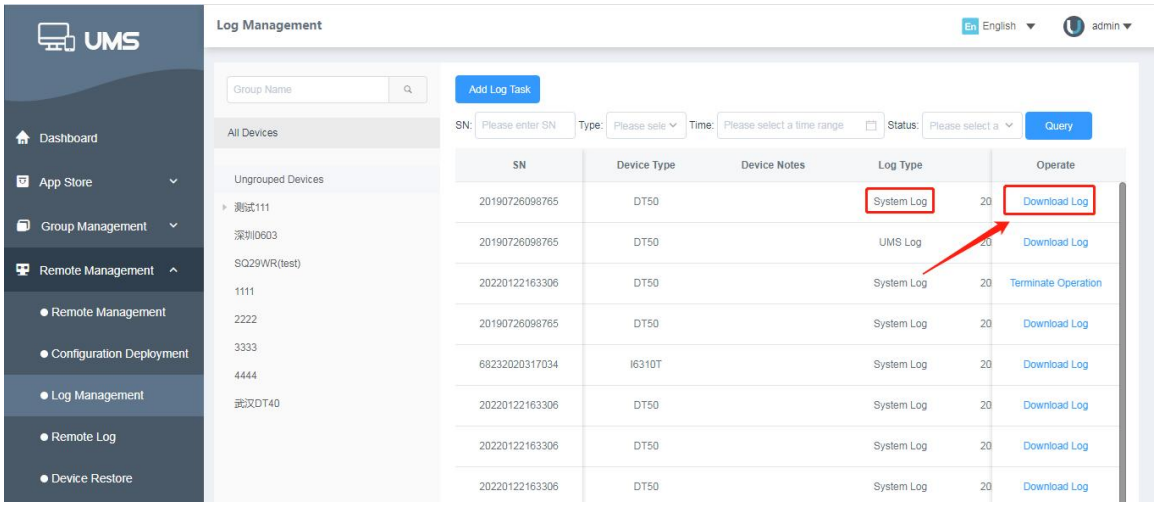


Figure (4.4.3.4)

1.3 Extract specified file

Select a log type in the pop-up window. Select to extract the specified file, enter the target path in the correct format, and click [OK] to extract the specified directory file, and download the file in the "Log Management" list. If the specified directory does not exist or is empty, "Execution failed" is recorded in the use record, and the status is "The file does not exist".

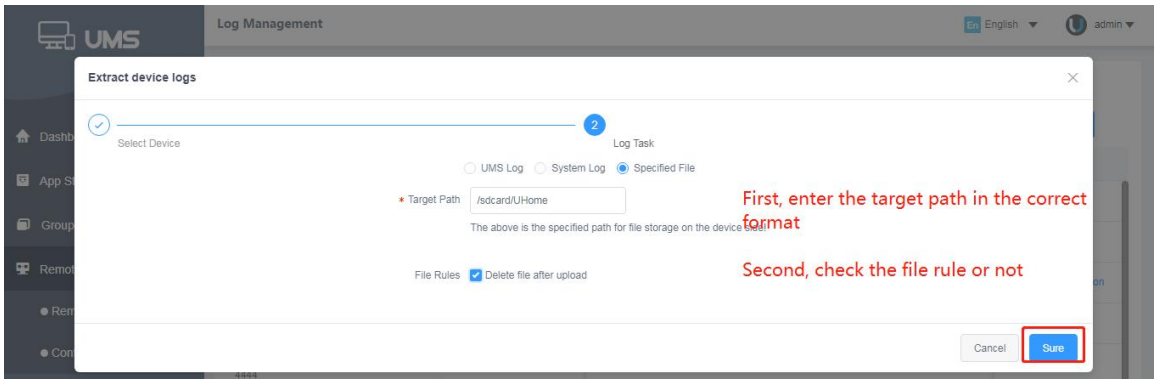


Figure (4.4.3.5)

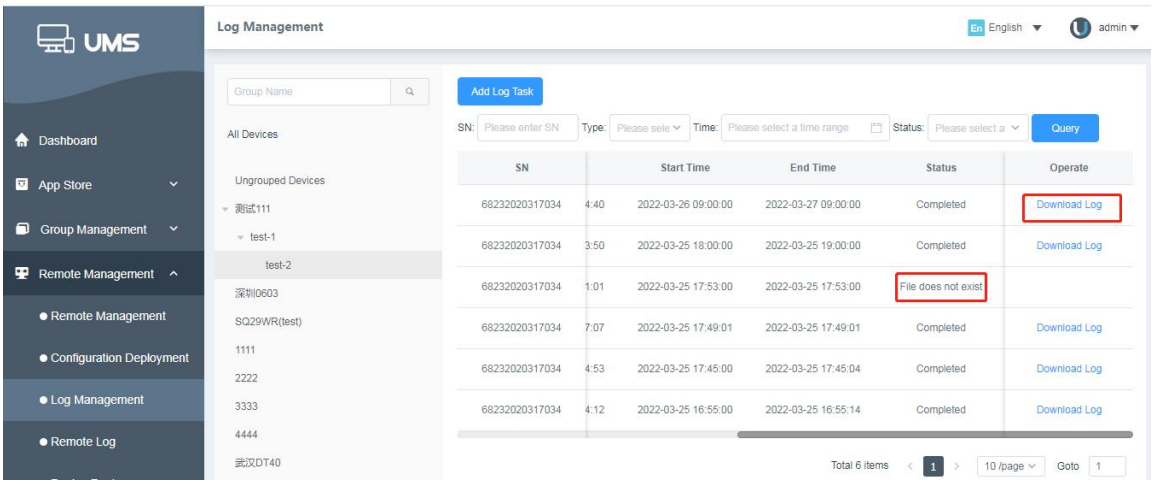


Figure (4.4.3.6)

4.4.4 Remote Log

Click [Remote Management] – [Remote Record], using the records page to display the logs and execution progress of remote batch operations, as shown in the image below:

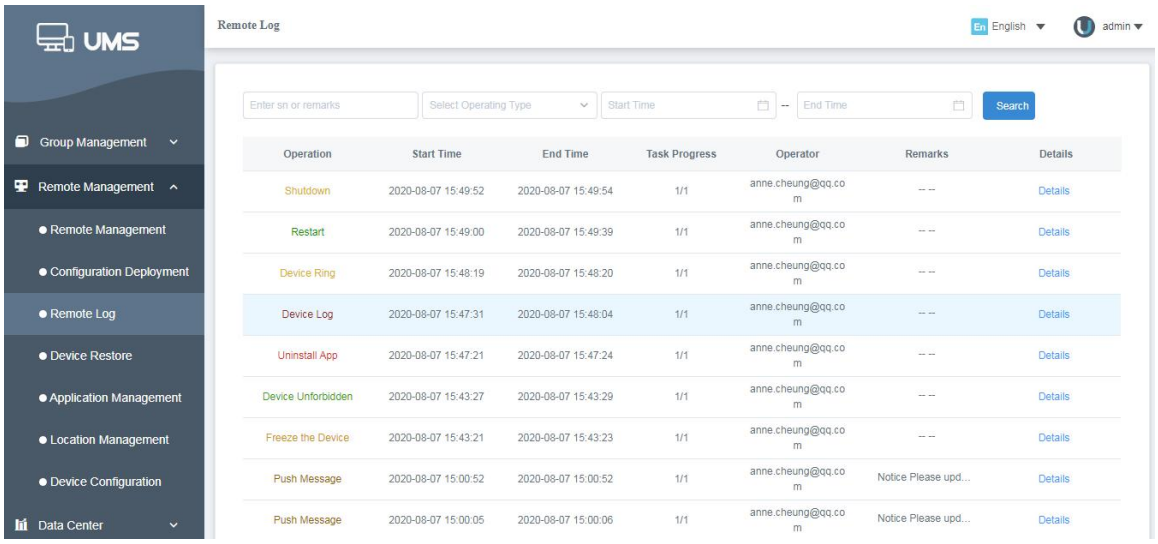


Figure (4.4.4.1)

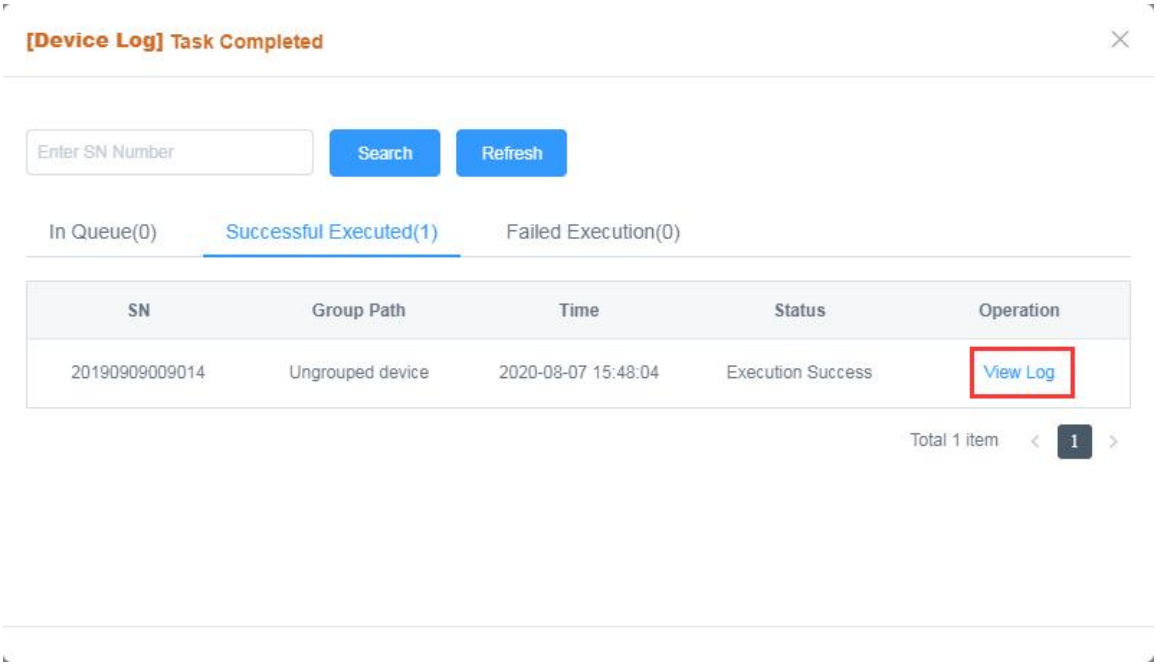


Figure (4.4.4.2)

1. Input SN, select the type of operation, input the start time and the end time, and click [Query] to query about the corresponding records, including operations, time, execution progress, etc.
2. Click [Details] in the list details column to view the execution status of a specific instruction.
3. Click [View Log] on the “Device Log” details page to download the log files.

4.4.5 Device Restore

In the figure (4.5), click [Remote Management]-[Device Restore], the device restore page displays a list of activated devices for this account, and you can "clear lock screen password" or "restore factory settings" for the devices of this account, As shown below:

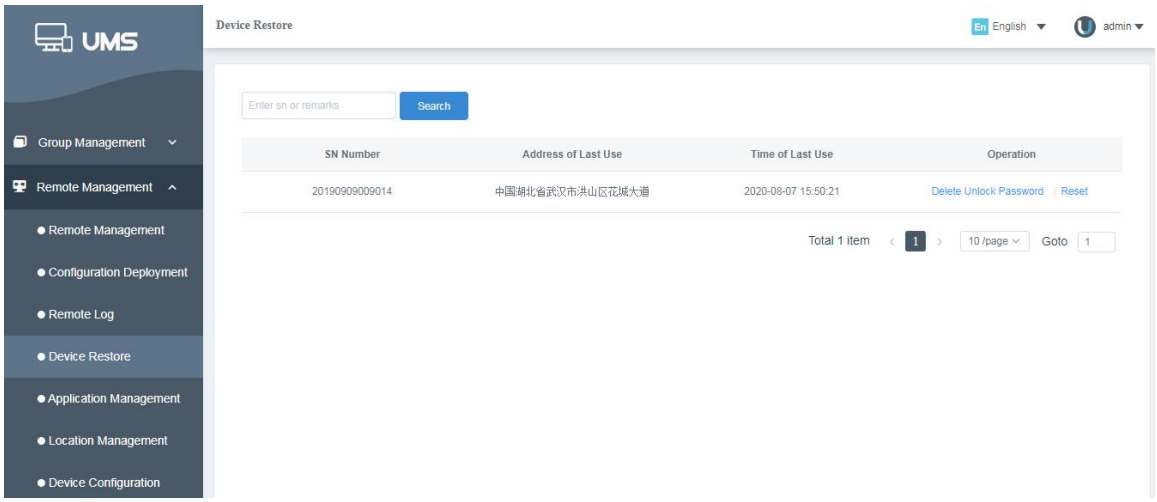


Figure (4.4.5.1)

1. Clear the lock screen password: Click the [Clear lock screen password] button in the operation bar to clear the password for the selected device. If the device has set a lock screen password, you can clear the password and change to slide to unlock;

2. Restore factory settings: Click the [Restore Factory Settings] button in the operation bar to restore the selected device to factory settings. After the device is restored to factory settings, the applications and data on the device will be cleared. This function should be used with caution;

4.4.6 Application Management

Click [Remote Management]-[Application Management] as shown in Figure (4.4), the upper page will display Application Deployment and Application Whitelist menu. Click the menu to enter respective page.

4.4.6.1 Application Deployment

Click [Remote Management] – [Application Management] as shown in figure (4.6), the upper page will display Application Deployment and Application Whitelist menu, and the page shows application deployment list by default. Add application deployment policy to certain group then push, the devices under the group will follow the policy to download, install applications automatically, as Figure 4.4.6.1 shows.

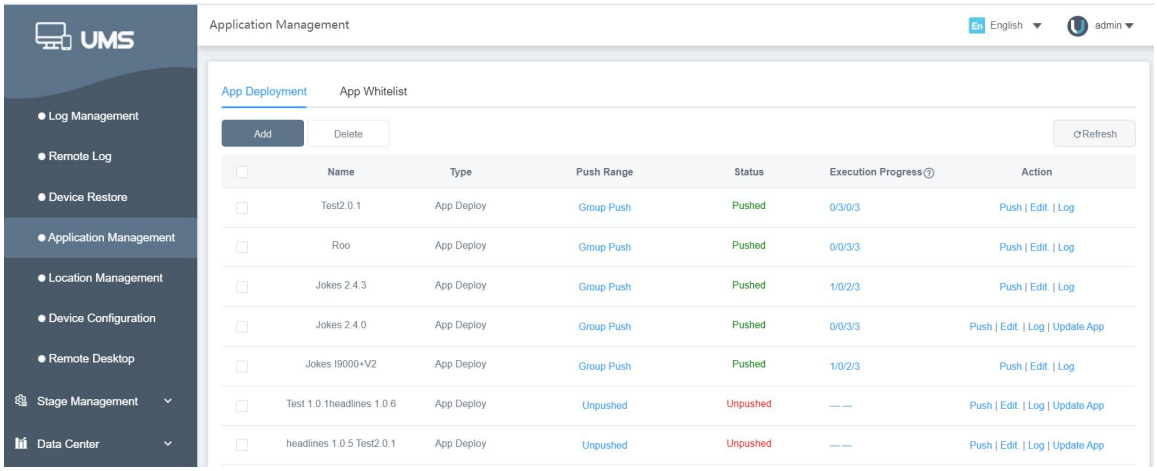


Figure (4.4.6.1)

1. Add application deployment policy

Click [Add] which at top of Application deployment list, enter policy name, deploy application, deploy method, deploy schedule in popup diagbox, click “confirm” to execute. If the policy is added successful, will show in application deployment list and marked “Not push” in status

(1) The name is required fields. You are advised to enter the application name and version number to distinguish other rules

(2) Click the Add button to select [Deploy App] or [Other Versions] for an application. One or more applications can be selected for a rule

(3) There are two deployment modes:①Silent installation: The device will automatically download and install the application without prompting after the manual application deployment instruction. ②Download notification: The device will download the application automatically after receiving the application deployment instruction, and then confirm the installation interface during installation. You can choose to upgrade immediately or upgrade later in the pop-up window. By clicking Upgrade Later, a floating ball will be displayed on the desktop.

(4) The deployment time can be "Deploy now" or "Deploy on the hour": ①Deploy now: After receiving instructions, the device will download and install the application immediately; ②Deploy on the hour: After receiving instructions, the device will wait until the hour to download and install the application.

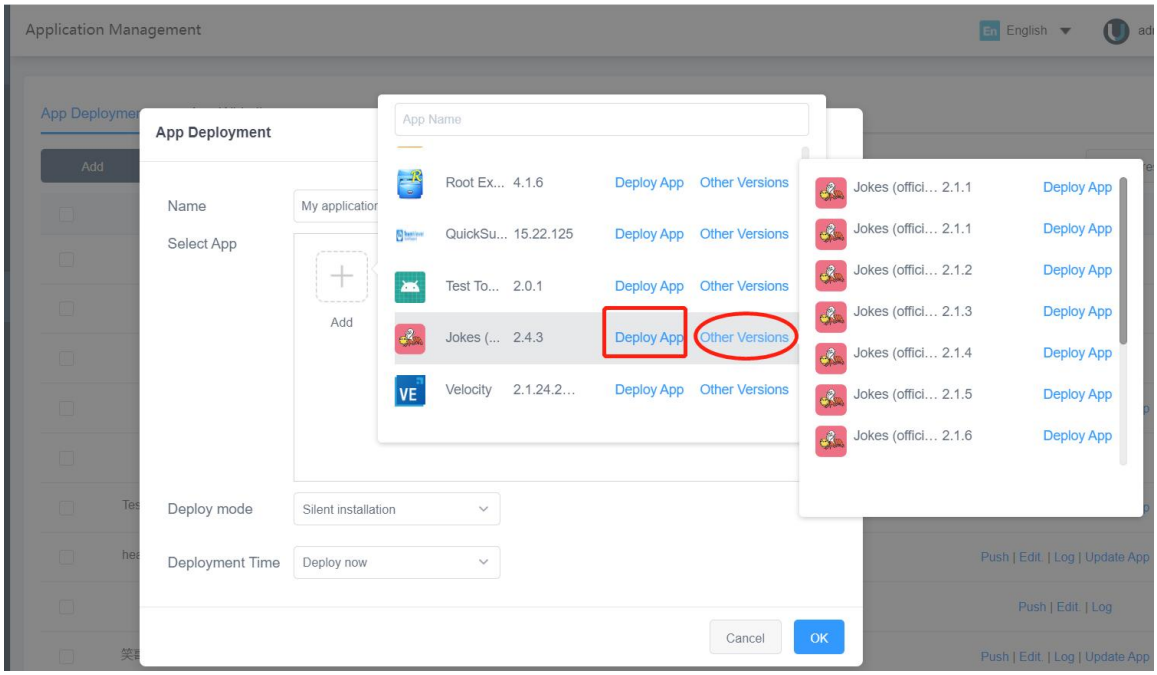


Figure (4.4.6.1.2)

2. Push Application deployment policy

2.1 Group push

Click [Push] in application deployment menu, popup “push management” message. Check single or multiple group then click [Next], diagbox will close and start pushing. Policy status will switch to “Pushed” Progress is Incomplete/Completed/Failed to Execute + Terminate Operation/All Devices. (For example: 100 devices have been pushed, 20 have been completed, 30 have not been completed, and 50 have been terminated, and the display is: 30/20/50/100)

As long as application successful installed at target devices, complete percentage will increase. The progress is shown as: progress is not completed/completed/execution failed + aborted operation/all devices. After all target devices successful installed deployment application, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

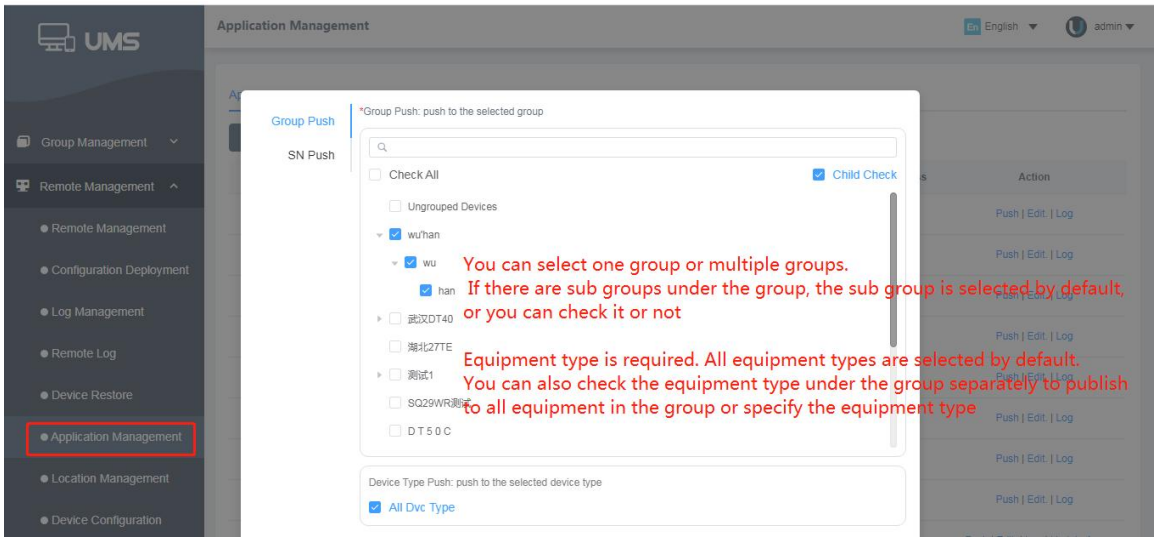


Figure (4.4.6.1.3)

2.2 SN publish and push

Click [Push] in the operation bar of application deployment list to pop up the window of "SN publish". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, the pop-up window will close, and the state of rule will change to "Pushed", and the progress is 0/total number of devices.

If the devices in the pushed group completes the application deployment command and successfully downloads and installs the application of the deployment rule, the progress of the rule will increase. The progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group; If the application is installed on all devices, the number of successfully executed devices displayed on the progress bar is equal to the total number of devices.

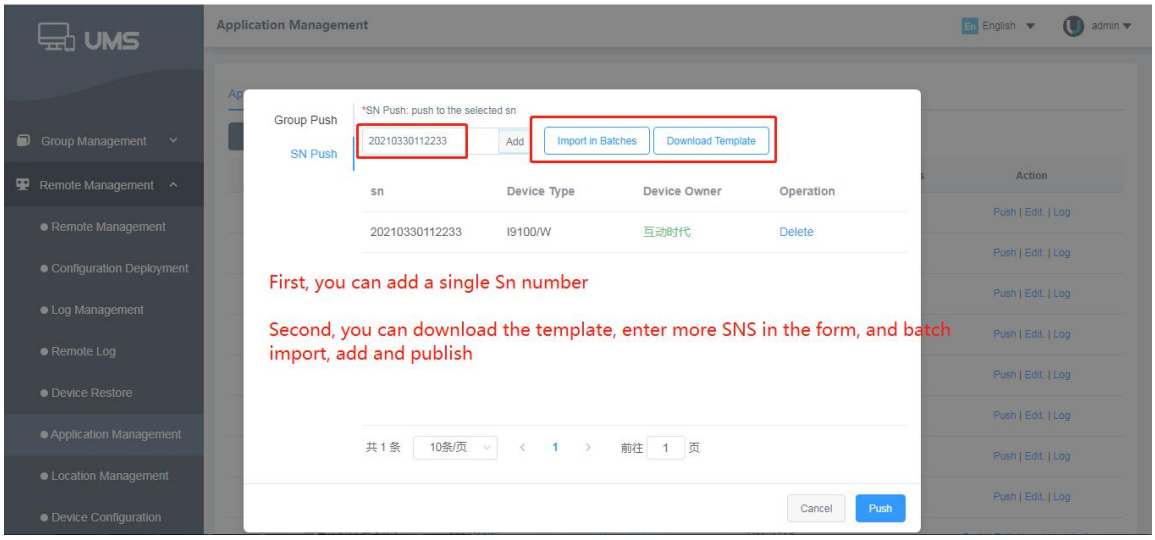


Figure (4.4.6.1.4)

Remarks:

1. After upgrading the higher version of [Application Market-Application Upload-Version Management], the [Update Application] button is displayed at the end of the rule on the lower version of the application deployment push;

2. Click the [Update Application] button. The rule status is changed from low version application to high version application, and the [Update Button] disappears; Click [Push] again, and the application deployment will push the high-version application;

3. If multiple rules are established in application deployment, the rules are pushed to the same device with different version numbers of the same application, and the device stops executing the lower version task and executes the highest version task.

4. Create the same rules and pop-up reminders to avoid repeated push; Add application and display version number in the rule to avoid error push

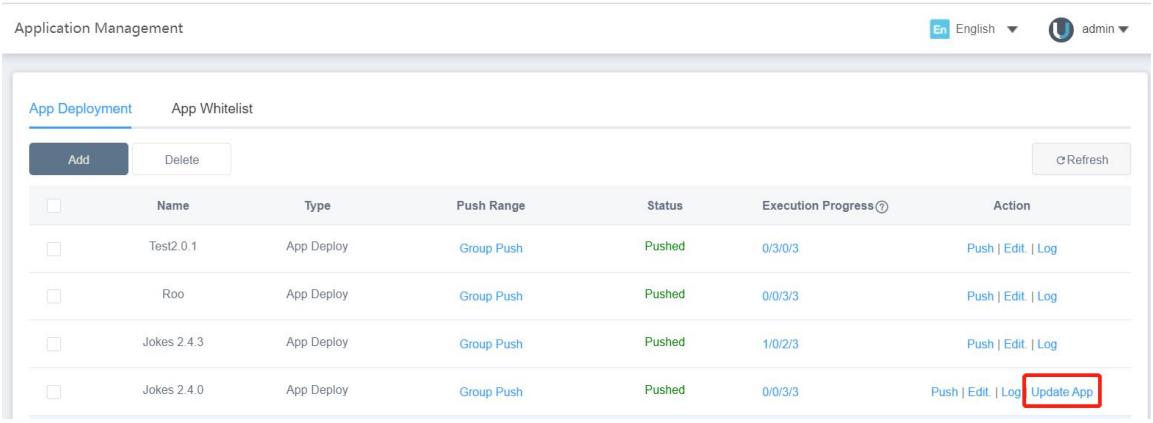


Figure (4.4.6.1.5)

3.Edit Application deployment policy

Click [Edit] from Application deployment list, popup “Application deployment edit” diagbox. Can modify deployment name, selected application, deployment method and schedule in this diagbox. After modified, all policy will be pushed again and progress bar completed percentage start from 0%.

