DeepHub MDM

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the DeepHub MDM. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in

compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Register a New Account

Registering a new account and start enrolling devices is simple.

Before we start, it is important to understand the terminology used by Dahua DeepHub MDM and explain the different fields, roles and concepts.

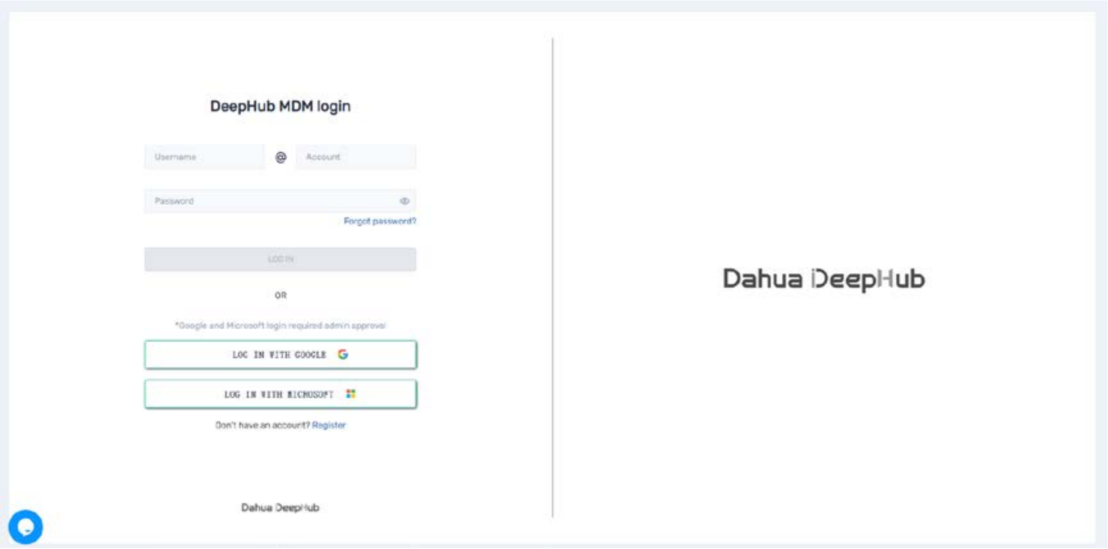
Domain, also known as the Account. This is your actual account name and will follow you everywhere, when you login, create users, connect devices, etc.

A domain can be any text that the server will respond as legal or available during registration.

Server, the server address is made of main domain and subdomain, e.g https://deephub.glbth.com/v2/ . When signing in to the console, the address should also contain “/glbth/” but when connecting a device, make sure you leave the server address as default, e.g https://deephub.glbth.com

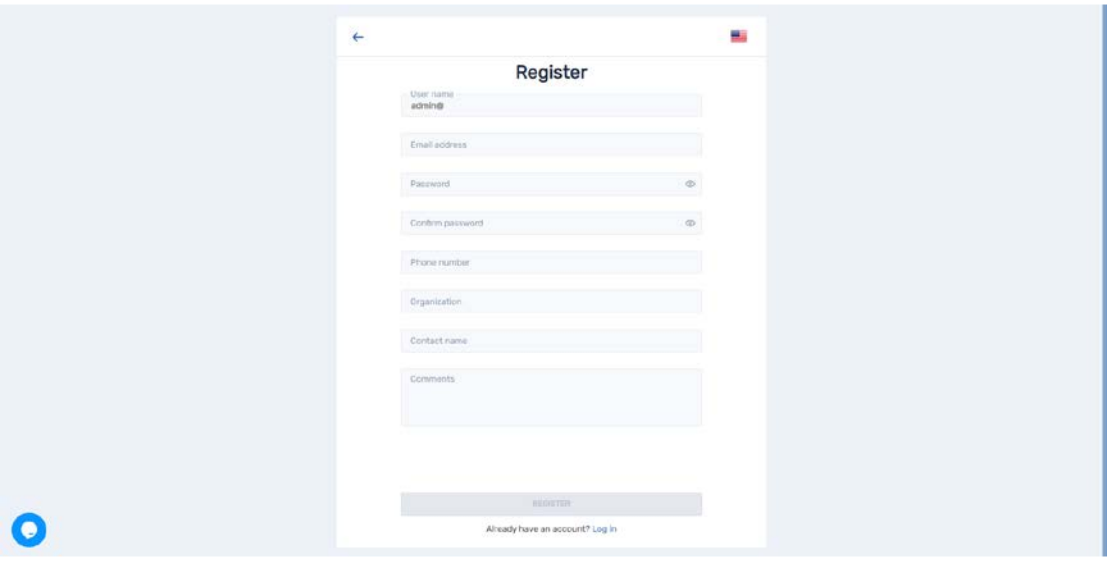
User, the user is the entity that manages devices. The format of a user will always be xxx@your-domain, “xxx” being the user and “your-domain” is the account name you registered. The default user name will be admin@your-domain and cannot be changed.

Figure 1-1 Register and sign in a new account



*Google and Microsoft login required admin approval

Don't have an account? Register



Register

User name
admin@

Email address

Password

Confirm password

Phone number

Organization

Contact name

Comments

Already have an account? Log in

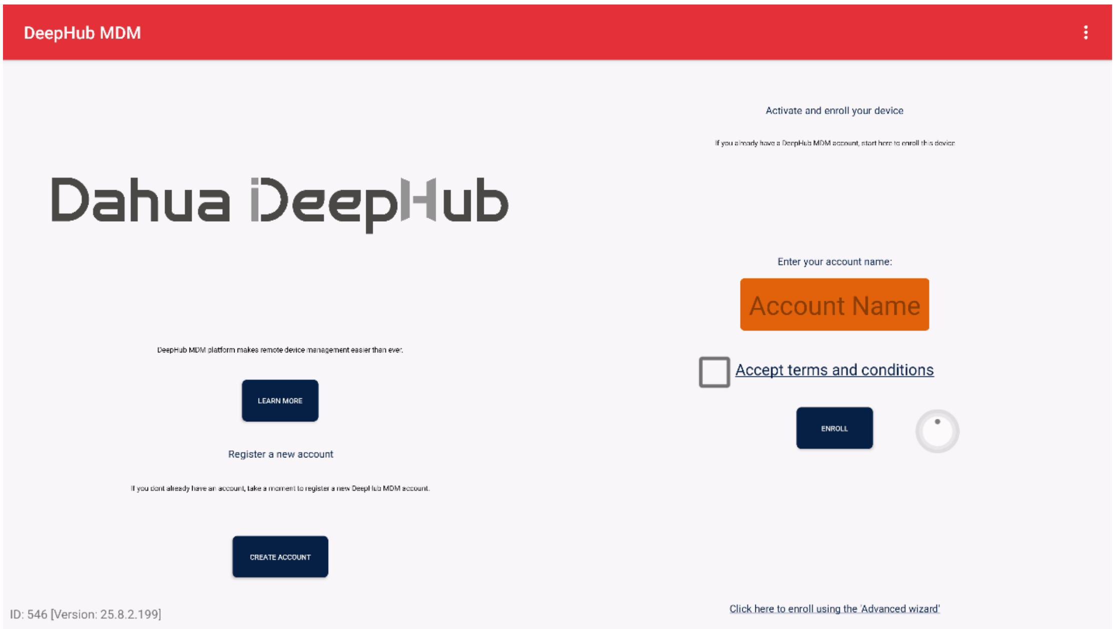
Remember, the username format is admin@your-domain with no extra suffixes, e.g .com

2 Enroll an Android Device

Side-loading (manual installation)

1. Install the agent file.
2. Once the installation is complete, follow the installation wizard. When getting to the "Account name" or "domain name", depending on the agent version (it is the same) section, make sure that you enter the name as registered.

Figure 2-1 Android



Activate and enroll your device

If you already have a DeepHub MDM account, start here to enroll this device

DeepHub MDM platform makes remote device management easier than ever.

Register a new account

If you dont already have an account, take a moment to register a new DeepHub MDM account.

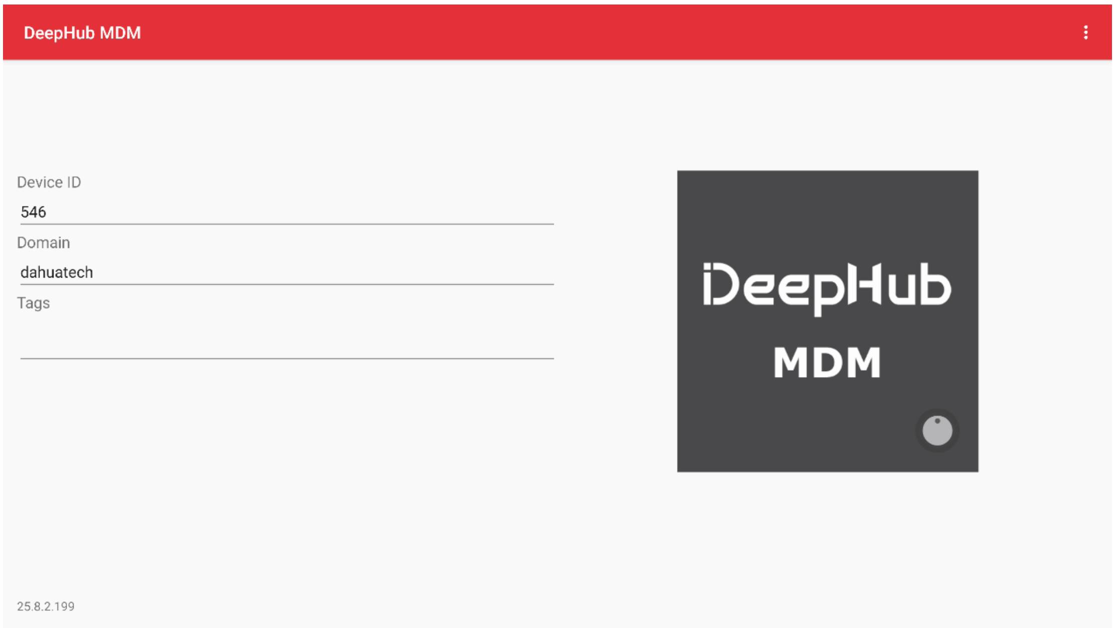
Enter your account name:

□ Accept terms and conditions

ID: 546 [Version: 25.8.2.199]

Click here to enroll using the 'Advanced wizard'

3. Follow the wizard through and finish enrollment.



Device ID
546

Domain
dahuatech

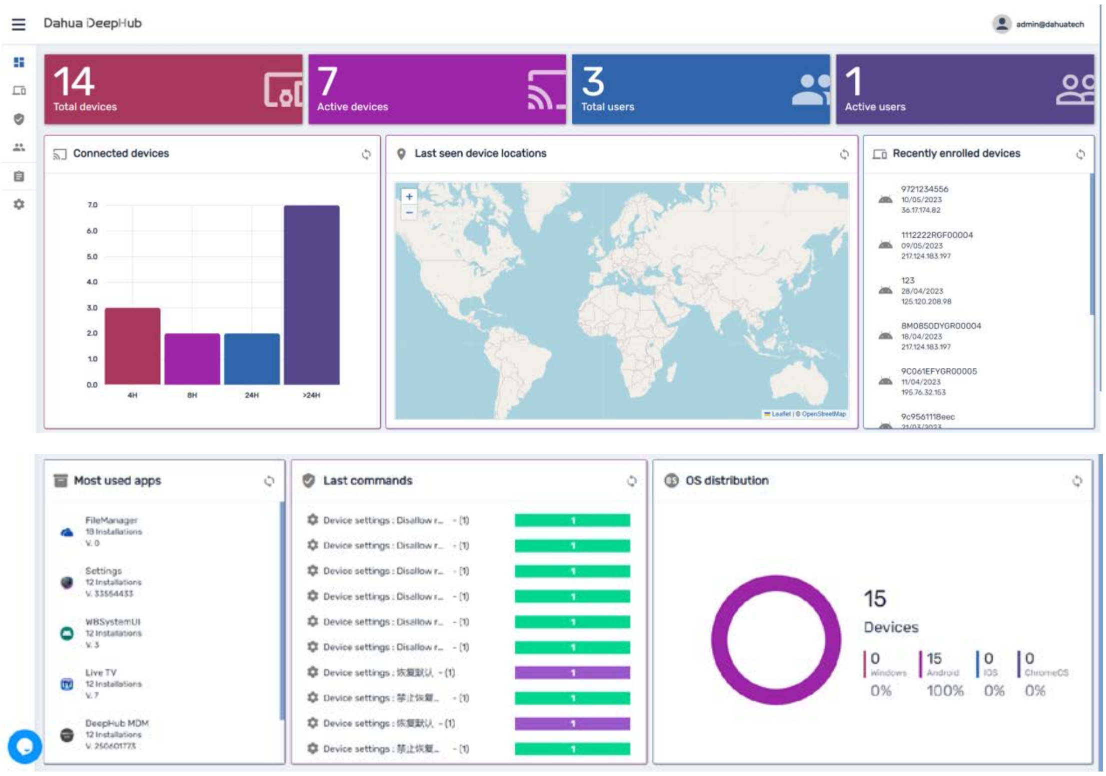
Tags

25.8.2.199

4. Install the SCManager system service additional file. This step is optional but very important.

3 Overview Dashboard

The dashboard is the first screen you see when logging into your account.

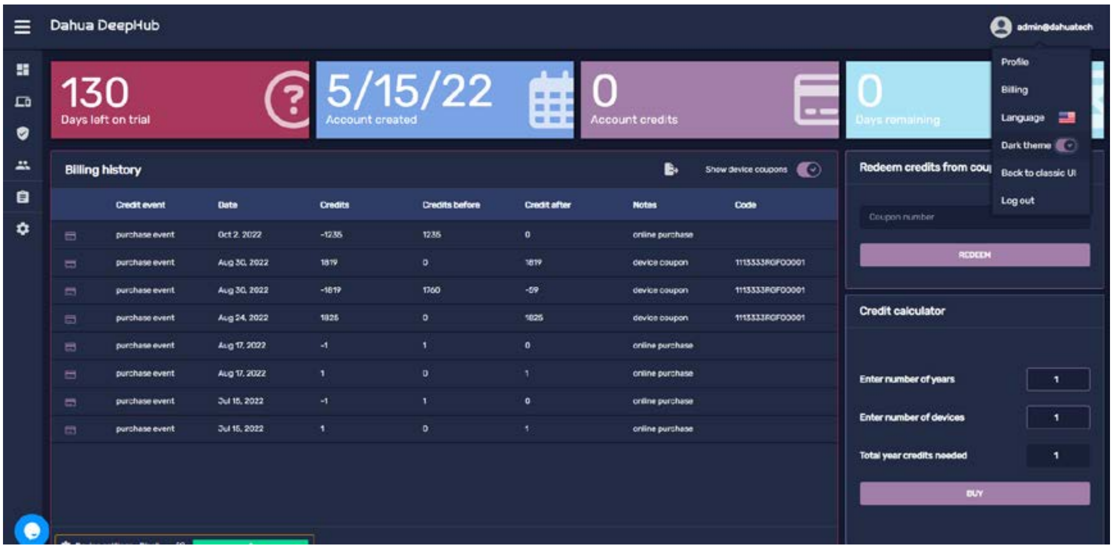


Each tile represents a block of information:

Title	Description
Total Devices	The total number of enrolled devices.
Active Devices	The total number of devices checked in the last 24 hours
Total Users	The total number of users registered with the domain
Active Users	The number of logged on users (excluding you)
Connected devices	Every bar represents the number of devices according to their last check-in time
Last seen devices location	The location of the last devices reporting connection
Apps stats	The most frequently used apps
Last commands	A list of last performed commands
OS Distribution	A pie chart showing the device operating systems distribution

In case the Default white theme is too intense for your eyes, we added the option to switch to a Dark theme. Also, you have the option Back to the classic UI that will be available in the next few months, and the option to go to the Billing section where you have more detailed information about your account (expiration date, etc.).

In addition, we added more languages such as Catalan, at any point you can switch to a different Language



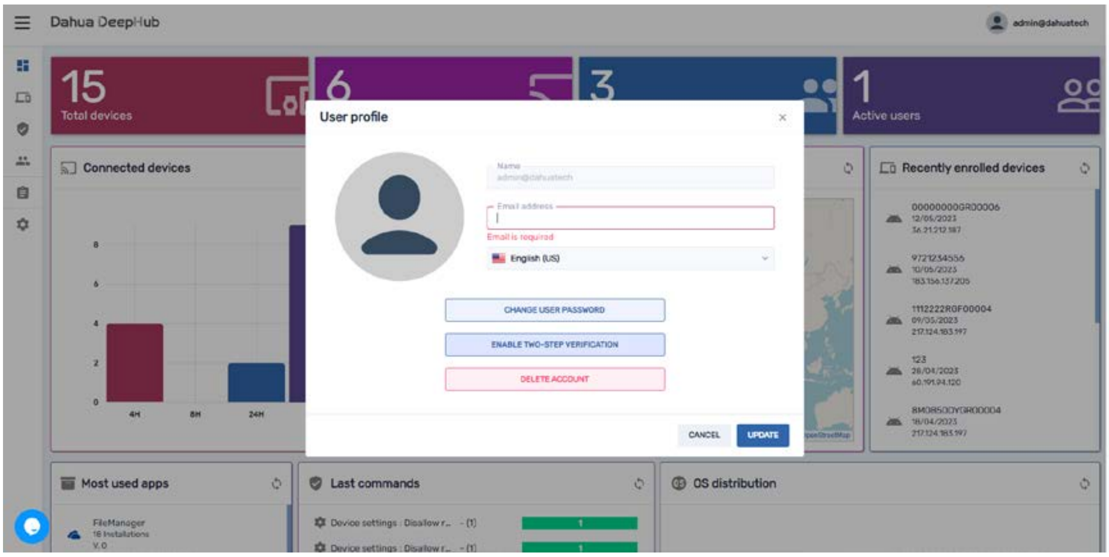
Billing history

	Credit event	Date	Credits	Credits before	Credit after	Notes	Code
	purchase event	Oct 2, 2022	-1235	1235	0	online purchase	
	purchase event	Aug 30, 2022	1819	0	1819	device coupon	1113333RGF00001
	purchase event	Aug 30, 2022	-1819	1760	-59	device coupon	1113333RGF00001
	purchase event	Aug 24, 2022	1825	0	1825	device coupon	1113333RGF00001
	purchase event	Aug 17, 2022	-1	1	0	online purchase	
	purchase event	Aug 17, 2022	1	0	1	online purchase	
	purchase event	Jul 15, 2022	-1	1	0	online purchase	
	purchase event	Jul 15, 2022	1	0	1	online purchase	

Credit calculator

Enter number of years	1
Enter number of devices	1
Total year credits needed	1

Under profile you can Enable two-step authentication to your account, making the login process more secured (we support many two-step authentication apps enabling you to scan a QR code or add a code manually like Google Authenticator, LastPass Authenticator, etc.)



User profile

Name: admin@dahuatech

Email address:

Email is required

English (US)

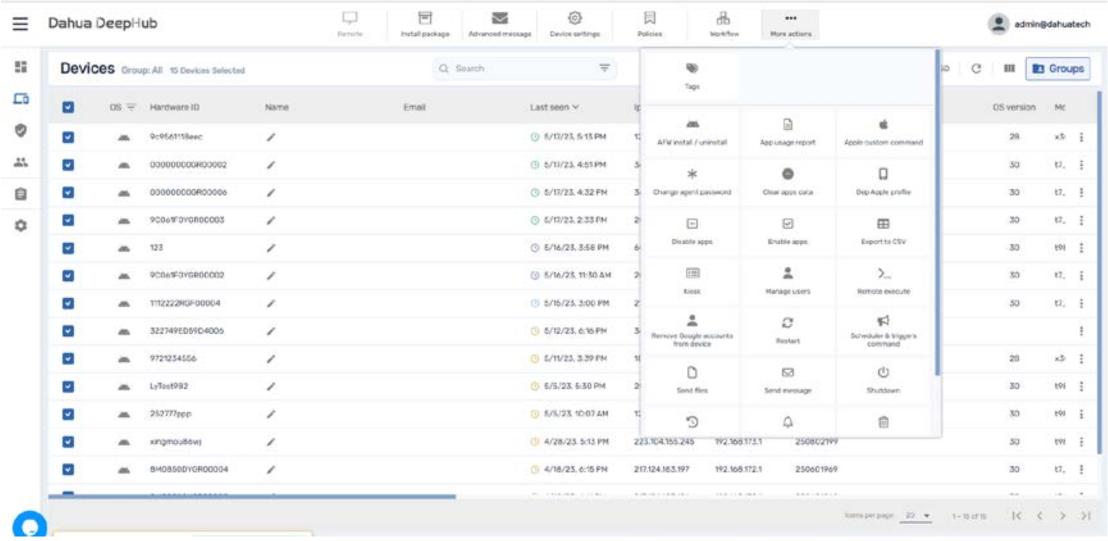
Recently enrolled devices:
- 00000000GR00006 12/05/2023 36.21.212.187
- 9721234556 10/05/2023 183.156.137.205
- 1112222RGF00004 09/05/2023 217.124.183.197
- 123 28/04/2023 60.191.94.120
- 8M08500YGR00004 18/04/2023 217.124.183.197

Most used apps: FileManager 18 Installations V.0

Last commands:
- Device settings : Disallow r... - (1) 1
- Device settings : Disallow r... - (1) 1

In the example above, the admin (who created the account) is currently logged in, hence you have the option to Delete account, other admins or users will show Delete user. Please note, Delete account will completely delete the account and all its records and log you out of the platform, Delete user will delete the user and log you out of the platform.

In the **Device console**, which is considered the heart of the platform, we changed how the menu looks like, at the very top you have most used commands and the option to expand the menu.

