



# **Allixon Device Management User Manual**

Version: v1.12

Release date: 13 May 2020

## Revision History

Version	Date	Author	Modification
V1.0	2017/10/27	Dora Wang	<ul style="list-style-type: none"> <li>• First release based on BDM Portal v1.02</li> </ul>
V1.1	2018/3/1	Dora Wang	<ul style="list-style-type: none"> <li>• Add regional server : China (Beijing)</li> <li>• Release based on BDM Portal v1.03</li> </ul>
V1.2	2019/08/26	James Chou	<ul style="list-style-type: none"> <li>• Release based on BDM Portal v2.07</li> <li>• Update the action list for “8.2 Manage roles”.</li> <li>• Update the content and pictures for “8.2.1 Create new roles” and “8.2.2 Edit/Delete Existing Roles”.</li> </ul>
V1.3	2019/08/28	James Chou	<ul style="list-style-type: none"> <li>• Release based on BDM Portal v2.07</li> <li>• Update the picture in “3. Sign In”</li> <li>• Remove the content “Switch the regional server” in “4.1 Enter Dashboard”.</li> </ul>
V1.4	2019/12/04	James Chou	<ul style="list-style-type: none"> <li>• Release based on BDM Portal v2.09</li> <li>• Add section “6.2 Prepare the Information for Your Application”</li> <li>• Add two notes and update the application release and distribute flow in section “6.5.1 Create Application Versions”</li> <li>• Update the version state in section “6.5.2 Modify the Application Build”</li> <li>• Update the apply policy flow in section “7.2 Apply Policy”</li> <li>• Remove section <ul style="list-style-type: none"> <li>– Approve/Reject Application Versions</li> <li>– Manage Apps</li> <li>– Recall Policy Change Approval Request</li> <li>– Add new section “Alerts”</li> </ul> </li> </ul>
V1.5	2019/12/06	James Chou	<ul style="list-style-type: none"> <li>• Release based on ADM Portal v2.09</li> <li>• Change all wording from “BDM” to “ADM”</li> <li>• Change all wording from “Acer” to “Allxon”</li> <li>• Change all wording from “Being Device Management” to “Allxon Device Management”</li> <li>• Remove wording “BYOC”</li> </ul>
V1.6	2019/12/12	Judy Tsui	<ul style="list-style-type: none"> <li>• Alert for hardware watchdog is only available on selected devices.</li> </ul>
V1.7	2019/12/18	James Chou	<ul style="list-style-type: none"> <li>• Release based on ADM Portal v2.09</li> <li>• Update the content and screenshot of “&lt;Note 1&gt; Self-defined Application GUID case” in section “6.5.1 Create Application Versions” for kindly reading and</li> </ul>

			understanding.
V1.8	2019.12/19	Judy Tsui	<ul style="list-style-type: none"> <li>Remove 6.5.2 redundant “edit application version” dialogue</li> </ul>
V1.9	2019.12/24	Judy Tsui	<ul style="list-style-type: none"> <li>“Alert” feature is available on web portal v. 2.10.</li> <li>"common component" section is removed due to the removal of approval flow.</li> <li>2.Add SMTP setting in the notification section.</li> </ul>
V1.10	2020/02/26	James Chou	<ul style="list-style-type: none"> <li>Release based on ADM Portal v2.11</li> <li>Update the content of the section “5.2.6 Delete Device”.</li> <li>Update the content of the section “9.1.3 Delete a group”.</li> <li>Update the content of the section “4.2.1 Device Status”.</li> <li>Remove the section “5.2.5 Deactivate Devices”.</li> </ul>
V1.11	2020/03/17	James Chou	<ul style="list-style-type: none"> <li>Release based on ADM Portal v2.12 and Agent v2.13</li> <li>Update the content of the section <ul style="list-style-type: none"> <li>5.2.3 Take Device Screenshot</li> <li>5.2.4 Get Device Logs</li> </ul> </li> <li>Add a new section “5.2.5 Send a command to the device” and the section “Delete Devices” is moved to 5.2.6.</li> <li>Add a new section “7.4 Set the Collect Logs Settings”.</li> <li>Combine the section 6.2 and 6.3 to "6.2 Register Applications"</li> <li>Combine the section 6.3.1 and 6.3.2 to a section “6.3 Application Profile”.</li> <li>Update the content of the section "6.4.1 Create Application Versions"</li> <li>Update the section "6.5.2 Modify the Application Build" to "6.5.2 Status in Version's Activities"</li> <li>Update the content of the section “9.2 Enter Sub-Groups”.</li> </ul>
V1.12	2020/05/13	James Chou	<ul style="list-style-type: none"> <li>Release based on ADM Portal v2.13 and Agent v2.14</li> <li>Update the content of the section “4.3 Reports”</li> <li>Add two new sections “7.5 Set the Software Watchdog Settings” and “7.6 Set the USB Keyboard &amp; Mouse Lock Settings”.</li> <li>Update the content of the section “10.1 Setup SMTP” and add a new section “10.2 Setup LINE”</li> </ul>

# Table of Content

<b>1. Introduction</b>	<b>5</b>
<b>2. Getting started</b>	<b>6</b>
2.1 Prerequisites	6
2.2 Operating Flow	6
<b>3. Sign In</b>	<b>7</b>
<b>4. Dashboard</b>	<b>8</b>
4.1 Enter Dashboard	8
4.2 View Data	11
<b>5. Devices</b>	<b>17</b>
5.1 Enroll new Devices	17
5.2 Device Management	19
5.2.1 Move device	19
5.2.2 Reboot device	20
5.2.3 Take Device Screenshots	20
5.2.4 Get Device Logs	22
5.2.5 Send a command to the device	23
5.2.6 Delete device	23
5.3 Device Profile	24
5.3.1 Change Device Name	24
5.3.2 Change Device Information	24
5.3.3 Change Device Group	24
5.3.4 Modify Device Configuration	25
5.4 View Devices	26
5.4.1 View Device Policy	26
5.4.2 View Device Status	27
5.4.3 View Device Activities Log	27
<b>6. Applications</b>	<b>28</b>
6.1 Enter Applications	28
6.2 Register Applications	29
6.3 Application Profile	32
6.4 Application Versions	33

6.4.1 Create Application Versions.....	33
6.5.2 Status in Version's Activities .....	38
<b>7. Policies .....</b>	<b>39</b>
7.1 Enter Policy Profile.....	39
7.2 Edit Policy Content .....	40
7.2.1 Change Settings.....	40
7.2.2 Modify Policy Extension Command .....	41
7.3 Apply Policy.....	41
7.4 Set the Collect Logs Settings .....	42
7.5 Set the Software Watchdog Settings.....	43
7.6 Set the USB Keyboard & Mouse Lock Settings .....	45
<b>8. Operators .....</b>	<b>47</b>
8.1 Add New Operators.....	47
8.2 Manage roles .....	49
8.2.1 Create new roles.....	49
8.2.2 Edit/Delete Existing Roles.....	51
8.3 Edit Operator Profile.....	51
8.3.1 Change Group.....	52
8.3.2 Change Role.....	52
8.3.3 Delete an operator .....	53
<b>9. Groups.....</b>	<b>54</b>
9.1 Edit groups .....	54
9.1.1 Create a New Group .....	54
9.1.2 Rename a Group.....	55
9.1.3 Delete a Group .....	55
9.2 Enter Sub-Groups.....	56
<b>10. Alerts .....</b>	<b>57</b>
10.1 Setup SMTP .....	57
10.2 Setup LINE .....	59
10.3 Alert Table .....	60
10.4 Enable the Alert Item and Set the Recipient.....	61

## 1. Introduction

Allxon Device Management (ADM) is the turnkey solution for vertical applications deployment. It has a complete device management with a Central Portal. Start from enrollment, ADM supports file or manual enrollment. Over-the-air software can be provisioned or updated by groups. All devices will be well configured through automated process for deploying group policy.

Most importantly, ADM collects real time data from devices at locations around the world and automatically removes sensitive data. Through the dashboard, ADM summarizes the data in charts and map view, you can simply overview the device status from the dashboard. The proactive alerts and audit reports give suggestions on device status for policy compliance and safely delete the device.



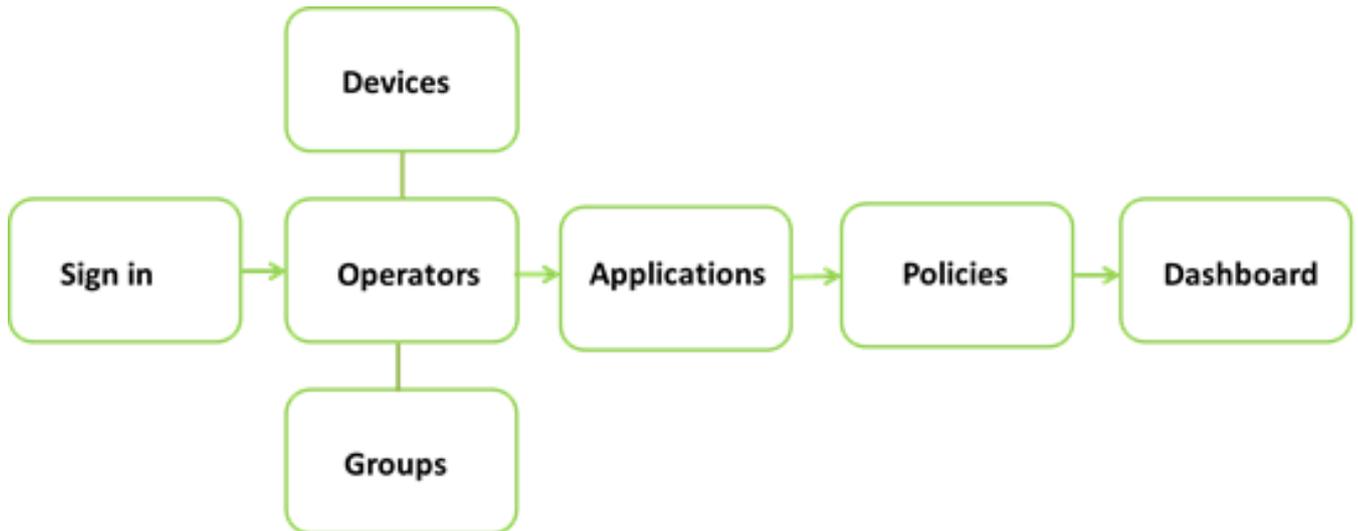
## 2. Getting started

Welcome to the Allxon ADM User Manual. This User Manual primarily describes the steps to configure the Allxon ADM.

### 2.1 Prerequisites

- ✓ User Account registering information (From Allxon Administrator)
- ✓ Make sure your network is accessible in order to connect with ADM portal

### 2.2 Operating Flow



When you sign in to ADM Portal, you may first look into “Devices”, “Operators” and “Groups”. In “Devices”, you may see basic information or activities of devices; In “Operators”, it is mainly used to manage the ADM operators and roles; In “Groups”, there is a hierarchical structure where you can organize the groups.

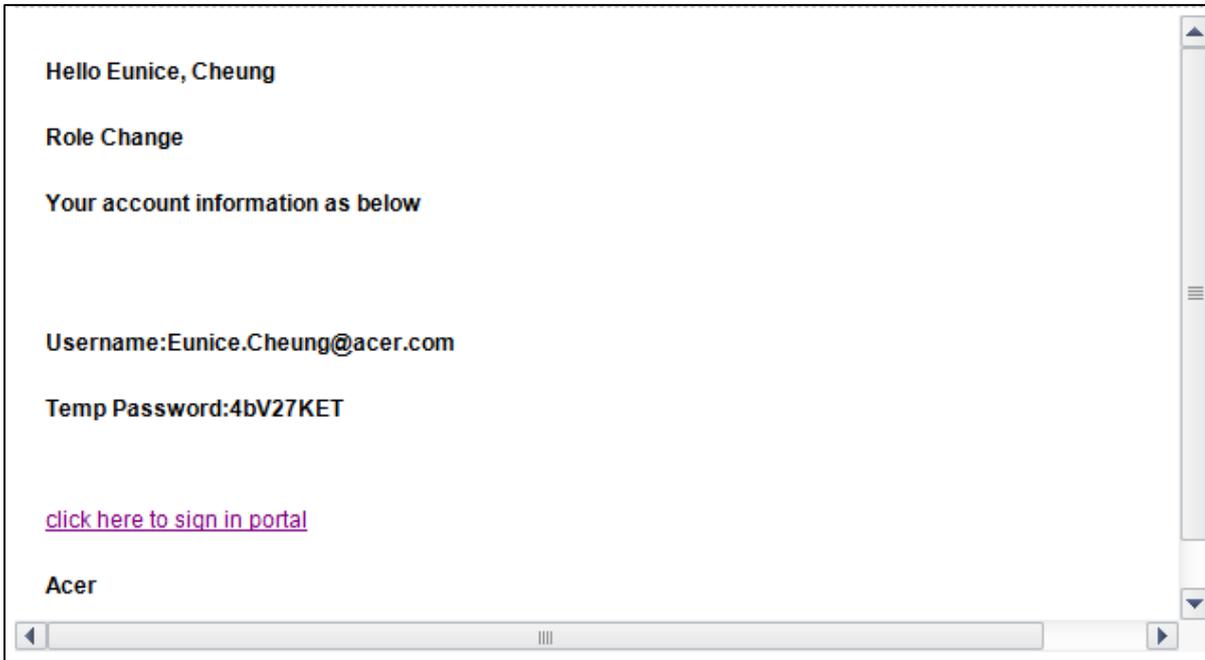
After managing the operators and devices in ADM, You can add more features by having new APPs for “Applications” and manage the APPs. The application can be installed through “Policies” and applied to the devices. In “Policies”, you can also modify the automatic settings of devices.

Through all the settings and modifications, the statistic of devices will be briefly shown on “Dashboard”. Users can utilize reports for further analysis.

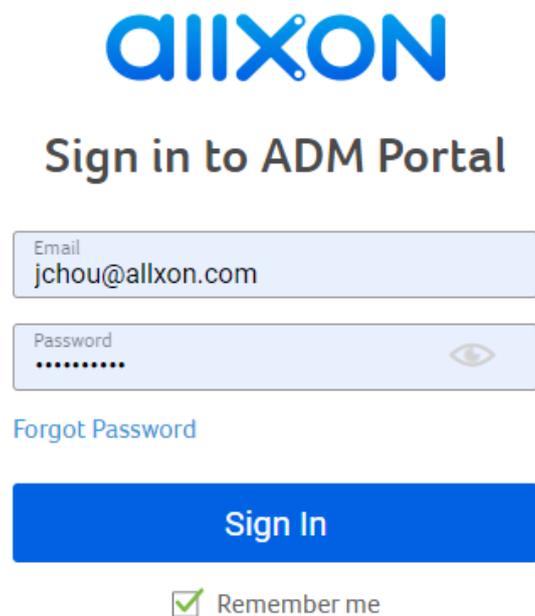
Let’s get started!

### 3. Sign In

Before the first time Sign In, you will receive an **Email Invitation**. Click the link on Email Invitation to launch the web browser and enter Sign In page.



User ID will be prepopulated into the Email input box on Sign In page. You manually enter the **temporary password**. The Create Password Dialog will pop up immediately to ask the new operator to **create a new password**.

The screenshot shows the Allxon sign-in interface. At the top is the Allxon logo. Below it is the heading "Sign in to ADM Portal". There are two input fields: "Email" containing "jchou@allxon.com" and "Password" with masked characters and a visibility icon. A "Forgot Password" link is positioned below the password field. A prominent blue "Sign In" button is centered below the inputs. At the bottom, there is a "Remember me" checkbox which is checked.

## 4. Dashboard

### 4.1 Enter Dashboard

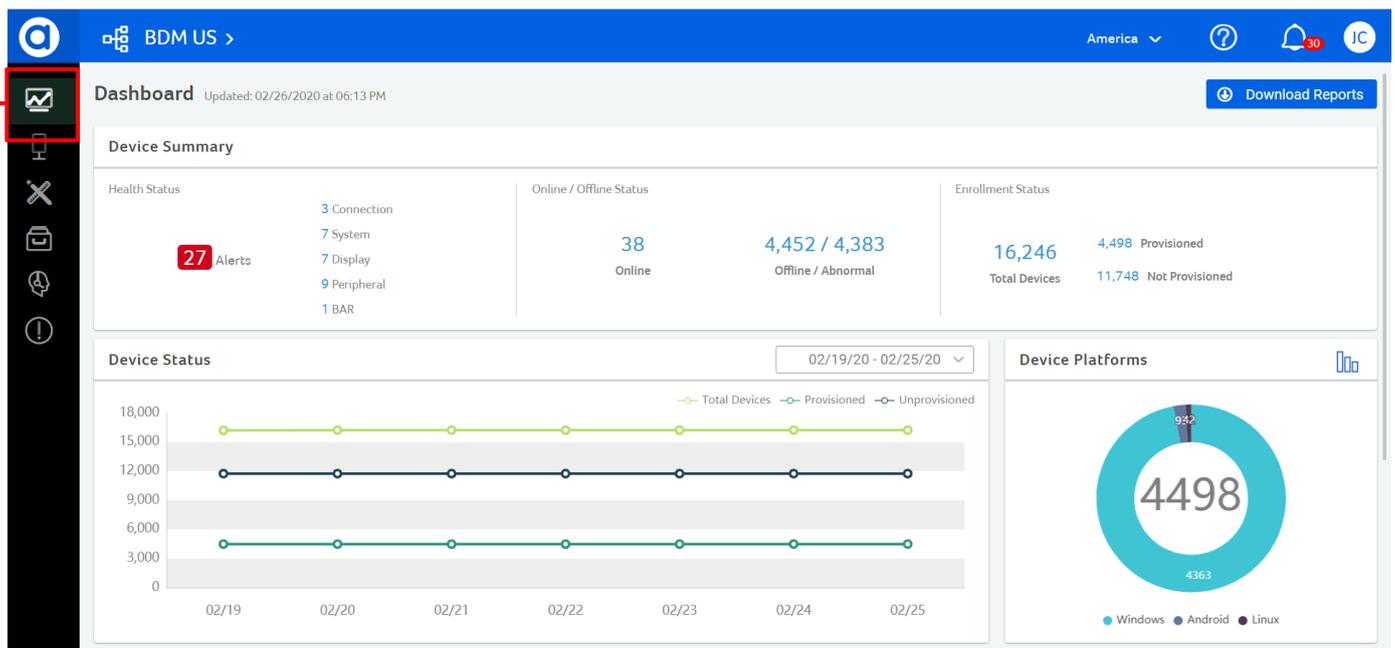
The dashboard is the starting point of ADM. It offers a quick overview status of your devices. You can map view with zoom in/out to check device distribution, check the device platform distribution, device type distribution and curve graph of device status for different time range.

**Health Status:** You can set device alert when CPU Usage, Memory Usage, Storage Usage, System Temperature are abnormal.

**Connectivity Status:** You can check device is Online, Offline or Unknown.

**Enrollment Status:** You can check device is Provisioned or Unprovisioned.

After signing in, you will land on the dashboard under the group(including all sub-groups) that you are assigned . If you want to enter Dashboard from Menu, click “Dashboard” icon on the left menu to enter Dashboard.



Enter Dashboard

If you want to check or edit your **personal profile**, click the logo of your name and choose profile. You can see/edit your basic information and password. For example, you can see/edit the **country, time zone** and **language** of the account.

The screenshot shows the BDM US dashboard. At the top right, there is a user profile dropdown menu for James Chou (JC) with options for Profile and Sign Out. The dashboard includes a 'Device Summary' section with health status (27 Alerts), online/offline status (38 Online, 4,452 / 4,383 Offline / Abnormal), and enrollment status (16,246 Total Devices, 4,498 Provisioned, 11,748 Not Provisioned). Below this is a 'Device Status' line chart and a 'Device Platforms' donut chart showing 4,498 total devices, with 932 Windows, 4,363 Android, and 0 Linux devices.

The screenshot shows the user profile page for James Chou. The 'Basic Information' section includes:

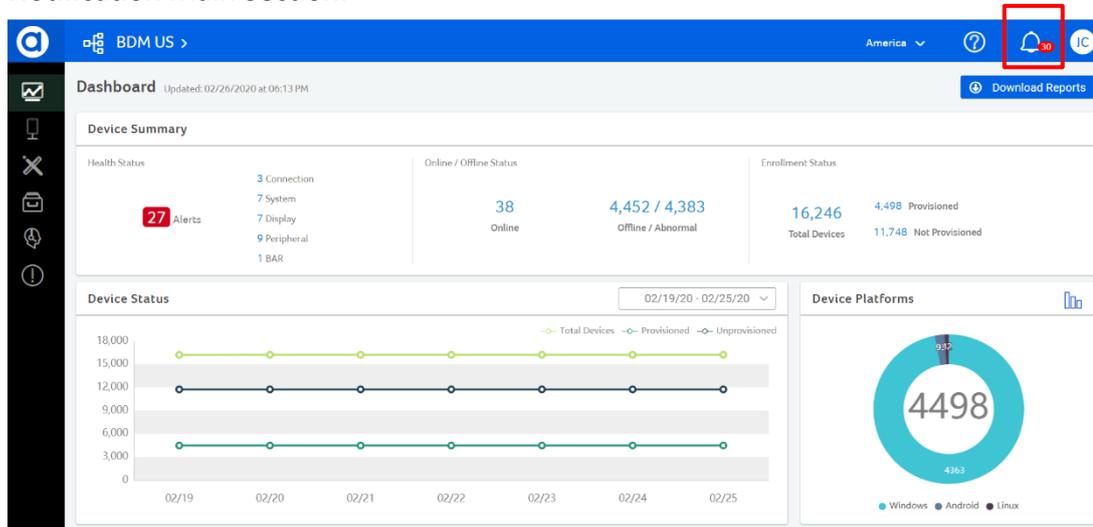
- Account: User ID: jchou@allxon.com, Joined Time: 10/04/2019 at 03:49 PM, Language: English
- Security: Password: \*\*\*\*\*
- Access: Group: BDM US, Role: Super admin

The 'Responsibilities' list includes: super.admin, Add Roles, Delete Roles, Update Roles, operator.create, Delete Operators, Manage Operators, View Operator Information, View Notifications, Enroll Devices, Delete Devices, Manage Devices, and Edit Device Information. A red box highlights the 'Super admin' role, with an arrow pointing to the text 'Admin of the group'.