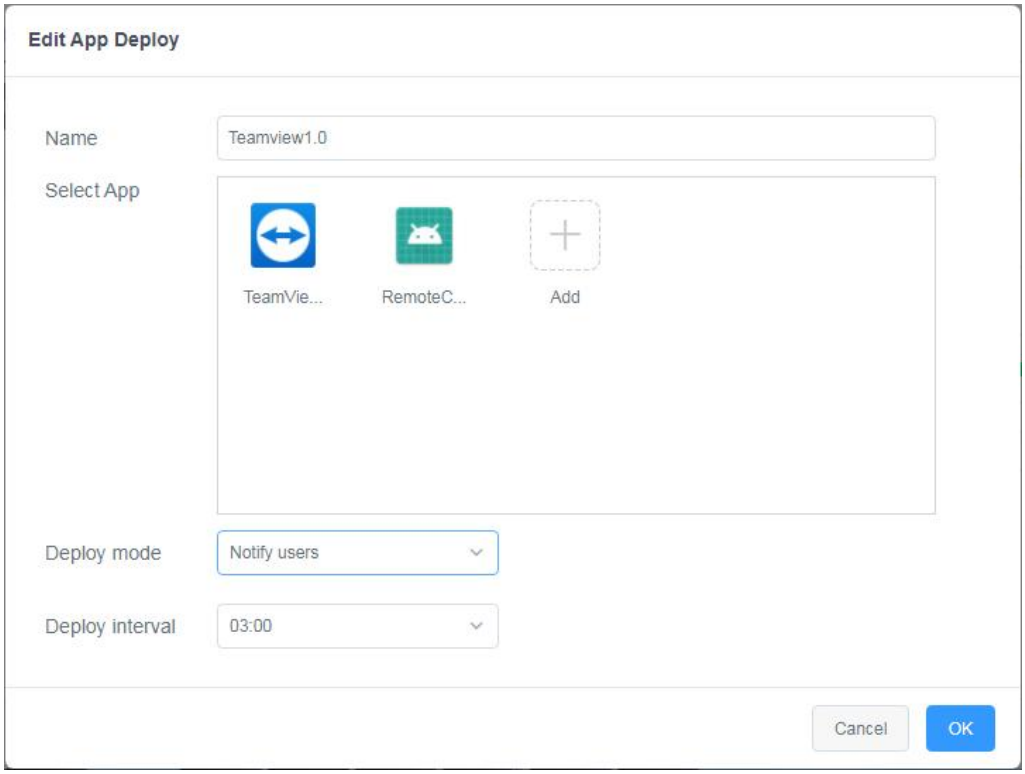


Figure (4.4.6.1.6)

4.Record

Click [Record] at application deployment policy, shows record of application deployment policy. Click [Check push content] can have detail of policy which pushed.

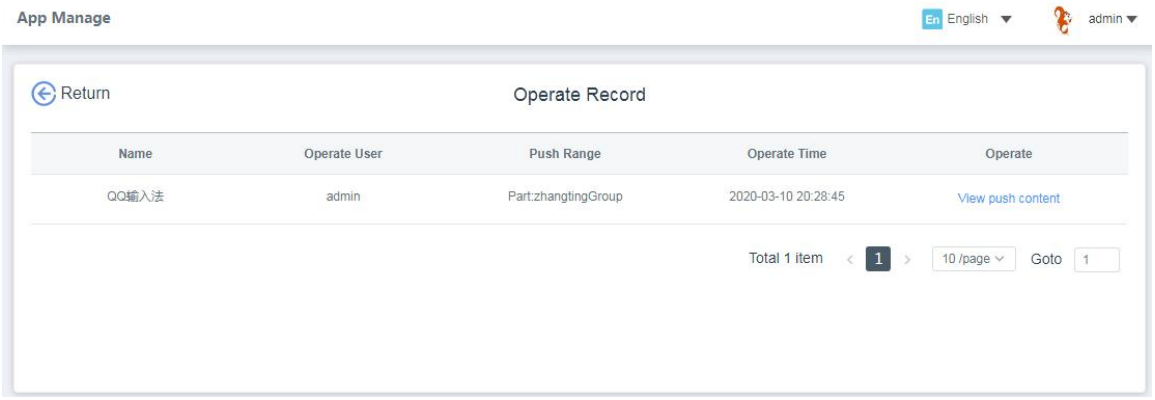


Figure (4.4.6.1.7)

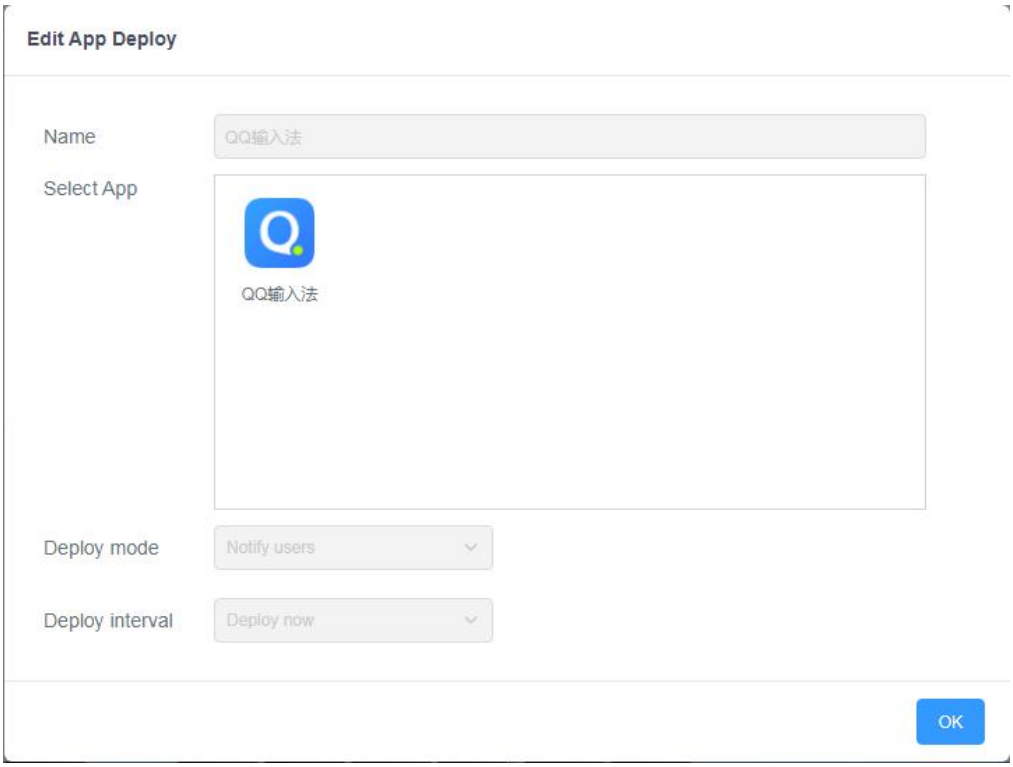


Figure (4.4.6.1.8)

5.execution progress

Click [Execution Progress] in the application deployment rule list, and the push execution progress interface of the application deployment rule will be displayed. You can view the details of the specific application deployment device execution rule. The execution status will display the unfinished device/completed device/termination operation.

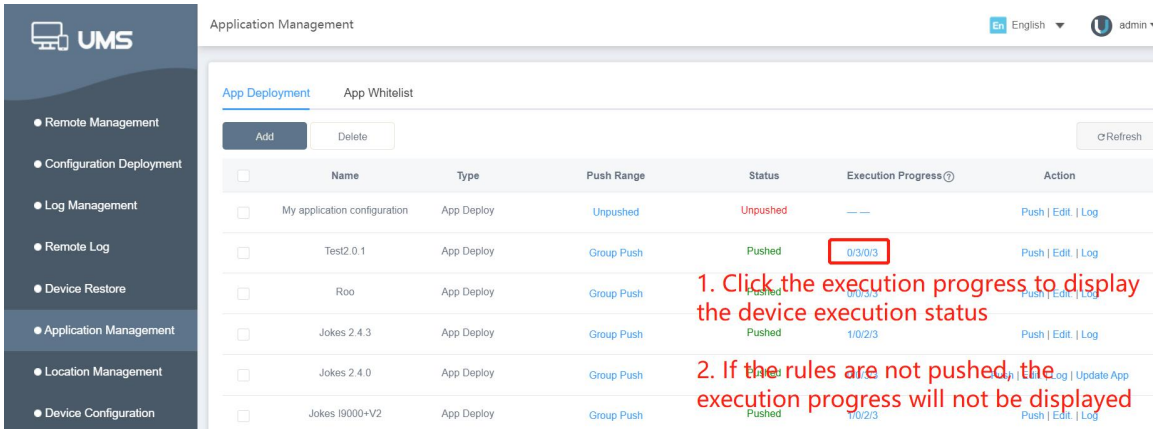


Figure (4.4.6.1.9)

【Unfinished device】: After the rule is pushed, the device has not been executed, and it will be displayed in the unfinished device.

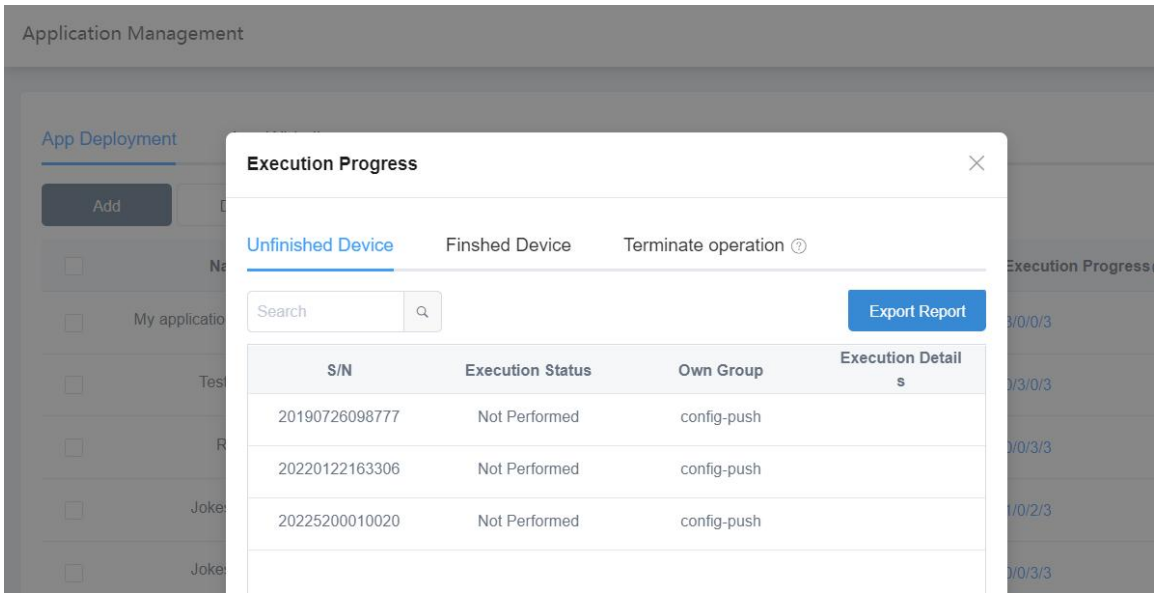


Figure (4.4.6.1.10)

【Finshed Device】: After the rule is pushed and the device is successfully executed, it will be fed back to the platform, and it will be displayed on the completed device.

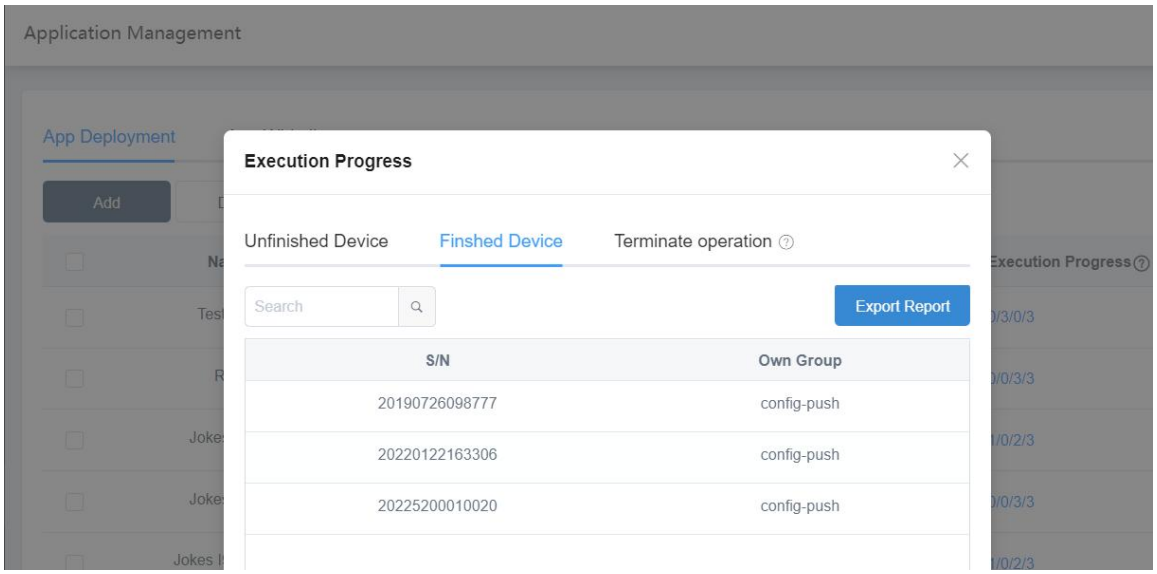


Figure (4.4.6.1.11)

【Terminate operation】:1. The device has installed the same application & same version

2. The device has installed the same application & higher version

3. Installation failed

These devices directly enter the termination operation, reducing the waste of data and power

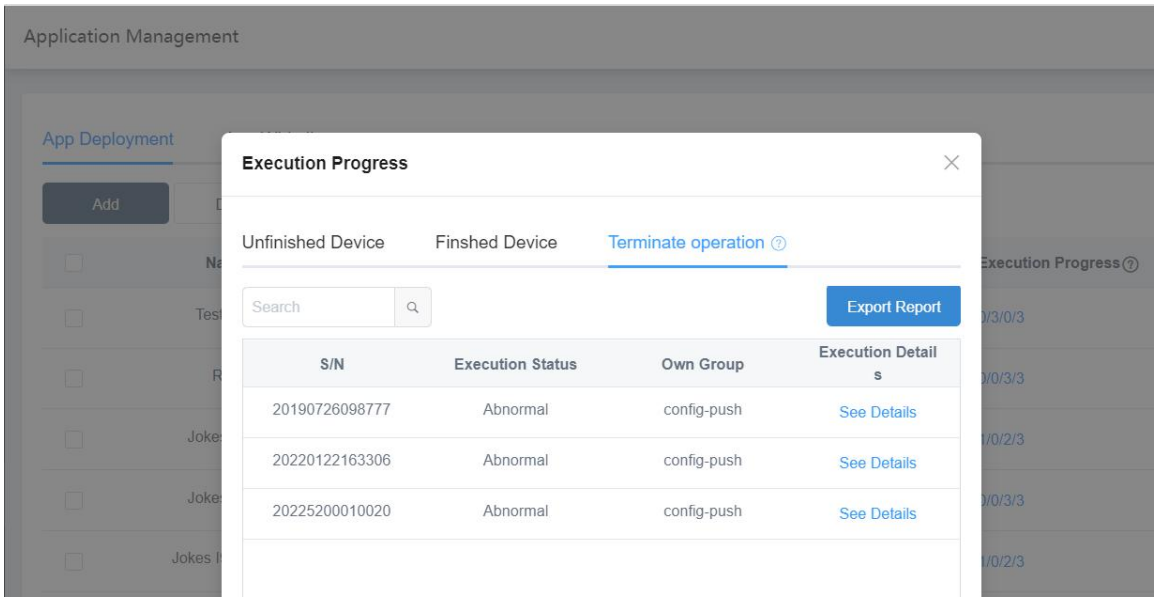


Figure (4.4.6.1.12)

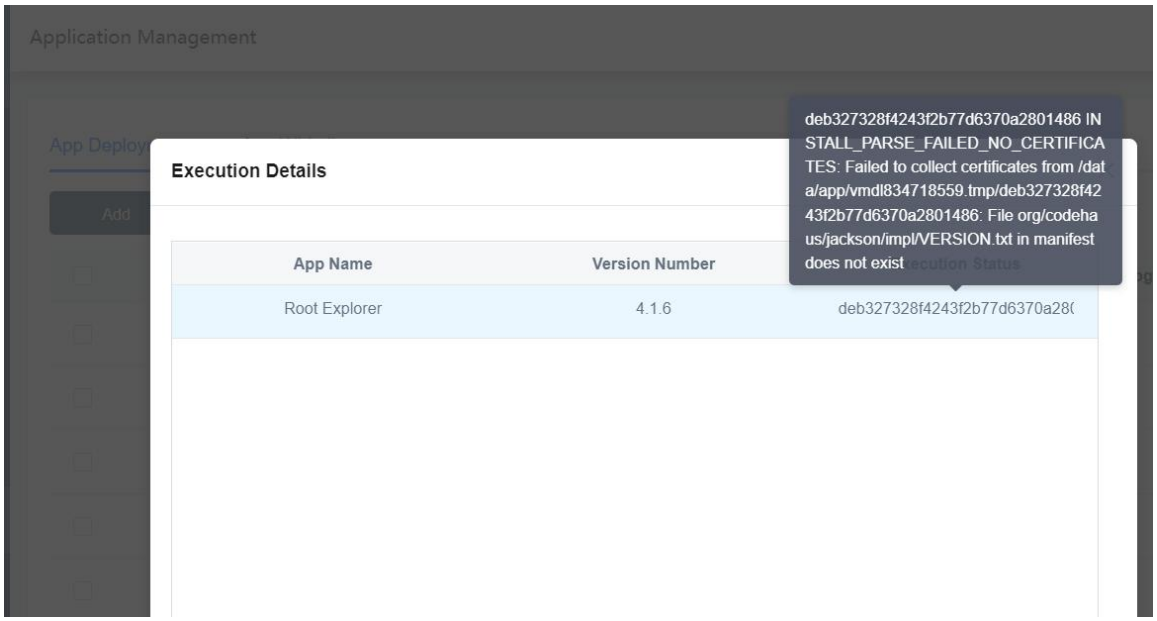


Figure (4.4.6.1.13)

6.Delete Application deployment policy

Click [Delete] at top of Application deployment list, the name of the policy will be deleted and removed from the list. If there still some devices do not receive or execute the policy, the push process will terminate. The policy name also cannot be checked by user.

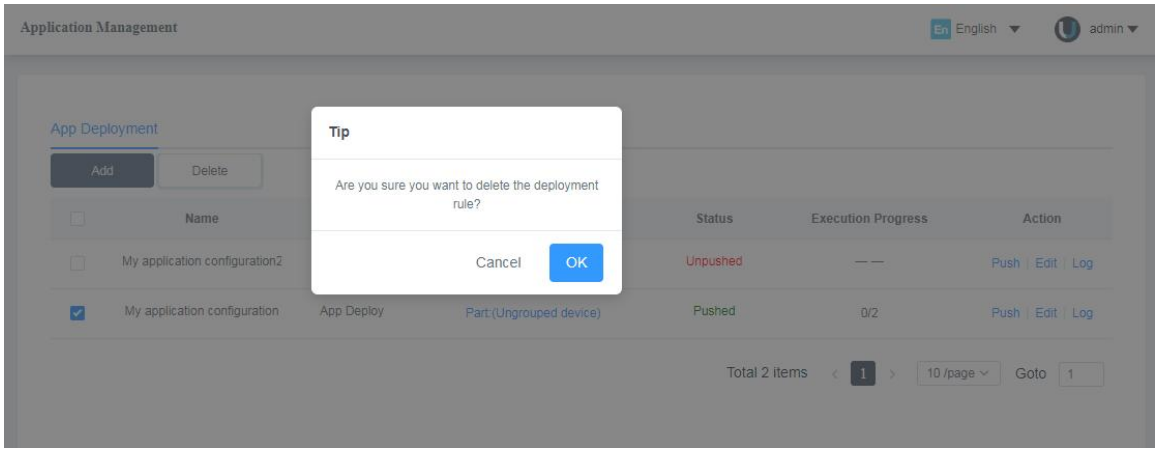


Figure (4.4.6.1.9)

4.4.6.2 Application Whitelist (New function)

In Figure (4.4.6.1), click “Application Whitelist” in the upper tab to go to the application whitelist settings page. Once a whitelist rule is added and pushed to specific groups, the devices that receive the whitelist push can no longer download applications undefined in the whitelist, but only be able to download and install applications defined, and their installed applications of undefined package names will be uninstalled.

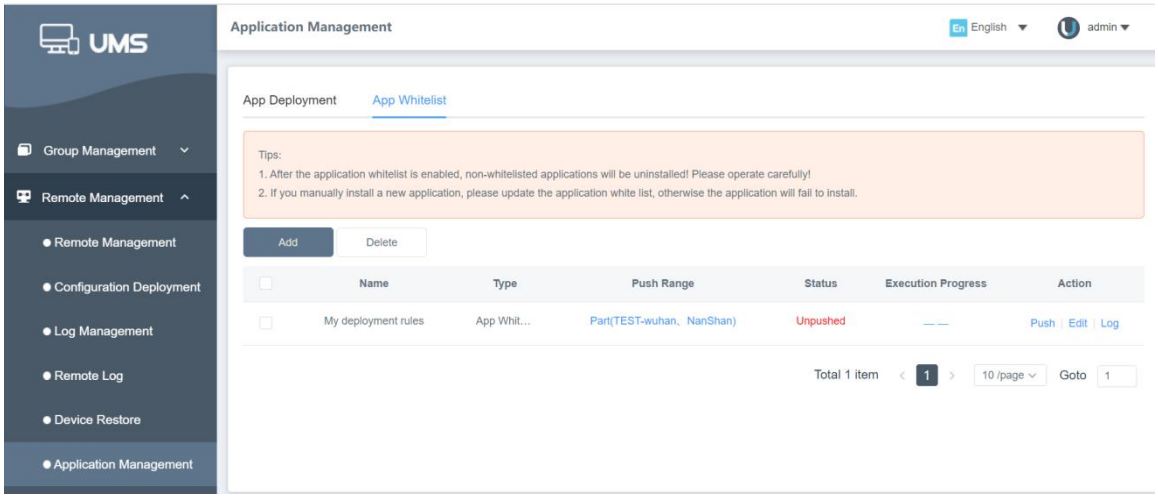


Figure (4.4.6.2.1)

Note:

After the application whitelist is opened, the non-whitelist application will be uninstalled! Please operate carefully!

When pushing the application whitelist rule to the device group, the application deployment and custom desktop pushed application name and package name are automatically maintained into the application whitelist.

If the application deployment and custom desktop add or delete the application of this group, the application whitelist will update synchronously

If a rule has been created in Group 1, Group 1 can no longer be selected when creating a new rule; that is, only one application whitelist can exist in a group.

If you push a new application, please update the application whitelist, otherwise the application will fail to install.

1. Add Application Whitelist Rules

1.1Click [Add], input the Rule Name, enter Application Name and Package Name in Application Selection box, then click [Confirm] to successfully add the app. To add multiple apps, click the [Add Application] button at the bottom, enter Application Names and Package Names for the added, then click [Confirm].

Before adding apps for a whitelist, please first add the application names and package names for the apps pushed by application deployment and the customized launcher, then proceed to add other required apps. Otherwise, the apps from application deployment and the customized launcher cannot be installed when pushed.

After adding all the whitelist apps, click [Confirm] in the lower right corner of the pop-up window to successfully add the rule. Once added, the deployment rule will be displayed in the application deployment list with status as “Not Pushed”.