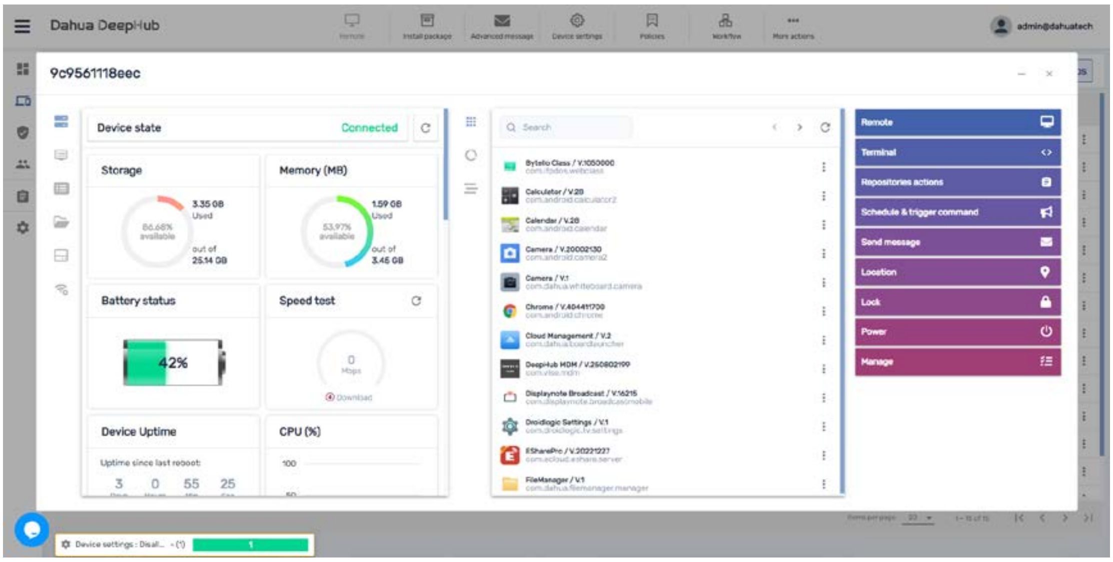


If you have a warning icon next to your device ID it means that you need to reset the device authentication token, by clicking it, a window will open asking you to confirm the reset.

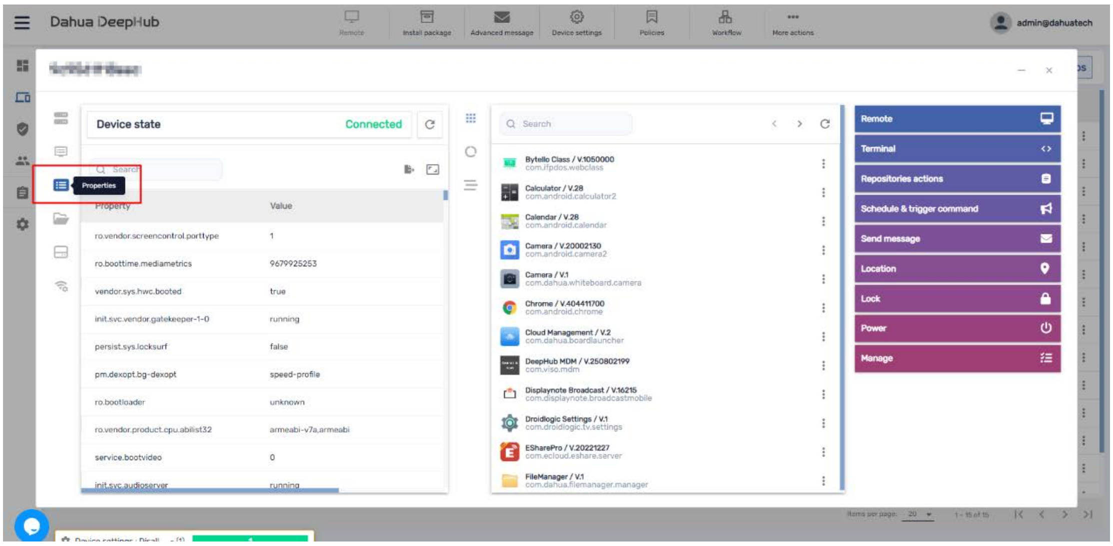
Once confirmed the warning icon will disappear

Once getting to the **Device dashboard**, things are getting much more interesting

On the left side – device information, we are providing much more information with many live dashboards such as CPU (%)/Temp, Memory/Swap Memory (MB), Wifi signal, Number of reboots and Speed test*



In addition, we added device Properties, File system and Storage stats enabling you to search, expand and export to CSV to work offline.



Device state Connected

Property	Value
ro.vendor.screencontrol.porttype	1
ro.boottime.mediametrics	9679925253
vendor.sys.hwc.booted	true
init.svc.vendor.gatekeeper-1-0	running
persist.sys.locksurf	false
pm.dexopt.bg-dexopt	speed-profile
ro.bootloader	unknown
ro.vendor.product.cpu.abilist32	armeabi-v7a,armeabi
service.bootvideo	0
init.svc.audioserver	running

Bytello Class / V.1050000
com.ifpdos.webclass

Calculator / V.28
com.android.calculator2

Calendar / V.28
com.android.calendar

Camera / V.20002130
com.android.camera2

Camera / V.1
com.dahua.whiteboard.camera

Chrome / V.404411700
com.android.chrome

Cloud Management / V.2
com.dahua.boardlauncher

DeepHub MDM / V.250802199
com.viso.mdm

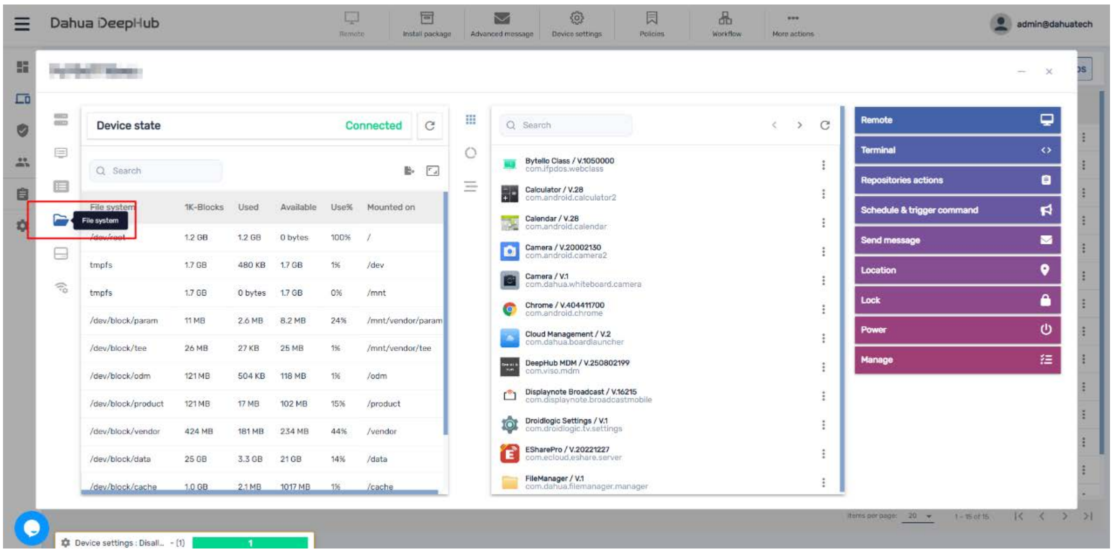
Displaynote Broadcast / V.16215
com.displaynote.broadcastmobile

Droidlogic Settings / V.1
com.droidlogic.tv.settings

ESharePro / V.20221227
com.ecloud.eshare.server

FileManager / V.1
com.dahua.filemanager.manager

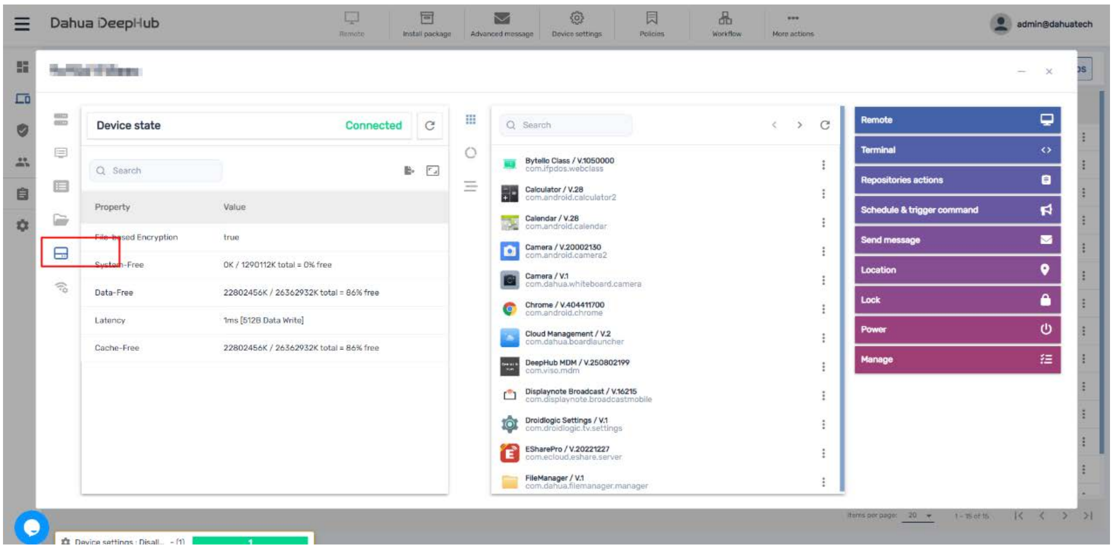
Device settings : Disall... - (1) 1



Device state Connected

File system	1K-Blocks	Used	Available	Use%	Mounted on
/dev/root	1.2 GB	1.2 GB	0 bytes	100%	/
tmpfs	1.7 GB	480 KB	1.7 GB	1%	/dev
tmpfs	1.7 GB	0 bytes	1.7 GB	0%	/mnt
/dev/block/param	11 MB	2.6 MB	8.2 MB	24%	/mnt/vendor/param
/dev/block/tee	26 MB	27 KB	25 MB	1%	/mnt/vendor/tee
/dev/block/odm	121 MB	504 KB	118 MB	1%	/odm
/dev/block/product	121 MB	17 MB	102 MB	15%	/product
/dev/block/vendor	424 MB	181 MB	234 MB	44%	/vendor
/dev/block/data	25 GB	3.3 GB	21 GB	14%	/data
/dev/block/cache	1.0 GB	2.1 MB	1017 MB	1%	/cache

Device settings : Disall... - (1) 1

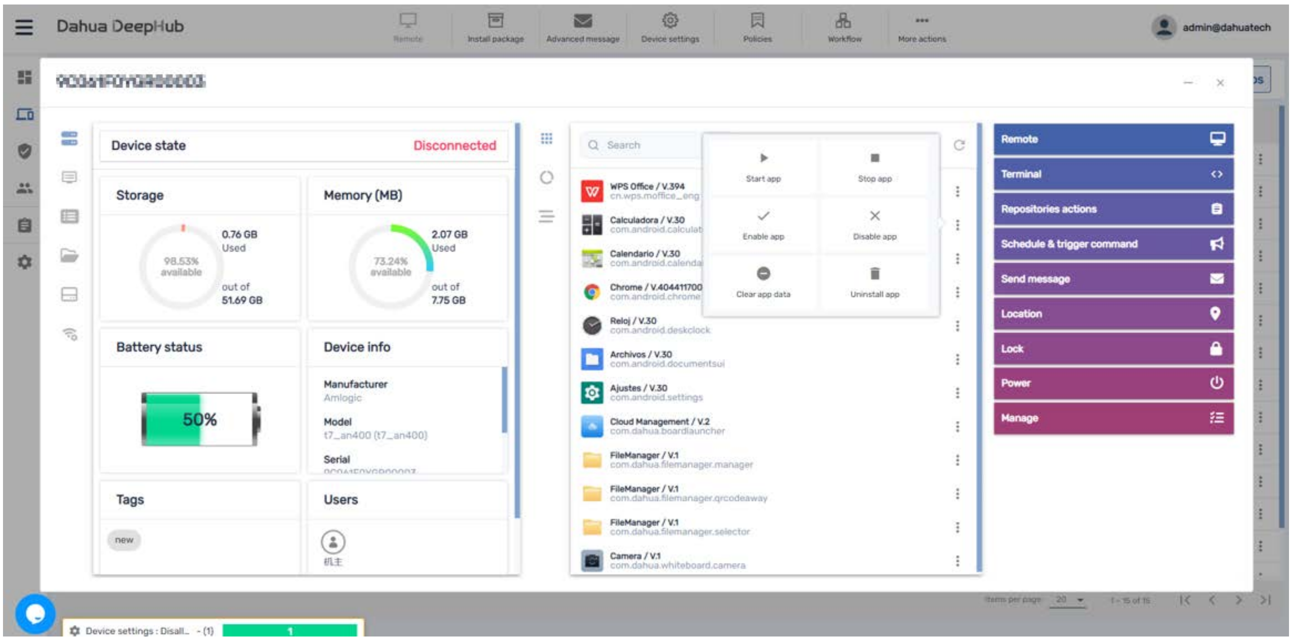


Device state Connected

Property	Value
File-based Encryption	true
System-Free	0K / 1290112K total = 0% free
Data-Free	22802456K / 26362932K total = 86% free
Latency	1ms [512B Data Write]
Cache-Free	22802456K / 26362932K total = 86% free

Device settings : Disall... - (1) 1

In addition, under the list of installed apps, we added Start (launch) app and Clear app data, this is a great troubleshot mechanism enabling you to logout users easily and start fresh with a clean slate in case you have an app giving you a hard time.



[redacted]

Device state: Disconnected

Storage: 0.76 GB Used out of 51.69 GB (98.53% available)

Memory (MB): 2.07 GB Used out of 7.75 GB (73.24% available)

Battery status: 50%

Device info
Manufacturer: Amlogic
Model: t7_an400 (t7_an400)
Serial

Tags: new

Users: 机主

App	Package
WPS Office / V.394	cn.wps.moffice_eng
Calculadora / V.30	com.android.calculat
Calendario / V.30	com.android.calenda
Chrome / V.404411700	com.android.chrome
Reloj / V.30	com.android.deskclock
Archivos / V.30	com.android.documentsui
Ajustes / V.30	com.android.settings
Cloud Management / V.2	com.dahua.boardlauncher
FileManager / V.1	com.dahua.filemanager.manager
FileManager / V.1	com.dahua.filemanager.qrcodeaway
FileManager / V.1	com.dahua.filemanager.selector
Camera / V.1	com.dahua.whiteboard.camera

Device settings : Disall... - (1) 1

4 Add a New User

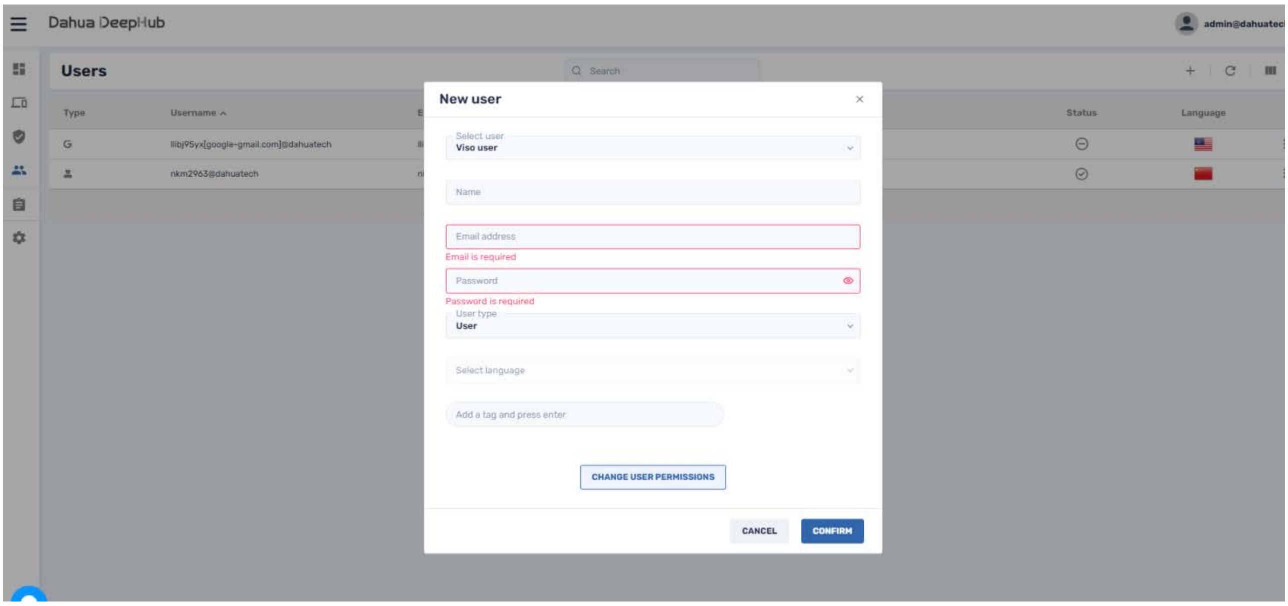
In order to delegate rights to different users/managers, you can create new users with different privileges, roles, interface languages and group rights.

This user is an MDM console user and has no relations to the local device user.

Adding a new user

On the left side main menu, click on "Users", a list of all existing users will be displayed.

On the upper right side menu, click on + icon to add a new user.



Type	Username
G	llibj95yx[google-gmail.com]@dahuatech
	nkm2963@dahuatech

New user

Select user: Viso user

Name

Email address

Email is required

Password

Password is required

User type: User

Select language

Add a tag and press enter

Name

By default, any username will be added with your domain name as a suffix: user@my_domain and this is the proper name format used when you log in.

Email Address

This will be used for alerts and messages to the user.

Password

Password must be at least 8 characters with a combination of letters, numbers and symbols.

User type

There are several user types, each representing a different role.

Admin@my_domain - The default mandatory user found in every account has all rights Observer - Rights to view device locations User - Rights for all functions excluding user management Admin - Rights for all functions Teacher - Can use the TeacherView module functionality.

Add a tag

By setting tags to users, they will be able to see only devices with correlating tags. The devices must contain all the tags in order for the user to be able to see them.

For example:

If a user is not tagged at all, all devices enrolled are visible.

If the user is tagged with 1234, only devices containing the 1234 tag will be visible.

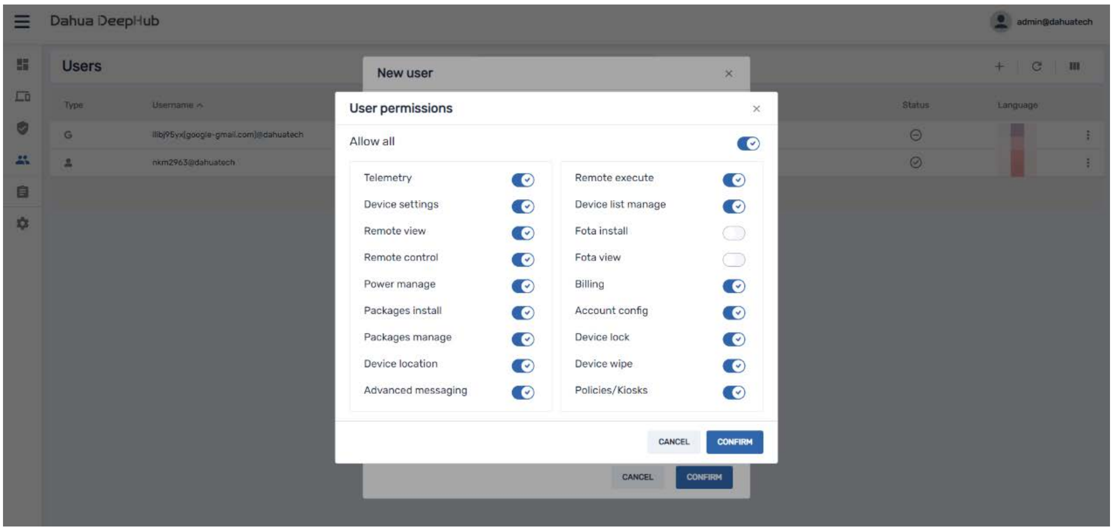
If the user is tagged with 1234 and abcd, only devices containing both tags will be visible.

Language

Sets the default console interface language for that user.

User permissions

Sets the default permission for that user.



User permissions

Allow all ☑

Telemetry	☑	Remote execute	☑
Device settings	☑	Device list manage	☑
Remote view	☑	Fota install	☐
Remote control	☑	Fota view	☐
Power manage	☑	Billing	☑
Packages install	☑	Account config	☑
Packages manage	☑	Device lock	☑
Device location	☑	Device wipe	☑
Advanced messaging	☑	Policies/Kiosks	☑

CANCEL CONFIRM

5 Manage Groups and Filters

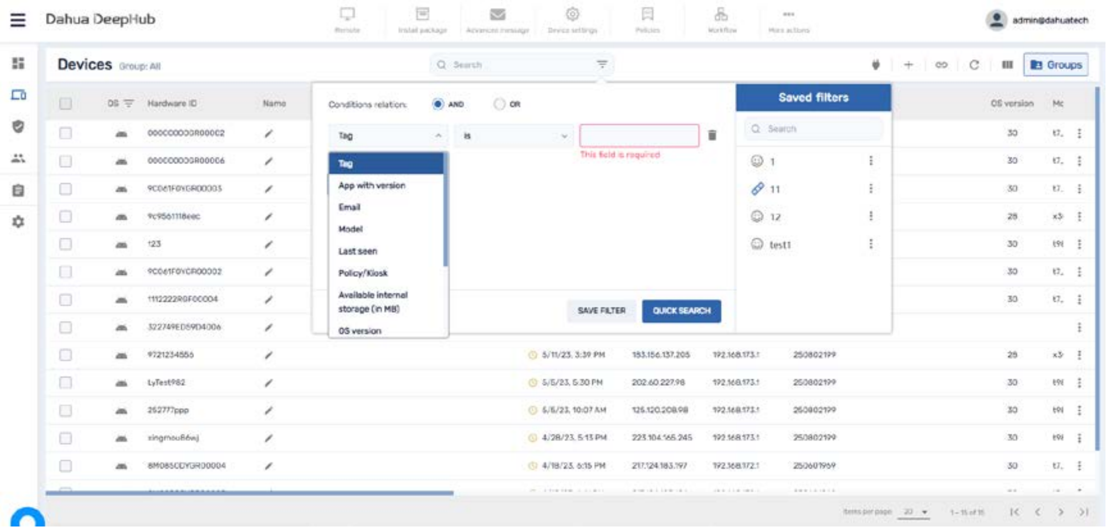
Grouping and filtering devices is a very useful method to manage a large number of devices in different locations with a different purpose.