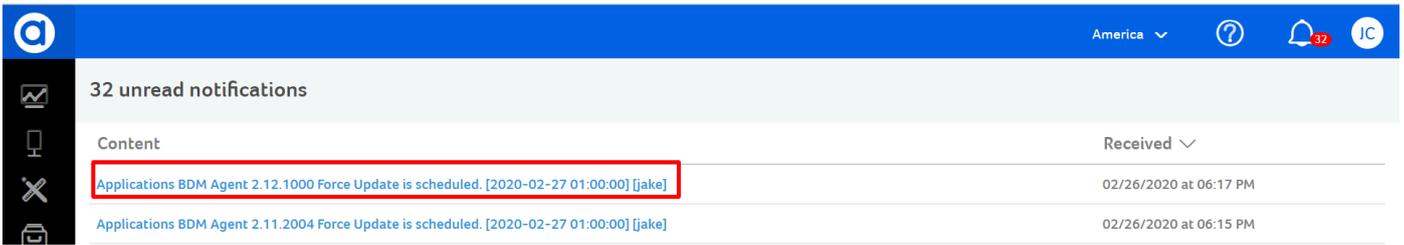
Allxon should have assigned the role for you before you enter ADM. Allxon has created several roles in ADM such as **Super Admin, Admin, Operators and Guest**. Below are the suggestions for users. You can add/delete actions for each role. Please refer to 8.2.2.

Main Category	Sub Category	Actions
Account Management	Role	Create/Delete Roles
		Update Roles
	User	Create/Delete Operators
		Manage Operators
		View Operator Info
	Group	Create/Delete Groups
Edit Group		
View Groups		
Device Management	Device	Input/Delete Devices SN
		Manage Devices
		Edit Device Info
		View Device Info
Policy Management	Policy	Update Policy
		Approve Policy
		View Policy
App Management	App	Register/Remove Apps
		Update App Versions
		Approve App Versions
		View App Info
Dashboard Management	Reports	View Reports
		Download Reports
		Subscribe Reports

When receiving new notifications, the **notification badge** will appear at the notification icon. The number of the new notifications will be displayed inside the notifications badge. Click the badge to enter the Notification Main Section.



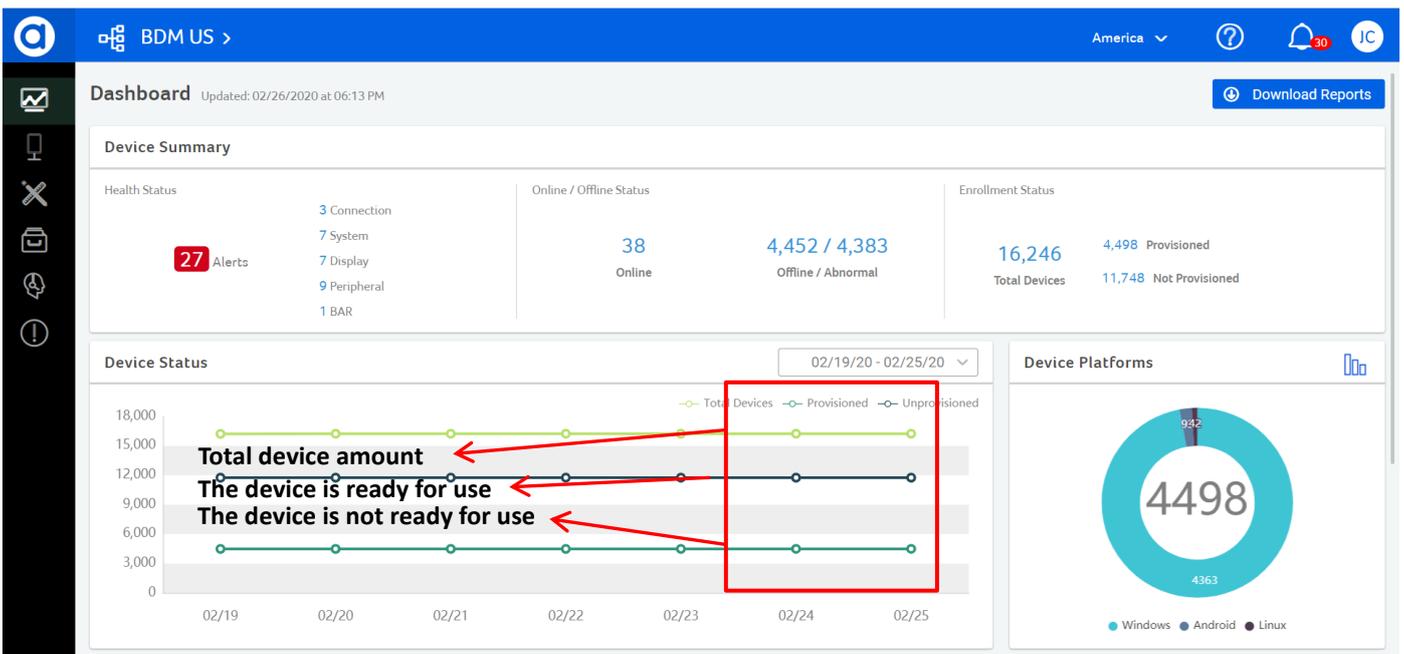
After entering the Notifications Main Section, the notifications badge will disappear. In the notifications list, unread notifications will be highlighted. Click each notification link to go to related section or profile page.



## 4.2 View Data

### 4.2.1 Device Status

If you want to view data with different presentations and data details, mouse over a data point on the **status line** to show the detail information. It shows three status of the device. **“Provisioned”** means the device is ready for use. **“Unprovisioned”** means the device is not ready for use.



## 4.2.2 Zoom In/Out Map

Mouse over a country/city on the map to show the detail information of device in different countries/cities. The map zoom level range is wide. Based on region data, the map will position the current region in the middle on the map. The **device number** within the cluster size range will be presented in the cluster.

Click the “+” button or the cluster to zoom in the map.

Click the “-” button to zoom out the map.

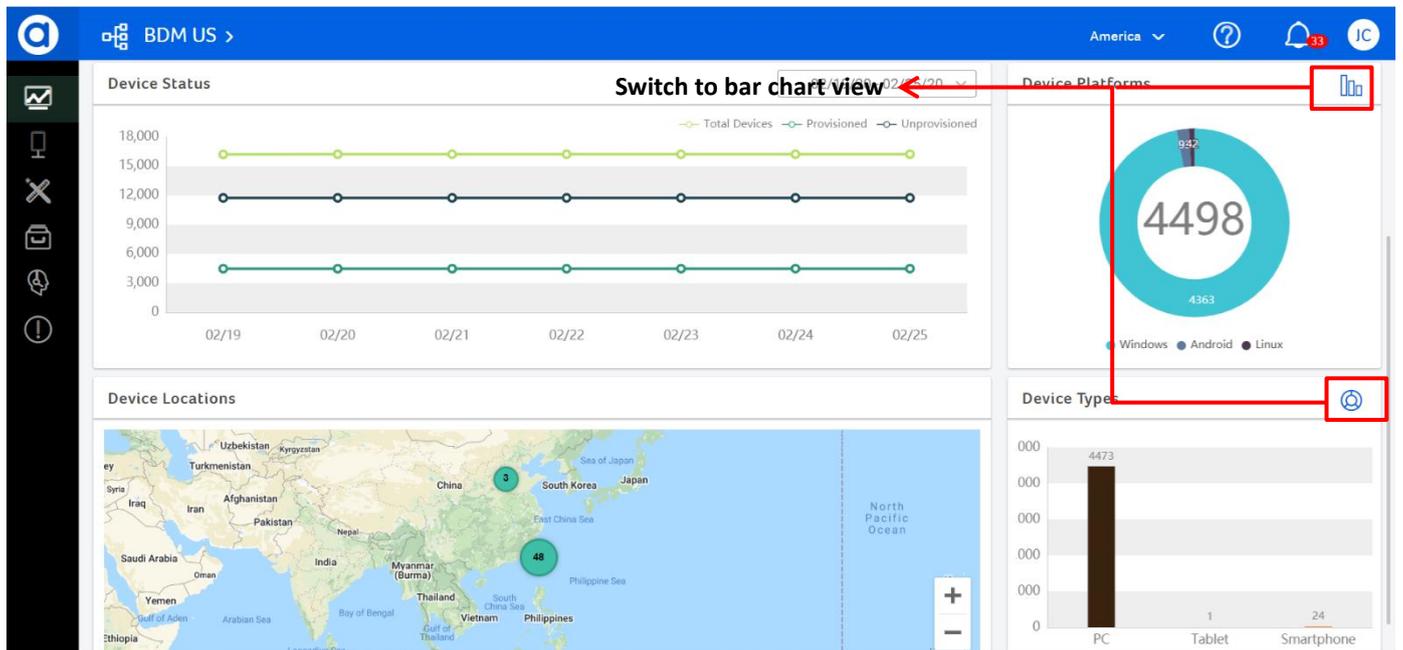
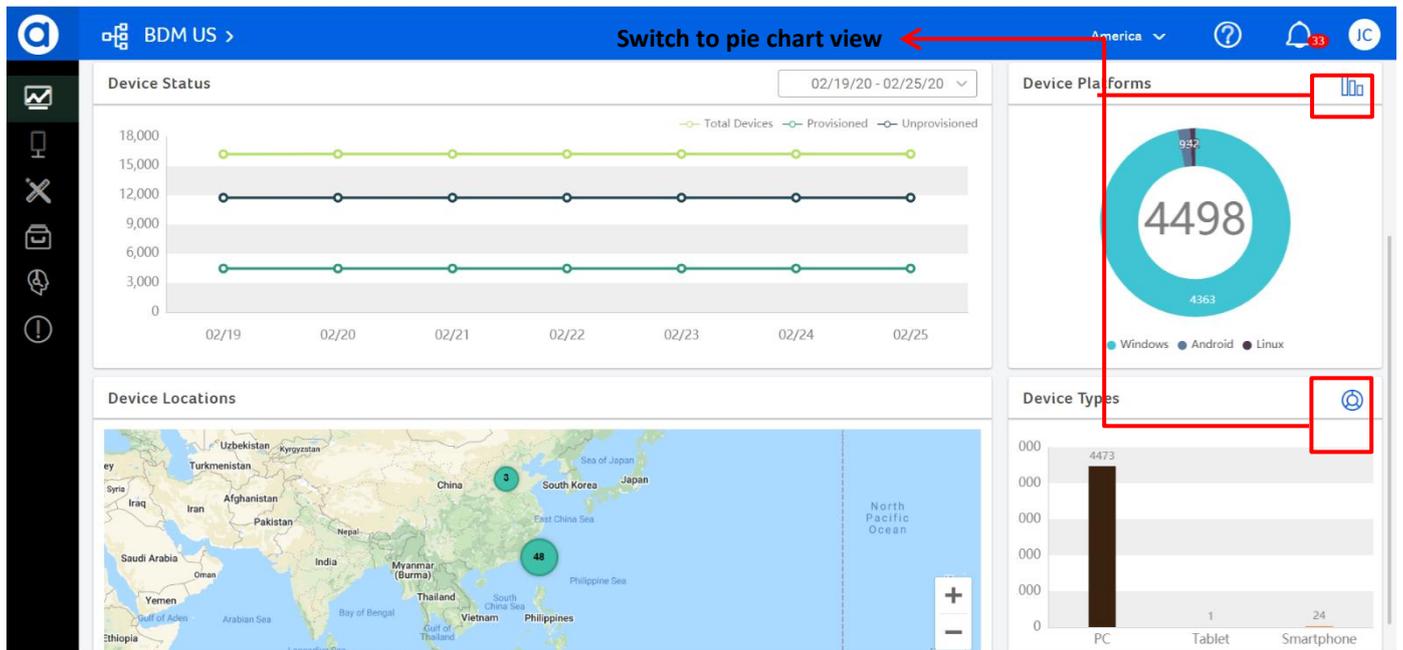
Click the “**Device Name**” on the cluster to enter the Device Profile page.



### 4.2.3 Switch View

“**Device Platforms**” show you the numbers and the systems your devices belong to. “**Device types**” show you the numbers and the type your devices belong to.

If you want to see data in different presentations, Platform and Type charts are able to switch views. You can click the “**Pie**” icon to switch the pie bar chart view to pie chart view or click the “**Bar**” icon to switch the pie chart view to bar chart view.



#### 4.2.4 Change Time Range – Custom Time Range

You can see data in different time range. Click the time range button to reveal the time range selection menu. It offers you the options of “Last 7 days”, “Last 30 days”, “This month”, “Last month” and “Custom Range”. If you want a specific time range, click “Custom Range” to reveal the date picker. Then click the desired date on the calendar to set the **start date** and **end date**. After the selection, click the “Apply” button to display the data within that time range.

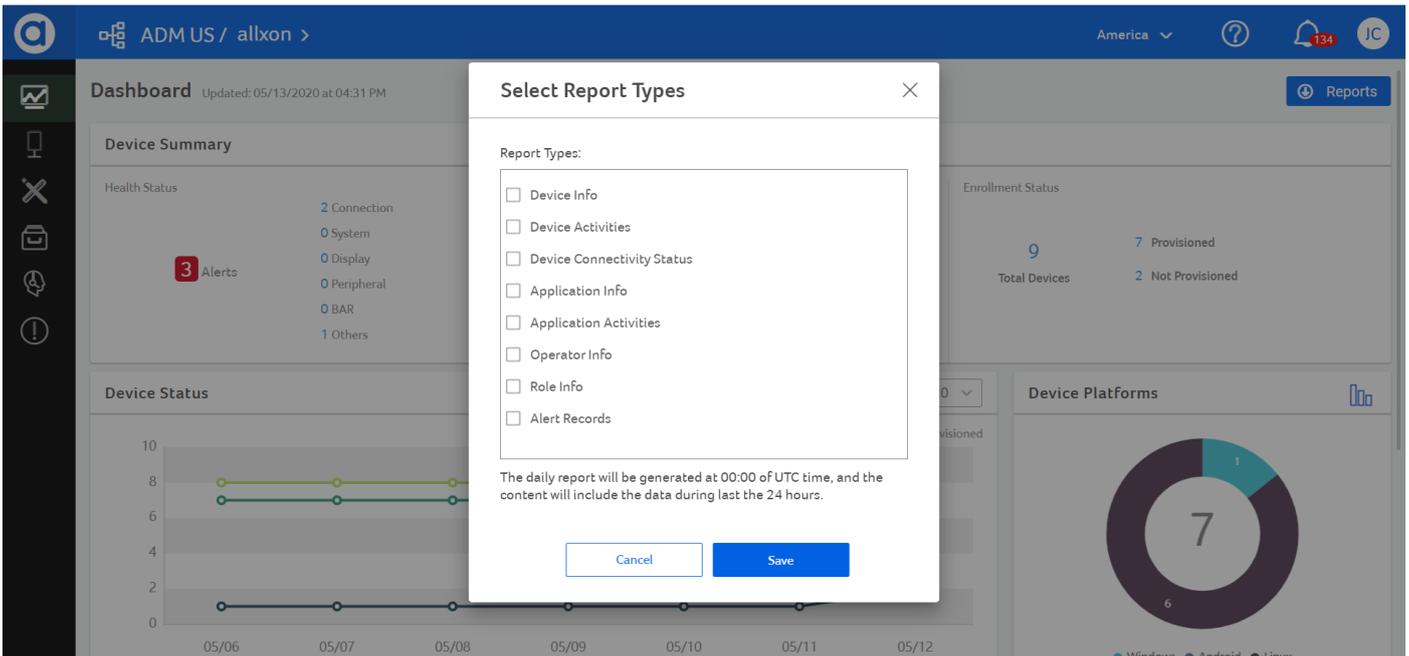
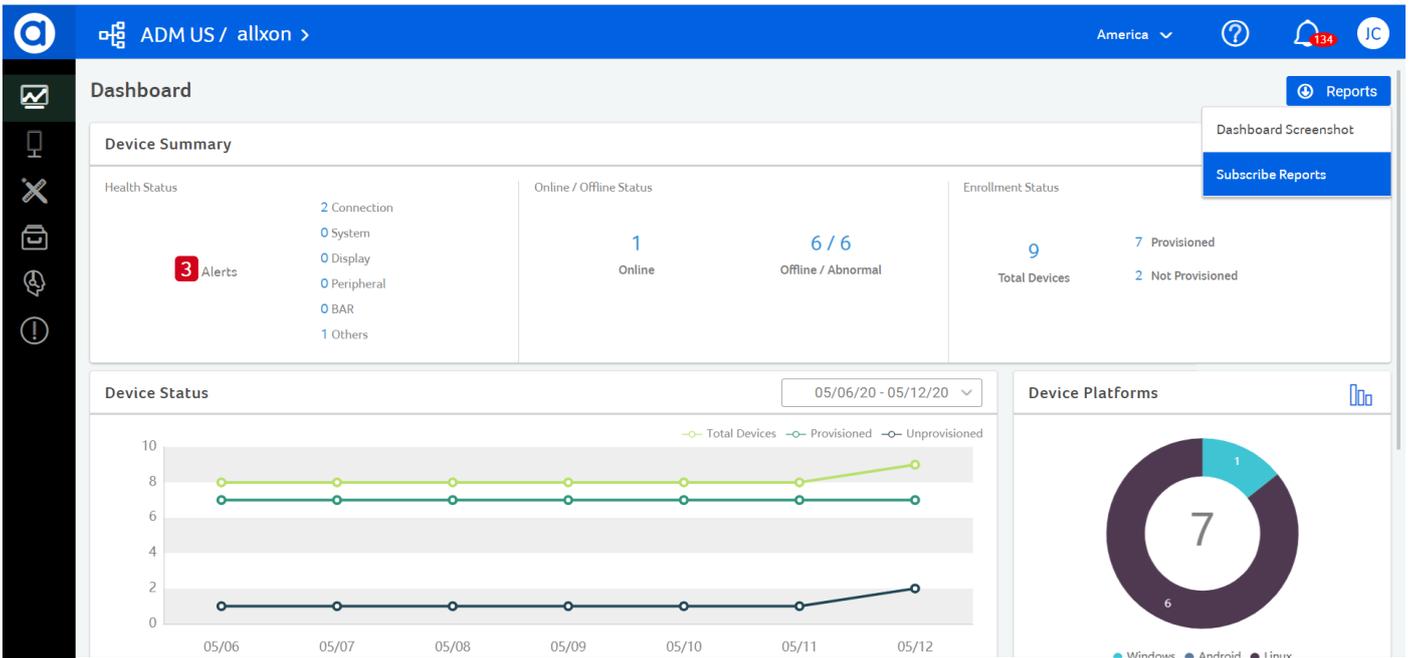
The screenshot displays a dashboard for 'BDM US' with a navigation sidebar on the left. The main content area is divided into several sections:

- Health Status:** 27 Alerts (3 Connection, 7 System, 7 Display, 9 Peripheral, 1 BAR).
- Online / Offline Status:** 38 Online, 4,452 / 4,383 Offline / Abnormal.
- Enrollment Status:** 16,245 Total Devices (4,498 Provisioned, 11,747 Not Provisioned).
- Device Status:** A line chart showing device counts from 02/19 to 02/23. A red box highlights the 'Time range selection' dropdown menu, which includes options for 'Last 7 Days', 'Last 30 Days', 'This Month', 'Last Month', and 'Custom Range'. The 'Custom Range' option is selected, revealing a date picker with a calendar for February 2020. The start date is 02/19/20 and the end date is 02/25/20. An 'Apply' button is visible.
- Device Platforms:** A donut chart showing 4,498 total devices, with 942 Windows, 4,363 Android, and 436 Linux.
- Device Locations:** A map showing device locations in China, South Korea, and Japan.

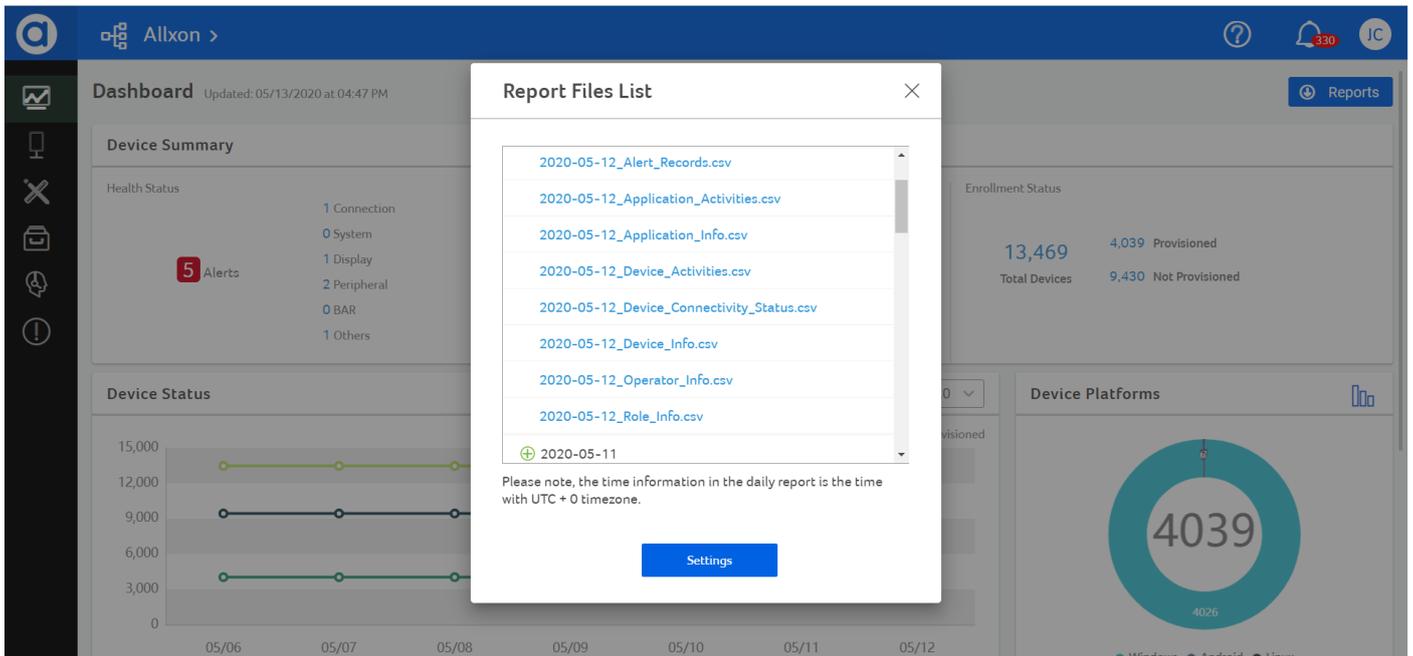
### 4.3 Reports

In order to provide the user more useful device data, we allow the user to subscribe the daily report from the portal, and the report types as below:

1. Device Info
2. Device Activities
3. Device Connectivity Status
4. Application Info
5. Application Activities
6. Operator Info
7. Role Info
8. Alert Records



The daily report is saved as a CSV file and keep on the Portal about 30 days. The user who has the action “Subscribe Reports” can adjust the Subscribe Reports Settings and download the daily report. Please note, the daily report will be generated at 00:00 of UTC time, and the content will include the data during last the 24 hours. For example, I will be able to get the new daily report at 8:00 AM when I live in Taiwan.