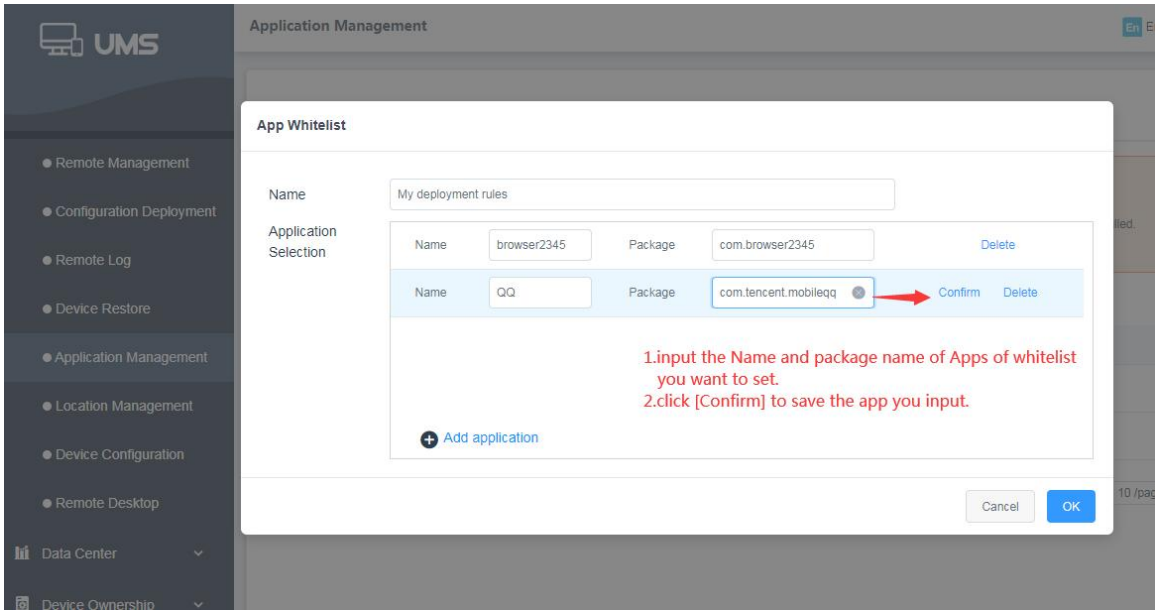


Figure (4.4.6.2.2)

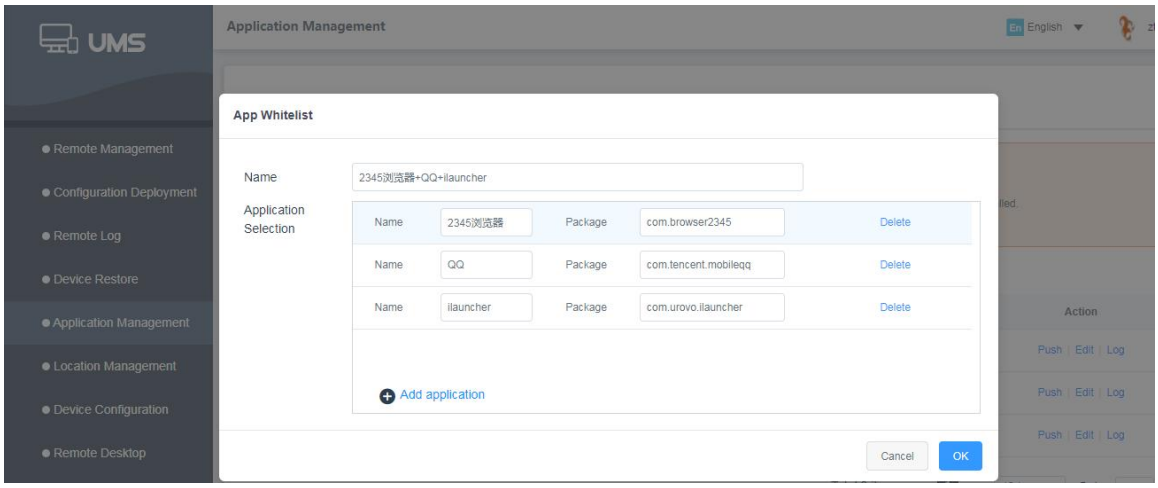


Figure (4.4.6.2.3)

1.2 Set the page in the whitelist; Add a whitelist rule, click [Add], enter the rule name, and select whether the push range is application deployment or custom desktop grouping; deployment and custom desktop pushed application name and package name are automatically maintained into the application whitelist. Display the grouped application deployment and custom desktop pushed applications. When application deployment and custom desktop application are added or deleted, the application whitelist is updated synchronously and pushed to the device.

After adding all the whitelist applications, click the [OK] button in the lower right corner of the pop-up window to add and apply the whitelist rules successfully. After adding successfully, the deployment rule will be displayed in the Application

Deployment list with the status of [Un-pushed].

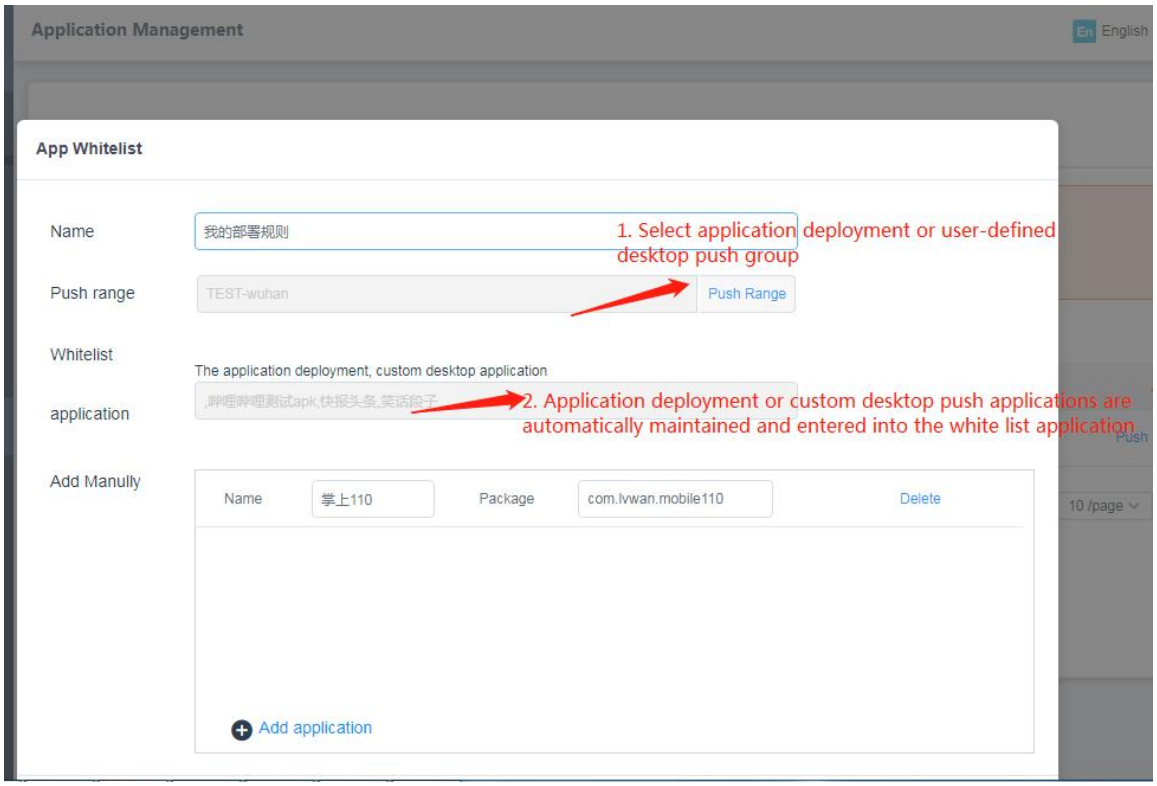


Figure (4.4.6.2.4)

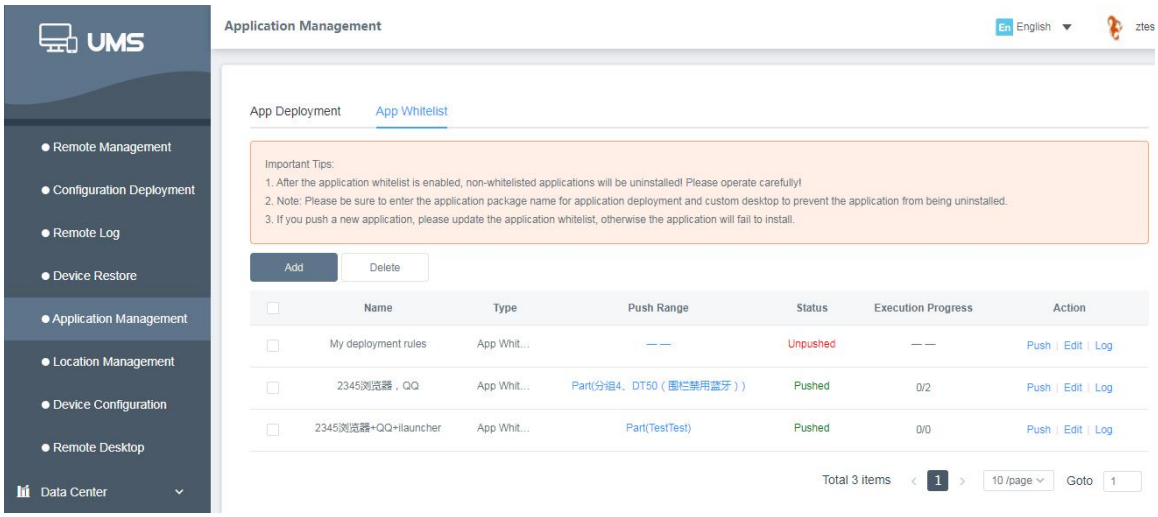


Figure (4.4.6.2.5)

2. Push application whitelist rules

Click [Push] in the application deployment list operation bar, and a pop-up window of [Prompt] will pop up. Prompt 1, after the application whitelist is opened, the non-whitelist application will be uninstalled! Please operate carefully! 2. If you install a

new application manually, please update the application whitelist, otherwise the application will fail to install. Click [OK] after confirmation, then the pop-up window closes, and the status of this rule changes to [Pushed], with a progress of 0/total number of devices.

If the devices under the pushed packet complete the application of the whitelist instruction, the progress of this rule will increase after the application of the whitelist instruction takes effect, and the progress will be displayed as: the number of devices successfully executed/the total number of devices in the pushed packet; If all devices are installed and applied, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

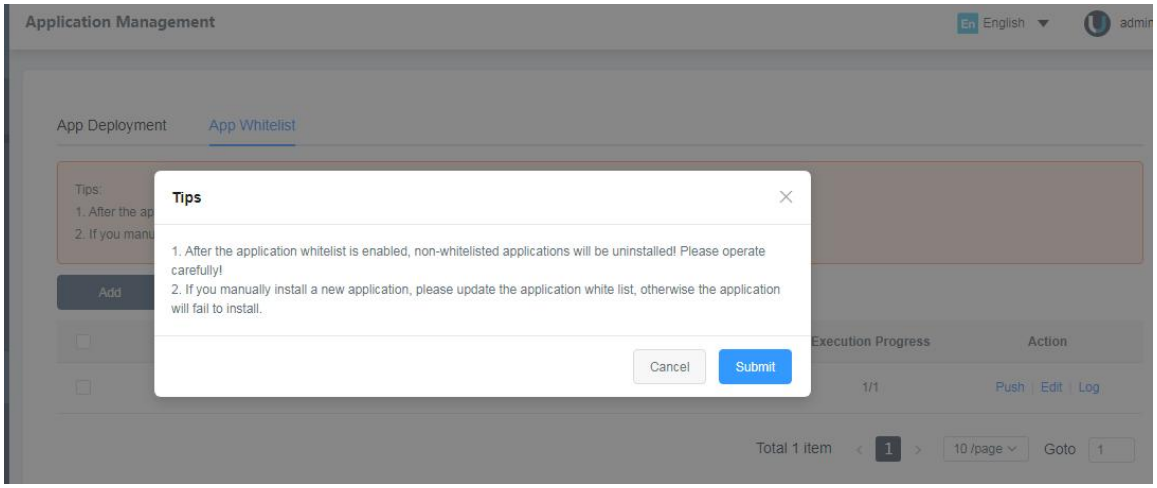


Figure (4.4.6.2.6)

2. Edit Application Whitelist Rules

Click [Edit] button to change the rule name or application name/package name, or delete certain apps from the whitelist, then click [Confirm], and the rule will be re-pushed to previously selected device groups, and the rule progress will change to 0. The new whitelist rule will be applied when the device receives the push.

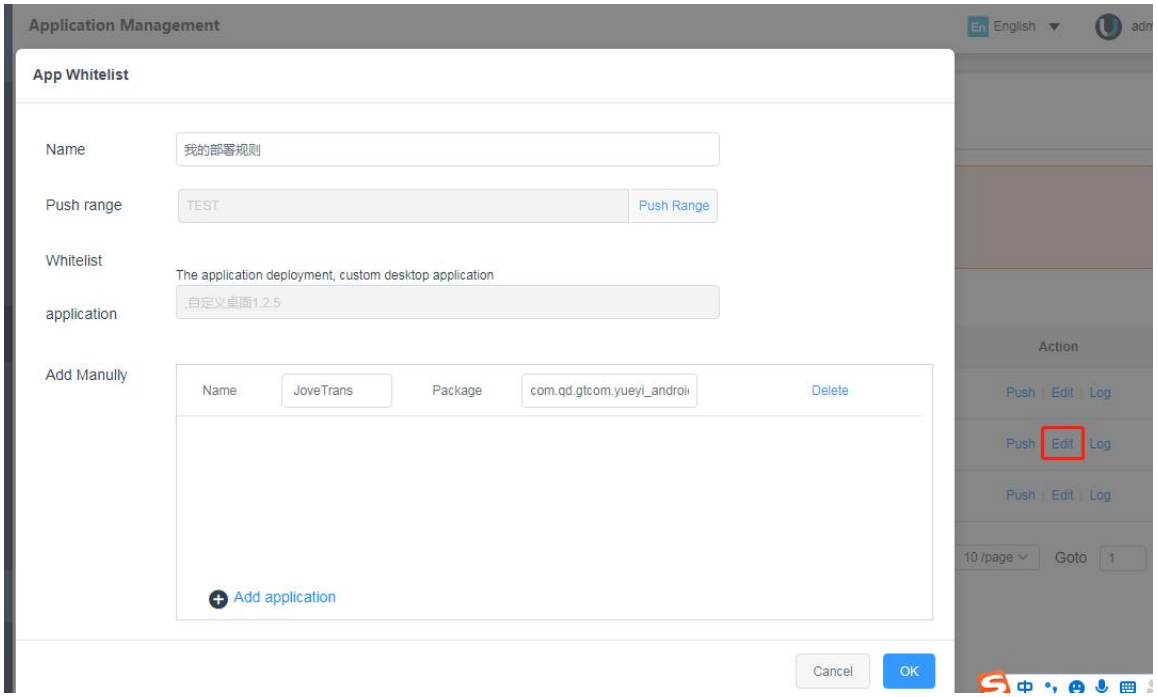


Figure (4.4.6.2.7)

3. Record

Click [Record] in the application whitelist operation column to display the push record of application whitelists. Click [View Push] in Operation Record to view respective details of the pushed whitelist rule.

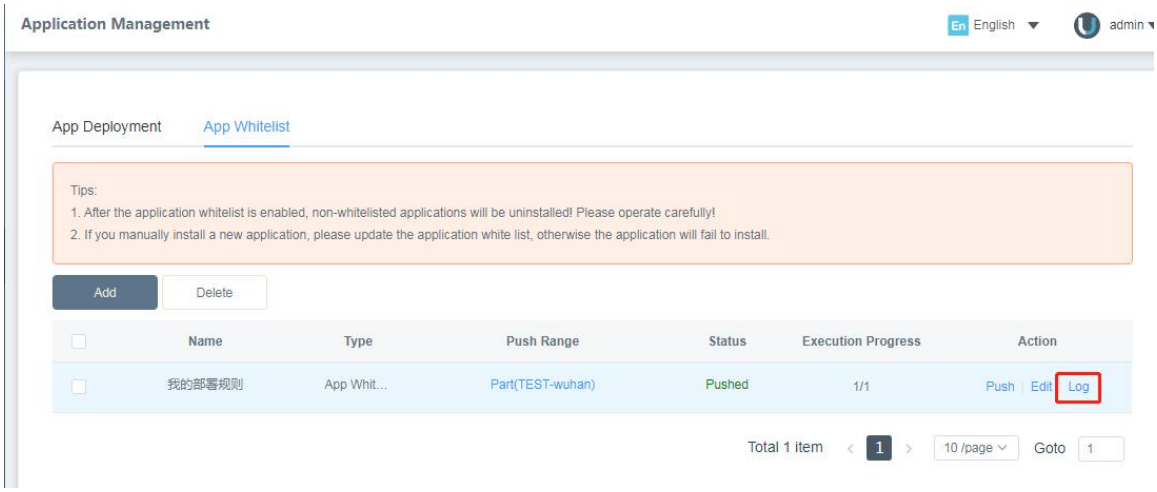


Figure (4.4.6.2.8)

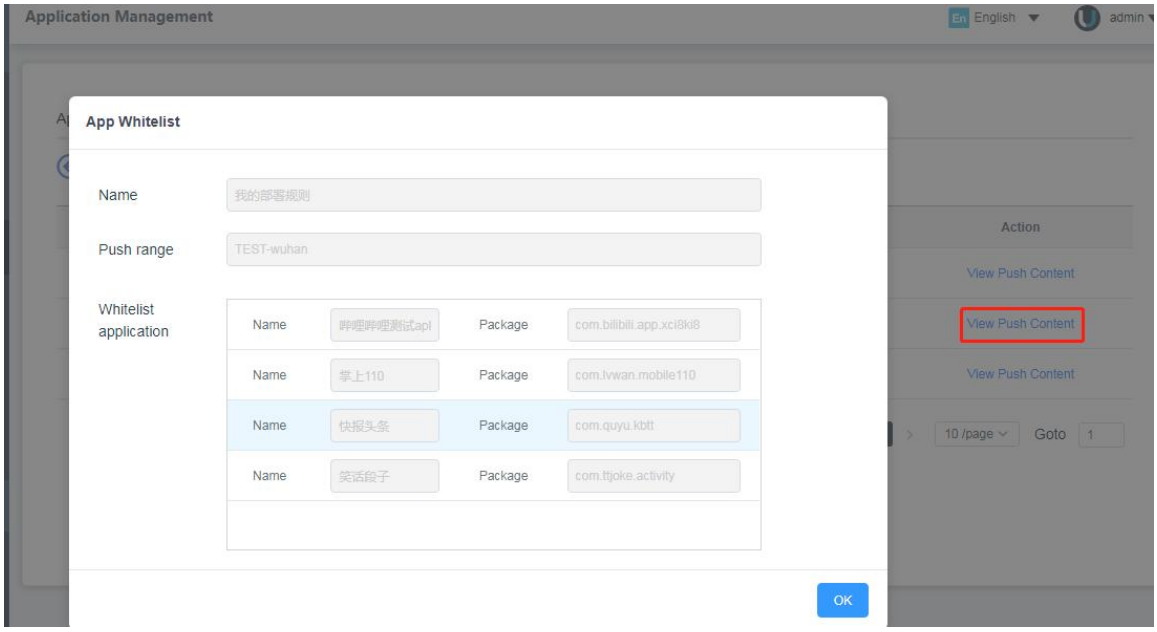


Figure (4.4.6.2.9)

4. Delete Application Whitelist Rules

Click [Delete] at the top of the application whitelist. Once deleted, the application whitelist rule will not be displayed in the whitelist list, and the devices will not be applied any application whitelist rule and can download and install any application.

4.4.7 Location Management

Click [Remote Management]-[Location Management], the location management page will display device grouping and geo-fence information, and the geofences of ungrouped devices is displayed by default. If the location information uploaded by the device in the device group is outside the fence range, and the fence switch is on, the device group will start the fence policy and disable the set restrictions, as shown in the following figure:

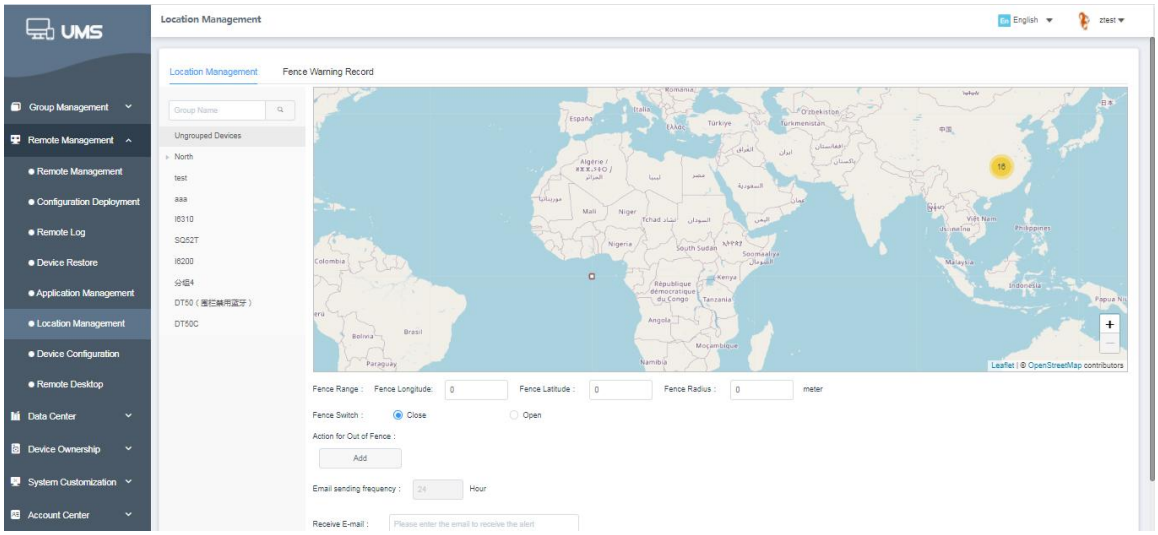


Figure (4.4.7.1)

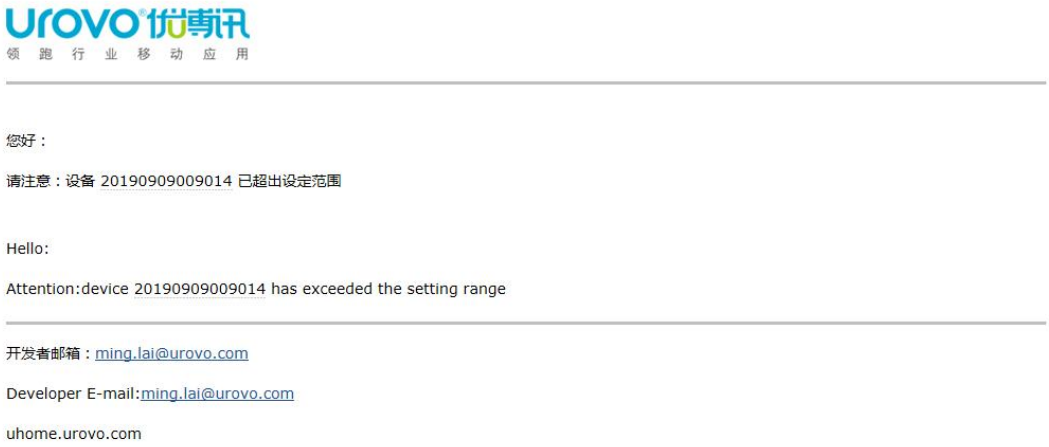


Figure (4.4.7.2)

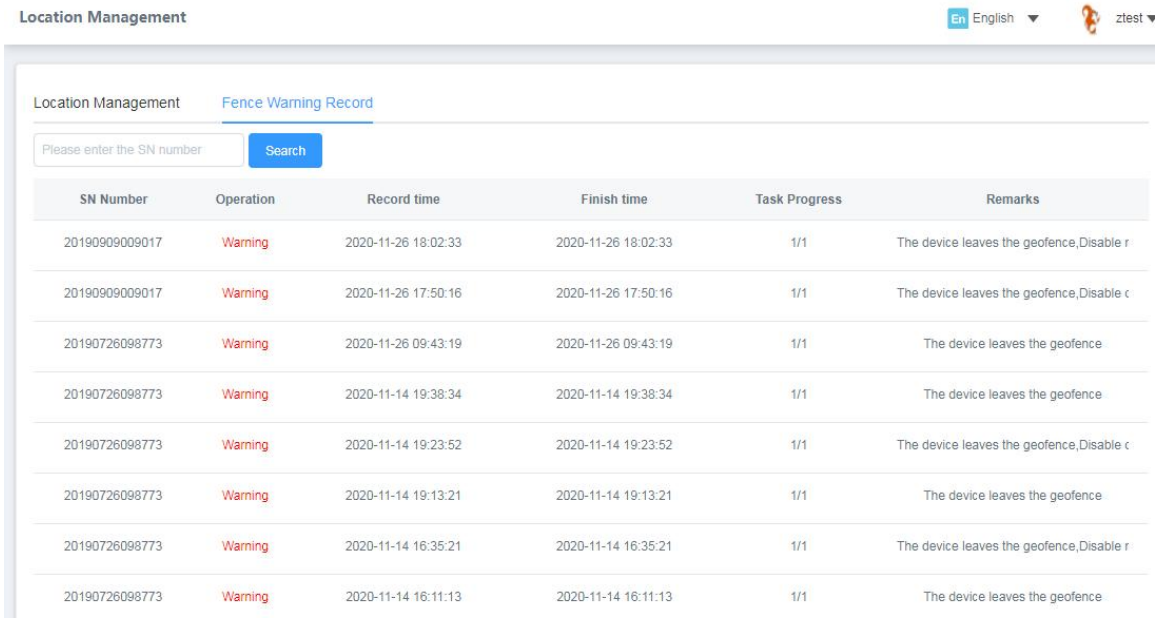


Figure (4.4.7.3)

Steps to set up the fence:

(1) Select a group, click a certain position on the map (as the center of the circle), and then click another position (as the boundary point), the distance between the two points is the radius, and the red part of the circle formed is the fence range. Or you can also set the geo-fence directly enter the corresponding values in the longitude, latitude, and fence radius input boxes below the map;

(2) The fence switch is set to "on";

(3) Click [Add] for items beyond the range limit, click [Add] button on the right side of the pop-up window, add the limit item “Disable mobile data/device disable/device start ringing”, and then click [Save] button below. If the device position in the device group is outside the fence range, the set items such as mobile data/device disable/device start ringing will be disabled; This function will take effect after polling time.

(4) Enter the email address in the receiving mailbox (such as: utest@qq.com). When the device detects that it is outside the fence, it will send an early warning message to this mailbox: "Warning XXXX device has exceeded the fence setting range".

(5) Click other device groups, you can switch device groups to set fences.

(6) If a fence is set and switched on, and a device is detected outside the fence range (the device will check the fence according to the polling time), a fence alert message will be added to the fence alert record (see Figure 4.4.6.3).

4.4.8 Device configuration (modification function)

Click [Remote Management]-[Device Configuration], you can configure power consumption & traffic configuration for each device group, as shown in the following figure:

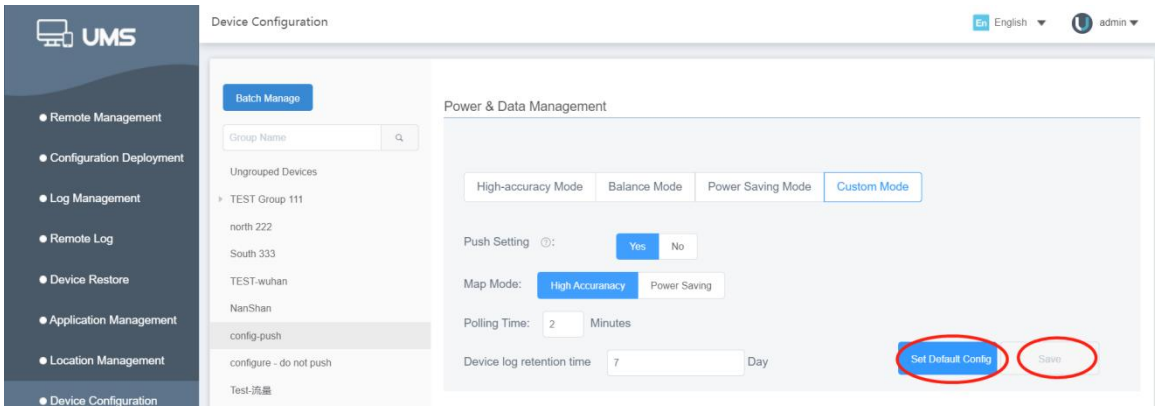


Figure (4.4.8.1)

By waiting for the polling time or restarting or switching the network, the terminal device can detect that the power consumption & traffic configuration configured in thbackground can be set to the default value, or directly click Apply.