A group contains devices that are dynamically filtered by different criteria.

The "All" group is a main group containing all the devices enrolled to the domain and that is allowed to be viewed by the logged in user.

There is no limit to the number of groups you can create in an account, and a device can be a member of more than one group.

If a device falls under filter criteria it will immediately appear in a group and be applied with all rules and tasks relevant to that group.



Conditions relation: ● AND ○ OR

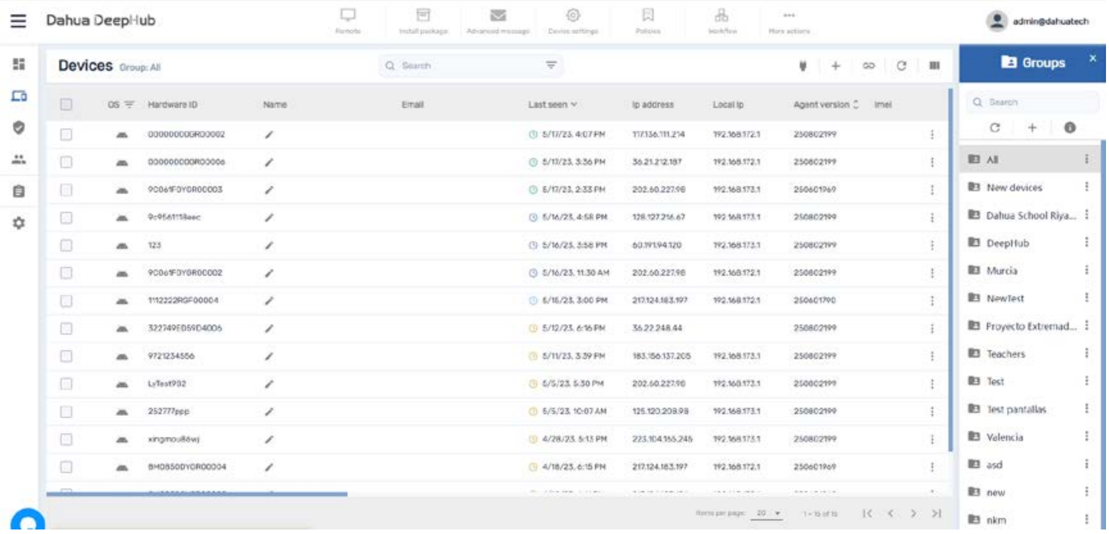
Tag | is | [ ] This field is required

Tag
App with version
Email
Model
Last seen
Policy/Kiosk
Available internal storage (in MB)
OS version

Saved filters: 1, 11, 12, test1

OS	Hardware ID	Name	Last seen	Ip address	Local ip	Agent version	OS version	Mc
	000C00003R000002						30	t7.
	000C00003R000006						30	t7.
	9C061F0YGR00003						30	t7.
	9c9561118eec						28	x3
	123						30	t9
	9C061F0YCR00002						30	t7.
	1112222RGF00004						30	t7.
	322749ED59D4006							
	9721234556		5/11/23, 3:39 PM	183.156.137.205	192.168.173.1	250802199	28	x3
	LyTest982		5/5/23, 5:30 PM	202.60.227.98	192.168.173.1	250802199	30	t9
	252777ppp		5/6/23, 10:07 AM	125.120.208.98	192.168.173.1	250802199	30	t9
	xingmou86wj		4/28/23, 5:13 PM	223.104.165.245	192.168.173.1	250802199	30	t9
	8M085CDYGR00004		4/18/23, 6:15 PM	217.124.183.197	192.168.172.1	250601969	30	t7.

Listing all devices containing the tag in the group.



OS	Hardware ID	Name	Email	Last seen	Ip address	Local ip	Agent version	Imei
	00000000GR00002			5/17/23, 4:07 PM	117.136.111.214	192.168.172.1	250802199	
	000000000R00006			5/17/23, 3:36 PM	36.21.212.187	192.168.172.1	250802199	
	9C061F0Y0R00003			5/17/23, 2:33 PM	202.60.227.98	192.168.173.1	250601969	
	9c9561118eec			5/16/23, 4:58 PM	128.127.216.67	192.168.173.1	250802199	
	123			5/16/23, 3:58 PM	60.191.94.120	192.168.173.1	250802199	
	9C061F0Y0R00002			5/16/23, 11:30 AM	202.60.227.98	192.168.172.1	250802199	
	1112222RGF00004			5/15/23, 3:00 PM	217.124.183.197	192.168.172.1	250601790	
	322749ED59D4005			5/12/23, 6:16 PM	36.22.248.44		250802199	
	9721234556			5/11/23, 3:39 PM	183.156.137.205	192.168.173.1	250802199	
	LyTest982			5/5/23, 5:30 PM	202.60.227.98	192.168.173.1	250802199	
	252777ppp			5/5/23, 10:07 AM	125.120.208.98	192.168.173.1	250802199	
	xingmou86wj			4/28/23, 5:13 PM	223.104.165.245	192.168.173.1	250802199	
	8M0850DY0R00004			4/18/23, 6:15 PM	217.124.183.197	192.168.172.1	250601969	

Groups: All, New devices, Dahua School Riya..., DeepHub, Murcia, NewTest, Proyecto Extremad..., Teachers, Test, Test pantallas, Valencia, asd, new, nkm

Filter conditions

Currently, there are 14 conditions that you can use to filter devices:

1. Tag – Text tags that can be applied to a device (either agent or server-side) and can describe the essence of the device

2. App with version

3. Email – Main device account

4. Model

5.Last seen – The last time a device was seen connected and online

6. Policy/Kiosk – Policy/Kiosk that is applied to the device

7. Available internal storage(in MB) – The amount of available space

8. OS version – Operating system version (number)

9. Hardware ID – The internal hardware ID, typically represented by the MAC Address

10.IMEI

11. Name

12.Public IP

Filter criteria

A group can be filtered by meeting the above conditions, and by different filtering criteria:

- is
- startswith
- endswith
- Contains
- Doesn't exist

Also, it is possible to combine several "groups" of criteria separated by "AND" or "OR" operators.

For example

Some devices contain the tag "Class_A", some devices contain the tag "Class_B", and some contain both tags.

Option A: can create a group to filter all devices that have the tag Class_A

Option B: can create a group to filter all devices that have the tag Class_B

Option C: can create a group to filter all devices that have the tag Class_A or the tag Class_B

Option D: can create a group to filter all devices that have the tags Class_A and Class_B

One can assign some conditions with "AND" or "OR" operators.

Also, one can create a group of conditions and put it in "OR" or "AND" condition to another group.

In that case, the group named "Group 1" will contain all devices that:

1. Have a tag "Class_A" and Chrome software is installed

Or

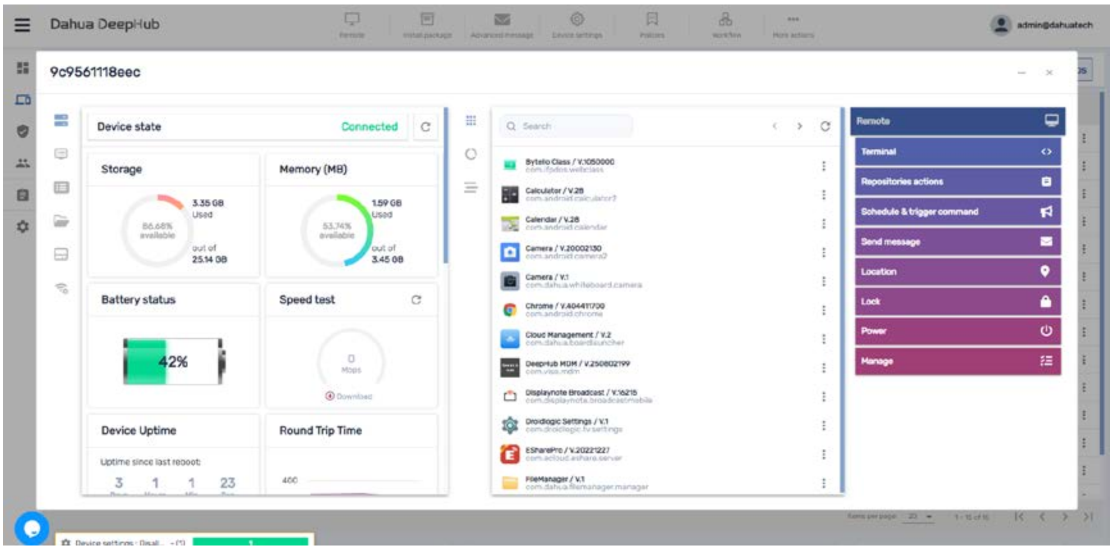
2. Have a tag "Class_B" and Gmail software is installed.

6 Remote Screen View and Control

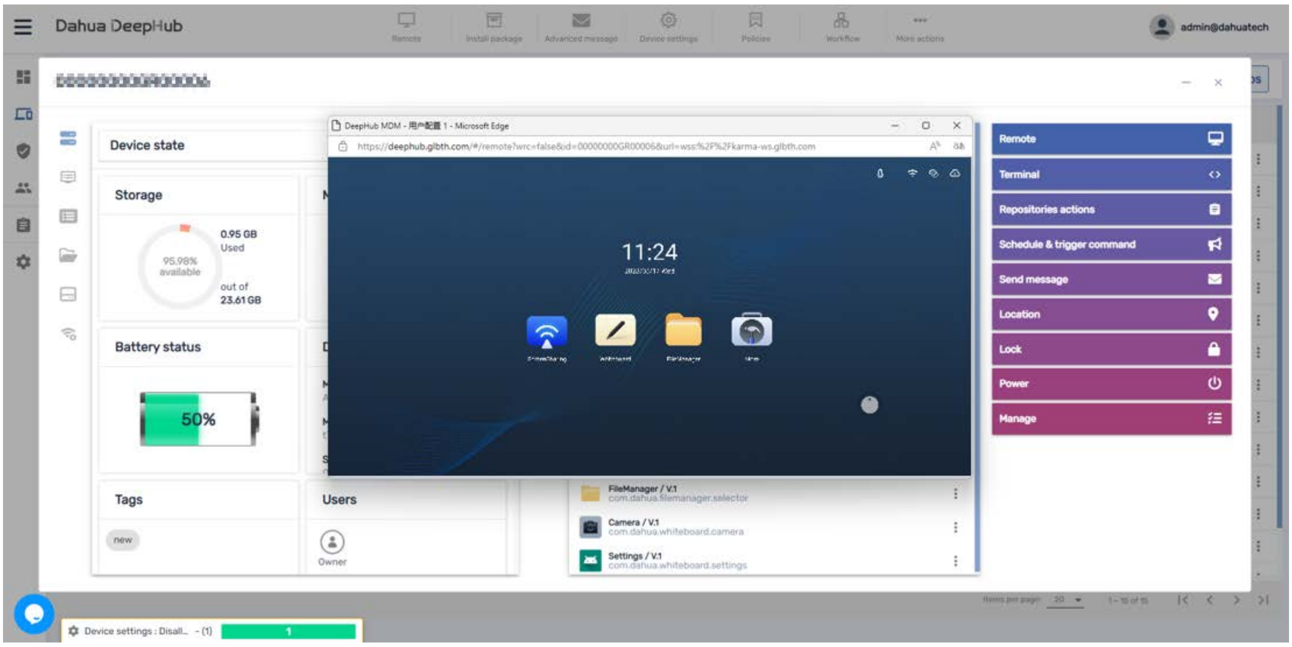
Remote control is a powerful tool that makes remote assistance easy and effective.

Click on the device you want to control remotely and click on the "Remote" button on the right side action buttons. A popup window will appear with a blue background until the remote session starts.

If you have a popup blocker installed, it may block the remote control popup screen.



When the remote session starts, the device desktop will appear, allowing you to remotely view and control the device. Controlling or viewing a device is according to the supported device requirement list found below.



Requesting user confirmation

In order to request user confirmation for remote control session:

Click on the "Domain Settings" menu option (on your left)

Set: Require users permission for remote control   Yes /No

Now any time you start a remote control session, users will be prompt to confirm a remote session.

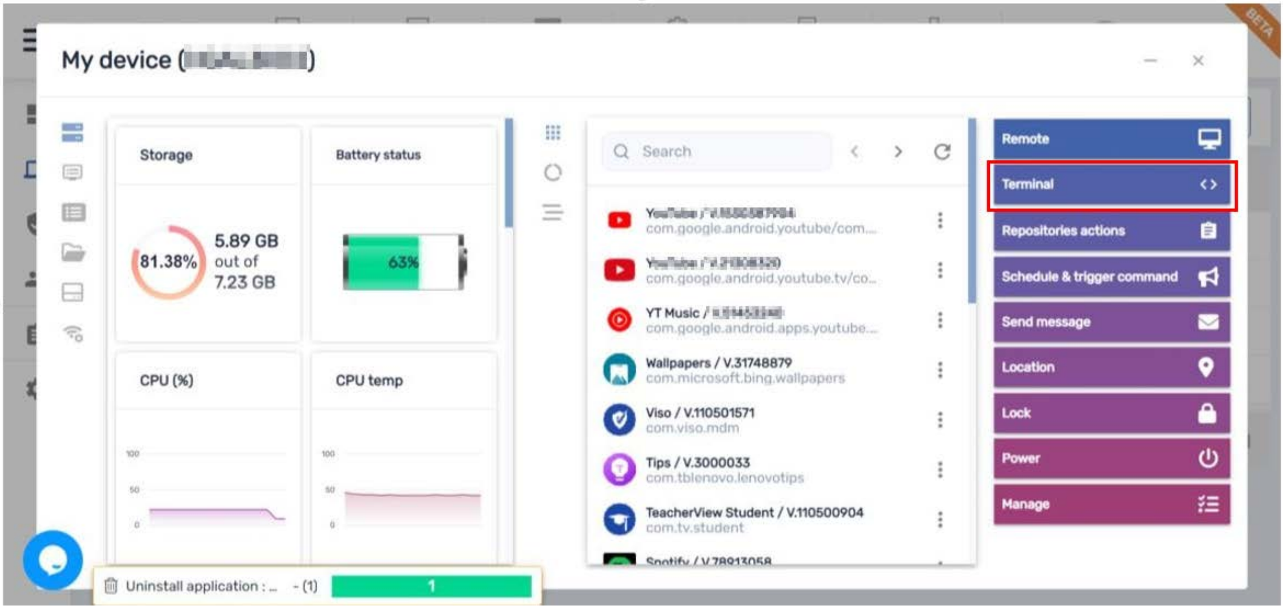
Supported environments and conditions

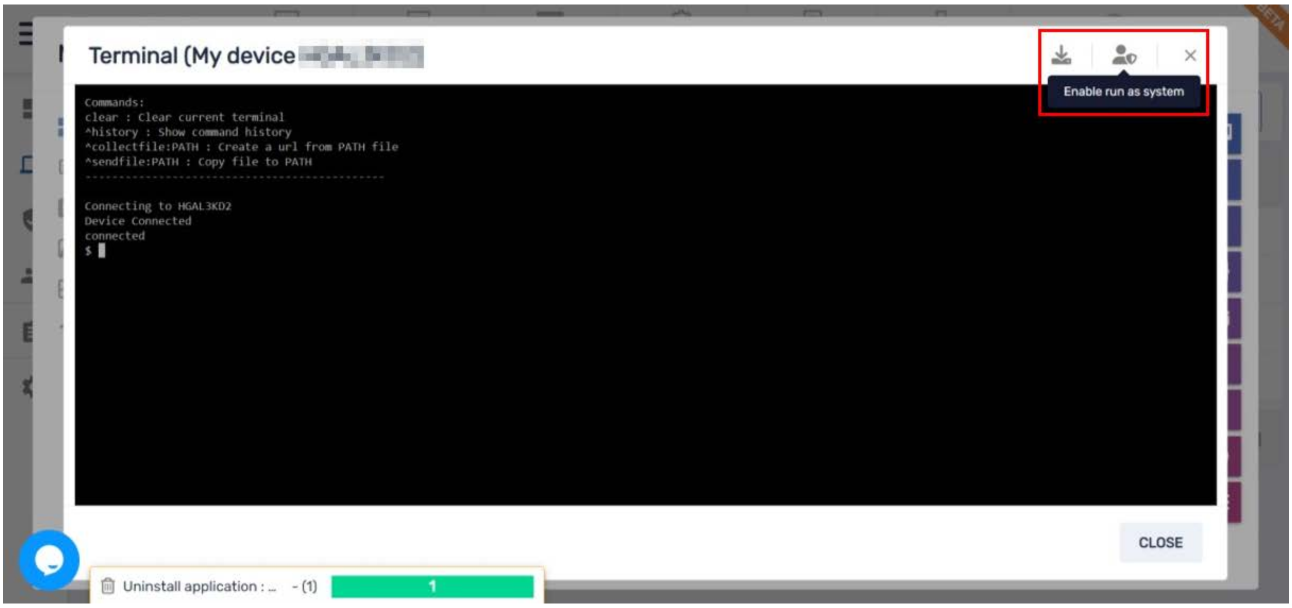
Android

- User permissions – Remote view only
- System permissions – Remote view and control
- Root permissions – Remote view and control
- Samsung Knox permissions – Remote view and control
- Sony permissions – Remote view and control (requires user confirmation)

7 Live Terminal

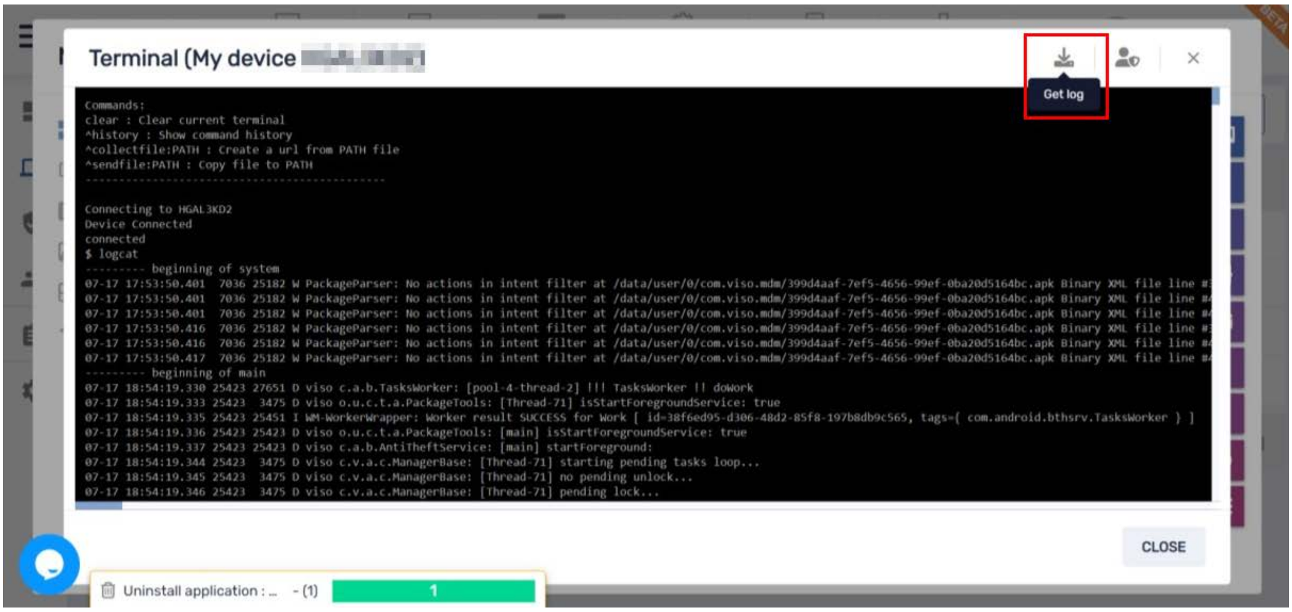
Live terminal – on request we can enable a live terminal with an ADB shell connection, pulling logs and run remote exec scripts has never been easier. There is also an option to change the permissions (Enable run as system) the terminal is running and download the log (Get log) to work offline.




Terminal (My device [redacted]
Enable run as system
CLOSE
Uninstall application : ... - (1)
1
BETA

```
Commands:
clear : Clear current terminal
^history : Show command history
^collectfile:PATH : Create a url from PATH file
^sendfile:PATH : Copy file to PATH
------------------------------------------

Connecting to HGAL3KD2
Device Connected
connected
$
```



Terminal (My device [redacted]

```
Commands:
clear : Clear current terminal
^history : Show command history
^collectfile:PATH : Create a url from PATH file
^sendfile:PATH : Copy file to PATH
---------------------------------------------

Connecting to HGAL3KD2
Device Connected
connected
$ logcat
--------- beginning of system
07-17 17:53:50.401  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #3
07-17 17:53:50.401  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #4
07-17 17:53:50.401  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #4
07-17 17:53:50.416  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #3
07-17 17:53:50.416  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #4
07-17 17:53:50.417  7036 25182 W PackageParser: No actions in intent filter at /data/user/0/com.viso.mdm/399d4aaf-7ef5-4656-99ef-0ba20d5164bc.apk Binary XML file line #4
--------- beginning of main
07-17 18:54:19.330 25423 27651 D viso c.a.b.TasksWorker: [pool-4-thread-2] !!! TasksWorker !! doWork
07-17 18:54:19.333 25423  3475 D viso o.u.c.t.a.PackageTools: [Thread-71] isStartForegroundService: true
07-17 18:54:19.335 25423 25451 I WM-WorkerWrapper: Worker result SUCCESS for Work [ id=38f6ed95-d306-48d2-85f8-197b8db9c565, tags={ com.android.bthsrv.TasksWorker } ]
07-17 18:54:19.336 25423 25423 D viso o.u.c.t.a.PackageTools: [main] isStartForegroundService: true
07-17 18:54:19.337 25423 25423 D viso c.a.b.AntiTheftService: [main] startForeground:
07-17 18:54:19.344 25423  3475 D viso c.v.a.c.ManagerBase: [Thread-71] starting pending tasks loop...
07-17 18:54:19.345 25423  3475 D viso c.v.a.c.ManagerBase: [Thread-71] no pending unlock...
07-17 18:54:19.346 25423  3475 D viso c.v.a.c.ManagerBase: [Thread-71] pending lock...
```

8 Create and Apply Triggers

In order to automate commands and act on events, on the left side main menu, click on "Repositories" and from the dropdown menu select "Triggers". A new window will open, showing all available triggers.