## 5. Devices

“**Devices**” is a control center of all devices. It includes Device enrollment, Device information, Device management. You can find all information related to device in “**Devices**” and the reports give suggestions on device status for policy compliance and safely delete the devices. It also thoroughly records the device activities to monitor the operating process.

**Enter Devices Main Section**

**First capital letter of device name**

Name	Status	Serial Number	Platform	Enrollment	Group
1		1	Windows	Unprovisioned	BDM US
2	Abnormal	2	Windows	Provisioned	ABS/..
3		KSA12345680	Windows	Unprovisioned	ABS/..
3	Abnormal	3	Windows	Provisioned	ABS/..
4		KSA12345681	Windows	Unprovisioned	ABS/..
4	Abnormal	4	Windows	Provisioned	ABS/..
5		KSA12345682	Windows	Unprovisioned	ABS/..
5	Abnormal	5	Windows	Provisioned	BDM US
6		KSA12345683	Windows	Unprovisioned	ABS/..
6	Abnormal	6	Windows	Provisioned	ABS/..
7		KSA12345684	Windows	Unprovisioned	ABS/..
7	Abnormal	7	Windows	Provisioned	ABS/..

### 5.1 Enroll new Devices

If you want to enroll new devices, click “**Devices**” icon on the left menu to enter Devices Main Section page. Click “**Enroll**” button on the right top. Click “**Select a File**” button to evoke the system file picker. You can select a CSV file (The device enroll template is below) or click on “**key in**” to enter the information.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	SerialNumber	ProductModel	DeviceType	DeviceName	StoreAddress	City	State	CountryCode	Zipcode	Longitude	Latitude	ChannelName	StoreId	StoreName	StorePhone	PicturemachinePlayerId	
2	NC91006430CiQube	PC	Financial Plaz	130 Merchan	Hon	Hawa	US	96813	-157.862	21.3084	Jamba Juice	352	Financial P	808-628-666	100123		

Only **Serial Number** is required information, others are optional.

**Country Code:** Refer to **ISO 3166 Codes** (Ex: Australia’ Country Code would be “AU”)

**Store Phone:** Additional Characters will not be accepted.

**Device Type:** Only accept “**PC/P/Smartphone/S/Tablet/T**”, other Device Types will be defaulted as “**PC**”.

**Store Address:** Should be separately key in to the column of “**Address, City, State, Country, and Zip**”.

*\*Zip Code, Longitude and Latitude: Only accept Digits.*

*\*Serial Number: Only accept uppercase letter, lowercase letter and digits.*

The device enroll template:

**A. Product Model:** The product model should be on your machine.

**B. Serial Number:** If you are using a laptop computer, you can easily find the service tag on your machine.

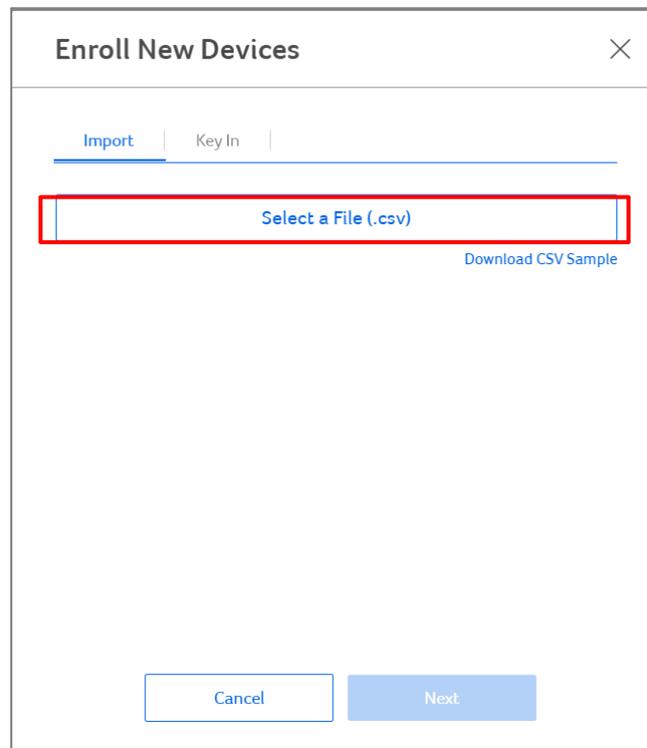
Alternative: Search "Command" in your machine and input the following command:

**"wmic bios get SerialNumber"**

\*The picture below is an example. All machines are applicable.

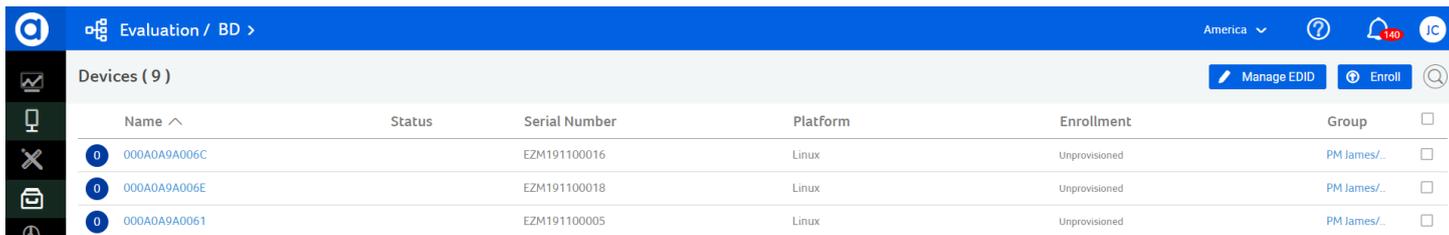


Click and select the desired group. The new enrolled devices will appear on the devices list with highlight for 5 seconds.



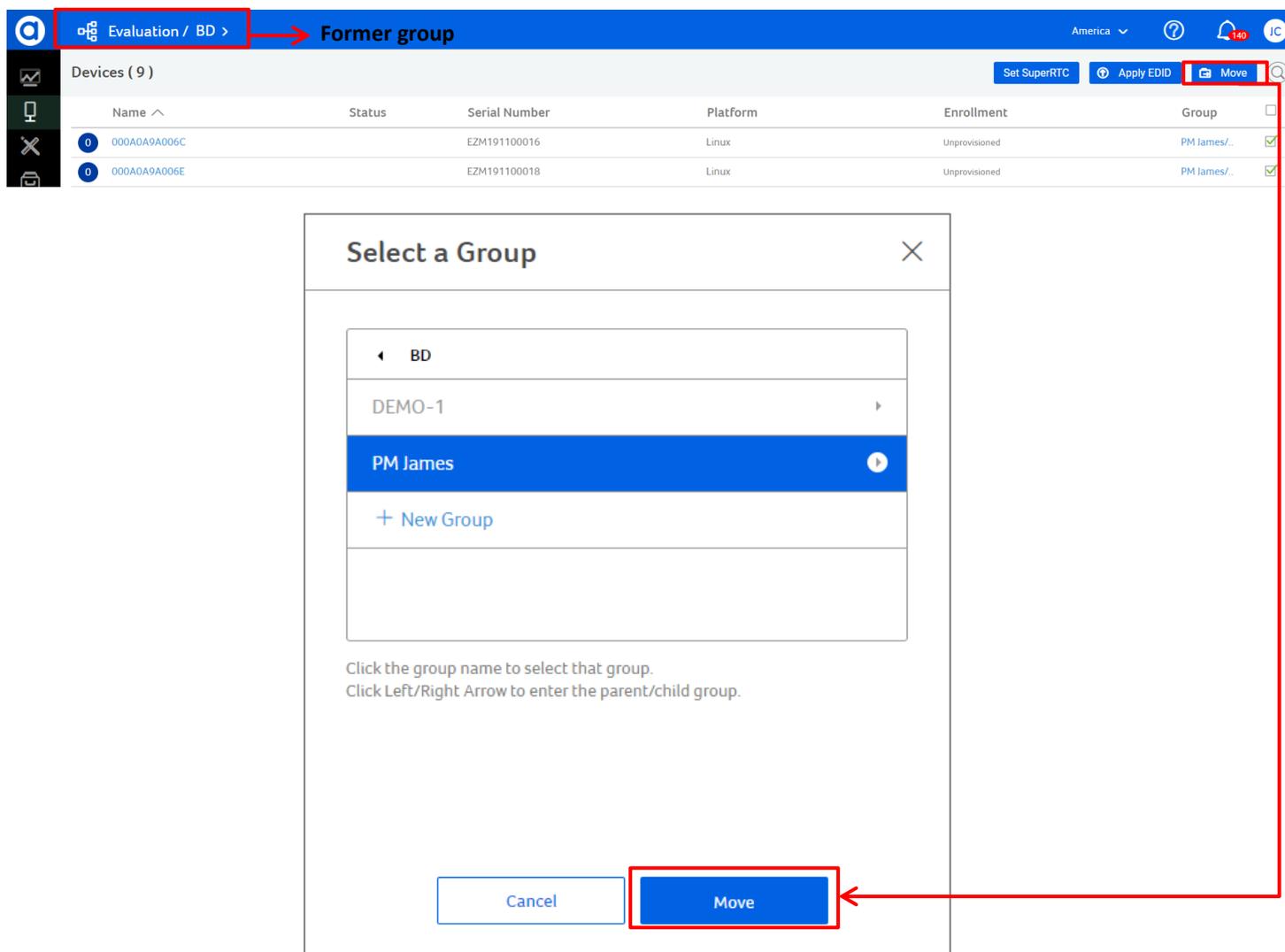
## 5.2 Device Management

### 5.2.1 Move device



Name ^	Status	Serial Number	Platform	Enrollment	Group	
000A0A9A006C	Unprovisioned	EZM191100016	Linux	Unprovisioned	PM James/..	<input type="checkbox"/>
000A0A9A006E	Unprovisioned	EZM191100018	Linux	Unprovisioned	PM James/..	<input type="checkbox"/>
000A0A9A0061	Unprovisioned	EZM191100005	Linux	Unprovisioned	PM James/..	<input type="checkbox"/>

You may need to move devices to other teams or different Administrators. Click the **check boxes** to select all the devices that need to be moved. After selections, click the **“Move”** button and then click the desired group to make the selection. Click **“Move”** button to confirm the action. After the move, the action feedback toaster will appear on the page for 5 seconds.



The screenshot shows the 'Devices (9)' page with a 'Move' button highlighted in red. A dialog box titled 'Select a Group' is open, showing a list of groups. The 'PM James' group is selected. The 'Move' button in the dialog is also highlighted in red.

Former group

Name ^	Status	Serial Number	Platform	Enrollment	Group	
000A0A9A006C	Unprovisioned	EZM191100016	Linux	Unprovisioned	PM James/..	<input checked="" type="checkbox"/>
000A0A9A006E	Unprovisioned	EZM191100018	Linux	Unprovisioned	PM James/..	<input checked="" type="checkbox"/>

### Select a Group

- BD
  - DEMO-1
  - PM James**
  - + New Group

Click the group name to select that group.  
Click Left/Right Arrow to enter the parent/child group.

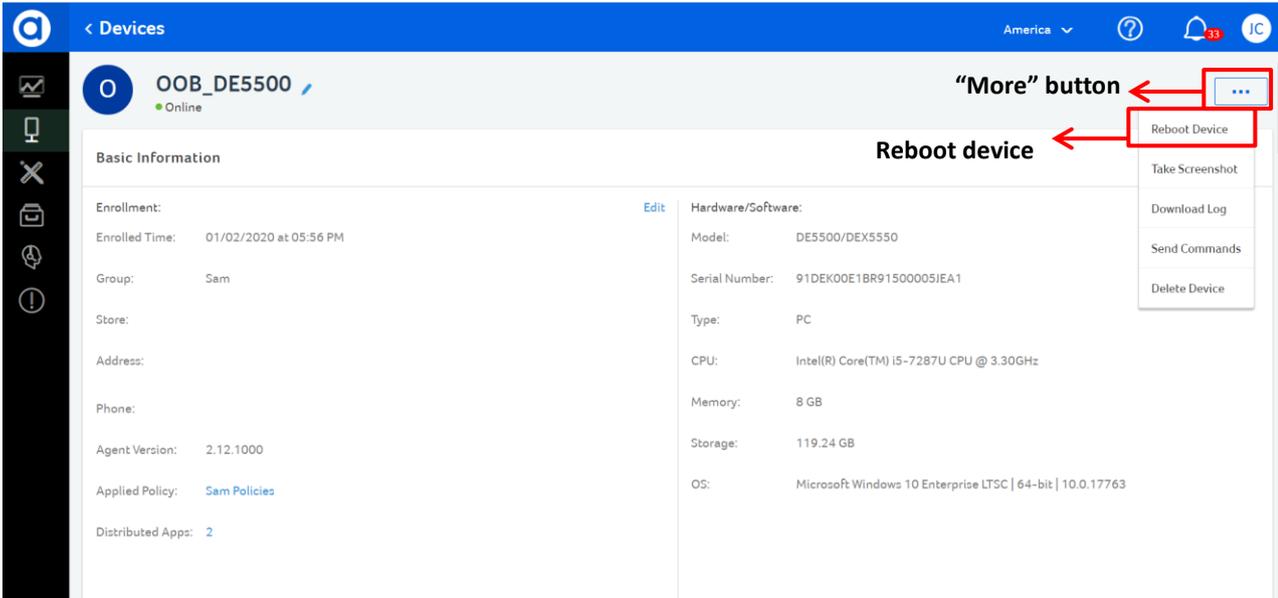
Cancel Move

## 5.2.2 Reboot device

There are two ways to reboot the device.

### 1. Remotely reboot

Click the desired **device's name** to enter the profile page. Click **"More"** button to reveal the contextual menu. Click **"Reboot Device"** button to send the reboot command to the device. The **"Rebooted"** activity will be added into the Activities log.



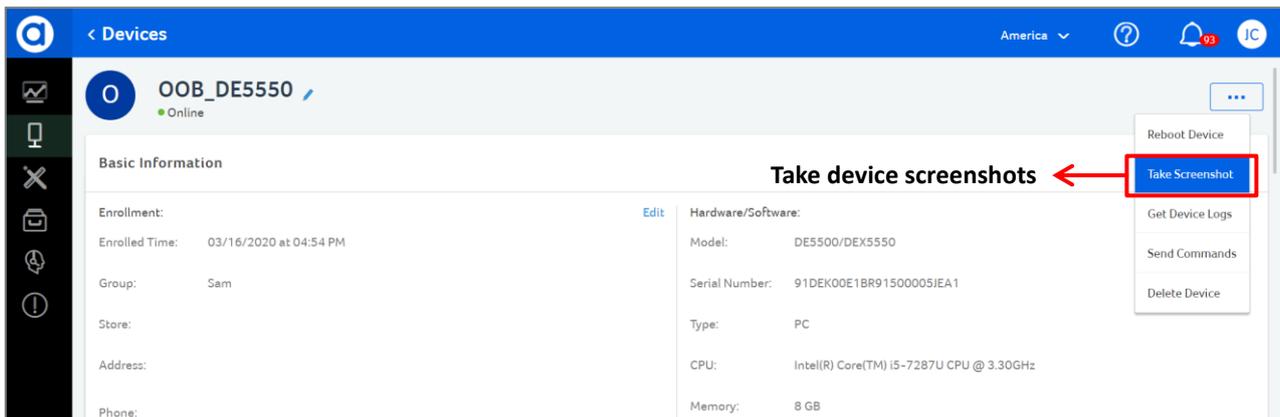
### 2. Automatically reboot

You can set the reboot device time in **"Policy"**. The device will automatically reboot.

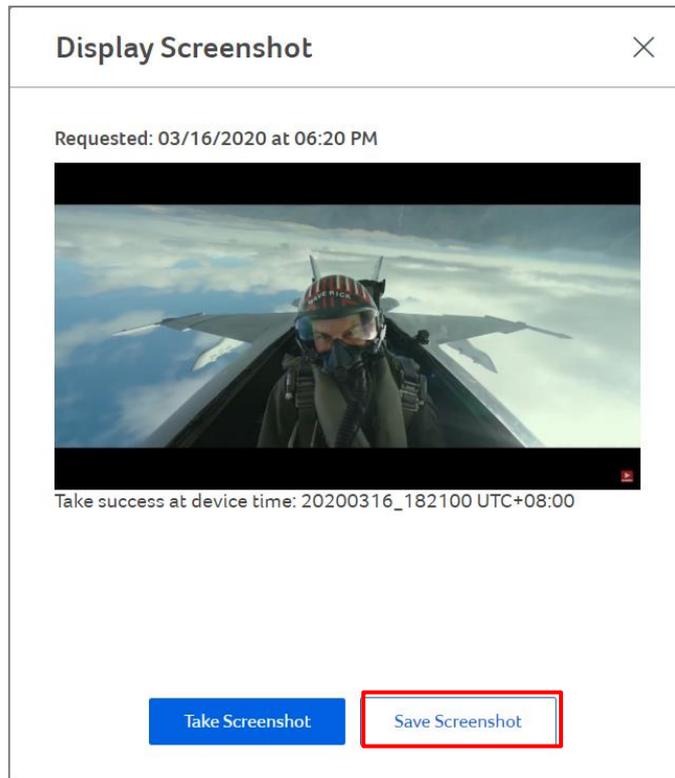
*\* Regularly reboot the device every day can reduce the wear of device.*

## 5.2.3 Take Device Screenshots

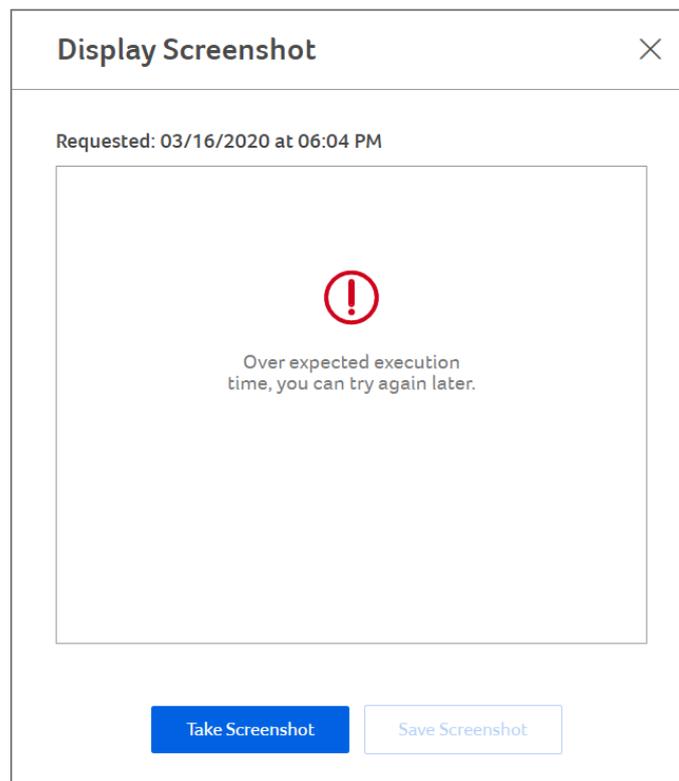
If you want to monitor the display remotely, you can take the real time screenshots of the device to see if the display is working well. Enter that device's profile page and select **"Take Screenshot"** from the list of **"More"** button. Click **"Take Screenshot"** item and it will invoke a window to display the previous success screenshot, and then you can click **"Take Screenshot"** button to trigger the device to take the screenshot and return the file.



When the screenshot is successfully displayed, the **“Save Screenshot”** button will be enabled.



If failed, the failure message will appear, and you can try again later.