1. Device default configuration: This rule is the default configuration of the account, which is synchronized to all groups in batches, and this rule is executed every time a new group is added. For example, add group A, which is a custom mode that executes the current configuration.

2. Apply to the current group: This rule takes effect only for the current group.

There are four modes for power consumption & flow configuration, including high-precision mode, balanced mode, energy-saving mode, and custom mode. After the device selects a certain mode, click [Apply] to take effect. The energy-saving mode is applied by default.

(1) High-precision mode: use push, map with high-precision, polling time is 10 minutes;

(2) Balanced mode: Use push, the map adopts energy-saving mode, and the polling time is 3 hours;

(3) Energy-saving mode: use push, map adopts energy-saving mode, polling time is 24 hours;

(4) Custom mode: You can set whether to use push, set map mode and polling time by yourself.

(5) Retention time of device logs: Local log files will be saved according to the set time. Logs that exceed the set time will be automatically cleared (the file size is not

limited). The default value is 30 days. The device will save logs at the set time and deletes logs only when the date changes or the device is powered on.

Notes:

(1) When the push setting selects "Use", the terminal will respond immediately when the background sends instructions to the terminal in the remote management. If it is set to "Not used", the terminal needs to wait until the polling time arrives before detecting the instructions sent in the background;

(2) When the map is set to "High-precision mode", the frequency of obtaining device positioning will be high, and when the map is set to "Energy-saving mode", the frequency of obtaining device positioning will be low;

(3) The device uses push, high precision, and the shorter the polling time, the higher the power consumption and traffic consumption of the device;

(4) The original third-party application installation and USB debugging functions have been moved to the remote settings-functional device page. If you want to disable it, you can set it on this page of Function Setting. The remote configuration of UMS2.5 version will continue to be retained, but will not be displayed.

4.4.9 Remote Desktop

Click [Remote Management] – [Remote Desktop], shows all devices sort by serial number under this account. As Figure 4.4.8.1 shows below:

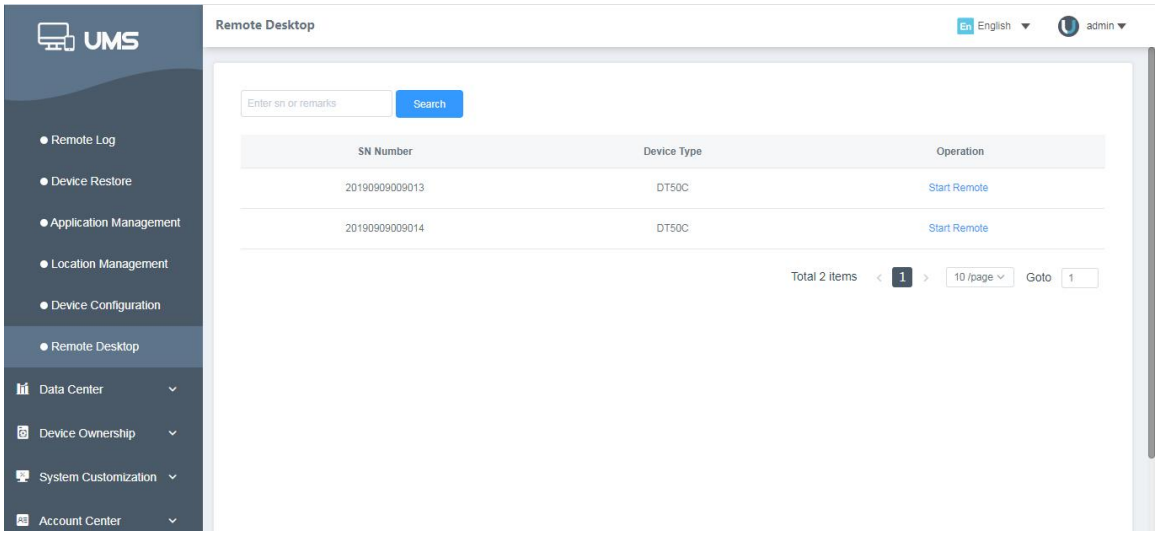


Figure (4.4.9.1)

Click [Start Remote] in the operation bar, if device preinstalled “RemoteControl APK”, device can open “RemoteControl App” automatically for remote control. If connect successfully , the remote control page will be opened in the background, and the device can be remoted through this page.

Figure (4.4.9.2)

Notes:

1. Under remote controlling, you can use the mouse to simulate finger touching the screen to complete operations such as clicking a button, sliding up, and (pulling) down …etc.

2. At the right of remote control screen is control panel, provide function buttons included HOME, back, menu, quick setting, lock(unlock), volume up/down, scroll

up/down. Can click the button to simulate visual key of remoted devices.

4.5 Device Ownership

Device ownership is the management of the accounts to which the device(s) belongs to. It can be bound to the sub-accounts through the device binding function, or it can be presented to other agents through the device presentation function, as shown in the following figure:

4.5.1 Distribute Device

Display the distribution information of all the devices in the current channel (sub-accounts included), namely SN Number, Device Type, Subordinated Account, Operation, etc. The user can distribute the agent's devices to sub-accounts.

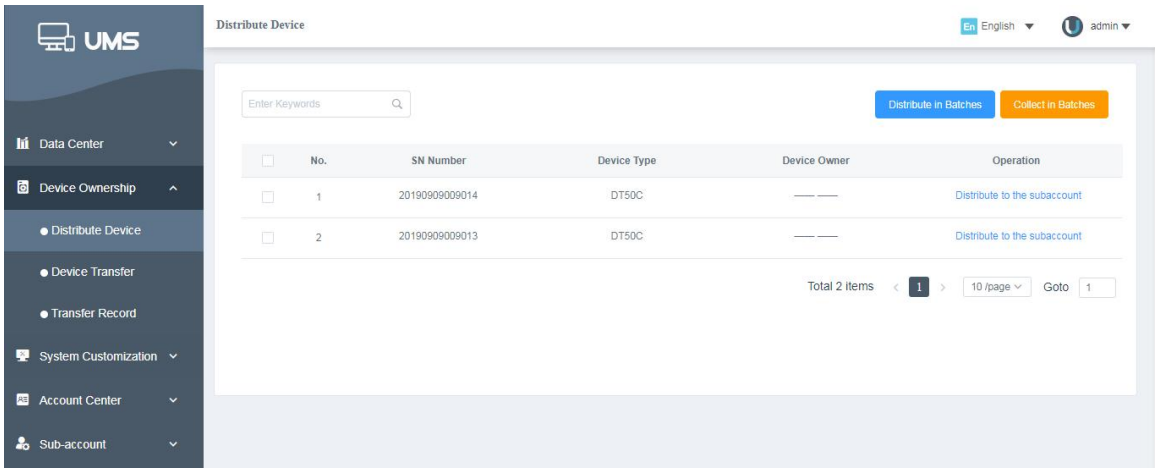


Figure (4.5.1.1)

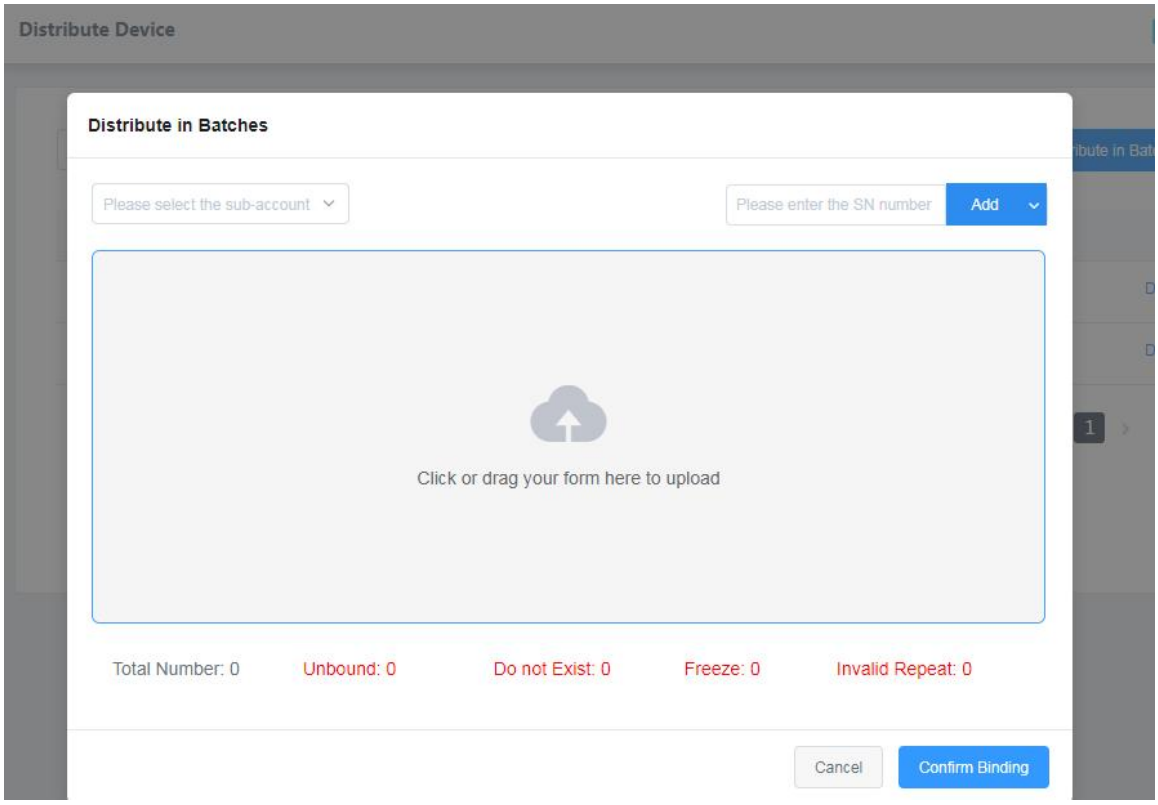


Figure (4.5.1.2)

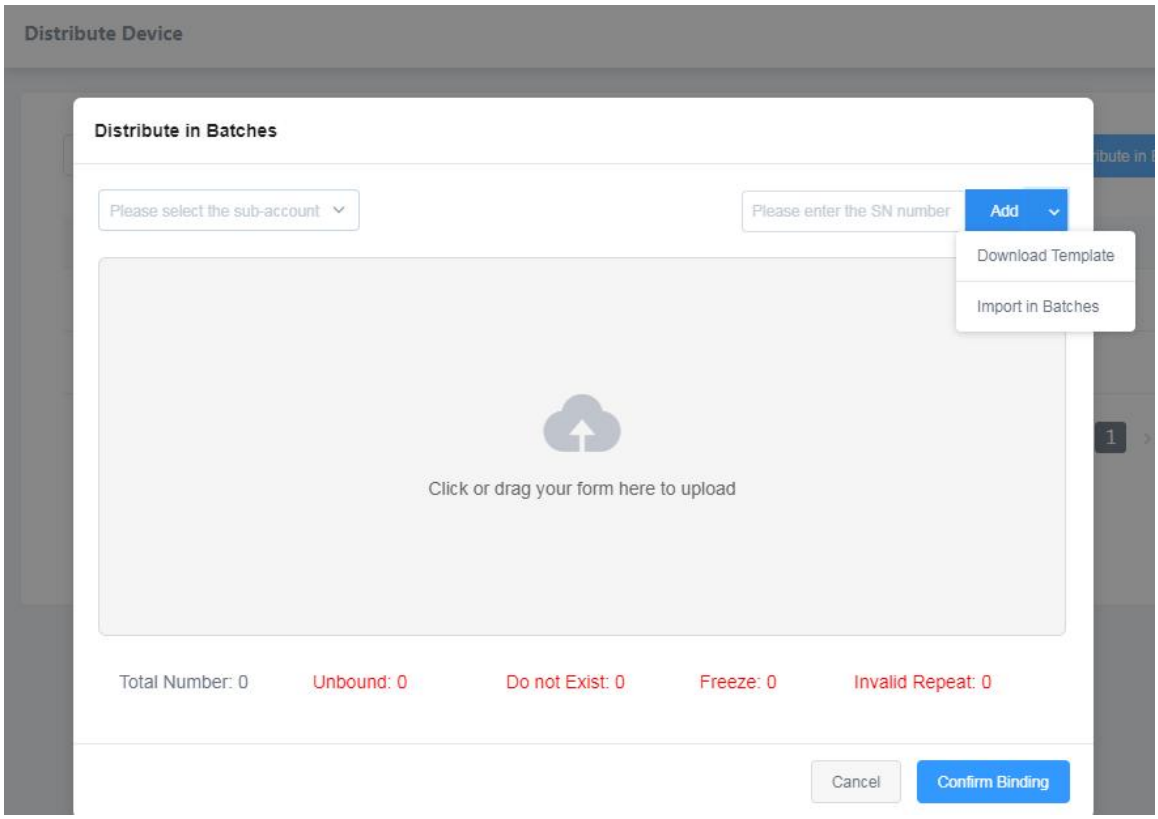


Figure (4.5.1.3)

Figure (4.5.1.4)

1. Single Binding: Choose one of the devices, click [Distribute in Batches] on the operation bar, choose a sub-account from the pop-up box, click [Binding], and the device is bound to that sub-account;
2. Sub-Account Replacing: Choose a device which is successfully bound, click Replace the Sub-account], select another sub-account to complete the replacement.
3. Device Unbinding: Click [Unbind] to retrieve the device of the sub-account;
   Note: The successfully bound device detects the application of the sub-account.
4. Batch Binding：Click [Distribute in Batches] button on the top right of the list, then click [Add] after entering the SN number, or download the template and then import in batches. After entering a SN number, the device and its subordinate account and its status will be displayed below. Click the drop-down box in the upper left corner to select a sub-account to which the device is bound.

4.5.2 Device Transfer

Display the distribution information of all the devices in the current channel (sub-accounts excluded), namely SN Number, Device Type, Subordinated Account, Operation, etc. The user can present the agent's devices to other agents, as shown in the following figure:

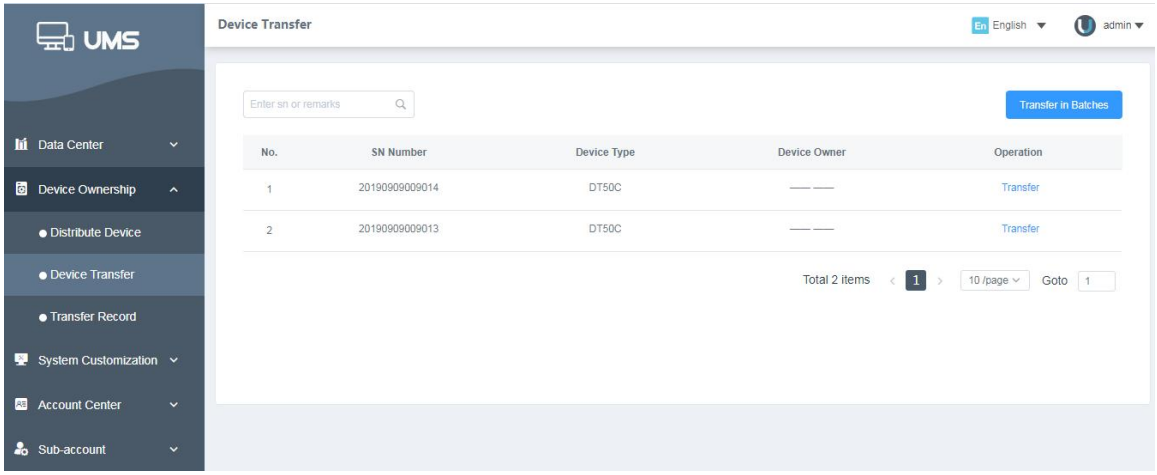


Figure (4.5.2.1)

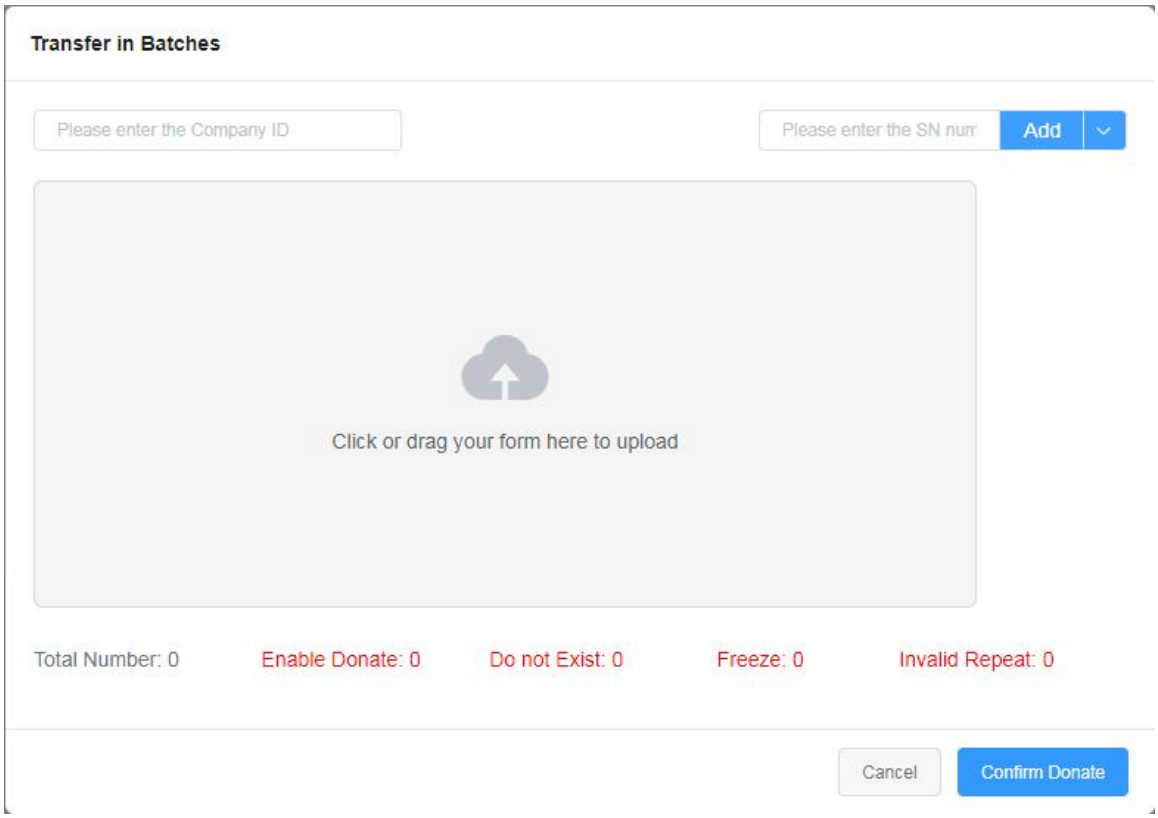


Figure (4.5.2.2)

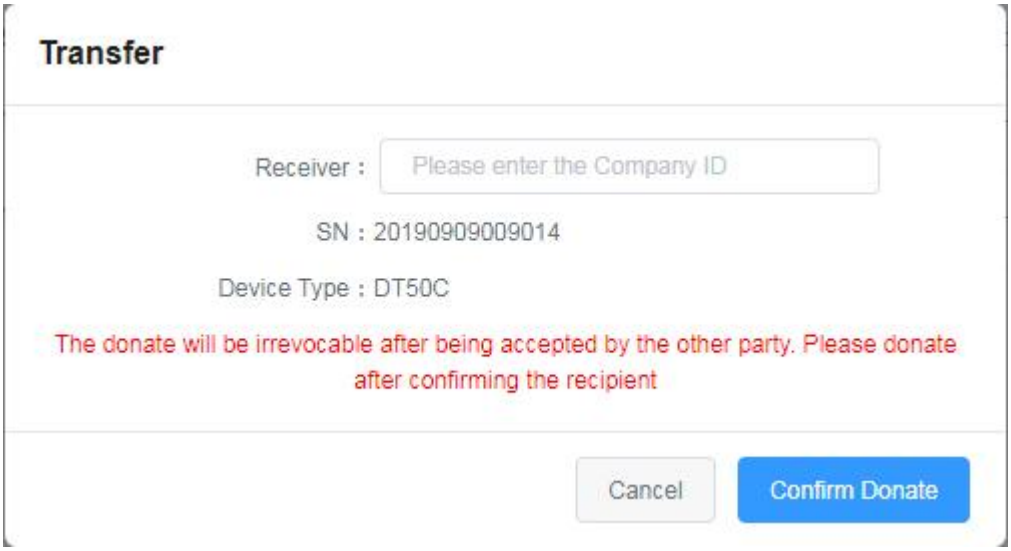


Figure (4.5.2.3)

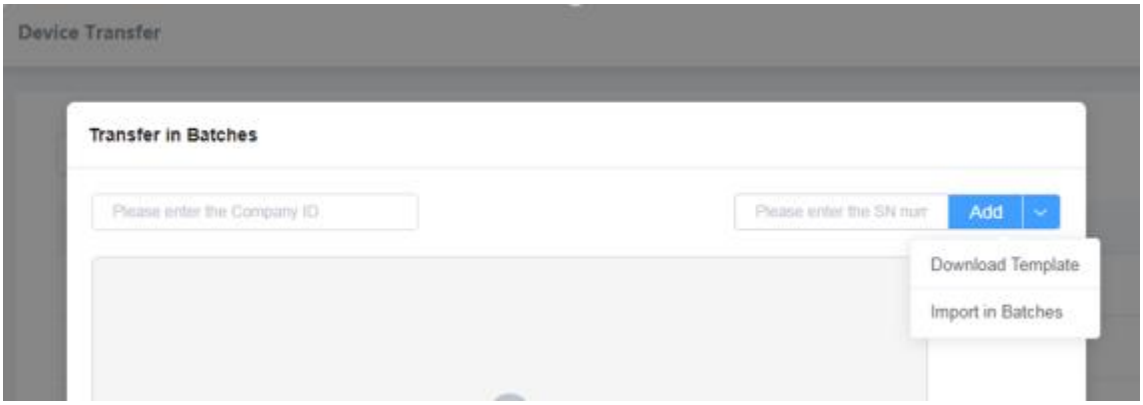


Figure (4.5.2.4)

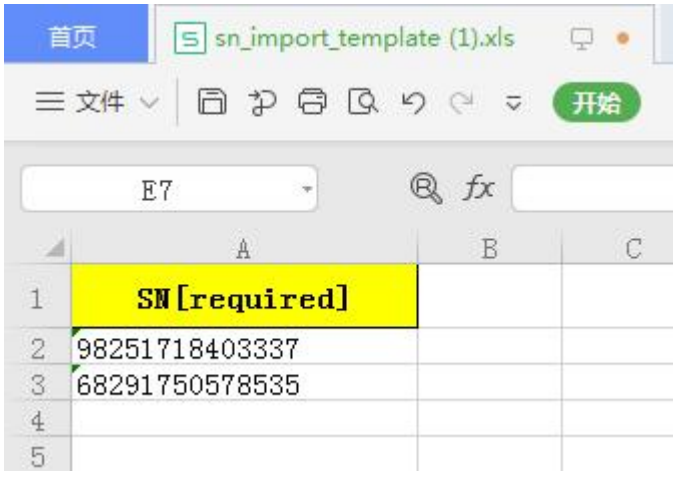


Figure (4.5.2.5)

1. Single Transfer: select a device, click [Tranfer] on the operation bar, enter the company number of the target agent (receiver) in the presentation pop-up window, and

click [Confirm Donate] to complete the presentation.

2. Batch Transfer: click the [Transfer in Batches] button in the upper right corner of the list, enter the SN number and click [Add], or download the template to import in batches. After adding the SN number, the device and its subordinate account and its status will be displayed below. Enter the recipient company number in the upper left corner, and click [Confirm Donate] to give the device to the recipient.

4.5.3 Transfer Record

Display the presentation and reception information of all the devices, as shown below:

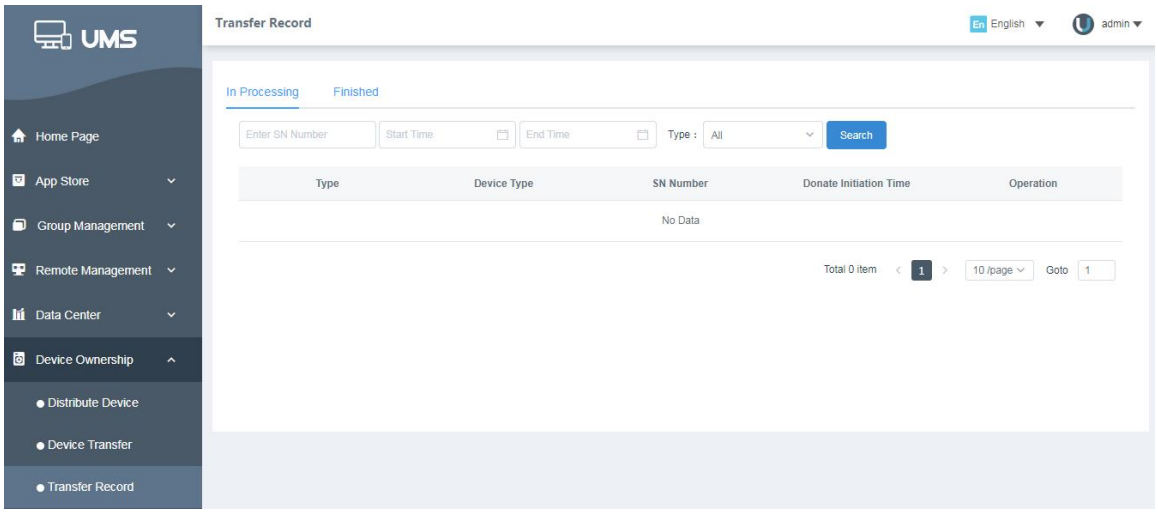


Figure (4.5.3.1)

1. Input the SN Number, or Start Time, or End Time, or Type as variables to search the corresponding records of donation or acceptance.