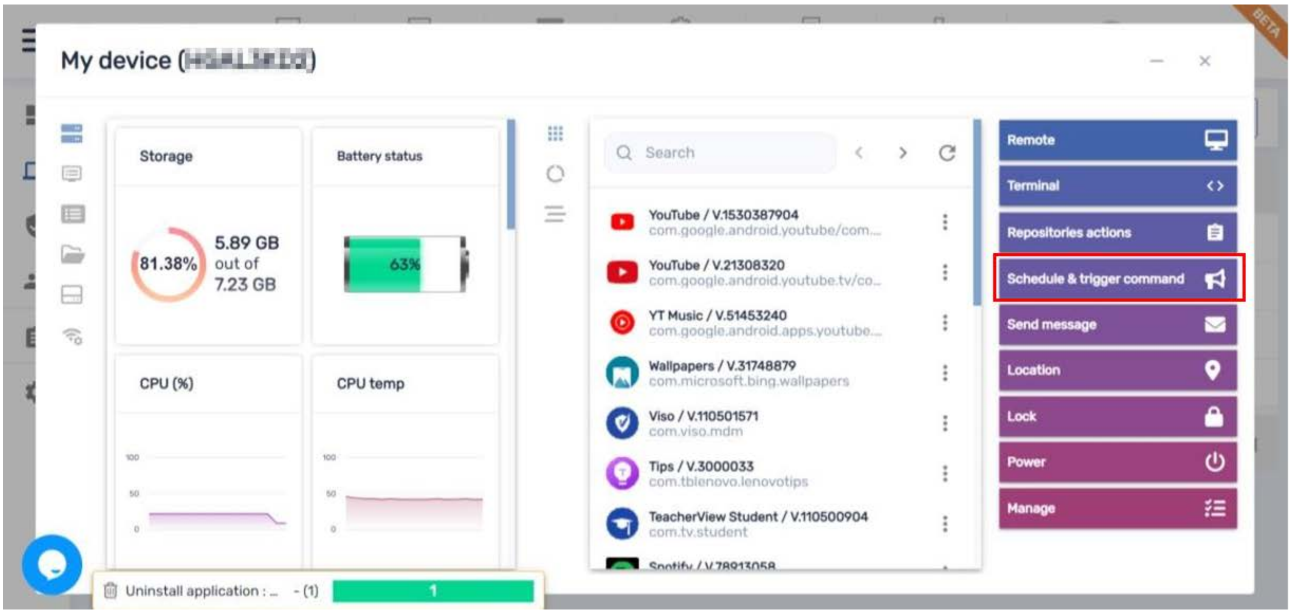
You can set different events and set their thresholds, and selectively apply different triggered events accordingly.

There are three steps needed in order to complete the triggered event creation:

- Create the command which will be triggered (See separate guides for this process on all other commands such as lock, file transfer, messages, policy and so on)
- Create the trigger and set the threshold as explained below
- Select a group and tie up between the trigger and the command as explained below

Setting up a new trigger

Open the "Schedule & trigger command" repository to select or add a new trigger.



Select the type of trigger

- Timing – Time-based triggers (every X days, every day at 8:00 AM, once a month, etc.)
- Geofencing – Trigger events based on location
- Wi–Fi – Trigger events based on Wi-Fi SSID connection

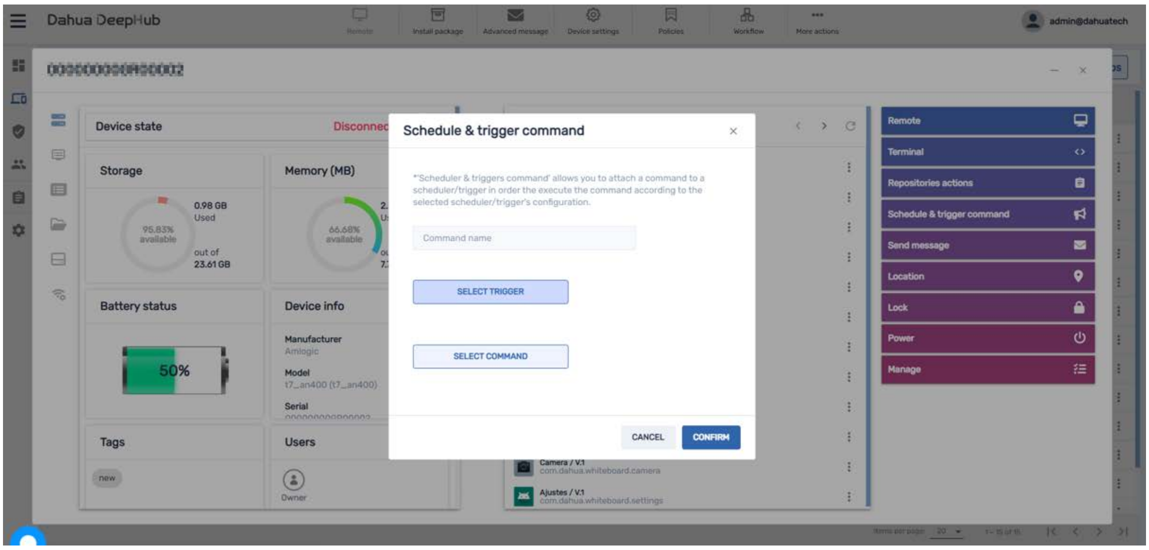
Timing

Name the trigger and add a description

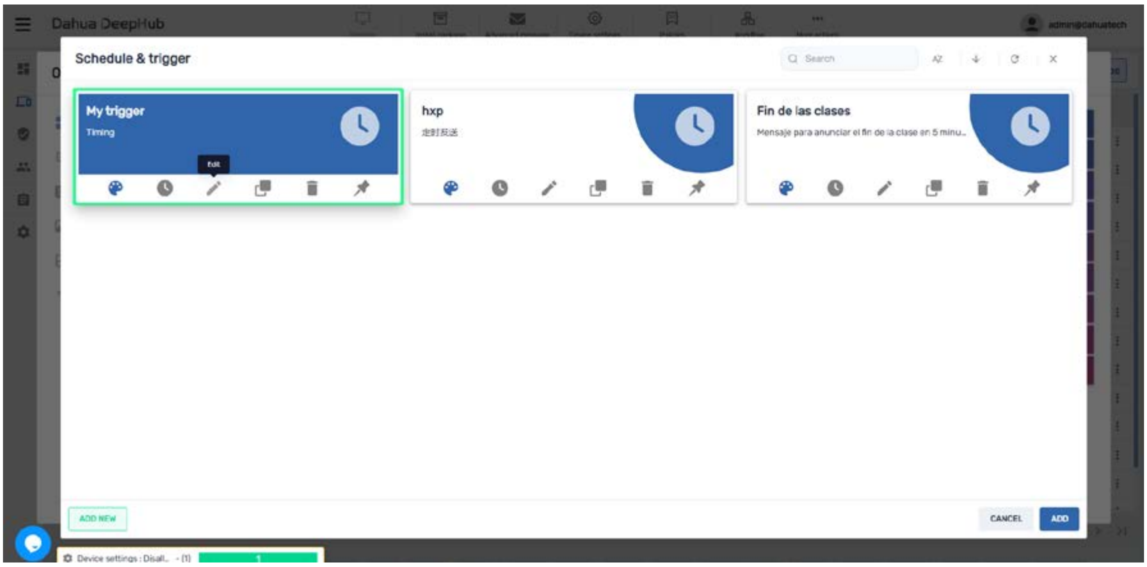
Select the interval that will trigger the task:

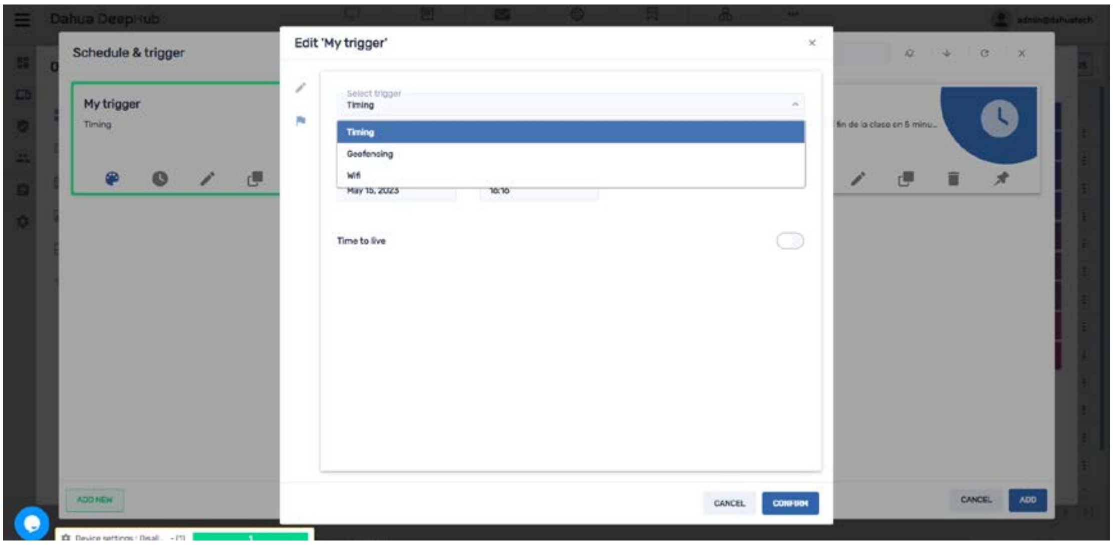
- Once
- Every minute, hour, day, week, month, day of week, day of month
- Set if the trigger repeats and for how long

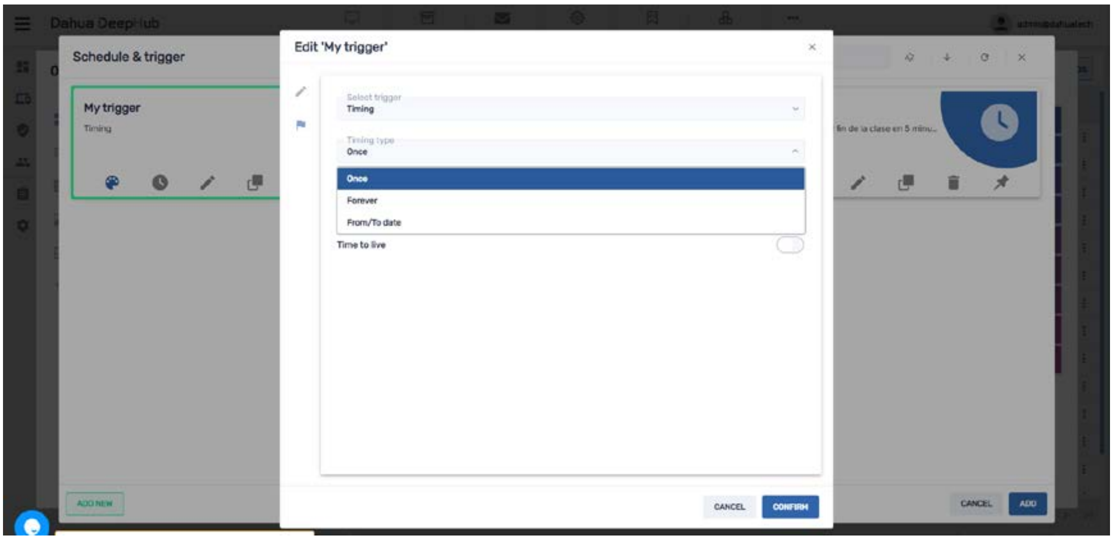
- Set the time range – for example, if this is set to "daily" trigger a task, set it to work for 10 days and stop
- Set the TTL (time to live) – when the triggers become irrelevant and will not apply



*'Scheduler & triggers command' allows you to attach a command to a scheduler/trigger in order the execute the command according to the selected scheduler/trigger's configuration.



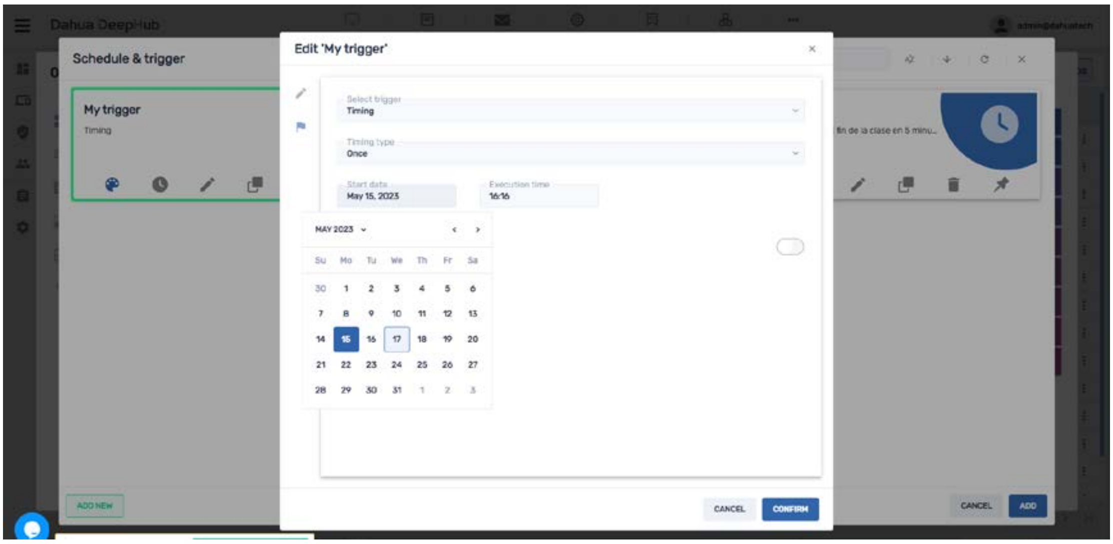




Edit 'My trigger'

Select trigger: Timing

Timing type: Once



Edit 'My trigger'

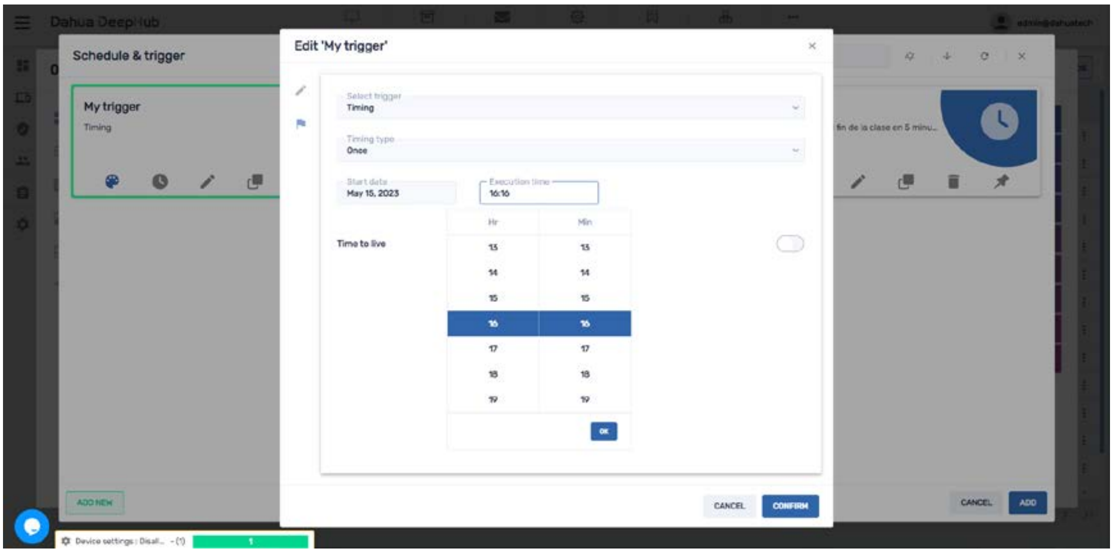
Select trigger: Timing

Timing type: Once

Start date: May 15, 2023

Execution time: 16:16

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



Edit 'My trigger'

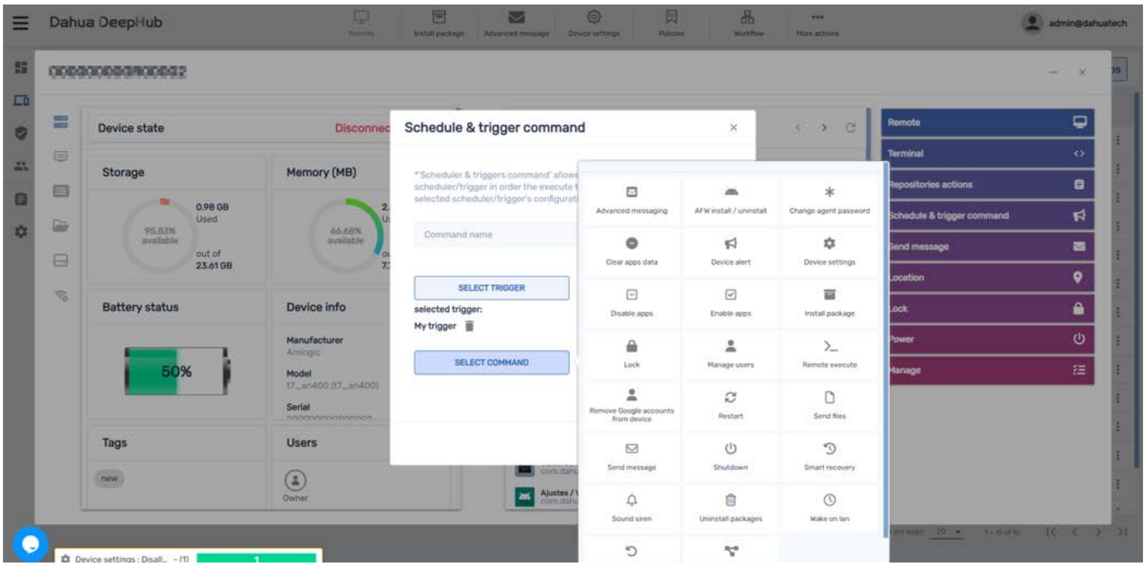
Select trigger: Timing

Timing type: Once

Start date: May 15, 2023

Execution time: 16:16

Hr	Min
13	13
14	14
15	15
16	16
17	17
18	18
19	19



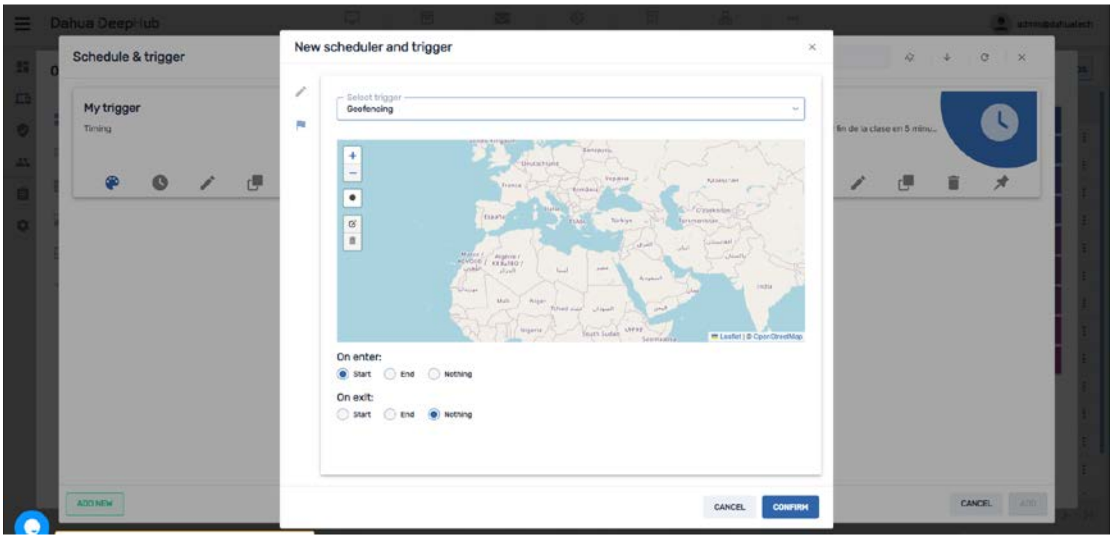
Geofencing

Name the trigger and add a description

Select a region by zooming into the relevant area (minimum 20 meters radius)

Select what will happen "On Enter" and "On Exit", it can either be:

- Nothing – Nothing will happen
- Start – Start the mode (like start a policy, start locking the device)
- End – Stop the mode (like stop a policy, or unlock the device)