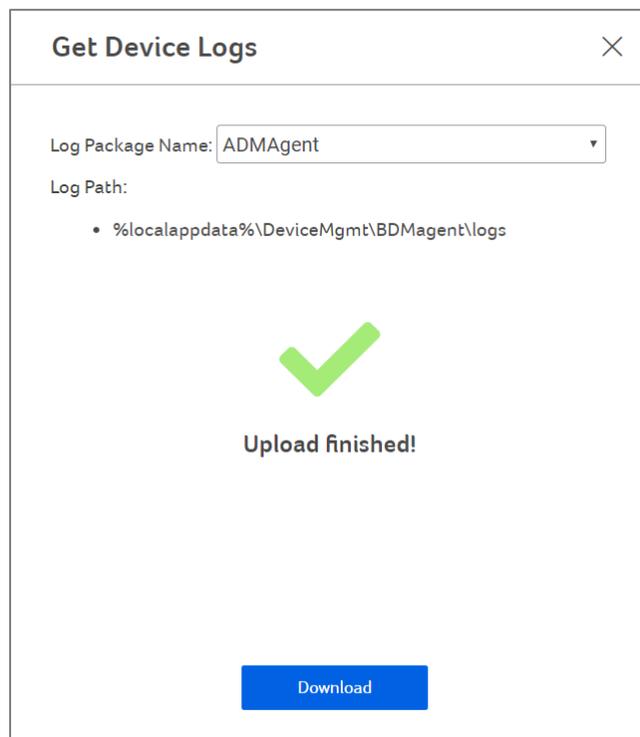
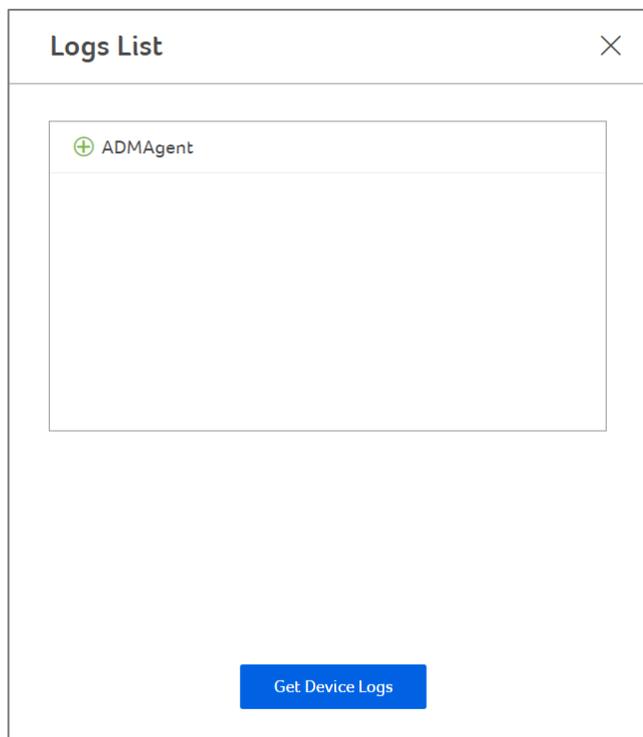
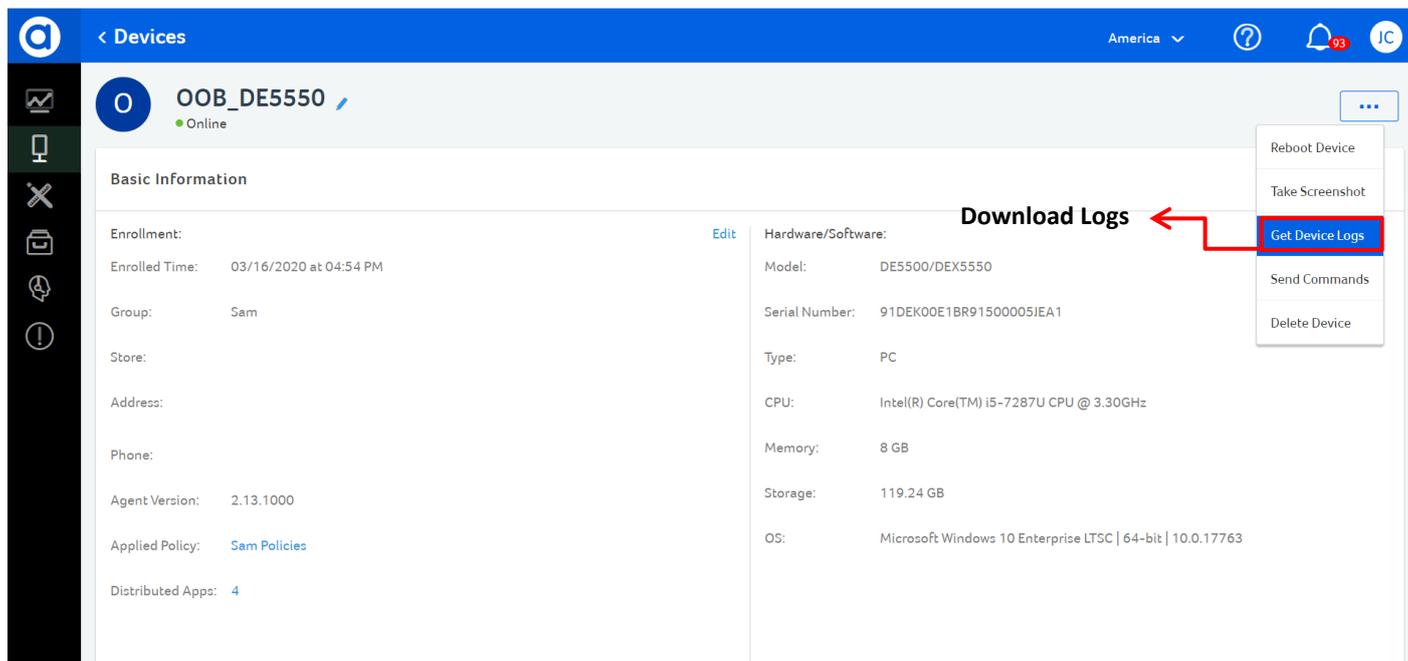


### 5.2.4 Get Device Logs

If you want to get the device's logs. Enter that device's profile page and select **"Get Device Logs"** from the list of **"More"** button. Click **"Get Device Logs"** item and it will invoke a window to display a list which shows the device logs of the last 90 days. You can click the log's link to download the log file from the list.

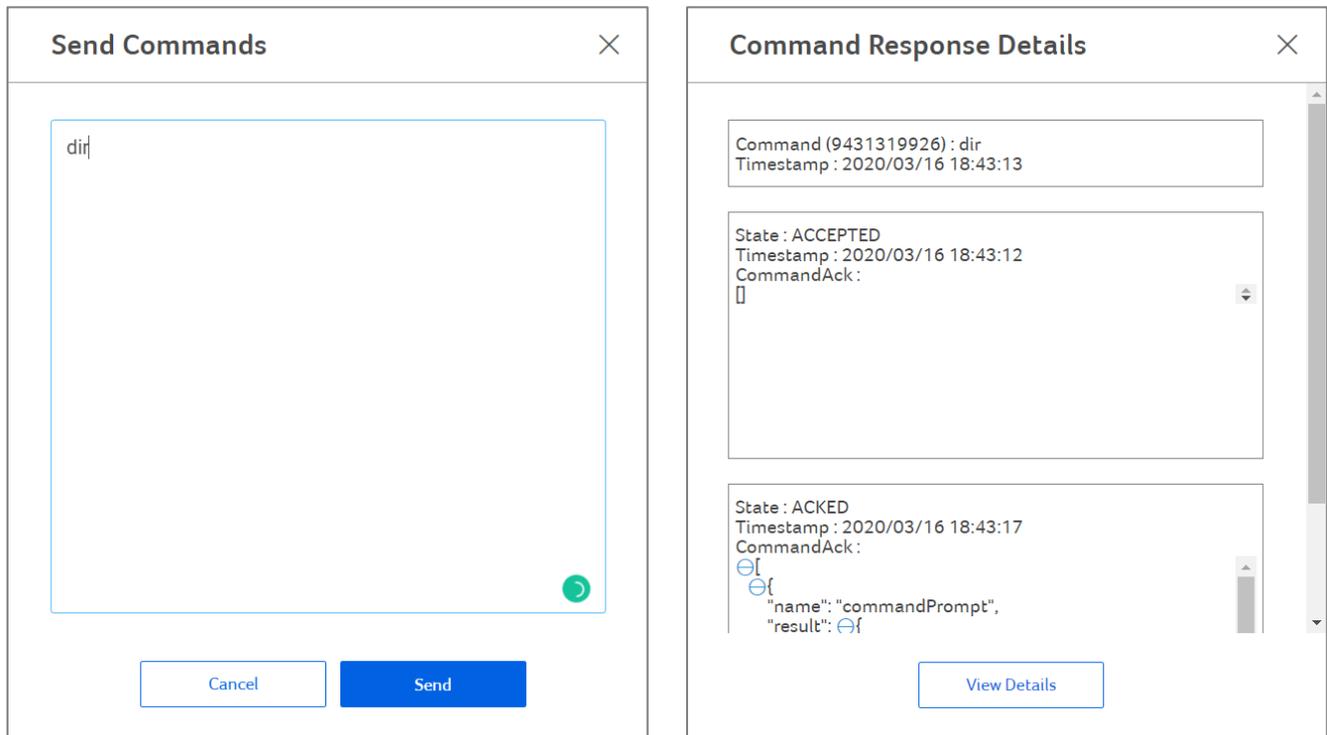
Besides, if you want to get the certain logs immediately, you can click the button **"Get Device Logs"** and select the logs you want, then it will trigger the Agent to collect the logs immediately.

\* You can assign the path of log through **"Collect Logs Settings"** in **"Policy"**(7.4).



### 5.2.5 Send a command to the device

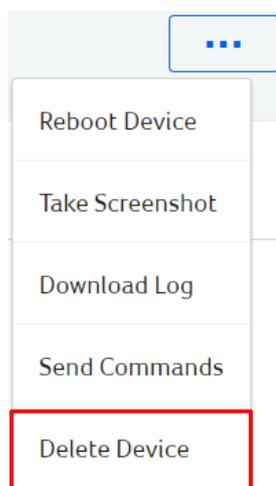
If you want to send a command to the device. Enter that device's profile page and select **"Send Commands"** from the list of **"More"** button. Click **"Send Commands"** item and it will invoke a window to allow the user to type in a command per each request. After sending the command, the **"Command Response Details"** dialog will display the progress of the command's execution, and you can click the button **"View Details"** to download the execution result.



### 5.2.6 Delete device

If you want to delete a device, you can delete the device from device profile page directly. Click the **"..."** button on the device profile page and choose **"Delete Device"**, then it will trigger the delete device process. If you want to use this device again on ADM Portal, please enroll the device again.

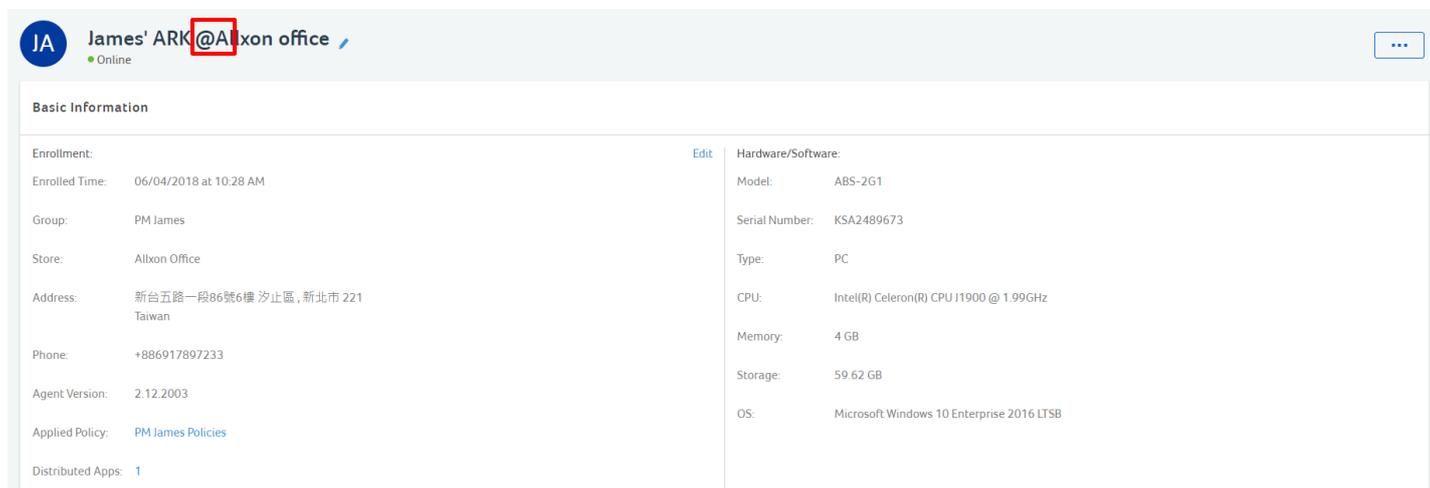
*\*Authority is needed for deleting devices.*



## 5.3 Device Profile

### 5.3.1 Change Device Name

If you want to change device's name, click on **device's name** to enter that device's profile page. Click **"Edit"** icon for the device name to enter device name edit mode. Enter the new device name to the input box and click **"Save"** button to save the change.



JA James' ARK@Allxon office Online

#### Basic Information

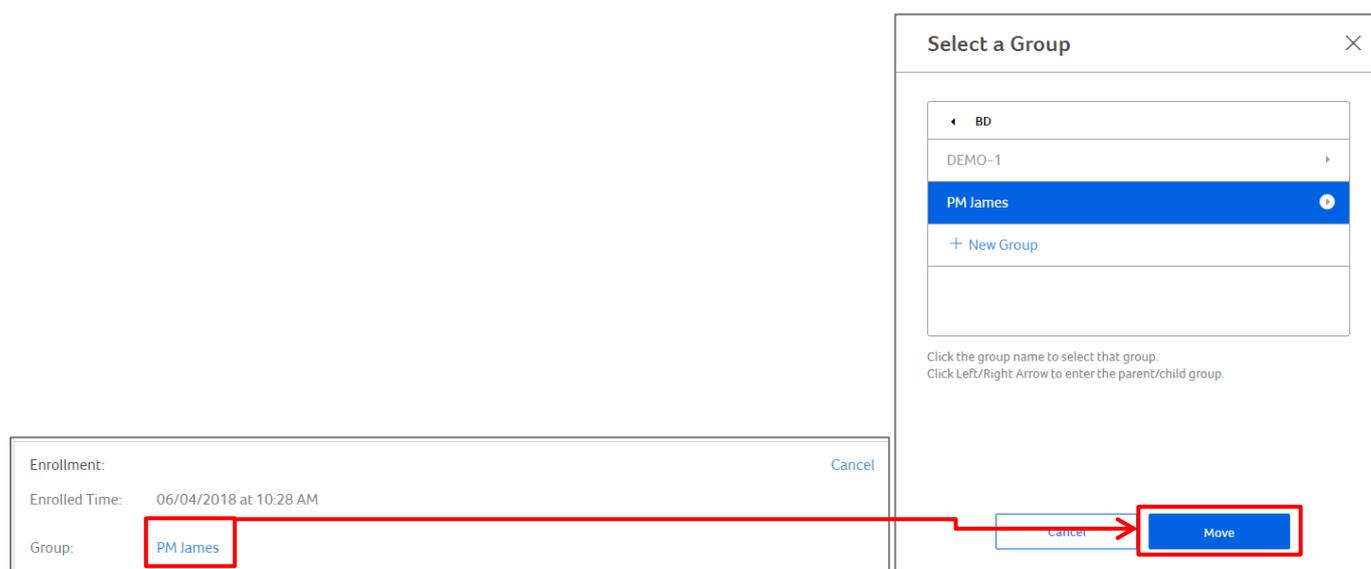
Enrollment:	<a href="#">Edit</a>	Hardware/Software:
Enrolled Time: 06/04/2018 at 10:28 AM		Model: ABS-2G1
Group: PM James		Serial Number: KSA2489673
Store: Allxon Office		Type: PC
Address: 新台五路一段86號6樓 汐止區, 新北市 221 Taiwan		CPU: Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
Phone: +886917897233		Memory: 4 GB
Agent Version: 2.12.2003		Storage: 59.62 GB
Applied Policy: <a href="#">PM James Policies</a>		OS: Microsoft Windows 10 Enterprise 2016 LTSB
Distributed Apps: 1		

### 5.3.2 Change Device Information

If you want to change device's information, click **"Edit"** button to enter information edit mode. The editable items (location, time zone) will become available, and the applied policy link will be disabled. After making the change, click **"Save"** button.

### 5.3.3 Change Device Group

If you want to change device's group, click **"Edit"** button to enter information edit mode. Click group name to evoke group selection dialog. Click desired group to make the selection. Click **"Move"** button to confirm the action and click **"Save"** to make the changes



Enrollment: [Cancel](#)

Enrolled Time: 06/04/2018 at 10:28 AM

Group: [PM James](#)

#### Select a Group

BD

- DEMO-1
- PM James**
- + New Group

Click the group name to select that group.  
Click Left/Right Arrow to enter the parent/child group.

[Cancel](#) [Move](#)

### 5.3.4 Modify Device Configuration

“Configuration” in Device Section is a function for you to add/return additional information for only one device. If you want to modify device configuration, click “**Edit**” button for Device Configuration to enter device configuration edit mode. Enter the new device in the box to make changes. Click “**Save**” button to save and apply changes to the device, the “**Updated Configuration**” activity will be added into the Activities log. If failed, an error message will appear.

#### Configuration

[Edit](#)

---

Click “Edit” button to configure the device by entering commands and scripts in JSON format.

*\*If you want to apply the configuration to all devices in one group, input commands in “Extension” in Policy Content. Please read 7.2.2 for details.*

## 5.4 View Devices

### 5.4.1 View Device Policy

If you want to view device policy, click the policy link to evoke Policy Details dialog. The dialog will display the device policy.

The image shows a user interface for viewing device information. The main section is titled "Basic Information" and lists several fields: Enrollment, Enrolled Time, Group, Store, Address, Phone, Agent Version, and Applied Policy. The "Applied Policy" field is highlighted with a red box and contains the text "PM James Policies". A red line connects this box to a "Policy Details" dialog box that is open in the foreground. The dialog box has a close button (X) in the top right corner. Inside the dialog, it displays the following information: "Effected :01/13/2020 at 10:44 PM", "Time Zone: Taipei Standard Time", "Reboot Device: None", and "Apply Policy to: Current Group Only". Below this, there is a section titled "Turn On Monitor" with a table of days and times. At the bottom of the dialog, there are two buttons: "Check Conditions" and "Done".

**Basic Information**

Enrollment: [Edit](#)

Enrolled Time: 06/04/2018 at 10:28 AM

Group: PM James

Store: Allxon Office

Address: 新台五路一段86號6樓 汐止區, 新北市 221  
Taiwan

Phone: +886917897233

Agent Version: 2.12.2003

Applied Policy: [PM James Policies](#)

**Policy Details** [X]

Effected :01/13/2020 at 10:44 PM  
Time Zone: Taipei Standard Time  
Reboot Device: None  
Apply Policy to: Current Group Only

Turn On Monitor

Mon	From 08:00	To 20:00
Tue	From 08:00	To 20:00
Wed	From 08:00	To 20:00
Thu	From 08:00	To 20:00
Fri	From 08:00	To 20:00

[Check Conditions](#) [Done](#)

### 5.4.2 View Device Status

The device status includes up/down time, CPU usage, Memory Usage, Storage Usage, Bandwidth Usage, System Temperature and Assigned Time Zone.

#### \*up/down time

*Up time: the time record device last power on time.*

*Down time: the time record device last shut down time.*

\*Click “C” to change the temperature unit to Celsius.

Click “F” to change the temperature unit to Fahrenheit.

The screenshot shows a 'Status' page with a timestamp of 02/26/2020 at 06:29 PM. On the left, system metrics are listed: Up/Down Time (Up since 02/26/2020 at 11:28 AM), Time Zone (UTC+08:00 | Taipei Standard Time), CPU Usage (0.00%), Memory Usage (1.41 GB), Storage Usage (15.56 GB), and System Temperature (30 °). The temperature unit selector shows 'F' and 'C' buttons, with 'C' highlighted by a red box. On the right, network details are provided for two connections: Intel(R) Ethernet Connection I219-LM and Intel(R) I210 Gigabit Network Connection #2, including MAC and IP addresses and bandwidth usage.

### 5.4.3 View Device Activities Log

If you want to know the device activities history and details, you can view the Device Activities Log. The activities log will include all the device activities such as enrollment, moving, activation and deactivation. Click the “**Details**” link at the deactivation activity to evoke the Deactivation Details dialog.

The screenshot shows an 'Activities' page with a date range filter set to 03/11/20 - 03/17/20. The log contains ten entries, each with a 'Details' link, the user who performed the action, and the timestamp. The activities include 'Send Commands' and 'Plugin Command' performed by 'sam.wu@acer.com' and 'Eason.sung@acer.com' on 03/16/2020. The last entry is 'Modified Configuration' performed by 'Eason.sung@acer.com' on 03/16/2020 at 01:42 PM. At the bottom right, there are links for 'Previous page' and 'Next page'.

## 6. Applications

Applications are responsible for the App Management. Windows installer and binaries are supported. You can **Add/Update/Remove apps** through ADM. You can also **Add/Edit the associated configuration** including Silent install/uninstall command, Log path, Upload time and Specific settings. It also supports approval flow.

### 6.1 Enter Applications

If you want to enter Applications from Menu, click “Applications” icon on the left menu to enter Applications.

The screenshot displays the BDM Applications management interface. The top navigation bar shows 'BDM >' and 'America'. The main content area is titled 'Applications ( 1,972 )' and features a 'Group' dropdown menu set to 'BDM Only (6)'. Below this is a table listing applications:

Name ^	Platform	Privilege	Latest Version	Distributed Version	Group
ABS-3G1 Image	Android	Open	1.023.00		BDM
ADM Agent	Windows	Restricted	2.12.2003		BDM
ADM Agent (aiSage)	Android	Restricted	2.12.2003		BDM
ADM Agent (Debian)	Linux	Restricted	2.07.2001		BDM
ADM Agent (Tinkerboard S)	Android	Restricted	2.12.2003		BDM
ADM Agent (Ubuntu)	Linux	Restricted	2.12.2003		BDM

Annotations in the image include a red box around the 'Register' button in the top right corner and a red arrow pointing from the text 'Enter Applications' to the 'Applications' icon in the left sidebar. Another red arrow points from the text 'Register applications' to the 'Register' button.

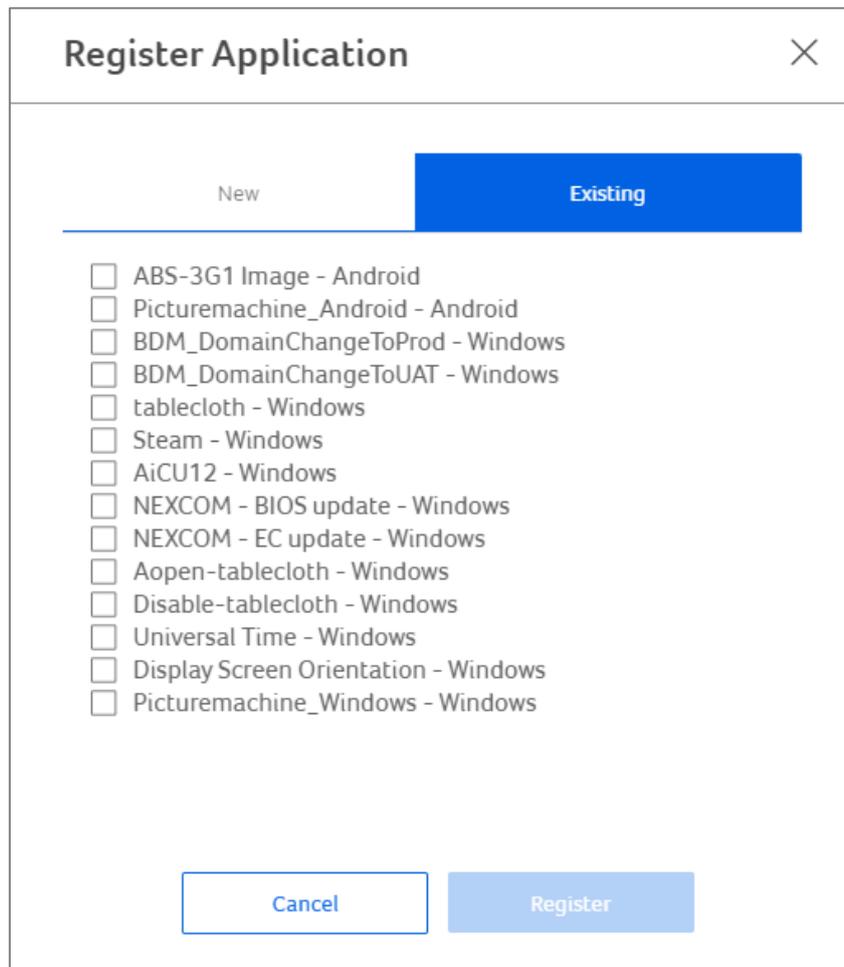
## 6.2 Register Applications

In Applications, there are two kinds of application you can register, the first one is Existing Application, the other one is New Application.