2. “Unfinished” shows the device donations to or from this account that are not received. The unfinished operations can be canceled or refused.

“Finished” shows the device donations to and from this account that are accomplished.

4.6 System Customization

System Customization, customer-oriented service for agents and their devices,

includes My Boot Animation, Kiosk Mode, Default Boot App, and Customizing Desktops.

4.6.1 My Boot Animation

My Boot Animation provides customized boot animation for all the devices of the current account. After selecting a model and uploading a customized animation, the devices will detect the new animation and download it. After restarting the devices, the customized animation is applied. If the customized animation is not set in the background, the devices apply the default Android animation.

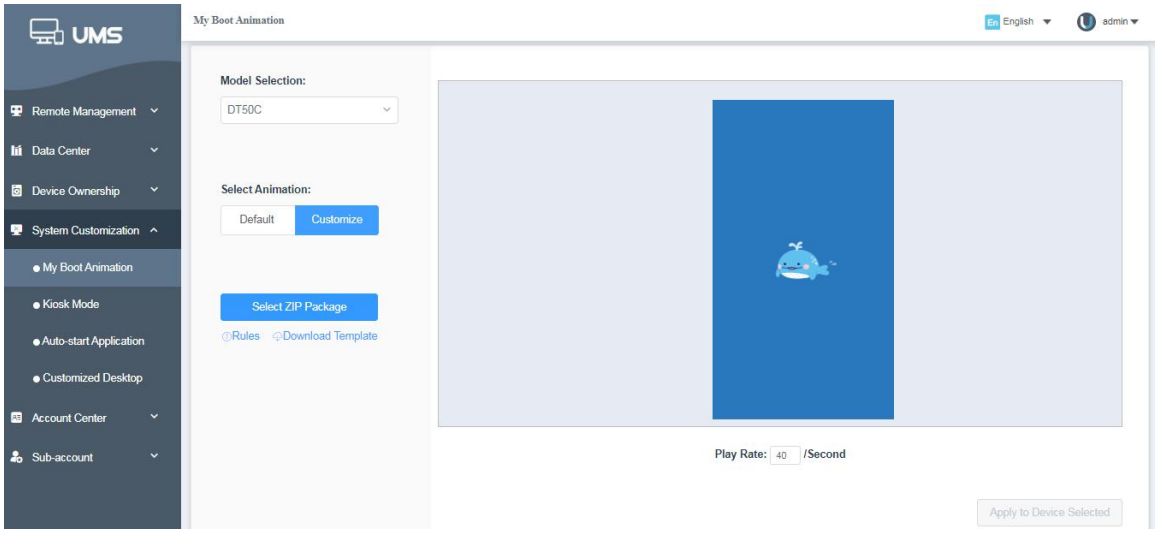


Figure (4.6.1.1)

1. Select a model (device model), and then click “Customize” to upload a ZIP package of a book animation. After uploading it, the uploaded boot animation will be displayed on the right side in the form of GIF. The play speed can be set.
2. Click “Apply to own device”, then the boot device will detect the uploaded boot animation under this account and download the boot animation, then apply the boot animation after restarting the device;
3. The format of the boot animation ZIP package is fixed. The user could download the Template first and adjust the uploading files according to it.

4.6.2 Kiosk Mode

Kiosk Mode function can be applied to all the devices of the current account. The page displays all the model types of the account and their applications set in the Kiosk list. See Figure 4.6.2.1. After the application is locked, the locked app will not be able to logout. The device user needs Kiosk unlock password to logout.

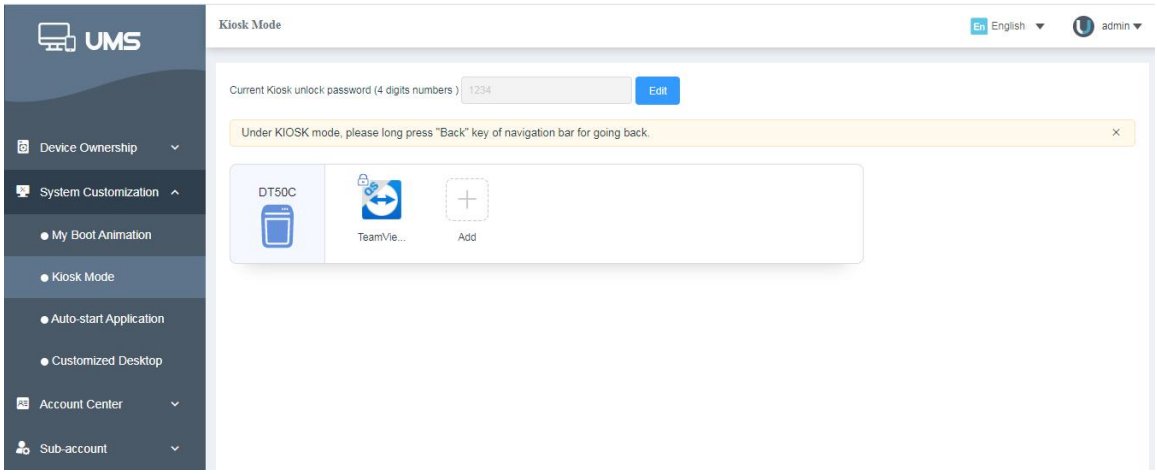
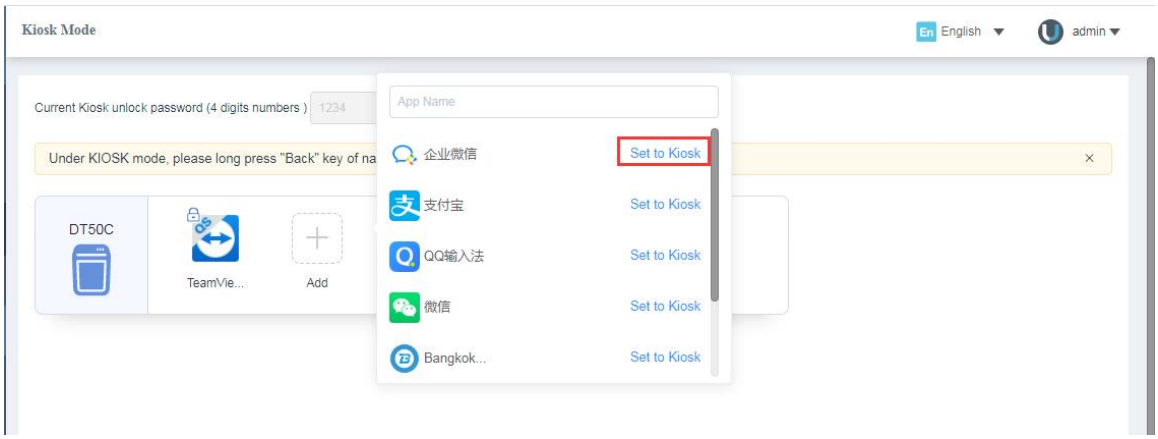


Figure (4.6.2.1)



FigFigure (4.6.2.2)

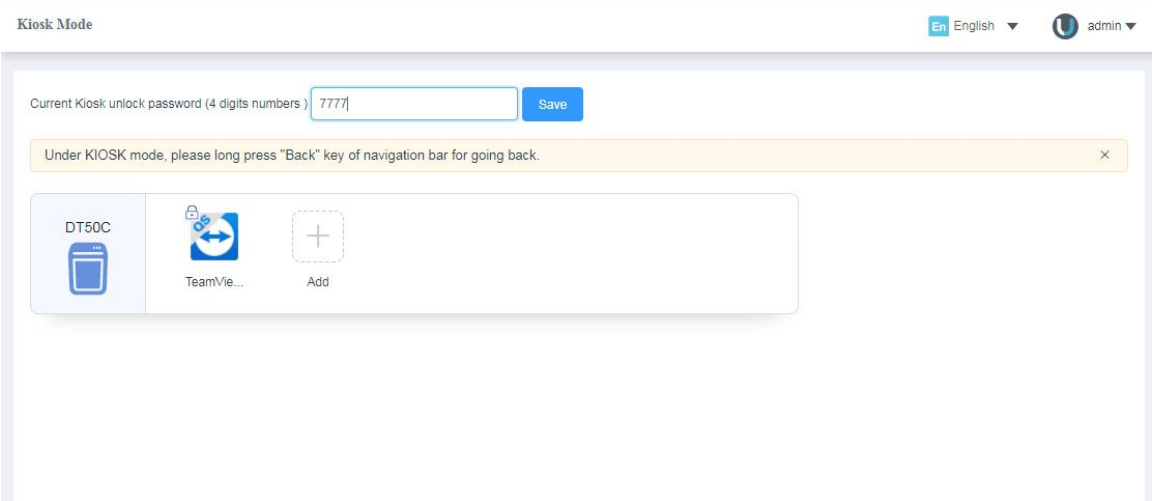


Figure (4.6.2.3)

1. Add an application to Kiosk: click the [Add] button on the right side of a model, the pop-up window will display all the applications that the model can detect. Click the [Set to Kiost] button to add it to the list of the Kiosk apps. The user can add mutiple apps;
2. Lock a Kiosk application: move the mouse on an app in the Kiosk list. Click the lock button on the upper left corner of the app. Click [Submit] to lock the app. After restarting the device, the application is locked as shown in Figure 4.6.2.3. Once the device detects the locked app, it is not allowed to logout. The device user needs to press and hold the return button to enter the password to logout from the app;
3. Change the Kiosk unlock password: click the [edit] button above, enter the four-digit password, and click “Save”. After the device detects the new Kiosk unlock password, the device user needs to enter the new password to logout from the locked application;
4. Remove an application from the Kiosk list: move the mouse on an app in the Kiosk list and click the button on the upper right corner to remove it;

4.6.3 Auto-start Application

Set the function of the default application for all devices in the current account. This page displays all the model types of the account and their set Auto-start applications. See Figure 4.6.3.1. After setting the application to default start, the default application will be

automatically opened after each boot.

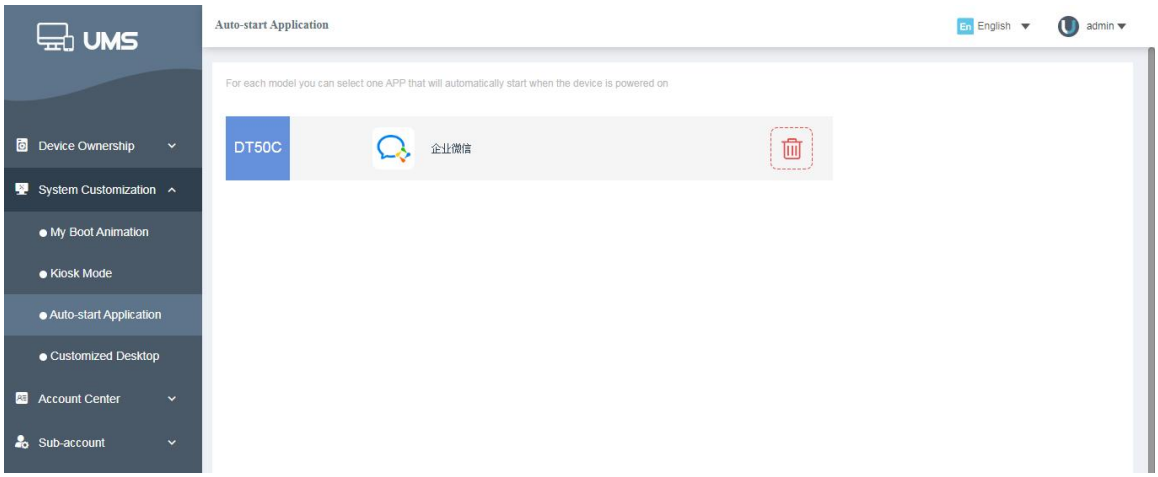


Figure (4.6.3.1)

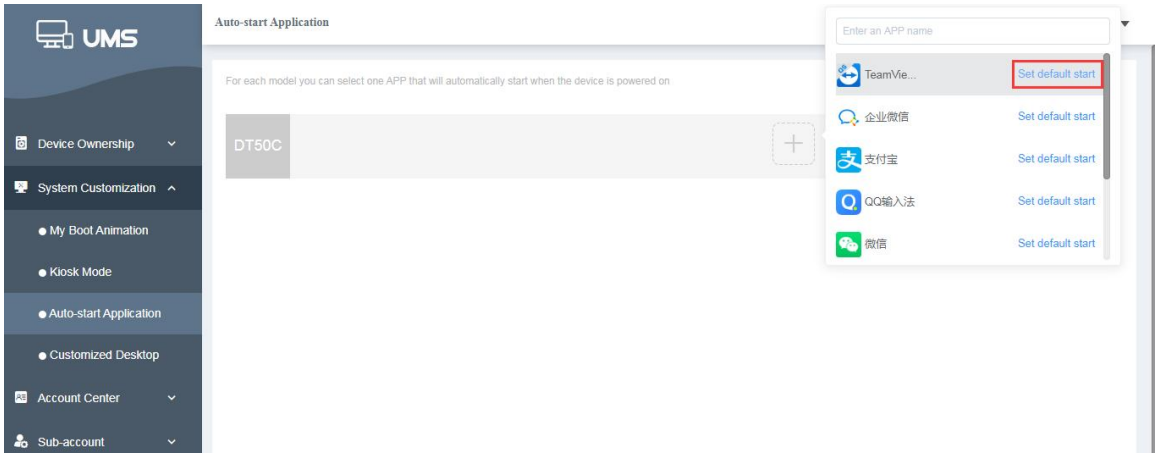


Figure (4.6.3.2)

1. Add a default application: click the Add button, the pop-up window will display all the applications that can be detected by the model device under the account, and then click the “Set Default Start” button. If the application is installed on the device, the application will be automatically opened after each boot;

2. Remove a default application: click the Trashcan-shape button on the right side of a model to remove the default application. After the app is removed, the device will not start the application automatically after each boot.

4.6.4 Customized Desktop

Provide the function of setting a custom desktop for all devices of the current account. Click [Customized Desktop] in the menu bar to enter the custom desktop page.

The page displays a list of rules. After adding custom desktop rules, uploading the Launcher APK and pushing it to the device, the device will download the custom desktop APK and make the custom desktop take effect.

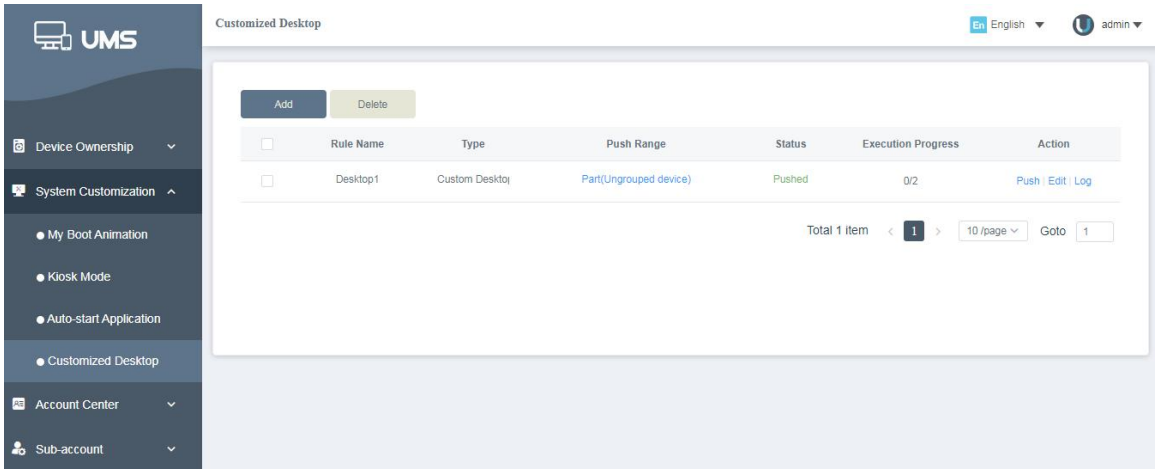


Figure (4.6.4.1)

1. Add custom desktop rules

1.1 Desktop type: custom template

Click [Add] at the top of the Customized Desktop list, add a pop-up page to the customized desktop, enter the rule name (default: my custom rules), upload the desktop APK on the custom template upload page. After uploading, click [Add] to add deployment rules successfully. After adding successfully, the custom desktop rules will be displayed in the Customized Desktop list with the status of “Un-pushed”;

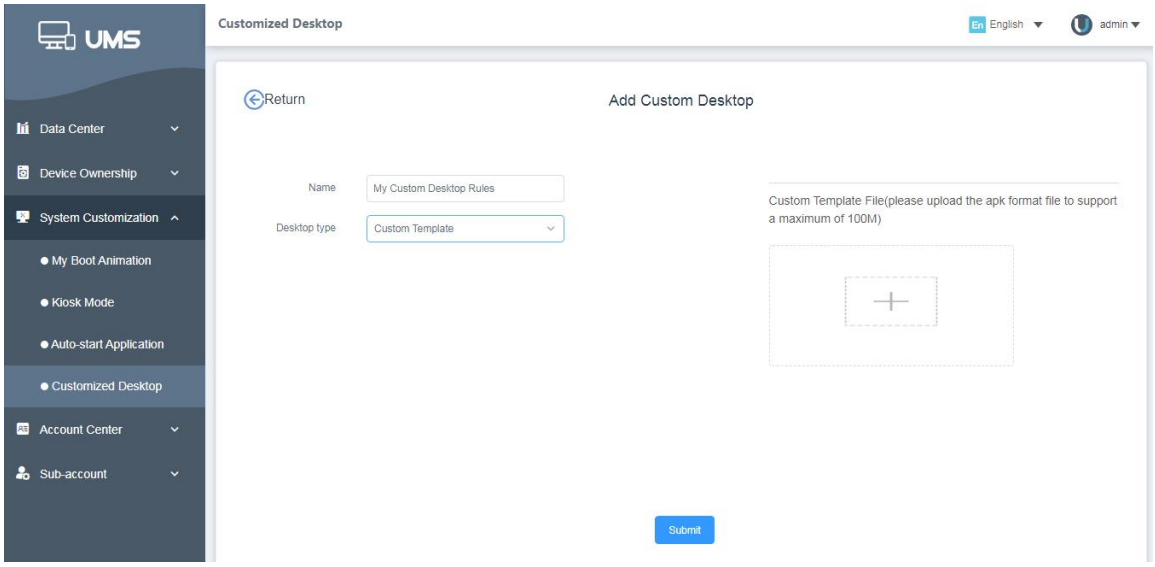


Figure (4.6.4.2)

Desktop type: Standard Template, Configuration Method: Configuration File Upload

Add pop-up page on the Customized Desktop, select the Desktop type as ‘Standard Template’ and the Configuration Method as ‘Configuration File Upload-’. After uploading the configuration file, click [Add] to add deployment rules successfully. After adding successfully, the custom desktop rules will be displayed in the Customized Desktop list with the status of “Un-pushed”;

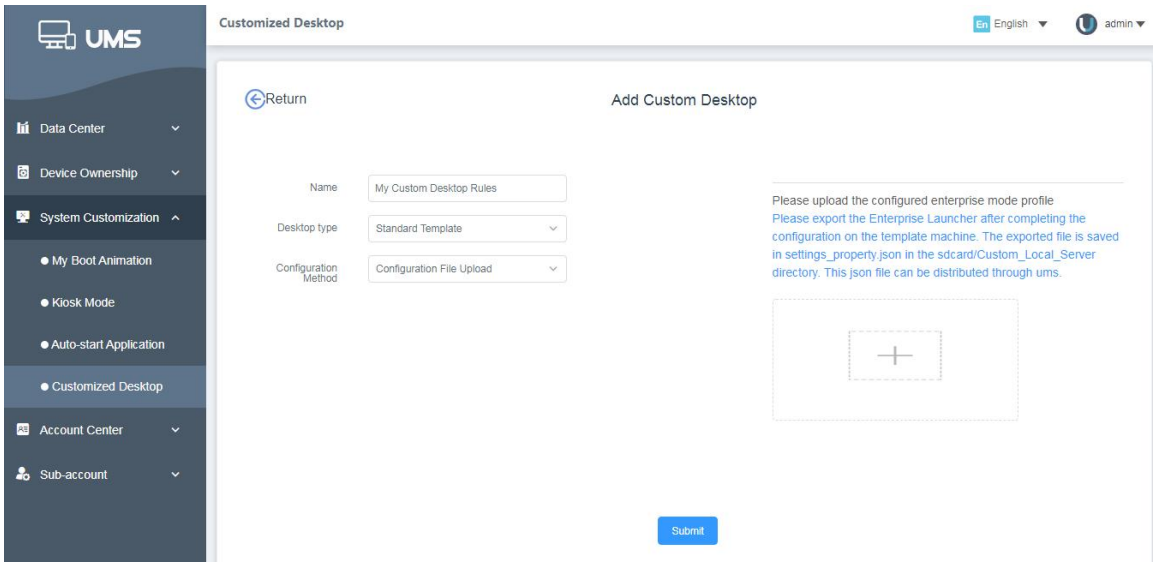


Figure (4.6.4.3)

Configuration Method: Standard Configuration

；Add a pop-up page on the Customized Desktop, select the Configuration Method as ‘Standard Configuration’, enter the Desktop Name, Admin Password (required), Desktop APP Package Name (required), select APP Icon Size (default: conventional) and click [Confirm to add] to add the deployment rules successfully. After adding successfully, the custom desktop rules will be displayed in the Customized Desktop list with the status of “Un-pushed”;

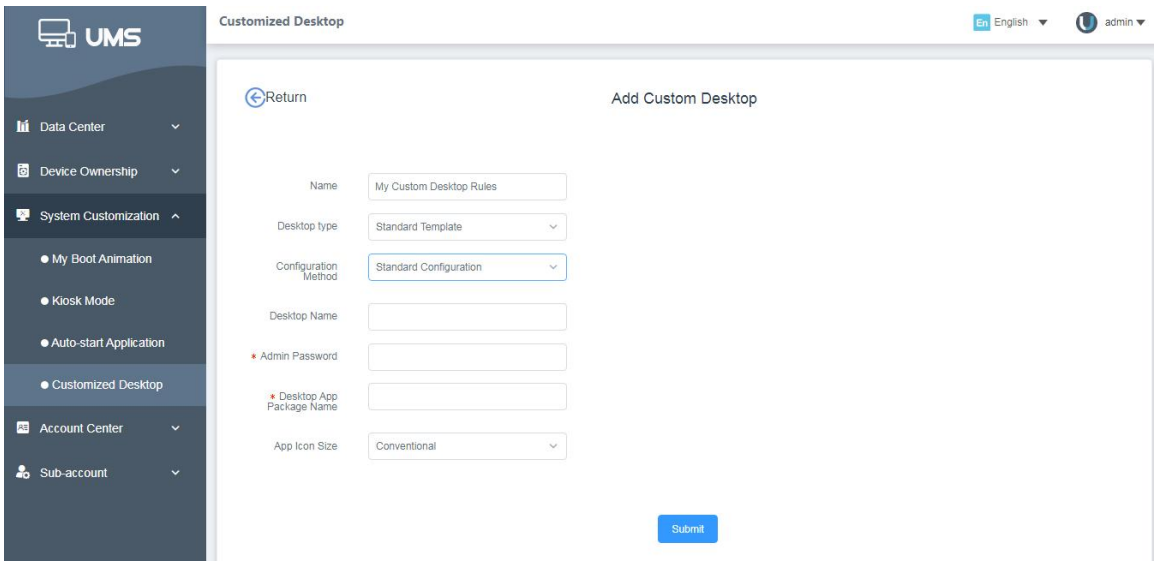


Figure (4.6.4.4)

Note:

1. The rule name is My Custom Desktop Rules by default, and the rule name cannot be repeated;

2. When multiple custom desktop rules are pushed to a group, only the latest custom desktop rules will be applied to the devices under the group;

2. Push custom desktop rules

2.1 Group push

Click [Push] in the operation bar of the custom desktop rule list, a pop-up window of "Customize desktop push" will pop up, select the group to be pushed, click [OK], and the pop-up window closes, and the status of the custom desktop rule changes to "Pushed", the progress is 0%. After receiving the instruction, the devices under the selected device group will execute this custom desktop rule, and the devices will correspondingly disable the set disabled items.

If the device under the pushed group receives a custom desktop instruction, the device displays the detected custom desktop instruction and will correspondingly disable the set disabled items. The percentage of the progress bar of this rule will increase, and the percentage of the progress bar is: **the number of the successfully executed devices/total number of devices of push group**. If all the disabled custom desktop items

are completed, the number of successfully executed devices displayed in the progress bar will be equal to the total number of devices.

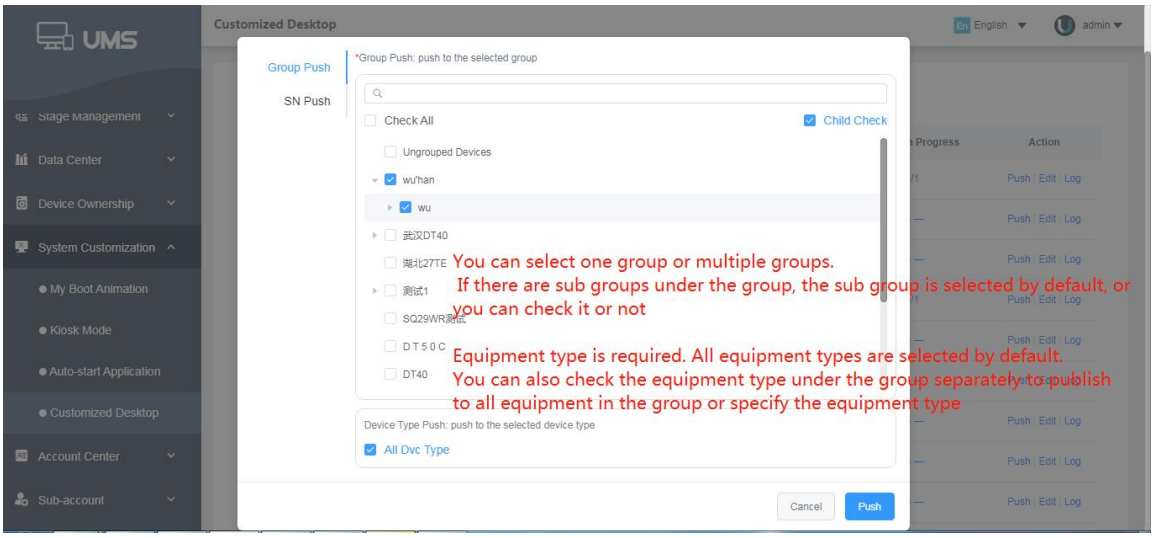


Figure (4.6.4.5)

2.2 SN push

Click [Push] in the operation bar of custom desktop rule list to pop up the window of "SN publish". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, the pop-up window will close, and the state of custom desktop rule will change to "Pushed", and the progress is 0. After receiving the command, the devices in the selected device group will execute the custom desktop rule and disable the disabled items accordingly.