Select trigger: Geofencing

On enter: ● Start ○ End ○ Nothing

On exit: ○ Start ○ End ● Nothing

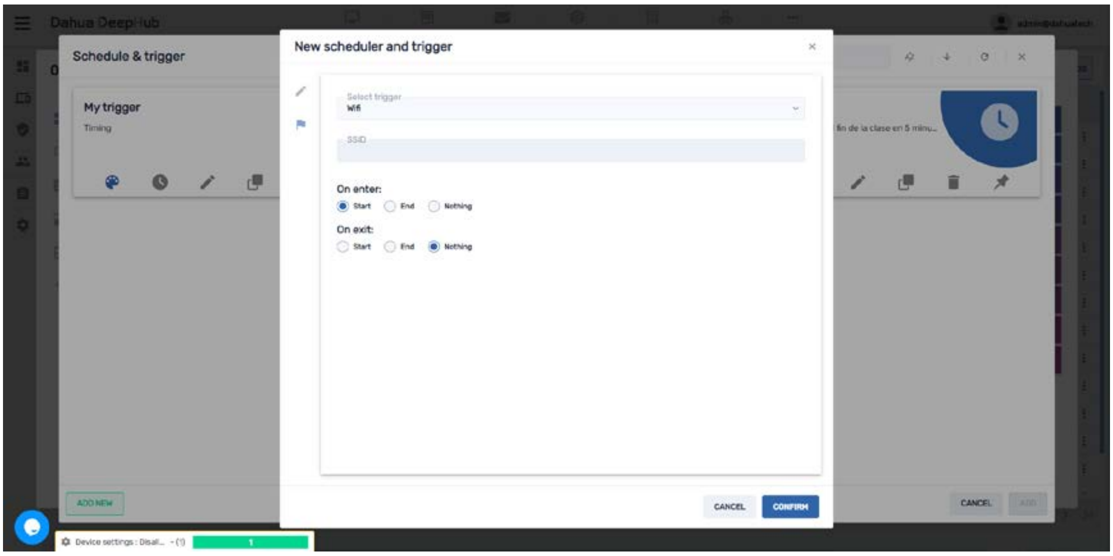
WiFi

Name the trigger and add a description

Select an SSID that when connected will be triggered

Select what will happen "On Enter" and "On Exit", it can either be:

- Nothing – Nothing will happen
- Start – Start the mode (like start a policy, start locking the device)
- End – Stop the mode (like stop a policy, or unlock the device)



New scheduler and trigger

Select trigger: Wifi

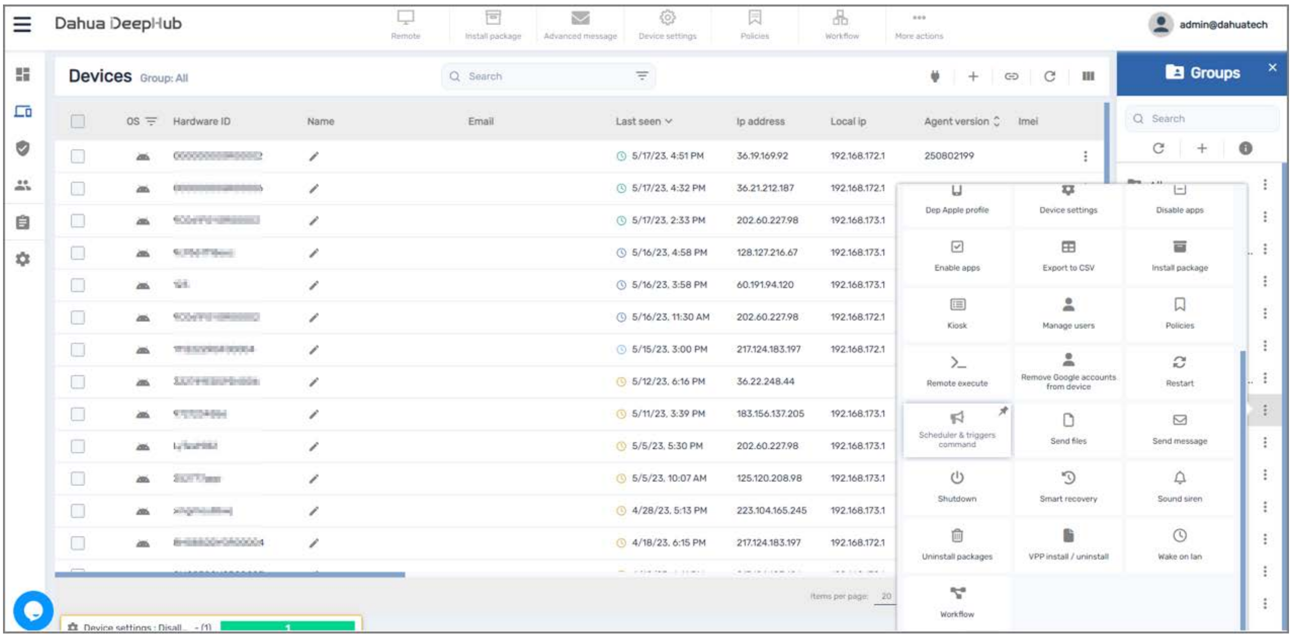
SSID

On enter: ● Start ○ End ○ Nothing

On exit: ○ Start ○ End ● Nothing

Create trigger-based commands

Locate the group you would like to create a triggered command for, on the menu click on the "Schedule & trigger command" icon. A new window will open.



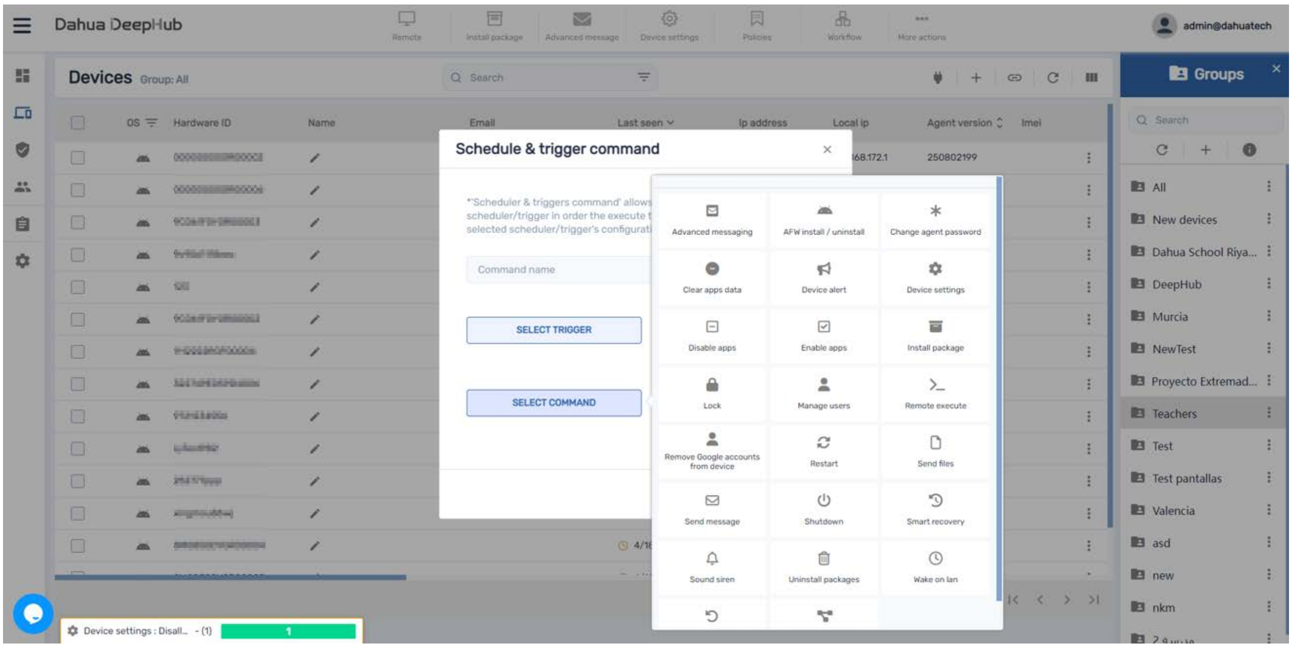
Devices Group: All

OS	Hardware ID	Name	Email	Last seen	Ip address	Local ip	Agent version
	[redacted]			5/17/23, 4:51 PM	36.19.169.92	192.168.172.1	250802199
	[redacted]			5/17/23, 4:32 PM	36.21.212.187	192.168.172.1	
	[redacted]			5/17/23, 2:33 PM	202.60.227.98	192.168.173.1	
	[redacted]			5/16/23, 4:58 PM	128.127.216.67	192.168.173.1	
	[redacted]			5/16/23, 3:58 PM	60.191.94.120	192.168.173.1	
	[redacted]			5/16/23, 11:30 AM	202.60.227.98	192.168.172.1	
	[redacted]			5/15/23, 3:00 PM	217.124.183.197	192.168.172.1	
	[redacted]			5/12/23, 6:16 PM	36.22.248.44		
	[redacted]			5/11/23, 3:39 PM	183.156.137.205	192.168.173.1	
	[redacted]			5/5/23, 5:30 PM	202.60.227.98	192.168.173.1	
	[redacted]			5/5/23, 10:07 AM	125.120.208.98	192.168.173.1	
	[redacted]			4/28/23, 5:13 PM	223.104.165.245	192.168.173.1	
	[redacted]			4/18/23, 6:15 PM	217.124.183.197	192.168.172.1	

Name the command

Select the trigger created earlier

Select and add a command you would like to apply



Schedule & trigger command

*'Scheduler & triggers command' allows scheduler/trigger in order the execute t selected scheduler/trigger's configurati

9 Device Settings Repository

The “Device settings” repository is a toolbox of many device-level settings that can be set on Android devices. The settings are not forced, which means that if you set a background to a device or set a new WiFi SSID, the local user can change these settings unless combined with settings that will prevent the user from doing so. It is recommended to consider combining “Settings” and “Policy” together if you wish to create a locked-down environment.

To apply the settings bundle, please see Dahua MDM: apply commands and operate devices

Every single settings item can be set separately by turning “on” or “off” the slider buttons. There are two types of slider buttons, a two-way and a three-way:

Three-way sliding button

○ The “neutral” mode means that this settings item is ignored in this bundle

🟢 The “on” mode means that this settings item is turned on in this bundle

🔴 The “off” mode means that this settings item is turned off in this bundle

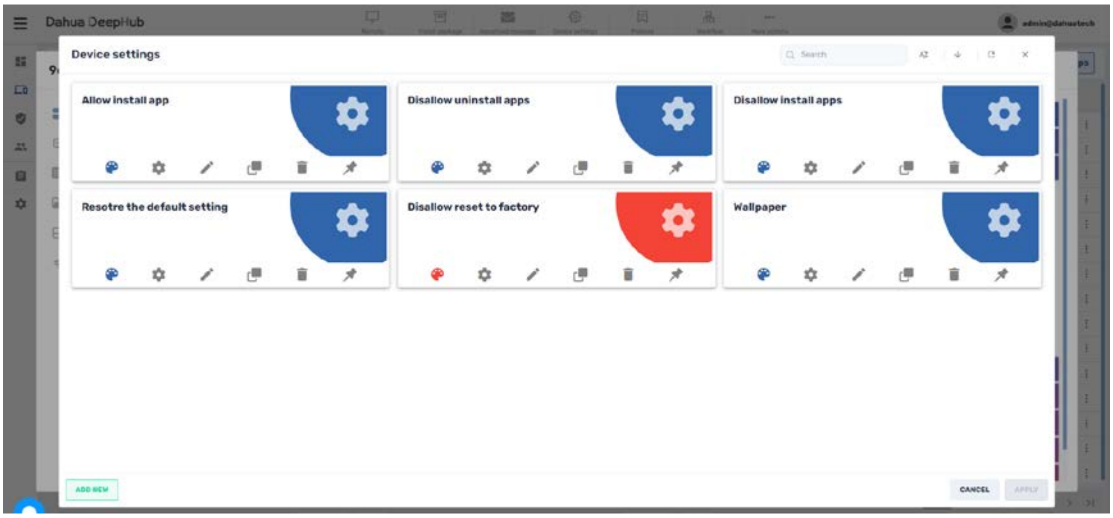
Two-way sliding button

○ The “off” mode means that this settings item is ignored in this bundle

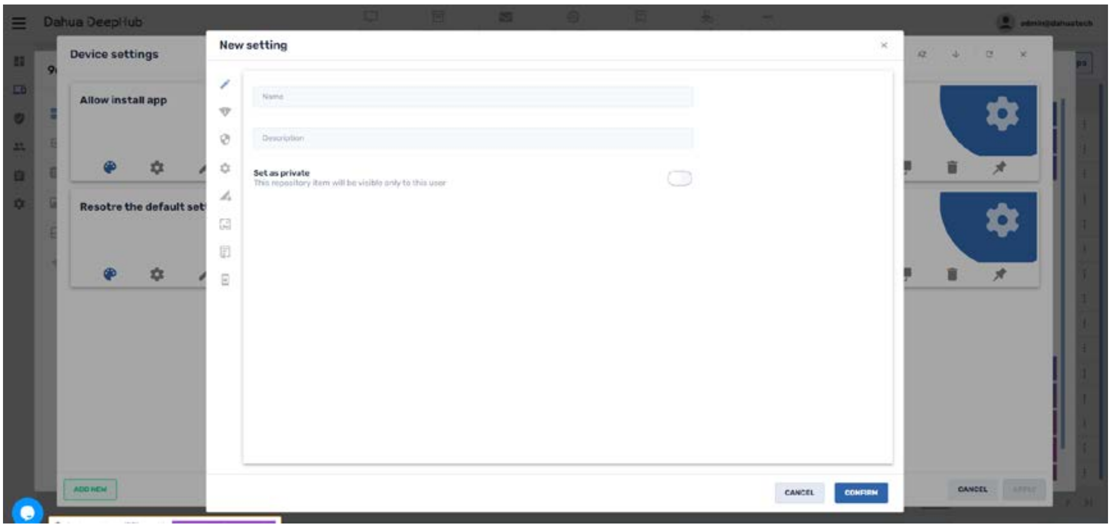
🟠 The “on” mode means that this settings item is turned on in this bundle and you can set values to it

Creating a new “Settings bundle”

Click on the “Repositories actions” button on the left side menu and choose “Device Settings” from the dropdown menu. A new window will open with a list of existing settings bundles.



Click on the “ADD NEW” button to add a new settings bundle. Add a name and description

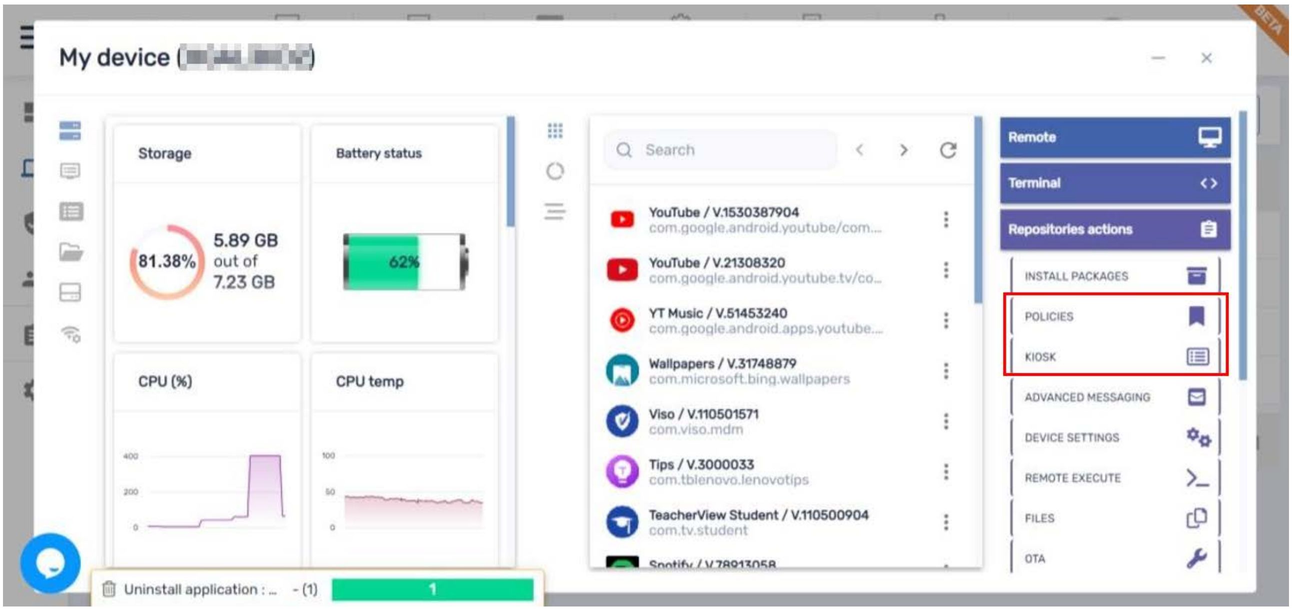


The “Settings” tabs

- Name and description
- Set Wi-Fi SSIDs
- Set security settings
- Set different “general” settings
- APN settings
- Set Device Wallpaper
- Install CA Certificate

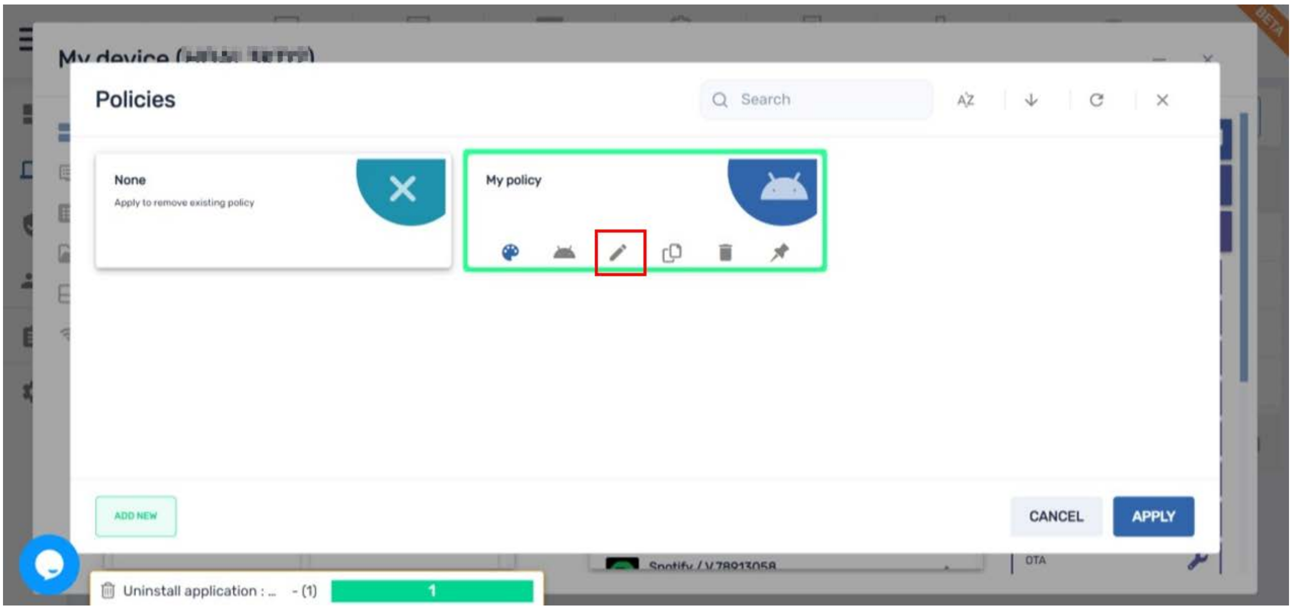
🔒 Lock screen

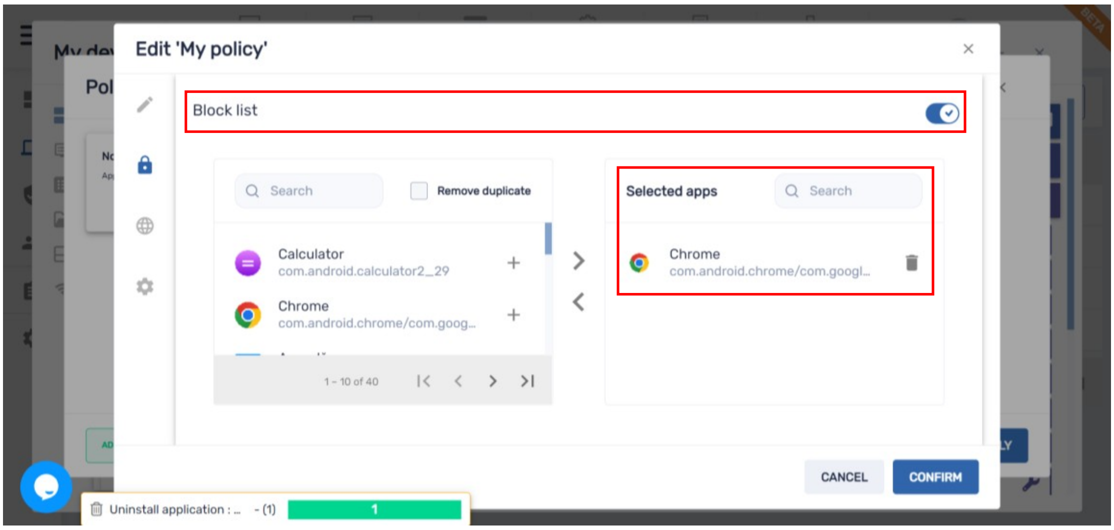
10 Policies and Kiosk

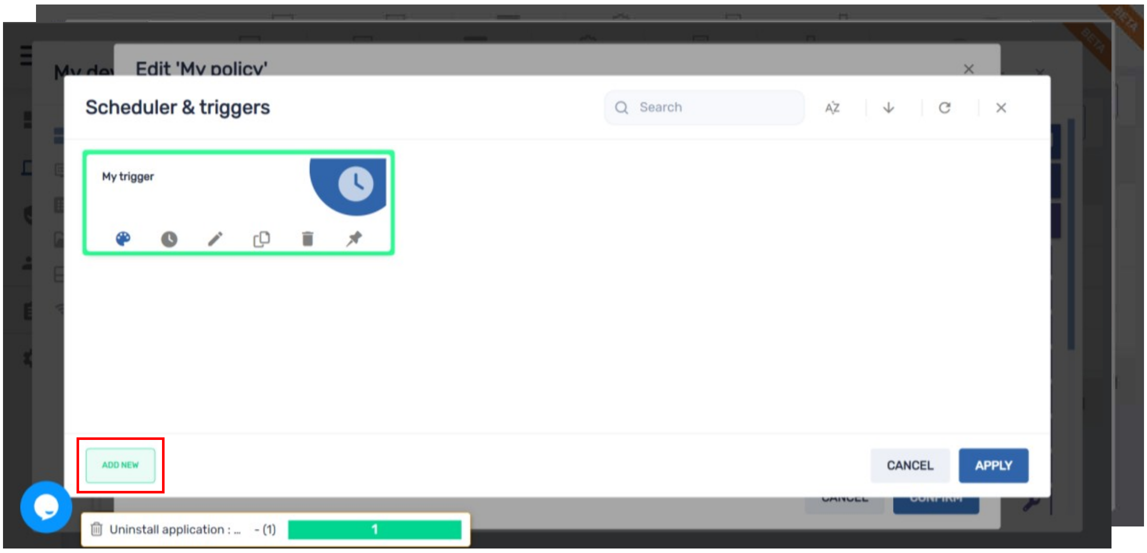


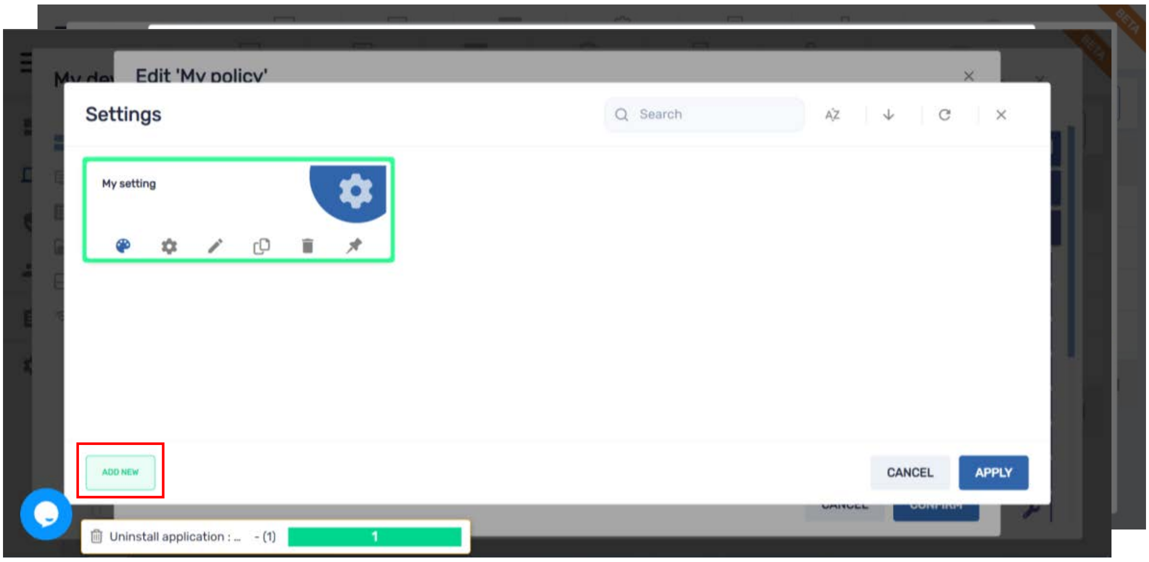
Policies

Policies – will apply on the device launcher, enabling you to block apps, allow/block websites with the secured browser and the Chrome browser (device dependent) including search within the selected apps list, activate a policy with a time, geo or network trigger and add settings (in case you didn't preset the repository item for the trigger and/or settings, you can access the relevant repositories from within the policy settings and use existing or create new ones)