### ● Existing Application

Register an Existing Application means you like a subscriber of application on this Portal. You will see several applications that are registered in your parent groups and listed in the “Existing” tab, and you can select the application you want to register. After registering that, the application you select will appear on your application list.

Please note, if you would like to register an Existing Application, you need to have the action “Register Existing Apps” in your role.



The screenshot shows a dialog box titled "Register Application" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "New" and "Existing". The "Existing" tab is currently selected and highlighted in blue. Below the tabs, there is a list of 15 applications, each with a checkbox to its left. The applications listed are:

- ABS-3G1 Image - Android
- Picturemachine\_Android - Android
- BDM\_DomainChangeToProd - Windows
- BDM\_DomainChangeToUAT - Windows
- tablecloth - Windows
- Steam - Windows
- AiCU12 - Windows
- NEXCOM - BIOS update - Windows
- NEXCOM - EC update - Windows
- Aopen-tablecloth - Windows
- Disable-tablecloth - Windows
- Universal Time - Windows
- Display Screen Orientation - Windows
- Picturemachine\_Windows - Windows

At the bottom of the dialog, there are two buttons: "Cancel" and "Register".

- New Application

Before registering a new application, there is an information you need to check: Application GUID. And the information which is used to be Application GUID is so different in three platforms.

- Windows: Windows application's GUID
- Linux: Linux application's package name
- Android: Android application's package name

**About the application's GUID and package name, please get that from the application's provider.** If you cannot get that information, there are few tips to help you to get that by yourself. The easiest way is that installs the application on a device first manually, and you can find the information as following steps:

- Windows

The first step is check whether the application is 32-bit or 64-bit version. Please follow the below steps to check that.

- Please use this keyboard shortcut: "**Ctrl + Shift + Esc**", it will open the "Task Manager".
- Go to the "**Details**" tab, and right-click or press and hold any column header and choose "**Select columns**".
- Find and check the "**Platform**" box. Then, click or tap OK.
- The application you are installed and look at the "**Platform**" column in the Task Manager. For each running application or process, this column tells you whether it is 32-bit or 64-bit.

According to the application bit version we find, we will use this information to find out the application's GUID.

- Please type "**regedit**" in the search box on the taskbar. Then, select the top result for "Registry Editor" (Desktop app).
- If application is 64-bit, go to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\**<NewApplicationGUID>**.
- If application is 32-bit, go to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\**<NewApplicationGUID>**.

If you cannot find the GUID from this way, use can define the GUID by yourself, then there are some steps you need to do when you create a version of the application, more details please refer to the section "6.4.1 Create Application Versions".

- Linux

Please use following command to list the matched applications and find out the package name of the application you want to find.

- `dpkg -l | grep <keyword>`

- Android

Please go to the file explorer of the device and go to the following path to find out the package name of the application you want to find.

- Internal Storage > Android > data

Now, I believe that you already understood the Application GUID of your application, and we can start to register the application.

Register a New Application means you like an application publisher on this Portal, and you can create, release new version for this application. All the children groups can register this application through register an Existing Application.

In order to register a New Application, there are several information you need to fill in. After finishing the information, the application will be registered in you group.

- Application Name
- Application GUID (It's provided by application provider or you can define it by yourself)
- Platform

Please note, if you would like to register an Existing Application, you need to have the action "Register Existing Apps" and "Register Open Apps" in your role.

**Register Application** [X]

**New** Existing

Title

**GUID**

Platform [v]

**Privilege**

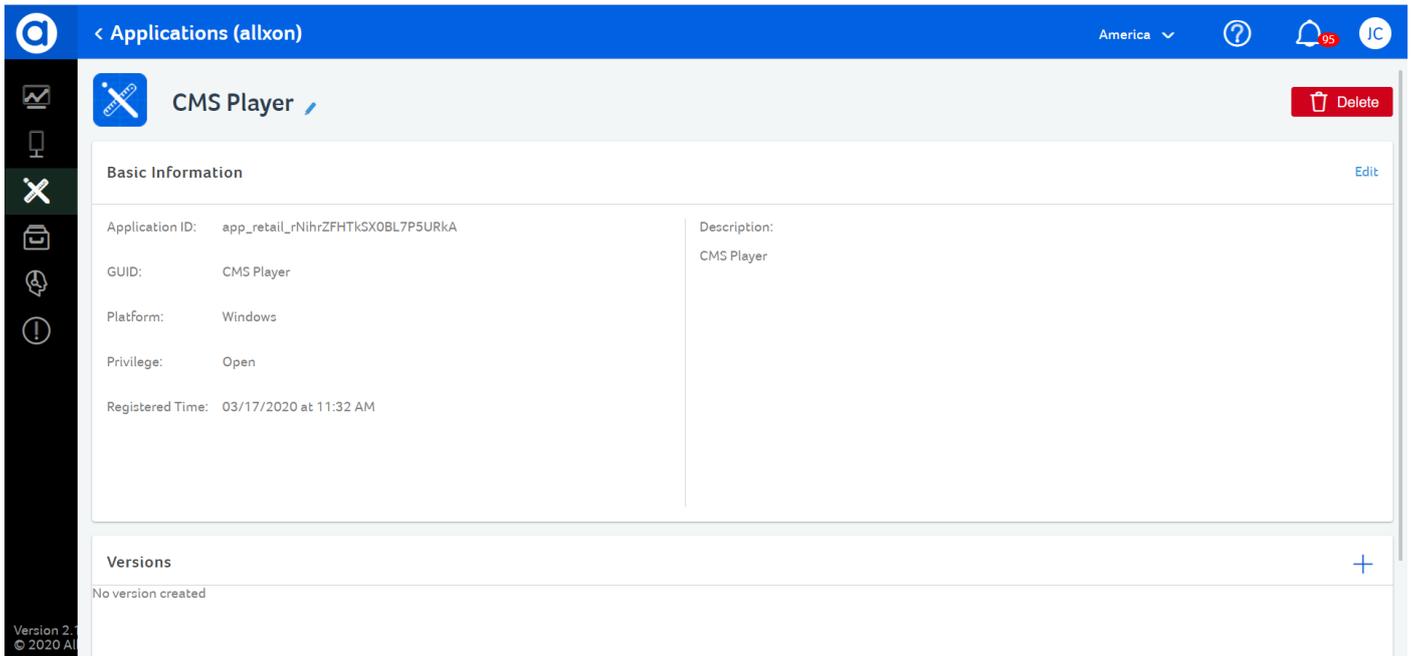
Open  
Allow children groups to install or uninstall

**Provided by the Application Company**

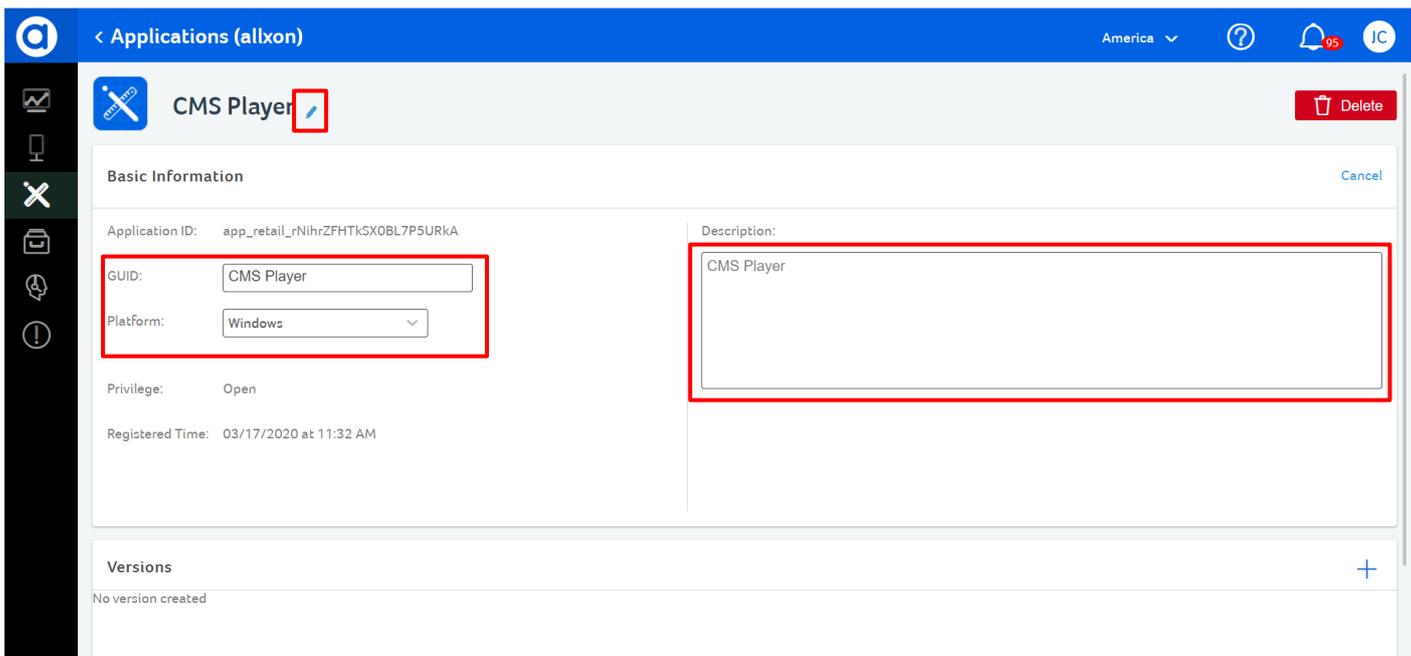
Cancel Next

## 6.3 Application Profile

When you enter the application profile page, if the application doesn't have any version, then the versions list will be **empty** before a new version is created.



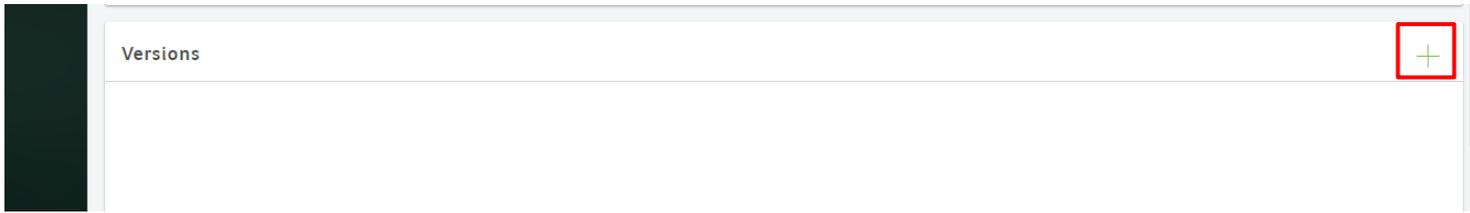
If you want to edit the **app title**, click “**Edit**” icon for the app title to enter app title edit mode. The app title input box will be focused and appear in place. Enter the new app title and make the change. If you want to edit the **app basic information**, click “**Edit**” button to enter information edit mode. Then click desired input box or drop-down selector (Platform, description) to make the desired changes. You can click “**Save**” button to save the change or click “**Cancel**” button to cancel the task and exit the edit mode.



## 6.4 Application Versions

### 6.4.1 Create Application Versions

If you want to create a new version of the application to the portal, click “+” button to evoke new version creation dialog.



Enter the version number, and then enter installation and uninstallation command. The installation and uninstallation command should have been provided by the Application Company. After entering the commands, click “**Upload a File**” button to evoke the system file picker. In this stage, the status is called “Preparing”, and the next step of this version is “Release”. Besides, you can edit this version anytime before you release this version.

#### <Note 1>

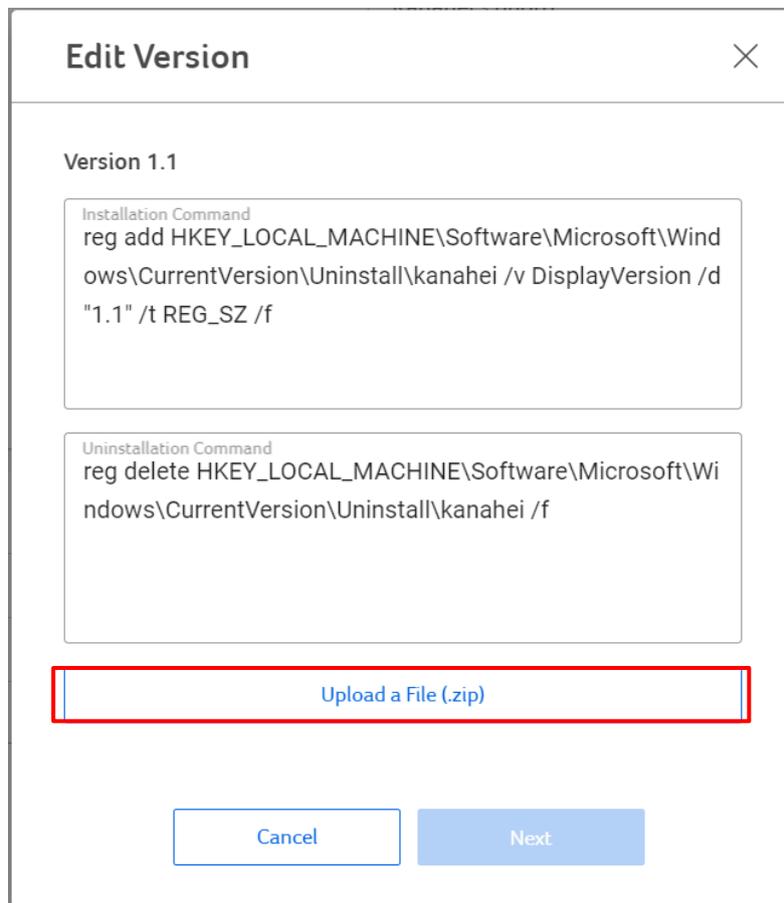
We’ve mentioned that if you cannot find out the Application GUID of your application from Windows system, you can define the GUID for your application (please refer to the section “6.2 Prepare the Information for Your Application”). Now we will teach you how to write the install and uninstall command for your application with self-defined Application GUID case.

#### ● Install command

- Insert the following content after the mark `reg add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\<NewApplicationGUID> /v DisplayVersion /d "<VersionNumber>" /t REG_SZ /f`
  - *NewApplicationGUID: The self-defined GUID of your application.*
  - *VersionNumber: The version number of your application, it must same with the version you write on the Portal.*

#### ● Uninstall command

- Insert the following content after the mark `reg delete HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\<NewApplicationGUID> /f`
  - *NewApplicationGUID: The self-defined GUID of your application.*
  - *VersionNumber: The version number of your application, it must same with the version you write on the Portal.*



<Note 2>

If the application is a Linux application, please add following command in the begin of your install command.

- `sudo unzip -o /var/lib/SyncAgent/download/<ZipFile> -d <UnzipFolderPath>`
  - `ZipFile`: The file name of your zip file.
  - `UnzipFolderPath`: The file path of the folder which you want to assign to put the extract files.

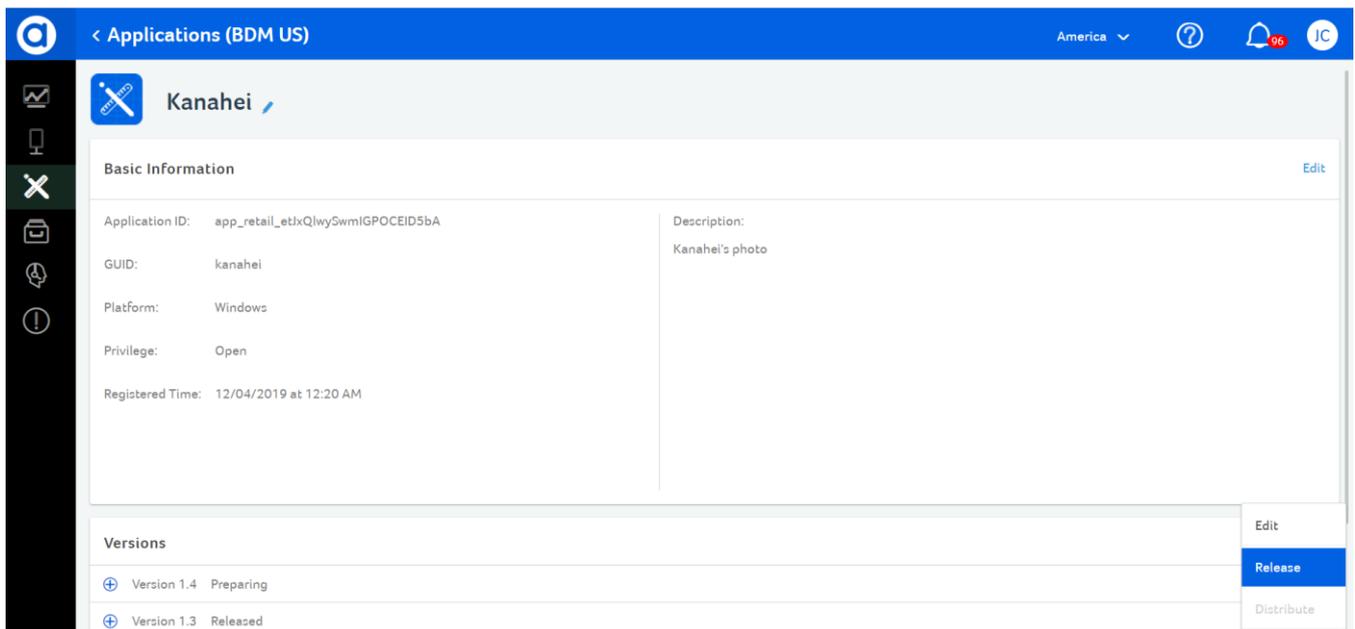
Select a file through the file picker. Then click “**Create**” button to confirm the action and dismiss the dialog. Click “**Cancel**” or “**X**” button to cancel the task and dismiss the Dialog.

\* All actions will not be saved if you click “Cancel” or “X”.

The file uploading progress bar will take place of the “**Upload a File**” button. The upload file name, the file upload percentage and the cancel upload button will be displayed on the progress bar. If you want to discard the file uploading, click the “Cancel” button and revert the progress bar back to “Upload a File” button.

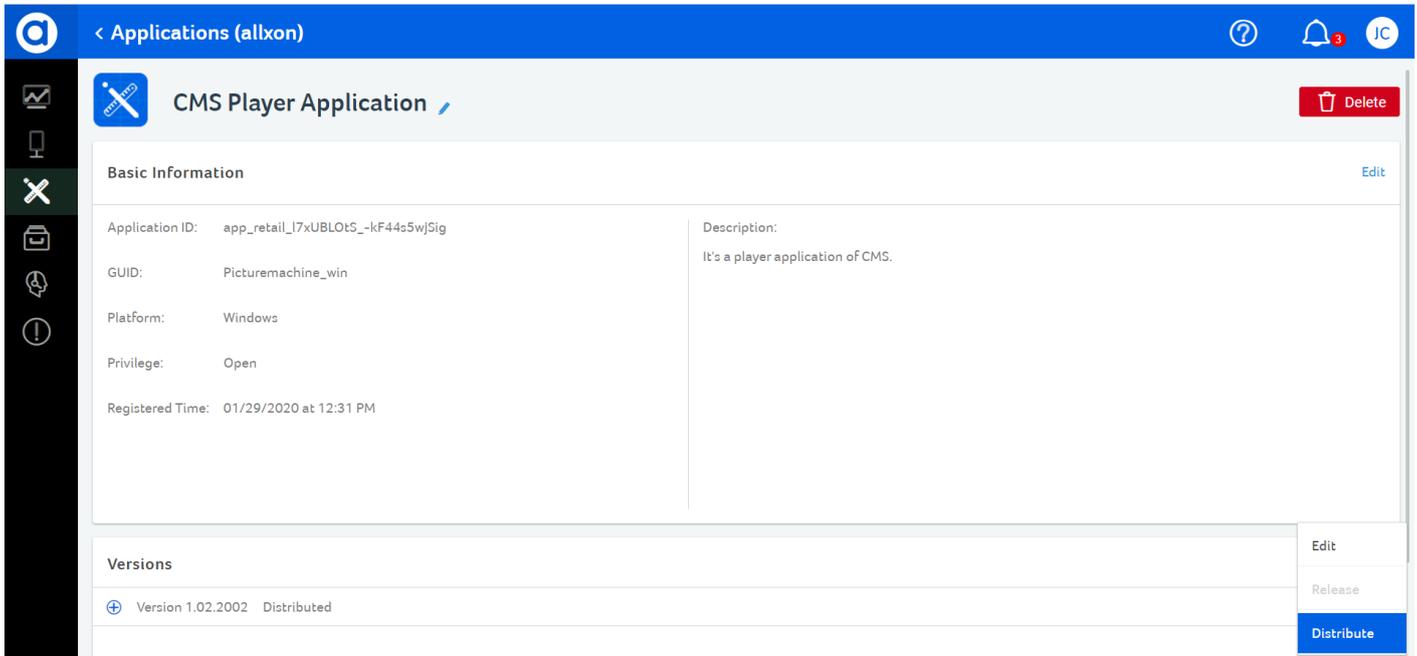


After uploading the file, just following the guidance of the dialog to finish adding a new version. Then click the “Release” to finish the release procedure, you can also write the description for this release version.



After finishing the release procedure, you can execute “Distribute” which means the application version will be distributed to the groups you assign. If you check the group from “uncheck” status, the application will be distributed to the group, on the other hand, if you uncheck the group from “checked” status, the distribution will be withdrawn from the group you select.

Besides, you can also assign the distribution schedule, the application will follow this schedule to do the distribution.