If the devices in the pushed group receive the custom desktop command, the devices will display the detected custom desktop command and disable the disabled items. The percentage of the progress bar of this rule will increase. The percentage of the progress bar is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If all custom desktop items are disabled, the progress bar is displayed as 100%.

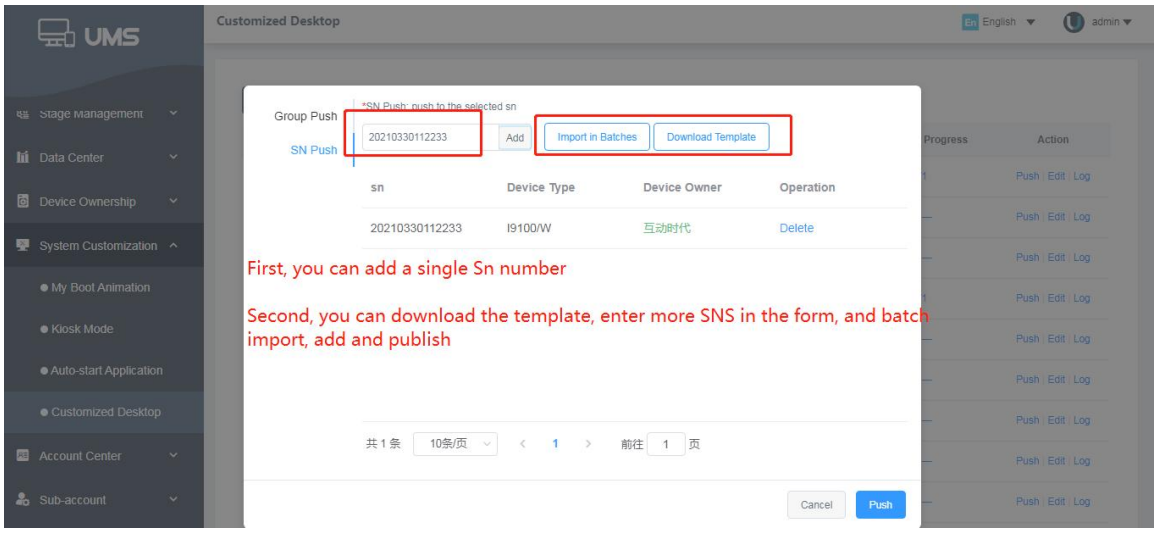


Figure (4.6.4.6)

3. Edit custom desktop rules

Click [Edit] in the operation bar of the custom desktop rule list, a pop-up window of "Customize Desktop Modification" will pop up, and you can change the custom desktop rule information. You can change the rule name, re-upload the desktop APK, etc. After modifying the rule, the previous rule will be pushed again. The progress bar for applying the rule will change to 0 again.

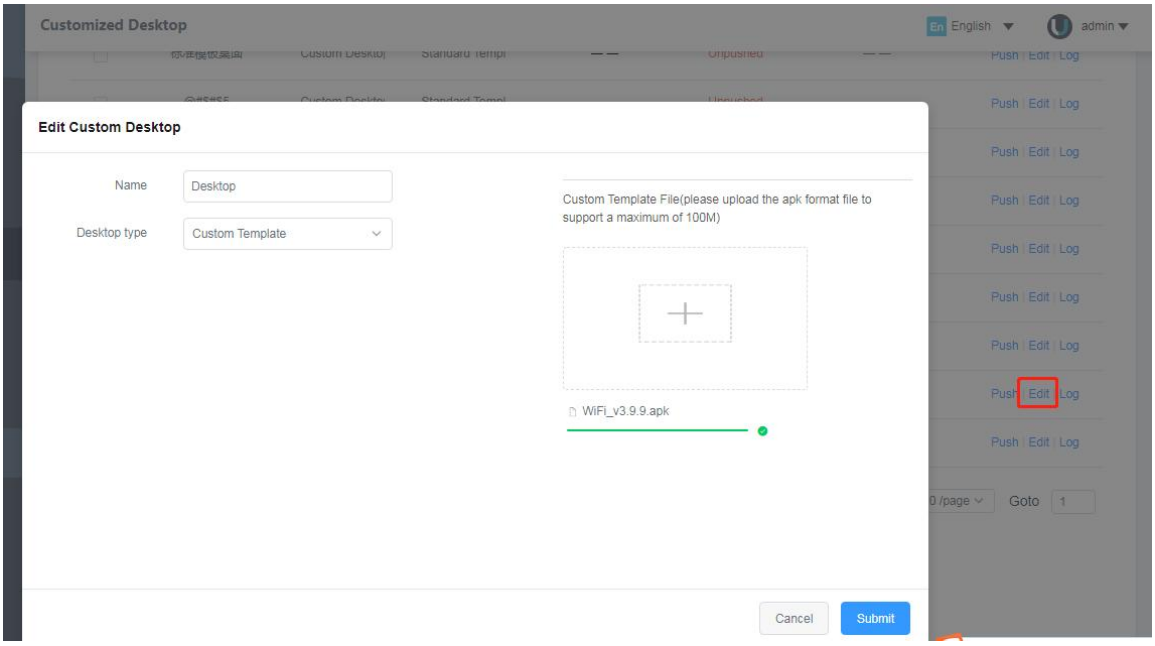


Figure (4.6.4.7)

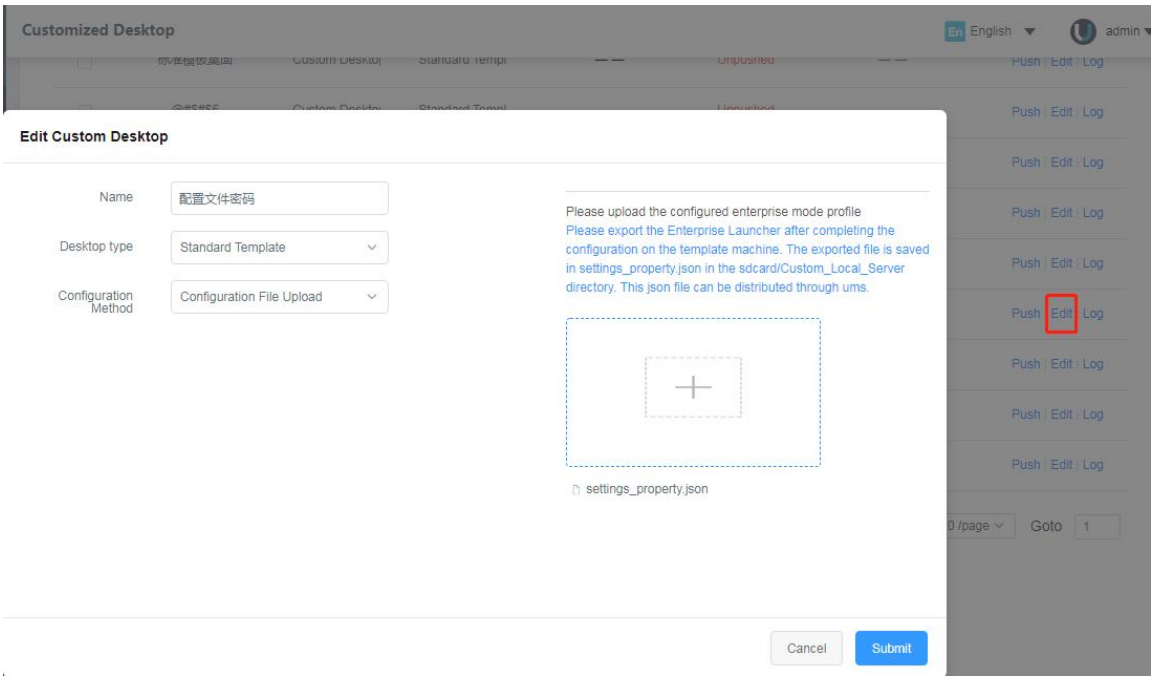


Figure (4.6.4.8)

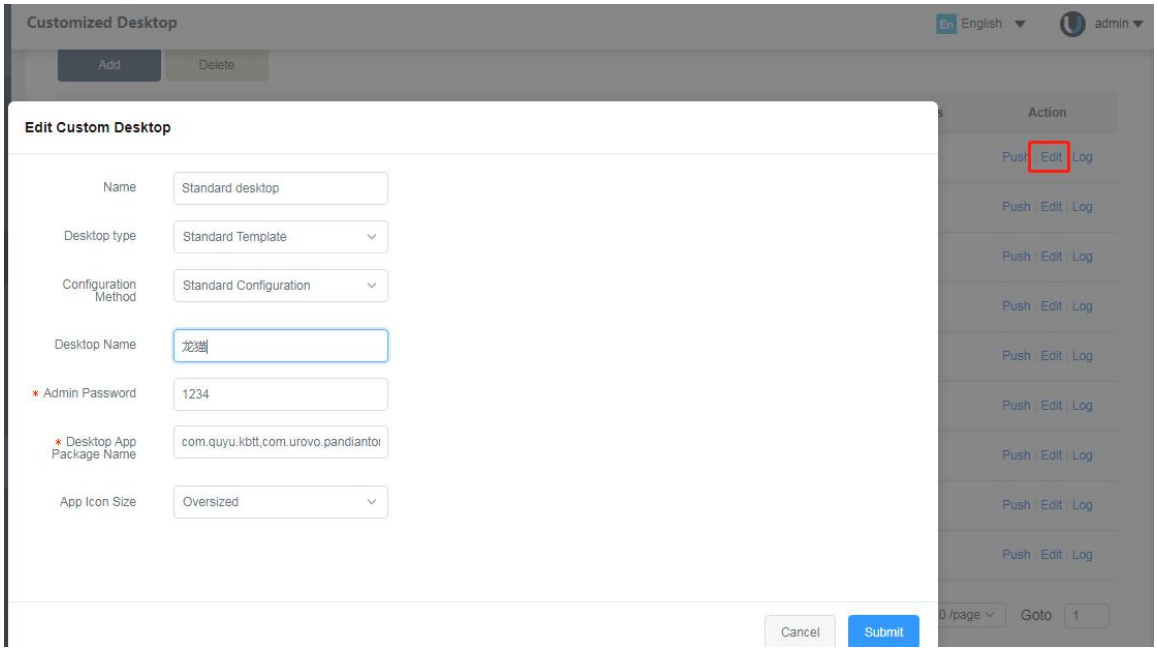


Figure (4.6.4.9)

4. Record

Click [Record] in the operation bar of the custom desktop rule, and the push record table of the custom desktop rule will be displayed. Click [View Push Content] in the operation record table to view the details of the specific push custom desktop rule

Figure (4.6.4.10)

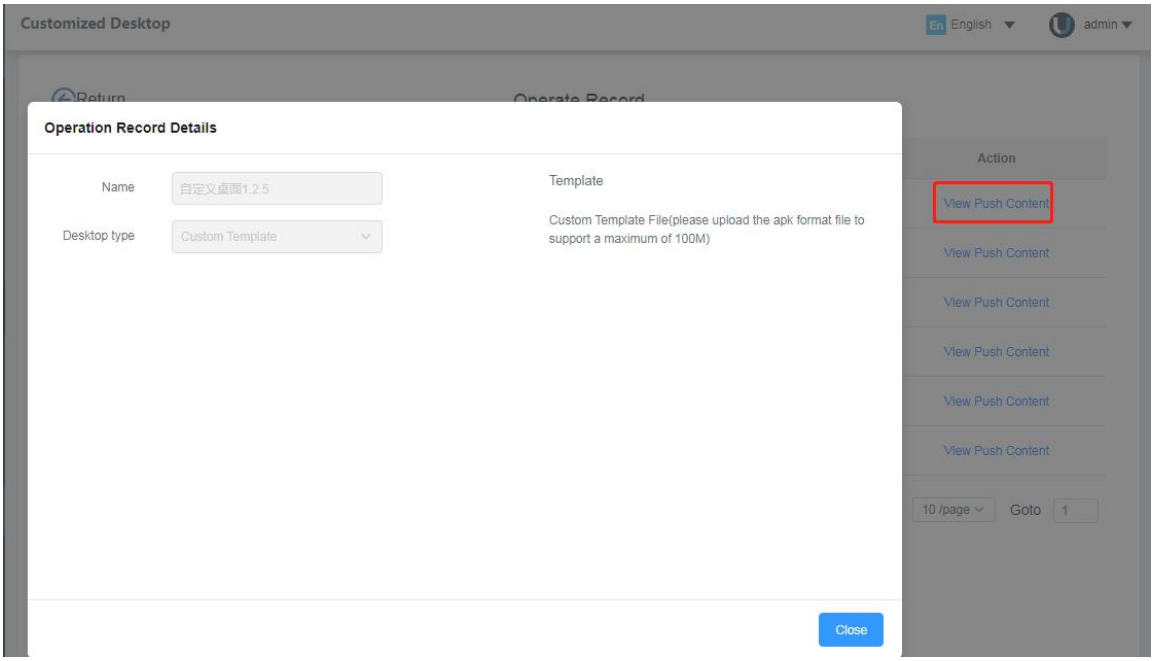


Figure (4.6.4.11)

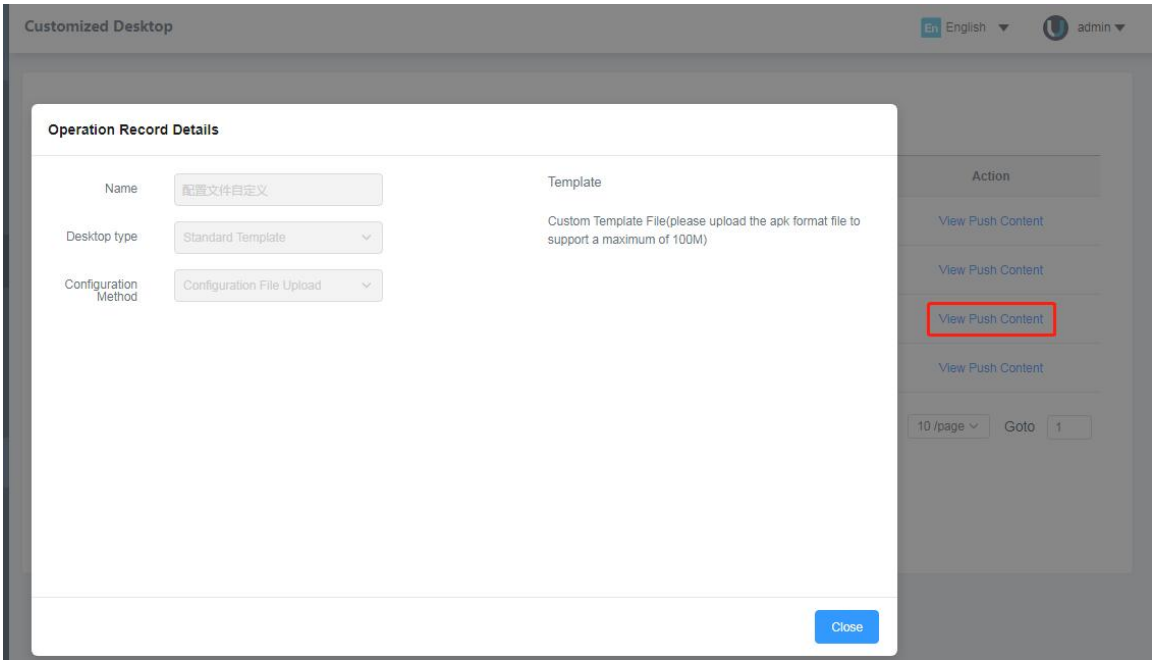


Figure (4.6.4.12)

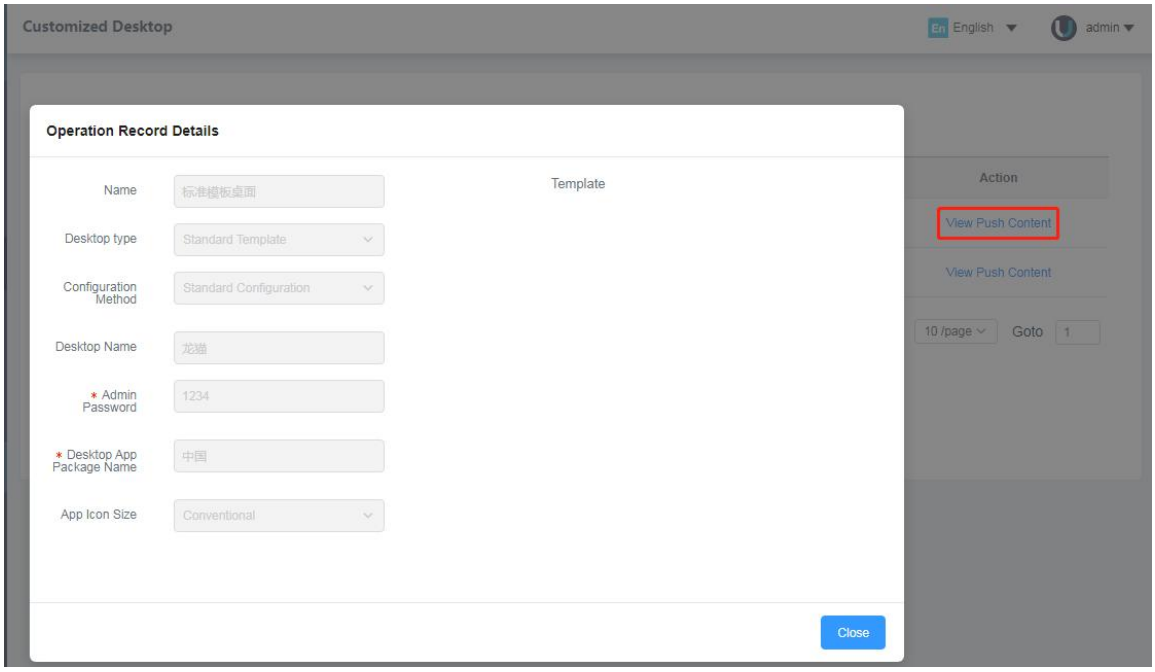


Figure (4.6.4.13)

5. Delete custom desktop rules

Click [Delete] on the top of the custom desktop list, and a delete instruction will be issued to the device. After the custom desktop rule is deleted, it will not be displayed in the custom desktop list. The device will receive the delete instruction. After receiving the delete instruction, the device will be deleted The downloaded desktop APK file and change to the default desktop rule of the application. Click the home button of the device to exit the Launcher desktop and return to the Android default desktop.

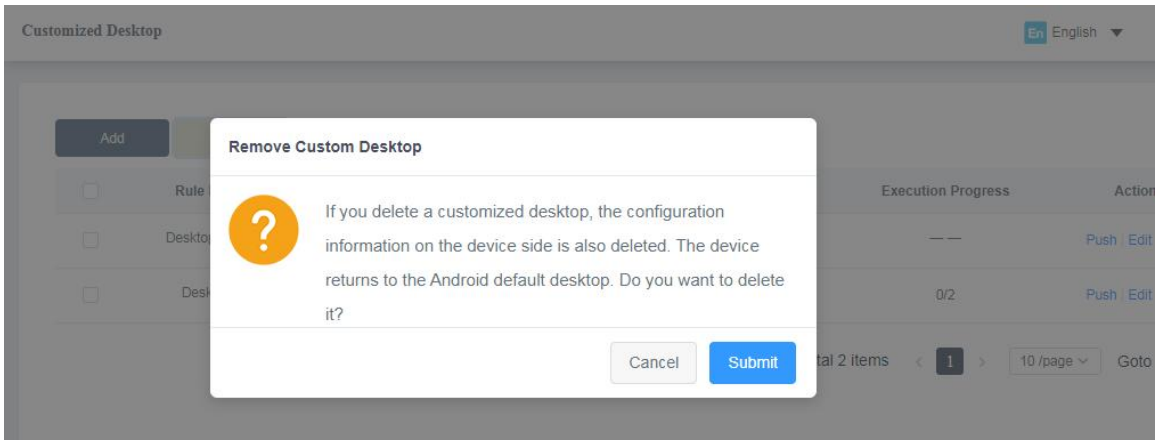


Figure (4.6.4.14)

4.7 Account Center

4.7.1 Company Information

The company information filled at registration and the generated company ID (company number) are displayed as shown below:

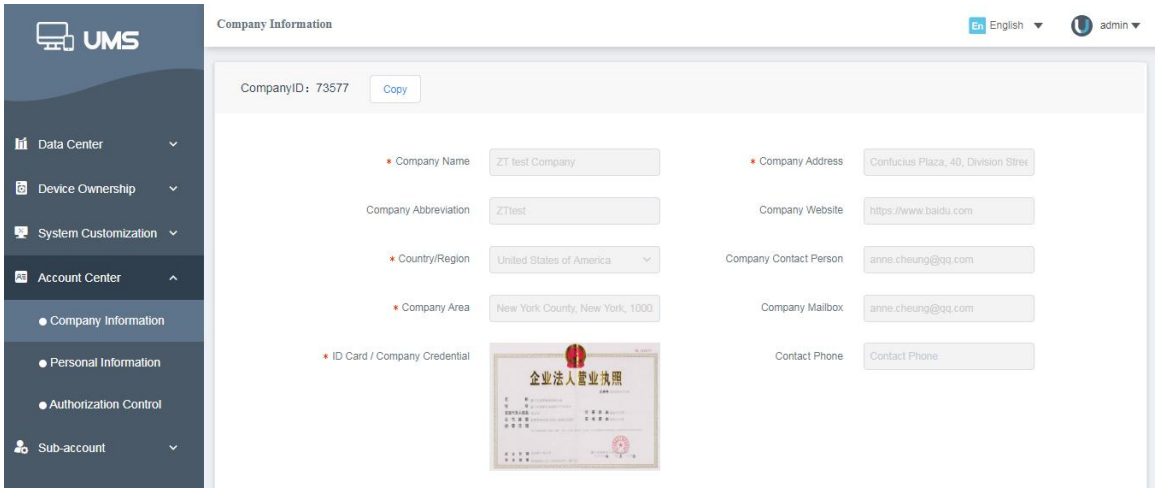


Figure (4.7.1.1)

Notes:

The registered company information can only be displayed but not be modified.

4.7.2 Personal Information

Users can modify personal information, namely editing password, name, binding e-mail and binding TEL number.

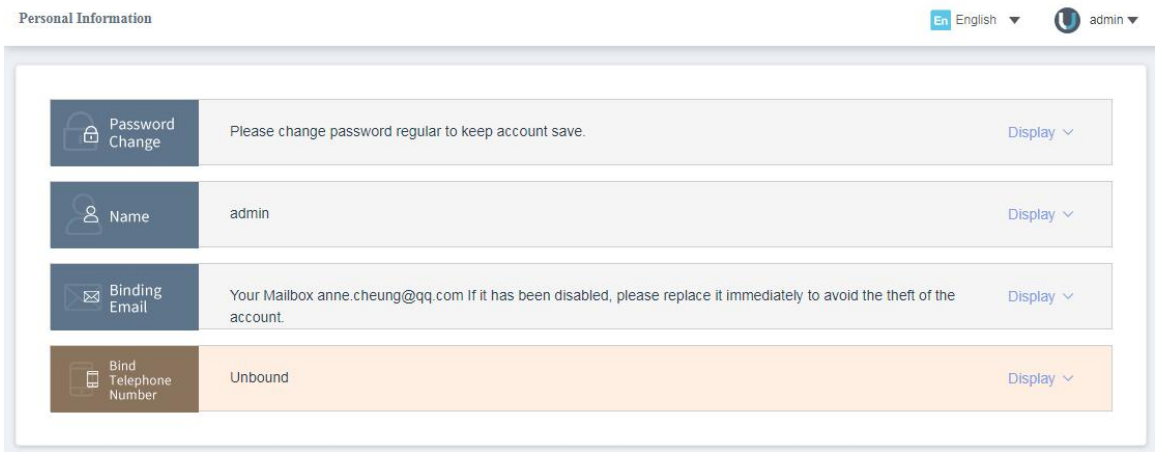


Figure (4.7.2.1)

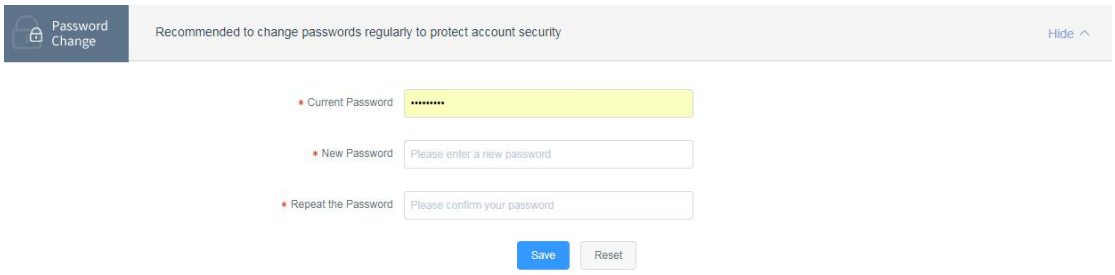


Figure (4.7.2.2)

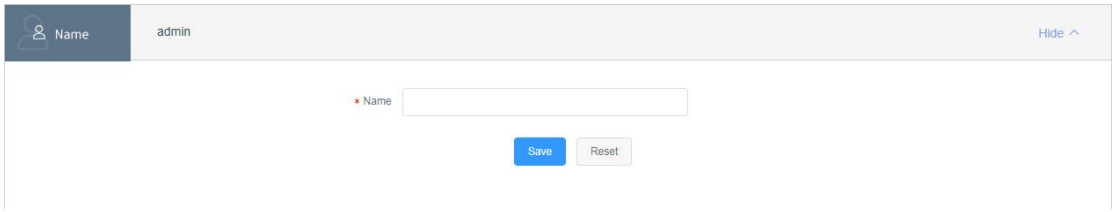


Figure (4.7.2.3)

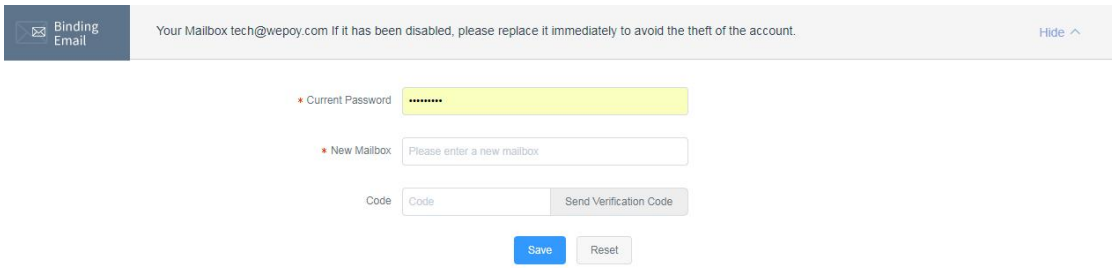


Figure (4.7.2.4)

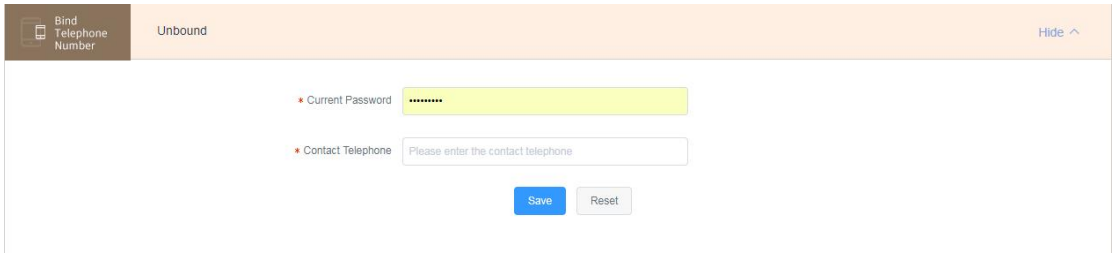


Figure (4.7.2.5)

1. Password Change: Input the Current Password, New Password, Repeat the Password, click [Save] to change the password successfully;
2. Name Change: input Name and click [Save] to modify the name;

   Attention: Password should be at least 8-digit number, which must include upper and lower case letters, number and special characters;
3. Binding E-mail Change: input the current password, new e-mail address, the mailbox

will receive verification code after click [Send verification code]. Input the verification code and click [Save] to change the E-mail successfully. The account will be logout automatically after this operation. The user needs to enter the new e-mail address to login the next time.