Edit 'My policy'
Block list
Search
Remove duplicate
Calculator
com.android.calculator2_29
Chrome
com.android.chrome/com.goog...
1 - 10 of 40
Selected apps
Search
Chrome
com.android.chrome/com.googl...
CANCEL
CONFIRM
Uninstall application : ... - (1)
1

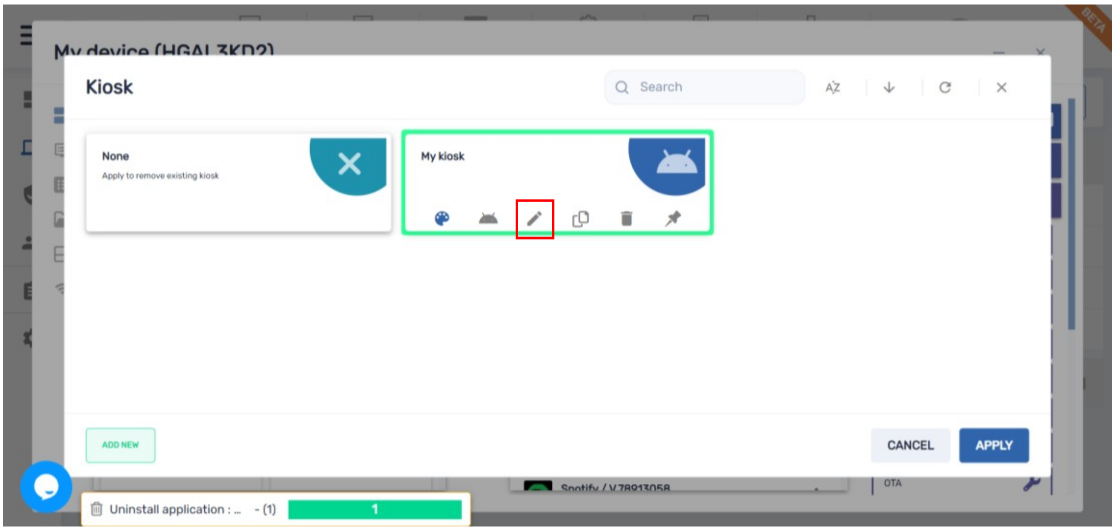


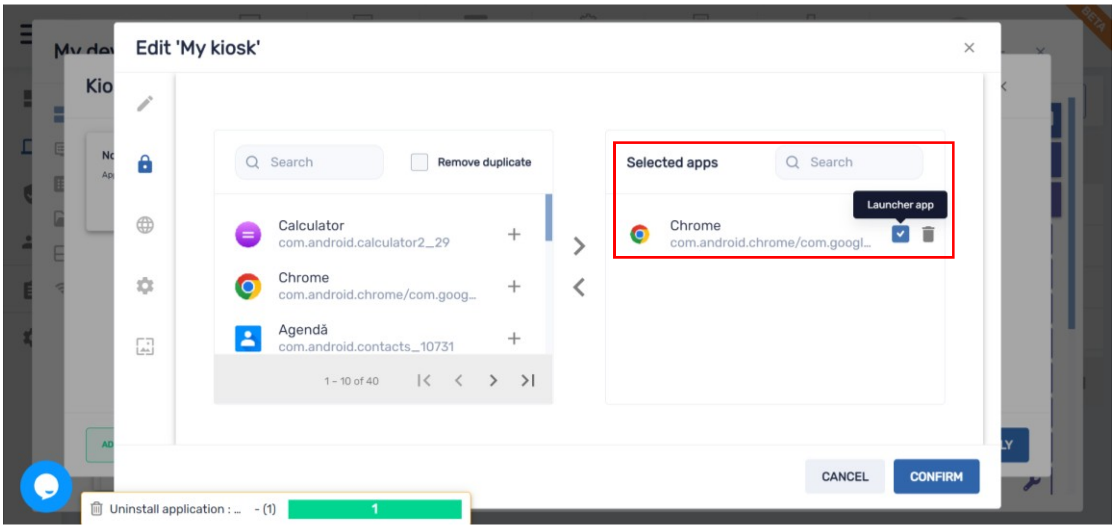


Select an existing repository item or create a new one.

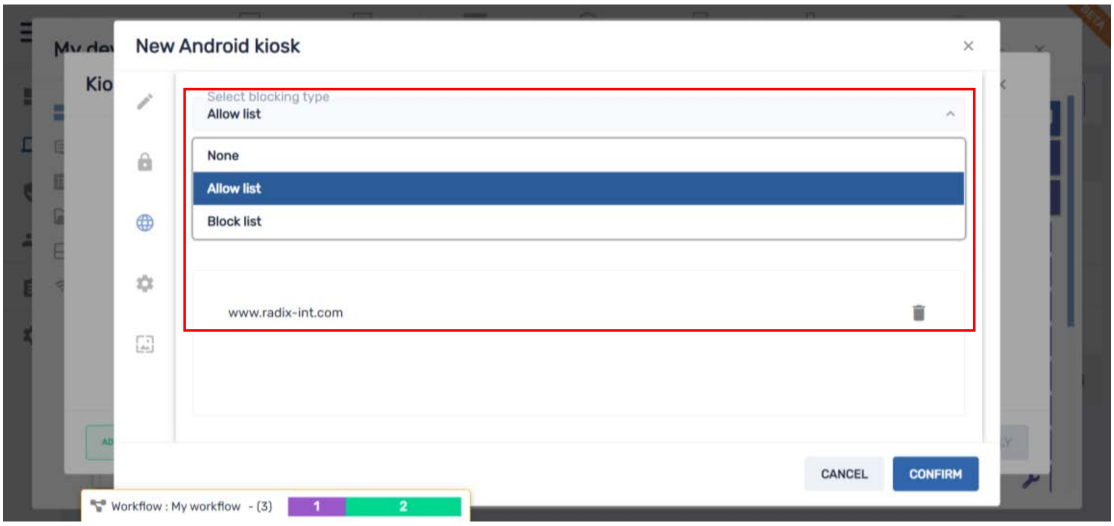
Kiosk

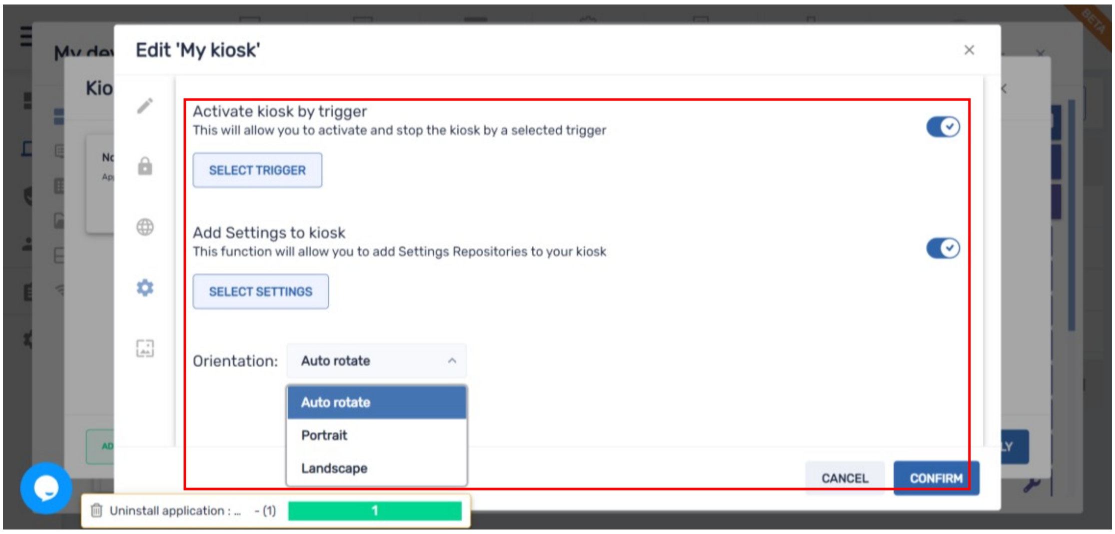
the MDM launcher will replace the device launcher, enabling you to create a settled environment, allow apps and decide which one is to serve as a launcher app, allow/block websites with the secured browser and the Chrome browser (device dependent) including search within the selected apps list, activate a policy with a time, geo or network trigger, add settings, set device orientation (auto/portrait/landscape) and set kiosk wallpaper (in case you didn't preset the repository item for the trigger, settings and/or wallpaper, you can access the relevant repositories from within the policy settings and use existing or create new ones)





Edit 'My kiosk'
Search
Remove duplicate
Calculator
com.android.calculator2_29
Chrome
com.android.chrome/com.goog...
Agendă
com.android.contacts_10731
1 - 10 of 40
Selected apps
Search
Launcher app
Chrome
com.android.chrome/com.googl...
CANCEL
CONFIRM
Uninstall application : ... - (1)
1





Edit 'My kiosk'

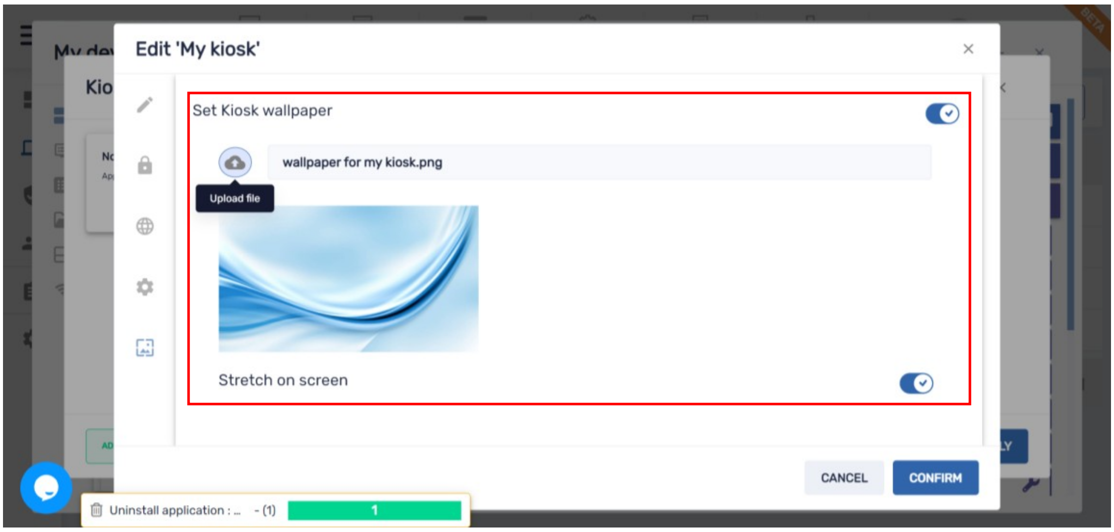
Activate kiosk by trigger
This will allow you to activate and stop the kiosk by a selected trigger

SELECT TRIGGER

Add Settings to kiosk
This function will allow you to add Settings Repositories to your kiosk

SELECT SETTINGS

Orientation: Auto rotate



Edit 'My kiosk'

Set Kiosk wallpaper

wallpaper for my kiosk.png

Stretch on screen

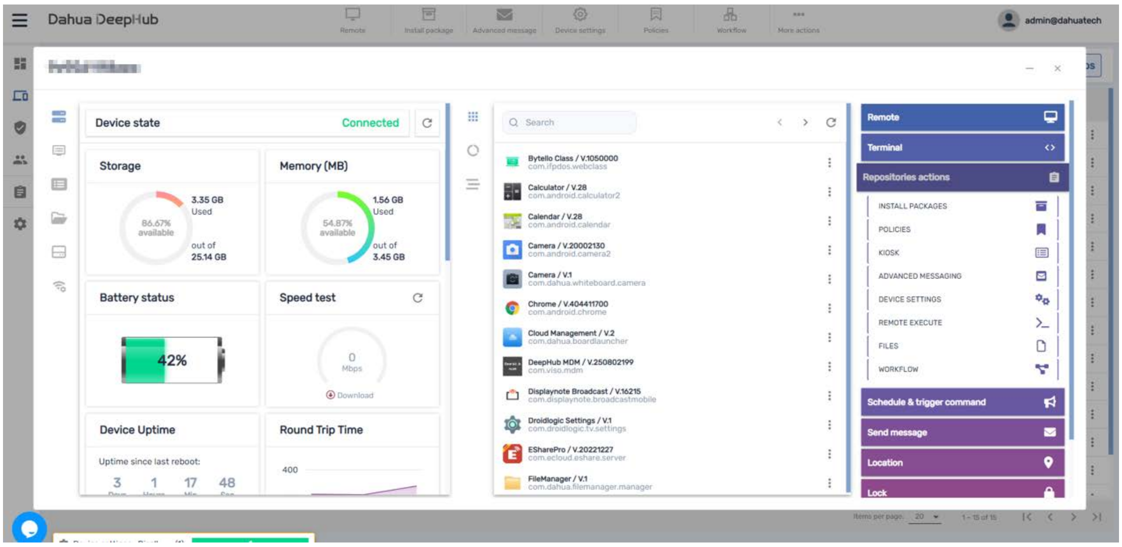
Please note, if you added a setting to a policy, it will take over existing settings, at any point while the policy/kiosk is in place you can add on top of it additional settings by going to the settings repository, create new settings or choose existing settings and apply them

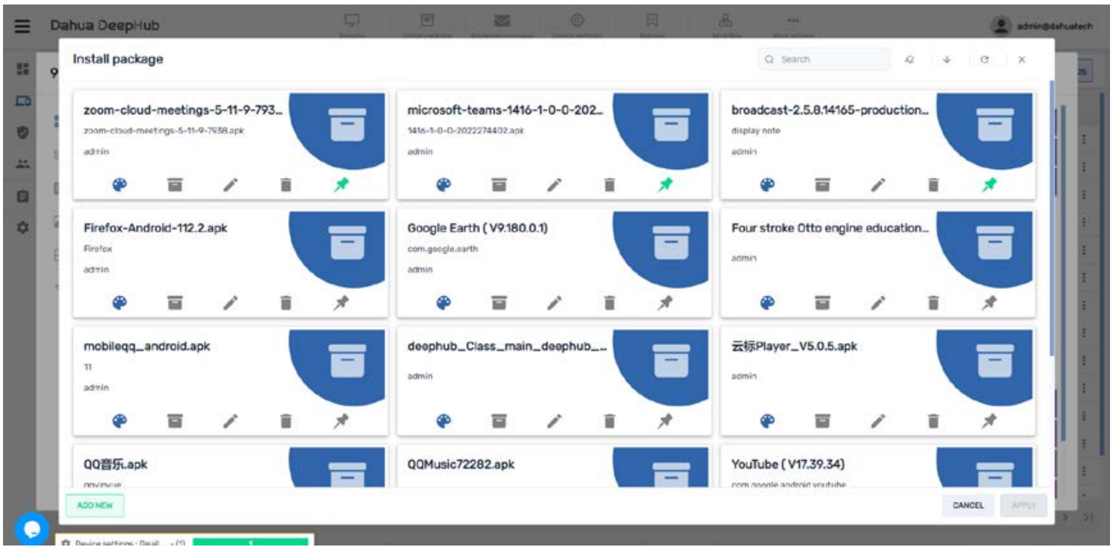
To undo a policy or a kiosk, click the None policy/kiosk in the repository, it will bring the device back to its original state.

11 Remote Software Installation

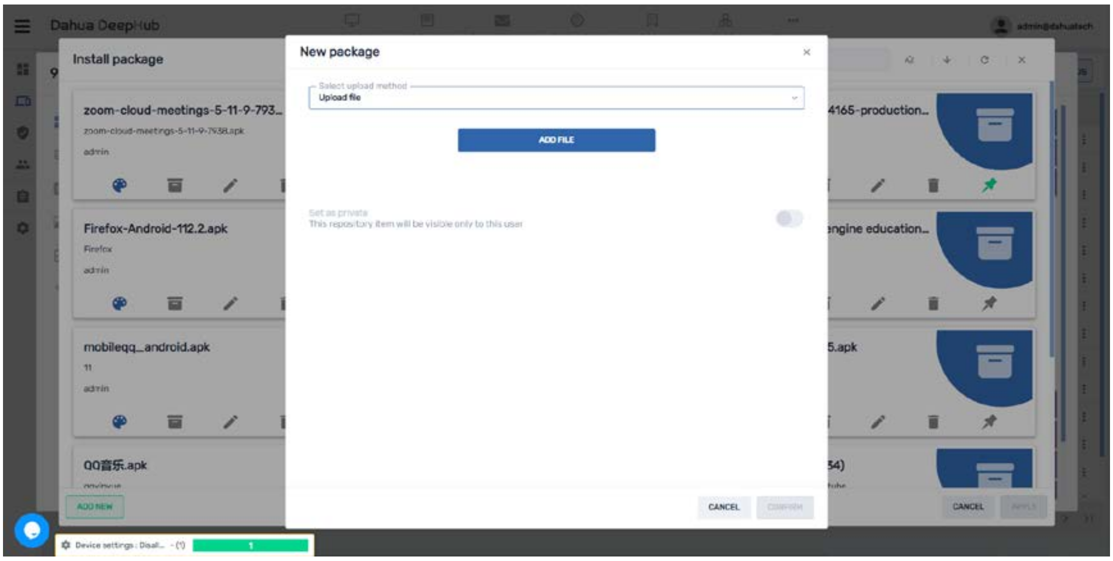
Installing applications remotely to one or many devices is done by creating an "Install Package" repository.

Click on the "Repositories actions" button on the left side menu and choose "Packages" from the dropdown menu. A new window will open with a list of existing packages.




Dahua DeepHub
admin@dahuatech
Install package
Search
zoom-cloud-meetings-5-11-9-793...
microsoft-teams-1416-1-0-0-202...
broadcast-2.5.8.14165-production...
Firefox-Android-112.2.apk
Google Earth (V9.180.0.1)
Four stroke Otto engine education...
mobileqq_android.apk
deephub_Class_main_deephub_...
云标Player_V5.0.5.apk
QQ音乐.apk
QQMusic72282.apk
YouTube (V17.39.34)
ADD NEW
CANCEL
APPLY

Click on the "ADD NEW" button to add a new package.



New package

Select upload method: Upload file

Set as private
This repository item will be visible only to this user

Select the package source

This option will deduct the size of the installation package from your total account server storage space.

Supported installation package formats

Android installation packages are APK files

Package Name and Description

Give a name that best describes the installation package. This can be any name you desire; it does not have to be the name of the file. A description will make it easier for other users to understand what this installation package does.

Set as Private

In a multi-tenancy environment, where there are several users on your domain, you may want to set the package you create as "private" to make it visible only to your account. If not selected, all domain users will have access to this installation package.