Now, I would like to help you to warm up this section, let us review the behavior of “Register”, “Release” and “Distribute”

Behavior	Object	Target	Description
<b>Register</b>	Application	To a group	<p>There are two behaviors of "Register":</p> <ol style="list-style-type: none"> <li>1. Register a "New" app <ul style="list-style-type: none"> <li>● This behavior is that the user likes an app publisher on App Store. When a user registers a "New" app in the group, this app can be registered by the children groups from "Existing apps list".</li> </ul> </li> <li>2. Register an "Existing" app <ul style="list-style-type: none"> <li>● This behavior is that the user likes an app subscriber on App Store. The user can register an app which is registered on parent groups from "Existing apps list".</li> </ul> </li> </ol>
<b>Release</b>	Version	To all children groups which register correspond app or been distributed earlier version before	<ul style="list-style-type: none"> <li>● The user who has the action "Update App Versions" can create a new version and release it for the app in the same group.</li> <li>● Once the new version is released, the group and all children groups which <u>register this app or been distributed earlier version before</u> will see the new version information in the "Latest Version" column in the Application List page.</li> <li>● The user can also set the force update when he</li> </ul>

			releases a new version, and the force update will apply to the group and all children groups which <u>register this app or been distributed earlier version before</u> .
<b>Distribute</b>	Version	To selected groups	<ul style="list-style-type: none"> <li>● After a new version of app is released by the user, the users who belong to the group and all children groups which <u>register this app or been distributed earlier version before</u> can distribute this new released version to the selected groups.</li> </ul>

After understanding the whole picture of this function, I would like to explain one more information "Privilege" and its behavior's difference between "Restricted" app and "Open" app. The major difference is "Distribute the app's version".

About the distribute the app's version, the general condition is that

- The user must have the action "Distribute Apps".
- But more details about the "Restricted" apps, the user **cannot distribute the earlier version** for the group or **unchecked the distributed groups**.

If you would like to distribute the earlier version to your group, please contact Allxon to help you to rollback the version.

## 6.5.2 Status in Version's Activities

The Edited Version activity will be added to activity log. The version status will be displayed as “Preparing”. Activity log includes “Created”, “Edited”, “Released” and “Distributed”.

Versions		
	Version 2.12.2003 Distributed	...
Activity	User	Date
Distributed ( <a href="#">Details</a> )	jchou@allxon.com	03/13/2020 at 04:26 PM
Distributed ( <a href="#">Details</a> )	jchou@allxon.com	03/09/2020 at 03:46 PM
Distributed ( <a href="#">Details</a> )	jchou@allxon.com	03/06/2020 at 11:14 PM
Distributed ( <a href="#">Details</a> )	jchou@allxon.com	03/06/2020 at 02:06 PM
Released	jchou@allxon.com	03/06/2020 at 02:04 PM
Created	jchou@allxon.com	03/06/2020 at 02:01 PM

## 7. Policies

“Policies” is mainly used to manage the content in device. You can add or remove apps from devices. You can also modify the settings on devices. All activities will be recorded in the Policy Activities section. Click the “Policies” icon at the left menu to enter Policies Main Section

Name ^	Platform	Status	Group
000 Policies - Android	Android	Effectuated on 02/10/2020 at 10:51 AM	AOPEN(acer)/..
000 Policies - Linux	Linux		AOPEN(acer)/..
000 Policies - Windows	Windows	Effectuated on 02/10/2020 at 10:51 AM	AOPEN(acer)/..
7-11 Policies - Android	Android	Effectuated on 01/08/2020 at 03:52 PM	License control test/..
7-11 Policies - Linux	Linux		License control test/..

### 7.1 Enter Policy Profile

If you want to enter policy profile, click the **Policy Title** from the Policies List to enter Policy Profile. The second column “Status” represents the effected day/time of the policy.

Name ^	Platform	Status	Group
000 Policies - Android	Android	Effectuated on 02/10/2020 at 10:51 AM	AOPEN(acer)/..
000 Policies - Linux	Linux		AOPEN(acer)/..
000 Policies - Windows	Windows	Effectuated on 02/10/2020 at 10:51 AM	AOPEN(acer)/..
7-11 Policies - Android	Android	Effectuated on 01/08/2020 at 03:52 PM	License control test/..
7-11 Policies - Linux	Linux		License control test/..

Settings

Time Zone: Taipei Standard Time

Reboot Device: None

Apply Policy to: Current Group Only

Turn On Monitor ( In device local time zone )

Day	From	To
Mon	00:00	00:00
Tue	00:00	00:00
Wed	00:00	00:00
Thu	00:00	00:00
Fri	00:00	00:00
Sat	00:00	00:00
Sun	00:00	00:00

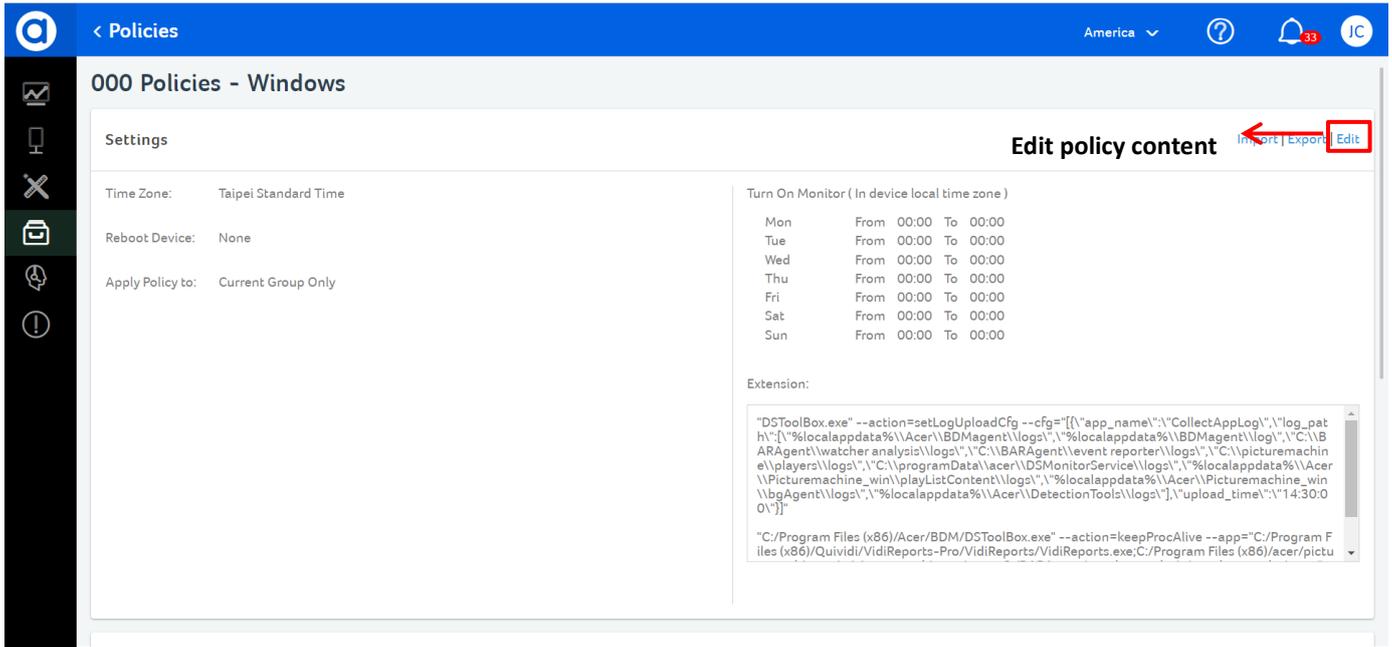
Extension:

```
"DSToolBox.exe" --action=setLogUploadCfg --cfg="{[{\"app_name\":\"CollectAppLog\",\"log_path\":\"%localappdata%\\Acer\\BDMAgent\\logs\",\"localappdata%\\BDMAgent\\log\",\"C:\\BDRAgent\\watcher\\analysis\\logs\",\"C:\\BDRAgent\\event reporter\\logs\",\"C:\\picturemachine\\players\\logs\",\"C:\\programData\\acer\\D5MonitorService\\logs\",\"%localappdata%\\Acer\\Picturemachine_win\\playListContent\\logs\",\"%localappdata%\\Acer\\Picturemachine_win\\bgAgent\\logs\",\"%localappdata%\\Acer\\DetectionTools\\logs\",\"upload_time\":\"14:30:00\"}]}"
```

```
"C:/Program Files (x86)/Acer/BDM/DSToolBox.exe" --action=keepProcAlive --app="C:/Program Files (x86)/Quividi/VidiReports-Pro/VidiReports/VidiReports.exe;C:/Program Files (x86)/acer/pictu
```

## 7.2 Edit Policy Content

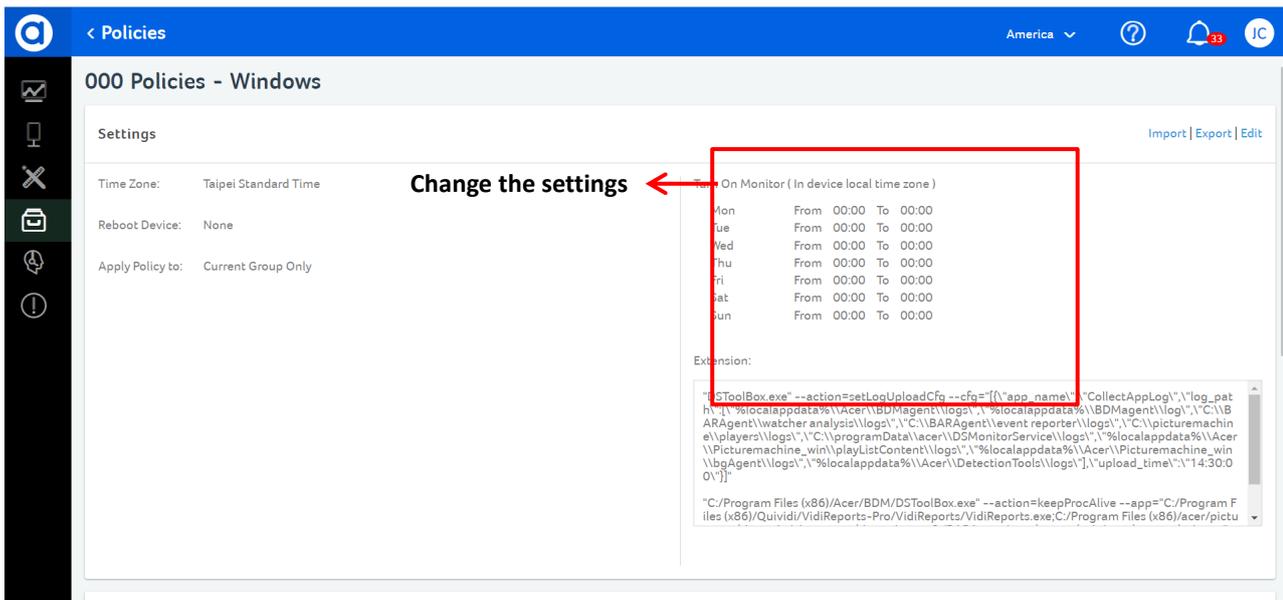
If you want to edit policy content, click **“Edit”** at right hand corner.



### 7.2.1 Change Settings

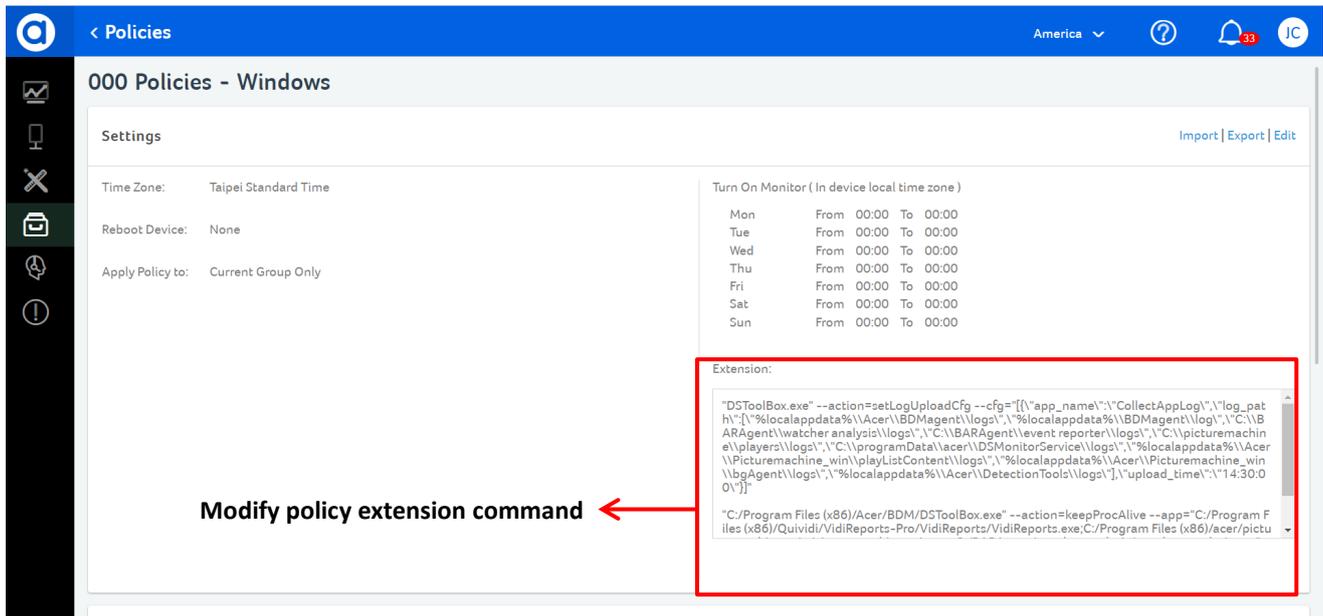
If you want to change settings, click **“Edit”** button to enter the edit mode. The editable areas will be available for editing. Click desired selectors (Time Zone, Reboot Device, Apply Policy to) or input box (Extension) to change the preference settings.

You can change the time zone; select the desired reboot time for the device; apply policies to different groups; modify the Trigger Alert threshold to send alert message. After changing the preferences, the **“Save”** button will be enabled. Click **“Save”** button to save the change and exit the edit mode.



## 7.2.2 Modify Policy Extension Command

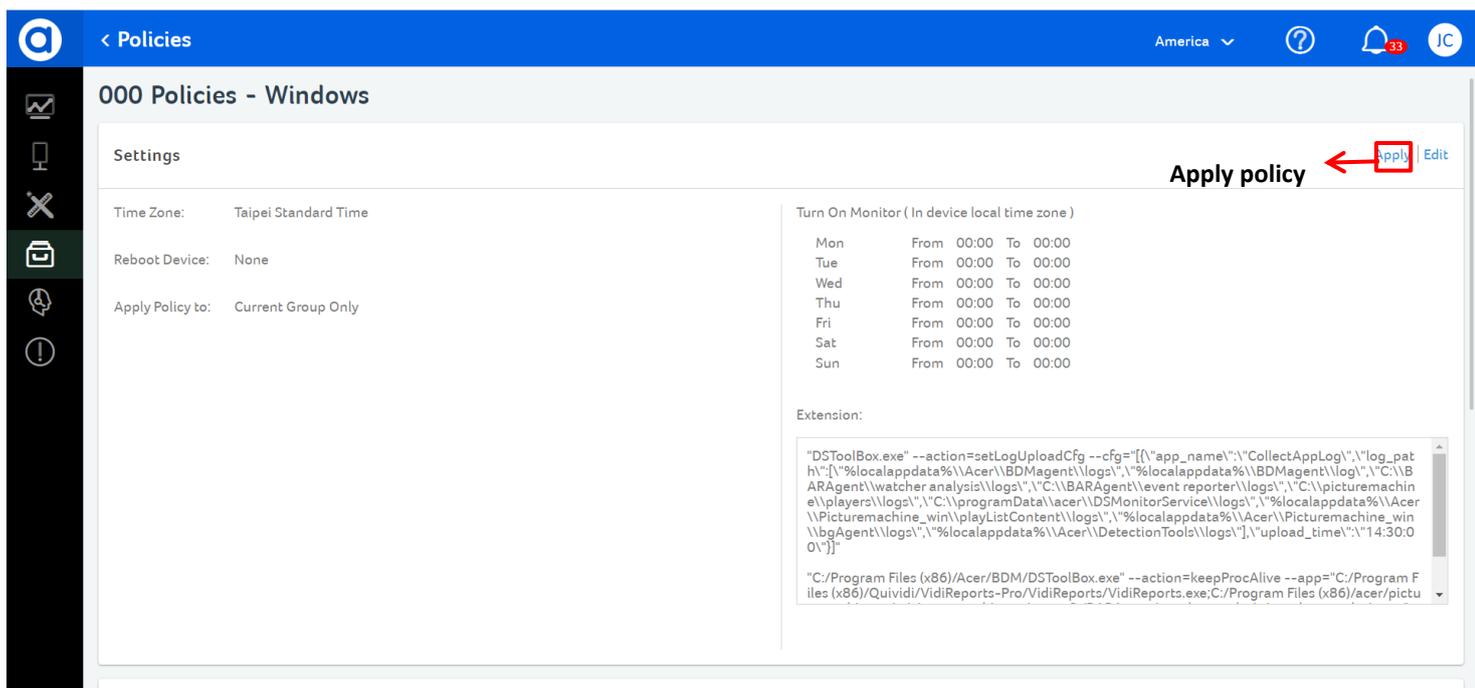
“**Extension**” in Policies Section is a function for you to add/return commands for additional information for a whole device group. The “**Extension**” dialog is about assigning the path of log. Click extension input box to modify the commands. Click “**Save**” button to save the change and exit the edit mode. When the command format is correct, execute requested action.



## 7.3 Apply Policy

When you want to deploy a new edited policy, click “**Save**” button to save the policy content changes and evoke the Apply Policy dialog. After setting the policy effective time, click “**Submit**” button to apply the latest settings of your policy to your devices.

*\*All actions will not be saved if you click “Cancel” or “X”.*



## 7.4 Set the Collect Logs Settings

From ADM Agent started supporting that the user can send command to trigger the Agent to collect the logs and return to the Portal, it becomes a popular command and function. But it is often to have typo issues about typing in the log path and other arguments of the command. In order to allow the user can get the logs from the devices easily, user can set up to 5 sets log settings in the “Collect Logs Settings” card of Policy Profile page. Especially, the user can set which log setting needs to collect the logs periodically or which log setting doesn’t need that. After finishing the setting, the Agent will follow the setting to collect the logs.

Upload Log Settings				+
⊖ AgentLogs	Everyday at 03:00 AM	by James Chou@OpenApp (Application Verification)	03/16/2020 at 04:53 PM	⋮
Log Path				
%localappdata%\DeviceMgmt\BDMagent\logs				
%localappdata%\BDMagent\log				

- Add a new setting for collecting the logs

When you click the “+” icon from the “Collect Logs Settings” card, it will pop up a window which allows you to set the following information:

1. Periodical collect schedule (optional)
2. Log package name (must have)
3. Log path (must have one path at least)

If you don’t set the periodical collect schedule, then the Agent won’t follow this setting to collect the log periodically. But it will be used if you execute the “Get Device Logs” in the Device Profile page, and the setting will appear in the list which allows the user to get the device logs immediately.

## 7.5 Set the Software Watchdog Settings

Both of us have this kind of situation is that the applications are unexpected crashed on the device, this is a pretty terrible experience. At this moment, we always need to relaunch the application through remote access.

Now, we do not need to pay a lot of effort once this situation happens again, the Software Watchdog of ADM Agent will help you to fix this situation automatically. The Software Watchdog will assist you to relaunch the application once its process is killed by the system or other factors. Let us start to know how to set the Software Watchdog for monitoring your applications.

Software Watchdog Settings ⓘ				+
Picturemachine4	C:/Program Files (x86)/acer/picturemachine_win/picturemachine_win.exe	by James Chou (Allxon)	05/13/2020 at 01:34 PM	...

- [Windows / Linux] Add a new setting for monitoring the app by Software Watchdog  
When you click the “+” icon from the “Software Watchdog Settings” card, it will pop up a window which allows you to set the following information:
  1. App Name: The application name which can help you to identify. (must have)
  2. App Path: The executable file path of the application on the device. (must have)

Software Watchdog Settings

App Name:

App Path:

- [Android] Add a new setting for monitoring the app by Software Watchdog  
When you click the “+” icon from the “Software Watchdog Settings” card, it will pop up a window which allows you to set the following information:
  1. App Name: The application name which can help you to identify. (must have)
  2. Package Name: The package name of the application. (You can get this information from the application provider) (must have)
  3. Class Name: The class name of the application. (You can get this information from the application provider) (must have)
  4. Type: The type of the application, there are three types are available. (must have)
    - Top Activity

- Activity
- Service

### Software Watchdog Settings ✕

App Name:

Package Name:

Class Name:

Type:  ▾

## 7.6 Set the USB Keyboard & Mouse Lock Settings

When ADM is used on the devices which are deployed in the field without the users to operate it, the device owner always afraid that the device may be hacked by inserting the USB keyboard or USB mouse then executing some malicious behaviors.

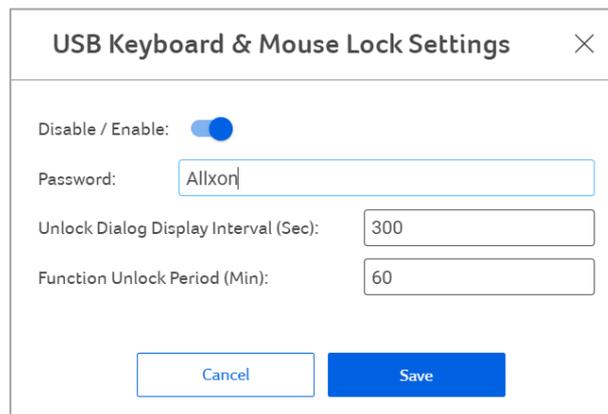
To prevent this kind of situation, ADM provides a feature about USB keyboard & mouse lock settings, it can help the users to prevent their device been hacked by unexpected behaviors with USB keyboard or mouse. Today, we will teach you how to enable this function and finish related settings for your devices.

USB Keyboard & Mouse Lock Settings (Disable) Ⓞ 
Unlock Dialog Display Interval (Sec): 300
Function Unlock Period (Min): 60

- **Enable the USB Keyboard & Mouse Lock Settings**

When you click the setting icon from the “USB Keyboard & Mouse Lock Settings” card, it will pop up a window which allows you to set the following information:

1. Password: The password which is used to unlock the function on the device.
2. Unlock Dialog Display Interval (Sec): The parameter about the display interval of the unlock password dialog on the device.
3. Function Unlock Period (Min): The parameter for how long the device will be re-locked after the device is unlocked.



USB Keyboard & Mouse Lock Settings ×

Disable / Enable:

Password:

Unlock Dialog Display Interval (Sec):

Function Unlock Period (Min):

Unlock USB Devices List <span>🔍</span>				+
Mouse	VID_DA34 & PID_4456	by James Chou (Allxon)	05/13/2020 at 03:27 PM	...

- Add an unlock device in the Unlock USB Devices List card to unlock the function on the device  
When you click the “+” icon from the “Unlock USB Devices List” card, it will pop up a window which allows you to set the following information:
  1. Device Name: It is named by yourself to assist you to recognize the device from the Unlock USB Devices List easily.
  2. PID: The PID of the Unlock USB device.
  3. VID: The VID of the Unlock USB device.