4. Binding Tel Number Change: input the current password and Tel number then click [Save] to bind the new Tel number.

4.7.3 Authorization Control

This page displays the operator information of the login account, including E-mail address, roles, and permissions. You can add operators and modify operator permissions.

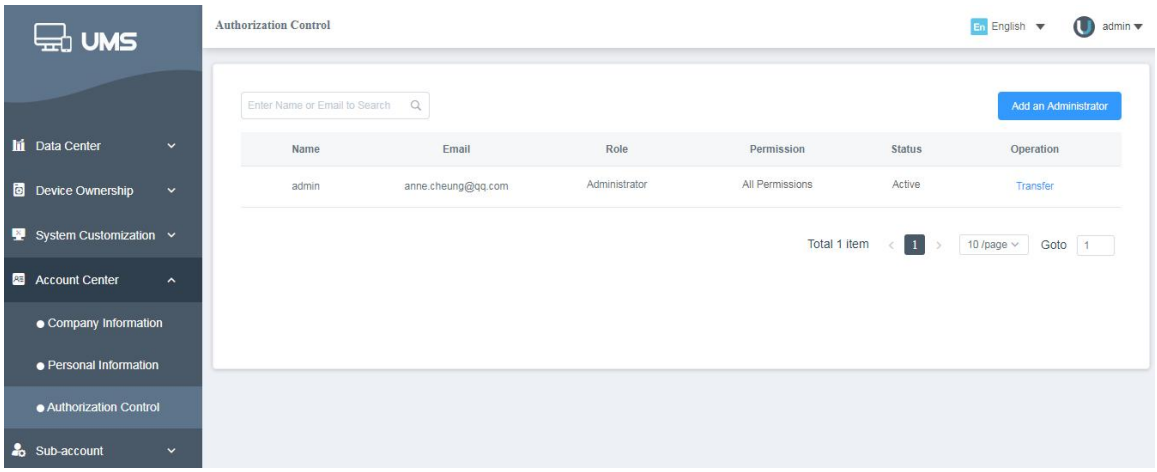


Figure (4.7.3.1)

1. Enter the merchant name or abbreviation, and then click the [Search] button to display the corresponding operator information;

2. Add operator: Click [Add operator], enter the email address, name, and click [Confirm], the system will send an email to the corresponding email address, and the email contains the initial login password. After the operator logs in, the initial password status changes to "Activated" "status;

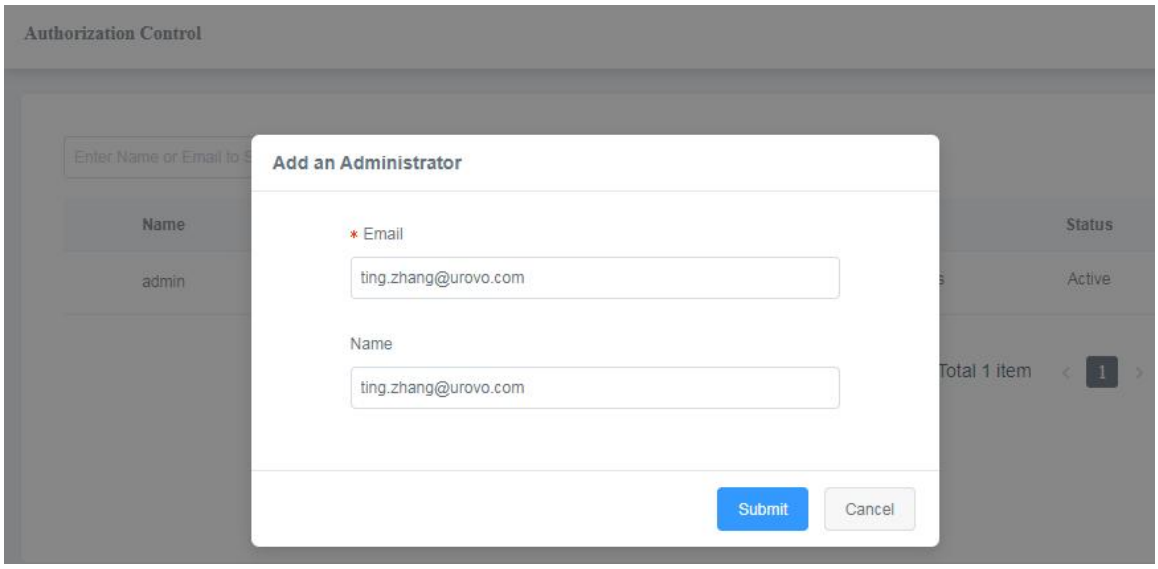


Figure (4.7.3.2)

3. Modify operator permissions: click on the permissions in the [Permissions] column, and check permissions in the select permissions pop-up window, then the operator will get the corresponding permissions after logging in to the system;

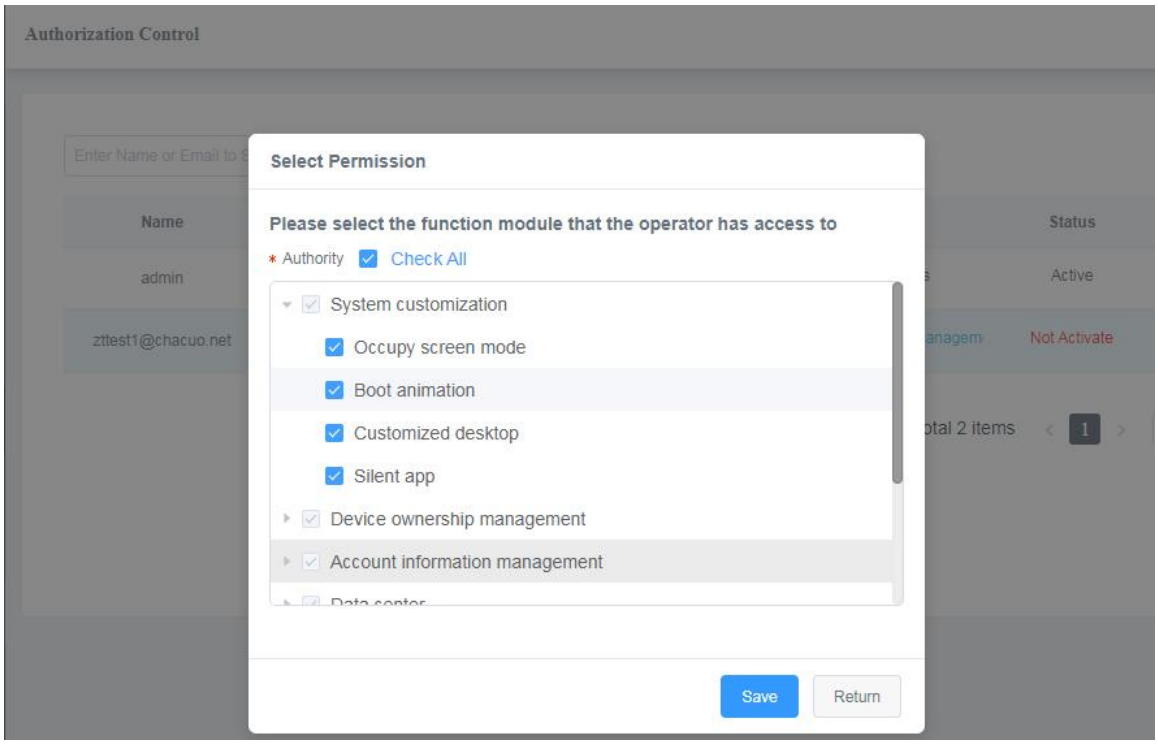


Figure (4.7.3.3)

4. Transfer to the administrator authority: Click the [transfer] button on the right side of the administrator user, select an operator, and enter the password of the currently logged-in user to transfer the administrator authority to the operator;

Note: After the authority is transferred, the operator becomes a new administrator with all the authority of the administrator, and the original administrator becomes an operator with all the authority, and the authority can be changed;

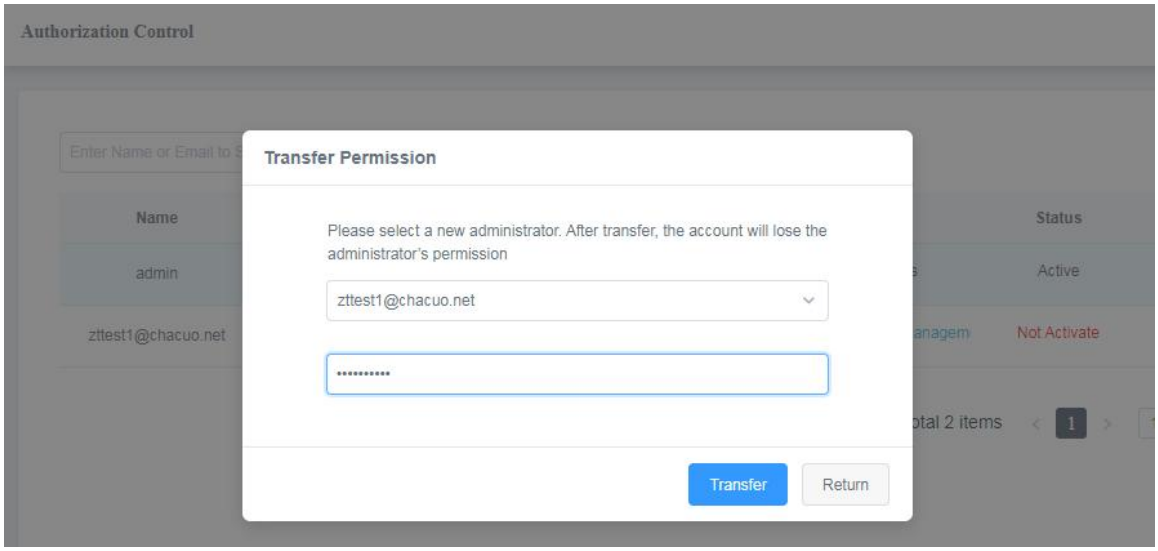


Figure (4.7.3.4)

4.8 Sub-account

Click [Sub-account]]-[Sub-account Brief] to view all the sub-accounts' information of the current account, including Control and Independent accounts, as shown below:

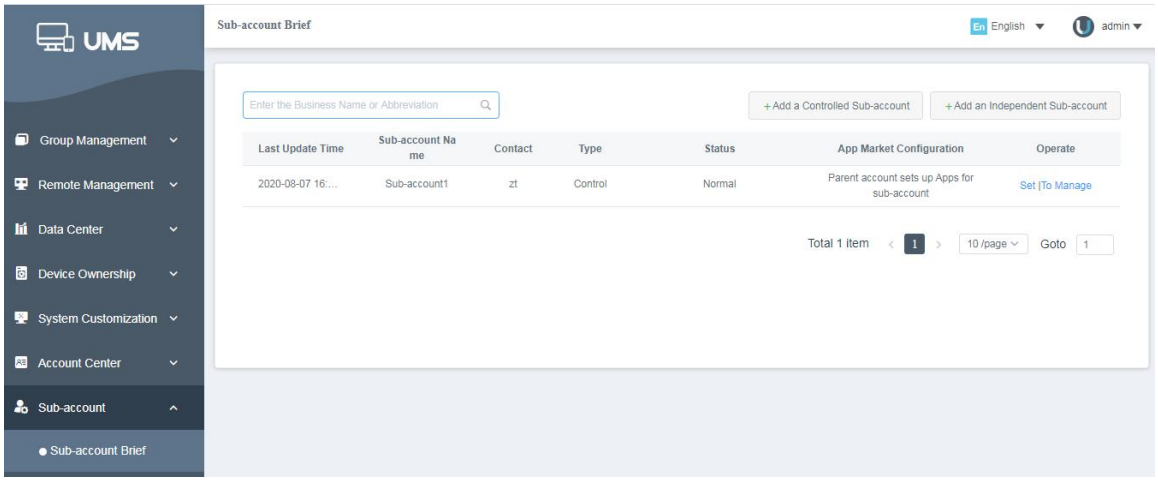


Figure (4.8.1)

(1) Controlled Sub-account： Parent Account can manage Controlled Sub-accounts directly. Controlled Sub-accounts have no own operators. Parent Account can distribute operators to manage its controlled sub-accounts. No application upload permission

without administrator;

The Controlled Sub-accounts cannot upload application. Apps from the app list are sourced from the Parent Account. There are four ways to configure apps to Controlled Sub-accounts' application market.

a) Completely independent and free App market: Sub-account chooses Apps from the list of Apps available on the App market. No control on Apps available for download by sub-accounts.

b) Clone the Apps of the parent account: Apps available to the sub-account will be exactly the same as the parent account, including the seting position of the auto-installed Apps. If the mother-user status bar is the group launched, sub-user condition also same like mother-user, system default tag all group of sub-user. The sub-account's [App List] cannot be operated and managed, only for display

c) Select from the App market of the parent account: Sub-account only selects from the Apps available on the main Parent account channel.

d) Parent account sets up Apps for sub-account: Apps available to Sub-account are completely fixed and decided by the parent account. The sub-account's [App List] cannot be operated and managed, only for display

(2) Independent Sub-account: Own operators allowed. The independent accounts are free to upload, shelf on and off applications.

1. Add a Sub-account:

1) Click [Add a Controlled Sub-account] to input the name, abbreviation and contact, and then click [Save] to add a controlled sub-account successfully. Click [To Manage] to add operators to the sub-account, giving the sub-account access to login to the account management platform;

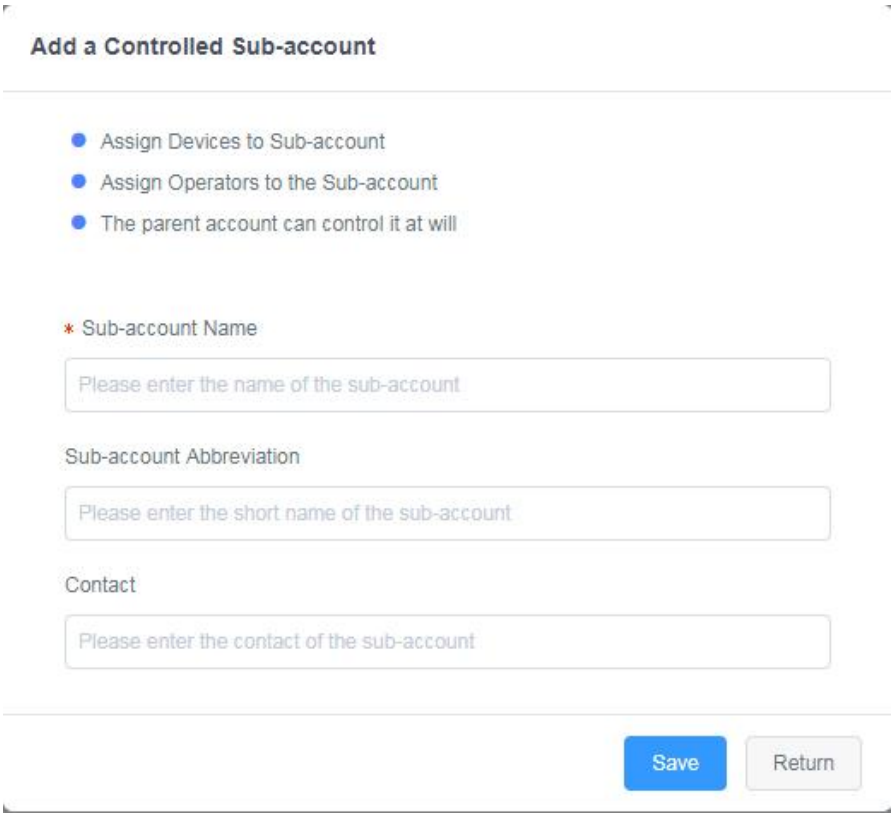


Figure (4.8.2)

2) Click [Add an Independent Sub-account] to input the name, abbreviation, contact, and admin mailbox, and then click [Save]. The system will send a dynamic password to the mailbox. Logging in to the system with the dynamic password will be considered as successful activation of the independent sub-account. After the activation, the sub-account can use the e-mail to login to the account management platform;

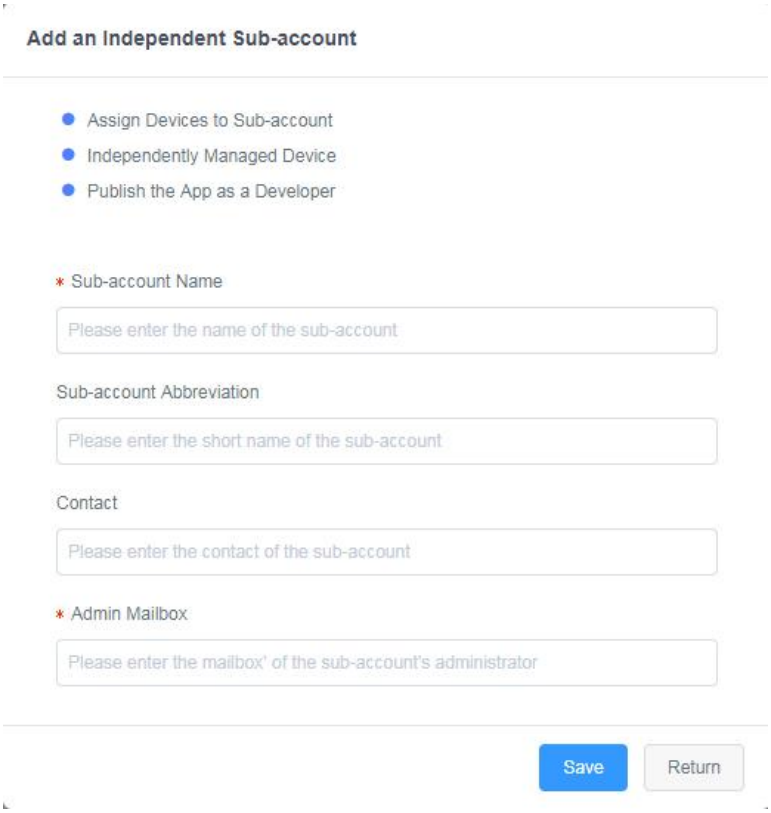


Figure (4.8.3)

2. Change the way of controlled sub-merchant application market:

Select a controlled sub-merchant, click [Settings] in the operation bar, select one of the four methods, and click [Submit] to change successfully;

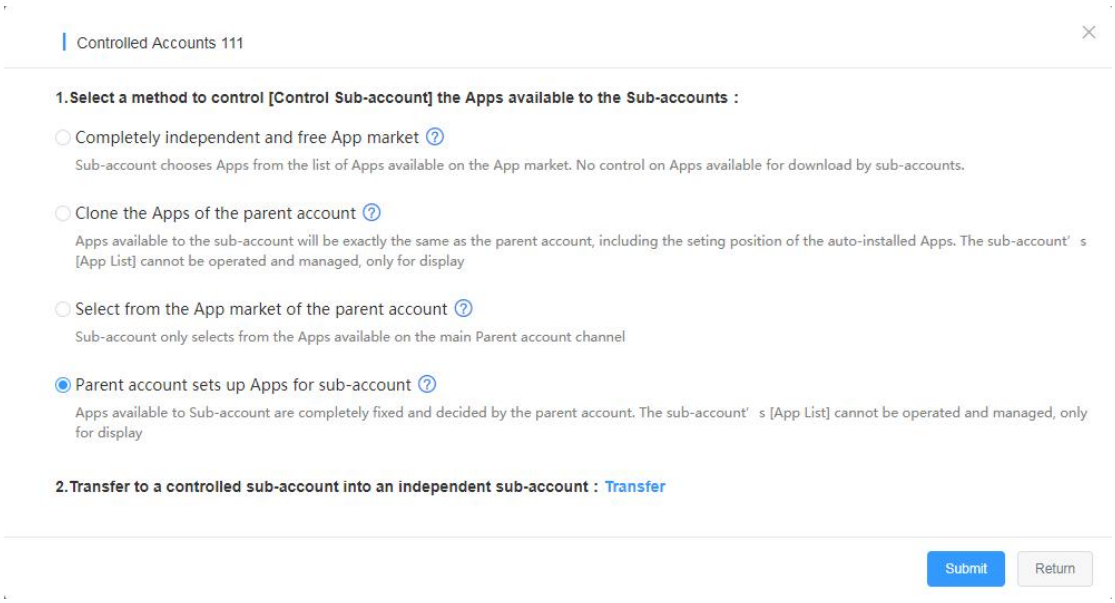


Figure (4.8.4)

3. Transfer a controlled sub-account to an independent sub-account:

Choose one of the independent sub-accounts. Click [Set] on the operation bar and then click [Transfer] on the pop-up window. Enter the Admin E-mail to receive a dynamic password. Login to the platform via the dynamic password and change the initial password to successfully transfer a sub-account;

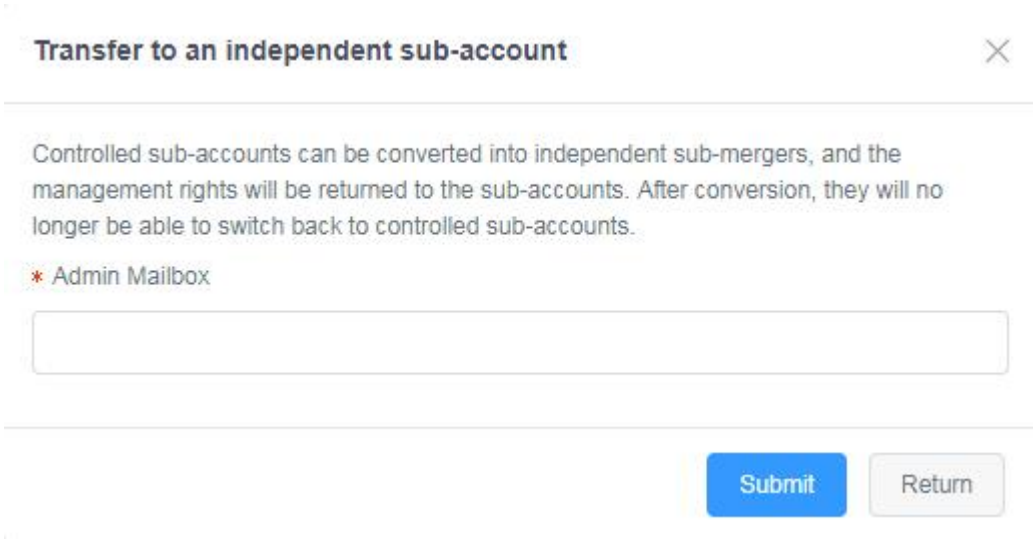


Figure (4.8.5)

4. To Manage:

Choose one of the controlled sub-accounts. Click [To Manage] to access into the sub-account. Operations to sub-account's devices and applications are available. Click [Return to the parent account] on the top right corner to go back to the parent account;

Notes:

The function of the sub-account platform is basically the same as that of the parent account platform except that the sub-account platform lacks the function of [Device Ownership] and [Sub-account]. The other functions, namely the [APP Store], [Remote Management], [Data Center] and [Account Center], are basically the same.