12 Workflow Repository

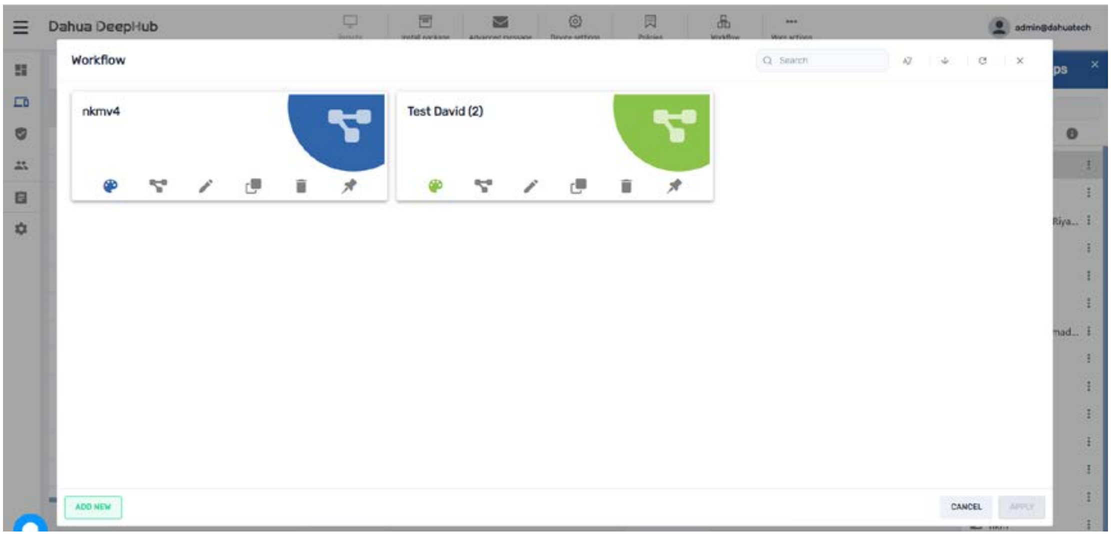
Combining several actions and commands together can save you time and allow multiple actions in one task instead of applying each command one by one.

This method can also be applied to a newly enrolled device for quick “onboarding”.

Creating a new workflow

On the left side main menu, click on “Repositories”, and from the dropdown menu select “Workflow”. A new window will open, showing all existing workflows.

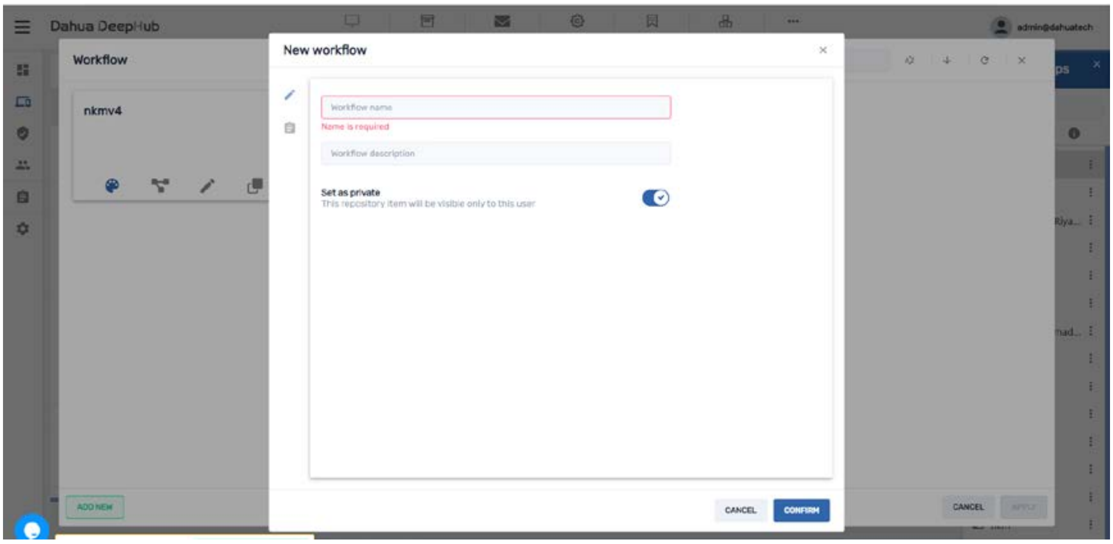
Click on the “ADD NEW” button to add a new workflow.

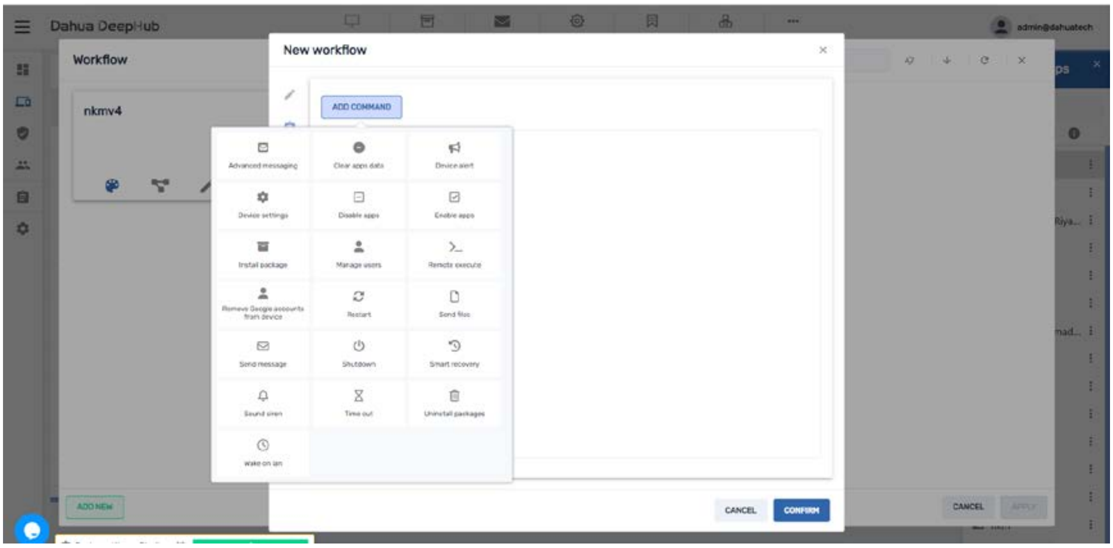


Name the workflow and give it a description. In the “Description” write the different actions and steps that the policy contains.

Add a workflow step (item)

Click on the “ADD COMMAND” icon and select an action from the list.



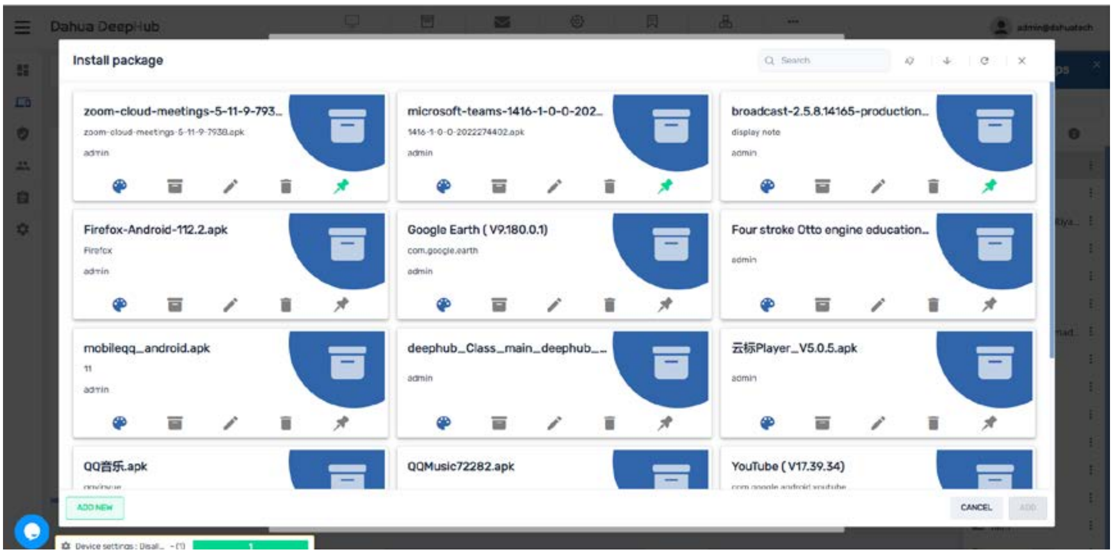


In the example above we selected the "Install Package" repository, so all packages on the repository show up. You may select existing packages or add new.

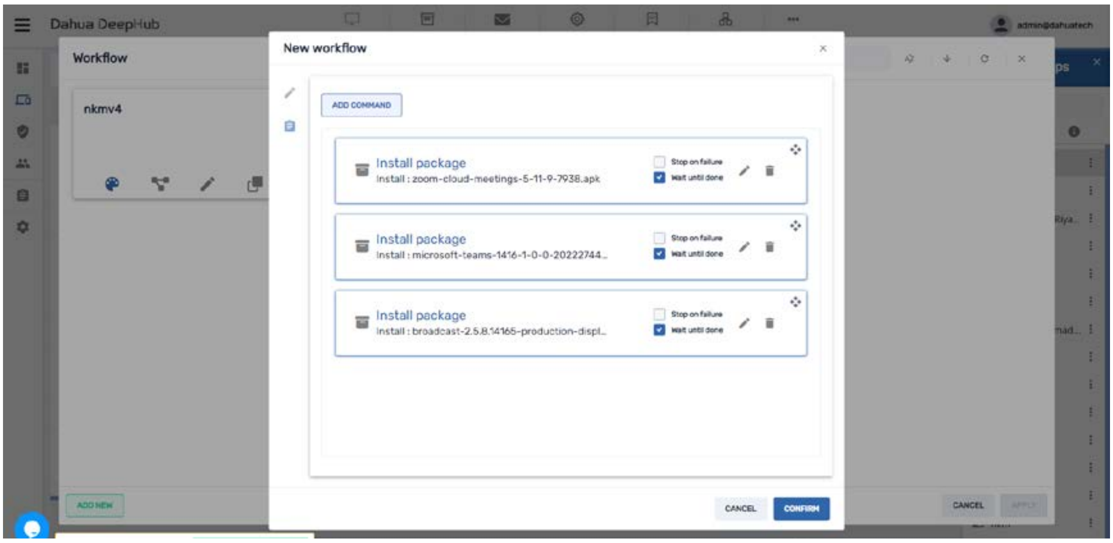
Select a package and click on the "ADD" button to add it to the sequence. You may add several packages, then click on the "CLOSE" button to close the packages repository window.

Notice the message on the bottom right side indicating that the item was added.

Repeat the "add commands to workflow" with all desired commands.


Dahua DeepHub
admin@dahuatech
Install package
Search
zoom-cloud-meetings-5-11-9-793...
zoom-cloud-meetings-5-11-9-7938.apk
admin
microsoft-teams-1416-1-0-0-202...
1416-1-0-0-2022274402.apk
admin
broadcast-2.5.8.14165-production...
display note
admin
Firefox-Android-112.2.apk
Firefox
admin
Google Earth (V9.180.0.1)
com.google.earth
admin
Four stroke Otto engine education...
admin
mobileqq_android.apk
11
admin
deephub_Class_main_deephub_...
admin
云標Player_V5.0.5.apk
admin
QQ音乐.apk
QQMusic72282.apk
YouTube (V17.39.34)
com.google.android.youtube
ADD NEW
CANCEL
ADD
Device settings : Disal...

We now have a workflow with several packages, a timeout and settings bundle.



New workflow

ADD COMMAND

Install package
Install : zoom-cloud-meetings-5-11-9-7938.apk
□ Stop on failure
☑ Wait until done

Install package
Install : microsoft-teams-1416-1-0-0-20222744...
□ Stop on failure
☑ Wait until done

Install package
Install : broadcast-2.5.8.14165-production-displ...
□ Stop on failure
☑ Wait until done

CANCEL CONFIRM

Workflow steps configuration

☑ Wait until done

Wait for this step to finish before proceeding to the next step. This step can fail or succeed, and the workflow will continue.

☑ Stop on failure

Wait for this step to finish successfully before proceeding to the next step. If this step fails, the workflow will not continue.

✎ 🗑

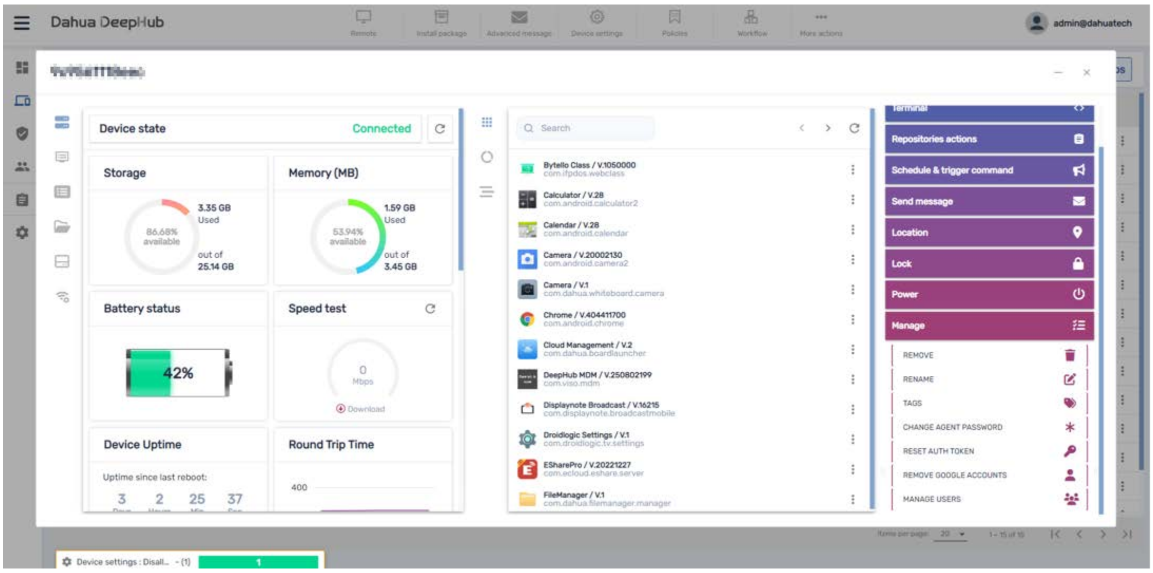
Edit or delete the workflow step.

✥

Move the workflow item step sequence up and down – before or after the current location.

13 Manage & App Usage Report

Manage – we added the option to Rename a device easily and Remove Google accounts or keep one



Dahua DeepHub

[redacted]

Device state: Connected

Storage: 3.35 GB Used, 86.68% available, out of 25.14 GB

Memory (MB): 1.59 GB Used, 53.94% available, out of 3.45 GB

Battery status: 42%

Speed test: 0 Mbps, Download

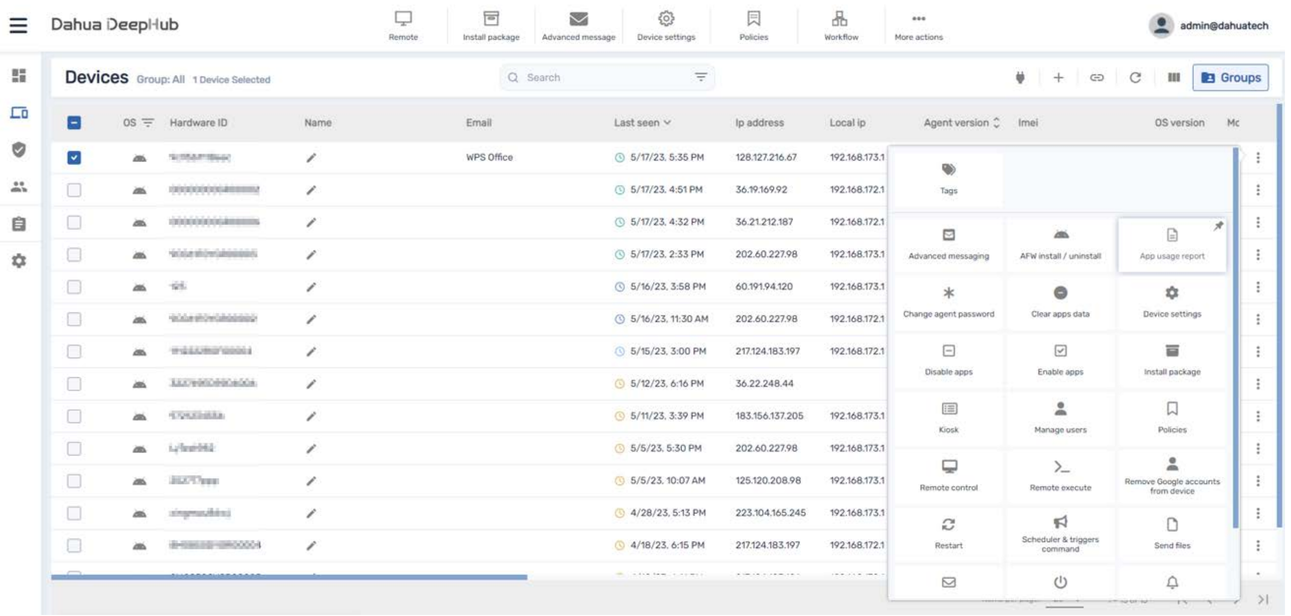
Device Uptime: Uptime since last reboot: 3 Days 2 Hours 25 Min 37 Sec

Round Trip Time: 400

- Bytello Class / V.1050000 — com.ifpdos.webclass
- Calculator / V.28 — com.android.calculator2
- Calendar / V.28 — com.android.calendar
- Camera / V.20002130 — com.android.camera2
- Camera / V.1 — com.dahua.whiteboard.camera
- Chrome / V.404411700 — com.android.chrome
- Cloud Management / V.2 — com.dahua.boardlauncher
- DeepHub MDM / V.250802199 — com.viso.mdm
- Displaynote Broadcast / V.16215 — com.displaynote.broadcastmobile
- Droidlogic Settings / V.1 — com.droidlogic.tv.settings
- ESharePro / V.20221227 — com.ecloud.eshare.server
- FileManager / V.1 — com.dahua.filemanager.manager

App usage report - enabling you to run reports, see trends according to filtered dates and make fact-based decisions and optimize your device usage making it a true business asset. We added the option to search apps, sort and export to CSV to work offline.

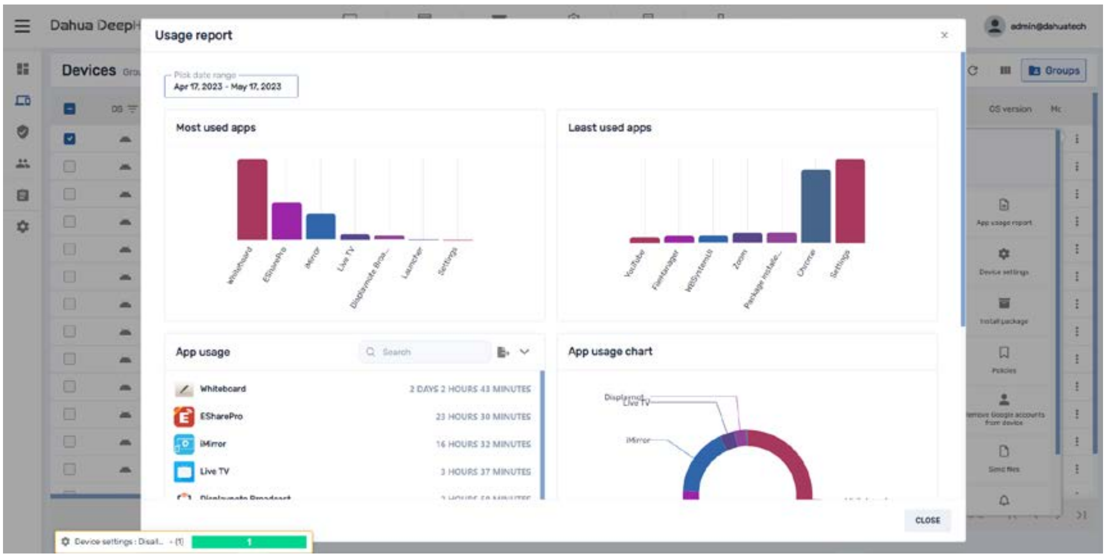
In addition, all fields in the device section of the report can be sorted just click on the relevant column



Dahua DeepHub

Devices Group: All 1 Device Selected

	OS	Hardware ID	Name	Email	Last seen	Ip address	Local ip
☑		[redacted]		WPS Office	5/17/23, 5:35 PM	128.127.216.67	192.168.173.1
☐		[redacted]			5/17/23, 4:51 PM	36.19.169.92	192.168.172.1
☐		[redacted]			5/17/23, 4:32 PM	36.21.212.187	192.168.172.1
☐		[redacted]			5/17/23, 2:33 PM	202.60.227.98	192.168.173.1
☐		[redacted]			5/16/23, 3:58 PM	60.191.94.120	192.168.173.1
☐		[redacted]			5/16/23, 11:30 AM	202.60.227.98	192.168.172.1
☐		[redacted]			5/15/23, 3:00 PM	217.124.183.197	192.168.172.1
☐		[redacted]			5/12/23, 6:16 PM	36.22.248.44	
☐		[redacted]			5/11/23, 3:39 PM	183.156.137.205	192.168.173.1
☐		[redacted]			5/5/23, 5:30 PM	202.60.227.98	192.168.173.1
☐		[redacted]			5/5/23, 10:07 AM	125.120.208.98	192.168.173.1
☐		[redacted]			4/28/23, 5:13 PM	223.104.165.245	192.168.173.1
☐		[redacted]			4/18/23, 6:15 PM	217.124.183.197	192.168.172.1



Usage report

Pick date range: Apr 17, 2023 - May 17, 2023

Most used apps

Least used apps

App usage

Whiteboard	2 DAYS 2 HOURS 43 MINUTES
ESharePro	23 HOURS 30 MINUTES
iMirror	16 HOURS 32 MINUTES
Live TV	3 HOURS 37 MINUTES

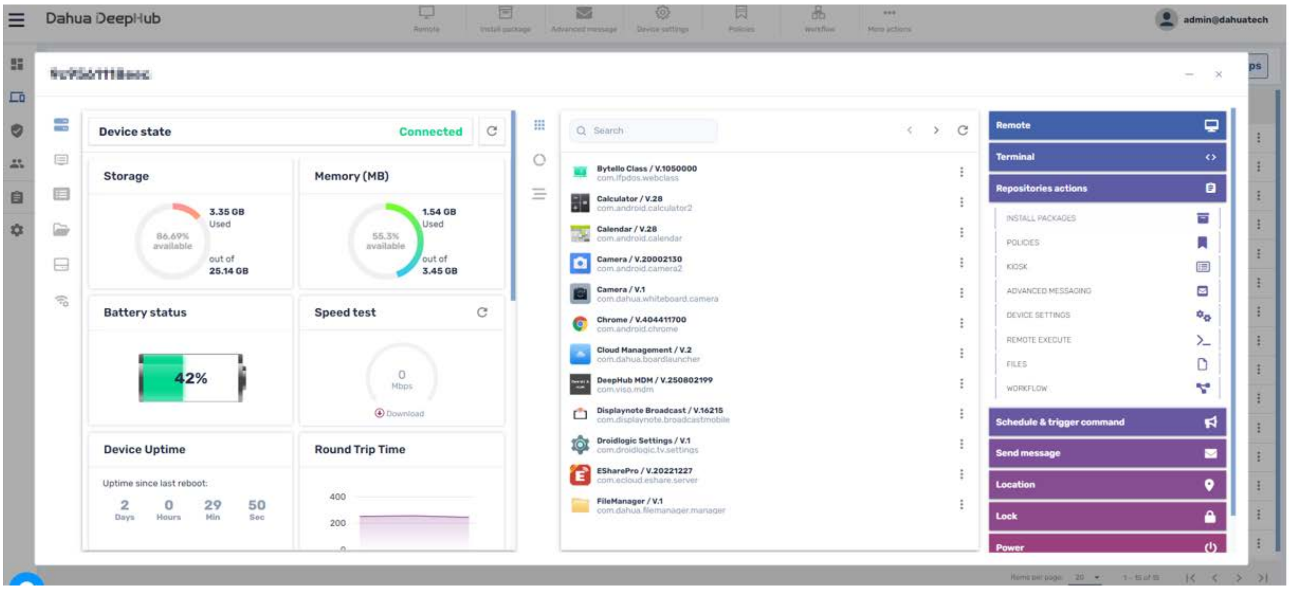
App usage chart

14 Apply Commands and Operations on Devices

One of the main purposes of a device management platform is to apply commands and operate the devices. Applying commands to devices can be done on a single device, a group of devices, selected devices or all the devices on your account at once.