**Add Unlock Device**
✕

---

Device Name:

PID:

VID:

<Note> This function is only allowed the user to add the device type is USB keyboard or USB Mouse, about the device type, it is determined by the system, and the bar code scanner is determined as a USB keyboard by the system generally. So when you add the USB storage device as an unlock USB device, it will NOT work!

## 8. Operators

“Operators” is mainly used to manage the ADM operators. You can add/delete new operators, assign responsibilities to operators and manage operators’ profile. Click “Operators” icon on the left menu to enter Operators Main Section.

The screenshot shows the 'Operators (478)' page in the BDM US system. The interface includes a top navigation bar with 'America' and a user profile 'JC'. A left sidebar contains navigation icons, with the 'Operators' icon highlighted and an arrow pointing to the text 'Enter operators' main section'. The main content area features a table of operators with columns for Name, Role, Joined, and Group. A red box highlights the 'Role' column header, with an arrow pointing to the text 'Operator's role'. The table lists various operators with their names, roles (e.g., BAR operator, Wellness, Tier0, BAR operator, Operator, QA Test), and groups (e.g., BDM US, ABS/.., AOPEN(acer)/..). At the top right of the table, there are buttons for 'Manage Roles' and '+ Add'.

Name	Role	Joined	Group
1, 30	BAR operator	01/30/2020	BDM US
OT 001, test	Wellness	01/26/2018	ABS/..
03, 二明	Wellness	03/22/2018	ABS/..
1R 111, react	Wellness	04/10/2018	ABS/..
OT 0219, t0	Tier0	02/19/2020	AOPEN(acer)/..
44 444, 444	Wellness	04/17/2018	ABS/..
11 1212, 1212	Operator	03/29/2018	ABS/..
12 11111, 2222	BAR operator	08/07/2018	ABS/..
12 12312, 213	Wellness	03/20/2018	ABS/..
12 111111, 22222	QA Test	02/18/2020	BDM US
1T 1231313, ttttt	Wellness	04/03/2018	ABS/..
1T 11111111, test	Wellness	05/04/2018	ABS/..

### 8.1 Add New Operators

If you want to add a new operator, Click “Add” button to evoke Add New Operator dialog. After entering the user information, the “Next” button will be enabled. Click and select the desired group. The “Next” button will be enabled.

*\*Only for those whom has the authority.*

This screenshot is identical to the one above, showing the 'Operators (478)' page. In this view, a red box highlights the '+ Add' button at the top right of the table, with an arrow pointing to the text 'Add a new operator'.

### Add a New Operator

First Name  
James

Last Name  
Chou

Email  
james@gmail.com

A temporary password will be auto-generated for the new operator.

### Select a Group

BDM DEV US

- James Test ▶
- KJ0H00 ▶
- KJ1900 ▶
- KJ1910 ▶
- K11070 ▶

Click the group name to select that group.  
Click Left/Right Arrow to enter the parent/child group.

### Assign an Operator Role

Operator Role  
ADMIN

Hide Responsibilities

- Add Roles
- Delete Role
- Update Roles
- Add Operators
- Delete Operators
- View Operator Information
- Enroll Devices
- Delete Devices
- Manage Devices
- Edit Device Information

*\*Click "Show Responsibilities" to reveal role responsibilities description when needed.*

Select desired role on the menu. The new operator will appear on the operator list. The "Pending" status will be marked to the new operator in the "Joined". The highlight will stay for 5 seconds and then fade out.

Operators ( 4 )				<input type="button" value="Manage Roles"/>	<input type="button" value="+ Add"/>	<input type="button" value="Search"/>
Name ^	Role	Joined	Group			
<span style="background-color: #007bff; color: white; border-radius: 50%; padding: 2px 5px;">JC</span> James, Chou	Admin	01/04/2020	allxon			
<span style="background-color: #007bff; color: white; border-radius: 50%; padding: 2px 5px;">JC</span> James, Chou@OpenApp	End User	03/16/2020	Application Verification			
<span style="background-color: #007bff; color: white; border-radius: 50%; padding: 2px 5px;">JC</span> Jeff, Chou	End User	01/08/2020	allxon			
<span style="background-color: #007bff; color: white; border-radius: 50%; padding: 2px 5px;">DJ</span> Derek, Jeter	End User	Pending				

## 8.2 Manage roles

The screenshot shows the 'Enter role management' section of the BDM US / allxon interface. A red box highlights the 'Manage Roles' button, and a red arrow points to it from the text 'Enter role management'. Below this, there is a table of operators.

Name ^	Role	Joined	Group
James, Chou	Admin	01/04/2020	allxon
James, Chou@OpenApp	End User	03/16/2020	Application Verification
Jeff, Chou	End User	01/08/2020	allxon

\*Here are the actions that user can decide for each role :

Function	Action
Operators	View Operator Information
	Add Roles
	Delete Roles
	Update Roles
	Add Operators
	Delete Operators
	Manage Operators (Edit)
	View Notifications
	View Group Mails
Devices	View Device Information
	Enroll Devices
	Delete Devices
	Manage Devices
	Edit Device Information
	Change Device Groups
Applications	Send Commands
	View App Information
	Register Apps
	Remove Apps
	Update App Versions
Policies	Edit App Information (Edit GUID...)
	Distribute Apps
Groups	View Policy
	Update Policy
	View Groups
	Create Groups
Reports	Delete Groups
	Edit Groups
	View Reports
	Download Reports
	Subscribe Reports

\*Only for those whom has the authority.

### 8.2.1 Create new roles

If you want to create a new role, click the **“Create”** button to evoke the Create Role dialog. After dialog pops up, you can edit the role name you want and check the **“checkboxes”** for the actions you need. Once all desired actions are selected finish, click the **“Create”** button to confirm the action and exit the edit mode, and the newly created role will be displayed on the role list with the highlight for 5 seconds and then fade out.

The screenshot shows the 'Roles' table in the BDM US / allxon interface. The table has columns for Name, Users, and Group. A '+ Create' button is visible in the top right corner.

Name ^	Users	Group
Admin	1	allxon
Device enroll person	0	RetailX
End User	2	allxon
End User	1	Application Verification

### Create a New Role ✕

Role Name

**Responsibilities**

Categories

- Operators**
- Devices
- Applications
- Policies
- Groups
- Reports
- Analytics
- Alerts
- AiCU Features

Actions

- View Operator Information
- Add Roles
- Delete Roles
- Update Roles
- Add Operators
- Delete Operators

### 8.2.2 Edit/Delete Existing Roles

If you want to edit the roles, select a role and click its **“Edit”** button to evoke the Edit Role dialog, and then you can select the functions you need and unselect the functions. After everything finish, don't forget clicking **“Save”** button to save your configuration. You can also click the **“Delete”** button to delete the role.

Roles <span style="float: right;">+ Create</span>			
Name ^	Users	Group	
Admin	1	allxon	
Device enroll person	0	RetailX	 
End User	2	allxon	
End User	1	Application Verification	

### 8.3 Edit Operator Profile

If you want to edit operator profile, click the desired operator's name to enter Operators' Main Section.

Operators ( 4 ) <span style="float: right;">Manage Roles</span> <span style="float: right;">+ Add</span> 			
Name ^	Role	Joined	Group
 <a href="#">Derek, Ieter</a>	End User	Pending	allxon
 <a href="#">James, Chou</a> <span style="border: 1px solid red; padding: 2px;">Enter operator's profile page</span>	Admin	01/04/2020	allxon
 <a href="#">James, Chou@OpenApp</a>	End User	03/16/2020	Application Verification
 <a href="#">Jeff, Chou</a>	End User	01/08/2020	allxon

### 8.3.1 Change Group

If you want to change the group, click **“Edit”** button to enter edit mode. Select the desired group to change the group. Click **“Save”** to save the change.

The screenshot shows the user profile for James Chou. At the top left is a profile card with a blue circle containing 'JC' and the name 'James Chou'. To the right is a red 'Delete' button. Below is a 'Basic Information' section with two columns of data. The left column contains: Account (User ID: james7800243+allxon@gmail.com), Joined Time (01/04/2020 at 03:50 PM), and Country (Taiwan). The right column contains: Access (with an 'Edit' link), Group (allxon), and Role (Admin with a 'Responsibilities' link).

The screenshot shows the user profile for James Chou in edit mode. The 'Basic Information' section is the same as in the previous screenshot. The 'Access' section now has 'Cancel' and 'Save' buttons. The 'Group' dropdown menu is open, showing a list of groups: 'allxon' (selected), 'BDM US', 'Allxon Training Program', 'AOPEN(acer)', and 'B2B'.

### 8.3.2 Change Role

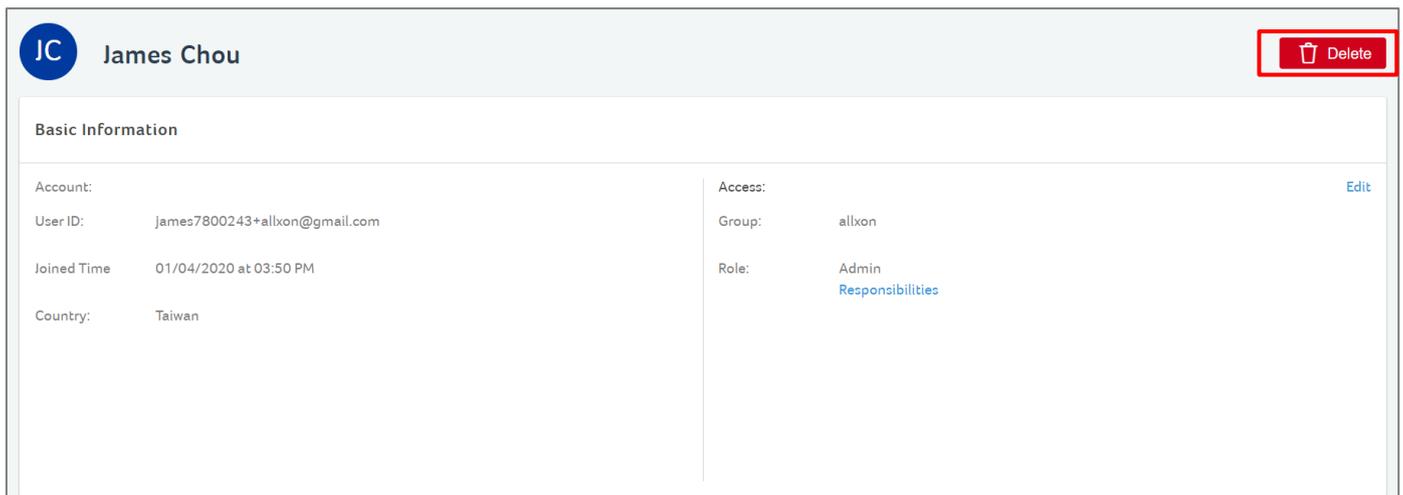
If you want to change role, click **“Edit”** button to enter edit mode. Select the desired role to change the Operator role. Click **“Save”** to save the change.

\*Click **“Responsibilities”** to reveal role responsibilities description when needed.

The screenshot shows the user profile for James Chou in edit mode. The 'Basic Information' section is the same. The 'Group' dropdown is set to 'allxon'. The 'Role' dropdown menu is open, showing 'Admin' and 'End User'. A red box highlights the 'Admin' option, and a red arrow points to it with the text 'Change the role'.

### 8.3.3 Delete an operator

If you want to delete an operator, click **“Delete”** button to evoke the Delete Operator dialog and then click **“Delete”** button to confirm the action.

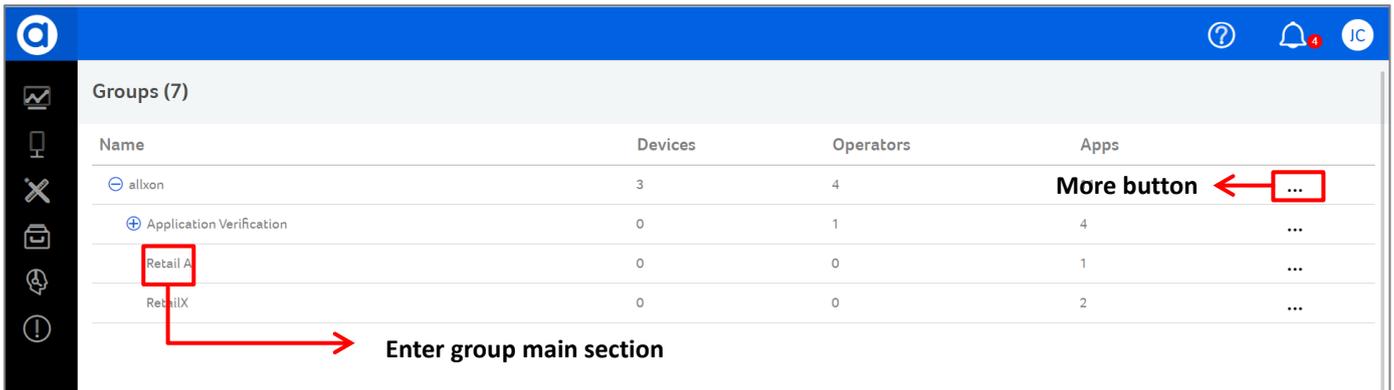


The screenshot shows a user profile page for James Chou. At the top left, there is a circular profile picture with the initials 'JC' and the name 'James Chou'. At the top right, there is a red button with a trash icon and the text 'Delete', which is highlighted with a red rectangular box. Below the header, there is a section titled 'Basic Information'. This section is divided into two columns. The left column contains the following information: Account: (blank), User ID: james7800243+allxon@gmail.com, Joined Time: 01/04/2020 at 03:50 PM, and Country: Taiwan. The right column contains: Access: (blank), Group: allxon, and Role: Admin. There is a blue 'Edit' link at the top right of the right column. Below the Role, there is a blue link for 'Responsibilities'.

Basic Information	
Account:	
User ID:	james7800243+allxon@gmail.com
Joined Time	01/04/2020 at 03:50 PM
Country:	Taiwan
Access:	
Group:	allxon
Role:	Admin
	<a href="#">Responsibilities</a>

## 9. Groups

“Groups” is a hierarchical structure where you can organize the groups and learn about the group hierarchy from his/her group level.



Name	Devices	Operators	Apps
allxon	3	4	More button ← ...
Application Verification	0	1	4
Retail A	0	0	1
RetailX	0	0	2

### 9.1 Edit groups

Click “Groups” icon at the left menu to enter Groups Main Section.

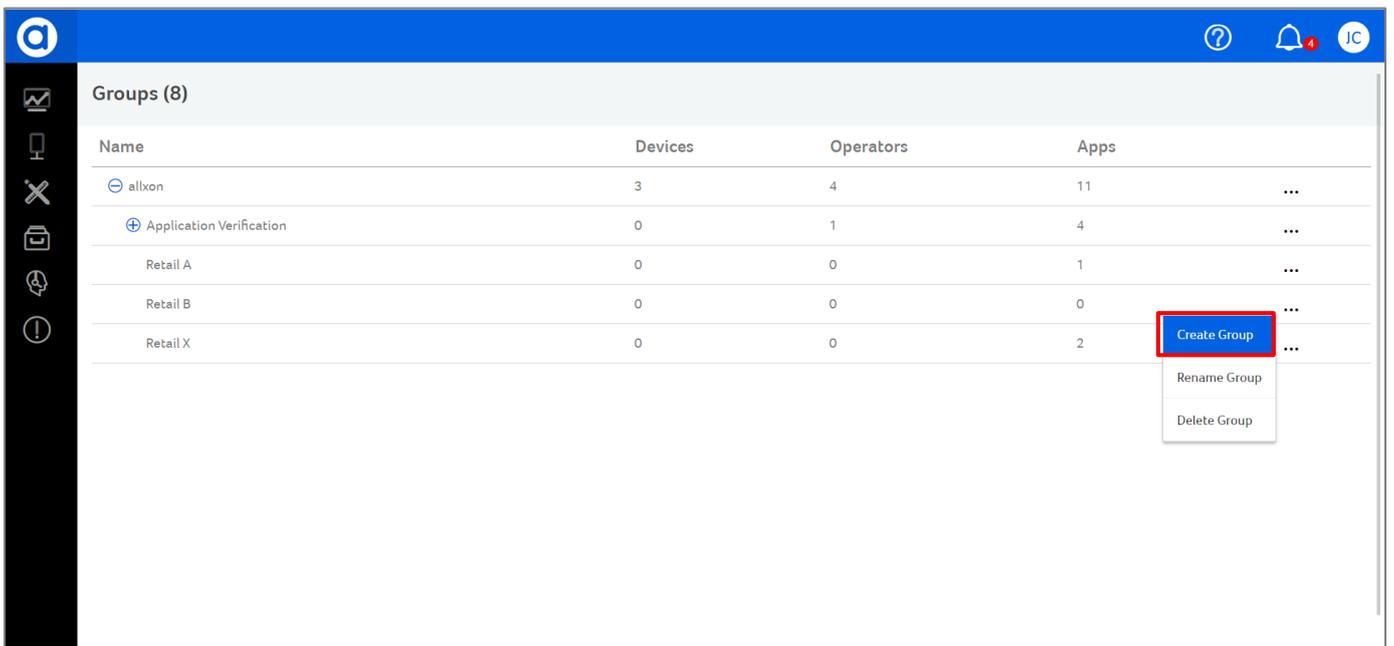
Click the “Expand Arrow” at the root group to show the child groups.

You can find data of ADM (devices, operators and Apps) on the group main section page.

#### 9.1.1 Create a New Group

If you want to create a new group, select a group and click its “More” button to reveal the group contextual menu. Click “Create Group” in the contextual menu to reveal the group input box. The selected group will expand and reveal its sub-group list. After the new group name entered, click “Create” button to confirm the action.

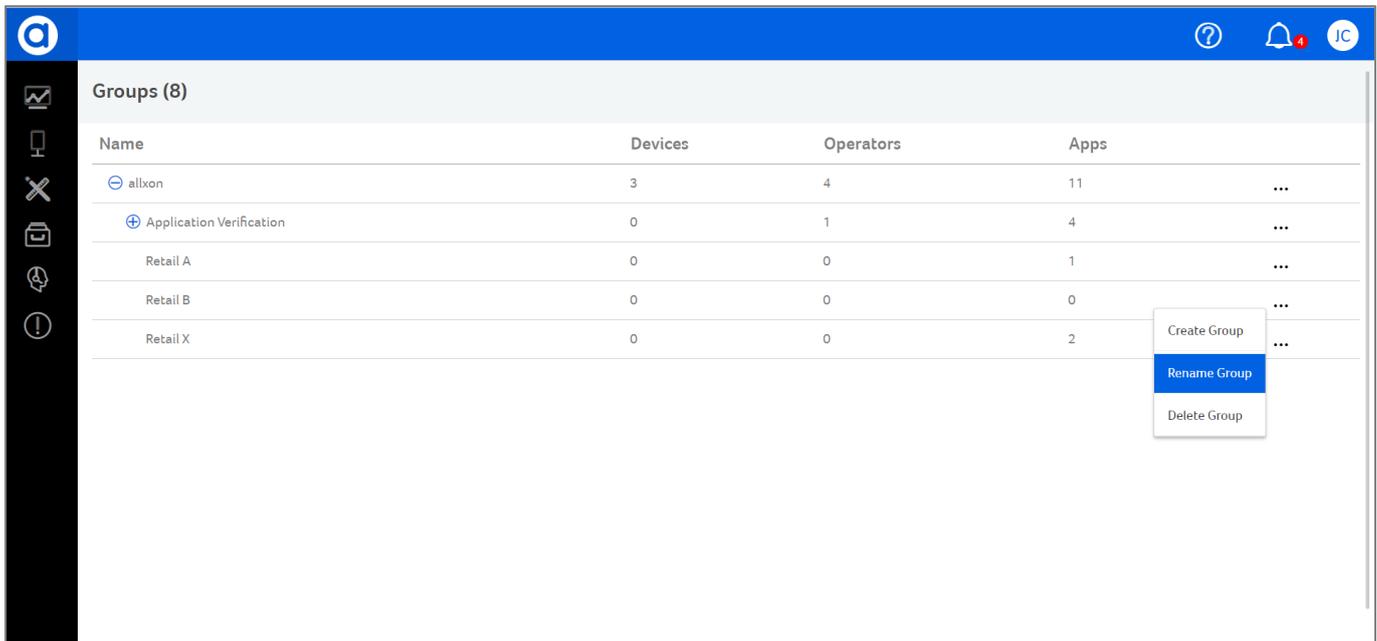
\*Only for those whom has authority.



Name	Devices	Operators	Apps
allxon	3	4	11
Application Verification	0	1	4
Retail A	0	0	1
Retail B	0	0	0
Retail X	0	0	2

### 9.1.2 Rename a Group

If you want to rename a group, select a group and click its **“More”** button to reveal the group contextual menu. Click **“Rename Group”** in the contextual menu to reveal the group input box, the group input box will be on focus and ready to edit. After the group name edited, click **“Save”** button to confirm the action. Only for those whom has authority.