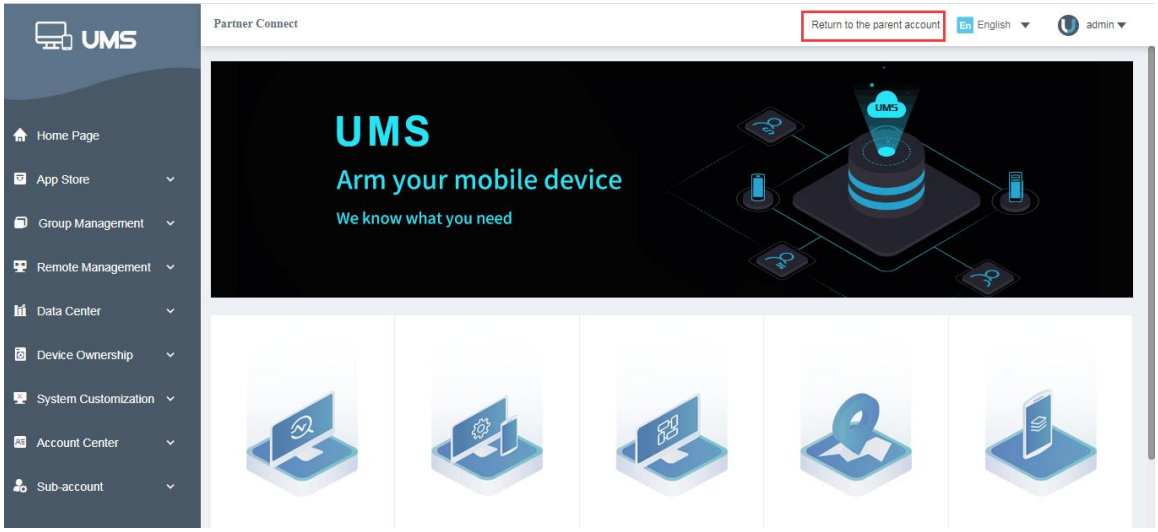


Figure (4.8.6)

Notes:

If a parent account is the first-level account, under the first-level account, sub-accounts can be rebuilt, and up to five levels can be established. The sub-account's authority is basically the same as that of its parent account. The fifth-level sub-account can no longer build up its sub-accounts.

4.9 Stage Management (new function)

Click [Stage Management] - [Configure Management] to display the rule configuration list on the configure management page. After the configuration rules are uploaded, they are published and pushed to certain groups or SNs. The devices in this group or SNs added separately will automatically configure files according to the rule, as shown in the Figure below:

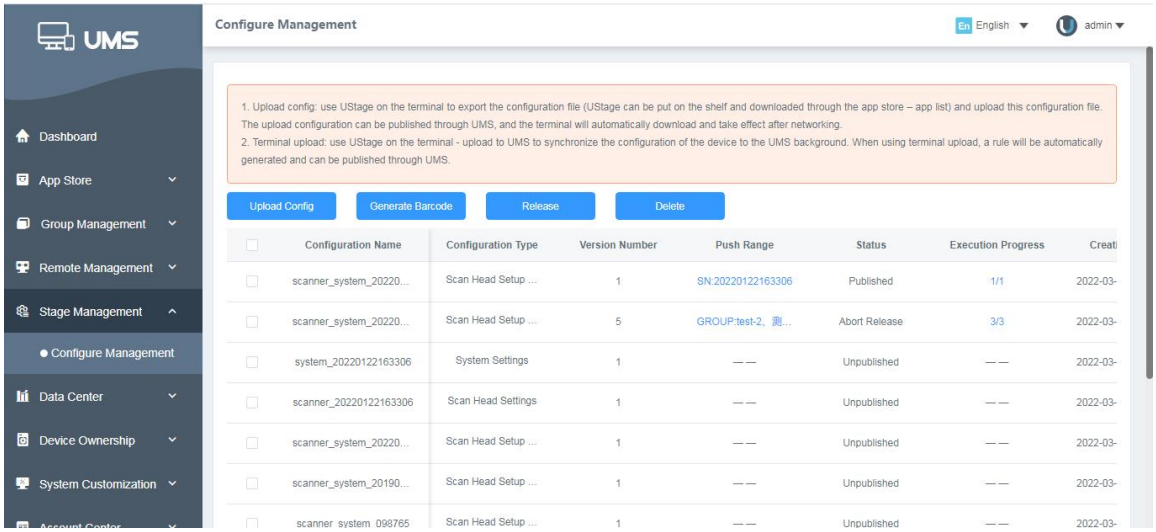


Figure (4.9.1)

1.1 Upload configuration (terminal upload)

Terminal upload: Use terminal application UStage to upload it to UMS, and synchronize the configuration of the device to the UMS background. A rule will be automatically generated when the configuration is uploaded to the corresponding account on a terminal. The configuration rule will be displayed in the configure management list and its status is "Not Published".

There are three types of uploaded files: Scanner (scanner configuration), System (system configuration), and ScannerSystem (scanner configuration and system configuration);

Note: For details on terminal operations, please refer to the operation document of terminal Ustage.

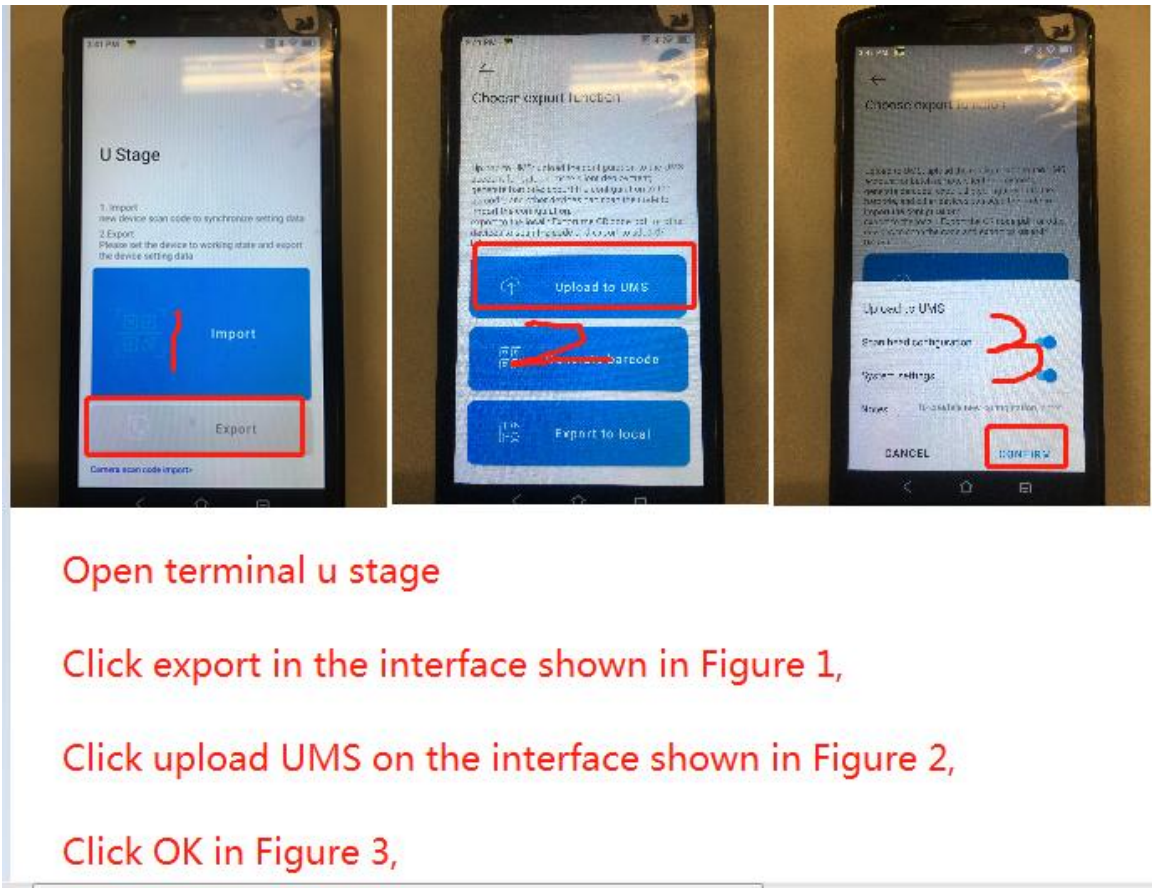


Figure (4.9.1)

1.2 Upload configuration (configuration file upload)

Use terminal application UStage to export the configuration file to Local (UStage can be added and downloaded through the application market). Export the configuration file from the device, copy it to the PC, and upload the configuration file. The configuration rule will be automatically generated on the page. The configuration rule will be displayed in the configure management list and its status is "Not Published", as shown in the Figure below.

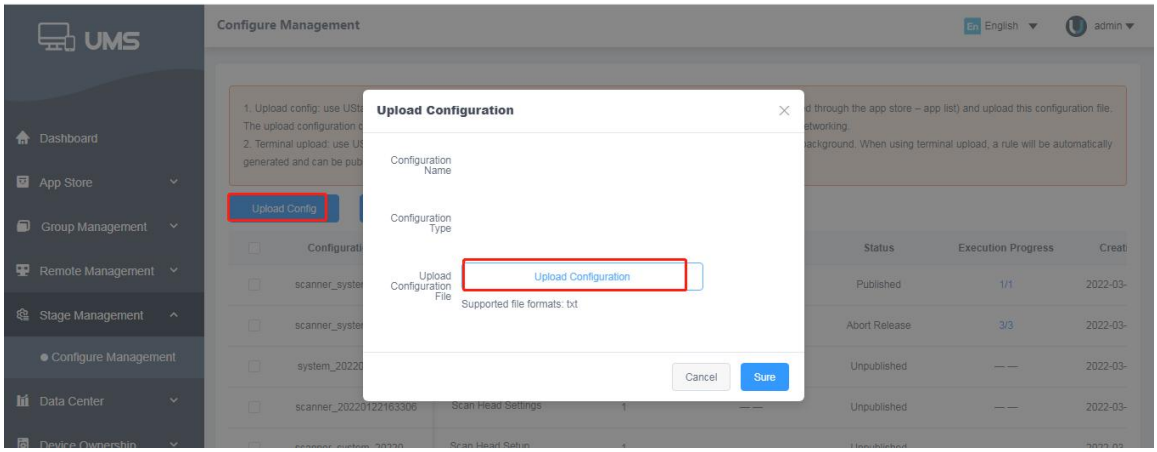


Figure (4.9.1.2)

Note:

1. In the case of no remarks field, only one rule is displayed in the background to overwrite the previous file when the configuration is uploaded multiple times on the same device; That is, with the configuration name as the judgment condition, duplicate names are overwritten and different names are created;

2. Barcode generation

Select a rule to generate a QR code. The pop-up window displays the following contents: configuration name, configuration type, prompt message, QR code, download QR code; The device can scan the QR code to import the configuration. Therefore, the configuration information can be written into the barcode and exported to a local file for scanning by all devices of the same type (import configuration by remote scanning);

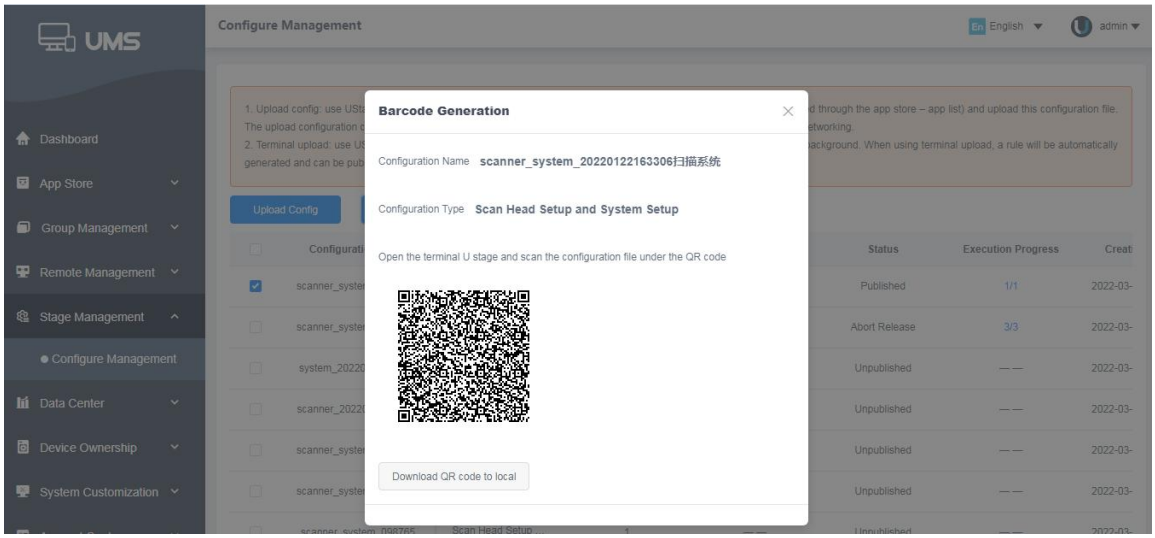


Figure (4.9.3)

1. Publish

2. 3.1 Group publish

Select a configuration rule from the configure management list and click [Publish] to pop up the window of "Group Publish". You can select one or more groups. By default, subgroups are associated. Select all devices in the group or specify the device type, and then click [Publish]. After that, the pop-up window will close. The state of the configuration rule will change to "Published", and the progress is 0/number of devices pushed. The devices in the selected device group will execute the configuration rule after receiving the command, and devices of the same type will execute the configuration.

The progress of the rule will increase, and the progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If all devices are connected to the configuration, the number of successfully executed devices displayed on the progress bar is equal to the total number of devices.

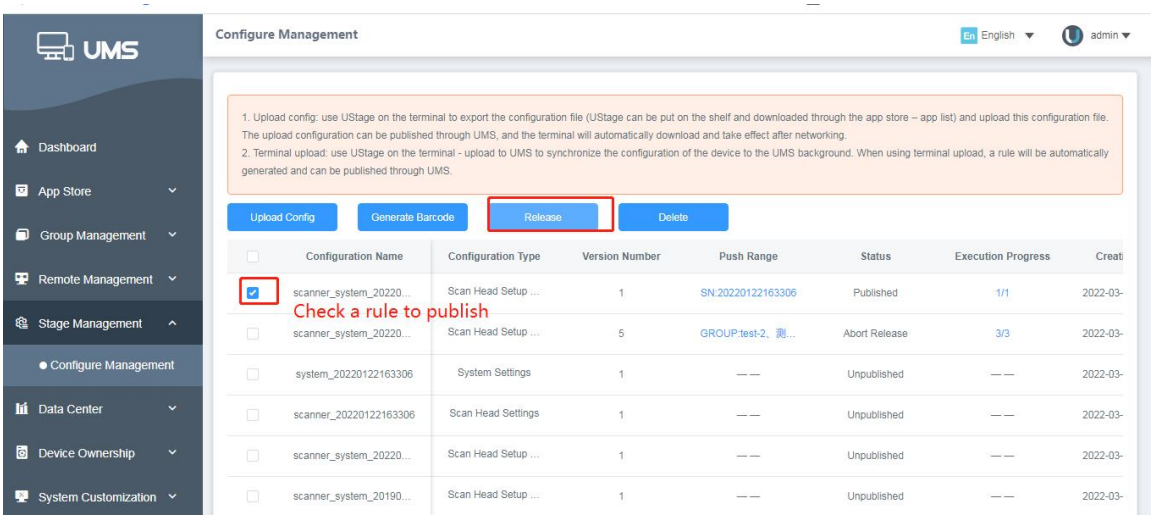


Figure (4.9.4)

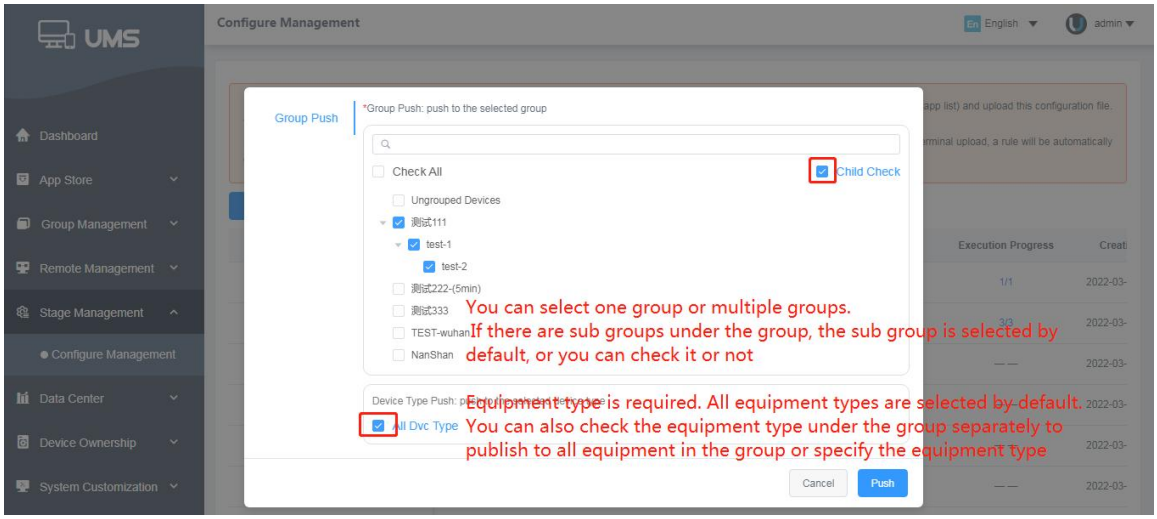


Figure (4.9.5)

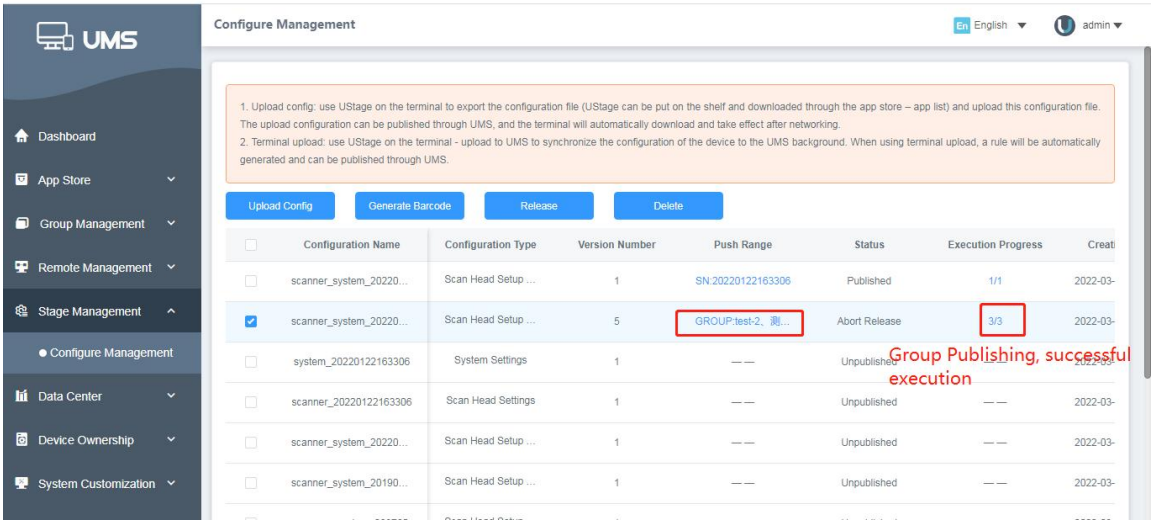


Figure (4.9.5)

3.2 SN publish

Select a configuration rule from the configure management list and click [Publish] to pop up the window of "SN Publish". You can add a single SN or add multiple SNs through [Download Template] - [Batch Import], and then click [Publish]. After that, the pop-up window will close, and the state of configuration rule will change to “Pushed”, and the progress is 0/number of devices pushed. After receiving the command, the devices in the selected device group will execute this configuration rule, and devices of the same type will execute the configuration.

The progress of the rule will increase, and the progress is displayed as: Number of successfully executed devices/Total number of devices in the pushed group. If all devices are connected to

the configuration, the number of successfully executed devices displayed on the progress bar is equal to the total number of devices.

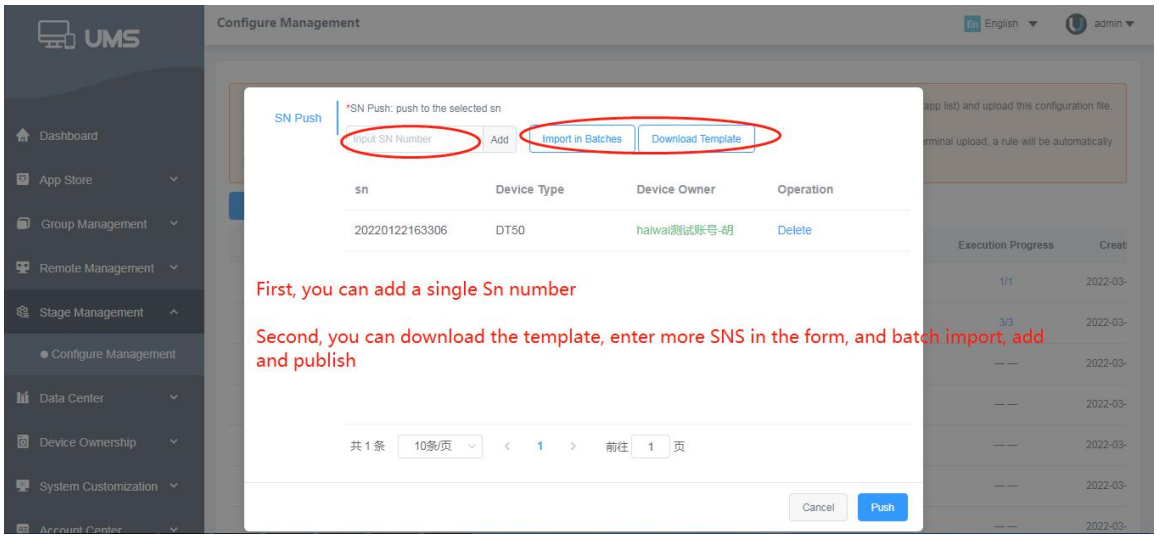


Figure (4.9.6)

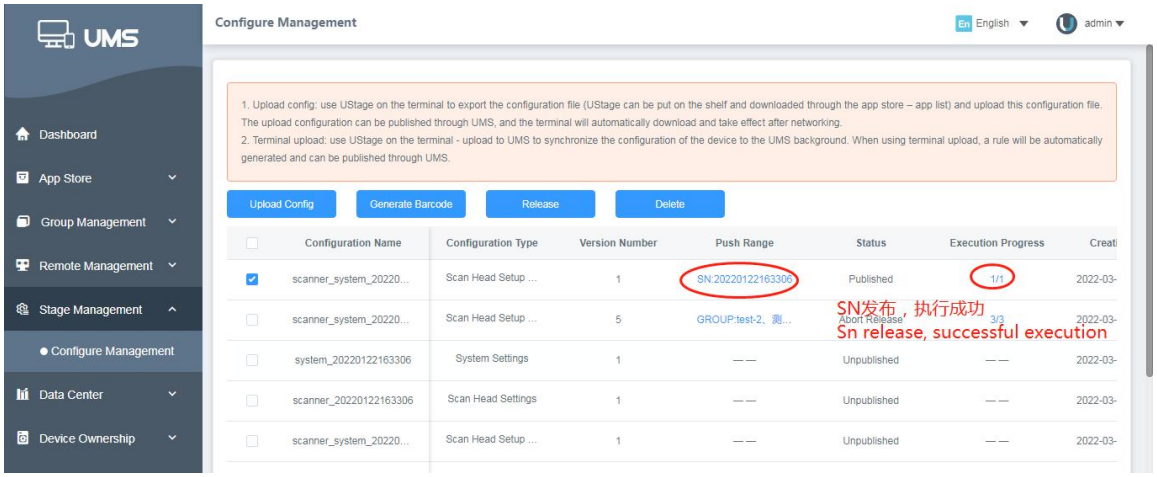


Figure (4.9.7)

Note:

When multiple configurations are pushed to the same device, the latest rule is executed;

4. Delete

Click [Delete] on the top of the configure management list. After the configure management rule is deleted, it will not be displayed in the configure management list. If any device has not received push or executed configure management command, this configure management rule will not be executed. The devices in the device group will no longer detect this configure management rule.

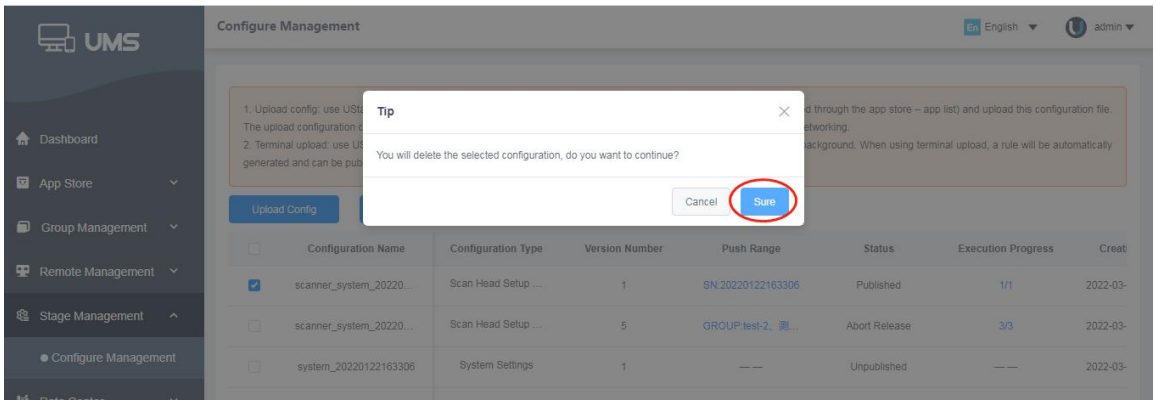

UMS
Configure Management
English
admin
Dashboard
App Store
Group Management
Remote Management
Stage Management
Configure Management
Upload Config
Tip
You will delete the selected configuration, do you want to continue?
Cancel
Sure
Configuration Name
Configuration Type
Version Number
Push Range
Status
Execution Progress
scanner_system_20220...
Scan Head Setup ...
1
SN:20220122163306
Published
1/1
2022-03-
scanner_system_20220...
Scan Head Setup ...
5
Abort Release
3/3
2022-03-
system_20220122163306
System Settings
1
Unpublished
2022-03-

Figure (4.9.8)