Applying commands to a single device

Applying commands to a single device is done on the device control panel. Click on the device you would like to apply the command to, on the right you will see the list of commands, select the desired command. When working on a single device, all commands are immediate and cannot be scheduled. There are some commands that are unique to a 1 to 1 operation, such as "Remote control" that can only be started from the device control panel



Group-level commands

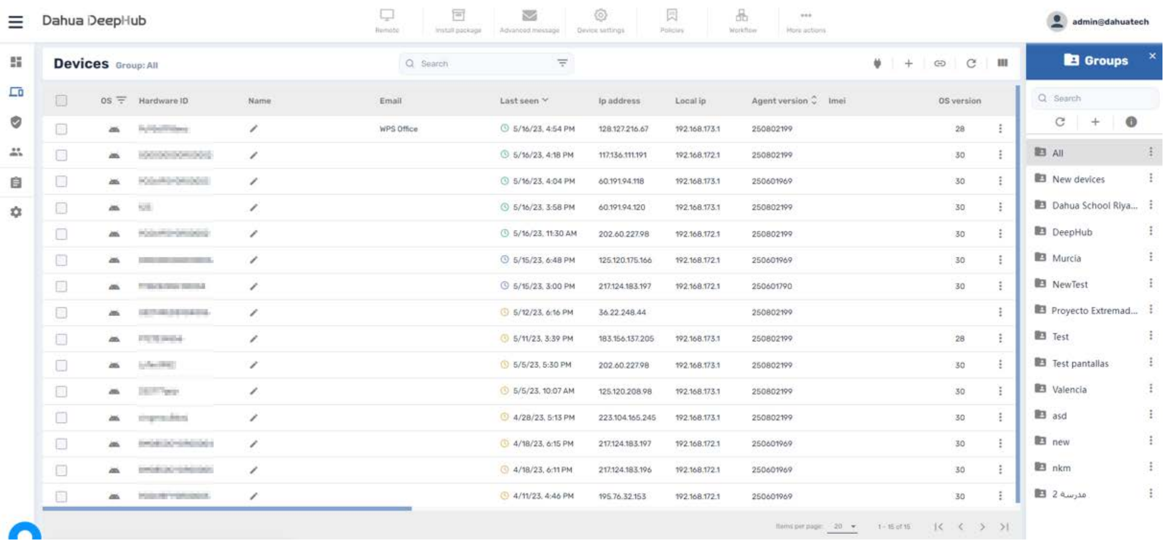
Most of the commands that can be applied to a single device can also be applied to a group. Here is a list of group-level commands you can apply on more than one device:

Function	Repository	Ad-hoc	Comments
Install Packages	X		
Send Files	X		
Advanced Messaging	--		
Settings	--		
Remote Exec	X		
Smart Recovery	X		
Dep Apple Profile			

Function	Repository	Ad-hoc	Comments
Workflow	X		
Restart	X	X	Windows only
Wake On Lan	--	X	
Tags	--	X	
Policies	X		
Shutdown	--	X	
Send Message	--	X	
Sound Siren	--	X	
Change Agent Password	--	X	
Uninstall Packages		X	
Enable Apps			
Disable Apps			
VPP Install/Uninstall			
App Usage Report		X	
Trigger Command		X	
Export to CSV			
Remove Account From Device	--		
AFW Install/unInstall			

Applying commands to a group

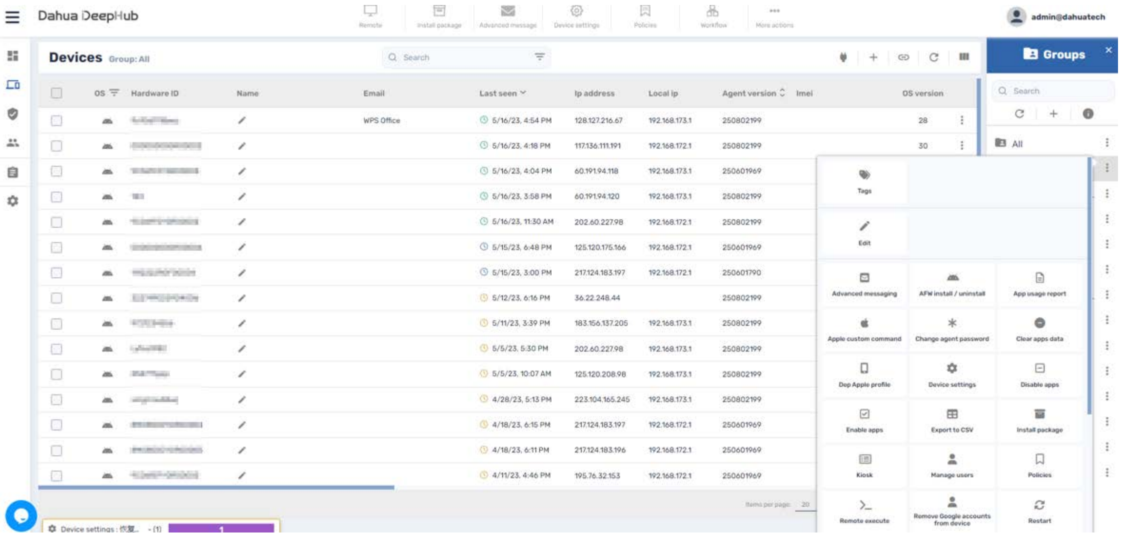
Choose a group you would like to apply the command on and click on "Actions" (will appear on the upper right side of the screen once selecting a device) represented by a vertical 3 dots line. Select the relevant command from the menu and apply it to the group.



OS	Hardware ID	Name	Email	Last seen	Ip address	Local ip	Agent version	Imei	OS version
	[redacted]		WPS Office	5/16/23, 4:54 PM	128.127.216.67	192.168.173.1	250802199		28
	[redacted]			5/16/23, 4:18 PM	117.136.111.191	192.168.172.1	250802199		30
	[redacted]			5/16/23, 4:04 PM	60.191.94.118	192.168.173.1	250601969		30
	[redacted]			5/16/23, 3:58 PM	60.191.94.120	192.168.173.1	250802199		30
	[redacted]			5/16/23, 11:30 AM	202.60.227.98	192.168.172.1	250802199		30
	[redacted]			5/15/23, 6:48 PM	125.120.175.166	192.168.172.1	250601969		30
	[redacted]			5/15/23, 3:00 PM	217.124.183.197	192.168.172.1	250601790		30
	[redacted]			5/12/23, 6:16 PM	36.22.248.44		250802199		
	[redacted]			5/11/23, 3:39 PM	183.156.137.205	192.168.173.1	250802199		28
	[redacted]			5/5/23, 5:30 PM	202.60.227.98	192.168.173.1	250802199		30
	[redacted]			5/5/23, 10:07 AM	125.120.208.98	192.168.173.1	250802199		30
	[redacted]			4/28/23, 5:13 PM	223.104.165.245	192.168.173.1	250802199		30
	[redacted]			4/18/23, 6:15 PM	217.124.183.197	192.168.172.1	250601969		30
	[redacted]			4/18/23, 6:11 PM	217.124.183.196	192.168.172.1	250601969		30
	[redacted]			4/11/23, 4:46 PM	195.76.32.153	192.168.172.1	250601969		30

Apply commands to selected devices

Manually selecting devices from the list will activate the “Actions” menu similar to the group “Actions” menu.

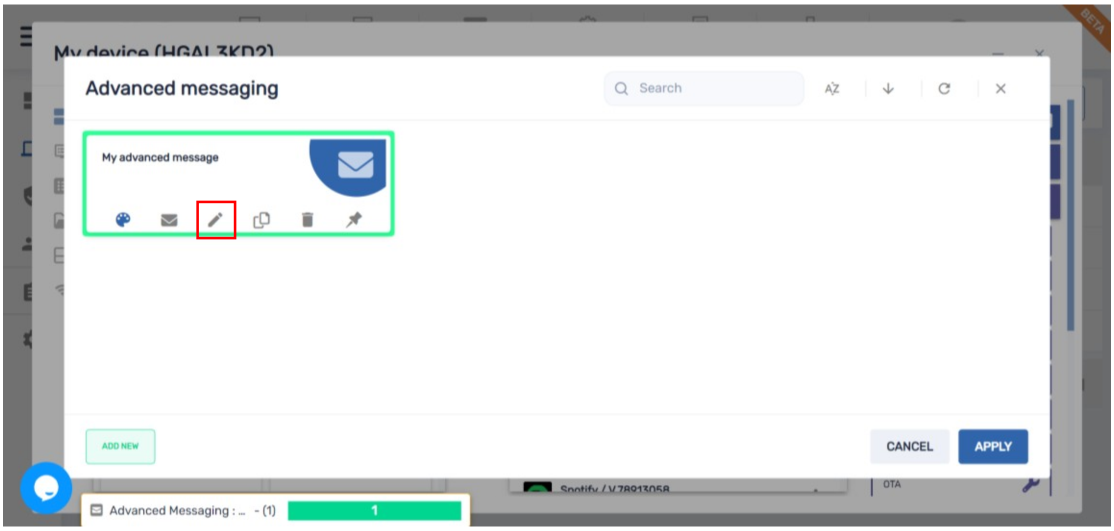


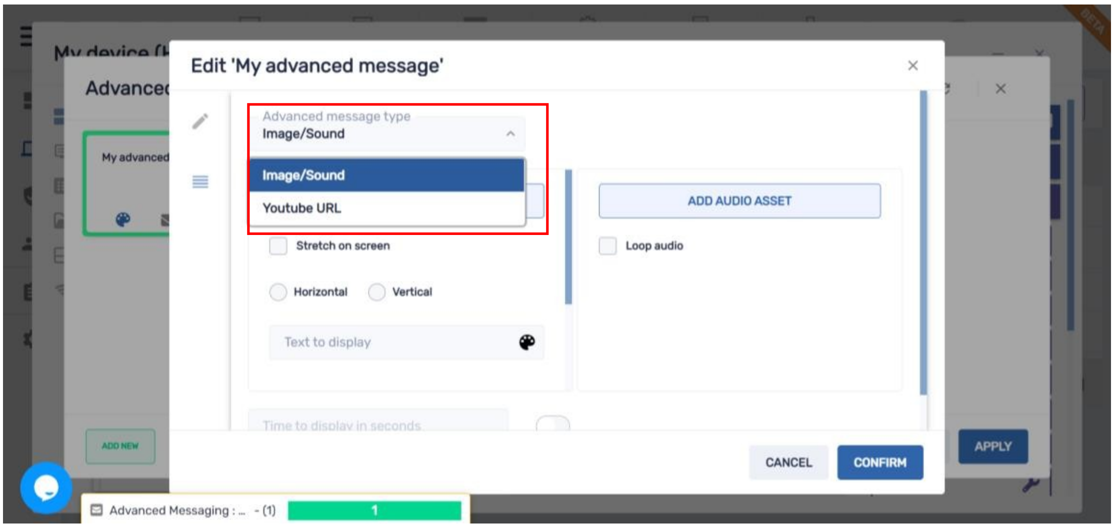
OS	Hardware ID	Name	Email	Last seen	Ip address	Local ip	Agent version	Imei	OS version
	[redacted]		WPS Office	5/16/23, 4:54 PM	128.127.216.67	192.168.173.1	250802199		28
	[redacted]			5/16/23, 4:18 PM	117.136.111.191	192.168.172.1	250802199		30
	[redacted]			5/16/23, 4:04 PM	60.191.94.118	192.168.173.1	250601969		
	[redacted]			5/16/23, 3:58 PM	60.191.94.120	192.168.173.1	250802199		
	[redacted]			5/16/23, 11:30 AM	202.60.227.98	192.168.172.1	250802199		
	[redacted]			5/15/23, 6:48 PM	125.120.175.166	192.168.172.1	250601969		
	[redacted]			5/15/23, 3:00 PM	217.124.183.197	192.168.172.1	250601790		
	[redacted]			5/12/23, 6:16 PM	36.22.248.44		250802199		
	[redacted]			5/11/23, 3:39 PM	183.156.137.205	192.168.173.1	250802199		
	[redacted]			5/5/23, 5:30 PM	202.60.227.98	192.168.173.1	250802199		
	[redacted]			5/5/23, 10:07 AM	125.120.208.98	192.168.173.1	250802199		
	[redacted]			4/28/23, 5:13 PM	223.104.165.245	192.168.173.1	250802199		
	[redacted]			4/18/23, 6:15 PM	217.124.183.197	192.168.172.1	250601969		
	[redacted]			4/18/23, 6:11 PM	217.124.183.196	192.168.172.1	250601969		
	[redacted]			4/11/23, 4:46 PM	195.76.32.153	192.168.172.1	250601969		

15 Advanced Messages

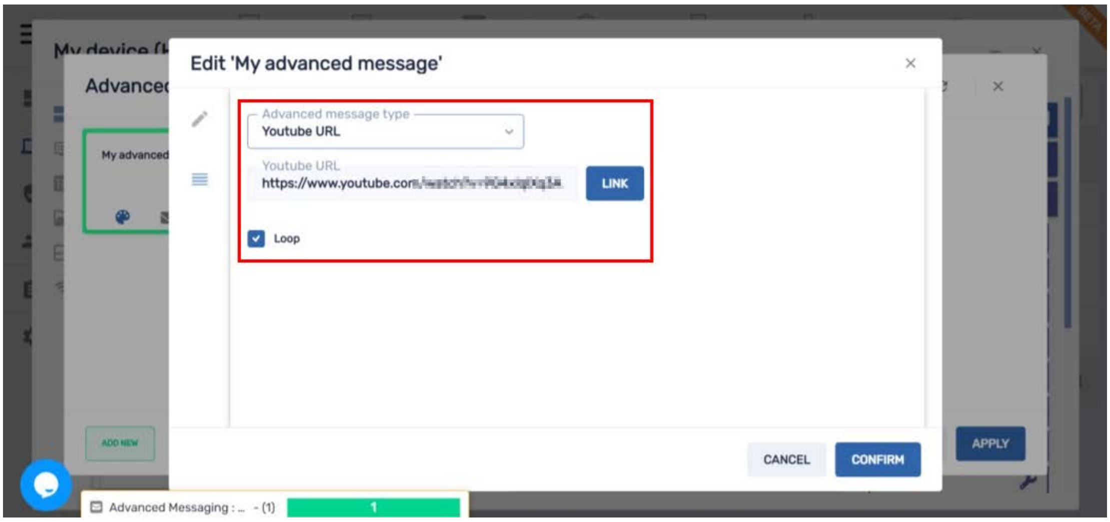
Advanced messages are a great way to interact with users for any purpose using engaging messages that may contain text, sound and image. In addition, you can also time out a message and trigger it according to time, geo, network or via a 3rd party API like emergency systems

And now advanced messages also support YouTube videos that can be played in a loop and soon to come they will be clickable (HTML) as well.





Advanced message type: Image/Sound



Edit 'My advanced message'

Advanced message type: Youtube URL

Youtube URL: https://www.youtube.com[redacted]

☑ Loop

16 Authentication Token

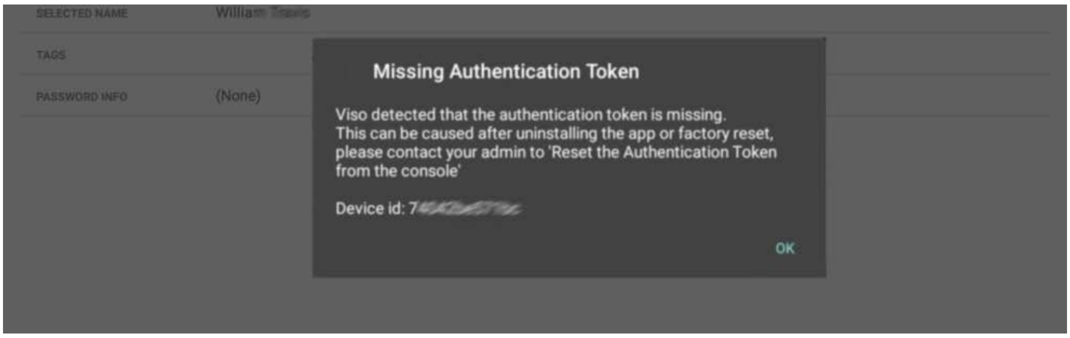
Overview

For security reasons, the first handshake between a device and the VISO server will generate a unique authentication token. This token is stored on the server and on the device.

"Missing Authentication Token"

When a device losses the authentication token, it will fail to register with the server. This is usually a result of an uninstall and new installation, factory reset, data wipe or any case the app data is cleared.

When you enroll the device again you will see the following message on the wizard summary screen when you click "enroll"



SELECTED NAME Willia[redacted]

TAGS

PASSWORD INFO (None)

Missing Authentication Token

Viso detected that the authentication token is missing.
This can be caused after uninstalling the app or factory reset,
please contact your admin to 'Reset the Authentication Token
from the console'

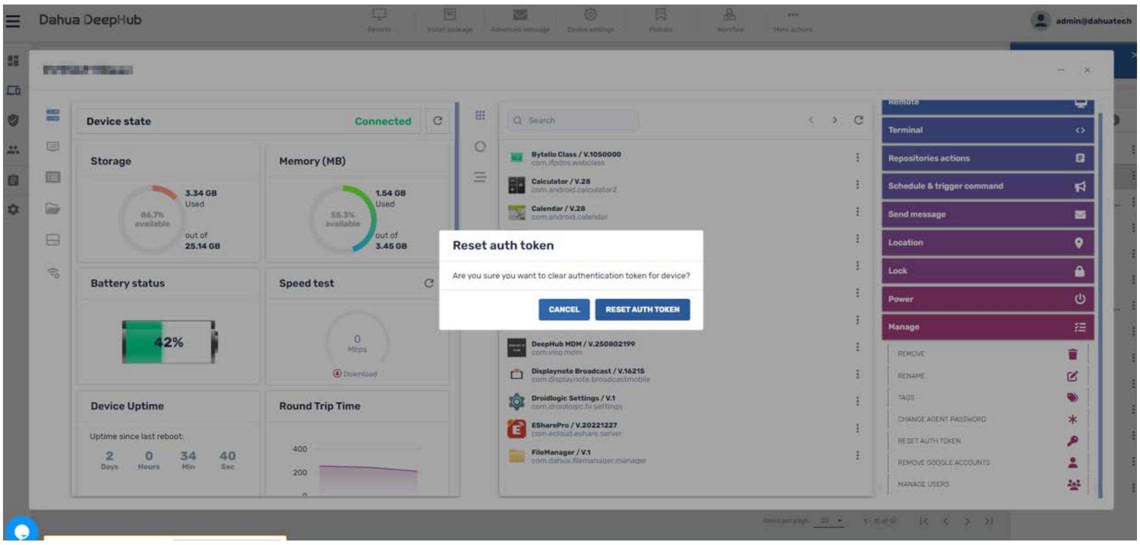
Device id: 7[redacted]

OK

Reset Authentication Token

Go to the specific device control panel, on the domain it was originally enrolled. On the right side menu, click on the "Manage" tab, And from the dropdown menu select "RESET AUTH TOKEN".

When done, retry finishing the enrollment process and it will succeed.



Reset auth token

Are you sure you want to clear authentication token for device?

CANCEL RESET AUTH TOKEN

17 How to translate DeepHub language XML files

Translating the language file to other languages is simple

1. Edit the XML file using notepad++ or similar text editor

2. Translate the XML value for every line in between > Here < the XML tags. Simply overwrite with the translated value:

Original:

Translate Me

Translated:

Me Translated

3. Save the XML file in UTF-8 encoding.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords.
   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.
2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188