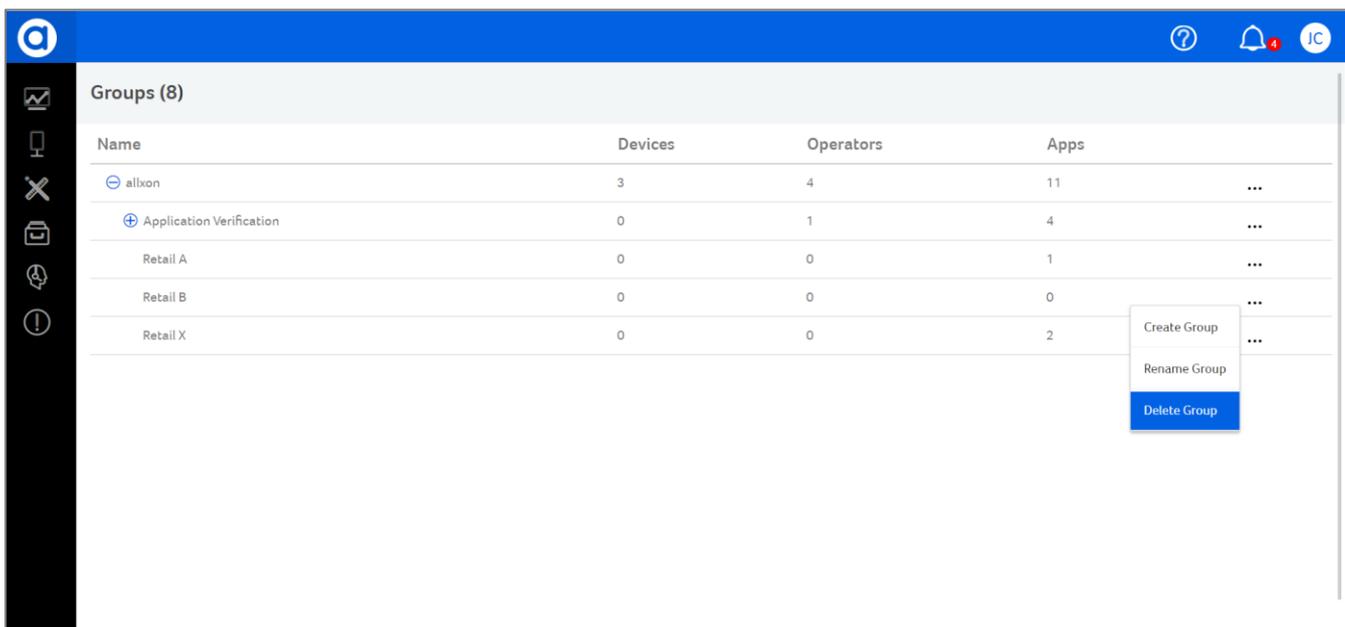


### 9.1.3 Delete a Group

If you want to delete a group, select a group and click its **“More”** button to reveal the group contextual menu. Click **“Delete Group”** button to evoke the delete group dialog. Click **“Delete”** button to confirm the action and dismiss the dialog, the selected group will be removed from the group list.

Please note, there is a condition of **“Delete Group”** is that the number of the Devices, Operators and Apps must be zero, then user can see the option **“Delete Group”** in the list and execute that.

\*Only for those whom has authority.



## 9.2 Enter Sub-Groups

If you want to enter a sub-group, you can click the right arrow near the group name on the Dashboard, and it will display a list which includes the next level children groups of this group, then you can select one of them and enter it.

The screenshot shows the Allxon dashboard interface. At the top left, the 'allxon' logo is followed by a right-pointing arrow icon, which is highlighted with a red box. A dropdown menu is open, listing sub-groups: 'Application Verification', 'Retail A', 'Retail B', and 'Retail X'. Below the dropdown, there are several dashboard widgets. The 'Device Summary' widget shows '0 Alerts' and a list of categories: 'System', 'Display', 'Peripheral', and 'Others'. The 'Online / Offline Status' widget shows '0 Online' and '3 / 3 Offline / Abnormal'. The 'Enrollment Status' widget shows '3 Total Devices', with '3 Provisioned' and '0 Not Provisioned'. The 'Device Status' widget is a line chart for the period '03/10/20 - 03/16/20', showing 'Total Devices' (green line), 'Provisioned' (blue line), and 'Unprovisioned' (grey line). The 'Device Platforms' widget shows a donut chart with the number '3' in the center, representing the total number of devices, with a legend for 'Windows', 'Android', and 'Linux'.

## 10. Alerts

In the device management field, the alert of device state is an important topic and function which allows user to get the information immediately when device has abnormal situation. In Allxon Device Management, we provide a function which is called "Alerts", user can enable the alert for his device and set the recipient for receiving the alert mail easily. After finishing the settings, you will receive the alert mail when your device has abnormal situation.

Firstly, users need to complete SMTP settings that enables alert emails to be delivered based on users' SMTP settings or finish the LINE settings to deliver the LINE message through LINE channel. Alert items and alert email recipients can be set through ADM web Portal user interface as well.

### 10.1 Setup SMTP

In the beginning, the user needs to get the SMTP settings from IT organization or apply from the SMTP service provider, after filling in the settings information, the user needs to do the verification to make sure this SMTP setting is workable or not.

The necessary information of SMTP settings as below:

- SMTP Client: We support two types SMTP client settings: "Internet" and "Intranet".
  - Internet: It means the alert mail will be sent out from outside of environment which SMTP server exists.
  - Intranet: It means the alert mail will be sent out from inside of environment which SMTP server exists. Because some enterprises have strictly IT policy which doesn't allow the mail which uses SMTP settings is sent out from outside of environment which SMTP server exists. So user needs to select this option and Agent will help to send out the alert mail.
- Enable/Disable: It allows user to enable and disable the SMTP settings. If user disables it although he set the SMTP settings completely, it won't send out the alert mail and user won't receive it.
- SMTP Host: It means the domain of user's SMTP server.
- SMTP Account: It means the account name of user's SMTP server account.
- SMTP Password: It means the password of user's SMTP server account.
- Port: It means the port of user's SMTP server. **Please note, Port 25 is easy to meet deny issue because of enterprise's IT Policy, and for security concern, we didn't allow user to set Port 25 when the "SMTP Client" is "Internet"!**
- Security Type: It means the security type which is supported by user's SMTP server. Currently, we only support two types: "None" and "TLS".
- Mail Sender: It means the mail address which will be used in alert mail's "sender".



Mail (SMTP) ⓘ

[Import](#) | [Export](#) | [Edit](#)

Settings

SMTP Client:

Primary SMTP Configuration

Disable SMTP / Enable SMTP:

SMTP Host:

SMTP Account:

SMTP Password:

Port:

Security Type:

Mail Sender:

Secondary SMTP Configuration

Disable SMTP / Enable SMTP:

SMTP Host:

SMTP Account:

SMTP Password:

Port:

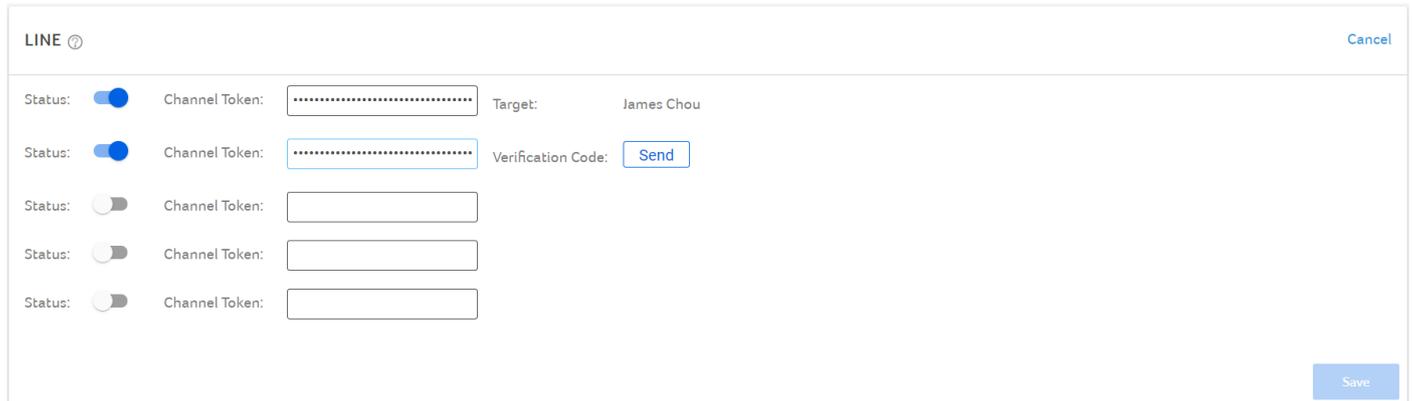
Security Type:

Mail Sender:

## 10.2 Setup LINE

Social media is an important message channel in our daily life. In order to let the operators can get the alert message much easier and faster, ADM starts to integrate with social channels so that the operators can set which alert message will be delivered to the correspond operational groups, we believe it will increase the efficiency of the management.

In the beginning, the user needs to apply the token of LINE Channel from the LINE's website, about this step, please refer to the [FAQ](#). After getting the LINE channel token, you can fill in the token in the card and enable it. In order to make sure the token is workable, you need to do the verification, you will get the verification code when you trigger the verification process.

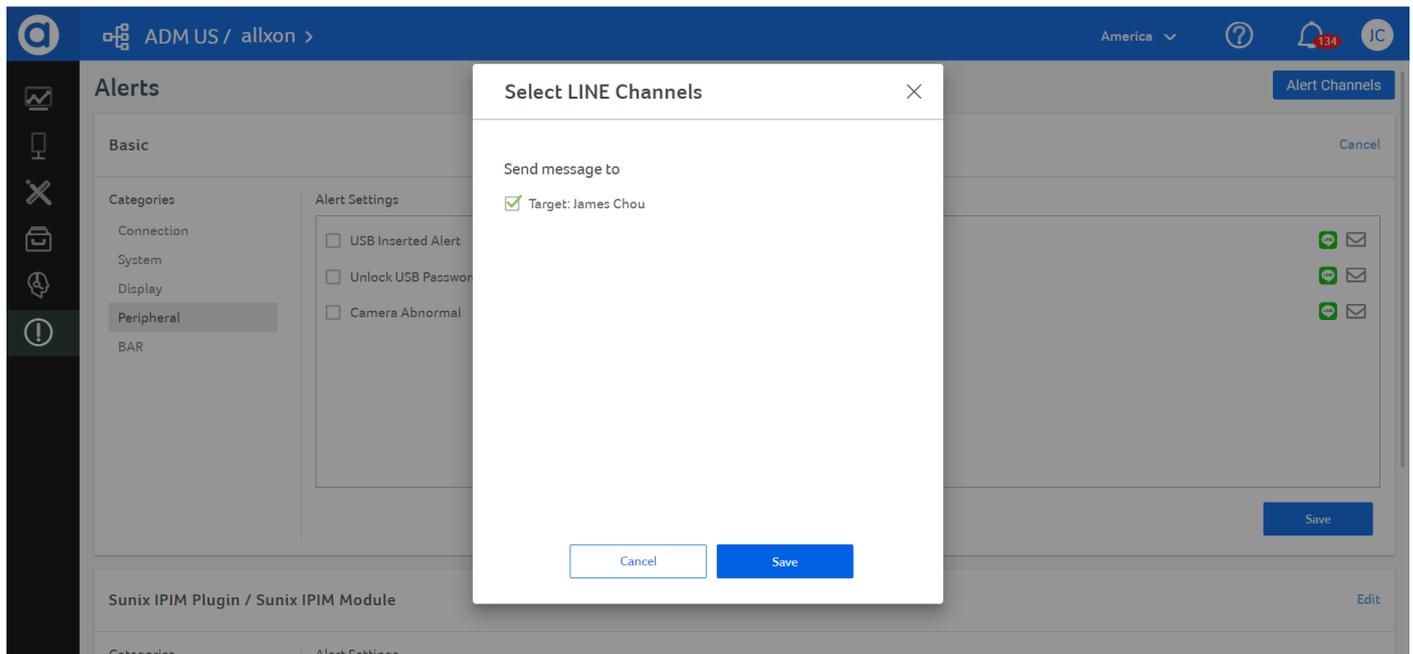


The screenshot shows a configuration window titled "LINE" with a "Cancel" button in the top right. It contains five rows of settings:

- Row 1: Status:  Channel Token: [masked] Target: James Chou
- Row 2: Status:  Channel Token: [masked] Verification Code: [Send]
- Row 3: Status:  Channel Token: [input field]
- Row 4: Status:  Channel Token: [input field]
- Row 5: Status:  Channel Token: [input field]

A "Save" button is located in the bottom right corner.

After finishing the LINE settings, the user is able to select which LINE channel will be used to delivered to alert message of the alert item.



The screenshot shows the ADM system interface with a "Select LINE Channels" dialog box open. The dialog box has a close button (X) in the top right and contains the following text:

Send message to

- Target: James Chou

At the bottom of the dialog box are "Cancel" and "Save" buttons. The background shows the "Alerts" configuration page with a sidebar menu and a main content area. The top navigation bar includes "ADM US / allxon", "America", a help icon, a notification bell with "134", and a user profile icon "JC".

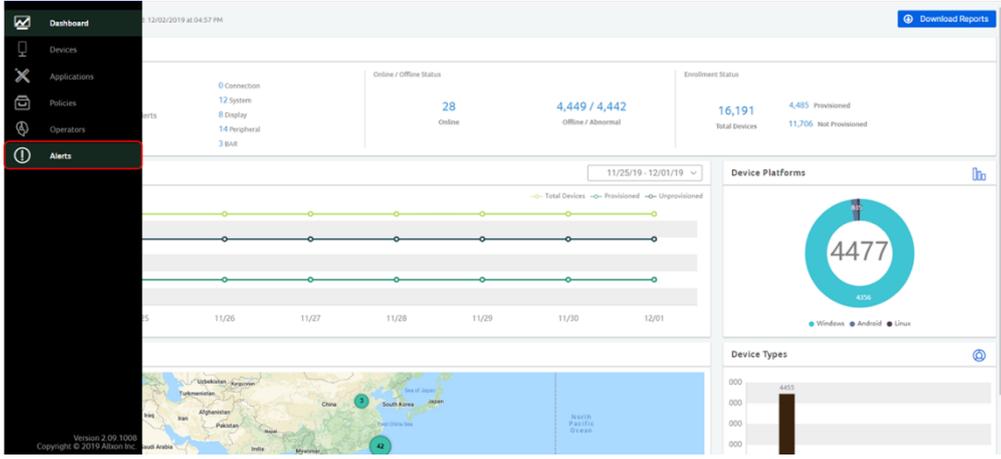
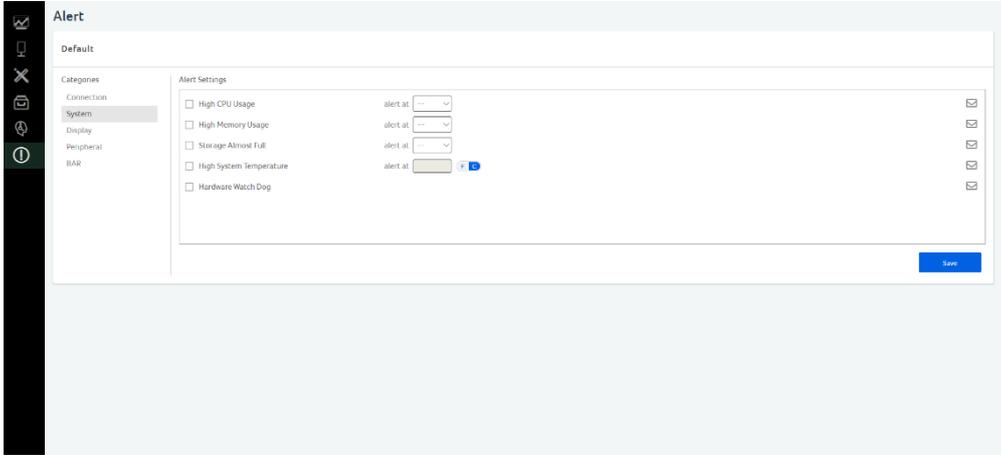
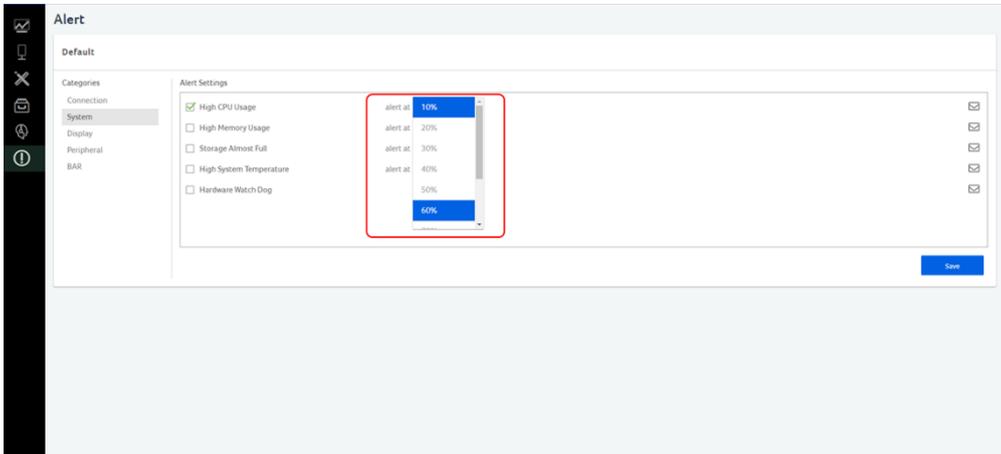
### 10.3 Alert Table

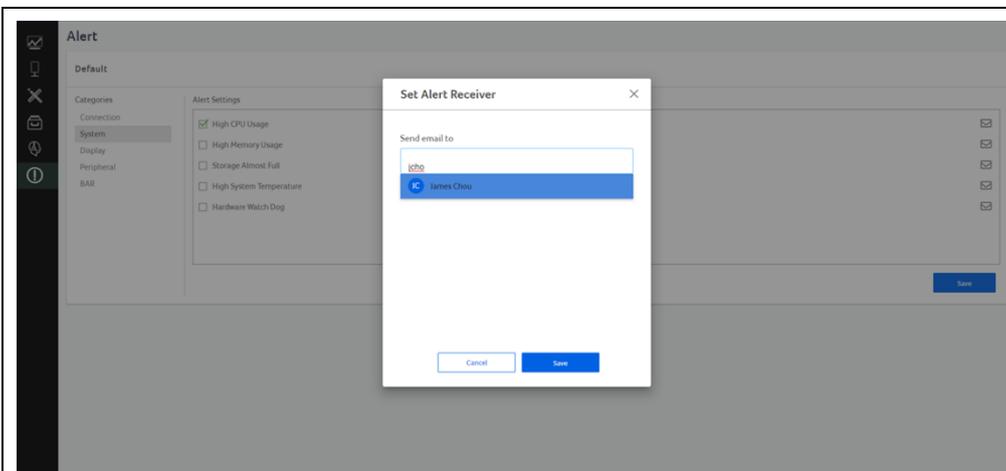
Category	Alert Item	Supported Platform	w/ Threshold	Note
Connection	abnormal offline	Windows / Android / Linux		
System	High CPU Usage	Windows / Android / Linux	√	
	High Memory Usage	Windows / Android / Linux	√	
	Storage Almost Full	Windows / Android / Linux	√	
	High System Temperature	Windows / Android / Linux	√	
	Hardware Watch Dog	Windows		(Selected Models; Please check with your hardware providers for availability)
Display	Player Black Screen	Windows / Android		
	Monitor Lose Power	Windows / Linux		
	Monitor Lose Signal	Windows / Android / Linux		
	Monitor Off	Android		In only available with the connected monitor which supports HDMI-CEC protocol.
Peripheral	USB Inserted Alert	Windows / Android / Linux		
	Unlock USB Password Error	Windows / Android / Linux		

Camera  
Abnormal

Android

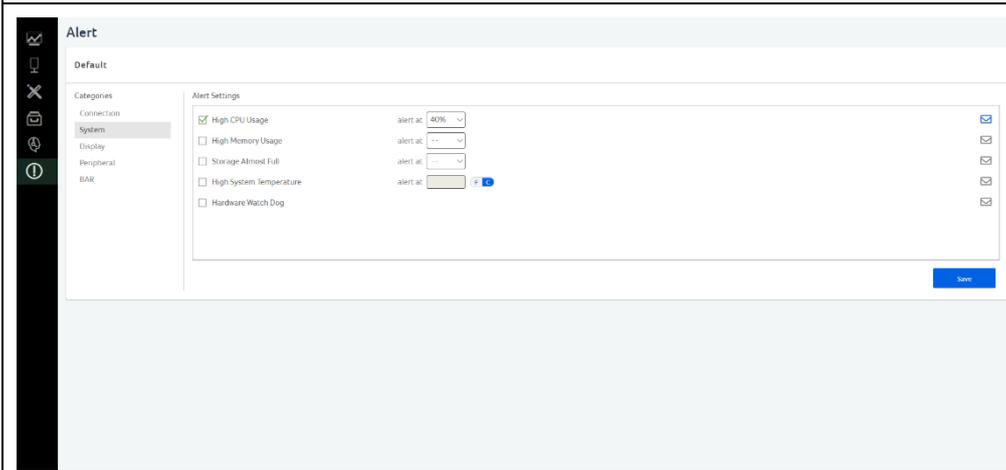
## 10.4 Enable the Alert Item and Set the Recipient

Screenshot	Steps and Description
 <p>The screenshot shows the main dashboard interface. On the left, a dark sidebar contains a menu with icons for Dashboard, Devices, Applications, Policies, Operators, and Alerts. The Alerts icon, which is a bell, is highlighted with a red rectangle. The main dashboard area displays various metrics: Online/Offline Status (28 Online, 4,449 / 4,442 Offline / Abnormal), Enrollment Status (16,191 Total Devices, 4,485 Provisioned, 11,706 Not Provisioned), Device Platforms (a donut chart showing 4477 total devices, with 42% for Windows, Android, and Linux), and Device Types (a bar chart). A map at the bottom shows device locations in South Korea.</p>	<p>Step 1. Please go to the "Alerts" page.</p>
 <p>The screenshot shows the 'Alert' configuration page. The left sidebar has the Alerts icon highlighted. The main content area is titled 'Alert' and has a 'Default' section. Under 'Categories', 'System' is selected. The 'Alert Settings' section contains several items with checkboxes and 'alert at' dropdown menus: High CPU Usage (unchecked), High Memory Usage (unchecked), Storage Almost Full (unchecked), High System Temperature (unchecked), and Hardware Watch Dog (unchecked). Each item has an 'alert at' dropdown menu with a mail icon to its right. A 'Save' button is at the bottom right.</p>	<p>Step 2. In this page, you will see several categories and alert items, just enable the alert you want to set for your devices.</p>
 <p>This screenshot is similar to the previous one, but the 'High CPU Usage' checkbox is now checked. The 'alert at' dropdown menu for 'High CPU Usage' is open, showing a list of percentage options: 10%, 20%, 30%, 40%, 50%, and 60%. The 10% option is highlighted with a blue background. A red rectangle highlights the dropdown menu.</p>	<p>Step 2-1. Some of the alert items may need to set the alert threshold. For example. CPU usage, memory usage, disk usage and system temperature need user to set the threshold for them.</p>



Step 3. After enabling the alert item, don't forget setting the recipient who is a valid user in ADM system for receiving the alert mail. When you type in the username or mail address, the system will help you to search out the match user automatically.

If you click the "Save" button without setting the recipient, you will see a red banner on the top of screen to remind you to set the recipient.



Step 4. Clicking the "Save" button with finishing all settings.

The alert email will be sent when the set threshold has been hit for longer than 5 minutes. The mechanism is designed to prevent the false alarm and reduce unnecessary email alerts. For example, if the CPU usage is back to normal in 4 minutes after the alert threshold is hit, the alert email will not be sent.